

User Management Pack™ 365 SP Edition

Installation and Administration

Version 8.0.450



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: February-06-2024

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>.

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>.

Stay in the Loop with AudioCodes



Related Documentation

Document Name
User Management Pack 365 SP Edition Release Notes
User Management Pack 365 SP Edition Upgrade

Document Revision Record

LTRT	Description
26382	Added Section: Location-Based Routing configuration and scripts; Managing the Replication cycle; Managing UMP-365 User Licenses
26383	Update to Section "Creating a Service Account"
26384	Correction to Installation ISO file package link in Section "Installing the Prerequisites"
26385	Correction to "Before Upgrading UMP-365"
26386	Added Section: Customizing Global License Factors; Filtering Data; Configuring Global License Settings; Onboarding Prerequisites including updates for Token-based authentication Updates to SBC Onboarding scripts; Managing User Licenses; Provisioning Users; LifeCycle Management; Managing Templates; Configuring Online Voice Routing; Customer Admins; Initial Access to UMP-365 and Assigning Customer Admins; Onboarding; Installing the Prerequisites
26387	Added Section UMP-365 Server Memory Calculation; Setting Up Hosted Essentials Customer
26388	Update to End Customer Onboarding Prerequisites (Security Settings).

Table of Contents

1	Introduction	1
Part I		2
Preinstallation		2
2	Installation Requirements	3
	Memory and Disk Space Calculations	4
	UMP-365 Server Disk Space Calculations	4
	UMP-365 Server Memory Calculations	5
	Change SQL Maximum Replication Cycles	6
	Limit SQL Memory Consumption	6
	Maximum Memory Calculation for SQL Example	7
3	Installing SSL Certificates on UMP Windows Server	8
4	UMP Networking and Firewall Configuration	17
	UMP Firewall Configuration	17
	VPN Configuration (Optional)	18
	OVOC Service Provider Firewall Configuration	20
5	SQL License Guidelines	25
6	Verifying Anti-Virus Access Scanning	27
	SQL	27
	ASP.NET	27
	Other Files and Directories	28
7	Creating UMP Service Account	29
Part II		44
Installation and Setup		44
8	Installing the Prerequisites	45
9	Installing UMP SP	46
	Adding SSL Certificate to IIS Website	47
10	Networking	51
	Configuring UMP Interface for WebSocket Tunnel (Cloud Architecture Mode)	51
	Configuring WebSocket Tunnel (Cloud Architecture Mode) on OVOC	53
	Configuring SBC	55
	Configuring HTTPS SSL Connection to OVOC Public IP	58
	Configuring Connection to OVOC Azure Private IP	61
	Managing Alarms	63
11	Multitenant Portal Licensing	65
	Installing the Multitenant License	65
12	Configuring Invitation Settings	67

13	Configuring Email Settings	69
14	Setting up Fully Automatic DNS Provisioning	70
	Registering DNS Application (Service Provider Tenant)	70
	Creating A Records for SBC Devices	74
	Assign Access Control	77
	Configure DNS API	82
15	Configuring Microsoft Teams Direct Routing SBC	86
16	Create Registration for Customer Administrators	87
17	Deploy Synchronization Application	91
	Deploy Synchronization Application (Customer Subscription)	96
18	Accessing UMP 365 with Service Provider Credentials	105
	Tenants Global View	108
	Configuring Number of Licensed Users	110
	Adding SBC Devices for New Site Locations	111
	Queue Replication	112
	Undo Deployment	113
	Upgrading Customer	113
19	Updating Service Provider Logos	116
Part III		117
Upgrade		117
20	UMP-365 Upgrade	118
21	Before Upgrading UMP-365	119
	Configure Firewall	121
	Backing up UMP-365 – Disk Snapshot	121
	Compiling List of Password Authenticated Customers	125
	Stop wyUpdate Processes	126
	Additional SysAdmin Verifications	130
22	Upgrading Main UMP-365 Tenant	131
23	Upgrading Customer Tenant	139
24	Post Upgrade Actions	143
	Restoring UMP Snapshot	143
	Verifying Tenant Admin Authentication	147
	Upgrading M365 Connection to Token Authentication	148
	Switching to Token Authentication	153
	Updating Scripts	159
	Verifying Component Statuses	159
	Device Status	162
	Updating SQL Server	166
	SBC Dialplan Verification	166

Part IV	167
Service Provider Management	167
25 Day Two Actions using the Multitenant Portal	168
Configuring Global License Settings	168
Managing Onboarding Script Templates	170
SBC Direct Routing Scripts	171
sbc-scenario7	172
sbc-add-prefix	179
sbc-scenario7 Cleanup	184
add-ipx-user	185
sbc-remove-prefix	190
M365 Template Scenarios	190
Default M365 Tenant Onboarding Script	191
Default M365 Tenant Cleanup Script	193
M365 Onboarding with Location-based Routing	194
M365 onboarding with Location-Based Routing and Custom Networks	201
Onboarding Wizard Defined Variables	208
Customer Variables	210
Scenario Scripts Templates Page	213
Script Scenario Comparison	214
Script Templates Updates	215
SQL DBA Script Pairing	219
Managing Security Settings	225
Customer Admins	225
Customer Invitations	225
Authentication Status	228
UMP Service Settings	234
Managing SBC Devices	235
Add SBC Devices	236
Show SBC Site Locations	237
Show Prefixes	239
Download Dial Plan from Managed SBC (Import Customer)	240
Queued Tasks	244
Managing the Replication Cycle	246
Part V	248
Onboarding a new Tenant	248
29 Introduction	249
30 Onboarding Prerequisites	250
Register End Customer Tenant DNS Sub domains	250
Setup Two-step Provisioning	250
Manual Provisioning	252
Registering Customer Tenant Subdomain	252

Activating the Customer Domain	258
End Customer Prerequisites	263
Verify License Availability	263
Create Customer Administrator Service Account	265
Assign Administrator Roles to IT Administrator	269
Configure Additional Security Settings	274
31 Onboarding Customers	282
Onboarding with Hosted Essentials	282
Setting Up Hosted Essentials Customer	288
Onboarding with Hosted Essentials +	290
Request Consent from End Customer	294
Onboarding with Default Global Admin	295
Onboarding with Tenant-Defined Service Account	311
Onboarding with both M365 Default Routing and SBC Configuration	333
Fully Automatic DNS Provisioning	341
Two-step DNS Provisioning	349
Onboarding with only SBC Configuration	356
Onboarding with Hosted Pro	361
Request Consent from End Customer	364
Secure Token Connection with Global Admin Credentials	365
Grant Consent using only Token-based Authentication (Global Admin)	369
Onboarding with both M365 Default Routing and SBC Configuration	383
Fully Automatic DNS Provisioning	393
Two-step DNS Provisioning	411
Onboarding with only SBC Configuration	418
Part VI	424
Second Day Operations	424
32 Day Two Management using Customer Tenant Portal	425
Initial Access to UMP-365 and Assigning Customer Admins	425
Customer Portal Direct Routing License Model Menus	428
Hosted Essentials	429
Hosted Essentials Plus	429
Hosted Pro	430
Provisioning with Direct Routing	432
Set Usage Location	439
Voice Routing Scenarios	442
Manually Provisioning Users	443
Manually Assigning Phone Numbers to Users	443
Manually Applying M365 User Policies	446
Lifecycle Management	451
Managing Unassigned Number Ranges	451
Creating a Bundle	454
Managing Templates	459

Upload M365 Users from File and Attach to Template	463
Export CSV	467
Create New Entry Manually	469
Binding Templates to Security Groups	469
Location-Based Routing	471
Location-Based Routing Configuration	472
Adding Network Sites	473
Adding Trusted Sites	478
Configure Network Topology in Microsoft Teams	481
Location-Based Network Sites	481
Location-Based Trusted Sites	484
Change Users Policies to Prevent Toll Bypass (mandatory)	487
Configure User Policy Manually	487
Configure User Policy Automatically	490
Configuring Online Voice Routing	495
PSTN Usage	495
Voice Routing Policy	496
Add Voice Routing Policy	497
Edit Voice Routing Policy	497
Delete Voice Routing Policy	498
Apply Routing Policy to Security Group	499
Voice Route	500
PSTN Gateways	501
Microsoft 365 Dial Plan and Normalization Rules	501
Reserving Customer Phone Numbers	507
Viewing Audit and Roll Back Historical Updates	507
Monitoring M365 Replication Actions Queue	508
Securing Microsoft 365 Service Provider Access	511
Get-CsOnlineUser (Microsoft Teams PowerShell)	513
Grant Consent	514
Switching to Token Authentication	519
Switching to User Password	525
Managing Site Locations	530
Add SBC Site Locations	531
Manage SBC Prefixes	533
Upload Dial plan to SBC	536
Import IP-PBX Users	538
Managing User Licenses	540
Customizing Global License Factors	545
33 Multitier Admin Access	547
34 Browser Settings- IETF Same Site Cookie Attribute	549
35 Backup the Customer Tenant Database	551
36 Restore the Customer Tenant Database	554

Restoring to a Point in Time	557
37 AudioCodes SfB2Teams Migration Tool	560
	560
	560
	560
	560
Installing the Prerequisites	560
Create and Register the Azure App	561
	562
Running SfB2Teams Application	566
ARM Auto Call Routing to Teams	569
38 Renewing Expired Tokens	571
39 SQL Server Configuration	583
Setup Microsoft SQL Server for SBC	583
SQL Server Database Updates	584
Optional SQL Script Updates	584
Updates for Backend SQL Server	586
Backup All Databases	587
Configure SQL Server for Enhanced Capacity	588

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.

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.



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

Part I

Preinstallation

2 Installation Requirements

The following table describes the Base Configuration for up to 100 Tenants for Hosted Pro and Hosted Essentials + models (Direct Routing and Operator Connect) with a single VM.

Table 2-1: Virtual Hardware Deployment Requirements

Deployment Size	Average Number of Users per Customer	Maximum Number of Users per Environment	Azure Machine Size	CPU Processors	Disk Type	Memory RAM
Small	500	20	Standard D4s v5	4 cores with at least 2.4 GHz per core	Premium SSD with 100 GB available disk space for application*	16 GB
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*	32 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	128 GB

Deployment Size	Average Number of Users per Customer	Maximum Number of Users per Environment	Azure Machine Size	CPU Processors	Disk Type	Memory RAM
					for application*	

■ Operating System: Single Windows Server 2019-- US English

- *Allocate an additional 80 GB of disk space for the Windows Server 2022 -- US English Operating System.



Only Windows Server 2019 and 2022 – US English is supported.

■ For customers with ~100,000 users, synchronization will take 20 minutes.

■ Each tenant synchronizes every five minutes utilizing the QuickReplicationCycleWorker process.

■ An additional Backend SQL VM server can be optionally implemented for disaster recovery and security reasons for the customer tenant databases.

See also [Memory and Disk Space Calculations](#) below



The OS License is not included in the product pricing (UMP CPN). The basic CPN includes 1 CAL for SQL, for additional SQL Admins, customers must order separate licenses.

Memory and Disk Space Calculations

See the following calculations for UMP-365 disk space and memory:

■ See [UMP-365 Server Disk Space Calculations](#) below

■ See [UMP-365 Server Memory Calculations](#) on the next page

UMP-365 Server Disk Space Calculations

The table below describes the average number of CS Online Users according to customer size category.

Customer Size	Average Number of CS Online Users
Basic customer	~1,000
Medium customer	~5,000
Large customer	~50,000

The table below describes required SQL server database disk space according to customer size category.

Customer Size	Diskspace
Basic customer	~1 GB
Medium customer	~5 GB
Large customer	~10 GB

The table below describes disk space reservation for UMP-365 software.

Description	Diskspace
Folder reservation per customer (with log files)	~2 GB
ACS main folder (with log files)	~16 GB
Windows OS	~80 GB

■ conclusion disk space: ~100 GB for OS and application, plus an additional:

- ~3 GB per Basic customer
- ~7 GB per Medium customer
- ~12 GB per Large customer



The SQL database can be moved to different Backend server. In this case, calculate ~2 GB per customer on the UMP-365 server running the Web application (Frontend). See [Updates for Backend SQL Server](#) on page 586 and also refer to the Microsoft Best Practice documentation for setting up a backend server for SQL.

UMP-365 Server Memory Calculations

- See [Change SQL Maximum Replication Cycles](#) on the next page
- See [Limit SQL Memory Consumption](#) on the next page
- See [Maximum Memory Calculation for SQL Example](#) on page 7

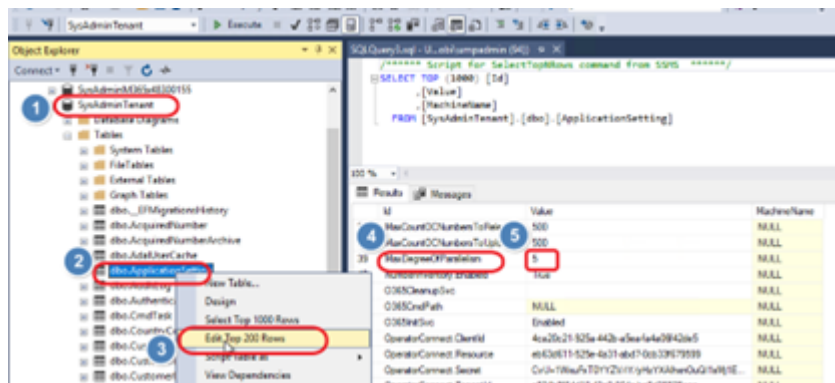
Change SQL Maximum Replication Cycles

UMP-365 Synchronization memory use is 2 GB per cycle for the UMP-365 processes. The maximum number of Simultaneous replication cycles in the UMP-365 database must be set to the number of cores -1. The procedure below describes how to set this configuration.

Perform this procedure in the **SQL Server Management Studio**.

➤ **Do the following:**

1. Connect to your database and select **SysAdminTenant**.
2. Open Tables and select **dbo.ApplicationSetting**.
3. Select **Edit Top 200 Rows**.
4. Add a new row type with the new Id: **MaxDegreeOfParallelism**.
5. Add the maximum number of server cores to -1.



Limit SQL Memory Consumption

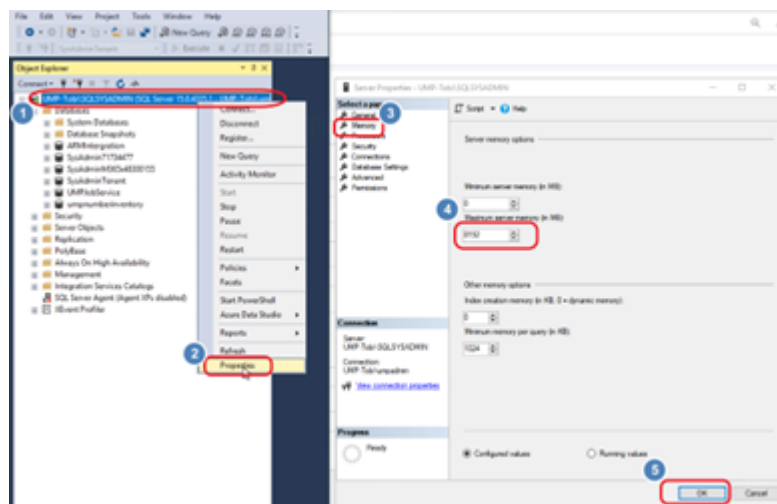
Limit the maximum memory consumption for SQL according to the table below.

Customer Size	Maximum SQL memory Usage
Small environment SQL	4 GB
Basic environment SQL	8 GB
Medium environment SQL	16 GB
Large environment SQL	32 GB

➤ **To set the SQL maximum server memory usage:**

1. Connect to your database, select **SQLSYSADMIN** and right-click.
2. Select **Properties**.
3. In server Properties, select **memory**.

4. Set it to the maximum value (maximum server memory – 8 GB for OS and 100 MB per customer). See table above.
5. Click **OK**.



Maximum Memory Calculation for SQL Example

The Maximum Memory calculation for SQL example described in the table below is for a Basic environment with a maximum number of 100 customers, where each customer cachesrv runs ~100 MB.

Memory Description	Memory Calculation
Server memory	32 GB
Memory used	
OS + IIS	8 GB
100 customers x 100 MB	~10 GB
Used memory for replication cycle	~6 GB
Residual Memory for SQL	
SQL server memory	8 GB

3 Installing SSL Certificates on UMP Windows Server

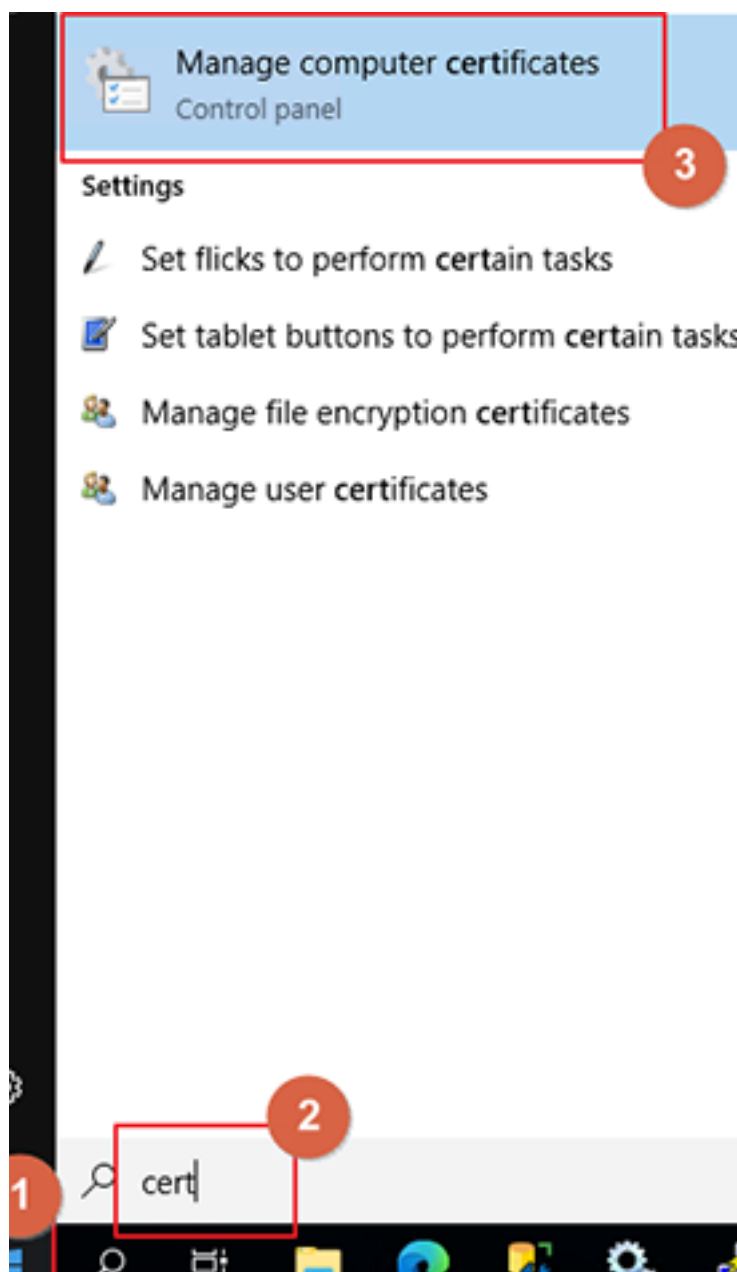
This section describes how to secure UMP HTTPS connections by installing an SSL certificate on the Windows server of the UMP platform.



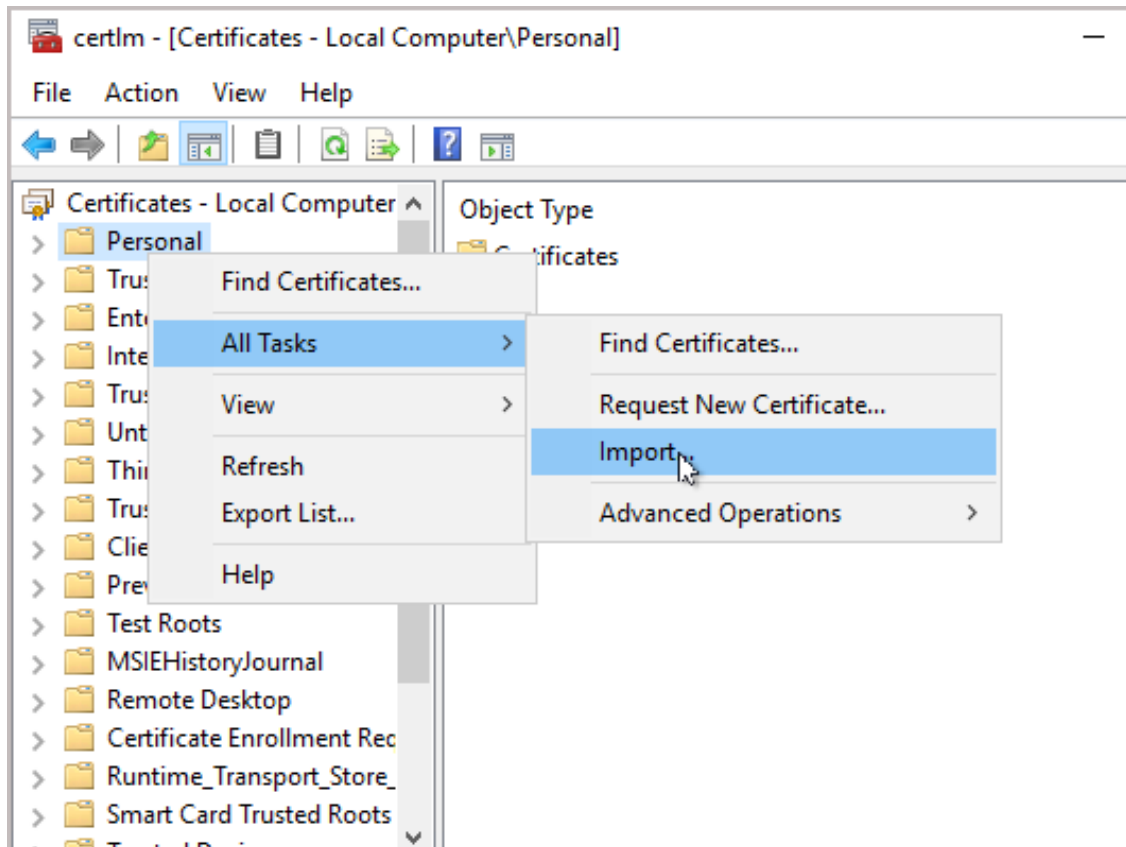
The UMP-365 can only be accessed over HTTPS.

➤ **To secure SSL connection with Azure:**

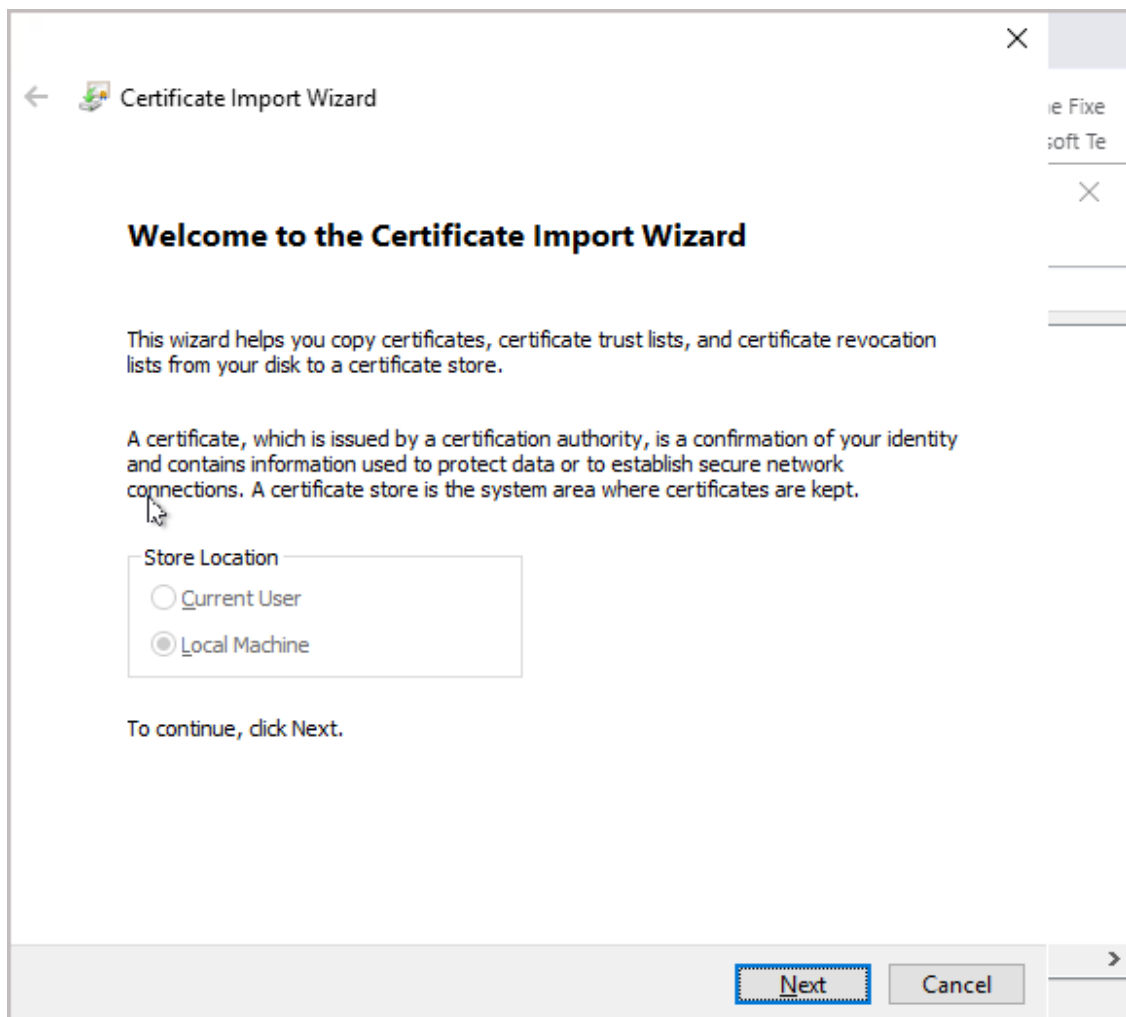
1. Make sure you have a valid SSL certificate with a private key available.
2. From the server open Certlm (Manager computer certificates), type cert at Windows start button and select Manage computer certificates.



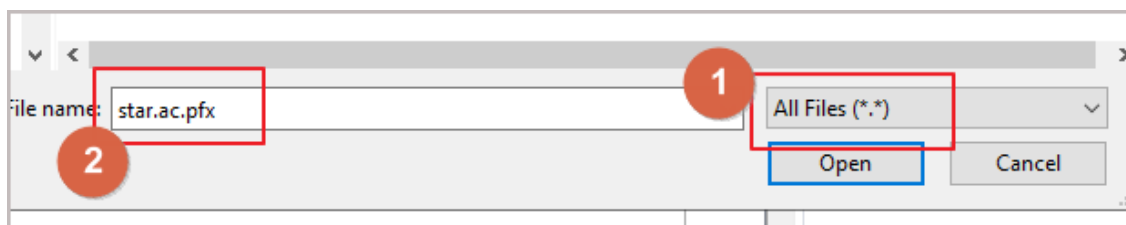
3. On Certlm select personal, right click and select All task then select Import.



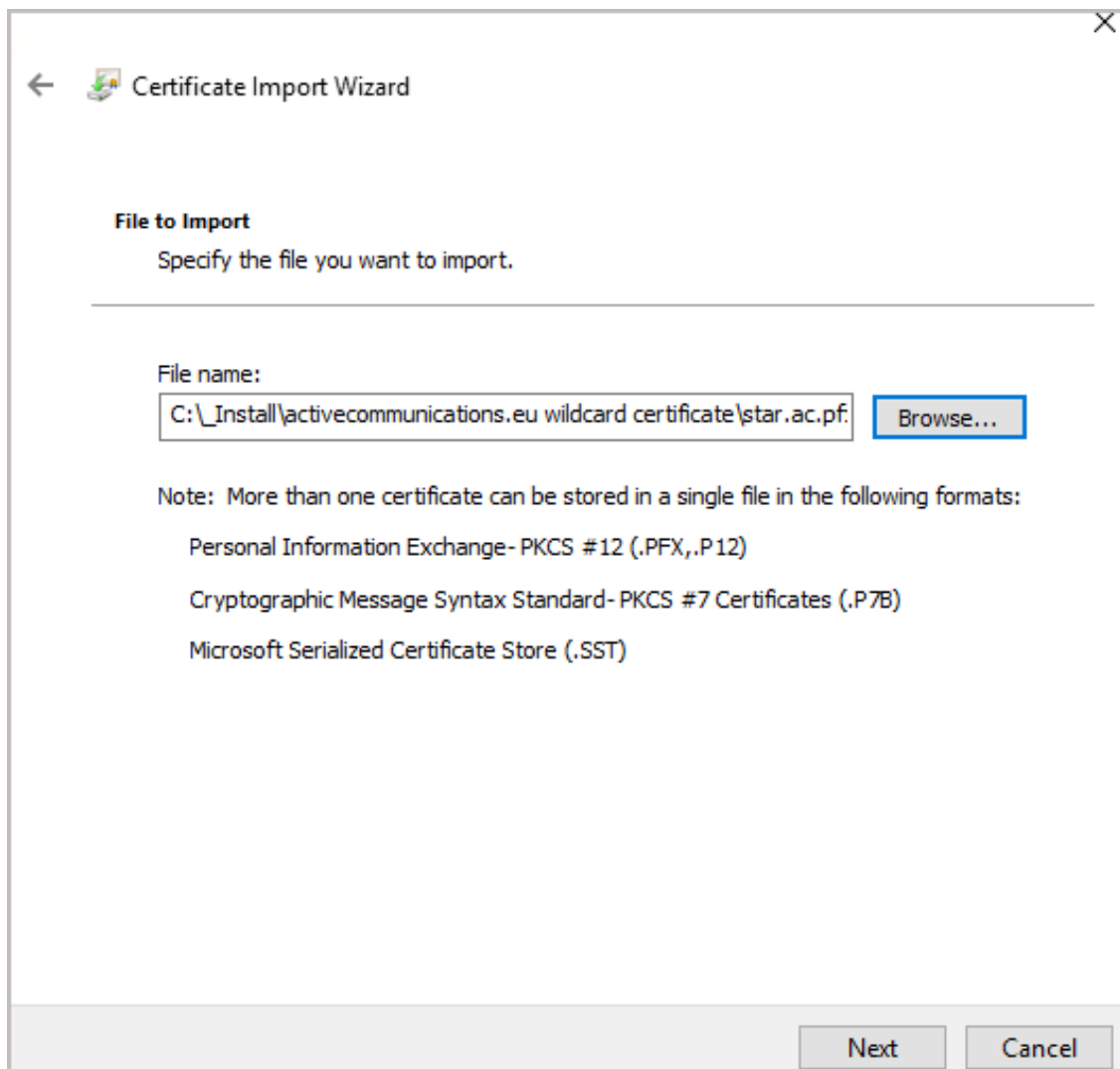
The Certificate Import Wizard is displayed.



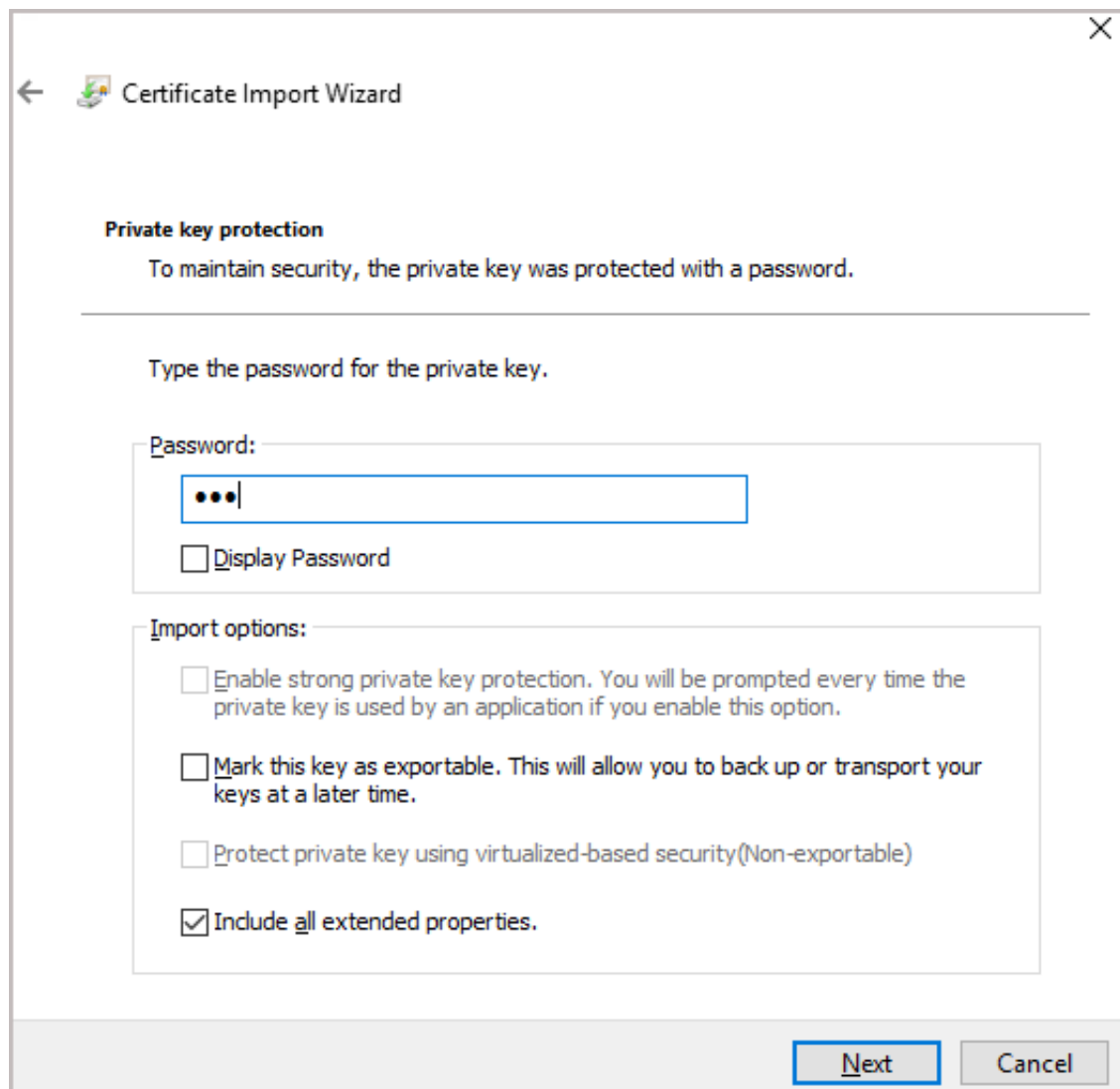
4. Click **Next** to continue.




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



6. Select **Next**.



The image shows a Windows dialog box titled "Certificate Import Wizard". It has a back arrow icon on the left and a close 'X' icon on the right. The main content area is titled "Private key protection" and contains the text "To maintain security, the private key was protected with a password." Below this, it says "Type the password for the private key." There is a text box labeled "Password:" containing three dots. Below the text box is a checkbox labeled "Display Password". Further down, there is a section titled "Import options:" with four checkboxes: "Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.", "Mark this key as exportable. This will allow you to back up or transport your keys at a later time.", "Protect private key using virtualized-based security(Non-exportable)", and "Include all extended properties." The "Include all extended properties." checkbox is checked. At the bottom right, there are "Next" and "Cancel" buttons. The "Next" button is highlighted with a blue border.

←  Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

●●●

☐ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

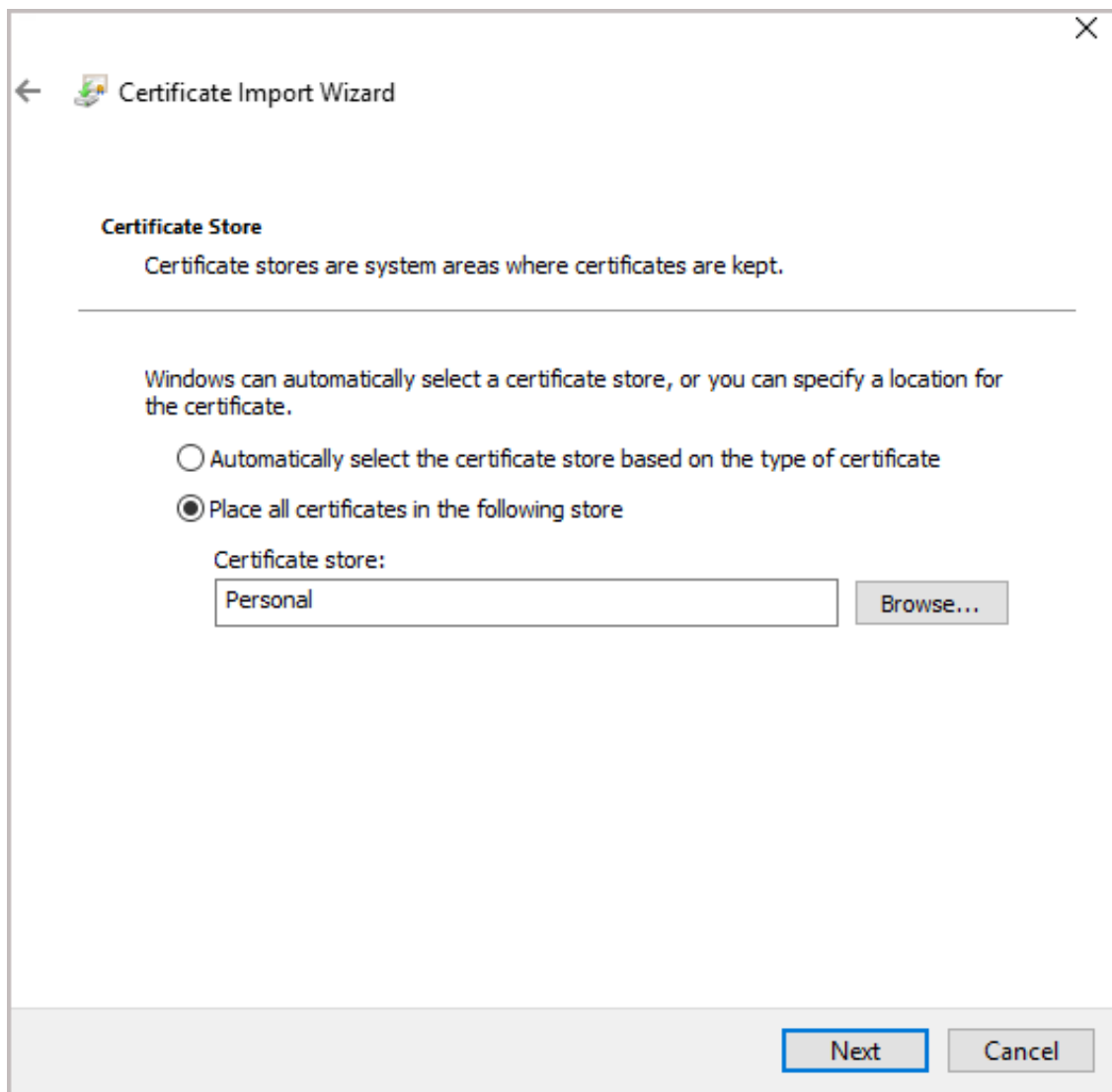
☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☐ Protect private key using virtualized-based security(Non-exportable)

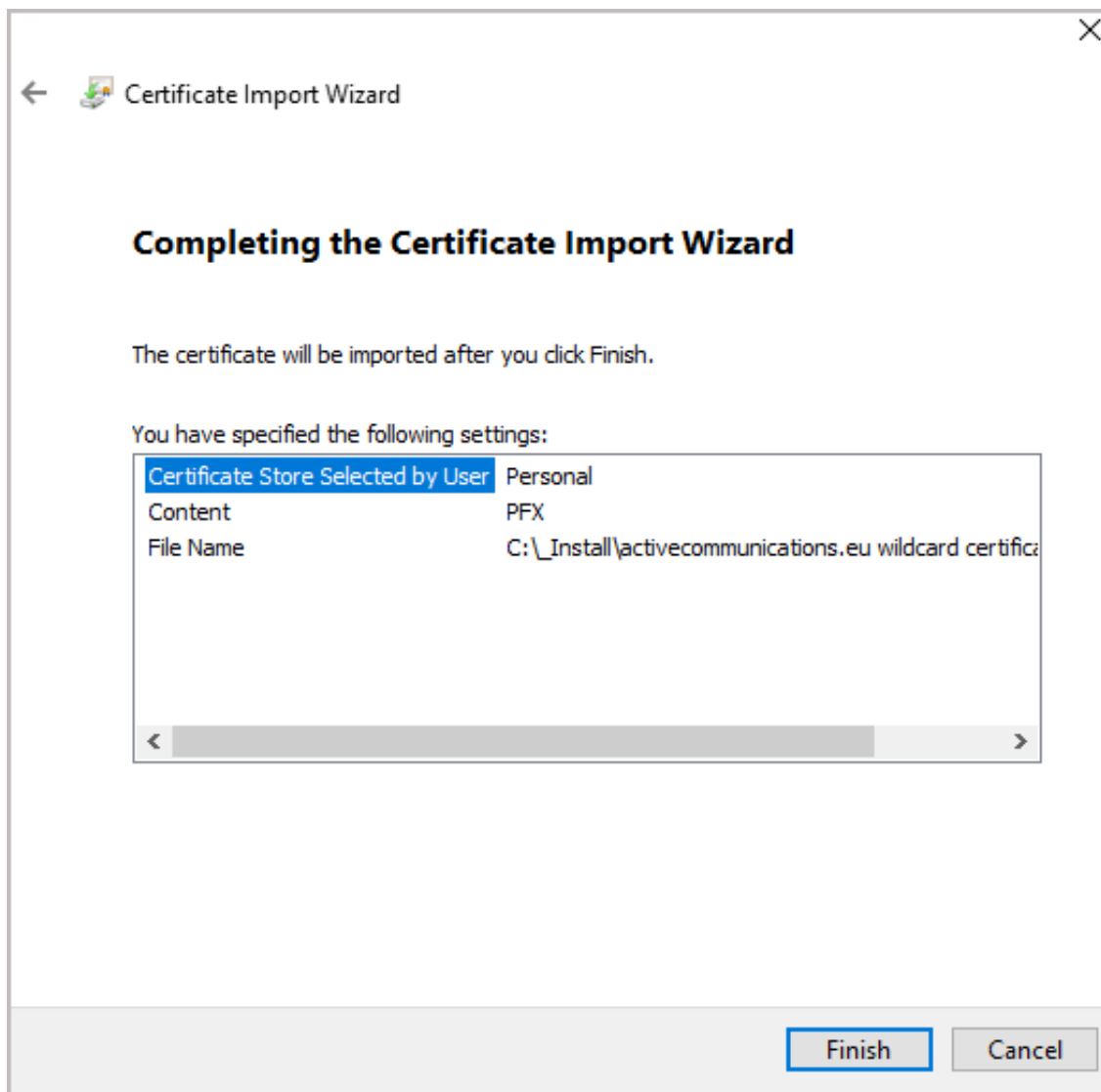
☒ Include all extended properties.

Next Cancel

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).

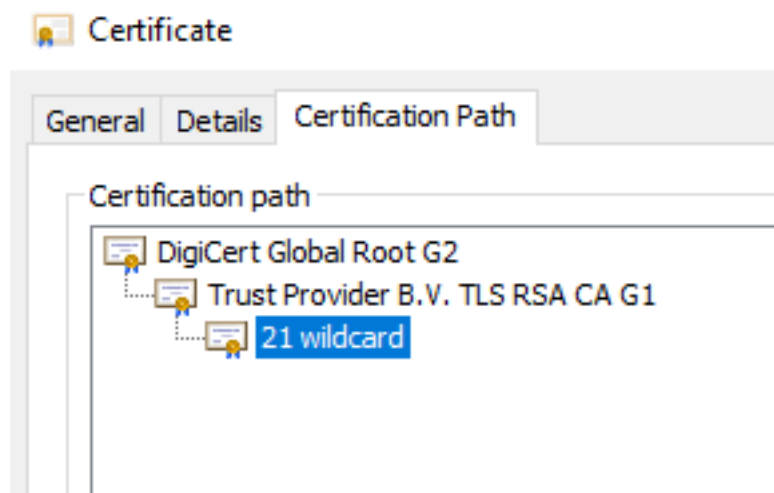
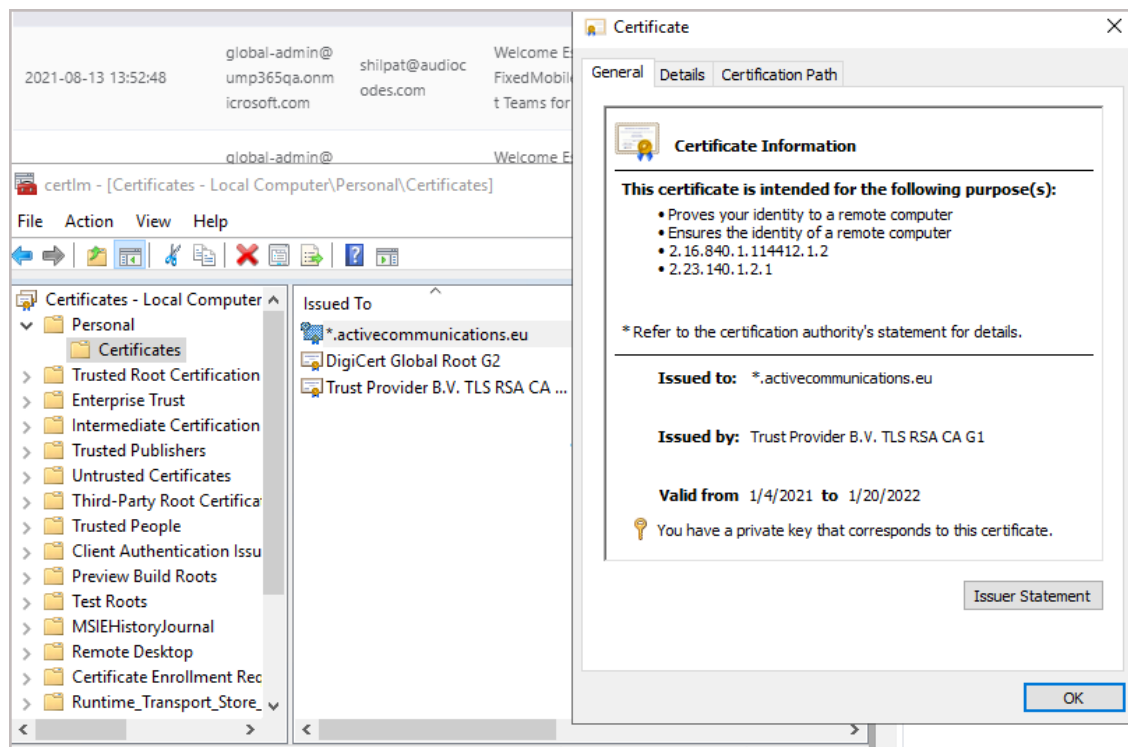


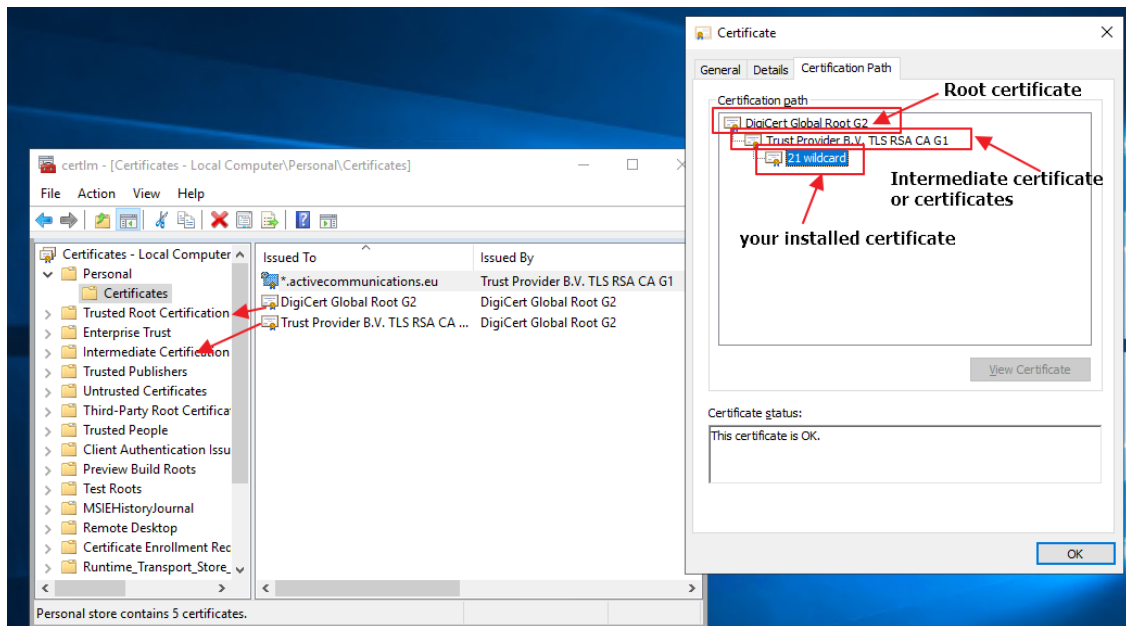
8. Browse to the location of the certificate store.



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).





4 UMP Networking and Firewall 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 ?
- Do you have different VNETS ?
- Have different locations been defined ? For example, OVOC in Azure, UMP and SBC in Customer Data Center ?

UMP Firewall Configuration

The following table describes the firewall configuration on the UMP-365 for the connection with the provider's Data Center where OVOC and the SBC are installed.

Table 4-1: UMP-365 Firewall

Port/Protocol	UMP > Data Center (provider)	Data Center (provider) > UMP	Description
TCP 80 (HTTP)	√	√	<ul style="list-style-type: none"> ■ Access to UMP-365 and SBC Web interface. ■ Outbound access for PowerShell to Microsoft Azure. ■ OVOC-UMP-365 ■ UMP - SBC connection ■ Rest API connection <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  Add the Source IP (OVOC server IP address). </div>
TCP 3389 (RDP) (Optional)	√	√	Access to Azure's Service Server using RDP from Data Center's Access to UMP-365 (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.

Port/Protocol	UMP > Data Center (provider)	Data Center (provider) > UMP	Description
UDP 1161 (Keep-alive)	√	-	Port used to send Keep-alive messages from UMP-365.
TCP 443 (HTTPS)	√	-	<ul style="list-style-type: none"> ■ Access to the Multitenant portal ■ PowerShell connection to Microsoft Azure ■ UMP - SBC connection ■ UMP-OVOC ■ Rest API connection
UDP Port 53	√	√	Port used for outbound DNS communication from UMP-365.

- PowerShell
 - No VPN is required
 - Current version requires “basic” direct internet access without a proxy server
- Office 365 URLs and IP address ranges: [urls-and-ip-address-ranges](#)

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)		√

Transport/Port/Protocol	AudioCodes > Customer	Customer > AudioCodes
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 for different customers topologies. The table should include all the required protocols and ports, according to the networking topology.

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: OVOC 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	TCP (HTTP)	✓	915	WebSocket Client and OVOC Server communication	OVOC server side / Bi-

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
Communication				(internal) according to RFC 6455, used for managing the alarm and task notification mechanism in the OVOC Web. Initiator (internal): WebSocket Client	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	Both sides / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
				configured as NTP client) Initiator: Both sides	
Device ↔ OVOC server	TCP (HTTP)	x	80	HTTP connection for files transfer and REST communication. Initiator: Both sides can initiate an HTTP connection	OVOC server side / Bi-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
Endpoints					
Endpoints ↔ WAF/Azure Blob	TCP (HTTPS)	√	443	HTTPS connection between the endpoints and the WAF. Initiator: Endpoints	OVOC server side / Bi-Directional
				HTTPS connection used by endpoints for downloading firmware and configuration files from the Azure Blob. Initiator: Endpoints	

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
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)	√	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)	√	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	TCP	√	443	HTTPS for OVOC / Cloud Service Initiator: OVOC REST client	OVOC REST client side / Bi-directional

Connection	Port Type	Secured Connection	Port Number	Purpose	Port side / Flow Direction
Service					
External Servers					
OVOC server ↔ Mail Server	TCP	√	25	Trap Forwarding to Mail server Initiator: OVOC server	Mail server side / Bi-directional
OVOC server ↔ Syslog Server	TCP	√	514	Trap Forwarding to Syslog server. Initiator: OVOC server	Syslog server side / Bi-directional
OVOC server ↔ Debug Recording Server	UDP	√	925	Trap Forwarding to Debug Recording server. Initiator: OVOC server	Debug Recording server / Bi-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

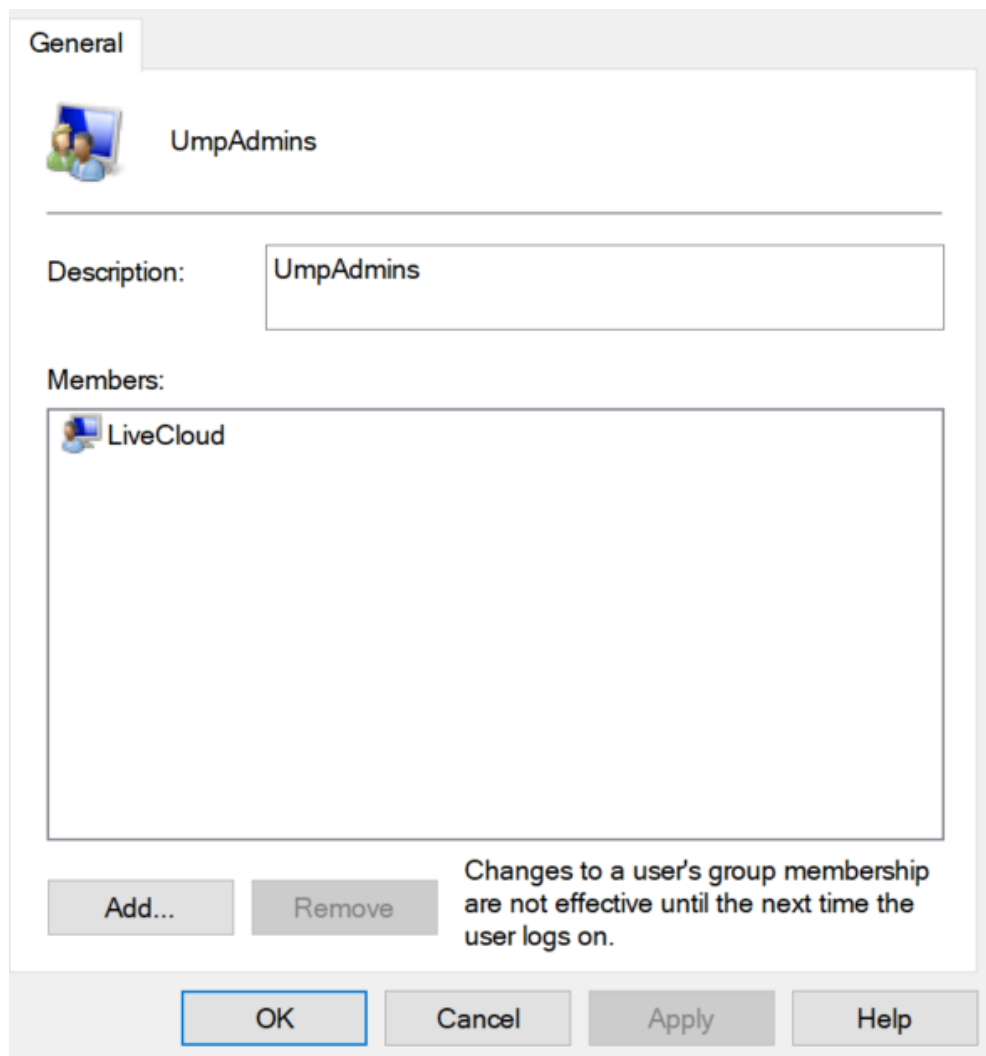
5 SQL License Guidelines

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.

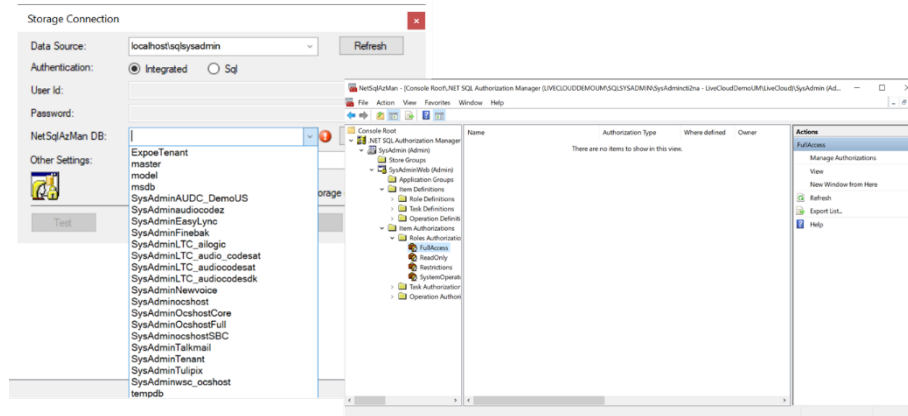
The list of Admin users requiring a license is as follows:

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

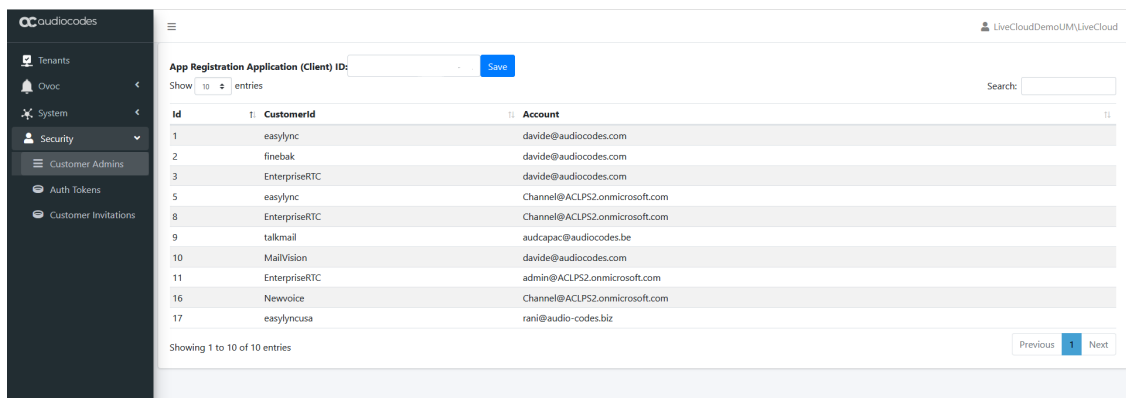


- UMP support two types of User Admin per tenant:
 - UMP SP Windows users per Tenant (customer) – Windows users per Tenant, our recommendation is to Grant Access to Account user (SSO with Azure AD). It is not

recommended to create Windows users per Tenant (customer). If you choose to create Window users per Tenant, this requires a license per user.



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



The following are the recommended guidelines:

- 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 Verifying Anti-Virus Access Scanning

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, testing must be performed both before and after the installation of anti-virus software. This is necessary to determine whether there are any performance affecting issues that may arise on the computer running the relevant component. Prior to installation of the UMP-365 server, its recommended to verify that files and directories that must be accessed during and after the installation or upgrade are not temporarily locked by the anti-virus software. These files or directories for the components listed below should be configured in the whitelist exclusion list on the Anti-virus software to prevent them from being locked. This improves the performance of the files and helps make sure they are not locked when the relevant service or component requires access:

- [SQL](#) below
- [ASP.NET](#) below
- [Other Files and Directories](#) on the next page

SQL

Running anti-virus software on a server where Microsoft SQL is installed is not recommended. The following Whitelist exception rules should be configured to allow the SQL Server service seamless access.

- 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

ASP.NET

As UMP uses ASP.NET with IIS, the folders should below should be excluded from Anti-virus scanning:

- 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

Other Files and Directories

■ The temp folder used to download and install Microsoft PowerShell module should be excluded from file access scanning.

■ For the User Management Pack™ 365 SP Edition server, exclude the following directory:

- Exclude c:\acs (Disable on access scan)

7 Creating 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 (**SysAdmin** user on the **local** UMP-365 machine):

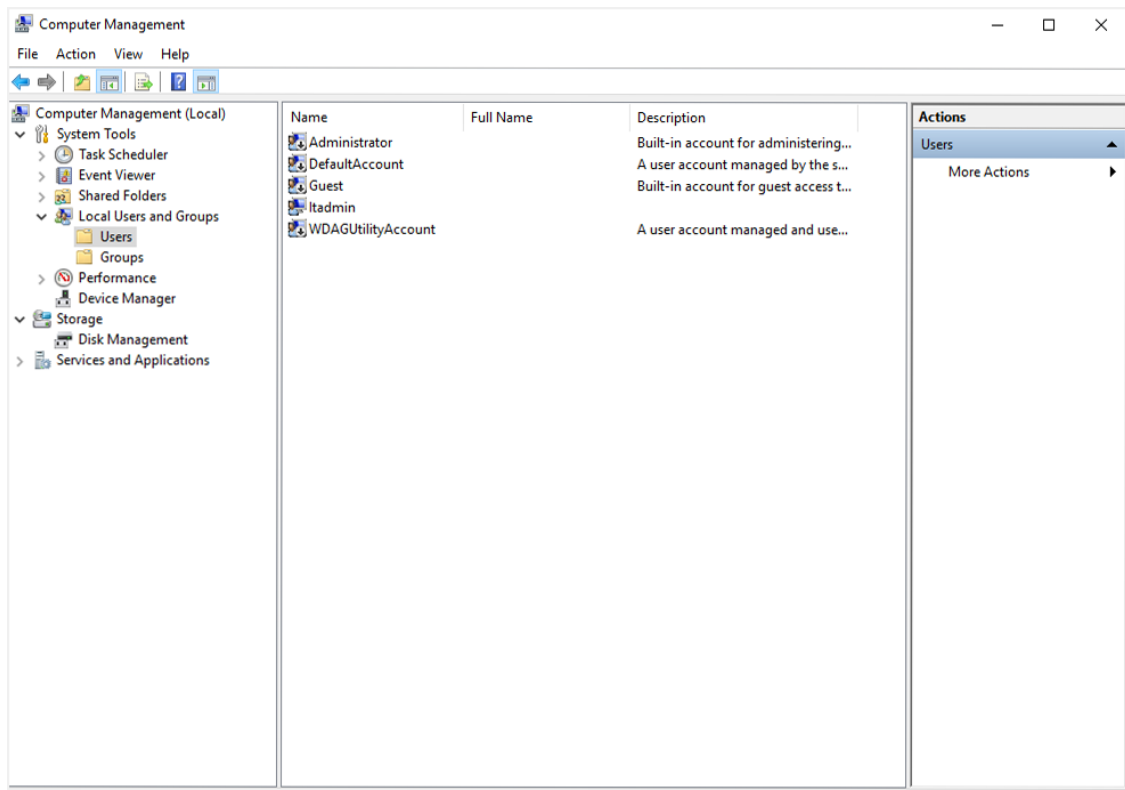
- Install UMP-365 (see [Installing UMP SP](#) on page 46)
- Create DNS Subdomains (see [Register End Customer Tenant DNS Sub domains](#) on page 250)
- App Registration for Background Processing (see [Configuring Microsoft Teams Direct Routing SBC](#) on page 86)
- Define Invitation Settings (see [Configuring Invitation Settings](#) on page 67)
- Define Email Settings (see [Configuring Email Settings](#) on page 69)
- App Registration for Customer Admins (see [Create Registration for Customer Administrators](#) on page 87)
- Configure License (see [Multitenant Portal Licensing](#) on page 65)
- Configure Service Provider Logos (see [Updating Service Provider Logos](#) on page 116)
- Secure networking between UMP, SBC and OVOC (see [Networking](#) on page 51)



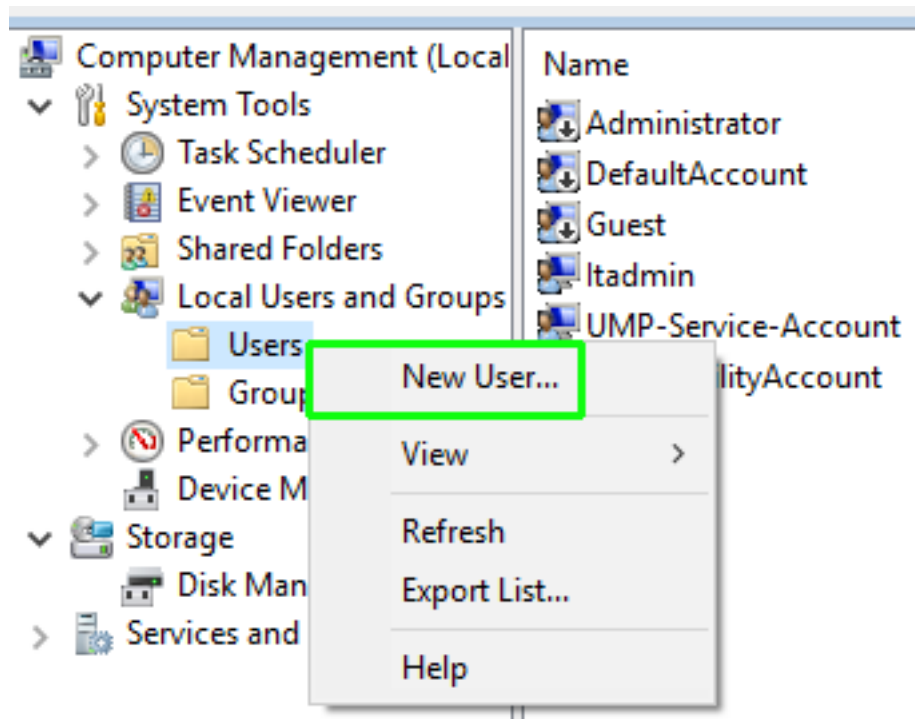
- For configuration on the Microsoft Azure platform, ensure that you have Global Admin permissions for both the Main Tenant and Service Provider operator tenant platforms. If customers are using a backend SQL server, then the same account must be used to login to the SQL server on the backend server.
- The names of the users created in the procedure below "UMP-Service-Account" and UMP-Admin-User" are examples only.

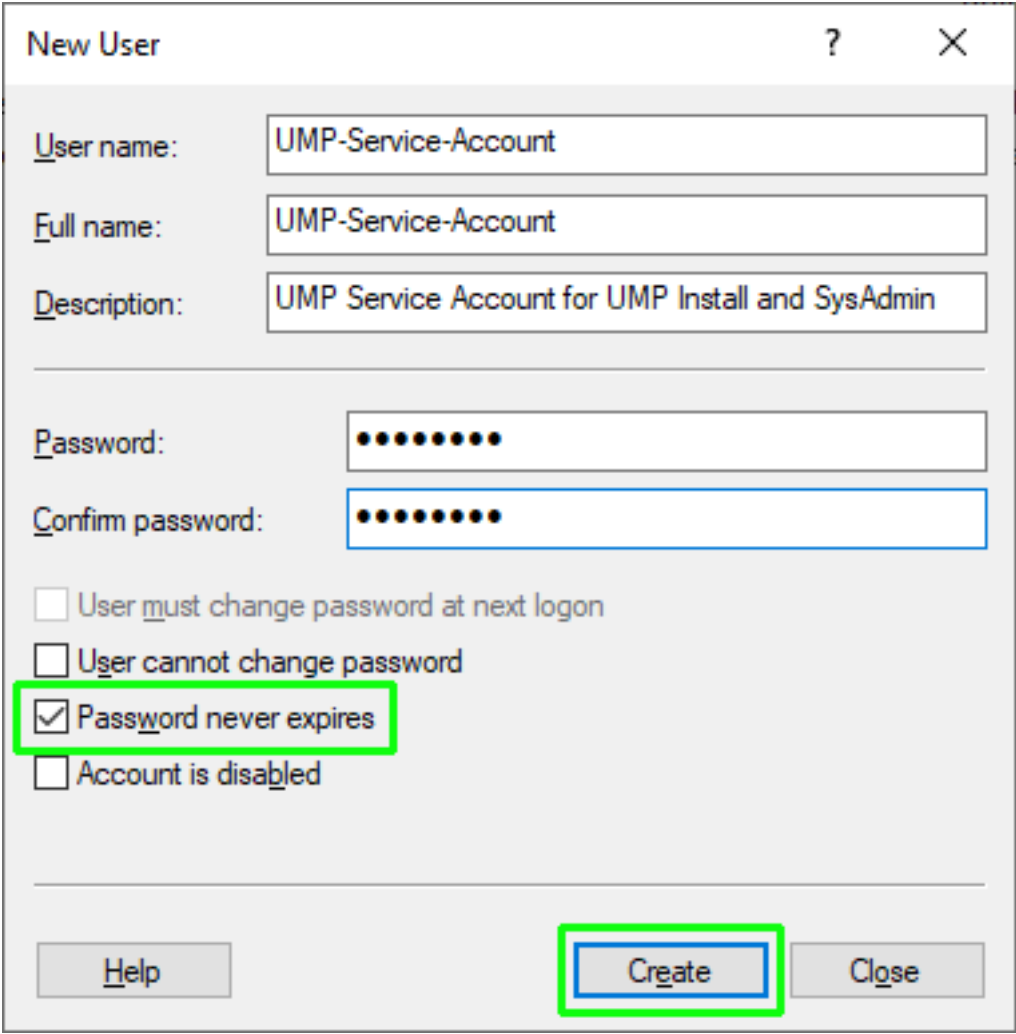
➤ To create a Windows UMP Service account:

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

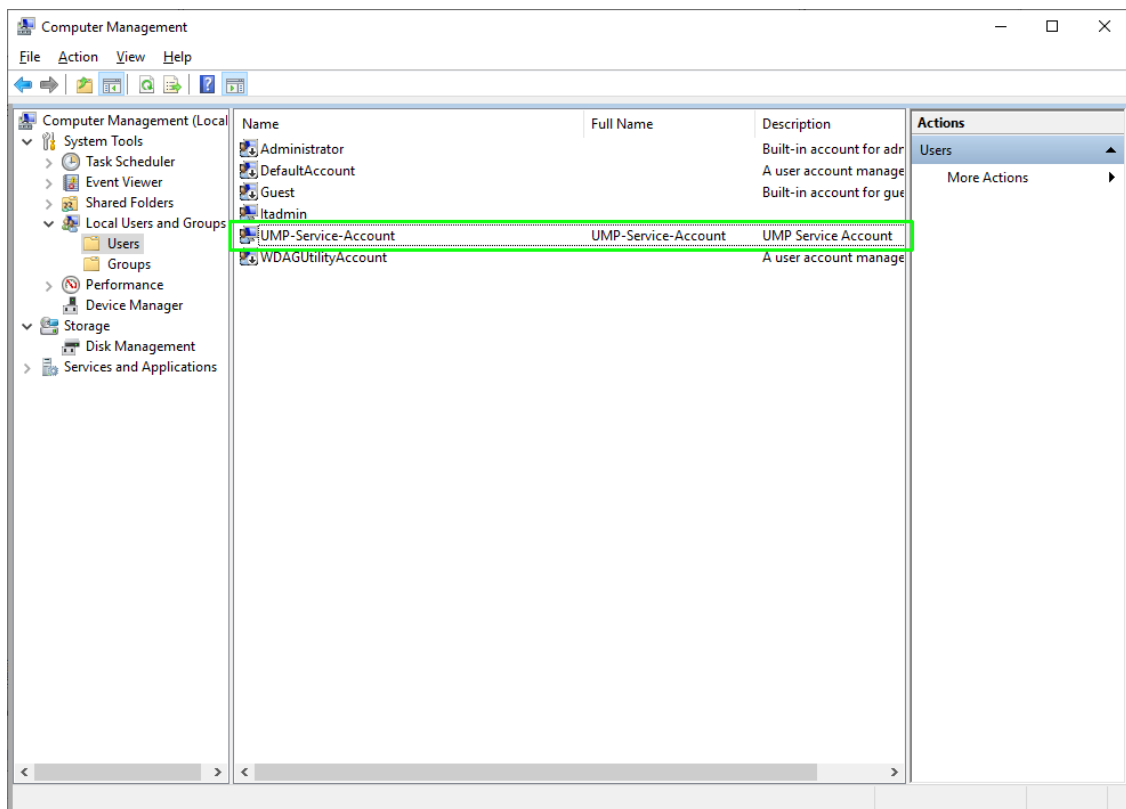


3. Create a new user **UMP-Service-Account**; right-click the Users folder, and then choose **New User**.

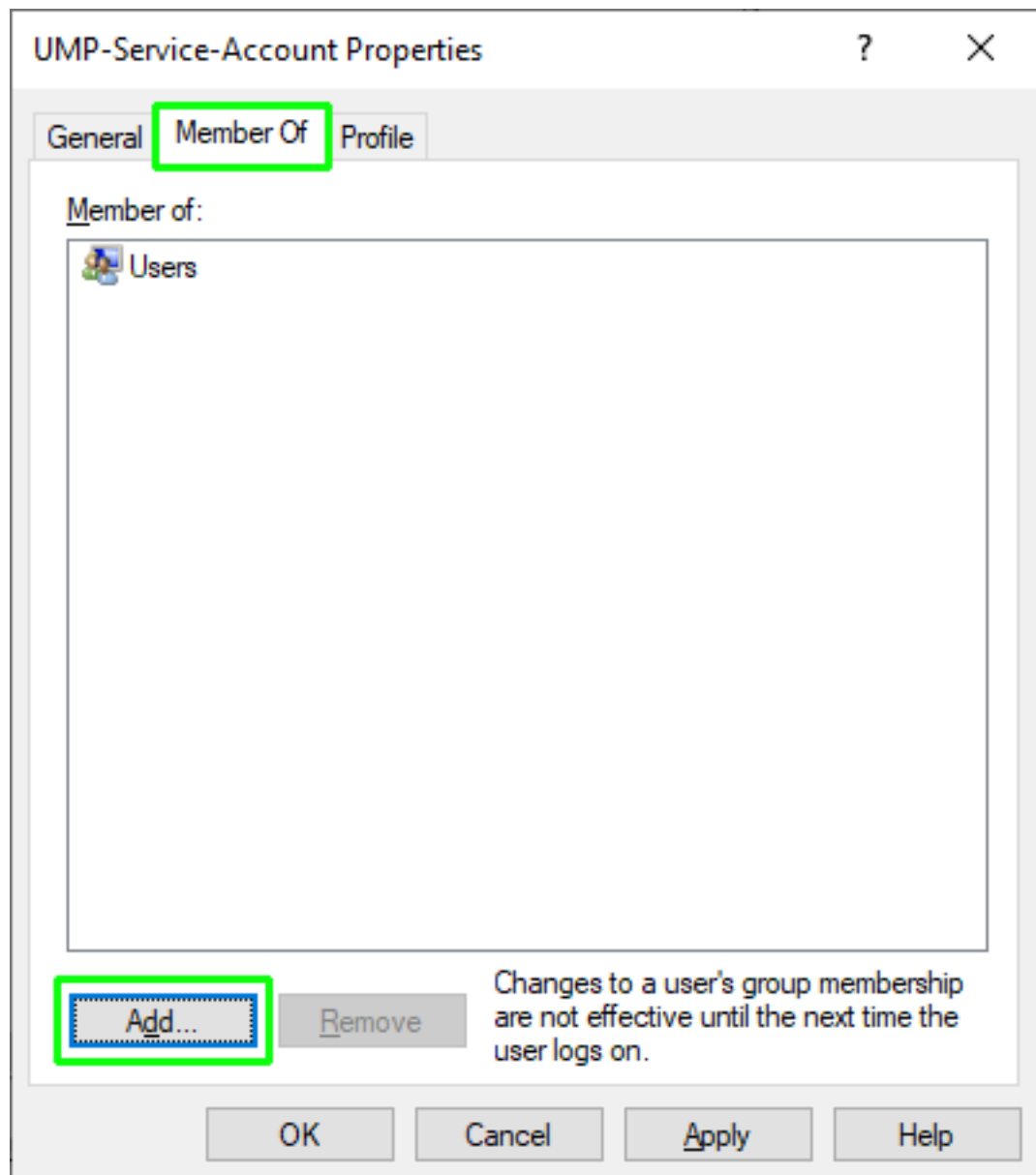


A screenshot of a 'New User' dialog box. The dialog has a title bar with a question mark and a close button. It contains several text input fields: 'User name:' with 'UMP-Service-Account', 'Full name:' with 'UMP-Service-Account', and 'Description:' with 'UMP Service Account for UMP Install and SysAdmin'. Below these are two password fields, both containing masked characters (dots). Under the password fields are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (checked and highlighted with a green box), and 'Account is disabled' (unchecked). At the bottom are three buttons: 'Help', 'Create' (highlighted with a green box), and 'Close'.

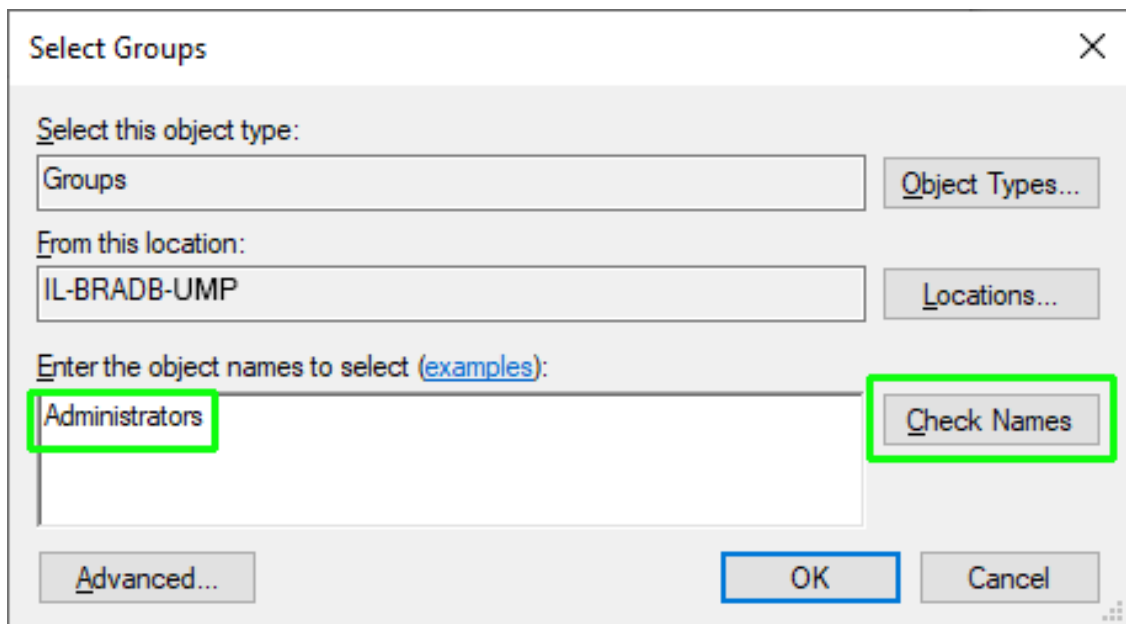
4. Enter the details of the SysAdmin user to manage the UMP-365 Service account (it's recommended to set **Password never expires** option. **Do not** use spaces in User name and Full name fields), and then click **Create**; the new user is added. See [Local Users and Groups](#) for information on creating and managing users and groups that are stored locally on a computer.



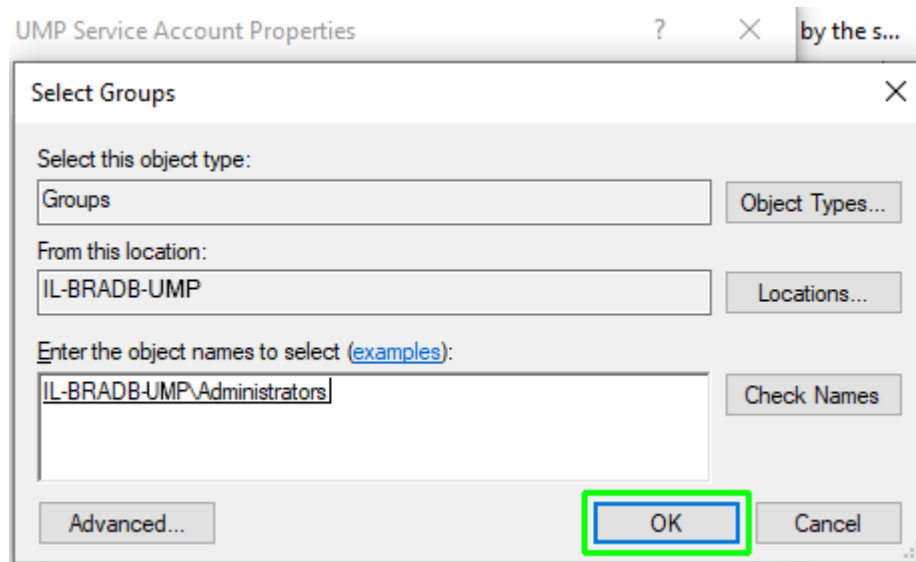
5. Right-click the user, and then select **Properties**.
6. Select the **Member Of** tab.



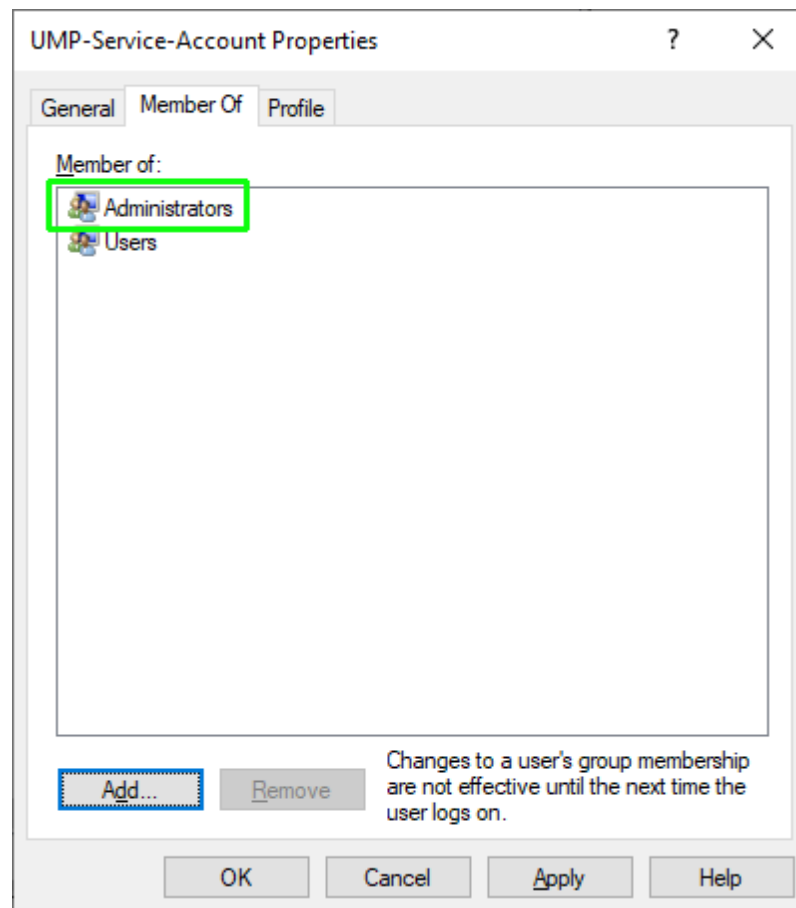
7. Click **Add** to add the UMP-Service-Account user to the Administrators group.



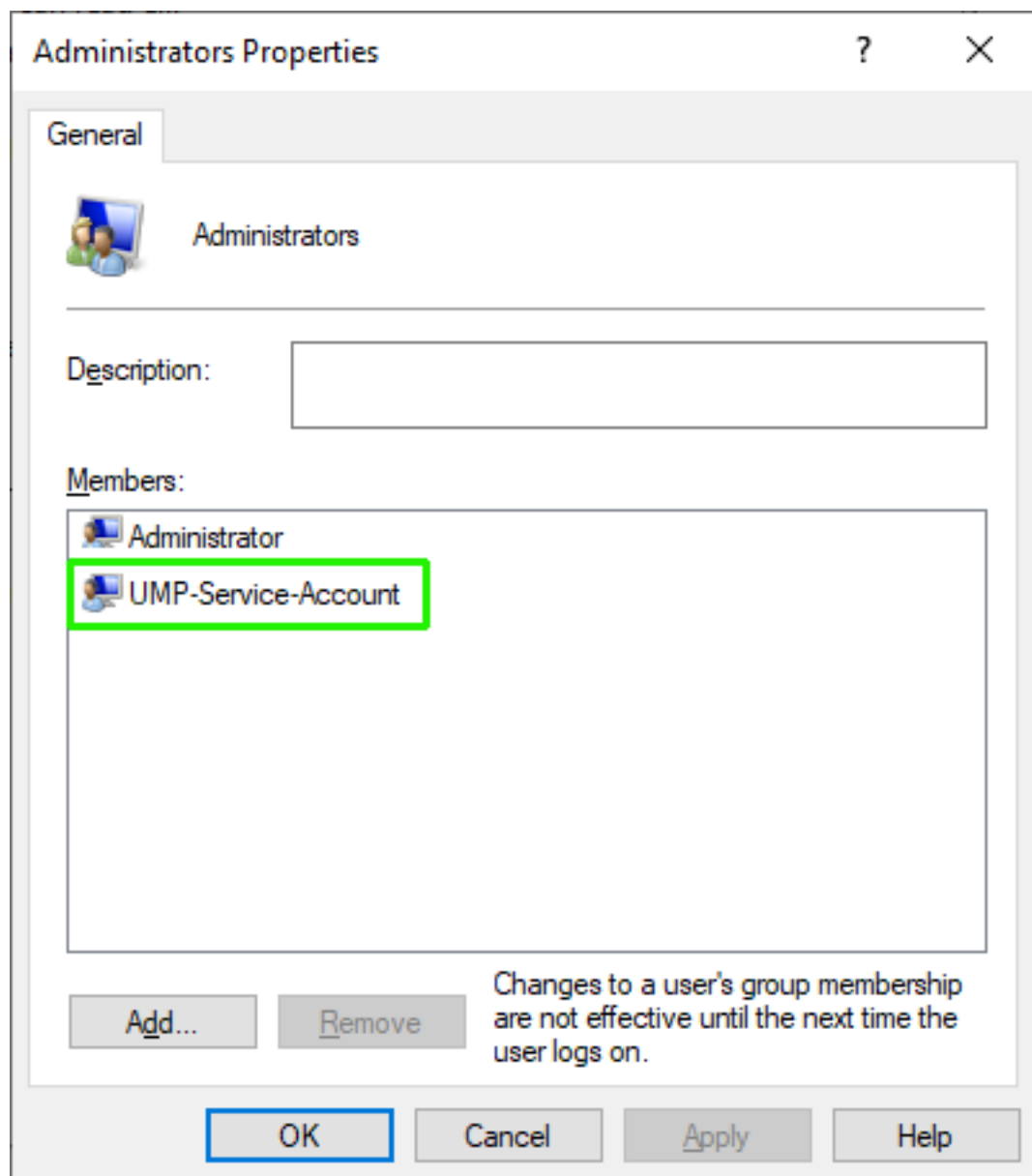
8. In the text box, type 'Administrators', and then click **Check Names**.



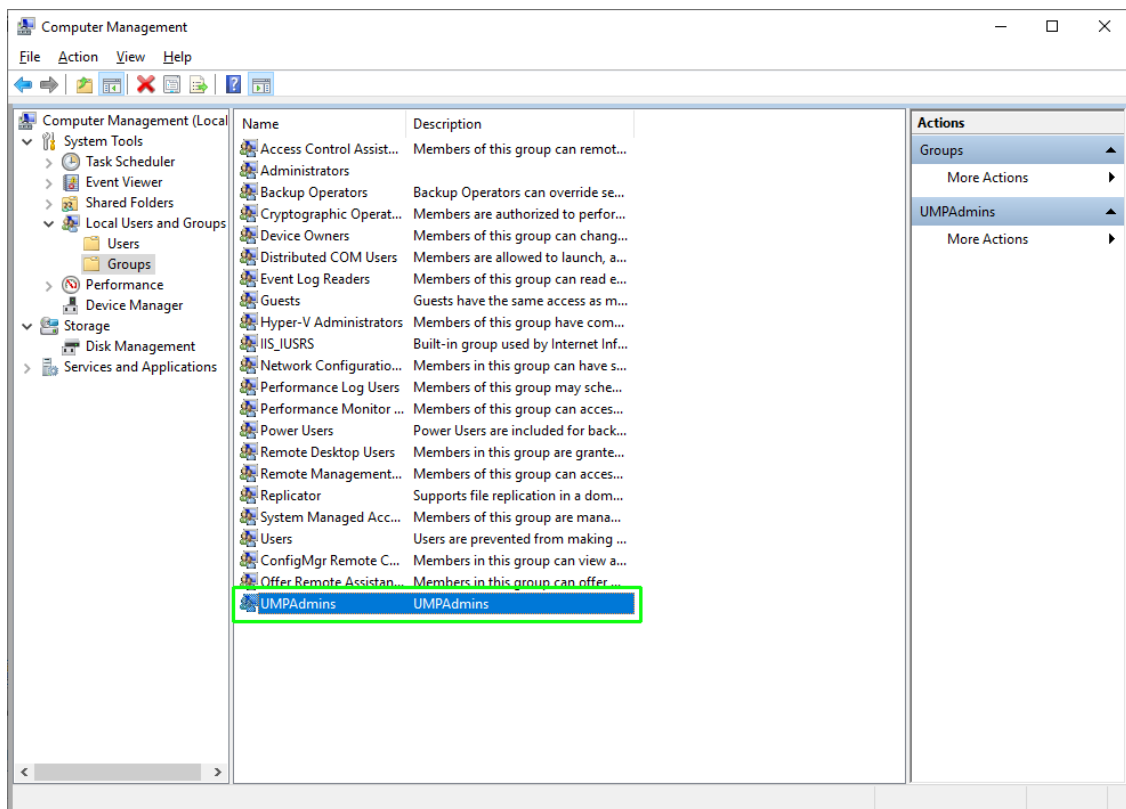
9. Click **OK**; the UMP-Service-Account is added to the Administrators group.

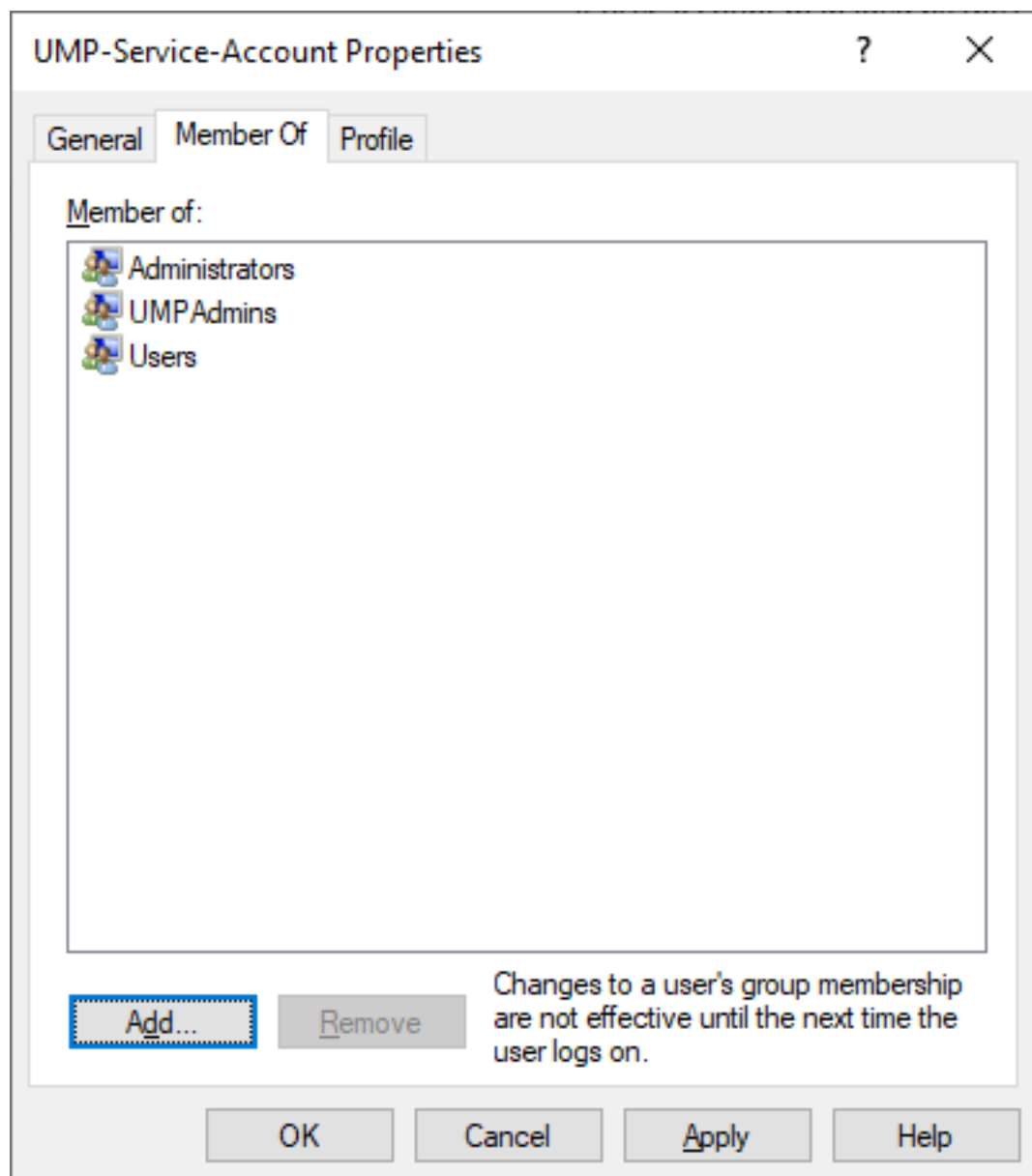


10. Open the Properties of the Administrators group; view that the UMP-Service-Account has been added to the Administrators group.

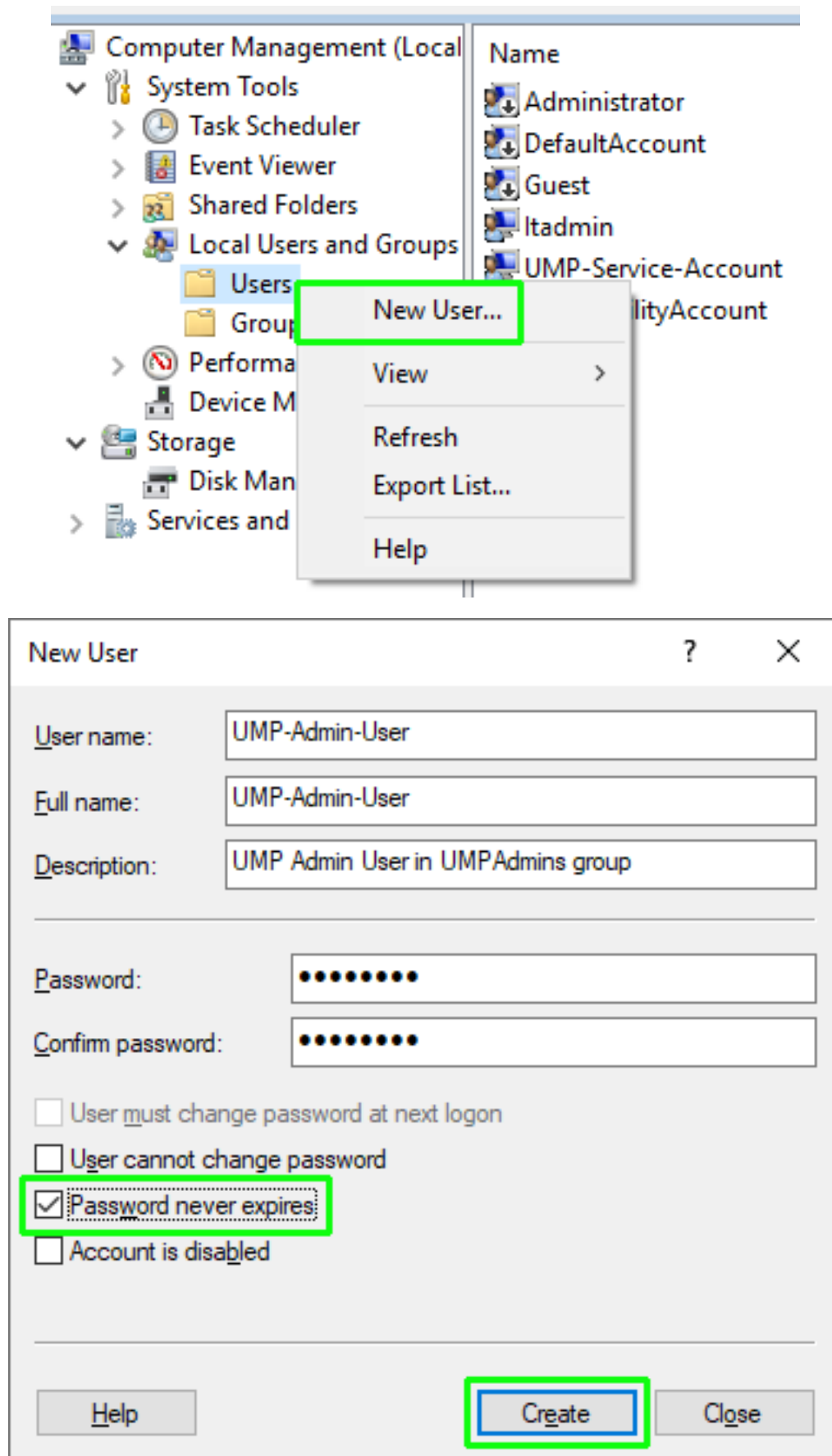


The example screen below shows a new group “UmpAdmins” that is created following the installation. The Administrator who ran the installation is automatically a member of this group.

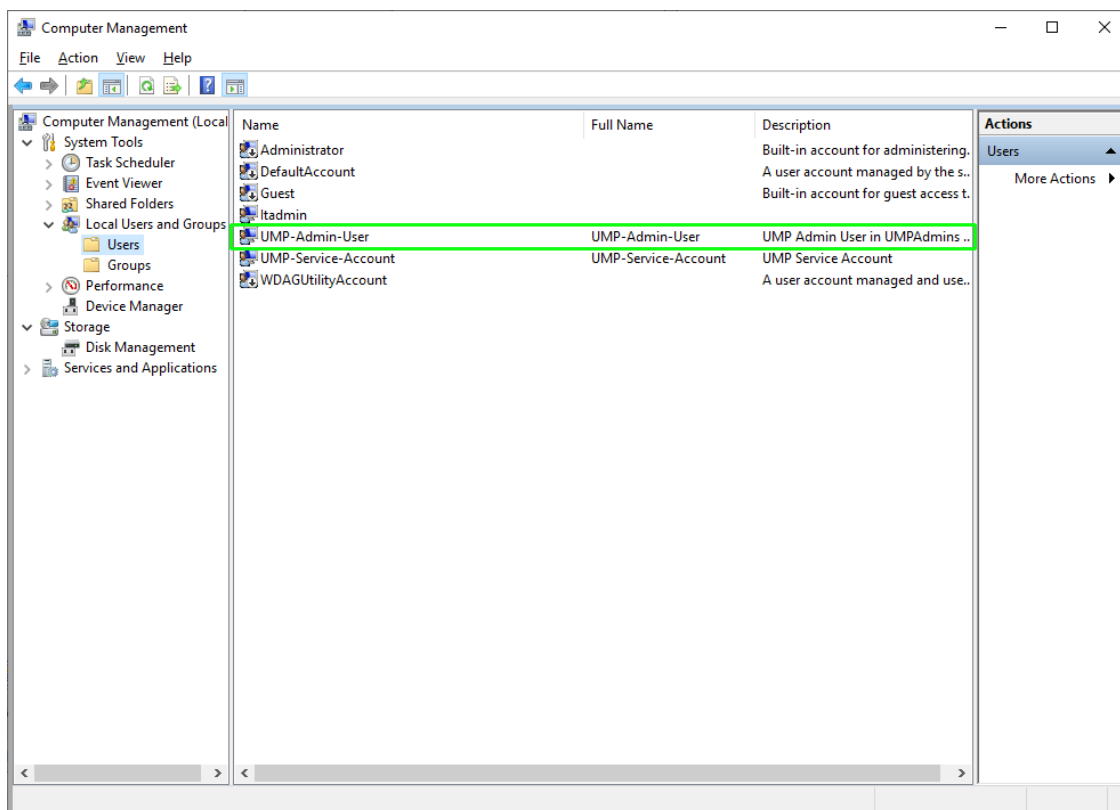




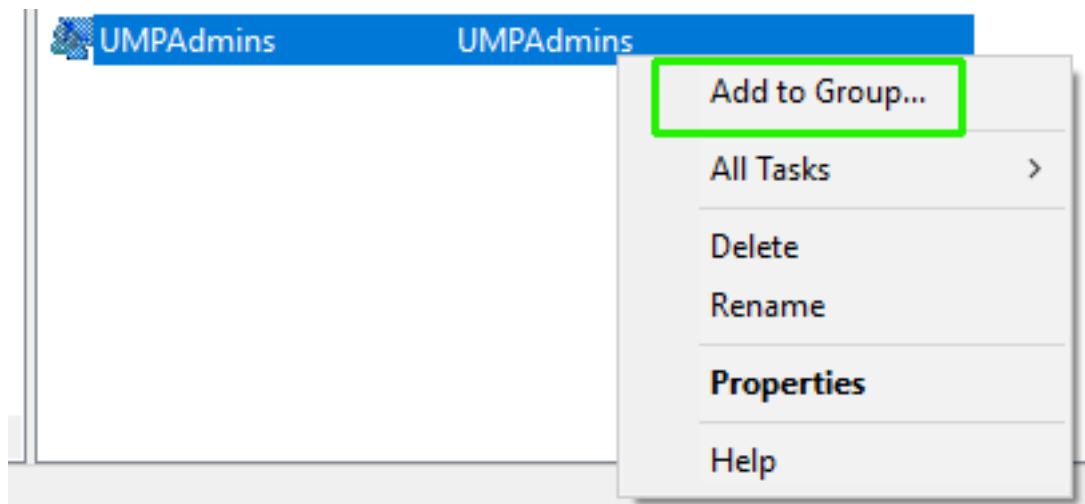
11. Create a new user to add to the UMPAdmin group; right-click the Users folder, and then choose **New User**.

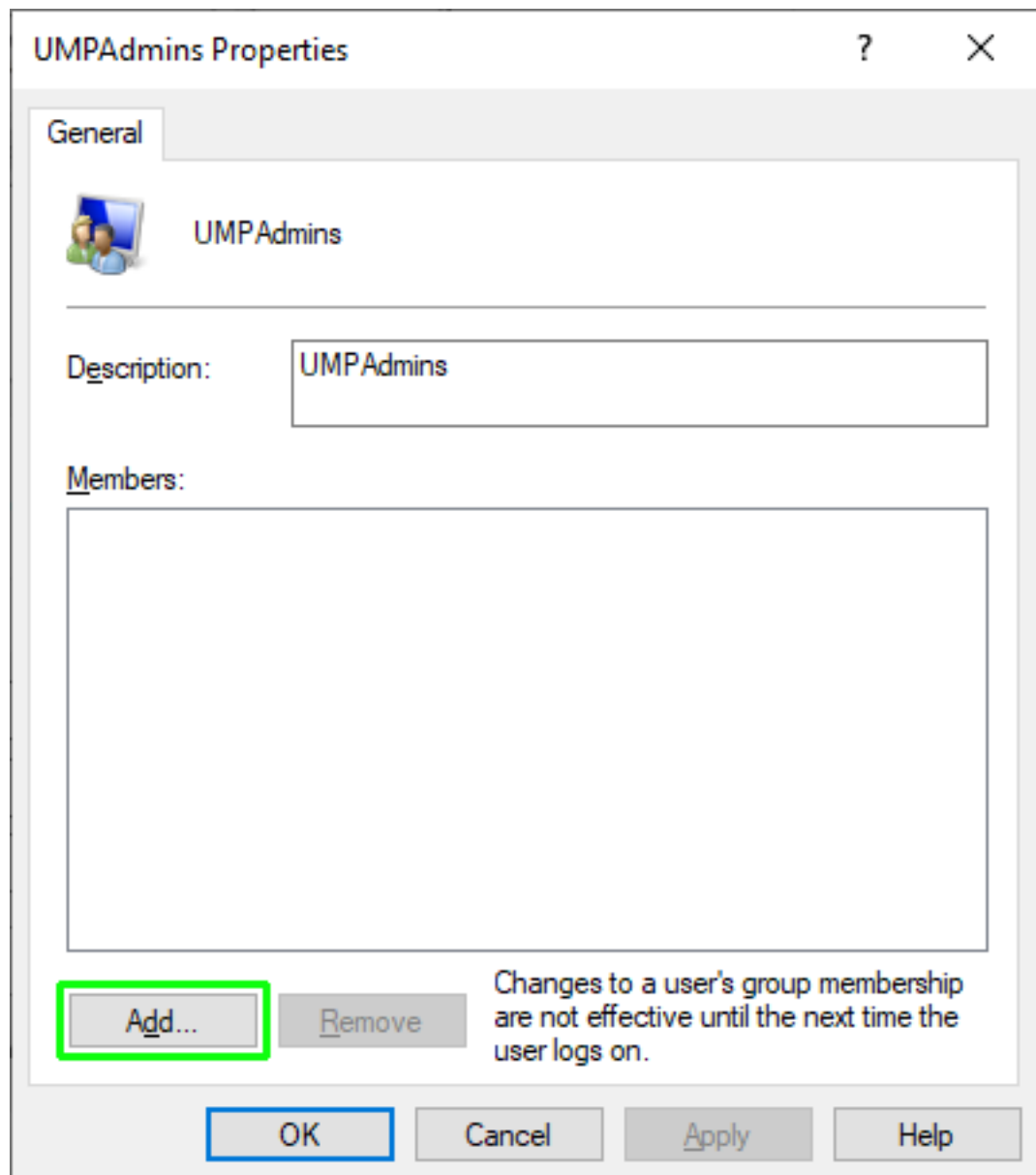


12. Enter the details of the user (it's recommended to set **Password never expires** option. **Do not** use spaces in User name and Full name fields), and then click **Create**; the new user is added. See [Local Users and Groups](#) for information on creating and managing users and groups that are stored locally on a computer.

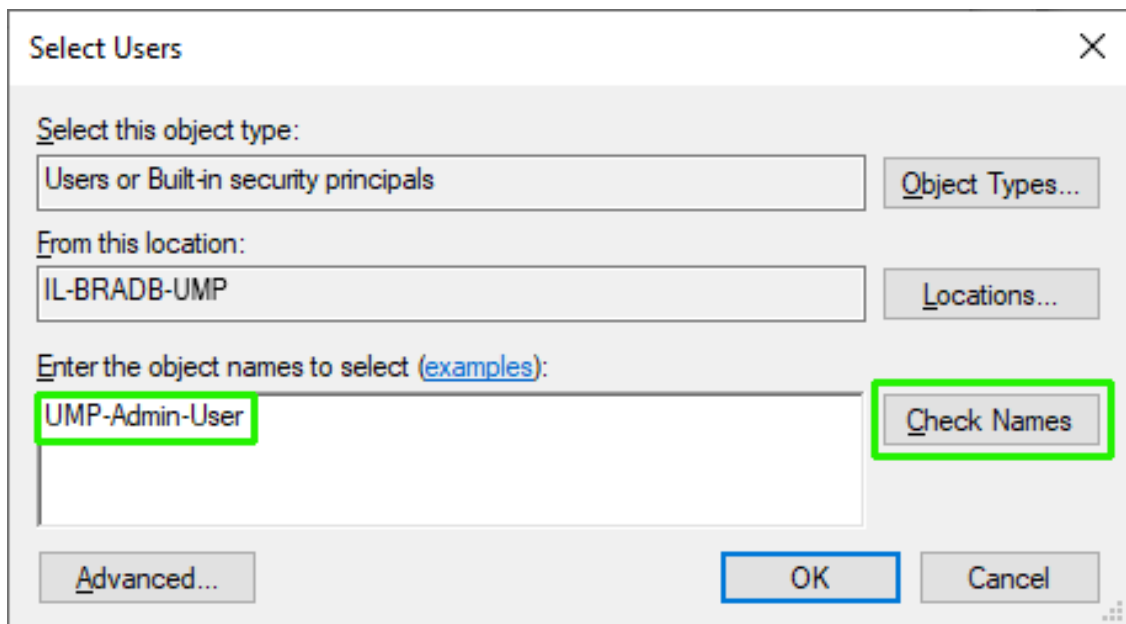


13. Right-click the UMPAdmins group, and then click **Add to Group**.

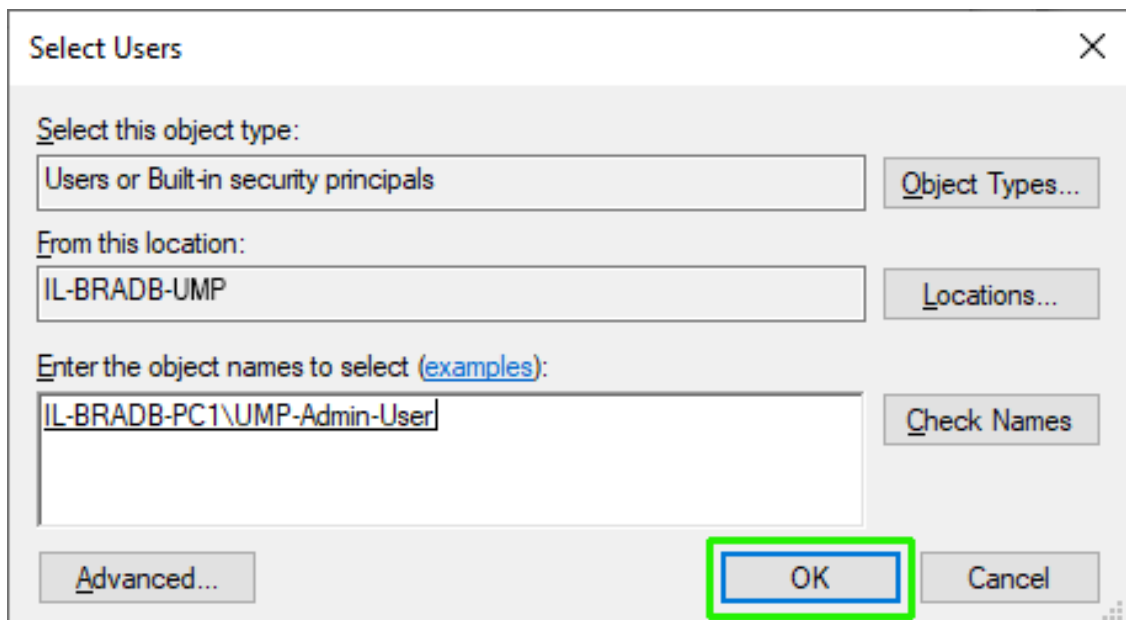




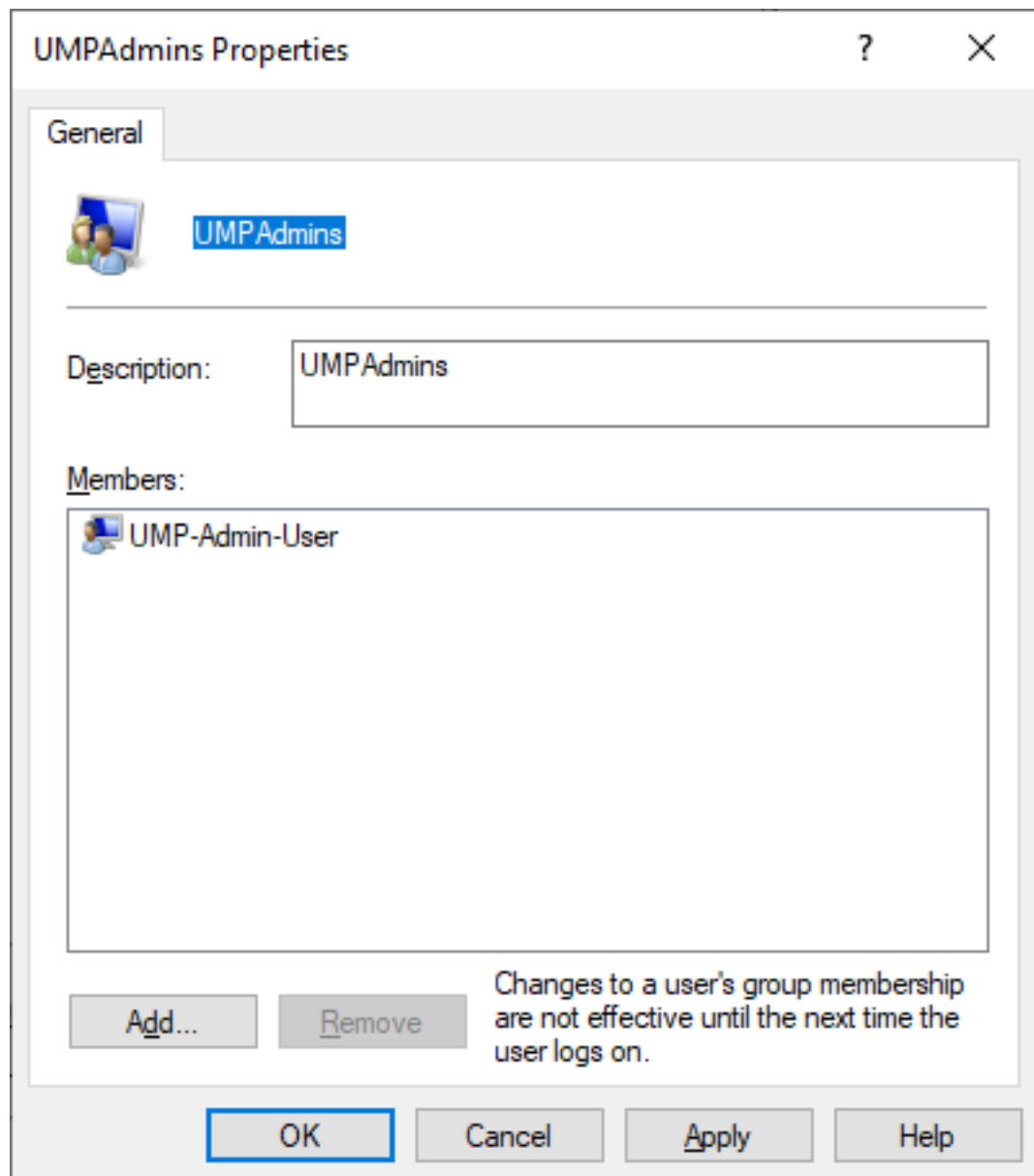
14. Click **Add** to add a new user to the group.



15. In the text box, type 'UMP-Admin-User', and then click **Check Names**.



16. Click **OK**; UMP-Admin-User is displayed under UMPAdmin Properties.



17. Click **OK** again.

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



All users defined in the **UmpAdmins** group can perform Wyupdates.

Part II

Installation and Setup

8 Installing the Prerequisites

This section describes how to install the prerequisites.



To keep the installation ISO as small as possible, the UMP-365 installation requires Chocolatey. Chocolatey released their latest version 2.0 last month which requires the use of TLS 1.2. Prior to installation of Chocolatey on Windows server 2019, you must manually install .net framework 4.8 and reboot the server before you can install the prerequisites. Click the link below to choose the web installer or download the file for Offline install:

[Download .NET Framework 4.8 | Free official downloads \(microsoft.com\)](#)

The ISO was tested and created for Windows server 2022, which is not affected by this issue.

➤ Do the following:

1. Login to server where you wish to install UMP-365 with newly created service account (see [Creating UMP Service Account](#) on page 29).
2. Download the installation package from the following location: [AC_UMP_MT_ISO](#)



3. Mount the UMP-MT ISO file.
4. Before installing UMP SP, the server needs to be prepared by installing the prerequisites by running the Install-UMPSPPrerequisites.ps1 script file running with Administrator permissions (Admin mode).
5. 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.

9 Installing UMP SP

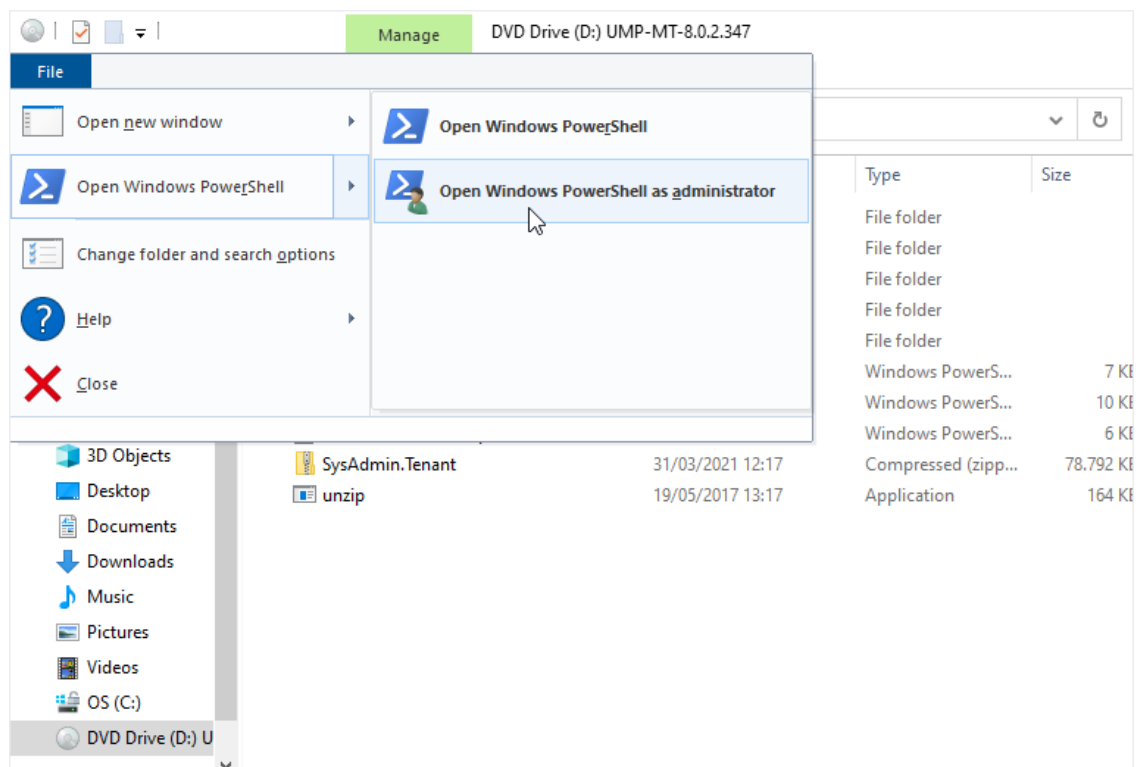
This section describes how to install UMP-SP. This installation must be run by the Windows UMP Service account.



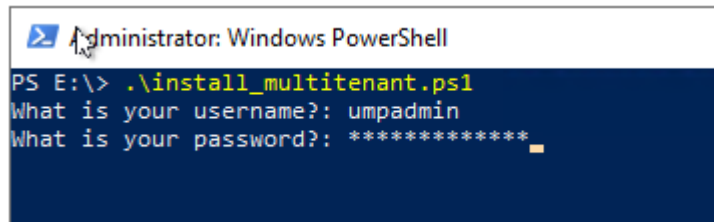
The details of the UMP Service account are displayed in the UMP Service Settings screen (see [UMP Service Settings](#) on page 234).

➤ To install UMP-SP:

1. Login with the UMP Service account credentials.
2. Mount the ISO file.
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



5. You are prompted for the user and password of the local server. The account entered must be the service account created in [Creating UMP Service Account](#) on page 29.



```
Administrator: Windows PowerShell
PS E:\> .\install_multitenant.ps1
What is your username?: umpadmin
What is your password?: *****
```

The installation process commences.

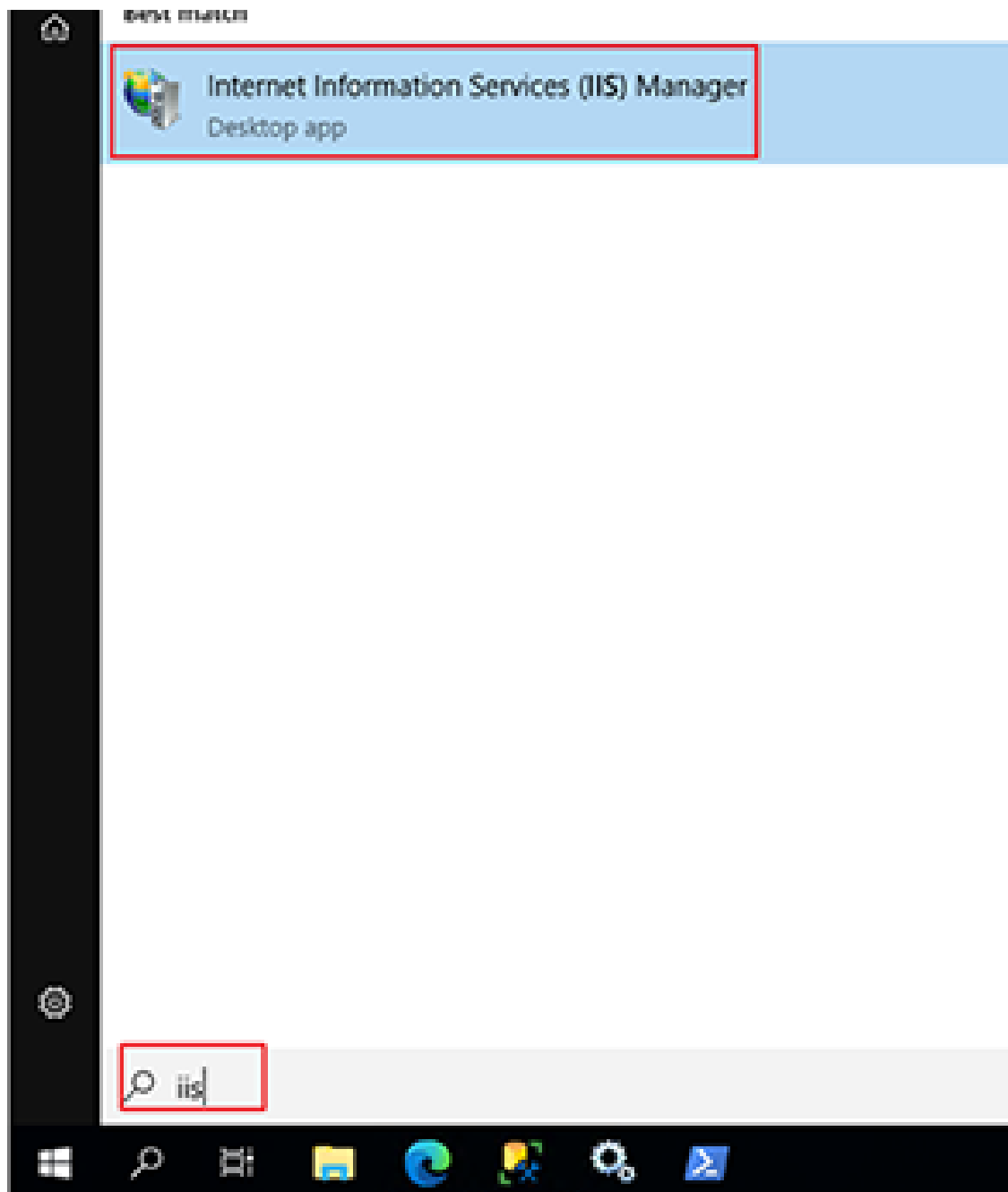
6. Once the installation has completed, reboot the server and check for the latest available updates (see [Upgrading Main UMP-365 Tenant](#) on page 131)

Adding SSL Certificate to IIS Website

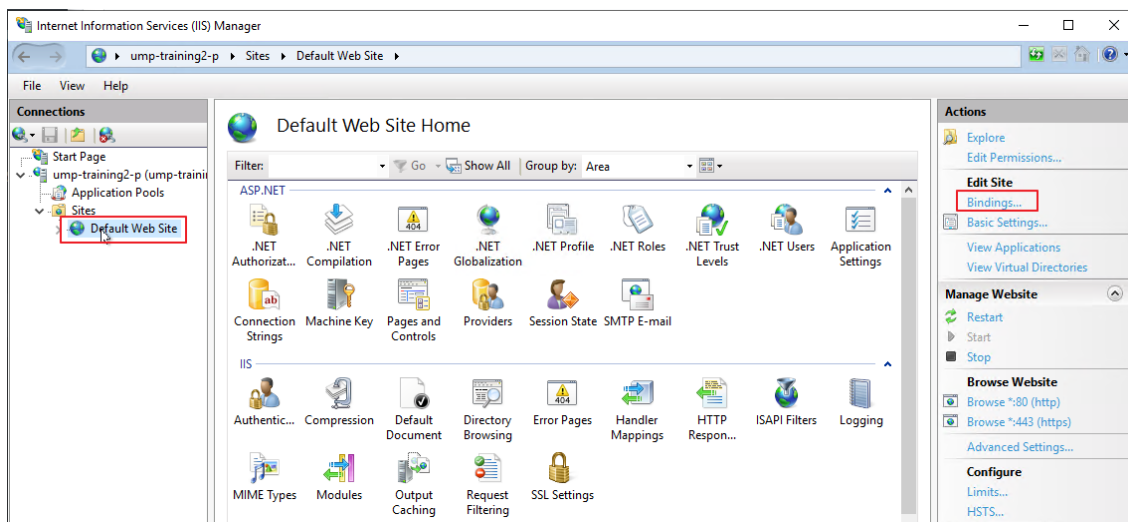
After installing the UMP-SP you must install the SSL certificate to the IIS Website.

➤ To install the certificate:

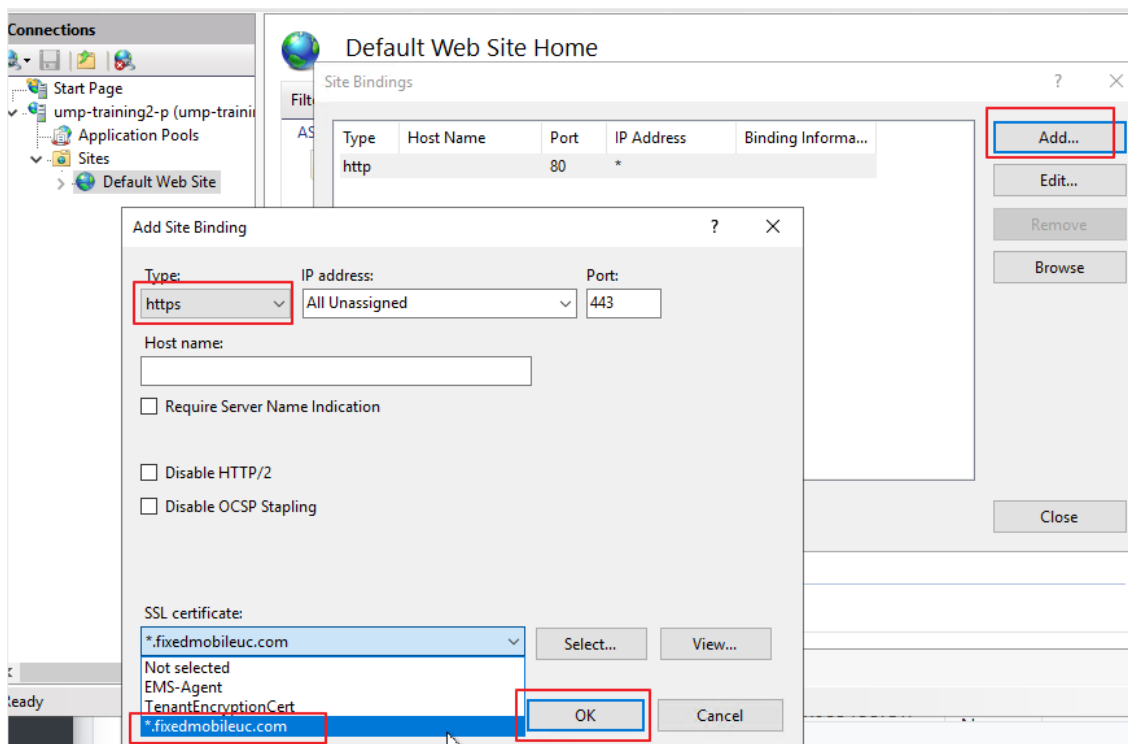
1. Open Internet Information Services (IIS) Manager.
2. Click Windows Start and type **IIS**.



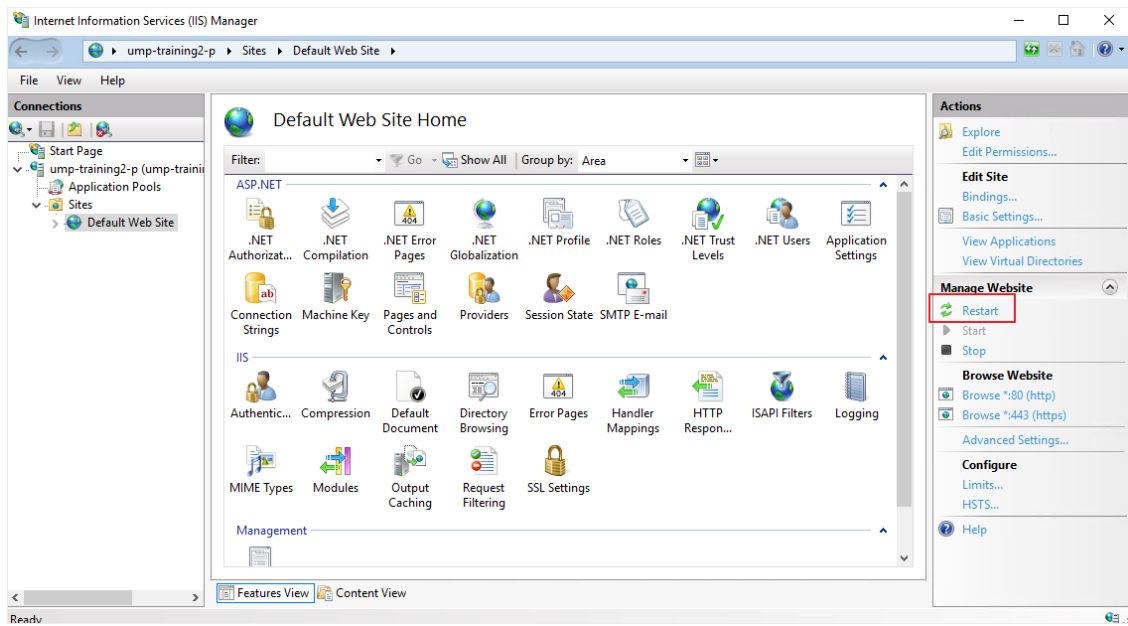
3. Browse in the Connections pane to Default Web Site and select **Bindings**.



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



5. Click **Close**.



6. Restart IIS.

10 Networking

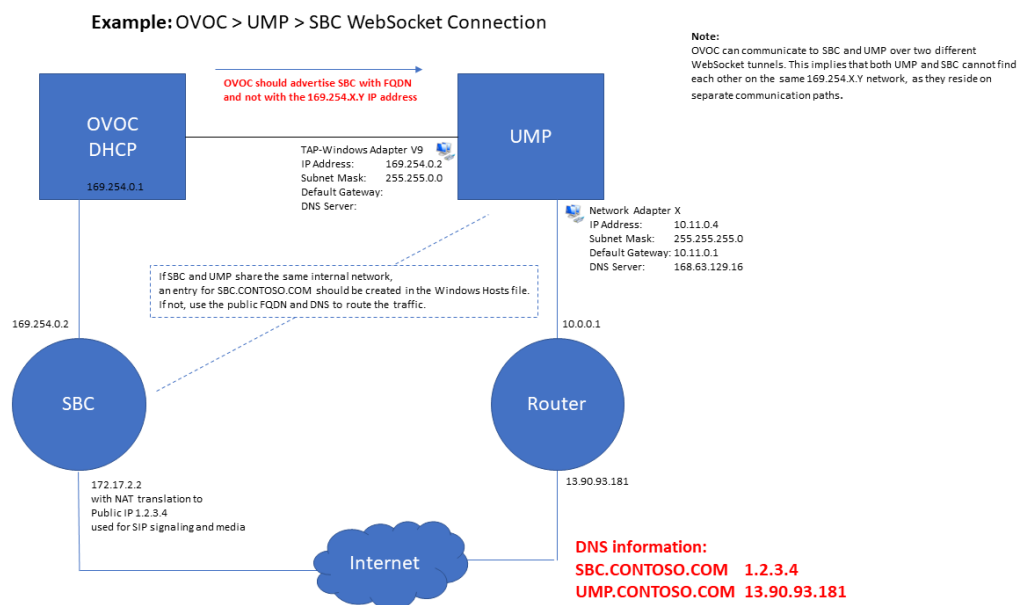
This section describes how to setup the connection between the UMP Web interface and the OVOC and UMP on Azure. Connection to the OVOC Server on Azure can be established using one of the following methods:

- OVOC Azure Public IP over WebSocket Tunnel (Cloud Architecture Mode) (see [Configuring UMP Interface for WebSocket Tunnel \(Cloud Architecture Mode\)](#) below).
- OVOC Azure Public IP over HTTPS SSL certificate with mutual authentication (see [Configuring HTTPS SSL Connection to OVOC Public IP](#) on page 58).
- OVOC Azure Private IP (see [Configuring Connection to OVOC Azure Private IP](#) on page 61).
- See also [Managing Alarms](#) on page 63 for monitoring managed alarms.



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

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



Configuring UMP Interface for WebSocket Tunnel (Cloud Architecture Mode)

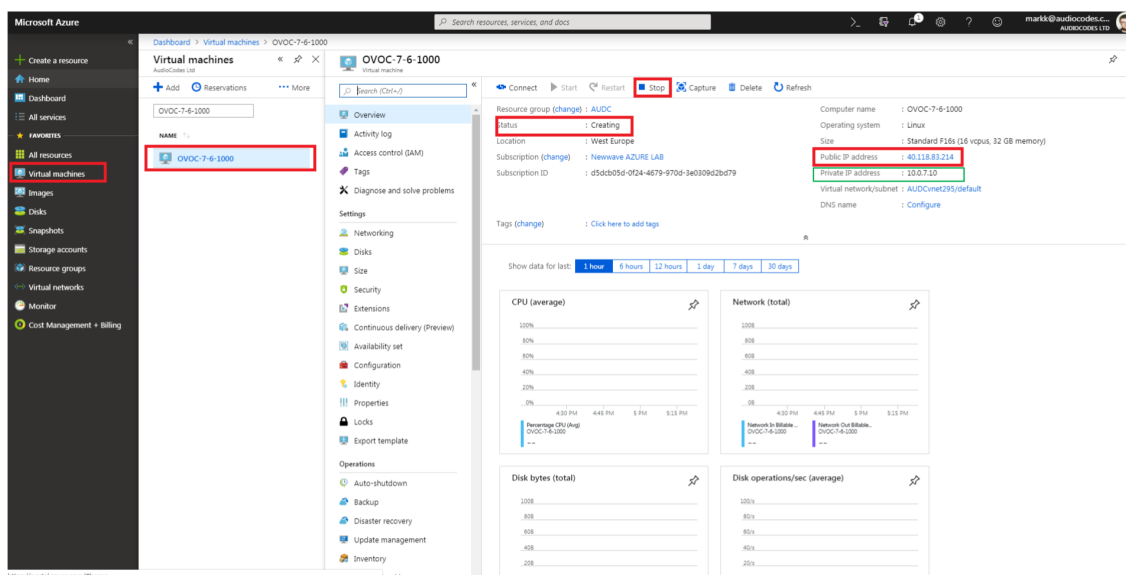
This section describes how to secure the connection to the OVOC server public IP address using WebSocket tunnel.

➤ **Do the following:**

1. In the Multitenant portal Navigation pane, open the OVOC Settings page (**System Configuration > OVOC Settings**).

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 following figure shows where to extract the OVOC server IP address 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**.

Configuring 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**.

```


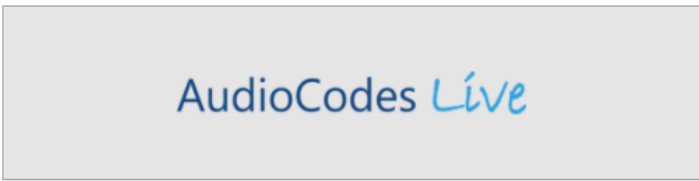
Main Menu> Network Configuration> Cloud Architecture

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 relevant IPv4 interface and then press Enter.
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**).

GENERAL SETTINGS

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

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\enterprise1user>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 "Server Certificates Updates" in the OVOC IOM manual).

Configuring SBC

This section describes the actions to perform on the SBC device.

➤ Do the following:

1. Install SSL certificates on managed SBC devices (refer to "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.

⬅ 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:

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:
a1:d1

```

2. Configure the OVOC Tunnel parameters that you configured in [Configuring WebSocket Tunnel \(Cloud Architecture Mode\) on OVOC](#) on page 53 [Configuring WebSocket Tunnel \(Cloud Architecture Mode\) on OVOC](#) on page 53.

The screenshot shows the 'Web Service Settings' page. On the left, a sidebar under 'NETWORK VIEW' lists various settings, with 'Web Service Settings' highlighted. The main panel is divided into two sections: 'GENERAL' and 'OVOC TUNNEL'.

GENERAL

- Topology Status: Enable (dropdown)
- Quality Status: ☐
- Quality Status Rate: 60 (text input)
- Debug Level: 1 (text input)
- Routing Server Registration Status: Disable (dropdown)

OVOC TUNNEL

- OVOC WebSocket Tunnel Server Address: 13.94.226.66 (text input with lightning bolt icon)
- Path: tun (text input with lightning bolt icon)
- Username: VPN (text input with lightning bolt icon)
- Password: ***** (password field with eye icon)
- Secured (HTTPS): ☒ (checkbox with lightning bolt icon)
- Verify Certificate: ☐ (checkbox with lightning bolt icon)

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

- HTTP and HTTPS
- HTTPS Only

The screenshot shows the 'Web Settings' page. On the left, a sidebar under 'TIME & DATE' lists various settings, with 'Web Settings' highlighted. The main panel is divided into two sections: 'GENERAL' and 'SESSION'.

GENERAL

- Secured Web Connection (HTTPS): HTTP and HTTPS (dropdown with lightning bolt icon)
- Require Client Certificates for HTTPS connection: Disable (dropdown)

SESSION

- Password Change Interval (minutes): 0 (text input)
- User Inactivity Timeout (days): 90 (text input)
- Session Timeout (minutes): 15 (text input)

Configuring 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 Multitenant portal Navigation pane, open the OVOC Settings page (**System Configuration > OVOC Settings**).
2. In the Public IP address field, enter the Public IP address of OVOC on Azure.

OVOC Settings

Connection

☐ Use public OVOC

IP Address: 10.0.1.4

Trap Port: 162

Keep Alive Port: 1161

SNMP

☒ SNMPv2 ☐ SNMPv3

Community Read: public

Community Write: private

Apply Changes Reset Changes

System Settings

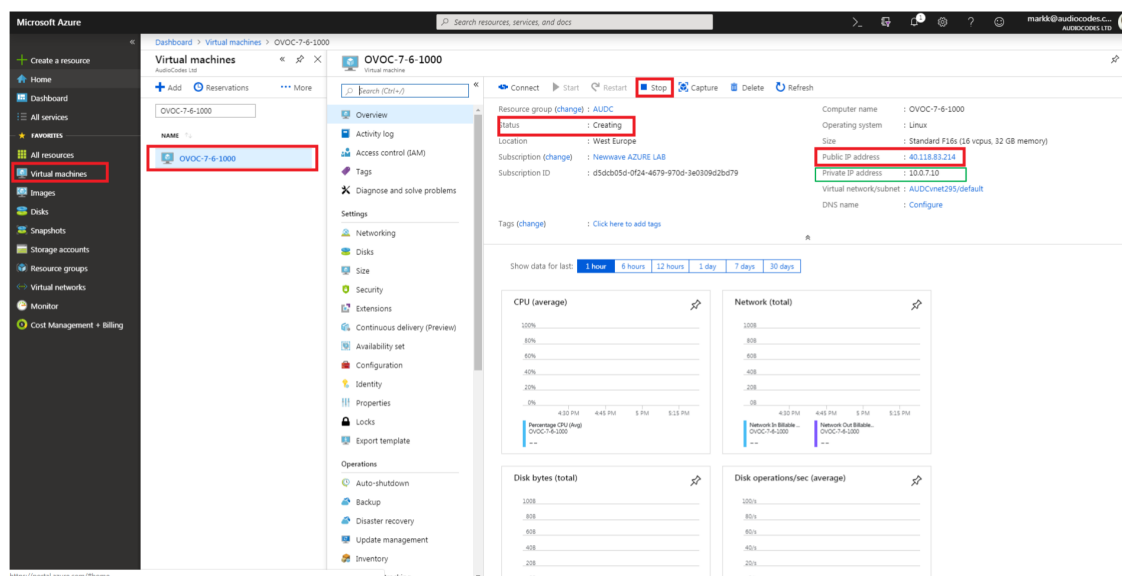
System Name: UMP Sandbox3 sp1

Location:

Access Settings

Login Url: http://10.0.2.5/tenantui

The following figure shows where to extract the IP address of OVOC server 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

3. Click **Apply Changes**.
4. 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.

GENERAL SETTINGS

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

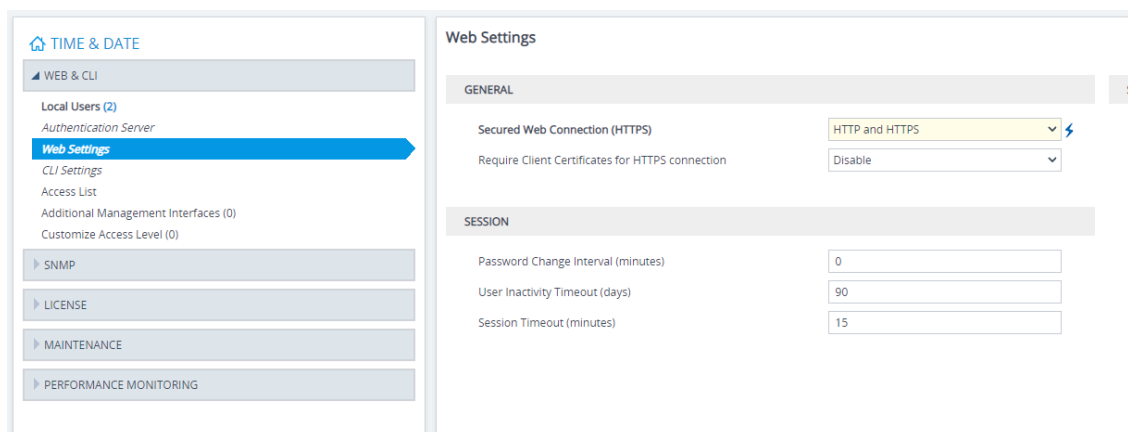
Submit

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

```
C:\Users\enterprise1user>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. **5.** In the OVOC Server Manager install Custom Certificates (see “Server Certificates Updates”).
4. **6.** 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



Configuring 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 Multitenant portal Navigation pane , open the OVOC Settings page (**System Configuration > OVOC Settings**).
2. In the IP Address field, enter the Private IP address of the OVOC Azure server.

OVOC Settings

Connection

☐ Use public OVOC

IP Address: 10.0.1.4

Trap Port: 162

Keep Alive Port: 1161

SNMP

☒ SNMPv2 ☐ SNMPv3

Community Read: public

Community Write: private

System Settings

System Name: UMP Sandbox3 sp1

Location:

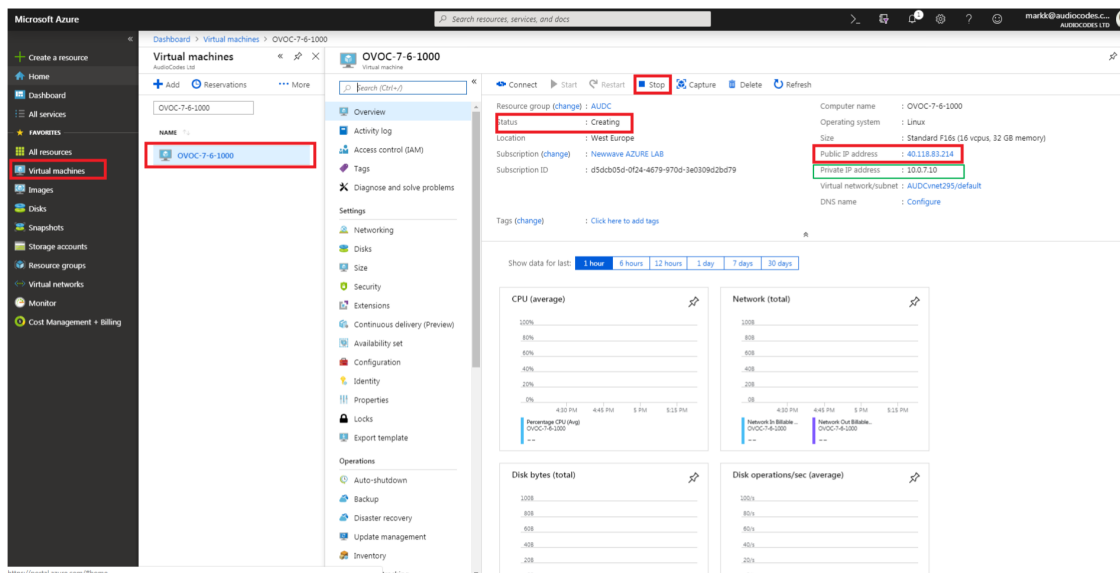
Access Settings

Login URI: http://10.0.2.5/tenantui

Apply Changes Reset Changes

Copyright © 2023 AudioCodes. All rights reserved.

The following figure shows where to extract the IP address of 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**.

Managing Alarms

The Alarms screen displays alarms that are raised on the UMP-365 server and are forwarded to Live Cloud for the following categories:

- Current alarms
- Cleared alarms
- Agent Alarms
- OVOC events



See [OVOC Alarms Guide](#) for details on alarms raised by UMP-365.

➤ To view alarms:

1. In the Navigation pane, select **OVOC > Alarms**.

Id	Alarm Time	Name	Source	Text	Severity
41964	January 20th 2024, 06:56	umpOcSyncOperationFailedAlarm	syncreleasefromaccountjob	SyncReleaseFromAccountJob.SyncAsync: Call failed with status code 403 (Forbidden): GET https://operatorconnect.microsoft.com/api/v2.0/number-management/tn-release-order?top=10000	Minor
42520	January 20th 2024, 21:55	umpOcSyncOperationFailedAlarm	syncacquirednumbers	SyncAcquiredNumbers.SyncAsync: Internal server error. Please contact support.	Minor
44338	January 22nd 2024, 23:10	umpOcSyncOperationFailedAlarm	syncleads	SyncLeads.SyncAsync: SyncLeads job finished with error during step: retrieve the civic addresses.	Minor
44339	January 22nd 2024, 23:36	umpOcSyncOperationFailedAlarm	syncuploadtoaccountjob	SyncUploadToAccountJob.SyncAsync: Call timed out: GET https://operatorconnect.microsoft.com/api/v2.0/number-management/tn-upload-to-account/?top=10000	Minor
44488	January 23rd 2024, 03:34	umpOcSyncOperationFailedAlarm	syncuploadtoaccountjob	SyncUploadToAccountJob.SyncAsync: Exception of type 'SysAdmin.Peering.Infrastructure.TnNumberManagementException' was thrown.	Minor
44526	January 23rd 2024, 03:59	umpOcSyncOperationFailedAlarm	syncuploadtoaccountjob	SyncUploadToAccountJob.SyncAsync: Exception of type 'SysAdmin.Peering.Infrastructure.TnNumberManagementException' was thrown.	Minor
46377	January 25th 2024, 06:05	umpOcSyncOperationFailedAlarm	syncacquirednumbers	SyncAcquiredNumbers.SyncAsync: Internal server error. Please contact support.	Minor
46600	January 25th 2024, 12:39	umpOcSyncOperationFailedAlarm	syncuploadtoaccountjob	SyncUploadToAccountJob.SyncAsync: Exception of type 'SysAdmin.Peering.Infrastructure.TnNumberManagementException' was thrown.	Minor
48007	January 27th	umpOcSyncOperationFailedAlarm	syncacquirednumbers	SyncAcquiredNumbers.SyncAsync: Exception of type	Minor

For each alarm the following information is displayed:

Field	Description
Id	SNMP OID

Field	Description
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.

11 Multitenant Portal Licensing

Multitenant portal supports the following licensing schemes:

■ **Tenants:** Tenants license includes the following features support:

- Quick Connect
- Tenant Online voice routing
- User view only



A **Tenant** License is mandatory requirement for Onboarding a new customer M365 Tenant and for managing the Voice Routing.

■ **Users:** 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 implementation)
- Manage emergency call Routing (Future)



A **User** License is not mandatory. The provider can offer this service as an upscale service for selected customers.

See the following:

- [Installing the Multitenant License](#) below
- [Configuring Global License Settings](#) on page 168

Installing the Multitenant License

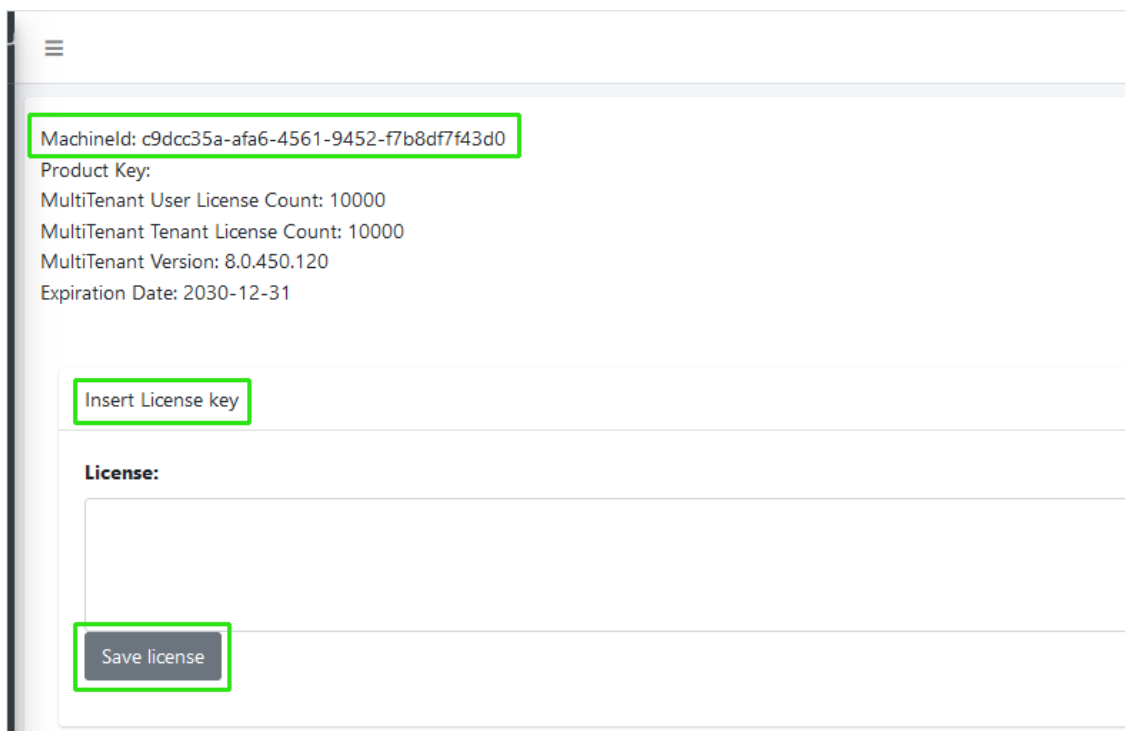
This section describes how to install the UMP 365 license. The license configuration includes the following parameters:

- MachineID: Generated by the UMP server; required for the license generator tool
- MultiTenant User License Count: total # of User Licenses across all tenants i.e. Pool License
- MultiTenant Tenant License Count: total # of Tenant Licenses
- MultiTenant Version: Software Version
- Expiration Date: Expiration Validation period for License file

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 available licenses. Existing users that have already been edited can still be edited, however new users cannot be edited until new licenses are generated. 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). A Tenant License is a mandatory requirement for Onboarding a new customer M365 Tenant and for managing the Voice Routing. A User License is required for mandatory for supporting Teams Calling plans and therefore The license should be allocated based on the total number of users required for Teams Calling plan licenses.

➤ **To configure the license:**

1. Login to the Multitenant interface with the Windows UMP Service account created in [Creating UMP Service Account](#) on page 29.
2. In the Navigation pane, select **System > License**.
3. Extract the MachineId.



MachinelD: c9dcc35a-afa6-4561-9452-f7b8df7f43d0

Product Key:

MultiTenant User License Count: 10000

MultiTenant Tenant License Count: 10000

MultiTenant Version: 8.0.450.120

Expiration Date: 2030-12-31

Insert License key

License:

Save license

4. Activate your product through the AudioCodes License Activation tool at <http://www.audiocodes.com/swactivation>



You require your Product Key and Fingerprint (MachineID) for this activation process. An e-mail will subsequently be sent to you with your Product License.

5. Copy the License Key string in the Insert License key field and then click **Save license**.

12 Configuring Invitation Settings

This step describes how to define Invitation Settings for requesting consent from customer IT administrators using the token-based authentication mechanism (See [Grant Consent using only Token-based Authentication](#)) 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 [Register End Customer Tenant DNS Sub domains](#) on page 250. 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 [Customer Invitations](#)).

➤ **Do the following:**

1. Login to the Multitenant portal with Windows UMP Service account created in [Creating UMP Service Account](#).
2. In the Multitenant portal Navigation pane, open the Invitation Settings page (**System > Invitation Settings**).

The screenshot displays the 'Invitation Settings' configuration page. It includes three main input areas: 'Invitation Subject', 'Invitation Email', and 'Customer Authentication Portal Uri'. The 'Invitation Subject' field is pre-filled with a template using a placeholder {{CustomerId}}. The 'Invitation Email' field shows a detailed email template, including a greeting, a welcome message, and a link to the authentication portal, also using placeholders. The 'Customer Authentication Portal Uri' field contains a specific URL. An 'Apply Changes' button is located at the bottom of the form. The page footer indicates copyright © 2020 AudioCodes.

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)

- `{{CustomerAuthenticationPortalUrl}}/{{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`

The value should be the DNS A record for domain that was created in [Creating A Records for SBC Devices](#). For example, Finebak.com to a Public IP xxx.xxx.xxx.xxx (UMP-365 – IP address).

See example email below.

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:
 - o Application Administrator

- o Skype for Business Admin

- o Teams Communications 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 Configuring Email Settings

This step describes how to define the email server settings for sending the invitation requests (configured in [Configuring Invitation Settings](#) on page 67) to the customer IT administrator for connecting to the Multitenant portal.

➤ **Do the following:**

1. Login to the Multitenant portal with Windows UMP Service account created in [Creating UMP Service Account](#) on page 29.
2. In the Multitenant portal Navigation page, open the Email Settings page (**System > Email Settings**).

The screenshot displays the 'Email Server Settings' configuration page. The form includes the following fields and values:

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

3. 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
4. Click **Apply Changes**.

14 Setting up Fully Automatic DNS Provisioning

Automatic provisioning of DNS records and derived trunk domain fully automates the onboarding process for a new Microsoft direct routing tenant. The wizard adds the new domain in the of end customer M365 tenant:

- Creates a PSTN gateway and domain
- Creates a TXT record in the Service Provider Azure DNS environment
- Adds A-Record to the Service Provider DNS environment
- Creates a temporary activation user in the end customer tenant with the newly created domain assigned and licensed with a Microsoft Office 365 Phone System user license.



- The following Administrative roles must be assigned to the Customer administrator (see [Assign Administrator Roles to IT Administrator](#) on page 269):
 - ✓ Domain Name Administrator (for txt and A-record creation)
 - ✓ User Administrator (for user license activation of the PSTN trunk)

The automatic provisioning of the DNS sub domains requires the following setup on Service Provider Azure tenant:

- [Registering DNS Application \(Service Provider Tenant\)](#) below
- [Creating A Records for SBC Devices](#) on page 74
- [Assign Access Control](#) on page 77
- [Configure DNS API](#) on page 82

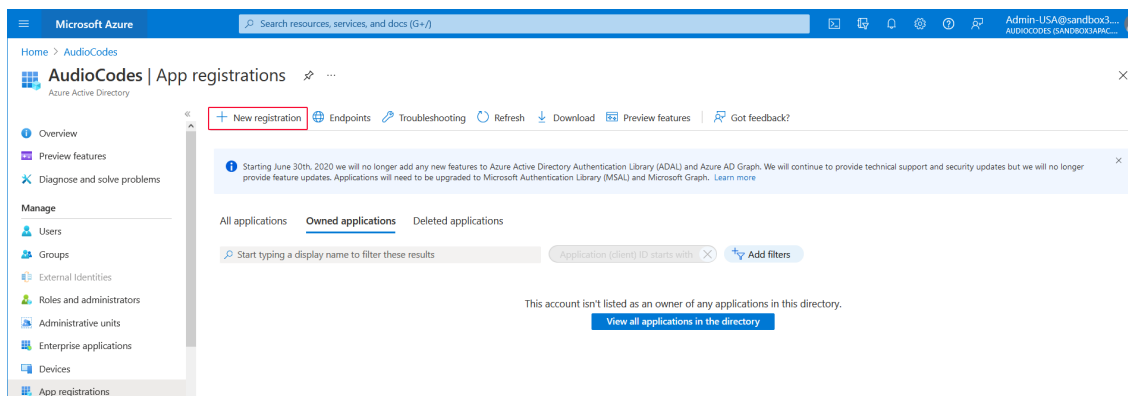
Once the above setup has been completed, the Onboarding wizard can be used to provision the DNS sub domains (see [Fully Automatic DNS Provisioning](#) on page 393).

Registering DNS Application (Service Provider Tenant)

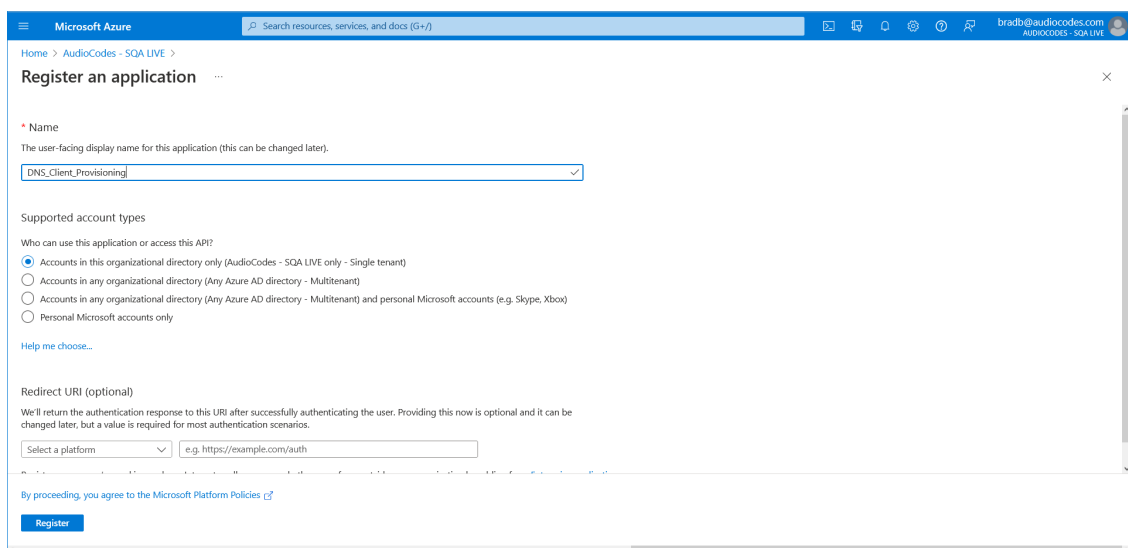
The DNS registration for the Service Provider tenant includes the generation of a Client Secret that is only displayed once. It should be captured and saved for later configuration in the Multi-tenant interface.

➤ To register the DNS domain:

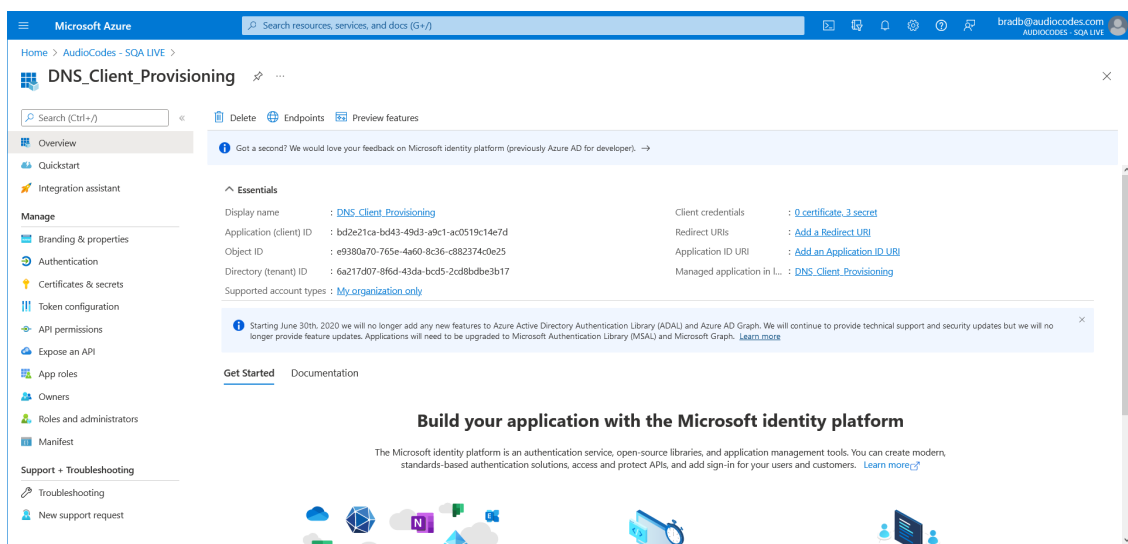
1. In the Navigation pane, select **App registrations** and then click **New registration**.



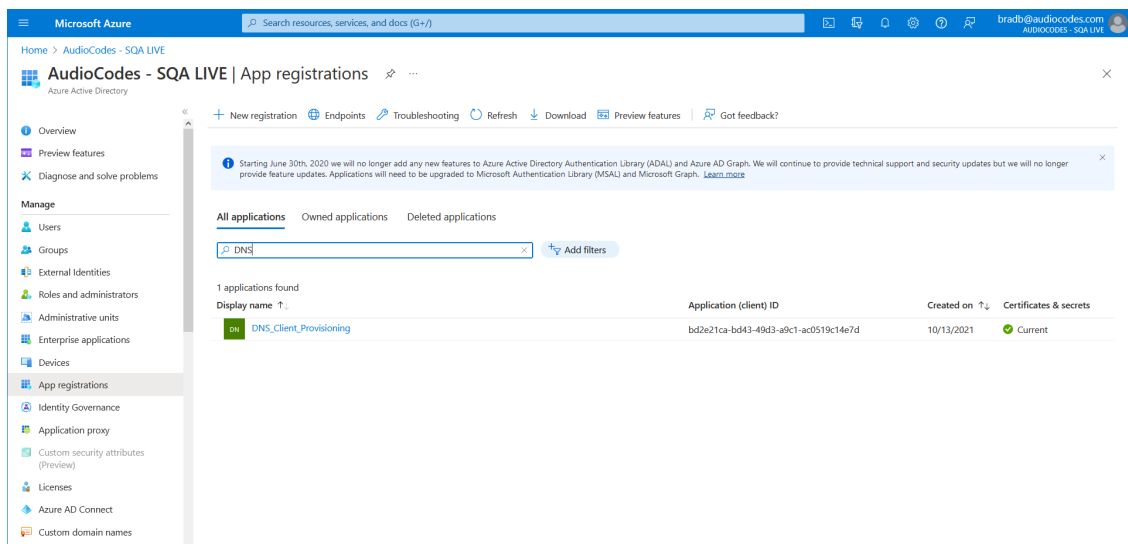
2. Enter the name of the new registration e.g. `DNS_Client_Provisioning` and then click **Register**.



A new registration is created.

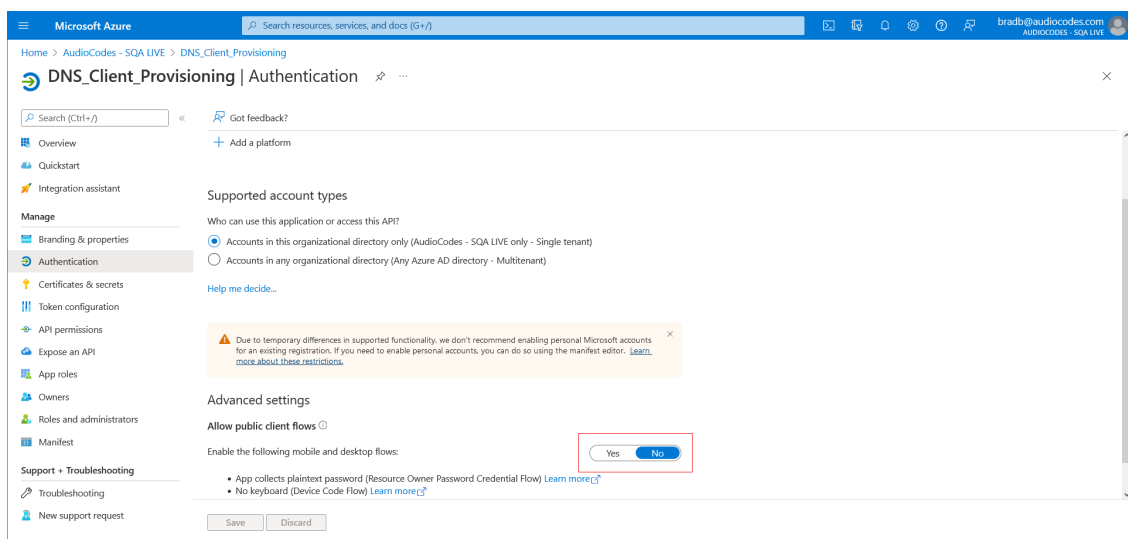


3. In the Navigation pane, select **App registrations**. The new registration is listed.



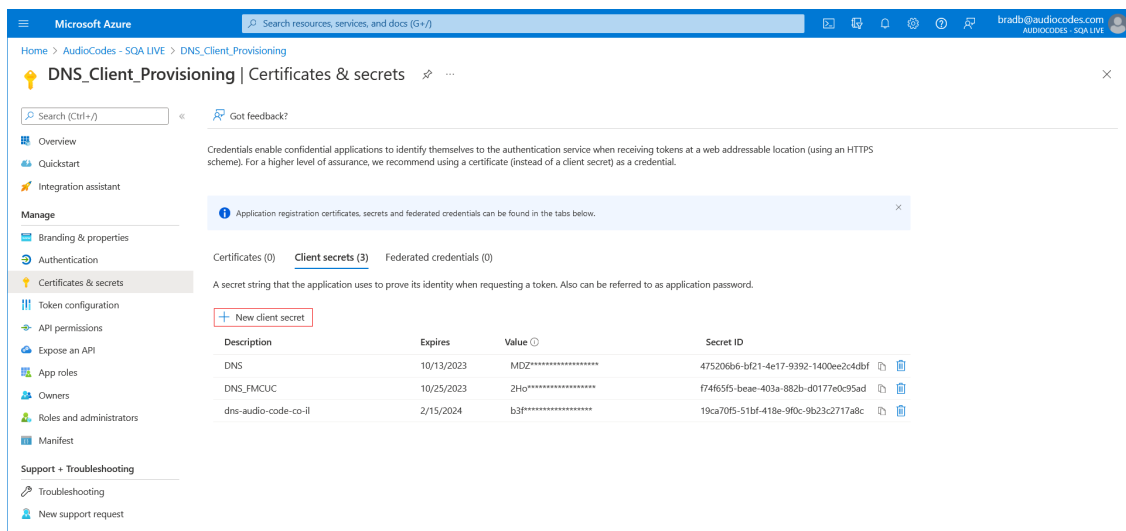
4. Click the new registration (Dns_Client_Provisioning) and then in the Navigation pane, select **Authentication**.

5. Under Advanced Settings, select **No** to disable mobile and desktop flows.



6. Click **Save**.

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



Microsoft Azure | Search resources, services, and docs (G+/J)

Home > AudioCodes - SQA LIVE > DNS_Client_Provisioning

DNS_Client_Provisioning | Certificates & secrets

Search (Ctrl+/) | Got feedback?

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

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

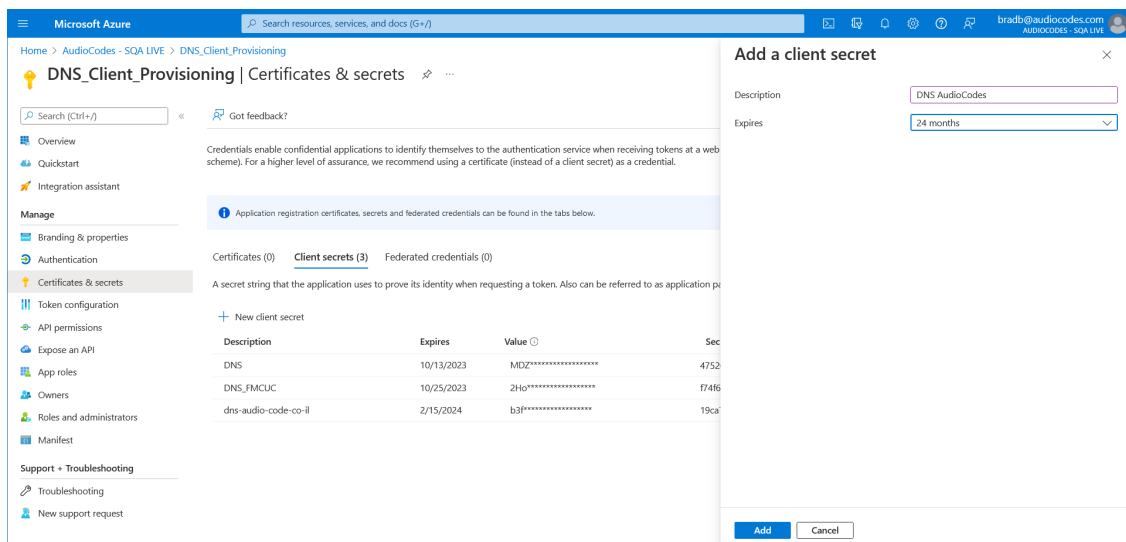
Certificates (0) **Client secrets (3)** Federated credentials (0)

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
DNS	10/13/2023	MDZ*****	475206b6-bf21-4e17-9392-1400ee2c4dbf
DNS_FMCUC	10/25/2023	2Ho*****	f7465f5-beae-403a-882b-d0177e0c95ad
dns-audio-code-co-il	2/15/2024	b3f*****	19ca70f5-51bf-418e-9f0c-9b23c2717a8c

8. Click New client secret.



Microsoft Azure | Search resources, services, and docs (G+/J)

Home > AudioCodes - SQA LIVE > DNS_Client_Provisioning

DNS_Client_Provisioning | Certificates & secrets

Search (Ctrl+/) | Got feedback?

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

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (3)** Federated credentials (0)

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
DNS	10/13/2023	MDZ*****	475206b6-bf21-4e17-9392-1400ee2c4dbf
DNS_FMCUC	10/25/2023	2Ho*****	f7465f5-beae-403a-882b-d0177e0c95ad
dns-audio-code-co-il	2/15/2024	b3f*****	19ca70f5-51bf-418e-9f0c-9b23c2717a8c

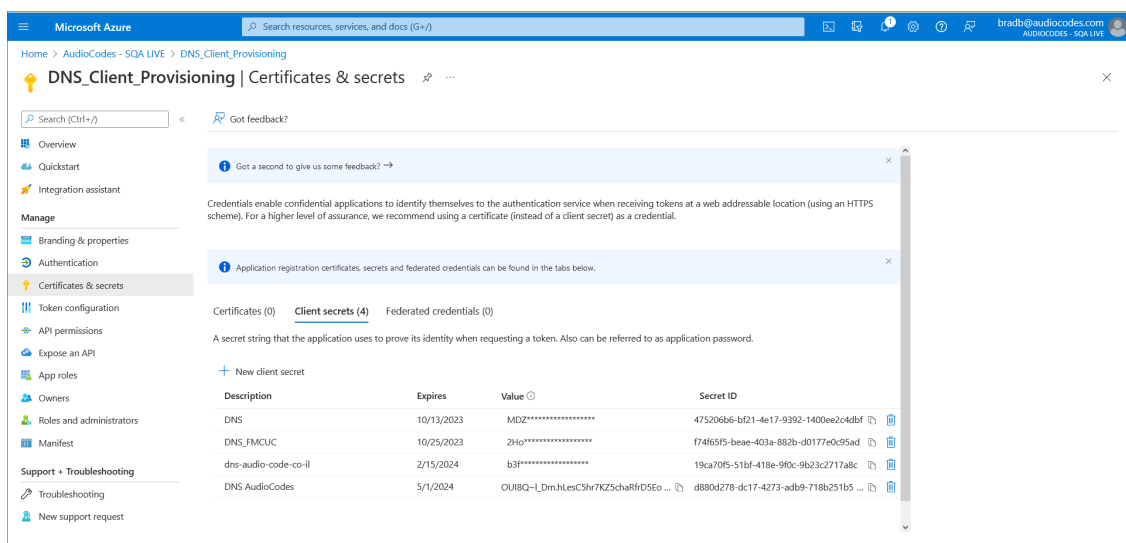
Add a client secret

Description:

Expires:

[Add](#) [Cancel](#)

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



Microsoft Azure | Search resources, services, and docs (G+/J)

Home > AudioCodes - SQA LIVE > DNS_Client_Provisioning

DNS_Client_Provisioning | Certificates & secrets

Search (Ctrl+/) | Got feedback?

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

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

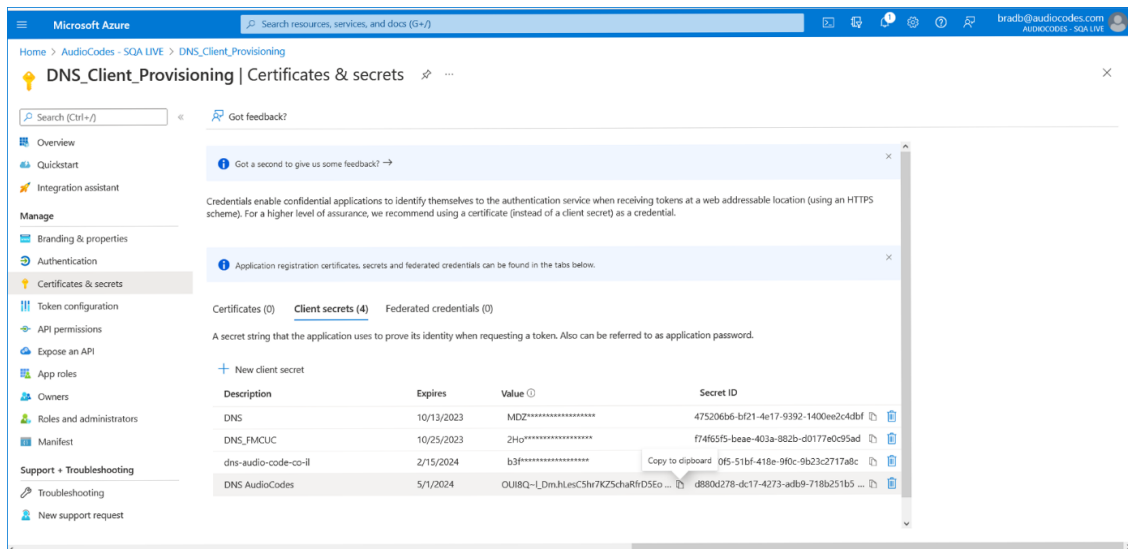
Certificates (0) **Client secrets (4)** Federated credentials (0)

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
DNS	10/13/2023	MDZ*****	475206b6-bf21-4e17-9392-1400ee2c4dbf
DNS_FMCUC	10/25/2023	2Ho*****	f7465f5-beae-403a-882b-d0177e0c95ad
dns-audio-code-co-il	2/15/2024	b3f*****	19ca70f5-51bf-418e-9f0c-9b23c2717a8c
DNS AudioCodes	5/1/2024	OUI8Q-L_Dm.hLesC5hr7KZ5chaRif05Eo ...	d880d278-dk17-4273-adb9-718b251b5 ...

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



Creating A Records for SBC Devices

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

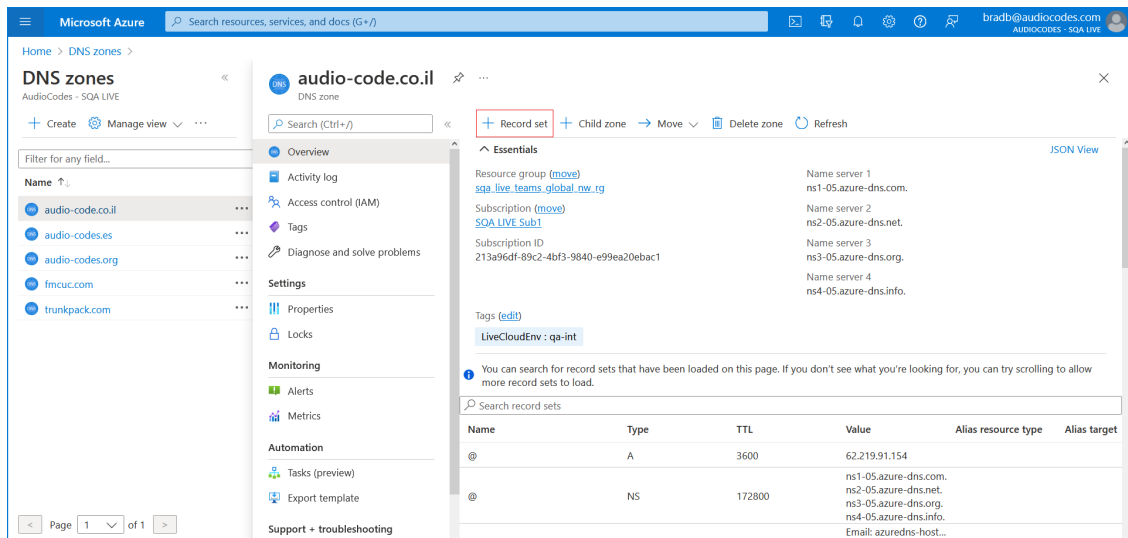
- US SBC = ussbc.audiocodes.be = IP of US SBC

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**.



The screenshot shows the Microsoft Azure portal interface for managing DNS zones. The left sidebar lists various DNS zones under the 'audio-code.co.il' domain. The main content area displays the 'audio-code.co.il' DNS zone details. A red box highlights the '+ Record set' button in the top navigation bar. Below this, the 'Essentials' section provides key information: Resource group (move), Subscription ID (213a96df-89c2-4bf3-9840-e99ea20ebac1), and Name servers (ns1-05.azure-dns.com, ns2-05.azure-dns.net, ns3-05.azure-dns.org, ns4-05.azure-dns.info). A table of record sets is displayed at the bottom, showing two records: an 'A' record for '@' with a TTL of 3600 and a value of 62.219.91.154, and an 'NS' record for '@' with a TTL of 172800 and a value of ns1-05.azure-dns.com, ns2-05.azure-dns.net, ns3-05.azure-dns.org, ns4-05.azure-dns.info.

Name	Type	TTL	Value	Alias resource type	Alias target
@	A	3600	62.219.91.154		
@	NS	172800	ns1-05.azure-dns.com, ns2-05.azure-dns.net, ns3-05.azure-dns.org, ns4-05.azure-dns.info		Email: azure-dns-host...

Add record set

×

audio-code.co.il

Name

customers ✓

.audio-code.co.il

Type

A – Alias record to IPv4 address ▼

Alias record set ⓘ

☒ Yes ☐ No

Alias type

☒ Azure resource ☐ Zone record set

Choose a subscription *

SQA LIVE Sub1 ▼

Azure resource *

qa-int-sbc3-ip ▼

TTL * TTL unit

1 Hours ▼

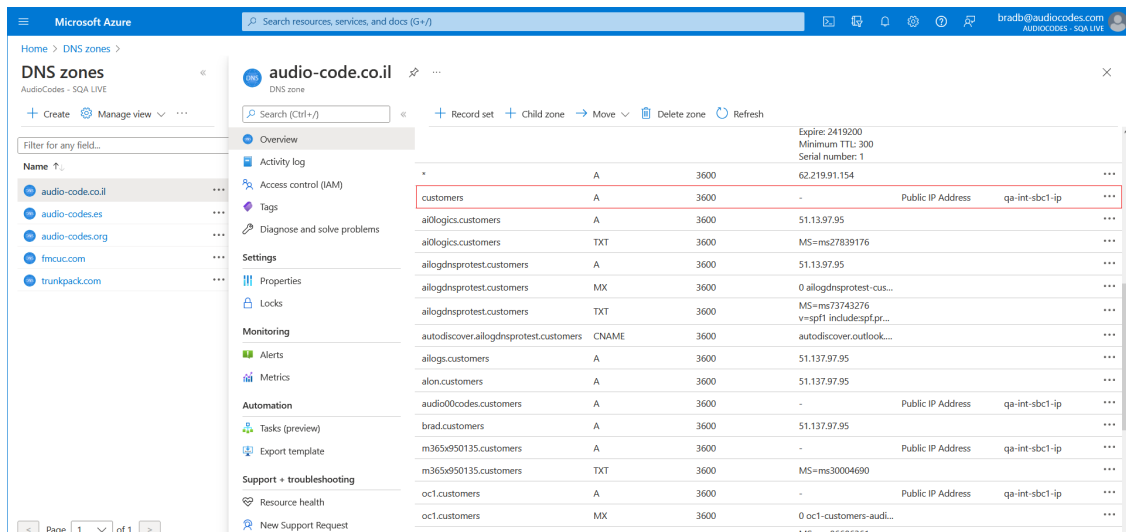
OK

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 following figure displays the newly added records.

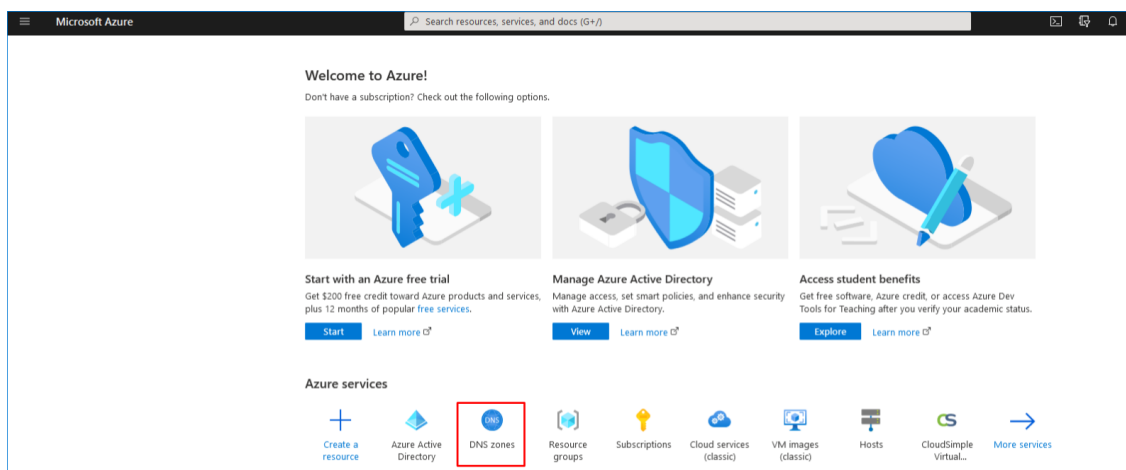


Assign Access Control

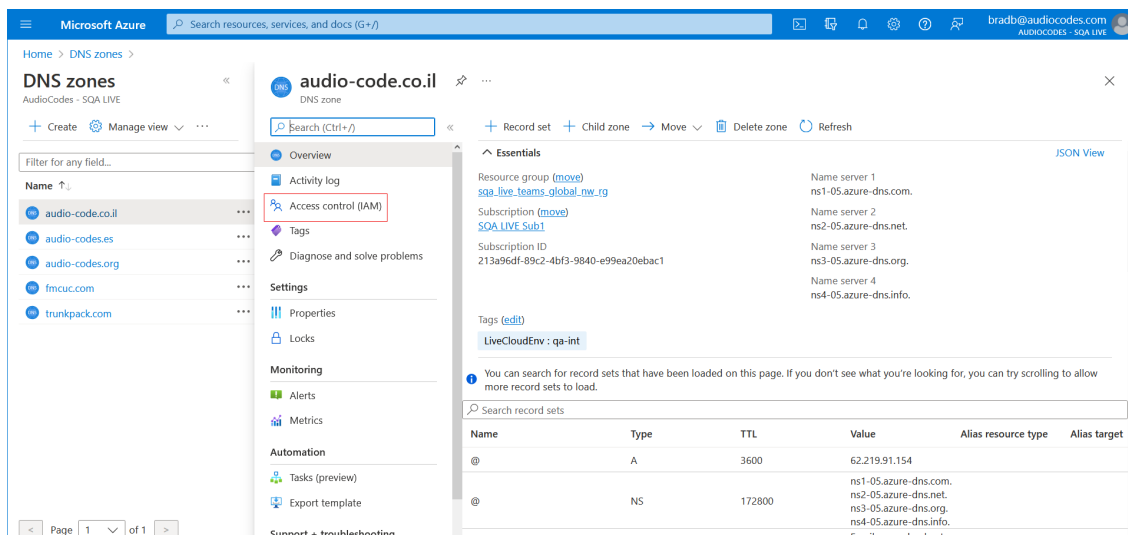
On the created subdomain, assign access control to the app registration to allow the DNS Application registration (Enterprise Application) to access the DNS zone. In this example, the DNS Application DNS_Client_Provisioning needs access to the subdomain customers.audio-code.co.il. The permission used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

➤ To assign access control:

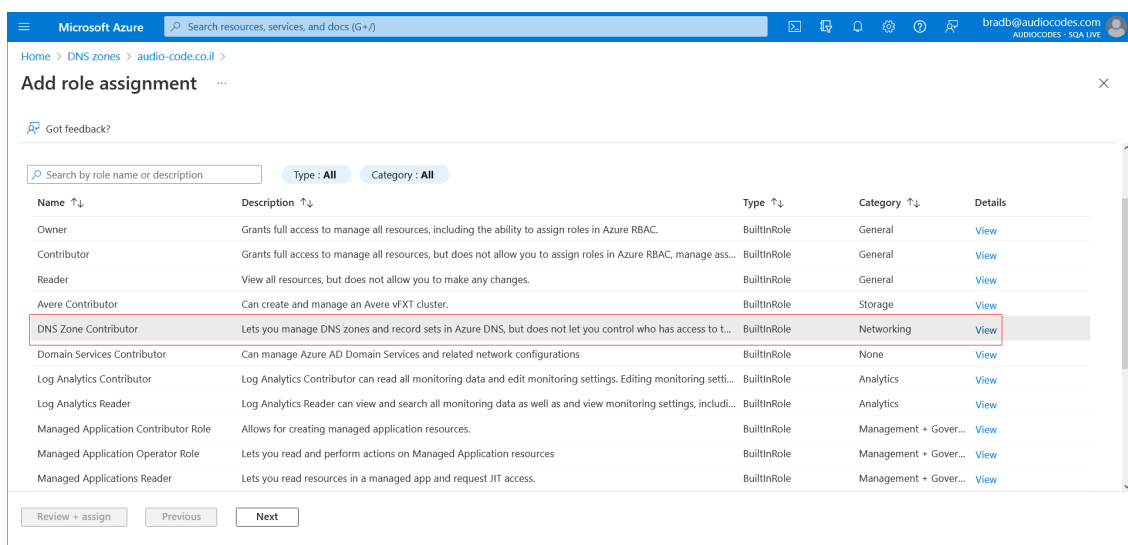
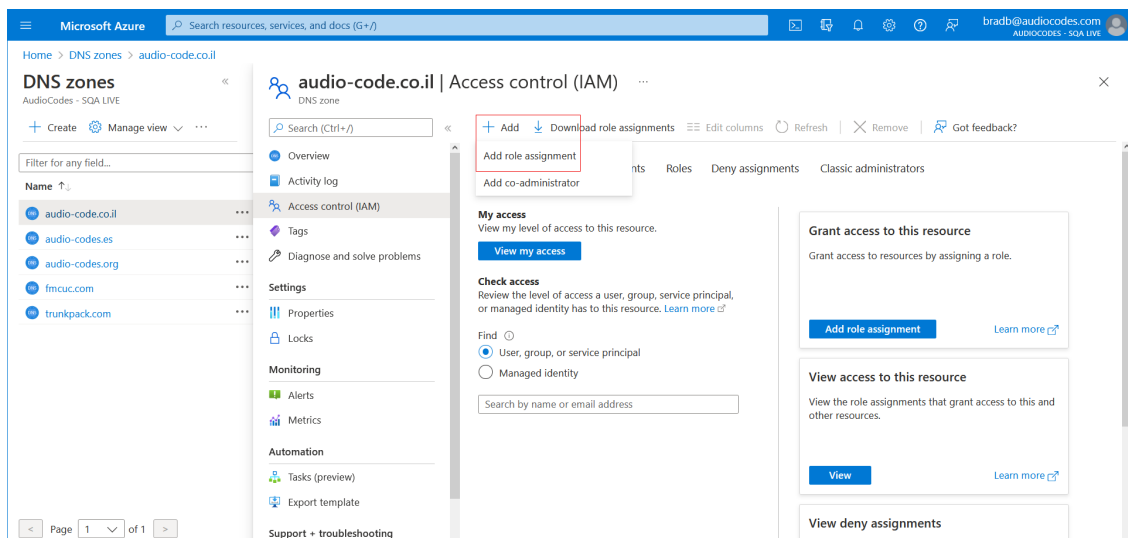
1. In the Azure Portal Home page pane, select **DNS Zones**.



2. Select the relevant Provider zone and then click **Access control (IAM)**.



3. Click Add > Add role assignment.



4. Configure the role assignment as shown in the following figure.

Microsoft Azure Search resources, services, and docs (G+)

Home > DNS zones > audio-code.co.il >

Add role assignment

Got feedback?

Role **Members** Review + assign

Selected role DNS Zone Contributor

Assign access to ☒ User, group, or service principal ☐ Managed identity

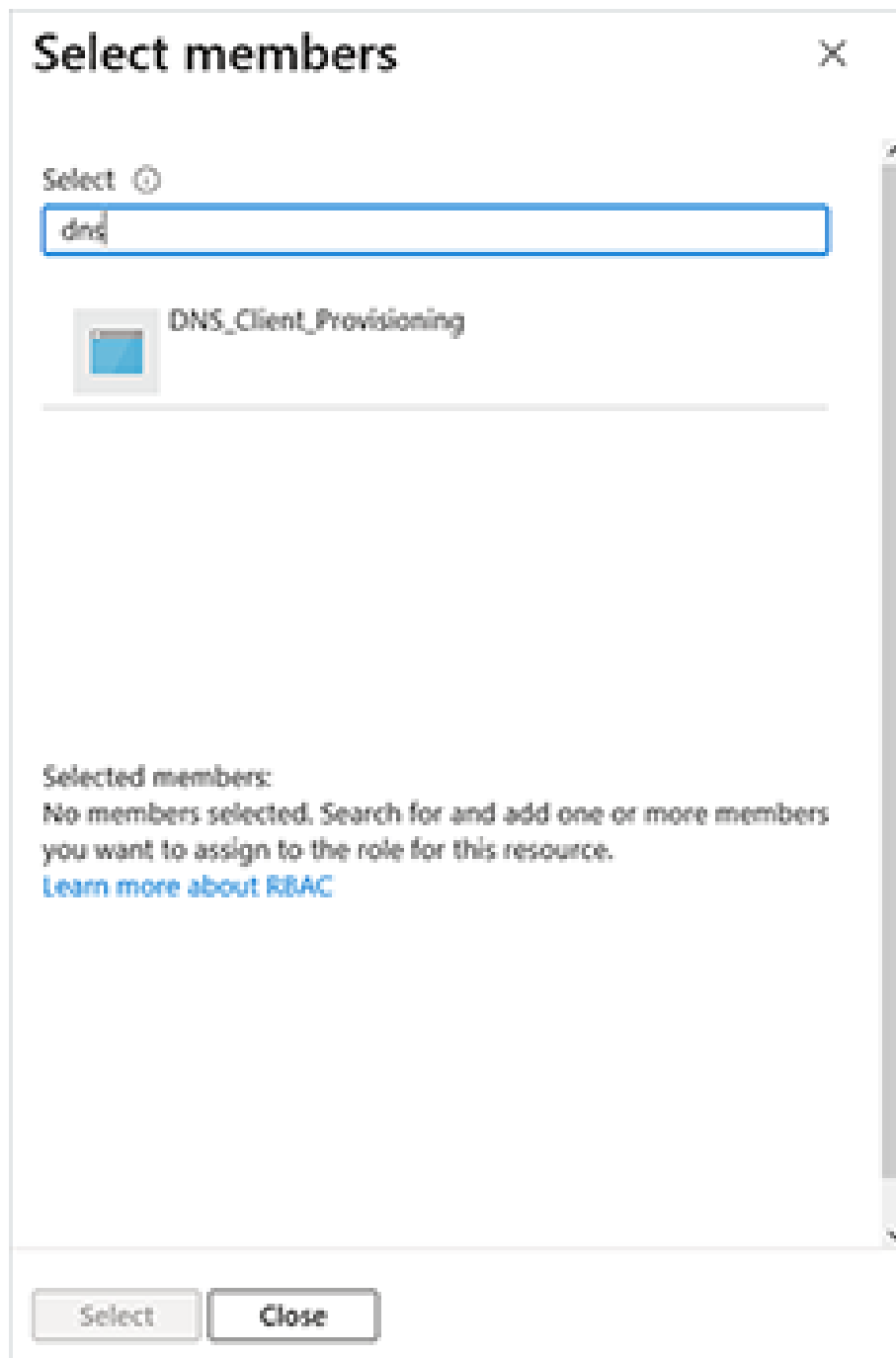
Members + Select members

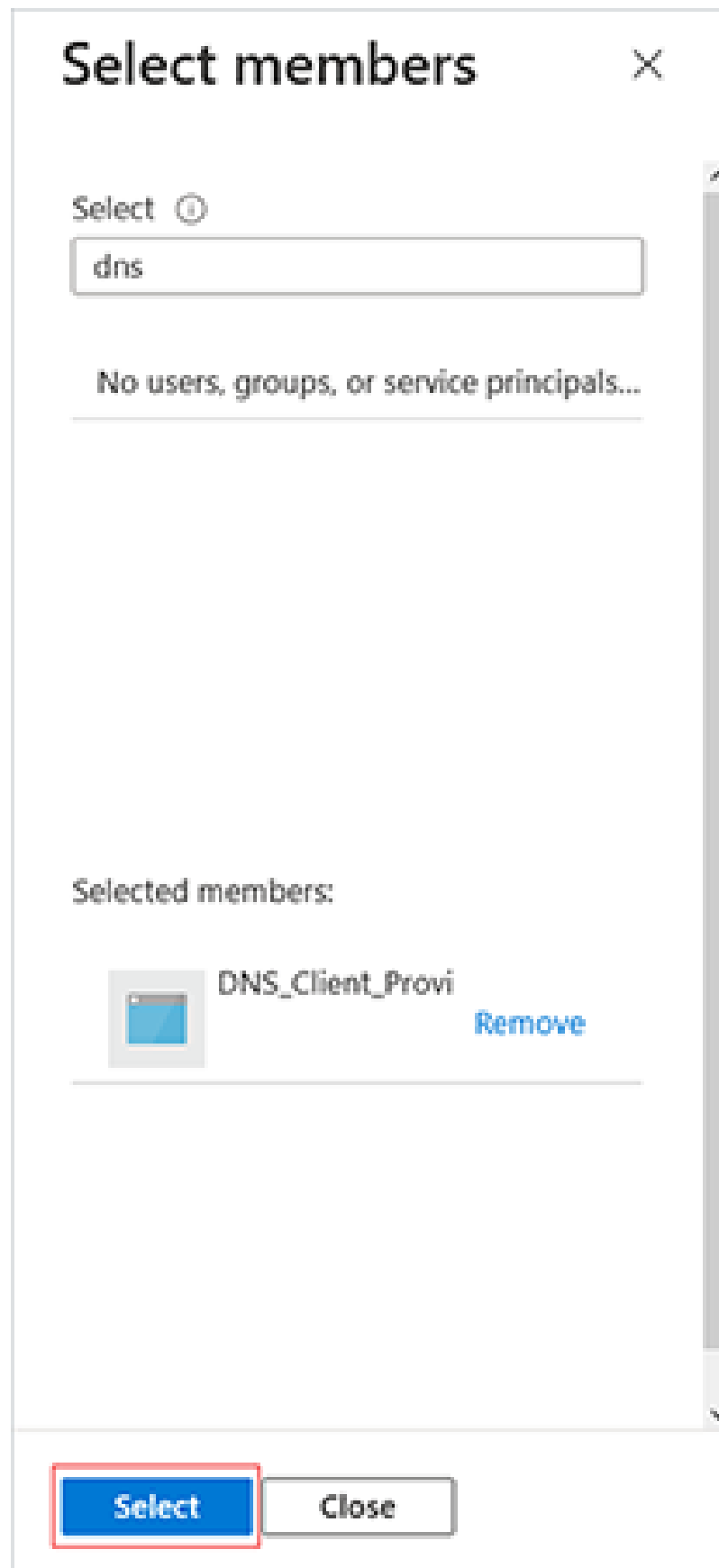
Name	Object ID	Type
No members selected		

Description Optional

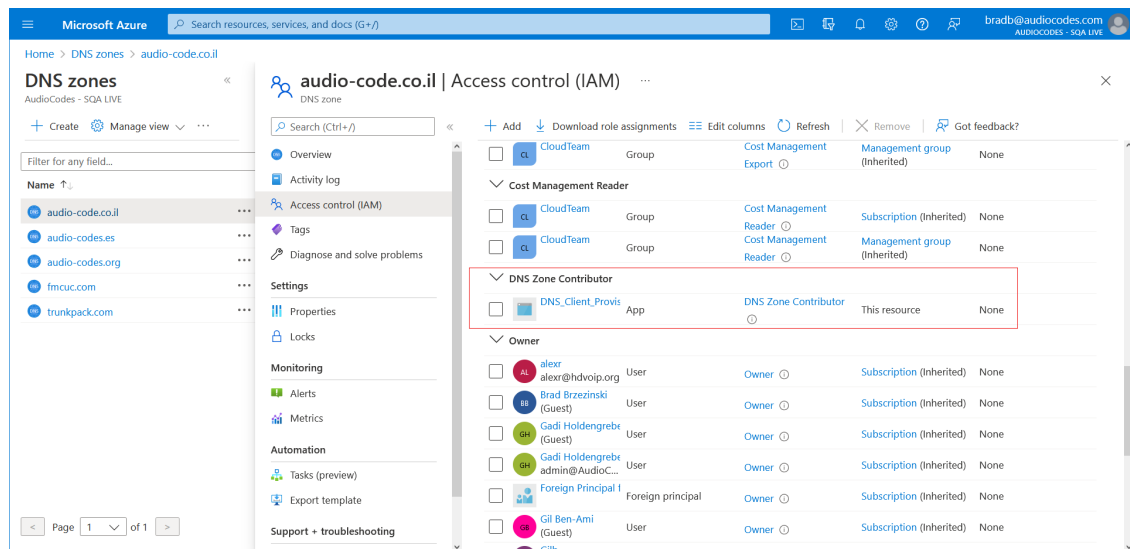
Review + assign Previous Next

5. Search for the DNS Registration that you created in [Registering DNS Application \(Service Provider Tenant\)](#) on page 70 and then click **Select**.





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



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 [Registering DNS Application \(Service Provider Tenant\)](#) on page 70 and the adding of DNS records for each region site locations based on the configuration in [Creating A Records for SBC Devices](#) on page 74.

➤ To configure DNS API:

- In the Multitenant Navigation pane, open the DNS API Configuration screen (**System > DNS API Configuration**).

#	Name	SbcId	Fqdn	Ip Address
1	OC1_SBC	2	customers.audio-code.co.il	51.137.97.95
2	OC2_SBC	3	customers.audio-code.co.il	52.178.43.85
3	test1	2	customers.audio-code.co.il	51.137.97.95

- Configure parameters as described in the table below.

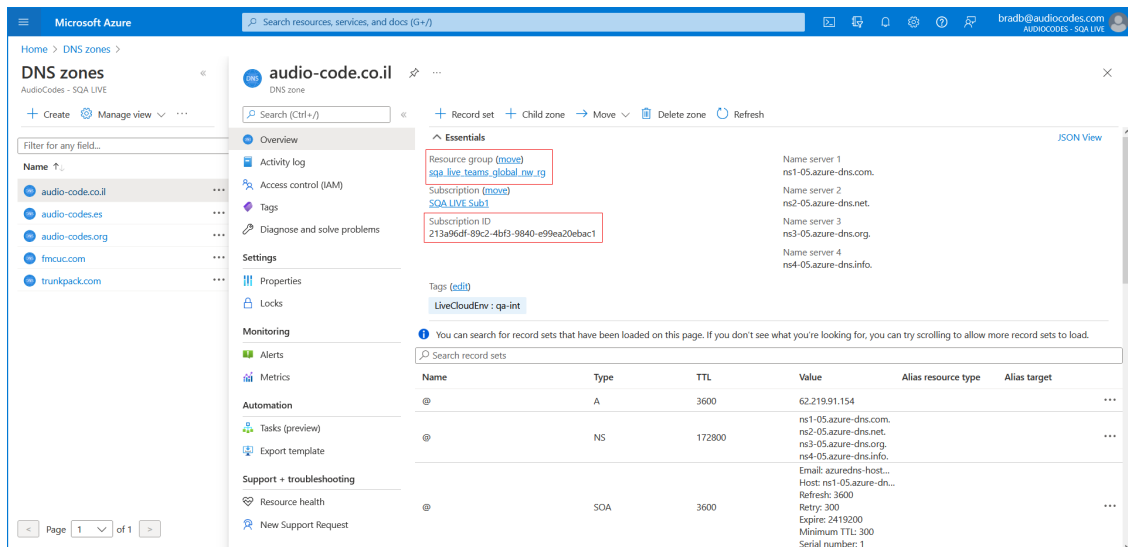
Table 14-1: DNS API Configuration

Parameter	Description
Tenant Id	Directory (tenant) ID for the UMP-365 (extracted from the Overview page of the DNS application registration (see example DNS_Client_Provisioning below).
Client Id	Application (Client) id of the DNS application registration (extracted from the Overview page of the DNS application registration).
Client Secret	Client Secret of the DNS application registration (extracted from the Certificates & Secrets page of the DNS application registration). This value is only shown during creation.
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.

The screenshot shows the Microsoft Azure portal interface for the 'DNS_Client_Provisioning' application. The left sidebar contains navigation links for 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, and New support request. The main content area displays the 'Essentials' section with the following details:

- 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-bcd5-2cd8bde3b17](#)
- 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 Essentials section, there is a 'Get Started' section with a 'Documentation' link. The bottom of the page features a banner for 'Build your application with the Microsoft identity platform' with a 'Learn more' link.



- 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 end 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 [Fully Automatic DNS Provisioning](#) on page 393 [Fully Automatic DNS Provisioning](#) on page 393 below).
 - **Sbclid:** Id of the SBC device in the SQL database.
 - **Fqdn:** A-Record added for the region SBC in [Creating A Records for SBC Devices](#) on page 74.
 - **IP Address:** IP address of the region SBC device.

Name **Sbc** **FQDN** **Ip Address**

Please enter a valid Name oc1.customers.audio-code.co.il oc1.customers.audio-code.co.il 51.137.97.95

Add **Reset Fqdn** **Resolve Address**

#	Name	Sbclid	Fqdn	Ip Address	
1	OC1_SBC	2	customers.audio-code.co.il	51.137.97.95	Edit
2	OC2_SBC	3	customers.audio-code.co.il	52.178.43.85	Edit
3	test1	2	customers.audio-code.co.il	51.137.97.95	Edit

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

The screenshot displays the Audiocodes management console interface. On the left is a sidebar with navigation options: Tenants, Ovoc, System, License, Invitation Settings, Email Settings, Script Templates, DNS API Configuration, Security, SBC List, and Queued Tasks. The main panel shows the configuration for a specific tenant. Fields include Tenant Id, Client Id, Client Secret, Subscription Id, Resource Group Name, and Dns Zone. A table lists configured DNS entries:

#	Name	Sbcl	Fqdn	Ip Address
11	APAC	1	customers.audiocodes.be	13.80.148.30
12	EMEA	2	customerslatam.audiocodes.be	23.97.197.41

Buttons for 'Add', 'Reset Fqdn', and 'Resolve Address' are visible above the table. The bottom of the console shows a copyright notice for 2020 Audiocodes and a Windows activation watermark.

Table 14-2: 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.

15 Configuring Microsoft Teams Direct Routing SBC

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:

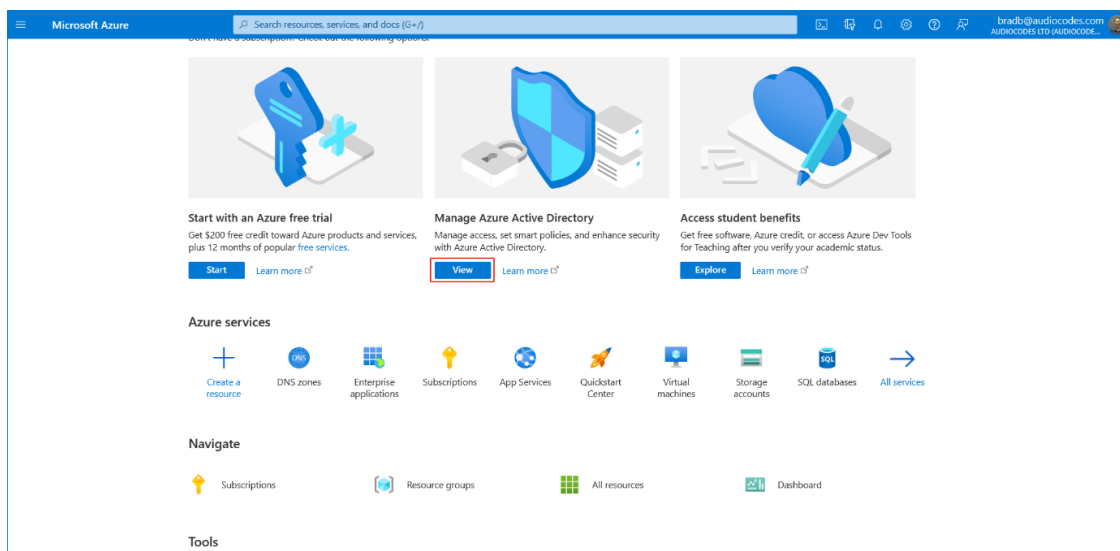
<https://www.audiocodes.com/media/13161/connecting-audiocodes-sbc-to-microsoft-teams-direct-routing-hosting-model-configuration-note.pdf>

16 Create Registration for Customer Administrators

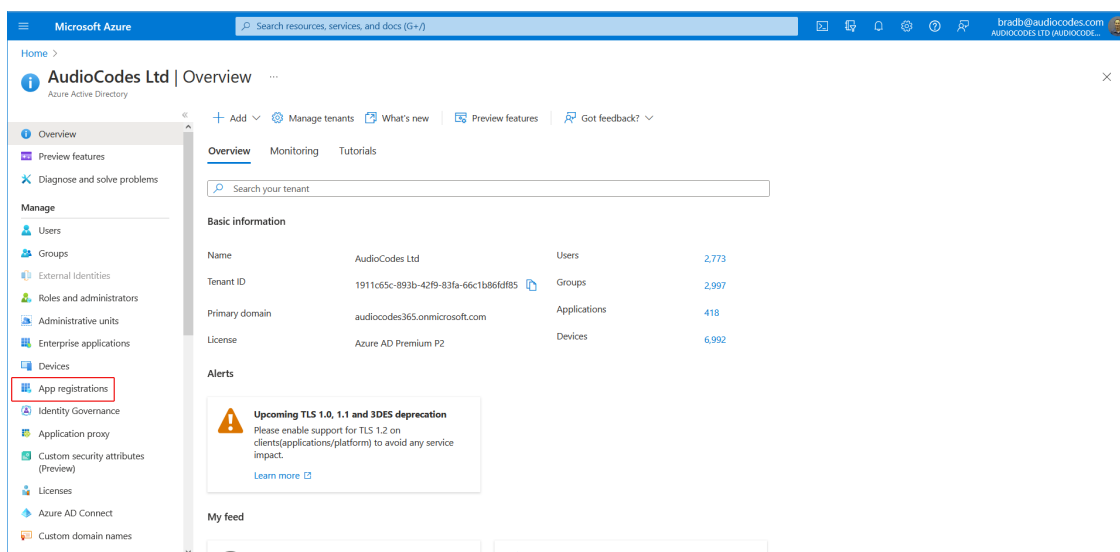
The Customer Admins App Registration enables the Azure sign-on for end user customer IT administrators (see [Initial Access to UMP-365 and Assigning Customer Admins](#) on page 425). Once this registration is complete, the Application (Client) ID must be added in the Customer Admins screen in the Multitenant interface. When the customer IT administrator logs into UMP-365, they view only 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**.



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



4. Click **New registration**.

The image shows two screenshots from the Microsoft Azure portal. The top screenshot displays the 'App registrations' page for 'AudioCodes Netherlands BV'. A red box highlights the '+ New registration' button. Below it, a table lists 27 applications, including 'AuthenticationDemo', 'Create-Domain-Automation-Demo', 'Demo-Dns-Client', 'Demo-MS-Teams-P5-Module', 'Demo auth tenant', 'Demo111', 'Fundatie Demo', 'MSAL-Token-simplify', 'My UWP App', and 'MyApp'. The bottom screenshot shows the 'Register an application' form. A red box highlights the 'Name' field, which contains 'UMP customer portal'. Another red box highlights the 'Supported account types' section, where the option 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)' is selected. A third red box highlights the 'Register' button at the bottom of the form.

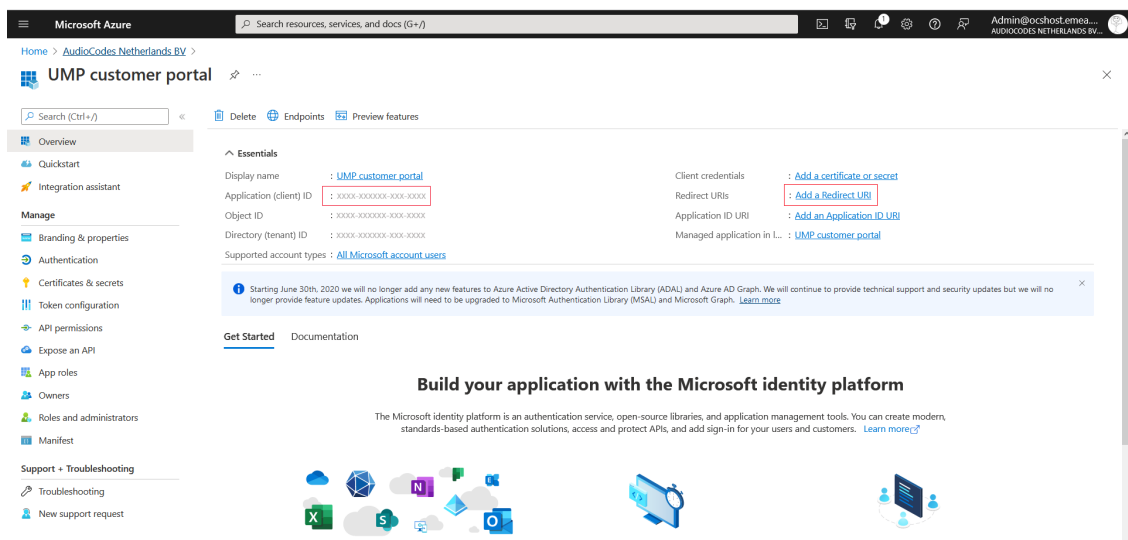
5. Enter the following details:

- Name: App registration name
- Select account type: Recommendation - Accounts in any organizational directory (Any Azure AD directory - Multitenant)

6. Click Register.

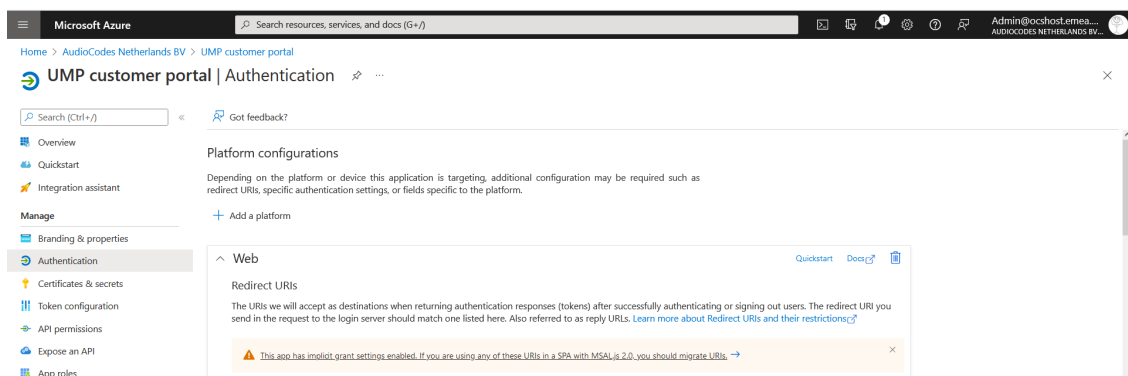
The new registration is created.

7. Navigate to the Overview page and copy the Application (client) ID to notepad (it must be configured later in this procedure).



8. Click the **Add a Redirect URI** link to add the WEB redirect URI for the provider's public portal.

The Authentication screen is displayed.



9. Click **Add URI** and add the Public Portal DNS subdomain name for the provider that you defined in Chapter [Register End Customer Tenant DNS Sub domains](#) on page 250 with the appended string “/tenantui/signin-aad” as shown in the following figure.



10. 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)

[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 Multitenant 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 [Navigate to the Overview page and copy the Application \(client\) ID to notepad \(it must be configured later in this procedure\)](#). on page 88 and then click **Save**.

App Registration Application (Client) ID [Save](#)

Show 10 entries

ID	CustomerID	Account
64	M365x202362	AlexWB@M365x202362.OnMicrosoft.com
66	essentials	admin@ocshost.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]
```

```
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>
```

17 Deploy Synchronization Application

The Synchronization Application Registration manages the automatic background synchronization between the UMP-365 and the customer's Microsoft 365 platform (see [Monitoring M365 Replication Actions Queue](#) on page 508). You must add this registration under the Service Provider Tenant's Azure subscription for each UMP device. In this procedure, a redirect URL is configured that 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 [Grant Consent using only Token-based Authentication \(Global Admin\)](#) on page 369).

In this procedure, the Client ID and the Redirect URL must be configured in the Auth Tokens screen in the Multitenant portal interface (see Step below and described in [Customer Invitations](#) on page 225). 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 [Securing Microsoft 365 Service Provider Access](#) on page 511).

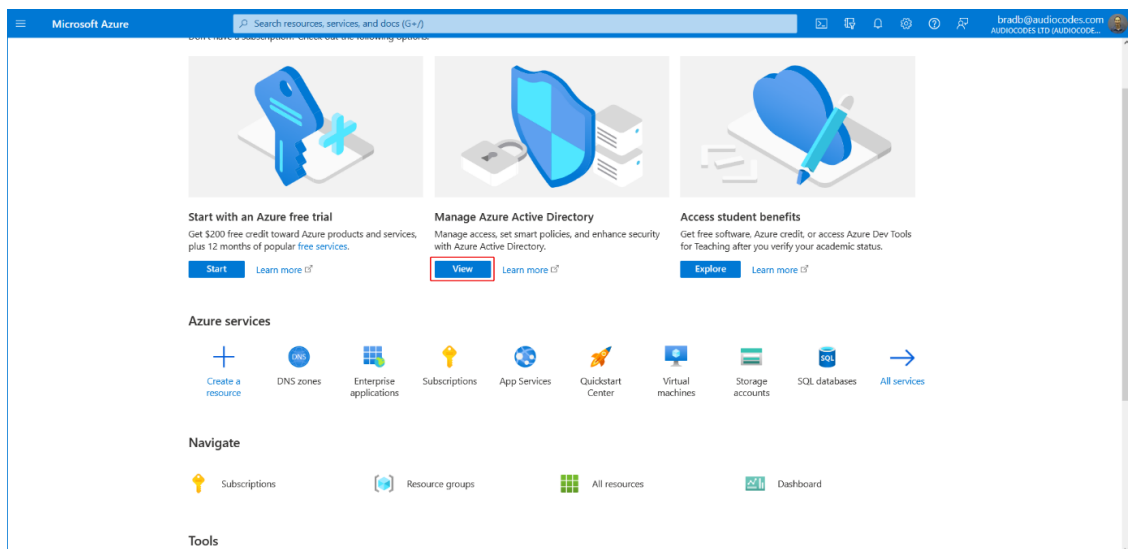
Once you complete this registration, administrator roles must be assigned to the customer IT administrator who provides consent to Service Provider IT administrator for using the token authentication (see [Assign Administrator Roles to IT Administrator](#) on page 269).



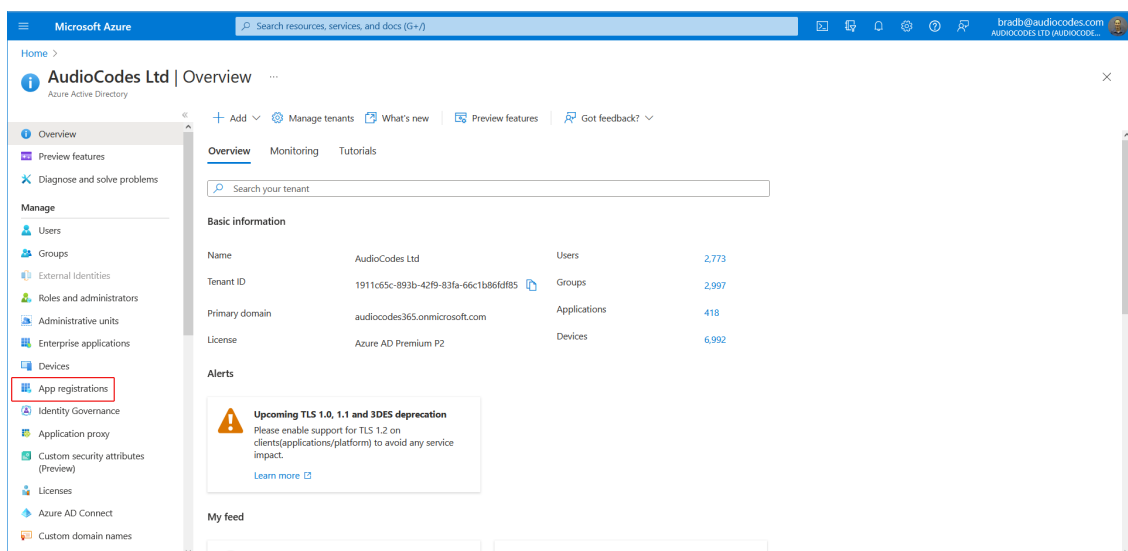
- The domain names shown in the procedure below are examples only.
- For each customer, a unique redirect URL is defined.
- This procedure must be performed by new customers running a clean installation. For existing customers, the registration must be updated as described in [Post Upgrade Actions](#) on page 143.
- This application does not require any M365 licenses.
- If the Azure subscription is managed by customer, see [Deploy Synchronization Application \(Customer Subscription\)](#) on page 96

➤ Do the following:

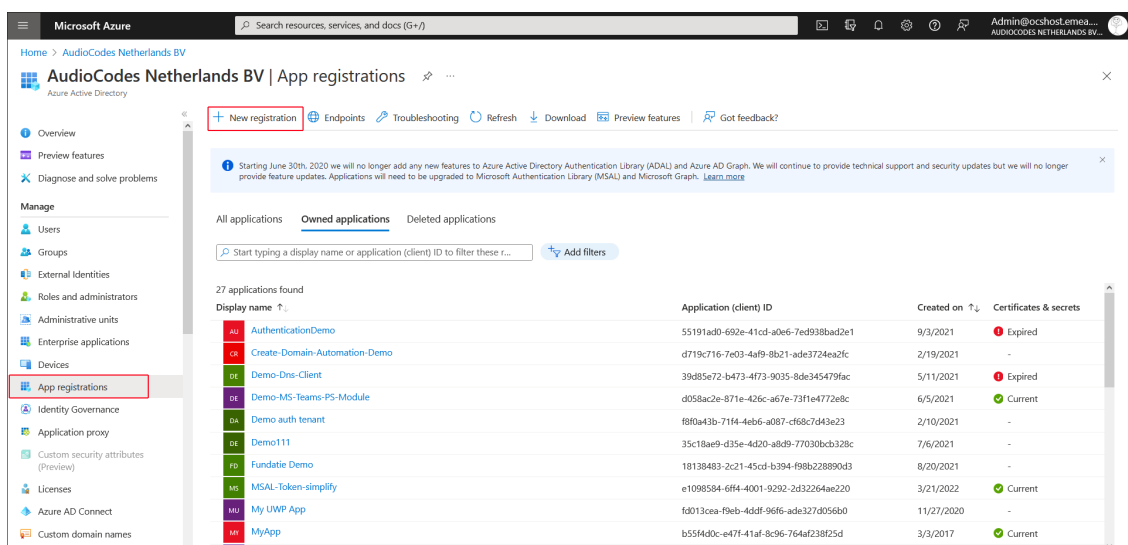
1. Sign-in to the Azure portal for the Service Provider operator tenant with Admin permissions.
2. Under Manage Azure Active Directory, select **View**.



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



4. Click **New registration**.



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:

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.

Microsoft Azure

Home > AudioCodes Netherlands BV >

Demo-MS-Teams-PS-Module

Search (Ctrl+/)

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	: XXXX-XXXX-XXXX-XXXX	Redirect URIs	: Add a Redirect URI
Object ID	: XXXX-XXXX-XXXX-XXXX	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: XXXX-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 MPA ID to verify publisher](#)

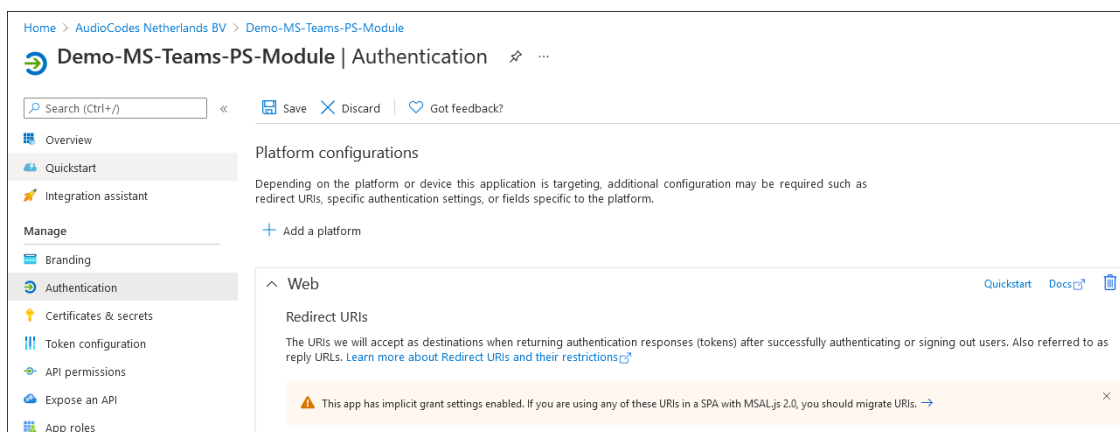
Get Started | Documentation

Build your application with the Microsoft identity platform

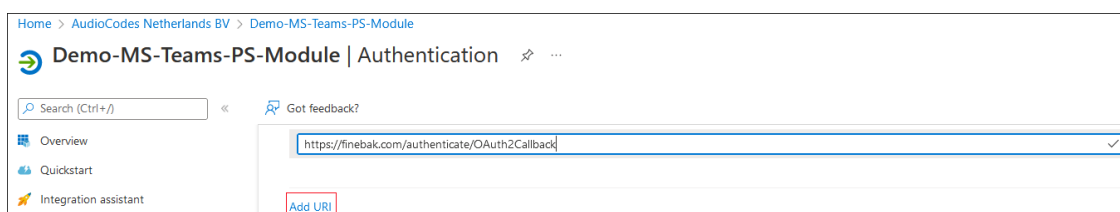
The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

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

The Authentication screen is displayed.



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



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

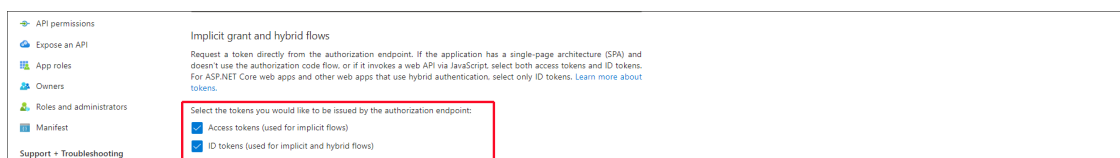
where:

- “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)



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

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

☒ Yes
 ☐ No

- 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](#)

App instance property lock ⓘ

Configure the application instance modification lock. [Learn more](#)

[Configure](#)



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**.

Certificates & secrets	Thumbprint	Start date	Expires	Certificate ID
<ul style="list-style-type: none"> Token configuration API permissions Expose an API App roles Owners Roles and administrators Preview Manifest Support + Troubleshooting Troubleshooting New support request 	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_x*****	*****	
tudor	8/9/2023	juX*****	*****	

Add a client secret

Description

Expires

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

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

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

Thumbprint

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_*****	*****
tudor	8/9/2023	ju*****	*****
Key for UMP Token	8/10/2023	-h7*****	*****

19. In the Multitenant portal, open the Authentication Status page (**Security > Authentication Status**) and do the following:

- Paste the Application (client) ID (see [Copy the Application \(client\) ID value to notepad as its required later in the configuration.](#) on page 93) and Client secret value to the respective fields.
- Enter the Redirect URI that you configured in [Register End Customer Tenant DNS Sub domains](#) on page 250 Enter the HTTPS URI of the UMP installation VM (e.g. <https://finebak.com/authenticate/OAuth2Callback>) on page 94. For example <https://finebak.com/authenticate/OAuth2Callback>

20. Click **Apply Changes**.

AuthenticationStatus
Monitor Authentication Status

Client Id: e1098584-6ff4-4001-9292-2d32264ae220

Client Secret: [Redacted]

Redirect Uri: <https://finebak.com/authenticate/OAuth2Callback>

Buttons: Apply Changes, Reset Changes

Customer Id	M365 Email	Authentication method	When Last Verified	Last Verification Status	Actions
Customer22	admin@M365x74218585.onmicrosoft.com	Password	Never		Check Credentials Switch to token
ETAS4	admin@M365x14313316.onmicrosoft.com	Password	Never		Check Credentials Switch to token
wsc	admin@M365x78596656.onmicrosoft.com	Password	Never		Check Credentials Switch to token
W20637721	admin@M365x20637721.onmicrosoft.com	Token	June 24th 2022, 10:02	✓	Check Credentials Switch to password

Showing 1 to 4 of 4 entries

Buttons: Reload, Verify All, Update

Deploy Synchronization Application (Customer Subscription)

This section describes how to setup and configure the App registration for the Background registration with a **Customer Azure subscription**. The App Registration manages the automatic synchronization between the UMP-365 and the customer's Microsoft 365 platform (see [Monitoring M365 Replication Actions Queue](#) on page 508). 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 [Grant Consent using only Token-based Authentication \(Global Admin\)](#) on page 369).

In this procedure, the Client ID and the Redirect URL must be configured in the Auth Tokens screen in the Multitenant interface (see Step below and [Customer Invitations](#) on page 225). 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 [Securing Microsoft 365 Service Provider Access](#) on page 511).

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 [Assign Administrator Roles to IT Administrator](#) on page 269).



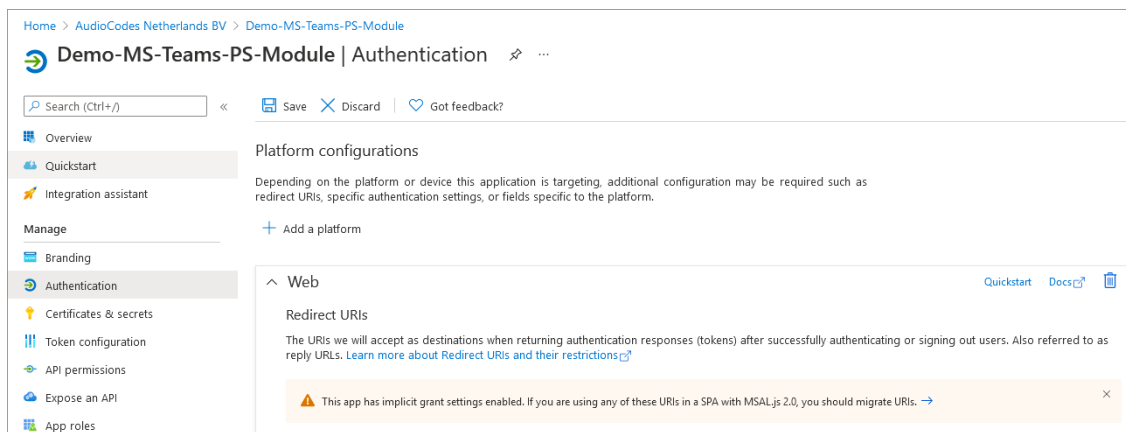
- The domain names shown in the procedure below are examples only.
- For each customer, a unique redirect URL is defined.
- This procedure must be performed by new customers running a clean installation. For existing customers, the registration must be updated as described in [Post Upgrade Actions](#) on page 143.

➤ **Do the following:**

1. Access the Provider Azure Active Directory admin center/ app registration on the Azure portal with System Admin permissions.
2. Enter the following details:
 - Name: **App registration name**
 - Select account type: **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**

The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The page is for 'AudioCodes Netherlands BV'. The 'Name' field is 'UMP_AUTH-Reg'. The 'Supported account types' section has three radio buttons: 'Accounts in this organizational directory only (AudioCodes Netherlands BV only - Single tenant)', 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)' (which is selected), and 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)'. The 'Redirect URI (optional)' section has a dropdown set to 'Web' and a text box containing 'e.g. https://example.com/auth'. At the bottom, there is a 'Register' button and a link to 'Enterprise applications'.

3. Click **Register**.
4. In the Navigation pane, select **Authentication**.



5. Under Platform configurations/Redirect URLs, click **Add URI**.



6. Enter the HTTPS URL of the UMP installation VM (e.g. `https://livecloud.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

7. Copy the URL to notepad as it is required later in the configuration.

8. 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)

Microsoft Azure

Search resources, services, and docs (G+)

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

Demo-MS-Teams-PS-Module | Authentication

Search (Ctrl+/) Save Discard Got feedback?

Overview
Quickstart
Integration assistant
Manage
Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest
Support + Troubleshooting
Troubleshooting
New support request

Mobile and desktop applications

Quickstart Docs

Redirect URIs

The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

- ☒ https://login.microsoftonline.com/common/oauth2/nativeclient
- ☐ https://login.live.com/oauth20_desktop.srf (LiveSDK)
- ☐ msal058ac2e-871e-426c-a67e-73f1e4772e8c//auth (MSAL only)

http://localhost

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.

e.g. https://example.com/logout

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](#).

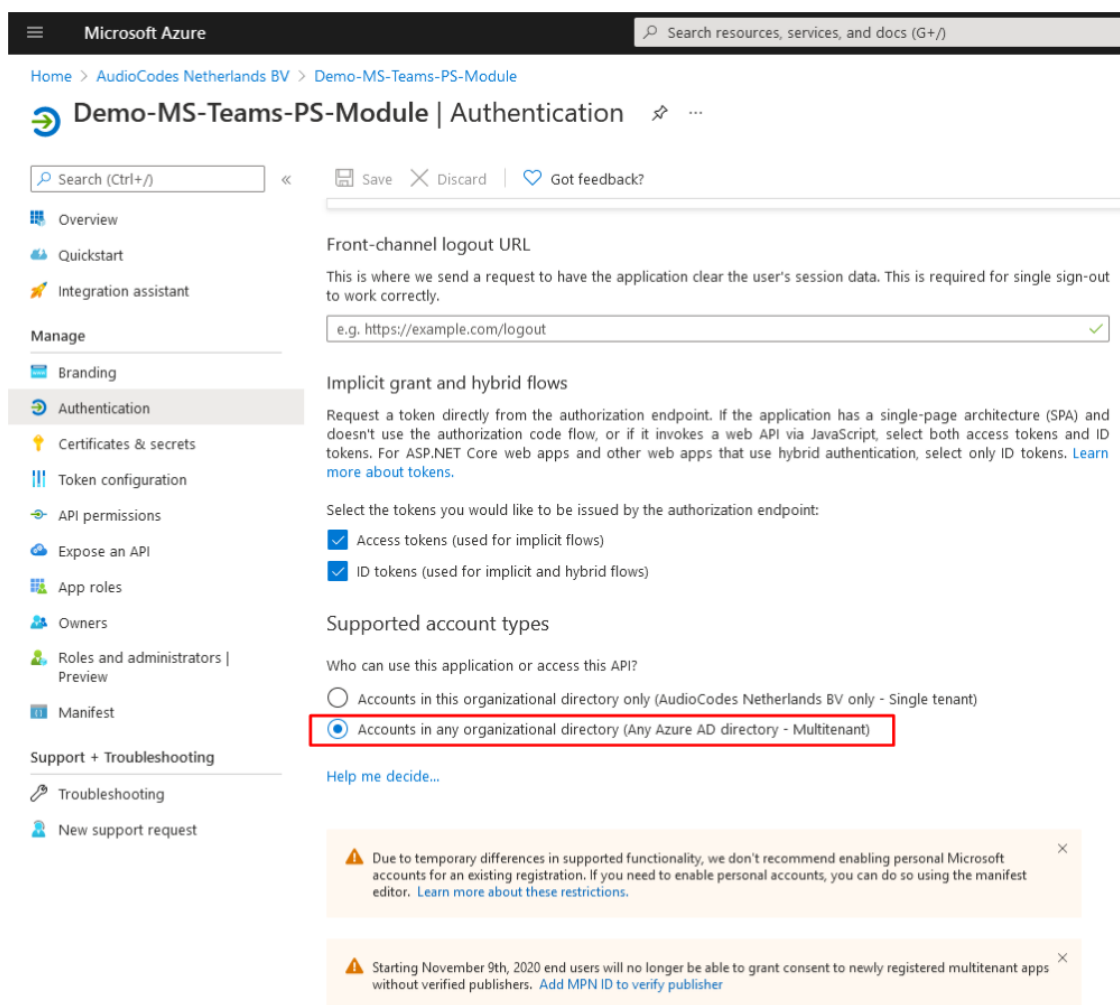
Select the tokens you would like to be issued by the authorization endpoint:

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

Supported account types

Who can use this application or access this API?

- Under Supported account types, select **Accounts in any organizational directory (Any Azure AD directory – Multitenant)**.



Microsoft Azure

Search resources, services, and docs (G+)

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

Demo-MS-Teams-PS-Module | Authentication

Search (Ctrl+/) Save Discard Got feedback?

- Overview
- Quickstart
- Integration assistant
- Manage
 - Branding
 - Authentication**
 - Certificates & secrets
 - Token configuration
 - API permissions
 - Expose an API
 - App roles
 - Owners
 - Roles and administrators | Preview
 - Manifest
- Support + Troubleshooting
 - Troubleshooting
 - New support request

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.

e.g. `https://example.com/logout`

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)

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)

[Help me decide...](#)

Warning: 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.](#)

Warning: 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](#)



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

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

Microsoft Azure

Search resources, services, and docs (G+)

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

Demo-MS-Teams-PS-Module | Authentication

Search (Ctrl+/) Save Discard Got feedback?

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)

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)

[Help me decide...](#)

Warning: 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.](#)

Warning: 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](#)

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

☒ Yes ☐ No

- 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](#)

11. In the Navigation pane, select **API Permissions**.

12. Set the permissions shown in the figures below.

Microsoft Azure

Home

>

AudioCodes Netherlands BV

>

Demo-MS-Teams-PS-Module

Demo-MS-Teams-PS-Module | API permissions

✕

⋮

Search (Ctrl+/)

«

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Support + Troubleshooting

Troubleshooting

New support request

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect:

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for AudioCodes Netherlands BV

API / Permissions name	Type	Description	Admin consent req...	Status
<div>Microsoft Graph (10)</div>				
AppCatalog.ReadWrite.All	Delegated	Read and write to all app catalogs	Yes	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
Directory.Read.All	Application	Read directory data	Yes	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
Directory.ReadWrite.All	Application	Read and write directory data	Yes	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
Group.ReadWrite.All	Application	Read and write all groups	Yes	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
offline_access	Delegated	Maintain access to data you have given it access to	No	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
openid	Delegated	Sign users in	No	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
profile	Delegated	View users' basic profile	No	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
User.Read	Delegated	Sign in and read user profile	No	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
User.Read.All	Delegated	Read all users' full profiles	Yes	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
User.ReadWrite.All	Application	Read and write all users' full profiles	Yes	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
<div>Skype and Teams Tenant Admin AP</div>				
application_access	Application	application_access	Yes	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
application_access_custom_sba_	Application	application_access_custom_sba_appliance	Yes	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>
user_impersonation	Delegated	Access Microsoft Teams and Skype for Business data as t...	Yes	<div>✓</div> <div>Granted for AudioCodes...</div> <div>...</div>

Other permissions granted for AudioCodes Netherlands BV

These permissions have been granted for AudioCodes Netherlands BV but aren't in the configured permissions list. If your application requires these permissions, you should consider adding them to the configured permissions list. [Learn more](#)

API / Permissions name	Type	Description	Admin consent req...	Status
▼ Microsoft Graph (8)				
AuditLog.Read.All	Delegated	Read audit log data	Yes	✔ Granted for AudioCodes... ✔
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	✔ Granted for AudioCodes... ✔
IdentityProvider.ReadWrite.All	Delegated	Read and write identity providers	Yes	✔ Granted for AudioCodes... ✔
Policy.ReadWrite.TrustFramework	Delegated	Read and write your organization's trust framework polici...	Yes	✔ Granted for AudioCodes... ✔
PrivilegedAccess.ReadWrite.AzureAD	Delegated	Read and write privileged access to Azure AD	Yes	✔ Granted for AudioCodes... ✔
PrivilegedAccess.ReadWrite.AzureResources	Delegated	Read and write privileged access to Azure resources	Yes	✔ Granted for AudioCodes... ✔
TrustFrameworkKeySet.ReadWrite	Delegated	Read and write trust framework key sets	Yes	✔ Granted for AudioCodes... ✔
User.Invite.All	Delegated	Invite guest users to the organization	Yes	✔ Granted for AudioCodes... ✔

To view and manage permissions and user consent, try [Enterprise applications](#).

13. Navigate to the Overview page.
14. Copy the Application (client) ID value to notepad.

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name

: Demo-MS-Teams-P5-Module

Application (client) ID

:

Object ID

:

Directory (tenant) ID

:

Supported account types

: [Multiple organizations](#)

Client credentials

: 0 certificate, 4 secret

Redirect URIs

: 4 web, 0 spa, 2 public client

Application ID URI

: [Add an Application ID URI](#)

Managed application in L...

: [Demo-MS-Teams-P5-Module](#)

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](#)

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

Certificates & secrets

Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest
Support + Troubleshooting
Troubleshooting
New support request

Thumbprint
No certificates have been added for this application.

Start date
Expires
Certificate ID

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
cnsole token	1/17/2022	Sn~*****	*****
ps-secret	6/5/2023	i_x*****	*****
tudor	8/9/2023	juX*****	*****

Add a client secret

Description

Enter a description for this client secret

Expires

24 months

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

17. **17.** Copy the newly generated secrets' Value to notepad.

Certificates & secrets

Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest
Support + Troubleshooting
Troubleshooting
New support request

Thumbprint
No certificates have been added for this application.

Start date
Expires
Certificate ID

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
cnsole token	1/17/2022	Sn~*****	*****
ps-secret	6/5/2023	i_x*****	*****
tudor	8/9/2023	juX*****	*****
Key for UMP Token	8/10/2023	-h7*****	*****

Certificates & secrets

Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators | Preview
Manifest
Support + Troubleshooting
Troubleshooting
New support request

Thumbprint
No certificates have been added for this application.

Start date
Expires
Certificate ID

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
cnsole token	1/17/2022	Sn~*****	*****
ps-secret	6/5/2023	i_x*****	*****
tudor	8/9/2023	juX*****	*****
Key for UMP Token	8/10/2023	-h7*****	*****

18. **18.** In the Multitenant Navigation pane, open the Auth Tokens page (**Security > Auth Tokens**) and do the following:

- Paste the Application (client) ID and Client secret value to the respective fields.
- Enter the RedirectUrl that you configured above.

For example <https://livecloud.finebak.com/authenticate/OAuth2Callback>

19. 19. Click **Apply Changes**.

20.

AuthenticationStatus
Monitor Authentication Status

Client Id: 3987f05f-3b81-4d26-8bb2-4e16a5a8ce2e
Client Secret:

Redirect Uri: https://tokensandbox3.finebak.com/authenticate/OAuth2Callback

Search:

Customer Id	M365 Email	Authentication method	When Last Verified	Last Verification Status	Actions
dr8	admin@Aud-Demo6.onmicrosoft.com	Token	May 29th 2023, 22:03	✗	Check Credentials Switch to password
Demo	admin@M365x08167531.onmicrosoft.com	Password	May 29th 2023, 22:08	✗	Check Credentials Switch to token
ManuelTest	admin@M365x29347113.onmicrosoft.com	Password	May 29th 2023, 22:04	✓	Check Credentials Switch to token
BradSuperT	admin@M365x29516837.onmicrosoft.com	Password	May 29th 2023, 21:56	✗	Check Credentials Switch to token
DemoTotSpo	admin@M365x62214376.onmicrosoft.com	Token	May 29th 2023, 22:02	✗	Check Credentials Switch to password
TRITzik	admin@M365x18234803.onmicrosoft.com	Password	May 29th 2023, 22:01	✓	Check Credentials Switch to token

18 Accessing UMP 365 with Service Provider 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.



Your connection is not private

Attackers might be trying to steal your information from `xxx.xx.xx.xx` (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID



To get Chrome's highest level of security, [turn on enhanced protection](#)

Hide advanced

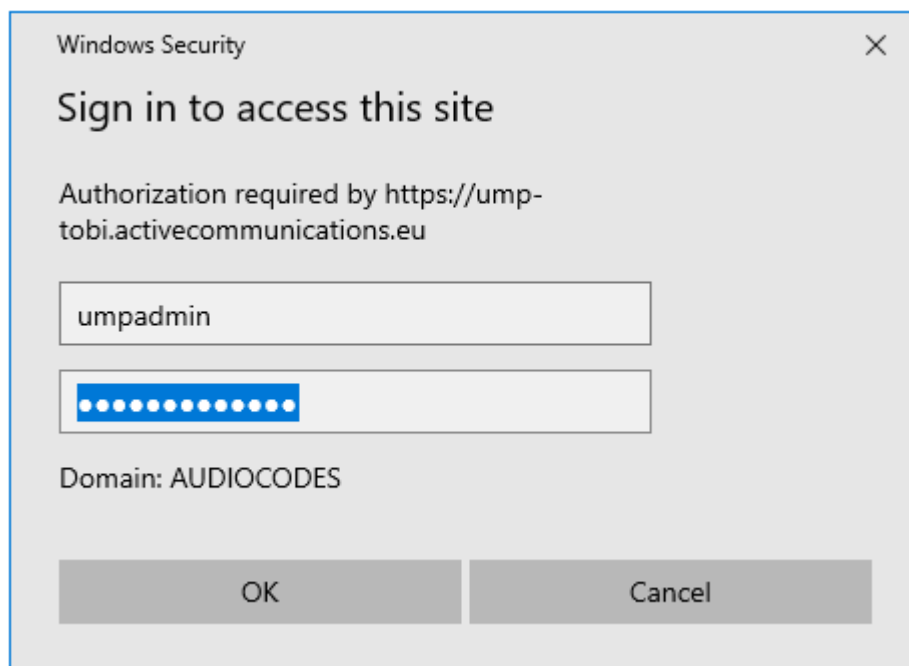
Back to safety

This server could not prove that it is `xxx.xx.xx.xx`; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

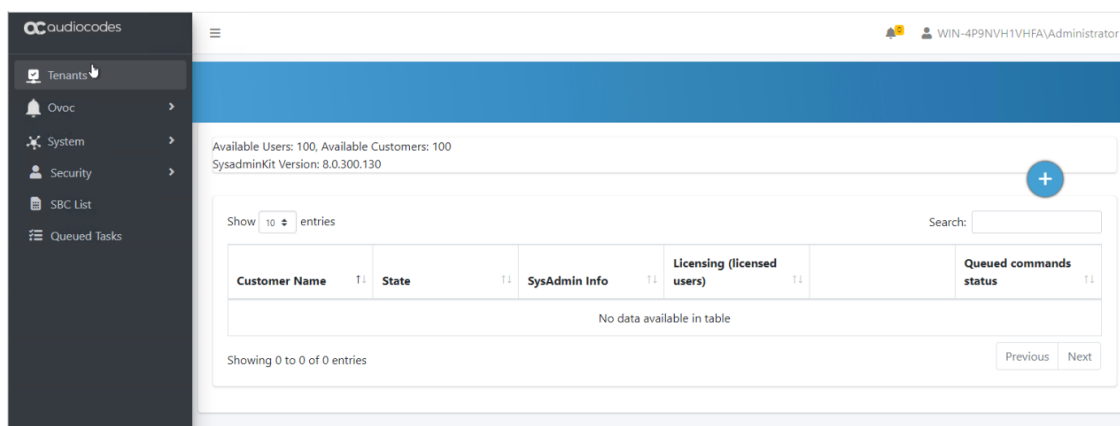
[Proceed to xxx.xx.xx.xx \(unsafe\)](#)

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



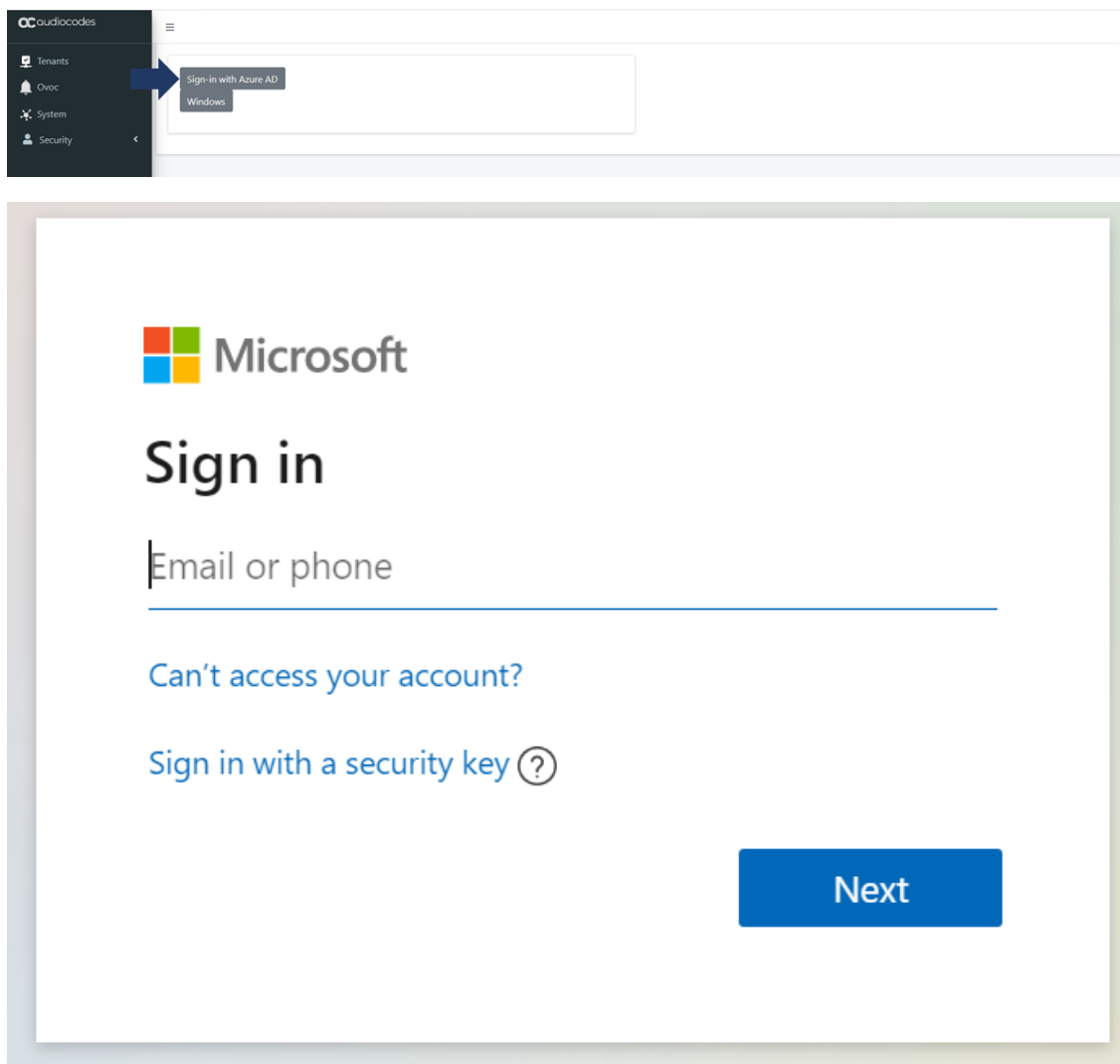
The following screen displays the UMP-365 interface after a clean installation for a new customer.



- **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 [Create Registration for Customer Administrators](#) on page 87.



The Tenants screen shown in the figure below displays all M365 tenants. Clicking **SysAdmin** link for any customer tenant opens the Multitenant portal for the customer (see [Day Two Management using Customer Tenant Portal](#) on page 425).

Customer Name	State	SysAdmin Info	Licensing (licensed users)	Queued commands status
Bradtest	Deployed	version: 8.0.450.41 replication: 2022.12.14.13.09.13 SysAdmin	M365 - EssentialPlus (10) Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
IPPBXTobi	Deployed	version: 8.0.450.41 replication: 2022.12.14.13.11.17 SysAdmin	M365 - Pro (20) Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
LBRS7147292	Deployed	version: 8.0.450.41 replication: 2022.12.14.13.10.25 SysAdmin	M365 - Pro (20) Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
LBRCustom1	Deployed	version: 8.0.450.41 replication: 2022.12.14.13.09.46 SysAdmin	M365 - Pro (10) Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
LBDRDefault	Deployed	version: 8.0.450.41 replication: 2022.12.14.13.09.20 SysAdmin	M365 - Pro (10) Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no

Tenants Global View

The following figure illustrates the screen elements and fields in the Tenants screen.



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

- 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

Link	Action
Total Available Licensed Users and Customers	<ul style="list-style-type: none"> ■ Total number of available customer tenant licenses. ■ Total number of available user licenses.
SysadminKit Version	The wyUpdate installation SysadminKit version of the Multitenant (Main Tenant). See Upgrading Main UMP-365 Tenant on page 131.
Deployment State	The customer Deployment status. One of the following values: <ul style="list-style-type: none"> ■ Deployed ■ Ready ■ Failed ■ Unknown
Customer	The wyUpdate installation Customer adminKit version of the

Link	Action
adminKit Version	customer tenant. See Upgrading Customer Tenant on page 139.
License Type (Licensed Users)	<p>The type of license and number of users licenses for each type:</p> <ul style="list-style-type: none"> ■ Hosted Essentials ■ Hosted Essentials + ■ Hosted Pro ■ OC Essential ■ OC Pro
User Actions pane	<ul style="list-style-type: none"> ■ Edit User Licenses (Configuring Number of Licensed Users on the next page) ■ Delete customer ■ Perform manual database synchronization (Queue Replication on page 112)
Database update tasks	Status of database synchronization updates for the customer. See (Queue Replication on page 112) and Monitoring M365 Replication Actions Queue on page 508.
Multitenant Navigation pane	<p>Opens the Multitenant Navigation pane menu:</p> <ul style="list-style-type: none"> ■ OVOC page (see Networking on page 51) ■ System: <ul style="list-style-type: none"> ✓ License (Multitenant Portal Licensing on page 65) ✓ Invitation Settings (Configuring Invitation Settings on page 67) ✓ Email Settings (Configuring Email Settings on page 69) ✓ Script Templates (Managing Onboarding Script Templates on page 170) ✓ DNS API Configuration (Configure DNS API on page 82) ■ Security: <ul style="list-style-type: none"> ✓ Customer Admins (Create Registration for Customer Administrators on page 87) ✓ Authentication Status (Authentication Status on page 228) ✓ Customer Invitations (Customer Invitations on page 225) ✓ UMP Service Settings (UMP Service Settings on page 234) ■ SBC List (Managing SBC Devices on page 235)

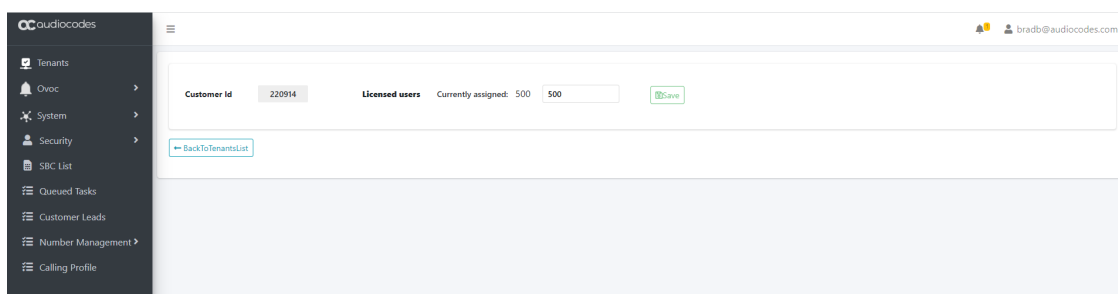
Link	Action
	■ Queued Tasks (Queued Tasks on page 244)
Customer Shortname	The customer shortname defined in the Onboarding.
SysAdmin	Opens the Customer portal for the selected tenant (see Day Two Management using Customer Tenant Portal on page 425).
Edit	Enables the configuration of the number of licensed users for the customer tenant (see Configuring Number of Licensed Users below).
Add SBC Site	Enables adding of SBC devices (see Add SBC Site Locations on page 531).
Delete	Deletes the customer tenant.
Undo Deploy	Resets the current deployment configuration for the customer tenant.
Queue Replication	Synchronizes the database with Microsoft 365 (see Queue Replication on page 112).
Upgrade Customer	Opens the Onboarding Wizard for upgrading the customer to Hosted Essentials+ or Hosted Pro (see Upgrading Customer on page 113).

Configuring Number of Licensed Users

The number of licensed users for each customer is initially configured in the Onboarding wizard. You can then later update this number according to site requirements.

➤ To configure the number of licensed users:

1. In the Tenants page, select the desired customer and then click **Edit**.



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

Adding SBC Devices for New Site Locations

Once the new M365 tenant has been added, you can add SBC devices to manage Enterprise Voice at new sites.

➤ To add an SBC device:

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

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: 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)	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 Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no

1 M365 Tenant

2 M365

3 Voice Route

×

ADD NEW SITE PRESS NEXT

Next

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

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.

Next

- Proceed to [Onboarding Customers](#) on page 282.

Queue Replication

After successful authentication, the User Management Pack 365 initial replication between the customer tenant and Microsoft 365 is automatically executed. This process loads all the M365 users who are enabled for Microsoft Teams under User Management. If the initial replication has not been completed yet, the Users list will be empty. For manual replication, select the **Queue Replication** option.

Tenant: **BradDTest** - [Last sync at: never]

First replication is ongoing! Please wait 5Min and Refresh the page.

User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voice R...	Online PSTN G...	Site Location	Usage Location	EnterpriseVoic...
No items to display										

Copyright © 2023 AudioCodes. All rights reserved. db.000.000.0507

Benelux JF demo tenant	Deployed	version: 8.0.450.101 replication: 2023.05.30.19.29.51 SysAdmin	M365 - Pro (30)	Edit Delete Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
------------------------	----------	--	-----------------	---	--

Tenant: **220914** - [Last sync at: June 1, 2023, 14:43:42]

User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voice...	Online PSTN...	Site Location	Usage Loc...	Enterprise...
Islands	Krijg ik Skype	skp:krijgikskyp...							BG	No
Islands	Dave Mc'Donald	skp:dave.mc'd...								No
TeamsOnly	Walter van Schaik - AudioCodes	skp:wanschal...			Technical	kuytr			NL	No
TeamsOnly	Abrona test voor teams license	skp:15446e655...							NL	No
Islands	test more than 20 character email	skp:thiSEMalla...								No
Islands	wsc 20191021	skp:wsc.20191...								Yes
Islands	teste dg-4	skp:teste-dg4...								No
Islands	user sg3	skp:useng3@a...								No
Islands	teste dg-1	skp:testedg.1...								No
Islands	cristi pantea 5	skp:cristigante...								No
Islands	exchange test	skp:exchanget...								No
TeamsOnly	SBC domain validation DO NOT REM...	skp:sbc@custo...							NL	No
TeamsOnly	wsc 20191209	skp:wsc201912...								No
Islands	permission test	skp:ptest@acti...	tel:+317777772							No
TeamsOnly	repl test, sipremoved	skp:replsip@ac...								No
Islands	dig t-1	skp:dgip-1@acti...								No
Islands	teste sg-3	skp:teste2@act...								No

1 - 20 of 46 items

Undo Deployment

If you wish to configure the M365 tenant deployment from scratch, use the **Undo Deployment** option to revert the Operator Connect customer to an Active Lead.



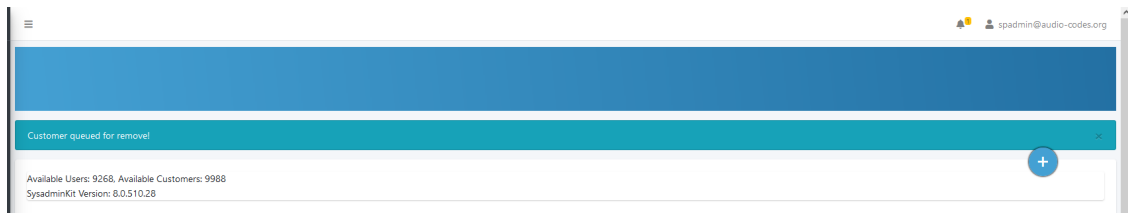
This option is only available for OC Essentials and OC Pro customers.

➤ Do the following:

1. Select the **Undo** action.

Customer Name	State	SysAdmin Info	Licensing (licensed users)		Queued commands status
aiOlogicsESS	Deployed	SysAdmin	M365 - Essential (0)	Edit Delete Upgrade Customer	Queued commands: 0 Executing commands: 0 Replication in progress: no
Brad4478	Deployed	SysAdmin	M365 - OC Essential (0)	Edit Delete Undo Deploy Upgrade Customer	Queued commands: 0 Executing commands: 0 Replication in progress: no

The following message is displayed.



Return to the New Leads page. Notice that the customer has been restored as a lead.

COMPANY NAME	SIZE	MARKET	MICROSOFT STATUS	LICENSE TYPE	TENANT ID	CONSENTED ON	LAST MODIFIED	CHANNEL NAME
Brad4478	1000 to 2999 people	AI, GB, CA, JP	Active		9896758-7197-4f1d-b945-5a8bc973d47	2024-01-11	2024-01-11	

Upgrading Customer

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

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
M365x202214	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**.

1 M365 Tenant

2 M365

3 Voice Route

✕

Start Upgrade Customer
PRESS NEXT

Next

2. Click **Next** to continue.

The screenshot shows a configuration wizard with three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. The first step is active. The form contains the following fields and options:

- Full Customer Name:** A text input field containing "essentials".
- Short Customer Name:** A text input field containing "essentials".
- License Type:** Three radio buttons: "Hosted Essential", "Hosted Essentials+" (selected), and "Hosted Pro". To the right is a "Licensed Users" dropdown menu.
- M365 Authentication:** Two radio buttons: "Send link to customer IT administrator for authentication:" and "Use M365admin account with known password" (selected).
- Authentication Fields:** Below the selected radio button, there is a text input for the email address containing "admin@ocshost.emea.microsoftonline.com" and a password input field with masked characters ".....".
- Navigation:** "Back" and "Next" buttons at the bottom right.

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 [Onboarding with Hosted Essentials +](#) on page 290 and [Onboarding with Hosted Pro](#) on page 361.

At the end of the process, the following confirmation message is displayed:

The screenshot shows a confirmation message dialog with three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. All steps are marked with green circles, indicating completion. The message text is as follows:

```
Processing Add New ...
-- UpgradeCustomer task started --
Tenant definition updated
Customer configuration updated and queued for installation.
-- UpgradeCustomer task completed --
```

A "Close" button is located at the bottom right of the dialog.

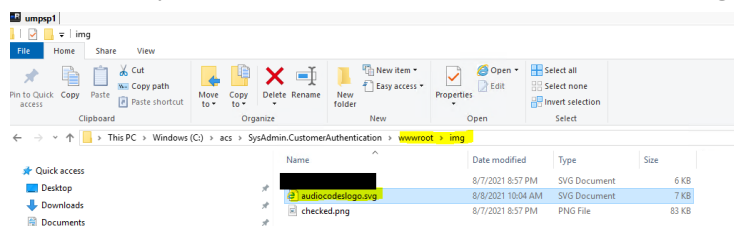
19 Updating Service Provider Logos

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

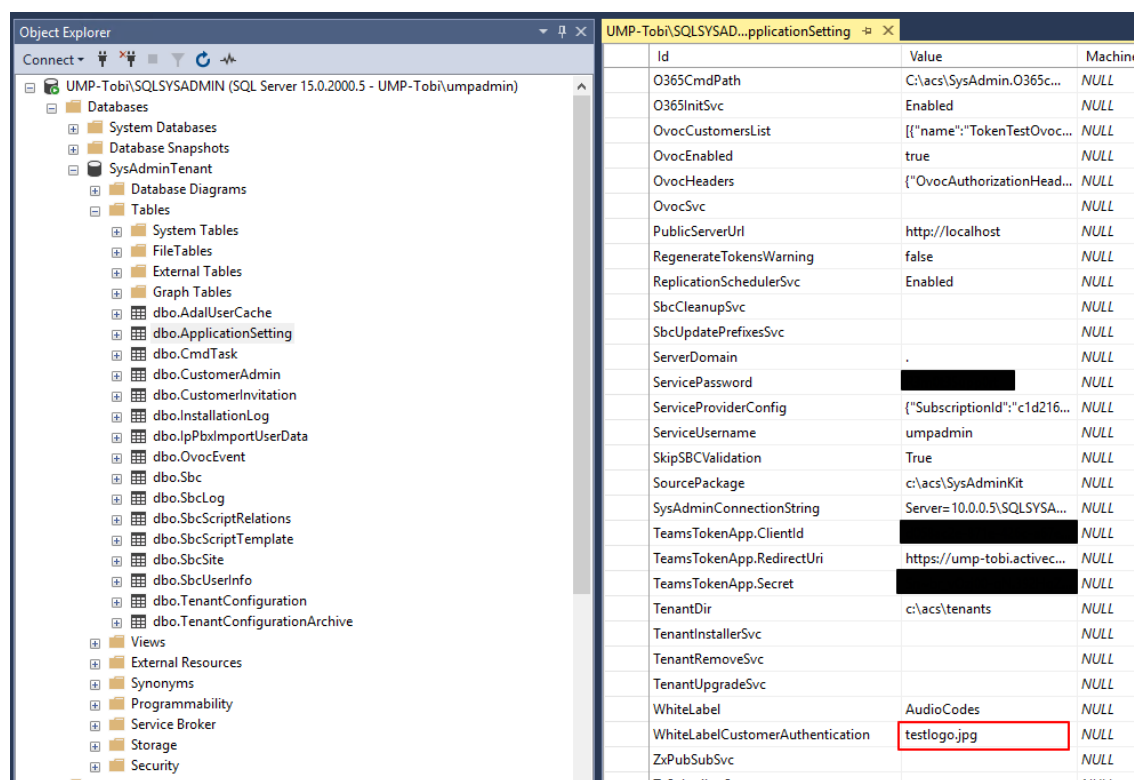
➤ **Do the following:**

1. Update the customer logo image in the following folder:

..\acs\SysAdmin.CustomerAuthentication\wwwroot\img



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



Part III

Upgrade

20 UMP-365 Upgrade

This guide describes how to run a version update using the **wyUpdate** tool:

- See [Before Upgrading UMP-365](#) on page 119 for important prerequisites prior to upgrade.
- See [Upgrading Main UMP-365 Tenant](#) on page 131 for upgrade of the Main UMP-365 tenant.
- See [Upgrading Customer Tenant](#) on page 139 for upgrade of the Customer tenant.
- See [Post Upgrade Actions](#) on page 143 for various actions required to perform following the completion of the upgrade.

21 Before Upgrading UMP-365

The following validations are performed automatically by wyUpdate:

- Verifies whether new patch updates are available for installation and if so, downloads them (to a temporary folder) and installs them.
- Verifies whether the UMP-365 version requires a version upgrade. For example, from Version 8.0.400.25 to Version 8.0.400.64.

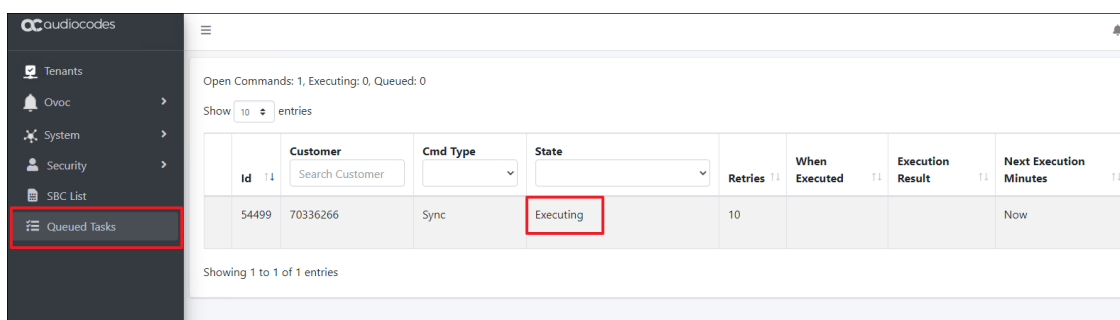
In addition, before upgrading, verify the following:

- Ensure ports HTTP/HTTPS ports are open on the Enterprise firewall (see [Configure Firewall](#) on page 121).
- Ensure all databases are backed up before removing the SQL server, so that they can be correctly restored (see [Backing up UMP-365 – Disk Snapshot](#) on page 121).
- Ensure the Authentication Status menu has been populated with the Azure Application Registration credentials (see [Authentication Status](#) on page 228):
 - For Standalone UMP-365 devices, the customer manages the application in their Azure environment.
- Connection to the customers' M365 platform must be performed using Token authentication instead of by username and password. This requirement is in accordance with stricter Microsoft security policies. Before upgrading, compile a list of all customers who are currently authenticated using username and password authentication. See [Compiling List of Password Authenticated Customers](#) on page 125.
- Stop processes prior to running the wyUpdate (see [Stop wyUpdate Processes](#) on page 126).
- Install SSL certificates on the UMP Windows server for securing the HTTPS connection with Microsoft Azure. See [Installing SSL Certificates on UMP Windows Server](#) on page 8.
- When using a Backend SQL server, create the following directory on the SQL server:
c:/acs/dbbackup/

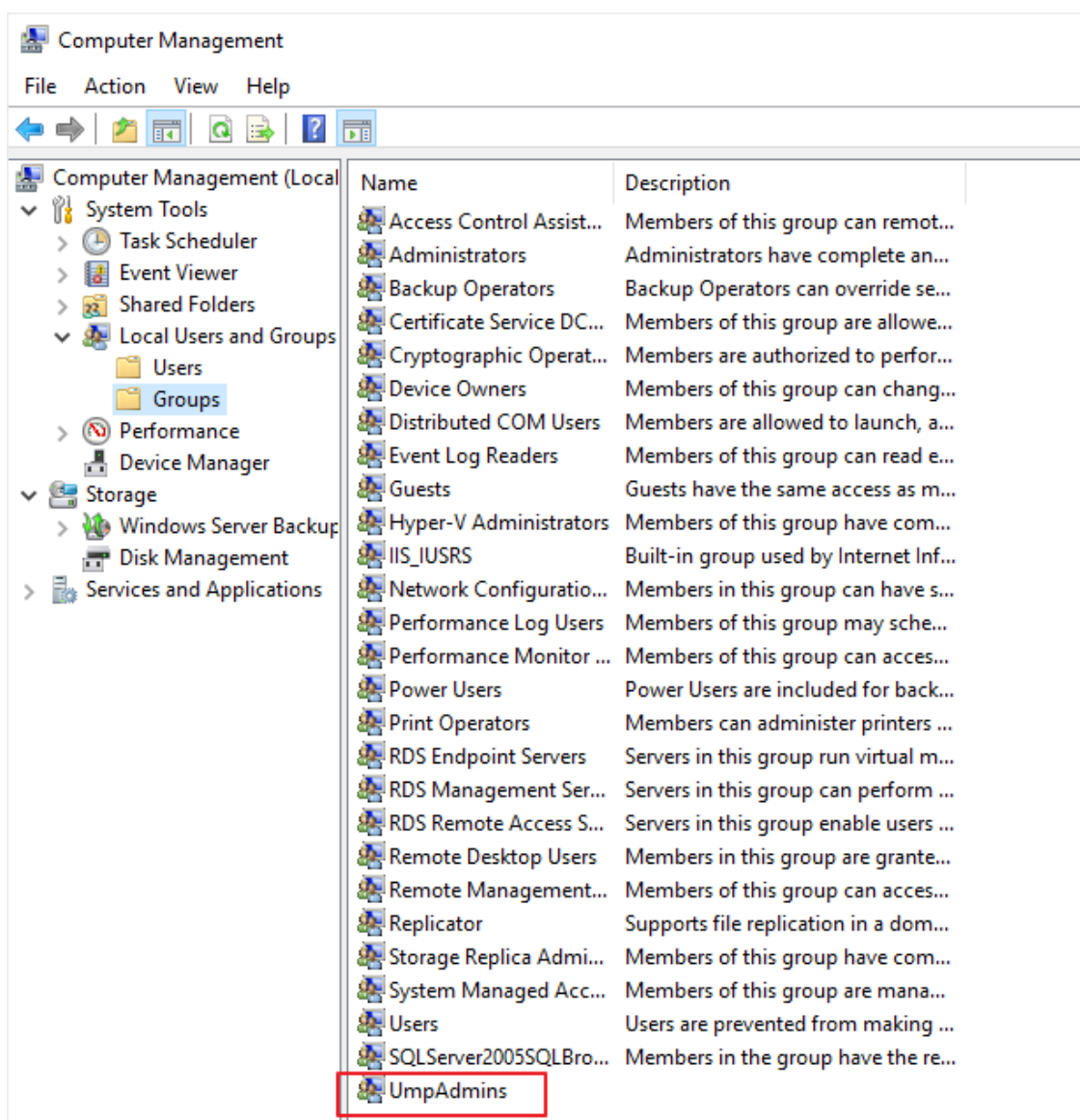


The Backend SQL server username and password must be identical to the Service Account used for the installation of the UMP server. For more information, see [SQL Server Configuration](#) on page 583.

- Ensure all folders and all log files are closed in the C:\acs\ & C:\acs\tenants\ folders as the wyUpdate and SysAdminCustomerUpgrade access these folders and create backups. If the folders/files are open or in use, the upgrade process is interrupted.
- Ensure that there are no replication processes currently being executed (see [Monitoring M365 Replication Actions Queue](#) on page 508). Wait until all replication processes have completed.



- Open an RDP connection to the UMP server Windows Server where the UMP is installed using the UMP service account created in "Create UMP Service Account" in User Management Pack 365 Administrator and Installation Manual, navigate to the C:\acs\ root directory folder and run wyupdate.exe as shown in the screen below.
- Run the wyUpdate as administrator using one of the administrator users defined in the **UmpAdmins** group. For more information, see [Creating UMP Service Account](#) on page 29.



- See [Additional SysAdmin Verifications](#) on page 130 for additional verifications.

Configure Firewall

Ensure ports HTTP80/HTTPS443 ports are open in the Enterprise firewall. The wyUpdate verification connects to the AudioCodes AWS repository. The following third-party proprietary installation components require internet access for download:

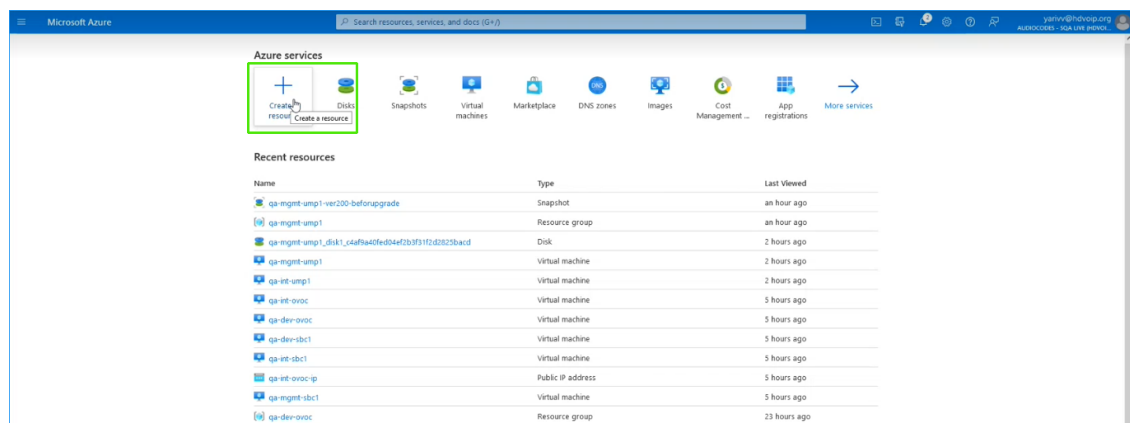
- PowershellGetModule
- MicrosoftTeamsModule
- Chocolatey
- DotNet
- Rabbitmq
- EmsMainAgent
- EmsClientAgent
- InstallPublicOvocConnector
- Installtap-windows-9.23.3-I601-Win10

Backing up UMP-365 – Disk Snapshot

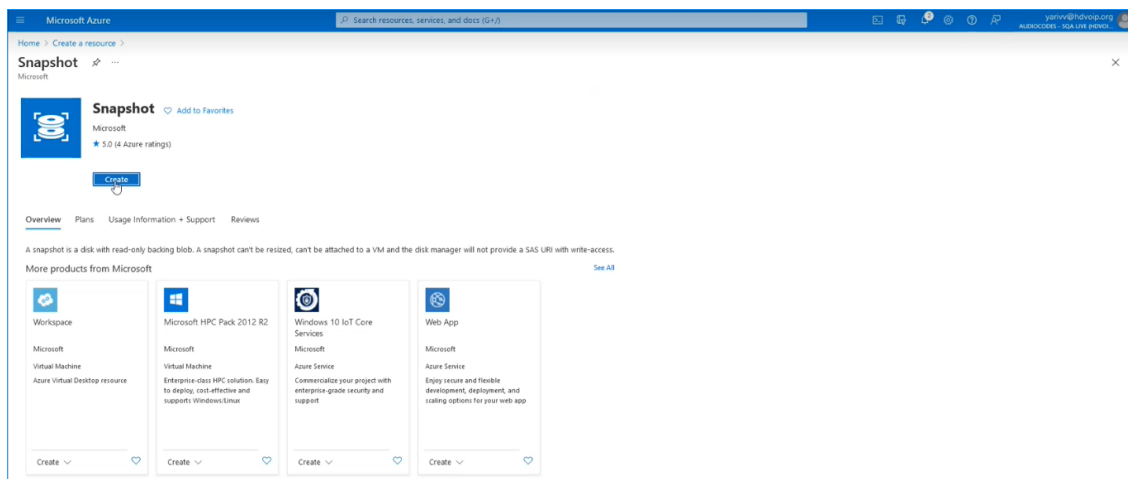
This section describes how to create a snapshot of the UMP Virtual Machine. This procedure should be performed prior to running the upgrade and then rolled back once the upgrade is complete (see [Restoring UMP Snapshot](#) on page 143).

➤ Do the following:

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



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



The screenshot shows the 'Create snapshot' form in the Microsoft Azure portal. The form is divided into several sections: Basics, Encryption, Networking, Tags, and Review + create. The Basics section contains a description of a snapshot and a link to learn more. Below this is the 'Project details' section, which includes a 'Subscription' dropdown menu (set to 'SQA LIVE Sub1') and a 'Resource group' dropdown menu (with a 'Create new' link). The 'Instance details' section includes a 'Name' text field, a 'Region' dropdown menu (set to '(Europe) North Europe'), and a 'Snapshot type' section with two radio buttons: 'Full - make a complete read-only copy of the selected disk.' (selected) and 'Incremental - save on storage costs by making a partial copy of the disk based on the difference between the last snapshot.' Below this is the 'Source subscription' dropdown menu (set to 'SQA LIVE Sub1'), a 'Source disk' dropdown menu, and a 'Storage type' dropdown menu (set to 'Zone-redundant'). At the bottom, there are three buttons: 'Review + create', '< Previous', and 'Next : Encryption >'. A mouse cursor is pointing at the 'Resource group' dropdown menu.

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**.

The screenshot shows the 'Create snapshot' wizard in the Microsoft Azure portal. The 'Tags' tab is selected, showing a table for defining tags. The table has three columns: 'Name', 'Value', and 'Resource'. The first row shows 'LiveCloudEnv' as the name, 'qa-mgmt' as the value, and '2 selected' as the resource. A second row is empty. Below the table, there are navigation buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next : Review + create >'. The breadcrumb trail at the top reads 'Home > Create a resource > Snapshot >'. The page title is 'Create snapshot'.

Name	Value	Resource
LiveCloudEnv	qa-mgmt	2 selected
		2 selected

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

Microsoft Azure

Home > Create a resource > Snapshot >

Create snapshot

Validation passed

Basics Encryption Networking Tags **Review + create**

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

Buttons: Create, < Previous, Next >, Download a template for automation

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

Microsoft Azure

Home >

Snapshot.qa-mgmt-ump1-ver200-beforupgrade-20211028162958 | Overview

Deployment

Search (Ctrl+/) < Delete Cancel Redeploy Refresh

Overview

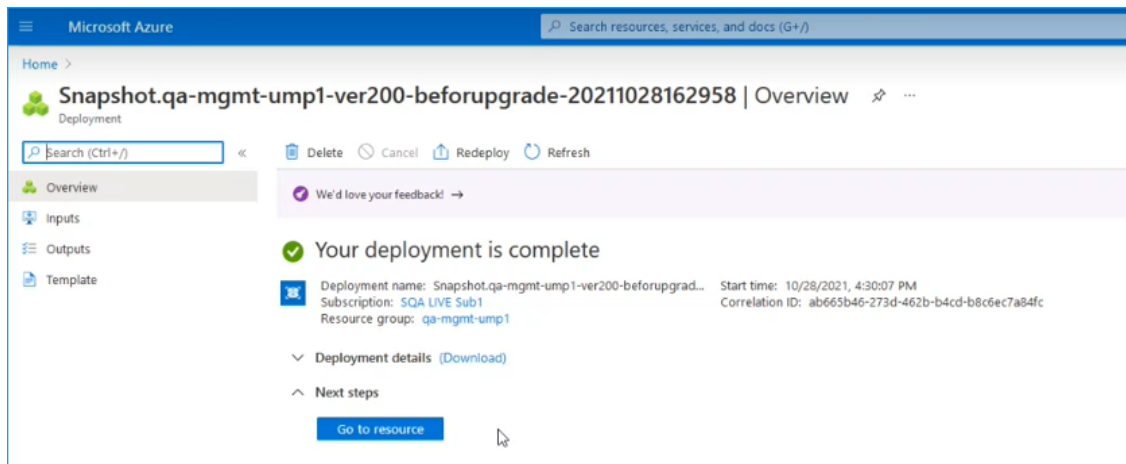
We'd love your feedback →

Deployment is in progress

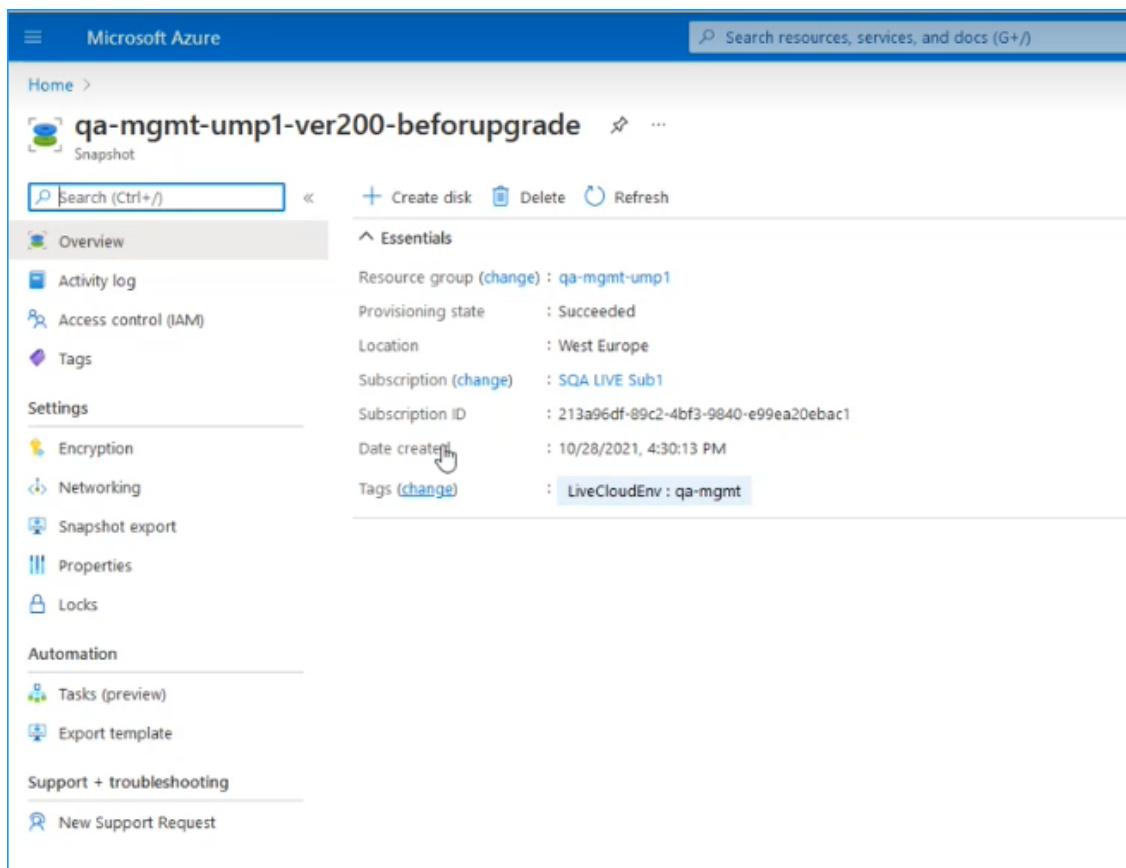
Deployment name: Snapshot.qa-mgmt-ump1-ver200-beforupgrad... Start time: 10/28/2021, 4:30:07 PM
 Subscription: SQA LIVE Sub1 Correlation ID: ab665b46-273d-462b-b4cd-b8c6ec7a84fc
 Resource group: qa-mgmt-ump1

Deployment details (Download)

Resource	Type	Status
No results.		



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



Compiling List of Password Authenticated Customers

For Version 8.0.450 and later connection to the customers' M365 platform must be performed using token authentication instead of by username and password. This requirement is in accordance to stricter Microsoft's security policies. Before upgrading, make a list of all customers that are currently authenticated using username and password authentication. Following the upgrade, connection to the M365 platform for these customers must be setup using token authentication.

➤ **To sort all customers authenticated with password:**

1. In the Multitenant Navigation pane, select **Security > Authentication Status**.

AuthenticationStatus
Monitor Authentication Status

Client Id
398705f-3b81-4d26-8bb2-4e16a5a8ce2e

Client Secret

Redirect Uri
https://tokensandbox3.finebak.com/authenticate/OAuth2Callback

Apply Changes Reset Changes

Search:

Customer Id	M365 Email	Authentication method	When Last Verified	Last Verification Status	Actions
Demo	admin@M365x08167531.onmicrosoft.com	Password	March 9th 2023, 15:38	✗	Check Credentials Switch to token
ManuelTest	admin@M365x29347113.onmicrosoft.com	Password	February 7th 2023, 18:26	✓	Check Credentials Switch to token
TRITZIK	admin@M365x18234803.onmicrosoft.com	Password	February 7th 2023, 18:24	✓	Check Credentials Switch to token
testpro	admin@M365x1164675.onmicrosoft.com	Password	March 9th 2023, 11:56	✗	Check Credentials Switch to token
roydemodns	admin@M365x605945.onmicrosoft.com	Password	March 9th 2023, 11:56	✗	Check Credentials Switch to token
thlab	admin@M365x307750.onmicrosoft.com	Password	March 9th 2023, 11:56	✗	Check Credentials Switch to token
PioCustomer	admin@M365x63013905.onmicrosoft.com	Password	March 9th 2023, 13:18	✓	Check Credentials Switch to token
jfsTestCX2	admin@M365x53135475.onmicrosoft.com	Password	March 9th 2023, 15:42	✓	Check Credentials Switch to token

2. From the Authentication Method drop-down list, select **Password**.
3. Capture the filtered list.

Stop wyUpdate Processes

The following processes must be stopped prior to running the wyUpdate.

Process	Detail
SysAdmin.TenantSvc	This service is the main service of UMP. It controls many operations. For example, it schedules and maintains the auto-replication cycles for all the customers, it sends information to the SysAdminTenant Database, etc.
SysAdmin.PeeringSvc	Used by Operator Connect when adding customers) – used only by Operator Connect set ups, whereby the OC Sync Task jobs are queued and executed.
all SysAdmin.CacheSrv. [tenant_shortname]	Each EssentialsPLUS and HostedPRO customer will have their own CacheService created, which will operate with each individual customer SQL database created. This operates by sending the relevant information to the SysAdmin[tenant_shortname] Database.

The table below lists of all the processes that are run during both major and patch upgrades in consecutive order.

Process	Detail	Executable
ClearWyupdateLog	Archive previous wyUpdate logging files	..\temp\000.__ClearWyupdateLog
CheckDuplicates	Remove duplicate SBC script templates in SQL.	..\temp\000.CheckDuplicates
CheckSQLConn	Check SQL server connection.	..\temp\001.CheckSQLConn
UmpAdmins	Check admin and user are on the same site.	..\temp\003.UmpAdmins
ClearUpgradefolderSQLscripts	refresh/clear SQL scripts and sysadminkit folders.	..\temp\005.ClearUpgradefolderSQLscripts
CheckServices	if not stopped SysAdmin* services, wyUpdate will pause, until services are stopped manually.	..\temp\005.CheckServices
SetServices	Configure services and create peeringSvc.	..\temp\005a.SetServices
StartPeeringSvc	Start peeringSvc.	..\temp\005b.StartPeeringSvc
CheckSQLDbBackupBackendFolder	Check SQL backend config	..\temp\005c.CheckSQLDbBackupBackendFolder
renameSysAdminKitFolder	Rename sysadminkit and SQL scripts folder by removing date-part	..\temp\005d.renameSysAdminKitFolder
RunSqlScripts	Run all upgrade scripts on SysAdminTenant database	..\temp\006.runsqlscript.exe
AddAuthPool	config pool in IIS	..\temp\070.AddAuthPool

Process	Detail	Executable
InstallPowershellGetModule	update/install PowerShell get	PowershellGet/PackageManagement
InstallMicrosoftTeamsModule	update/install Microsoft Teams	MicrosoftTeams
InstallChocolatey	update/install Chocolatey	Chocolatey
InstallDotNet	update/install DotNet	choco dotnet-6.0-runtime/dotnet-6.0-windowshosting
InstallRabbitmq	update/install RabbitMQ	choco rabbitmq
InstallEmsMainAgent	update/install EMS Main Agent	EmsMainAgent.msi 7.8.19.51806
InstallEmsClientAgent	update/install EMS Client Agent	EmsClientAgent.msi 7.8.21.52131
InstallPublicOvocConnector	update/install Public OVOC Connector	PublicOvocConnector.msi 1.0.8.51546
Installtap-windows-9.23.3-l601-Win10	update/install Tap-Windows	tap-windows-9.23.3-l601-Win10.exe
RunCheckAzureTenantId_220	check tenants-ids/passwords	c:\acs\CheckAzureTenantId_220\CheckAzureTenantId_220.exe
RunCheckAzureTenantId_220_Password	check tenantid/password	c:\acs\CheckAzureTenantId_220\CheckAzureTenantId_220.exe
AlertCustomerUpgrade	warning to run customer upgrade after wyUpdate finishes successfully	..\temp\170.AlertCustomerUpgrade.bat
runLogReport	show results wyUpdate process	c:\acs\tools\LogReport\LogReport.exe
Refresh_EMSCClientAgent_ignoreList	Refresh data on the ignorelist with default values	..\temp\EMSCClientAgentConfigIgnoreListData.ps1

Process	Detail	Executable
SysAdmin.QuickReplicationCycleWorker	Triggers the Cachesync mechanism for a specific customer.	
SysAdmin.UMP.Watchdog	Manages the database replication timer mechanism according the preconfigured setting in the <code>dbo.ApplicationSetting</code> {QuickReplicationCycleDelay}. Default-five minutes. Replication is processed only when no new changes are sent within the five minute interval. Grabs process threads for available queues.	
CacheSyncAzAd	Downloads users, groups and group membership using MSGraph.	
CacheSync/CacheSyncV2	<ul style="list-style-type: none"> ■ Downloads all the CsOnlineUsers ■ Downloads all the Teams user policies 	
SysAdmin.UMP.SyncAcquiredNumber	Used by Operator Connect (OC) for updating the Assignment Status column in the Number Management table in the	

Process	Detail	Executable
	self-service portal. It is run every 5 minutes.	

Additional SysAdmin Verifications

- If a UMP 365 server is hardened through stricter Security policies and services are required to be white-listed, add the following services (created when upgrading to version 8.0.450) to the white-list:

- SysAdmin.QuickReplicationCycleWorker
- SysAdmin.UMP.Watchdog
- SysAdmin.SyncAcquiredNumber

See [Managing the Replication Cycle](#) on page 246 for details on the above services.

- Microsoft Graph PowerShell module is installed by the installation script (the AzureAD PowerShell module is approaching end-of-service). Consequently, ensure that any 3rd party Anti-virus software does not restrict the installation of the Microsoft Graph module.
- Ensure that the SQL Server Management Studio's server collation is correctly set to **SQL_Latin1_General_CP1_CI_AS**. If not, then a re installation of the SQL server is required to change the Server Collation.



Make sure all databases are backed up before removing the SQL server, so that they can be correctly restored (see [Backing up UMP-365 – Disk Snapshot](#) on page 121).

22 Upgrading Main UMP-365 Tenant

This step describes how to run the wyUpdate Tool to upgrade the UMP version on the UMP server.

➤ **Do the following:**

1. On the UMP server, open the Windows Services Manager, stop all sysadmin services, or type the following command in PowerShell (Run as Admin) to stop all UMP sysadmin services:

```
stop-service sysadmin*
```

2. Type the following PowerShell command to stop all www services/internet IIS services.

```
stop-service w3svc
```

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


```
get-service sysadmin*
```

```
get-service w3svc
```

4. If one of the above services has not been stopped, open the Windows Services Manager



Services

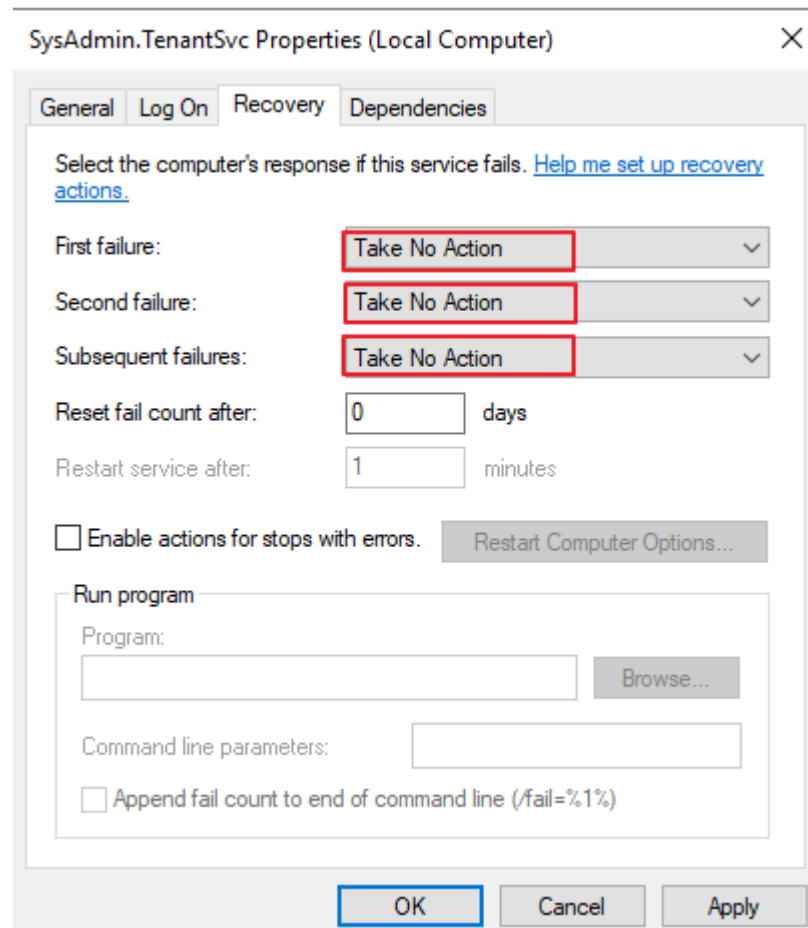
(click  and type **Services**) right-click each of the above services, and then select **Stop**.



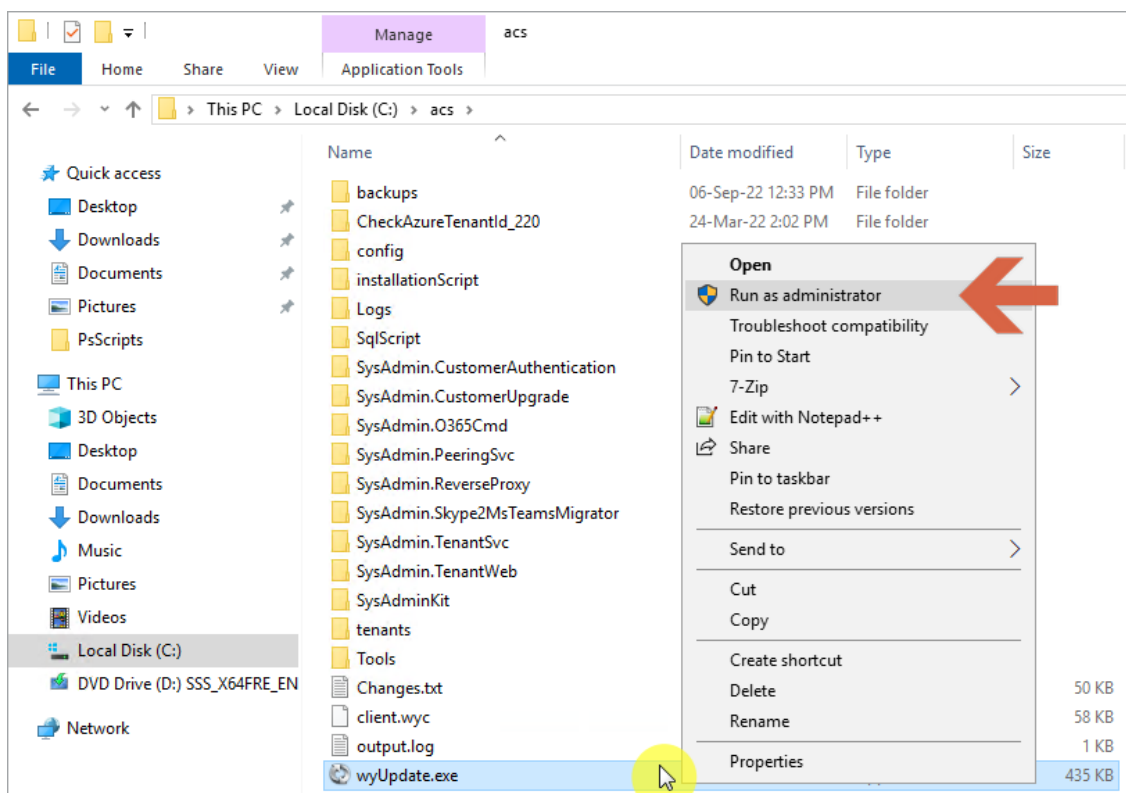
To save time, type only the following command:
`stop-service sysadmin*, w3svc`

The following services are stopped prior to running the wyUpdate.exe:

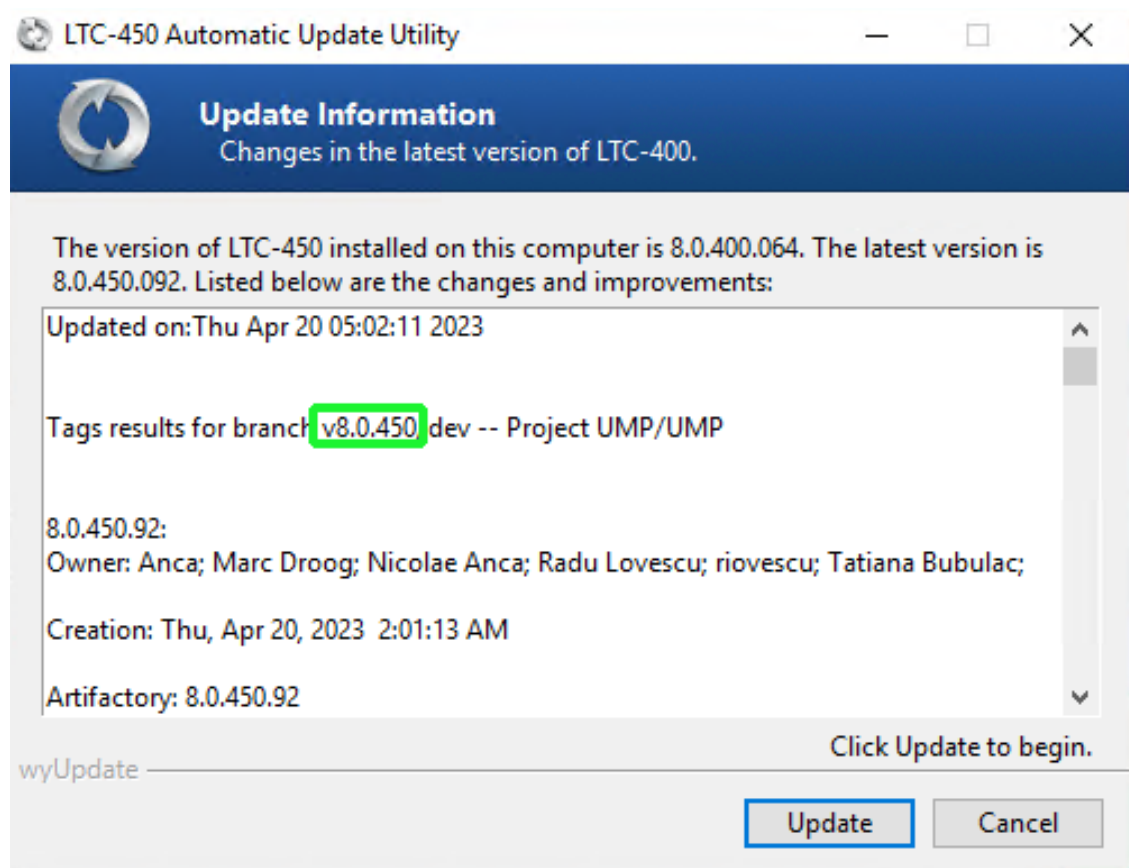
- SysAdmin.TenantSvc
 - SysAdmin.PeeringSvc
 - all SysAdmin.CacheSrv.[tenant_shortname]
5. If a service keeps restarting, set the properties of the service SysAdmin.TenantSvc to **Take No Action** (see example in figure below).



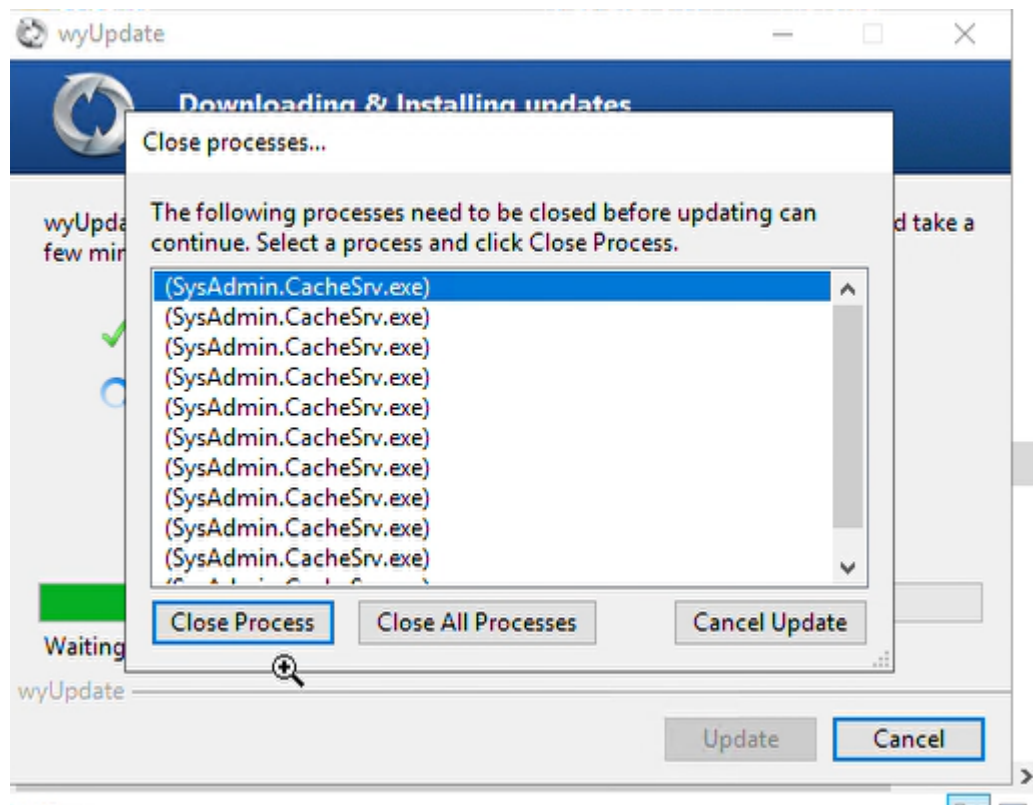
6. Run wyUpdate.exe. (right-click **Run as Administrator**).



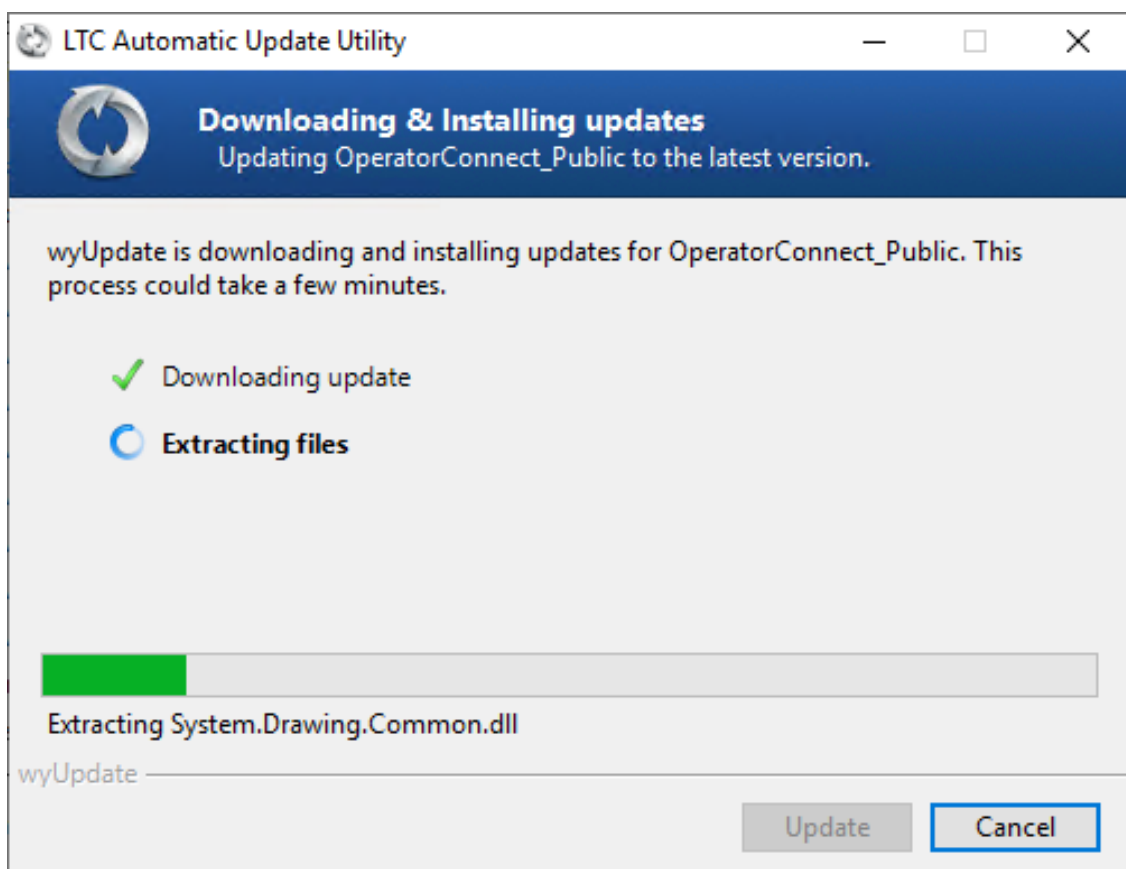
7. In the Updated dialog, click **Update**. The wyUpdate tool validates the installed version to determine whether updates are available, or an upgrade is required.



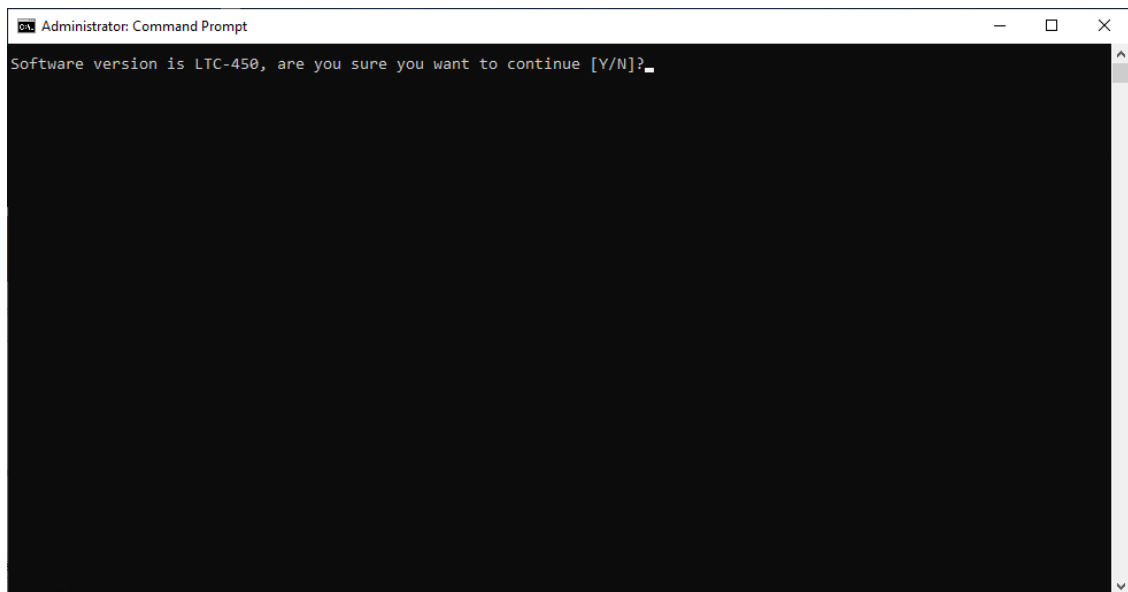
8. If you did not close all the services via PowerShell, then during the update you are prompted to "Close processes...". Confirm this action. This kills the running processes and continues the upgrade.



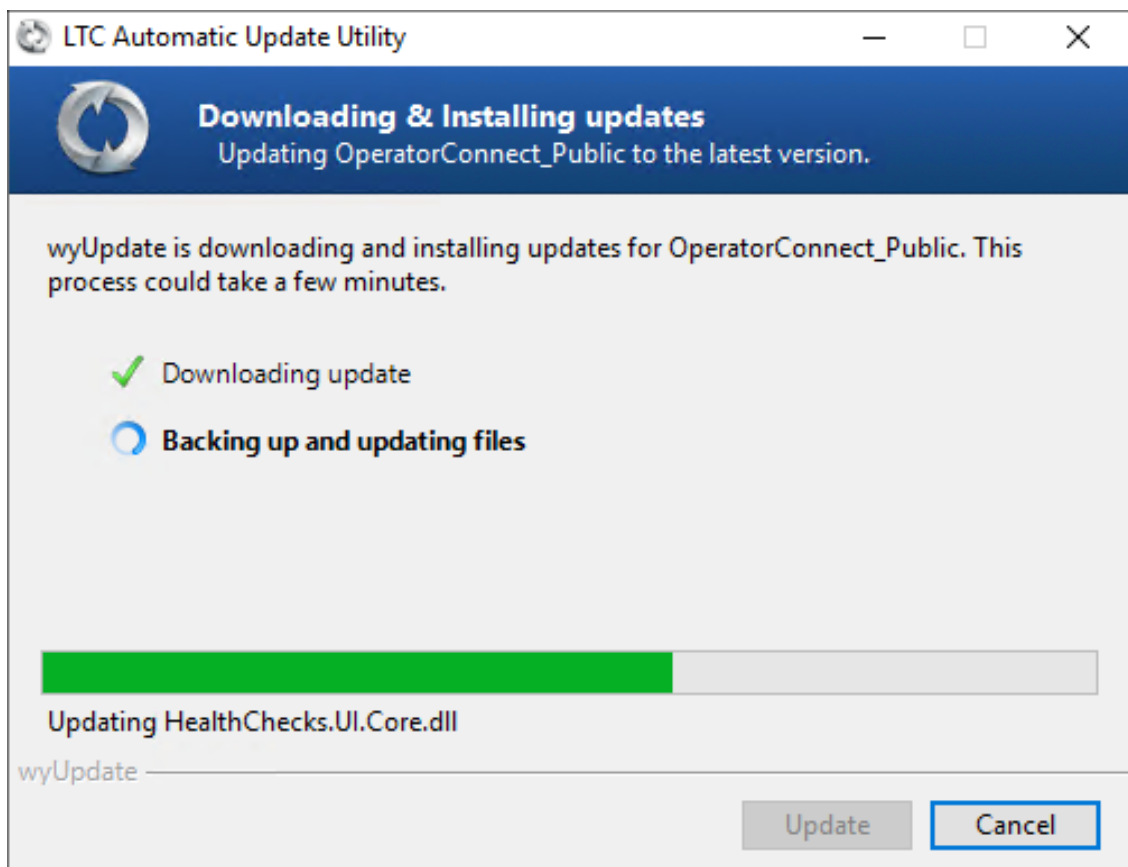
The available updates / version upgrade packages are downloaded to a temporary folder and the files are installed.



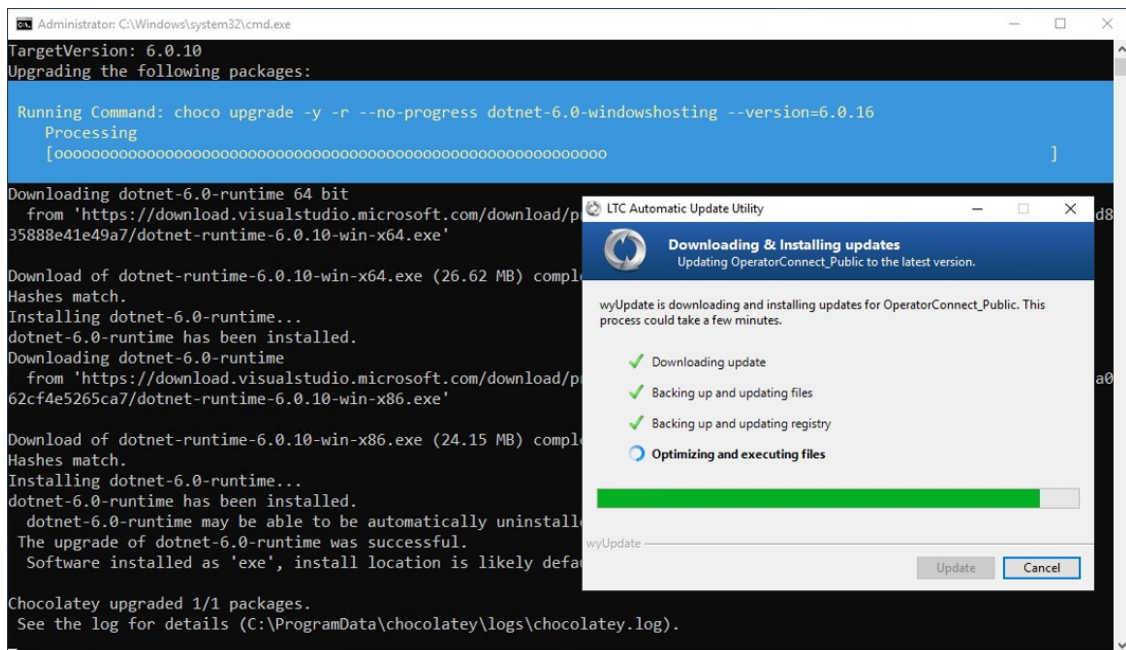
9. The upgrade process is interrupted via the CMD window pop-up. The following prompt is displayed:
Warning ... Are you sure you want to continue. [Y / N] ?
10. Type **Y** and press Enter.



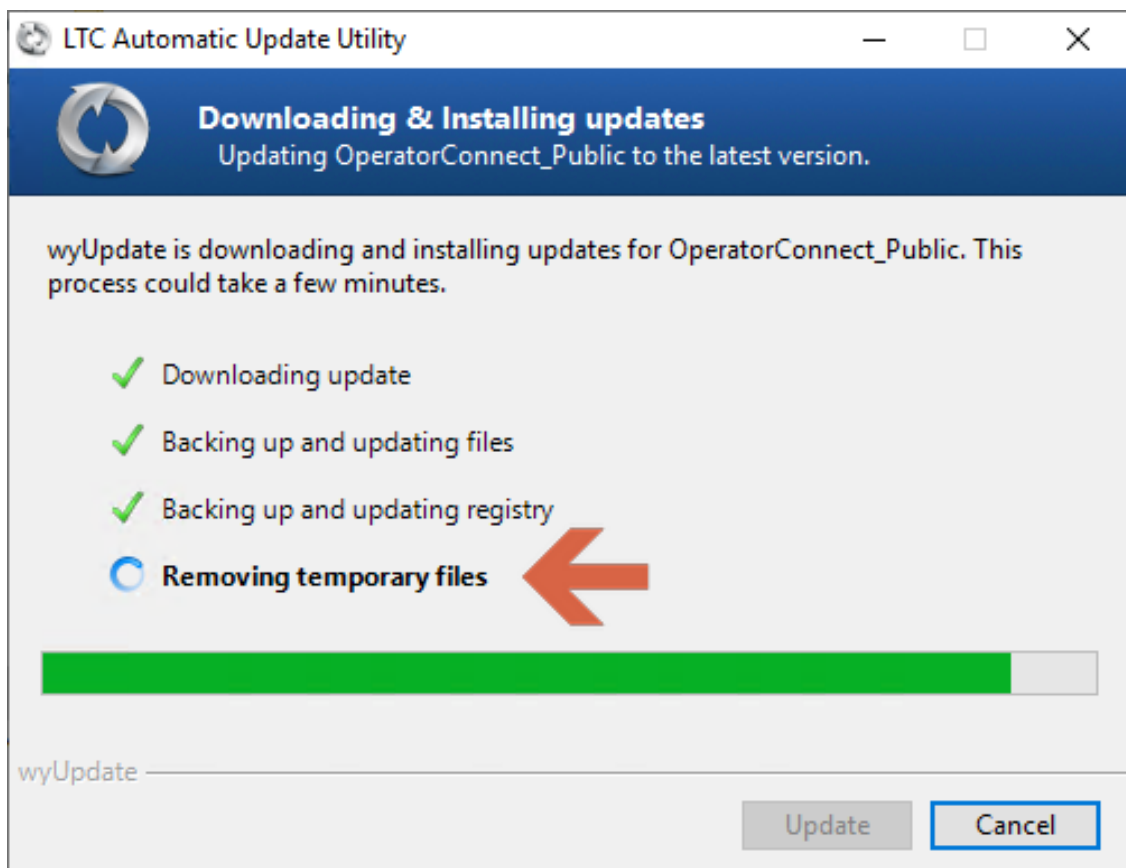
- Folders are backed up and files are updated.



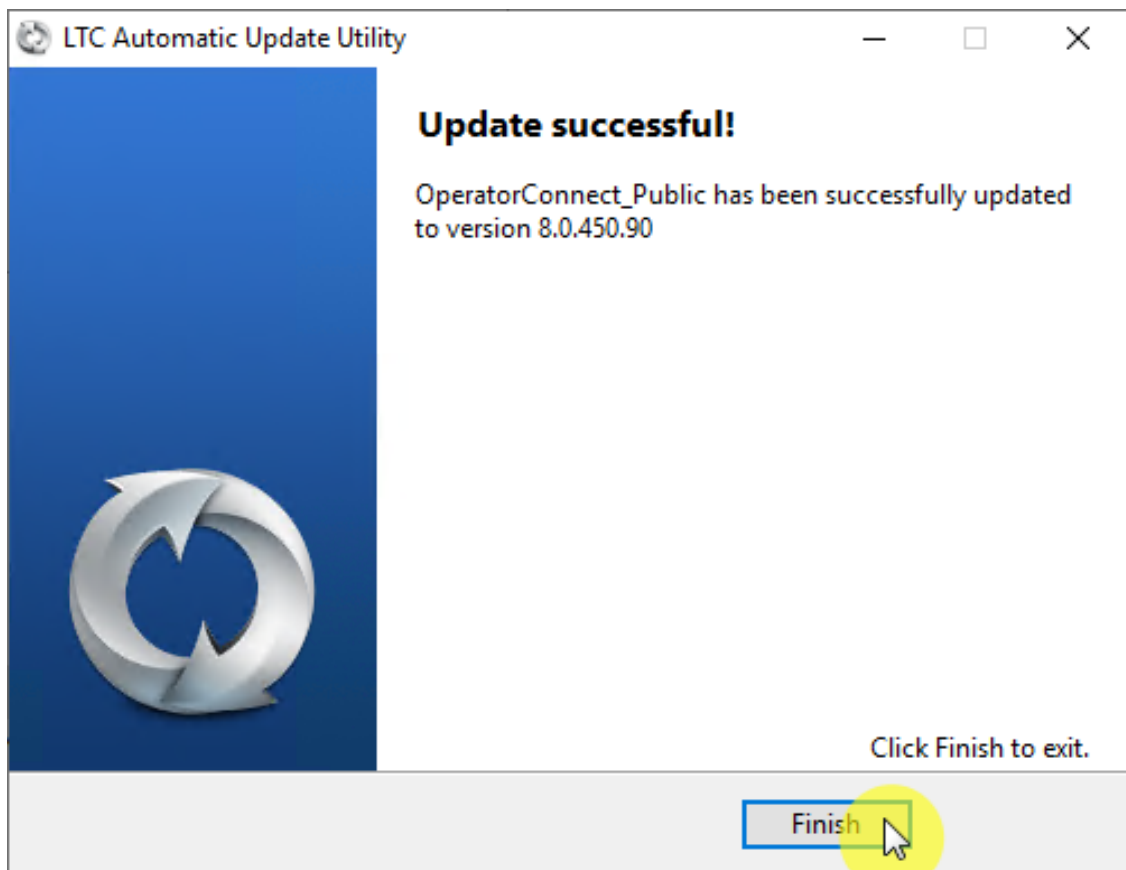
- During the optimization and execution, various necessary software packages are installed as described in [Stop wyUpdate Processes](#) on page 126.



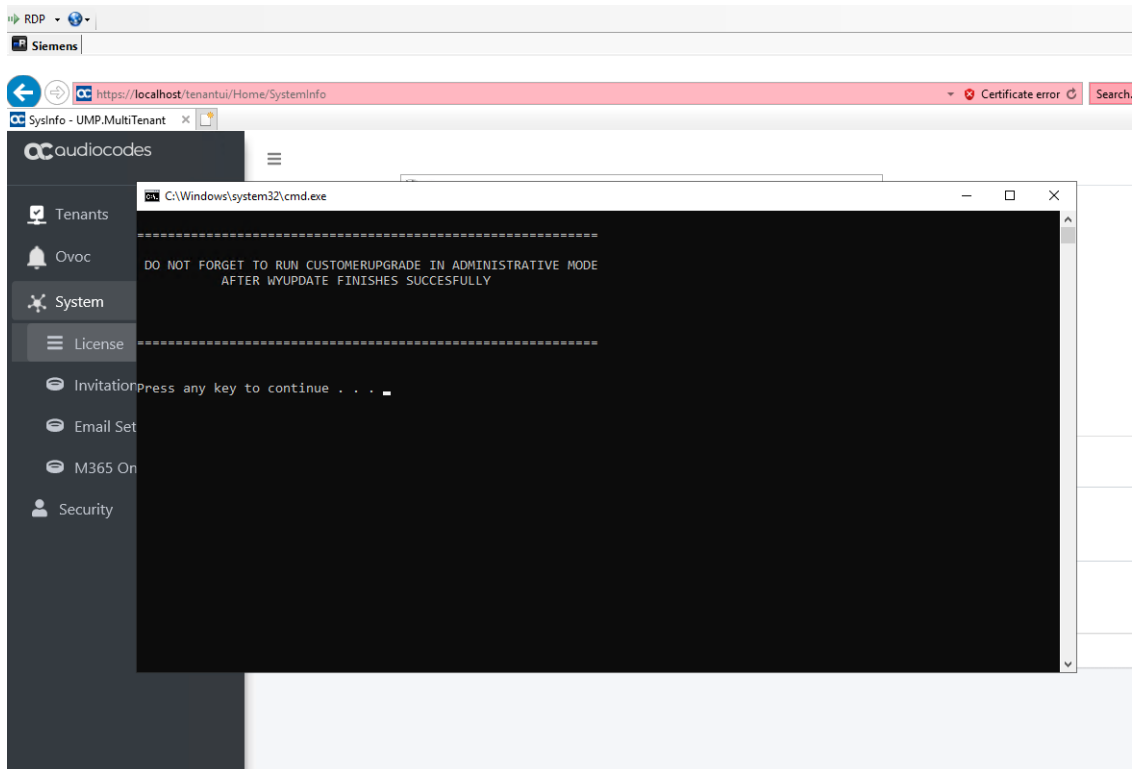
- Temporary files are removed.



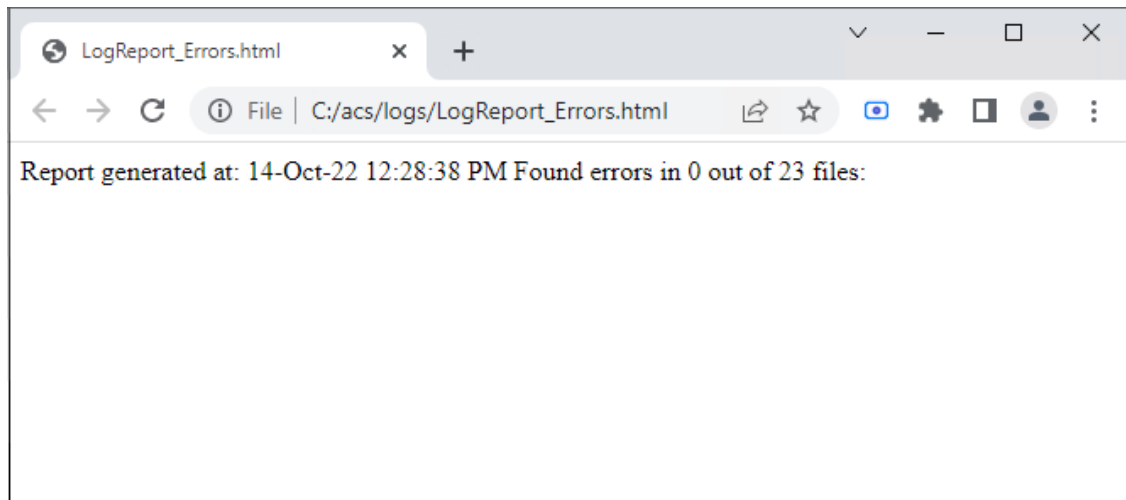
- Click **Finish**.



12. In the Command shell, press any key to continue or wait a few seconds.



A LogReport for all Errors found during the upgrade is displayed in the default browser.



23 Upgrading Customer Tenant

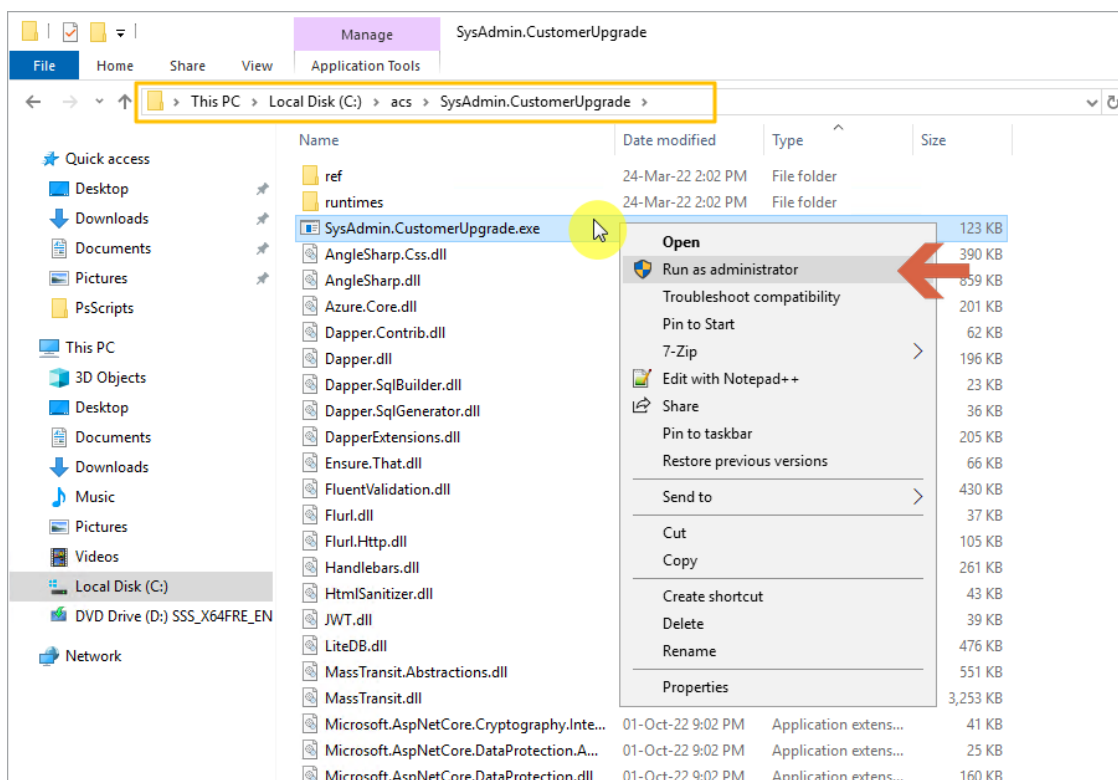
This step describes how to run the Customer Upgrade service for updating each customer tenant.



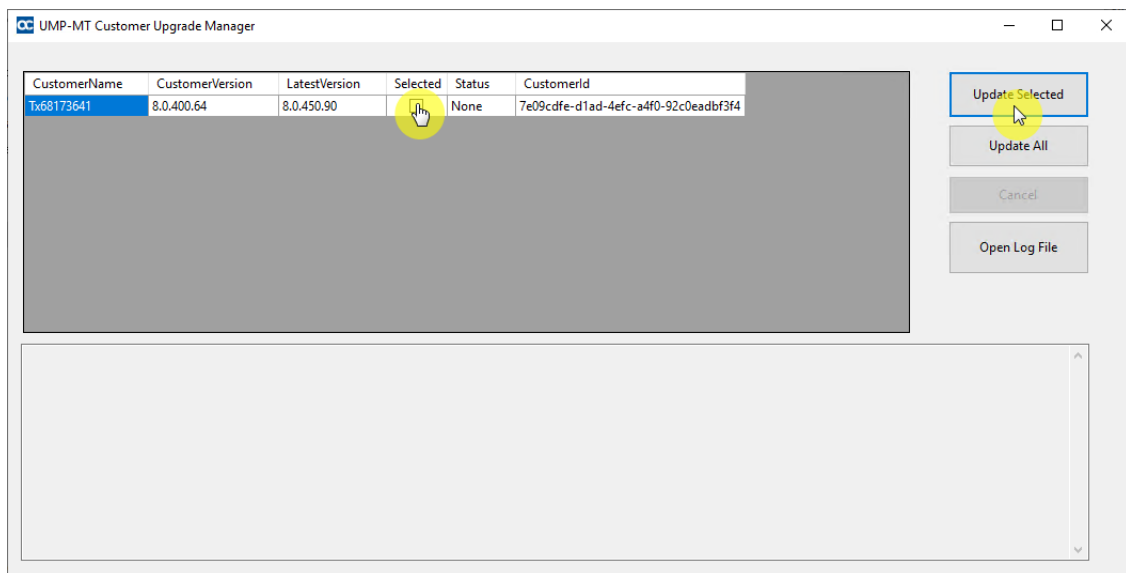
- Run the Sysadmin.CustomerUpgrade.exe as an Administrator using the UMP service admin account that was created in "Create UMP Service Account" in User Management Pack 365 Administrator and Installation Manual.
- If you have a back-end SQL server for all your tenants, ensure that the username and password for the UMP service accounts are the same for both servers.

➤ Do the following:

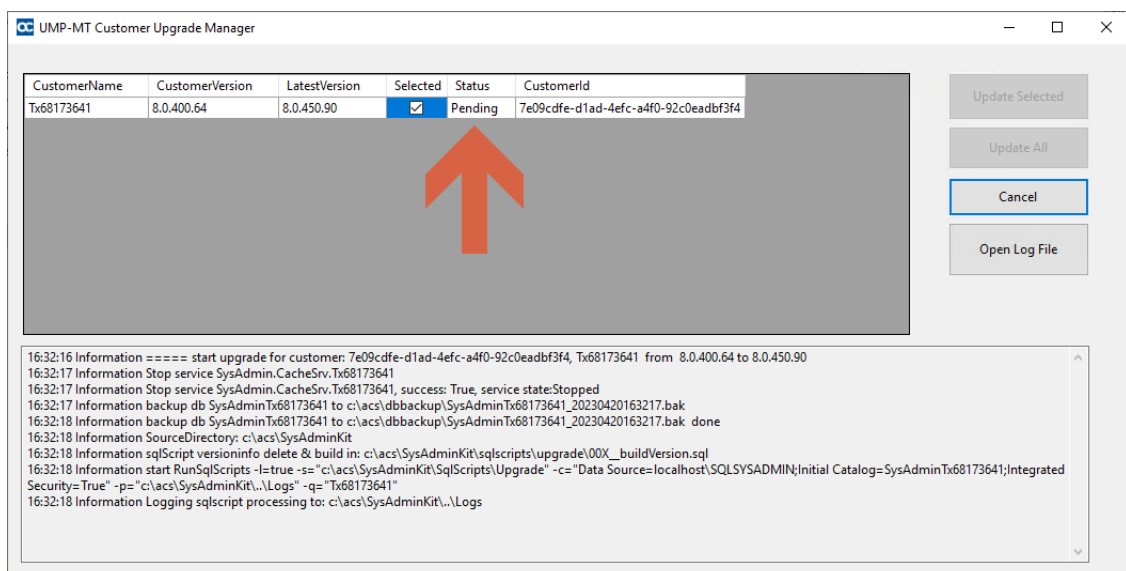
1. Run the file Sysadmin.CustomerUpgrade.exe from directory C:\acs\SysAdmin.CustomerUpgrade.



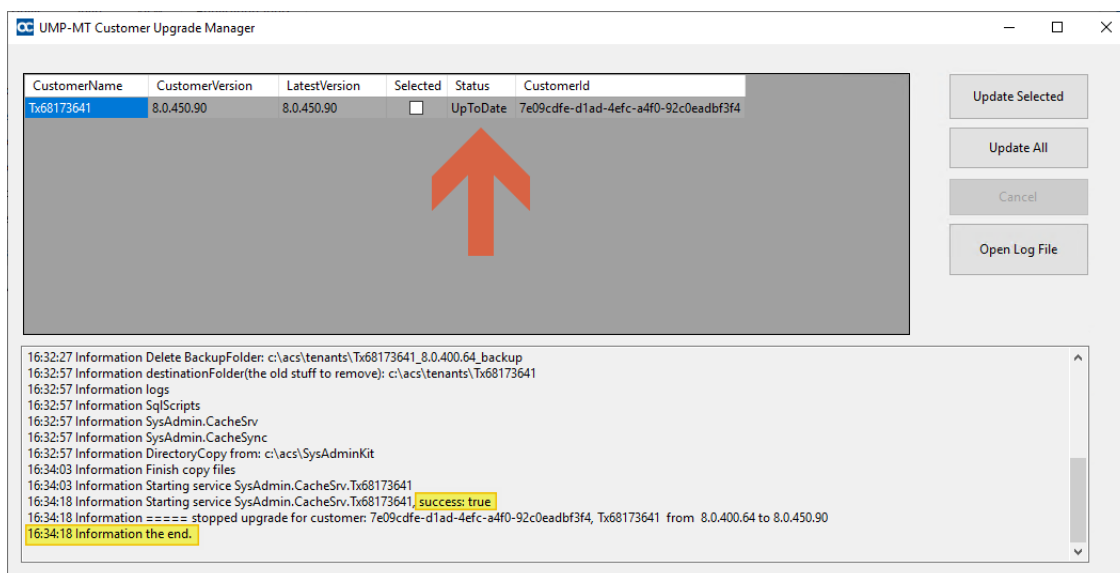
2. In the Customer Upgrade Manager, select the customers for which you wish to upgrade and then click **Update Selected**.





During the upgrade process, a pending message is displayed.



- At the end of the process, verify in the log that the upgrade session has been successfully completed, indicated with status "UpToDate" and then close this window.



4. Open the Windows Services Manager  **Services** (click  and type **Services**), start all sysadmin* and the World Wide Web services, or in PowerShell, type the following command:

```
Start-Service sysadmin*, w3svc
```

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

PS C:\Users\Administrator> Start-Service sysadmin*, w3svc
PS C:\Users\Administrator> Get-Service sysadmin*, w3svc

Status      Name                DisplayName
-----
Running     SysAdmin.CacheS...  SysAdmin.CacheSrv.24009835
Running     SysAdmin.Peerin...  SysAdmin.PeeringSvc
Running     SysAdmin.TenantSvc  SysAdmin.TenantSvc
Running     w3svc               World Wide Web Publishing Service

PS C:\Users\Administrator> 
```



Execute the Get-Service sysadmin*, w3svc command to ensure that all the services are running.

5. In the Multitenant portal, open the Tenants page and verify that the following upgraded versions are displayed:
- The wyUpdate version of the main UMP sysadminKit.
 - The SysAdminCustomerUpgrade version of the customers.

The screenshot shows the Multitenant portal interface. On the left is a sidebar with navigation links: Tenants, Overview, System, Security, SBC List, and Queued Tasks. The main content area displays a table of tenants. At the top, a summary bar shows 'Available Users: 9970, Available Customers: 499' and 'SysadminKit Version: 8.0.400.64'. Below this is a table with the following columns: Customer Name, State, SysAdmin Info, Licensing (licensed users), and Queued commands status. The first row of the table shows a tenant with Customer Name 'M365x24009835', State 'Deployed', SysAdmin Info 'version: 8.0.400.64' and 'replication: 2022.10.14.12.59.41', Licensing 'M365 - Pro (30)', and Queued commands status 'Queued commands: 0, Executing commands: 0, Replication in progress: no'. The version number '8.0.400.64' and the replication status '2022.10.14.12.59.41' are highlighted with red boxes and red circles with the numbers 2 and 1 respectively. The table also includes action links like 'Edit', 'Delete', 'Undo Deploy', 'Add SBC Site', and 'Queue Replication'. At the bottom, it shows 'Showing 1 to 1 of 1 entries' and navigation buttons 'Previous', '1', and 'Next'.

24 Post Upgrade Actions

This section describes the actions to perform following the upgrade:

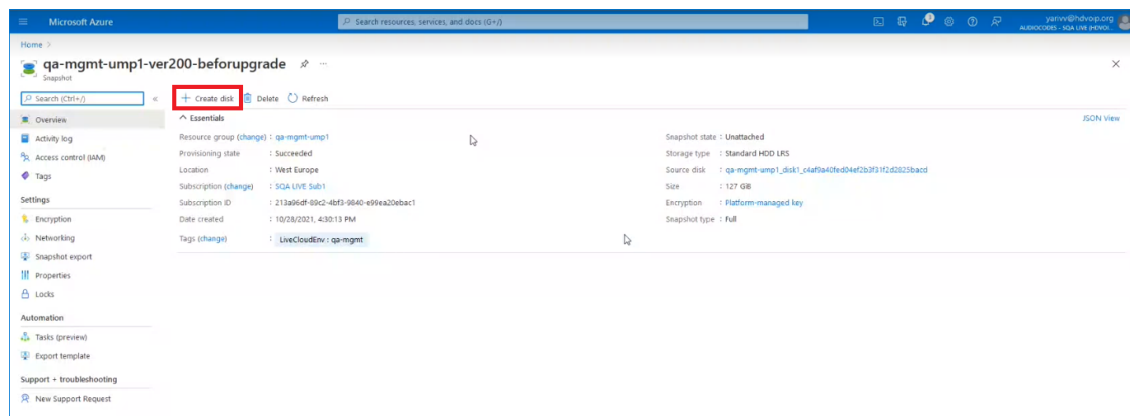
- [Restoring UMP Snapshot](#) below
- [Verifying Tenant Admin Authentication](#) on page 147
- [Upgrading M365 Connection to Token Authentication](#) on page 148
- [Updating Scripts](#) on page 159
- [Verifying Component Statuses](#) on page 159
- [Updating SQL Server](#) on page 166
- [SBC Dialplan Verification](#) on page 166

Restoring UMP Snapshot

This section describes how to create a new disk on the UMP VM and to restore the snapshot image created in [Backing up UMP-365 – Disk Snapshot](#) on page 121 to this disk (create a new VHD image for this disk).

➤ Do the following:

1. Open the new snapshot that you created in [Backing up UMP-365 – Disk Snapshot](#) on page 121 and click **Create Disk**.



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

The screenshot shows the 'Create a managed disk' page in the Microsoft Azure portal. The breadcrumb trail is 'Home > qa-mgmt-ump1-ver200-beforupgrade >'. The page title is 'Create a managed disk'. Below the title are tabs for 'Basics', 'Encryption', 'Networking', 'Advanced', 'Tags', and 'Review + create'. The 'Basics' tab is selected. A message states: 'Select the disk type and size needed for your workload. Azure disks are designed for 99.999% availability. Azure managed disks encrypt your data at rest, by default, using Storage Service Encryption. [Learn more about disks.](#)'

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

Subscription * ⓘ: SQA LIVE Sub1
Resource group * ⓘ: qa-mgmt-ump1
[Create new](#)

Disk details

Disk name * ⓘ: qa-mgmt-ump1-ver200 ✓
Region ⓘ: (Europe) West Europe
Availability zone: 1
Source type ⓘ: Snapshot
Source subscription ⓘ: SQA LIVE Sub1
Source snapshot ⓘ: qa-mgmt-ump1-ver200-beforupgrade
Size * ⓘ: 128 GiB
Premium SSD LRS
[Change size](#)

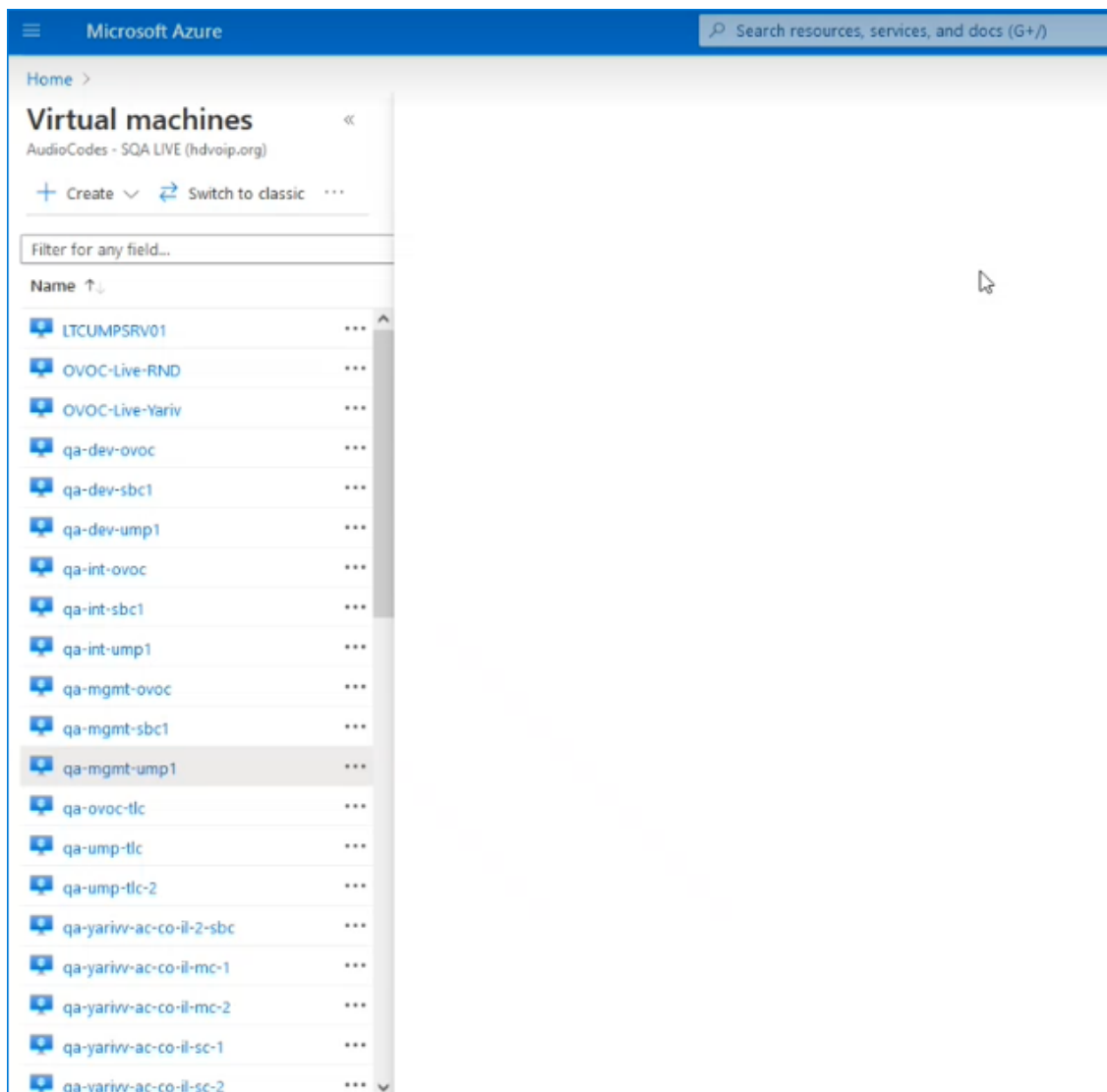
Navigation buttons at the bottom: 'Review + create' (blue), '< Previous' (disabled), and 'Next : Encryption >' (active, with a mouse cursor clicking it).

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

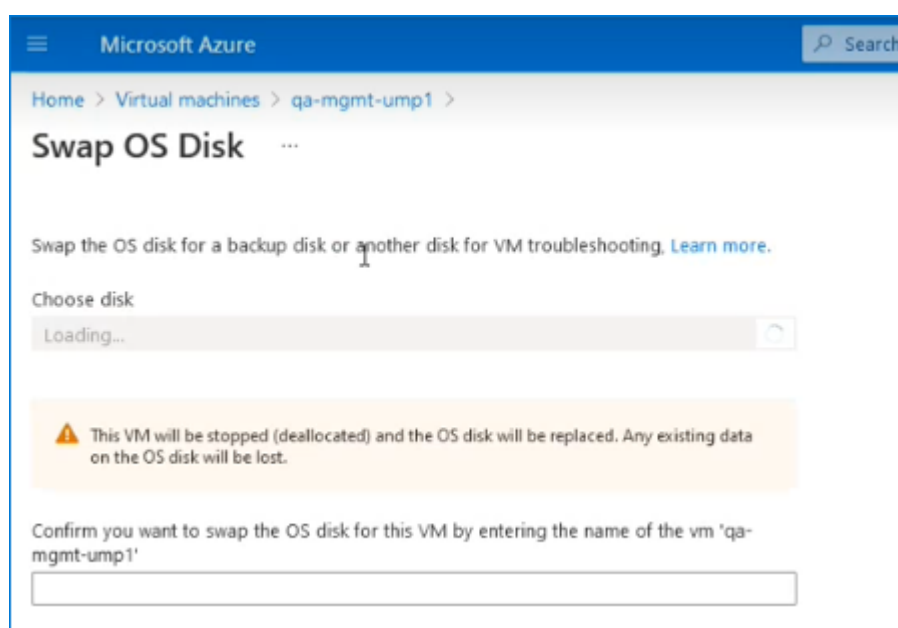
The screenshot shows the 'Create a managed disk' page in the Microsoft Azure portal. The breadcrumb trail is 'Home > qa-mgmt-ump1-ver200-beforupgrade >'. The page title is 'Create a managed disk'. Below the title are tabs for 'Basics', 'Encryption', 'Networking', 'Advanced', 'Tags' (which is selected), and 'Review + create'. A paragraph explains that tags are name/value pairs for categorizing resources and consolidated billing, with a link to 'Learn more about tags'. A note states that tags will be automatically updated if resource settings change on other tabs. The 'Tags' section contains a table with three columns: 'Name', 'Value', and 'Resource'. The first row has 'LiveCloudEnv' in the 'Name' column, an empty input field in the 'Value' column, and a dropdown menu in the 'Resource' column showing '2 selected'. A second row has an empty input field in the 'Name' column, a dropdown menu in the 'Value' column showing 'qa-dev', 'qa-int', and 'qa-mgmt' (with a mouse cursor hovering over it), and another dropdown menu in the 'Resource' column showing '2 selected'. At the bottom of the page are three buttons: 'Review + create' (in blue), '< Previous', and 'Next : Review + create >'.

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

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



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



- From the Choose Disk drop-down list, choose the snapshot that you created in [Backing up UMP-365 – Disk Snapshot](#) on page 121 (in this example “qa-mgmt-ump1-ver200”).

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

Verifying Tenant Admin Authentication

Ensure that the Customer Tenant Global Admins authentication for connecting to their respective Microsoft 365 platform is successful for all managed tenants on the UMP 365 server.

➤ Do the following:

- Open the Authentication Status screen (**Security** menu > **Authentication Status**).

Customer Id	M365 Email	Authentication method	When Last Verified	Last Verification Status	Actions
Tx74860876	alexw@M365x74860876.onmicrosoft.com	Password	April 20th 2023, 16:54	✓	Check Credentials Switch to token
Tx68173641	alexw@M365x68173641.onmicrosoft.com	Token	April 20th 2023, 16:50	✓	Check Credentials Switch to password
Tx52595777	admin@M365x52595777.onmicrosoft.com	Token	April 20th 2023, 16:50	✓	Check Credentials Switch to password

- Update the table (1).
- Verify the status for all tenants (2).
- Reload the table (3).

5. If any Tenant verification fails, verify credentials and retry.

Customer Id	M365 Email	Authentication method	When Last Verified	Last Verification Status	Actions
dr8	admin@AudcDemo6.onmicrosoft.com	Token	July 30th 2023, 17:41		Check Credentials Switch to password
Demo	admin@M365x08167531.onmicrosoft.com	Password	July 30th 2023, 15:37		Check Credentials Switch to token

Upgrading M365 Connection to Token Authentication

Customers upgrading from version 8.0.400 who consented to the Service Provider for securing access to their Microsoft 365 platform with provided username and password, must now secure this connection using Microsoft Graph Token-based authentication as a result of enhanced Microsoft security policies.



Queued tasks will not be synchronized with Microsoft 365 until Token-based authentication is implemented and the connection successfully verified.

The Token-based authentication can be secured using the following methods:

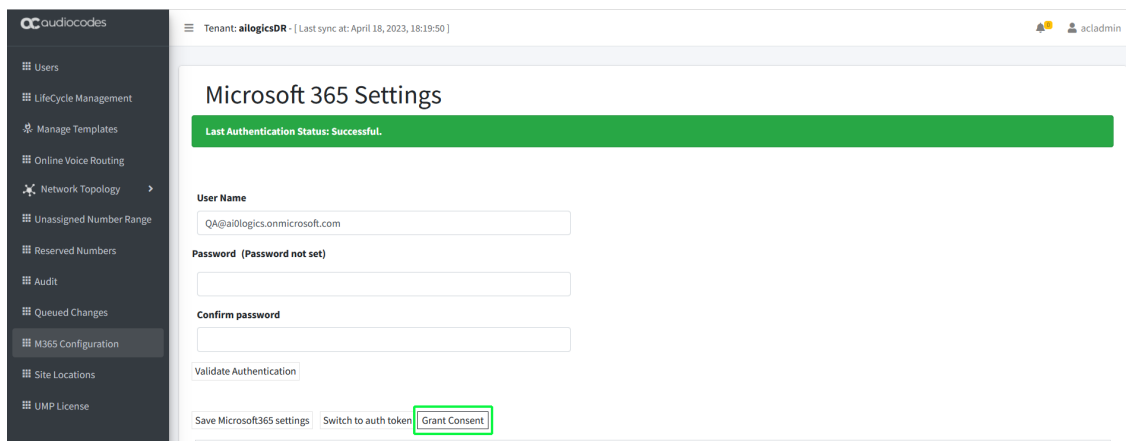
- **Password-based authentication and Token authentication:** A Microsoft Graph access token is claimed based on the configured user name and password. For implementing this option, select the **Grant Consent** option in the Microsoft 365 Settings screen (see procedure below).
- **Token-only authentication:** A Microsoft Graph access token is claimed directly, triggered by an email link sent to the customer. For implementing this option, select the **Switch to auth token** option in the Microsoft 365 Settings screen (see [Switching to Token Authentication](#) on page 519). This is the **recommended** the method.

Once consent is provided, an Enterprise application is created on the customer Azure tenant including the following permissions:

- Access Microsoft Teams and Skype for Business as the signed in user
- Read and write all groups
- Access directory as the signed-in user
- Read all users' full profiles
- Read and write to all app catalogs
- Maintain access to data you have given it access to

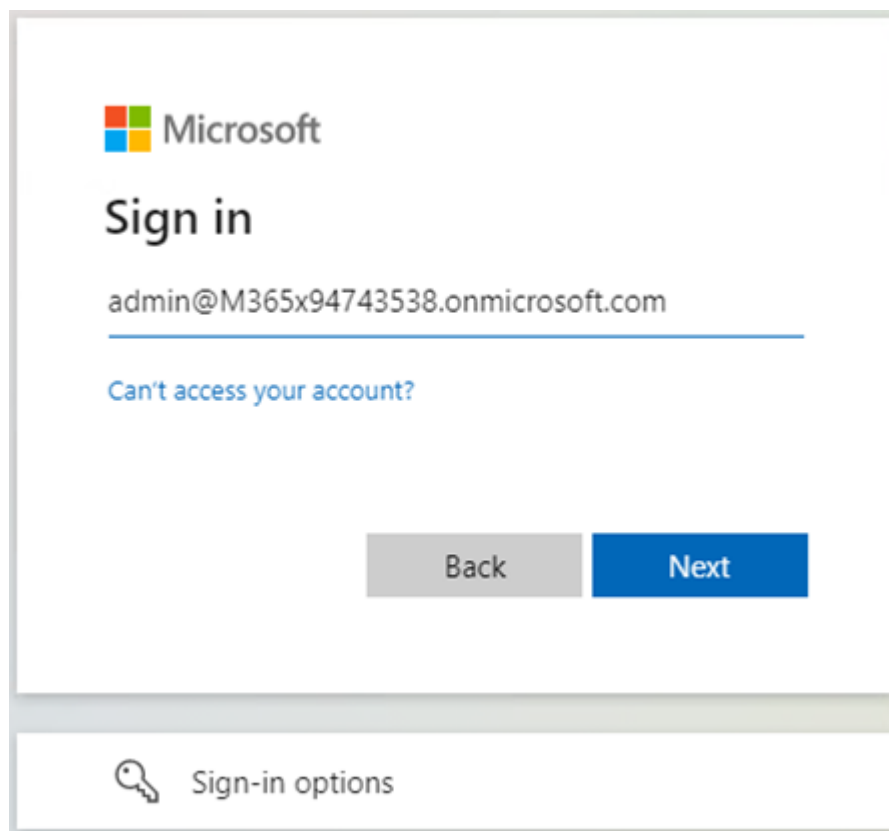
➤ To secure Token-based connection with Grant Consent:

1. In the Customer portal Navigation pane, select **M365 Configuration**.

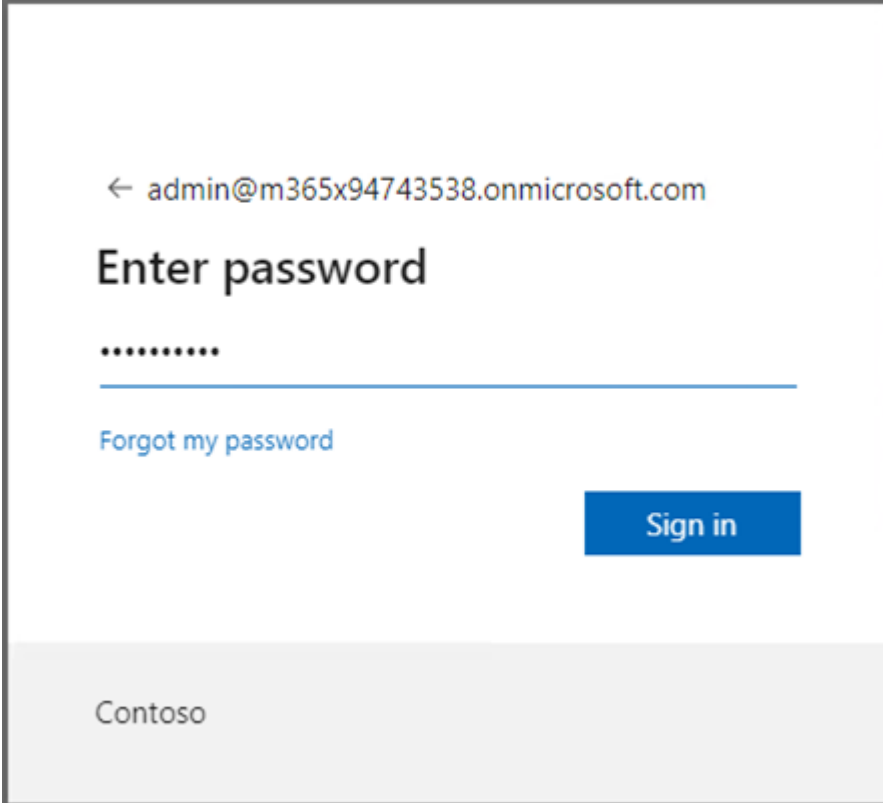


The screenshot shows the 'Microsoft 365 Settings' page in the alicodes interface. The left sidebar contains a menu with items: Users, Lifecycle Management, Manage Templates, Online Voice Routing, Network Topology, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration (highlighted), Site Locations, and UMP License. The main content area has a header 'Tenant: alicodesDR - [Last sync at: April 18, 2023, 18:19:50]' and a user icon 'aadmin'. Below the header is a green bar stating 'Last Authentication Status: Successful.' The form includes fields for 'User Name' (QA@allogics.onmicrosoft.com), 'Password (Password not set)', and 'Confirm password'. There is a 'Validate Authentication' button and a 'Grant Consent' button highlighted with a green box. At the bottom, there are buttons for 'Save Microsoft365 settings', 'Switch to auth token', and 'Grant Consent'.

2. Click **Grant Consent**.



The screenshot shows the Microsoft Sign in page. It features the Microsoft logo at the top left, followed by the text 'Sign in'. Below this is the email address 'admin@M365x94743538.onmicrosoft.com' with a blue underline. A link 'Can't access your account?' is visible. At the bottom right, there are two buttons: 'Back' (grey) and 'Next' (blue). At the bottom left, there is a key icon and the text 'Sign-in options'.




The screenshot shows a web-based sign-in interface. At the top, there is a back arrow and the email address 'admin@m365x94743538.onmicrosoft.com'. Below this is the heading 'Enter password'. A password field is shown with eight dots. Underneath the password field is a blue link that says 'Forgot my password'. To the right of the password field is a blue button labeled 'Sign in'. At the bottom of the page, the name 'Contoso' is displayed in a light gray bar.

- a. Enter customer IT Administrator credentials with "Global" Admin permissions.



The M365 User Account must have "Global" Admin permissions, otherwise the "Consent on behalf of the organization" check box does not appear.



admin@m365x94743538.onmicrosoft.com

Permissions requested

Warrick_Token_Background_Replication
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to
- ☒ **Consent on behalf of your organization**

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

- b. Click "Consent on behalf of your organization" and then click **Accept**.

Once the process has completed successfully, the following confirmation is displayed:

Thank you!

You may close this window

Service provider will contact you when service is ready for operation

audiocodes Thank you!

You may close this window

Service provider will contact you when service is ready for operation

Microsoft Azure

Home > Contoso > Enterprise applications > Enterprise applications | All applications > Warrick_Token_Background_Replication

Warrick_Token_Background_Replication | Permissions

Overview Deployment Plan Diagnose and solve problems Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Self-service Custom security attributes (Preview) Security Conditional Access Permissions Token encryption Activity Sign-in logs Usage & insights Audit logs Provisioning logs Access reviews Troubleshooting + Support

Refresh Review permissions Got feedback?

Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application. [Learn more](#).

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

[Grant admin consent for Contoso](#)

Admin consent User consent

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph					
Microsoft Graph	Group.ReadWrite.All	Read and write all groups	Delegated	Admin consent	An administrator
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed in user	Delegated	Admin consent	An administrator
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated	Admin consent	An administrator
Microsoft Graph	AppCatalog.ReadWrite.All	Read and write to all app catalogs	Delegated	Admin consent	An administrator
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	Admin consent	An administrator
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Skype and Teams Tenant Admin API					
Skype and Teams Tenant Admin API	user_impersonation	Access Microsoft Teams and Skype for Business data as the signed in user	Delegated	Admin consent	An administrator

Microsoft Azure

Home > Contoso > Enterprise applications > Enterprise applications

Enterprise applications | All applications

Overview Overview Diagnose and solve problems Manage All applications Application proxy User settings App launchers Custom authentication extensions (Preview) Security Conditional Access Consent and permissions Activity Sign-in logs Usage & insights Audit logs Provisioning logs Access reviews Admin consent requests Bulk operation results Troubleshooting + Support New support request

+ New application Refresh Download (Export) Preview info Columns Preview features Got feedback?

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Background Application type == Enterprise Applications Application ID starts with Add filters

1 application found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status
Warrick_Token_Background_Replicat...	e4c42766-9690-45c4-89ad-e4ee9545931	102a2c69-9495-430e-9c0f-9ad33d93e560		4/19/2023	-

Switching to Token Authentication

Customer consent for securing Service Provider access to their Microsoft 365 platform can be secured using **only** Microsoft Graph Token-based authentication.



This is recommended method for securing connection to Microsoft 365.

➤ To switch to token authentication:

1. In the Customer portal Navigation pane, select **Microsoft 365 Settings**.
2. Click **Validate Authentication** to ensure current token is valid. Last Authentication Status: Successful is displayed.

3. In the **Microsoft 365 Settings** screen, click **Switch to auth token**.

The following dialog is displayed.

4. Enter the email address of the customer administrator to whom you wish to send the invitation.

The following confirmation screen is displayed showing the invitation sent to the customer IT administrator from the Service Provider IT administrator.

- In the Main Tenant interface, open the Customer Invitations screen (see [Customer Invitations](#) on page 225) View the Customer Invitation sent to the email address entered above.

ID	Full Name	Invitation Email	M365 Admin Email	Email Sent	Email Invitation Sent Count	Created at	Expires at	Device Authenticated	Tenant Installed	Actions
20220823		test@gmail.com	admin@M365x74218585.onmicrosoft.com	true	1	2022-08-29	2022-09-03		Yes	Send Reminder Revoke Request Auth URL

An email similar to the following is sent to the customer administrator.

<onboarding@audiocodes.be> בתאריך: 24 באפריל 2023, 18:13

Dear Administrator of BradSIP,

We at Sandbox3.FineBak welcomes you to join our "AudioCodes Live Cloud" service.

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

http://url1207.audiocodes.be/ls/click?uon=a12WafR444P7.2B7DSb5PxErMoe1UbCLZS.2BkTVw/NmXwDap5D33qLeRR5p7ZuQRBqJIDwChScjKnlXdtGMMKIPX.2FF3UFVBEKEDCHIAMZDzhvOkKYuum9xudKobc2py_JSLV81wauxhQzQz3qQH4H4JXCL.2FonCqkofH5.2BmleXrgQH7NmITNR0TB6eR.2Bof35teooWaxVUQqRB6bAqoXaATCHAq8.2B##af-2BEEhGCoOX.2Bxmgy5wQxcB9DAAdAnyQJ42lrmS9GTOMDVGradmyG8xPDeexhtlws7gq7pXSCdDECFWcolbnGUs4Fdc5RlkXyS.2BQz65.2FB9C298yhsWzBkCHIElmt5.2BcaFqA.3D

Please Note that Global Admin will be required in order to approve the LiveCloud consents.

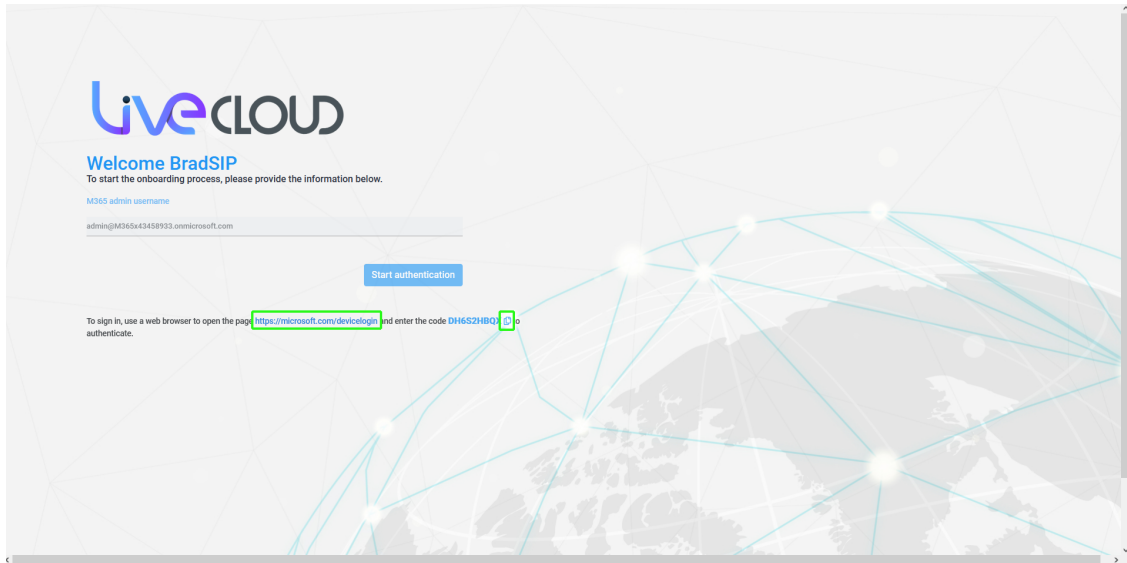
- The Authentication process will run against your Microsoft M365 Tenant, we will not know or save your password.
- Revoke Token Authentication: you are able to revoke the authentication at any time. Revoking the authentication will stop the service.

Thank you and best regards,

Sandbox3.FineBak Team

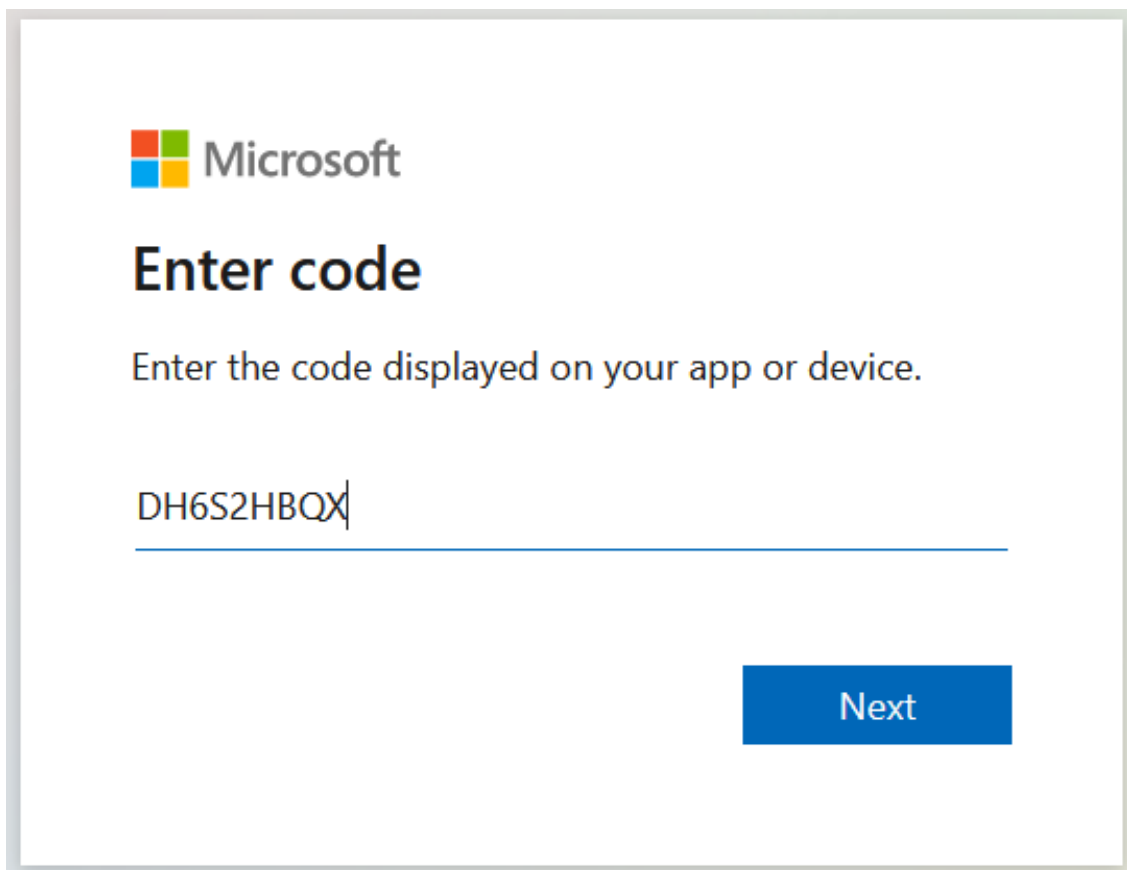
- Click the link sent in the mail to start the authentication process.

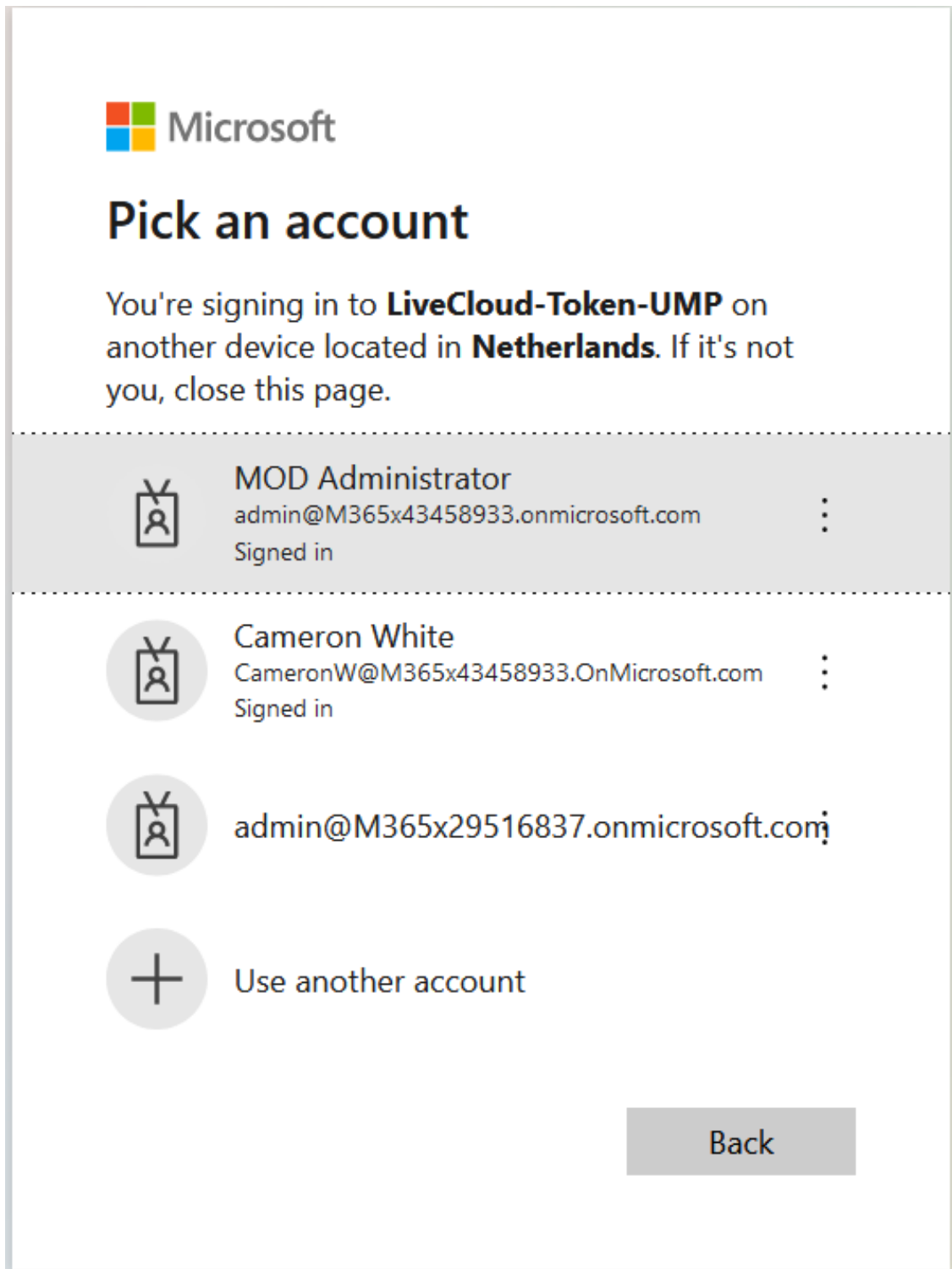
7. Click **Start authentication**.



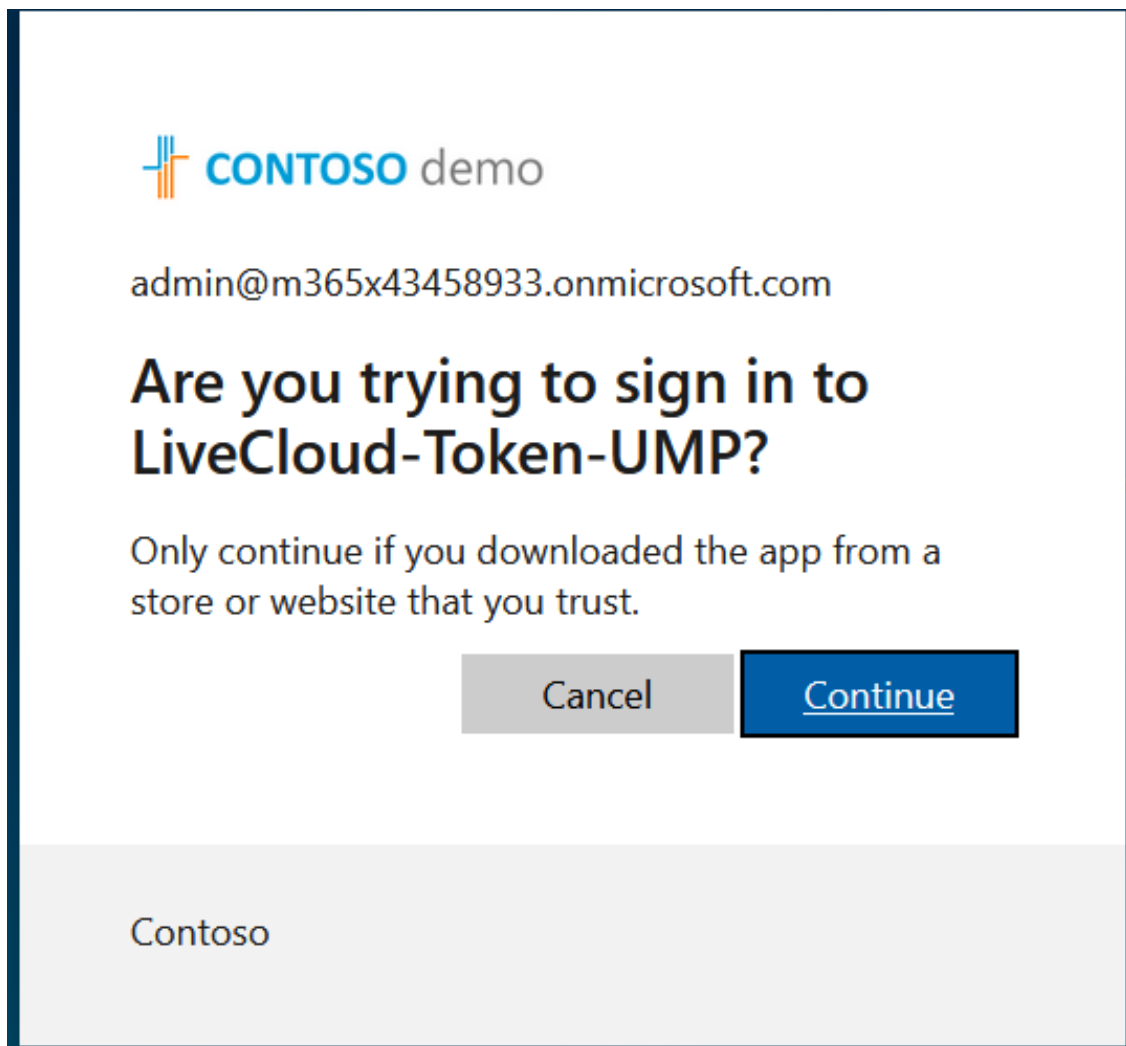
8. Copy the displayed code to clipboard.

9. Open the web browser link shown below the **Start authentication** button.

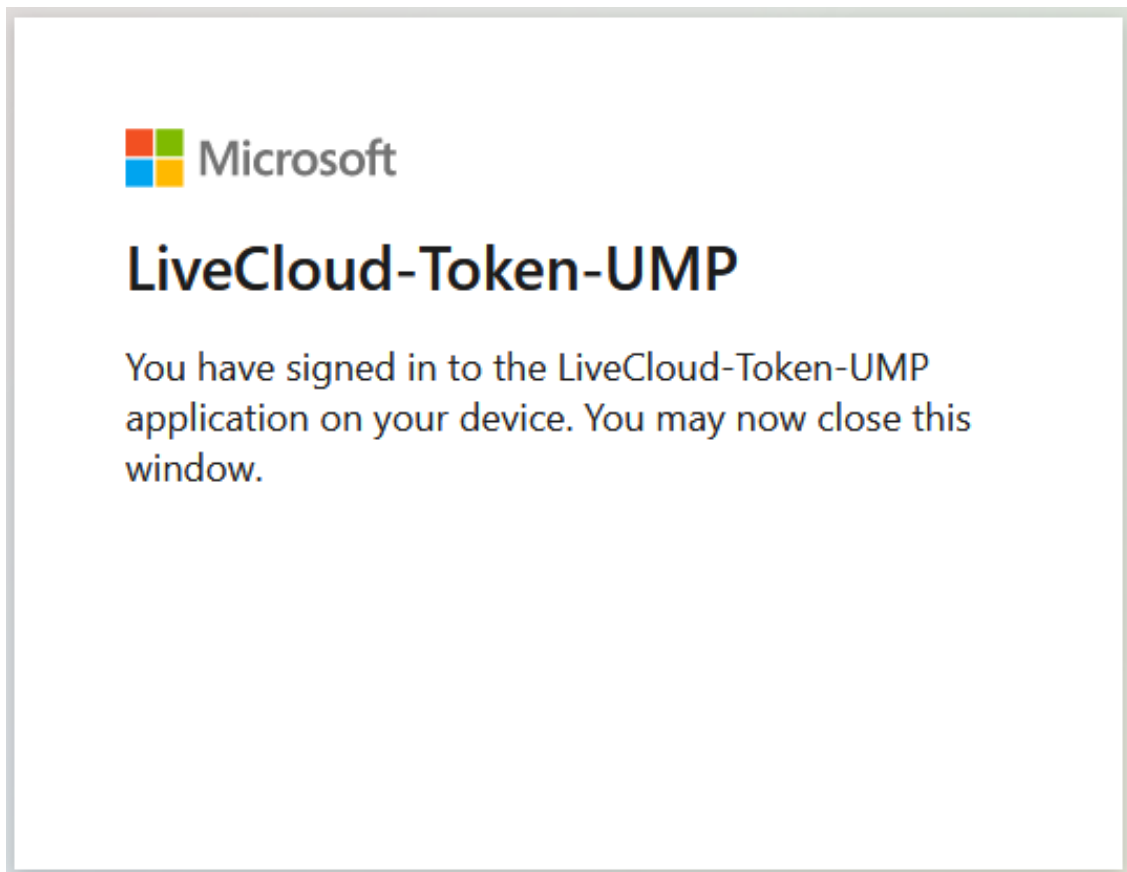




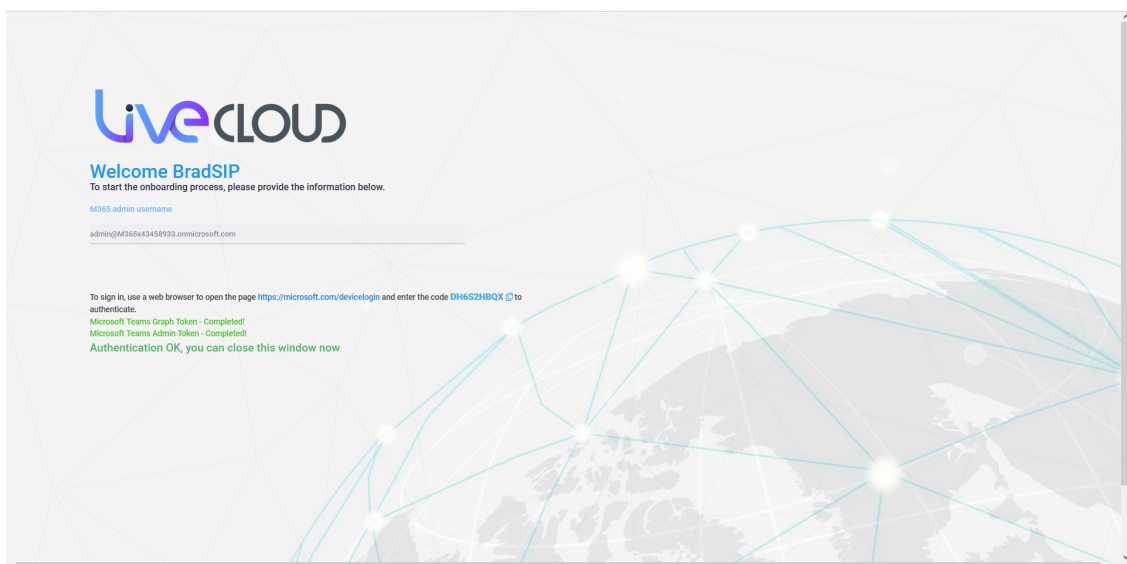
10. Choose the account of the customer tenant administrator with "Global" permissions.



11. Click **Continue**.



12. Close the above window. The confirmation of the completion of the authentication process is displayed.



13. Close the above window.
14. Return to the **Microsoft 365 Settings** screen. Note that "Authentication Status: Successful" is displayed and that the **Switch to user/pwd** button is displayed.

Microsoft 365 Settings

Last Authentication Status: Successful.

User Name
admin@M365x43458933.onmicrosoft.com

The customer is configured to use Authentication Token, password is not needed.

Validate Authentication

Save Microsoft 365 settings: **Switch to user/pwd**

QOE Integration with Microsoft Teams

Azure Application Id

Azure Application Password

Save QOE Integration settings

OnlineUser Filter

15. In the Main Tenant interface, open the Customer Invitations screen (see [Customer Invitations](#) on page 225, view the "Created at" and "Expires at" of the claimed token.

Customer Invitations

Reload data Edit

Search:

ID	Full Name	Invitation Email	M365 Admin Email	Email Sent	Email Invitation Sent Count	Created at	Expires at	Device Authenticated	Invitation Type	Tenant Installed
BradConnect	BradConnect	Brconnect@gmail.com		true	1	2023-04-24	2023-04-29		Invite	No
BradSIP	BradSIP	BradSIP@gmail.com	admin@M365x43458933.onmicrosoft.com	true	1	2023-04-24	2023-04-29	true	Request	No
BradTrunk2	BradTrunk2	BradTrunk2@gmail.com		true	1	2023-04-20	2023-04-25		Invite	No
SinhaCnslt	Ranjan Consulting	acenterprise.demo1@gmail.com	admin@M365x434560539.onmicrosoft.com	true	1	2023-04-19	2023-04-24	true	Invite	No

Updating Scripts


Use the script compare feature to verify that the template scenario scripts have the correct syntax notation (see [Scenario Scripts Templates Page](#) on page 213).



Template scripts containing incorrect syntax will not be executed.

Verifying Component Statuses

Verify the status of the components described in the table below.

Interface	Menu Navigation Path	Check	Configuration Action
Live Cloud/OVOC	Network > Device > Manage	<input type="checkbox"/>	Verify the UMP-365 Device Status is Active in the Devices table (see Device Status on page 162).
		<input type="checkbox"/>	Open the Managed Device page, select device , click Show and verify that “UMP Management” displays Connected (see Device Status on page 162).
Live Cloud Only	Open Device Page for UMP Tenant	<input type="checkbox"/>	Verify Customers Deployment State is Deployed . See Deployment Status.
		<input type="checkbox"/>	Verify for each customer that the SysAdminKit version is the latest version. See Upgrading Main UMP-365 Tenant on page 131.
UMP-365	System > License	<input type="checkbox"/>	Verify "MultiTenant Version: latest version. See Multitenant Portal Licensing on page 65.
		<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. See Configuring Invitation Settings on page 67.
	Security > Authentication Status	<input type="checkbox"/>	Verify that the Client ID and Secret ID are provided by the Synchronization app registration (check PMP site).
		<input type="checkbox"/>	Verify that the Redirect Url is set to: https://<UMP_FQDN>/authenticate/OAuth2Callback
			 Verify that the same redirect Uri is configured for the Synchronization App registration. See Authentication Status on page 228.

Interface	Menu Navigation Path	Check	Configuration Action
	SBC List	<input type="checkbox"/>	Verify that the SBC exists. See Managing SBC Devices on page 235.
Live Cloud Only	Network > Customers	<input type="checkbox"/>	Verify the Customers Status and Deployment status is OK in the Devices table. See Managing SBC Devices on page 235.
		<input type="checkbox"/>	Verify "Enabled" is checked.
		<input type="checkbox"/>	Verify the "total number of DIDs and "users count". See Customer Details Quick Glance.
		<input type="checkbox"/>	Verify that the Azure Tenant Id exists.
		<input type="checkbox"/>	Navigate to "Provider side" and verify the "Users Count" is displayed. See Customer Details Quick Glance.
	Customer Actions Menu > Edit Customer	<input type="checkbox"/>	<ul style="list-style-type: none"> ■ Edit User, update a parameter (e.g. Department) and then verify that the change has been implemented (see Manually Provisioning Users on page 443). ■ To enforce the Teams update, in the Multitenant interface, navigate to Queue Changes > Process All (see Monitoring M365 Replication Actions Queue on page 508). ■ To verify users, see User Details. ■ To verify users in Microsoft Teams: Open https://admin.Teams.microsoft.com
Multitenant portal	Site Locations	<input type="checkbox"/>	Verify that the SBC indicates "Deployed" status; click Add/Edit SBC Prefix (see Add SBC Site Locations on page 531).
		<input type="checkbox"/>	Verify that the DIDs are configured for the customer (see Download Dial Plan from Managed SBC (Import Customer) on

Interface	Menu Navigation Path	Check	Configuration Action
			page 240 and Manage SBC Prefixes on page 533).
		<input type="checkbox"/>	Add DID and verify that it has been successfully added on the SBC.

Device Status

Open the Device's page (**Devices > Manage**) to verify the status of the managed device.

The screenshot shows the 'DEVICE MANAGEMENT' page in the UMP-365 interface. The main table lists various devices, including 'q-ump-1c:trunkpack.c...' which is highlighted. The right sidebar shows the 'DEVICE DETAILS' for this device, including its name, status (Error), IP address, version, serial number, product type (User Management Pa...), HA status, tenant, region, and active alarms.





NAME	IP ADDRESS / FQDN	PRODUCT TYPE	HA	STATUS	QOE STATUS	CALLS	MAX CONCURRENT CALLS	QUALITY	SUCCESSFUL/FAILED	VERSION	MANAGEMENT
10.14.0.13-LTCeeeee...	10.14.0.13	Voice AI Solution	✗	●	●					5.5.0	
acRoPrivilege1		Generic Device	✗	●	●						
acRoPrivilege2		Generic Device	✗	●	●						
acRoPriv		Generic Device	✗	●	●						
acRoPriv2		Generic Device	✗	●	●						
acRoPriv3		Generic Device	✗	●	●						
Analog71335399		Generic Device	✗	●	●						
audc_at		Generic Device	✗	●	●						
audc_at1		Generic Device	✗	●	●						
audc_at2		Generic Device	✗	●	●						
audc_A22		Generic Device	✗	●	●						
audc_ik		Generic Device	✗	●	●						
BrufMAC		Generic Device	✗	●	●						
crfSpOper_atk2		Generic Device	✗	●	●						
dSpCall		Generic Device	✗	●	●						
DRSdApIP		Generic Device	✗	●	●						
GolanPro		Generic Device	✗	●	●						
GolanTest		Generic Device	✗	●	●						
GRWLKOKVNSOYL		Generic Device	✗	●	●						
GRWTAPQRHGYGR		Generic Device	✗	●	●						
oc1.customers.fmcuc...	oc1.customers.fmcuc...	SW SBC	✗	●	●					7.40A.250.754	
oc2.customers.fmcuc...	oc2.customers.fmcuc...	SW SBC	✗	●	●					7.40A.250.754	
q-ump-1c:trunkpack...	169.254.1.196	User Management Pa...	✗	●	●					8.0.450.101	
site10		Generic Device	✗	●	●						
site10		Generic Device	✗	●	●						

The screenshot shows the 'NETWORK SUMMARY' page in the UMP-365 interface. A detailed view of the device 'q-ump-1c:trunkpack.com [20.82.99.210]' is shown, including its IP address, version, serial number, product type, HA status, tenant, region, and active alarms. The right sidebar shows the 'NETWORK SUMMARY' with counts for devices, links, sites, endpoints, and active alarms.

NAME	IP ADDRESS / FQDN	PRODUCT TYPE	HA	STATUS	QOE STATUS	CALLS	MAX CONCURRENT CALLS	QUALITY	SUCCESSFUL/FAILED	VERSION	MANAGEMENT
q-ump-1c:trunkpack...	169.254.1.196	User Management Pa...	✗	●	●					8.0.450.101	

SUMMARY									
QA-UMP-TLC.TRUNKPACK.COM [20.82.99.210]									
Actions Edit Open Device Page									
DEVICE INFORMATION									
NAME	TENANT	STATUS	PRODUCT TYPE	VERSION					
qa-ump-tlc.trunkpac...	fmouc	OK	User Management P...	8.0.450.101					
REGION	AutoDetection	SAVE NEEDED	No	IP ADDRESS	169.254.1.201	SERIAL NUMBER	1407707651	RESET NEEDED	No
Management: OK • Cleared DEVICE ALARMS STATUS • Unlocked ADMINISTRATION STATUS • Connected CONNECTION STATUS					License: OK • Managed MANAGEMENT STATUS • Unmanaged (NO LICENSE STATUS)				

Table 24-1: UMP Device Status

Status	Topology Map	Device Management Page	Description
Error			Device status is Error when one or more of the following exist: <ul style="list-style-type: none"> Management status is Error (if device alarms status or connection status is disconnected) Voice quality status is Error (if control status or media status is Error, or if connection status is disconnected) License status is Error only if license pool is failed or expired
Warning			Device status is Warning when one or more of the following exists: <ul style="list-style-type: none"> Management status is Warning (if device alarms status or administration status is Warning) Voice quality status is Warning (if control status or media status or connection status is Warning) License status is









Status	Topology Map	Device Management Page	Description
			Warning (if a reset/apply action is required in the license pool or if there is no management license in the device or if there is no voice quality license)
OK			<p>Device status is OK when all of the following exists:</p> <ul style="list-style-type: none"> ■ Management status is OK - Clear or Undetermined (if device alarms status or connection status is OK - Clear or Undetermined) ■ Voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear or Undetermined) ■ License status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) <p>Strikethrough = locked No strikethrough = unlocked</p>

Table 24-2: SBC Device Status

Status	Topology Map	Device Management Page	Description
Error			Indicates an SBC belonging to AudioCodes communicating with the OVOC.

Status	Topology Map	Device Management Page	Description
			<p>Device status is Error when one or more of the following exist:</p> <ul style="list-style-type: none"> ■ Management status is Error (if device alarms status or connection status is disconnected) ■ Voice quality status is Error (if control status or media status is Error, or if connection status is disconnected) ■ License status is Error only if license pool is failed or expired
Warning			<p>Device status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> ■ Management status is Warning (if device alarms status or administration status is Warning) ■ Voice quality status is Warning (if control status or media status or connection status is Warning) ■ License status is Warning (if a reset/apply action is required in the license pool or if there is no management license in the device or if there is no voice quality license)

Status	Topology Map	Device Management Page	Description
OK			<p>Device status is OK when all of the following exists:</p> <ul style="list-style-type: none"> ■ Management status is OK - Clear or Undetermined (if device alarms status or connection status is OK - Clear or Undetermined) ■ Voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear or Undetermined) ■ License status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) Strikethrough = locked No strikethrough = unlocked

Updating SQL Server

In SQL Server Management Studio, navigate to the SysAdminTenant database, in Tables search for dbo.ApplicationSetting, and then in the 'ApiAllowedIps' row, add the OVOC Private or Public IP address manually (see [Networking](#) on page 51). For example ["169.254.0.1","10.201.80.4"]



The default WAN interface for the OVOC IP public address is 169.254.0.1

SBC Dialplan Verification

If the customer is assigned with a Hosted Essentials license, the SBC prefixes must be routed through the SBC Dial plans. The Dial plan prefixes should comply with the UMP-365 syntax rules i.e. +4455896552 ; +44587996[01-20]. Do not use any notations in the prefixes (e.g. x, n, z or #).

Part IV

Service Provider Management

25 Day Two Actions using the Multitenant Portal

The Multitenant portal can be used by Service Provider operators to perform the following Day Two actions:

- [Configuring Number of Licensed Users](#) on page 110
- [Configuring Global License Settings](#) below
- [Managing Onboarding Script Templates](#) on page 170
- [Managing Security Settings](#) on page 225
- [Managing SBC Devices](#) on page 235
- [Queued Tasks](#) on page 244
- [Managing Alarms](#) on page 63

Configuring Global License Settings

You can globally configure the following settings in the License page for customer deployments:

- Set Threshold to trigger UMP Customer License threshold alarm and a Grace interval to determine license exceed limits.
- Configure License Factors to determine whether these factors are used in the license calculation for customer billing (SysAdmn only).

➤ Do the following:

1. In the Multitenant Navigation pane, select **System > License**.

UMP Customer License Settings

Warning Limit (%)
90

Grace Interval (%)
10

Apply license settings

License Factors [Global]:

- ☒ Managed Users - By Template
- ☒ Managed Users - By User Interface
- ☒ Managed Service Numbers

2. Configure the following UMP Customer License Settings:
 - **Warning Limit:** Defines the percentage threshold for the number of globally licensed users for all customers on the managed UMP deployment. When the threshold is reached, a warning alarm is raised (User License Threshold alarm). For example, if there are 10,000 allocated licensed users on the deployment instance (as shown in the figure above) then the alarm is raised when 9,000 users are reached. The user is calculated as

licensed if a feature has been configured for a specific user. For example, "Enterprise Voice" has been enabled for the user.

- Grace Interval:** Defines the percentage number of user licenses remaining active for a limited time period when the total number of allocated licenses has expired. The amount of allocated temporary licenses is calculated as percentage of the total license allocation. For example, if there are 10,000 allocated user licenses on the deployment instance and the Grace time is set to 10% then 1000 temporary licenses are allocated.
3. **Configure License Factors (Global):** This configuration determines the default settings in the Customer UMP License screen. You can then either use the default settings or override the by applying local settings for the customer (see [Managing User Licenses](#) on page 540)



Configuration of these options is only available for SysAdmin.

License Factor	Description	Priority																																																																		
Managed Users-By Template	<p>Total number of users assigned to M365 templates (see Managing Templates on page 459).</p> <table><tr><th>User Type</th><th>Full Name</th><th>SIP Address</th><th>Line Uri</th><th>Template</th><th>Department</th></tr><tr><td>TeamsOnly</td><td>Alex Wilber</td><td>sip:alexw@m365x...</td><td>tel:+97239776655</td><td>Testing</td><td>Marketing</td></tr></table>	User Type	Full Name	SIP Address	Line Uri	Template	Department	TeamsOnly	Alex Wilber	sip:alexw@m365x...	tel:+97239776655	Testing	Marketing	3																																																						
User Type	Full Name	SIP Address	Line Uri	Template	Department																																																															
TeamsOnly	Alex Wilber	sip:alexw@m365x...	tel:+97239776655	Testing	Marketing																																																															
Managed Users-By User Interface	<p>Total number of users with User properties updated using this interface (see Manually Provisioning Users on page 443).</p> <table><tr><th>User Type</th><th>Full Name</th><th>SIP Address</th><th>Line Uri</th><th>Template</th><th>Department</th><th>Online Voice R.</th><th>Online PSTN C.</th><th>Site Location</th><th>Usage Location</th><th>Enterprise...</th></tr><tr><td>TeamsOnly</td><td>Alex Wilber</td><td>sip:alexw@m365x...</td><td>tel:+97239776655</td><td>Testing</td><td>Marketing</td><td>Unconnected</td><td></td><td></td><td>IL</td><td>Yes</td></tr><tr><td>TeamsOnly</td><td>Christie Cline</td><td>sip:christac@m365x...</td><td>tel:+97239776655</td><td>Testing</td><td>Sales</td><td>Unconnected</td><td></td><td></td><td>IL</td><td>Yes</td></tr><tr><td>TeamsOnly</td><td>Nector Wilke</td><td>sip:nectorw@m365x...</td><td>tel:+97239776655</td><td>Operations</td><td>Unconnected</td><td></td><td></td><td></td><td>IL</td><td>Yes</td></tr><tr><td>TeamsOnly</td><td>Ump Activation User</td><td>sip:ump-act@m365x...</td><td></td><td></td><td></td><td>Unconnected</td><td></td><td></td><td>BE</td><td>No</td></tr><tr><td>TeamsOnly</td><td>Pauli Fernandez</td><td>sip:paulif@m365x...</td><td></td><td>Executive Manage</td><td>Unconnected</td><td></td><td></td><td></td><td>IL</td><td>Yes</td></tr></table>	User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voice R.	Online PSTN C.	Site Location	Usage Location	Enterprise...	TeamsOnly	Alex Wilber	sip:alexw@m365x...	tel:+97239776655	Testing	Marketing	Unconnected			IL	Yes	TeamsOnly	Christie Cline	sip:christac@m365x...	tel:+97239776655	Testing	Sales	Unconnected			IL	Yes	TeamsOnly	Nector Wilke	sip:nectorw@m365x...	tel:+97239776655	Operations	Unconnected				IL	Yes	TeamsOnly	Ump Activation User	sip:ump-act@m365x...				Unconnected			BE	No	TeamsOnly	Pauli Fernandez	sip:paulif@m365x...		Executive Manage	Unconnected				IL	Yes	4
User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voice R.	Online PSTN C.	Site Location	Usage Location	Enterprise...																																																										
TeamsOnly	Alex Wilber	sip:alexw@m365x...	tel:+97239776655	Testing	Marketing	Unconnected			IL	Yes																																																										
TeamsOnly	Christie Cline	sip:christac@m365x...	tel:+97239776655	Testing	Sales	Unconnected			IL	Yes																																																										
TeamsOnly	Nector Wilke	sip:nectorw@m365x...	tel:+97239776655	Operations	Unconnected				IL	Yes																																																										
TeamsOnly	Ump Activation User	sip:ump-act@m365x...				Unconnected			BE	No																																																										
TeamsOnly	Pauli Fernandez	sip:paulif@m365x...		Executive Manage	Unconnected				IL	Yes																																																										
Managed Service Numbers	<p>Total number of users configured with numbers that are tagged to a PSTN Gateway that is different to the PSTN gateway that is associated with the Site Location SBC. These numbers may be typically Service numbers such as those configured for Fax IVR or Emergency numbers. In the example below, the tag BradTest is mapped to the 911 prefix, however, the actual tag of the PSTN Gateway for the site location is 'BradTokenTest.oc1.sandbox2.audiocodes.be'.</p> <table><tr><th>Ext Plan Name</th><th>Prefix</th><th>Tag</th></tr><tr><td>ConfDialPlan</td><td>911</td><td>BradTest</td></tr><tr><td>ConfDialPlan</td><td>+9723990011</td><td>BradTokenTest.oc1.sandbox2.audiocodes.be</td></tr></table> <table><tr><th>Site</th><th>SBC Name</th><th>Configuration</th><th>PSTN Gateway</th><th>Site Deployment State</th><th>MSIS Deployment State</th><th>Notes</th><th>Actions</th></tr><tr><td>BradService1</td><td>oc1.sandbox2.audiocodes.be [20.102.31.206]</td><td>SipTrunk</td><td>BradTokenTest.oc1.sandbox2.audiocodes.be</td><td>Deployed</td><td>Error</td><td>Pending commands: 0</td><td>Uninstall Manage Sbc Profiles</td></tr></table>	Ext Plan Name	Prefix	Tag	ConfDialPlan	911	BradTest	ConfDialPlan	+9723990011	BradTokenTest.oc1.sandbox2.audiocodes.be	Site	SBC Name	Configuration	PSTN Gateway	Site Deployment State	MSIS Deployment State	Notes	Actions	BradService1	oc1.sandbox2.audiocodes.be [20.102.31.206]	SipTrunk	BradTokenTest.oc1.sandbox2.audiocodes.be	Deployed	Error	Pending commands: 0	Uninstall Manage Sbc Profiles																																										
Ext Plan Name	Prefix	Tag																																																																		
ConfDialPlan	911	BradTest																																																																		
ConfDialPlan	+9723990011	BradTokenTest.oc1.sandbox2.audiocodes.be																																																																		
Site	SBC Name	Configuration	PSTN Gateway	Site Deployment State	MSIS Deployment State	Notes	Actions																																																													
BradService1	oc1.sandbox2.audiocodes.be [20.102.31.206]	SipTrunk	BradTokenTest.oc1.sandbox2.audiocodes.be	Deployed	Error	Pending commands: 0	Uninstall Manage Sbc Profiles																																																													

Managing 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.



Before Onboarding new customers, SBC device CLI script files should be pre-configured according to M365 tenant site requirements.



Warning: Editing the script, can damage the onboarding process and the SBC configuration.

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 [Customer Variables](#) on page 210)

SBC Direct Routing Scripts

The following table describes the template scenario scripts that are provided for Direct Routing functionality in User Management Pack™ 365 SP Edition. These scripts are saved in the SQL database in the **dbo.SbcScriptTemplate** file.



For reference to SBC Direct Routing configuration, see [Configuring Microsoft Teams Direct Routing SBC](#) on page 86.

ID	Scenario Script	Type	Description	Related To	Custom er Variabl es	Referen ce
7	sbc-scenario7script	SbcOnboarding (1)	Adds the basic SBC configuration.	sbc-scenario7Cleanup	-	sbc-scenario7 on the next page
100	sbc-add-prefix	Background processing only (the functionality performed by this script cannot be customized).	Adds dial plan prefix when the provider side is configured as either an IP-PBX or a SIP Trunk.	sbc-remove-prefix	-	sbc-add-prefix on page 179
700	sbc-scenario7cleanup	SbcCleanup (2)	Removes the basic SBC configuration.	sbc-scenario7	-	sbc-scenario7 Cleanup on page 184
101	sbc-remove-prefix	Background processing only (the functionality performed by this script cannot be customized).	Removes prefixes to dial plan when the	sbc-add-prefix	-	sbc-remove-prefix on page 19

ID	Scenario Script	Type	Description	Related To	Custom er Variabl es	Referen ce
		y performed by this script cannot be customized).	provider side is configured as either an IP-PBX or a SIP Trunk.			0
103	add-ipx-user	Background processing only (the functionality performed by this script cannot be customized).	Adds an IP-PBX registered user when provider side is configured as an IP-PBX.	-	-	add-ipx-user on page 185

sbc-scenario7

The **sbc-scenario7** script is triggered during the Onboarding wizard. It applies the following configuration on the SBC device that is configured to connect calls to the customer site location:

- Configures a new IP Group for the Carrier leg for each new site location (indicated on SBC by <name>-c):
 - Configures customer name based on the Customer Short Name.
 - Configures a new Proxy Set and IP Profile based on the Carrier value configured in the Onboarding wizard. For example, Proxy_Set, SIP Trunk.
 - Configures 'Tags' parameter in IP Group based on the customer sub domain name. For example 'Trunk=BradDRService.sandbox2.audiocodes.be'.
 - Disables classification by Proxy Set.
 - Applies Call Setup Rules Set ID 1 for Carrier IP Group (see details in table below).
- Configures a new IP Group for the Teams leg for each new site location (indicated on SBC by <name>-t):
 - Configures customer name based on the Customer Short Name.

- Configures a new Proxy Set 'Teams' and new IP Profile 'Teams'
 - Configures 'Local Host Name' based on the customer sub domain name. For example, 'BradDRService.sandbox2.audiocodes.be'.
 - Enables 'Always Use Src Address' which enables the device to always send SIP requests and responses, within a SIP dialog, to the source IP address received in the previous SIP message packet.
 - Configures 'Tags' parameter in IP Group based on the customer sub domain name. For example 'Tenant=BradDRService.sandbox2.audiocodes.be'
 - Disables Classification by Proxy Set.
 - Applies the Call Setup Rules Set ID **0** for Teams IP Group (see details in table below).
- If CAC is enabled in the Onboarding wizard, configures the selected CAC Profile and enables CAC.
- If Carrier registration is enabled in the Onboarding wizard, a SIP Registration account is configured on the SBC with the following (wizard configured parameters are indicated in parenthesis):
- account-name (Customer ShortName)
 - served-ip-group-name (Teams IP Group Name)
 - serving-ip-group-name (Carrier IP Group Name)
 - user-name (Carrier User Name)
 - password (Carrier Password)
 - host-name (Carrier Host Name)
 - contact-user (Carrier Main Line)

The table below summarizes the Call Setup Rules called by this script.

Index	Rules Set ID	Name	Request Type	Request Target	Request Key	Condition	Action Subject	Action Type	Action Value
1	0	-	Dial Plan	CustDialPlan	Param.Call.Src.User	DialPlan.Found exists	DstTags.Trunk	Modify	DialPlan.Result
2	0	-	Dial Plan	CustDialPlan	Header.P-Asserted-Identity.URL.User	DialPlan.Found exists	DstTags.Trunk	Modify	DialPlan.Result

Index	Rules Set ID	Name	Request Type	Request Target	Request Key	Condition	Action Subject	Action Type	Action Value
3	0	-	None	-	-	var.session.0 == "	var.session.0	Modify	Param.IPG.Src.Tags.Tenant
4	0	-	None	-	-	-	SrcTags.Source	Modify	'Teams'
5	1	-	Dial Plan	CustDialPlan	Param.Call.Dst.User	var.session.0 == "	var.session.0	Modify	DialPlan.Result
6	1	-	-			var.session.0 != "	DstTags.Tenant	Modify	Var.Session.0
7	1	-	None	-	-	-	SrcTags.Source	Modify	'SIPTrunk'

```
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:

```
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
```

```
sbcdial-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
```

sbc-add-prefix

The **sbc-add-prefix** is triggered when adding new phone numbers in the Customer portal (see [Manage SBC Prefixes](#) on page 533). The script adds new phone prefixes to the Dial Plan configured on the SBC device which corresponds to the matching Online PSTN gateway tag for the customer sub domain.

```
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
```

The script parameters are described in the table below.

Parameter	Description
DialPlanName	<p>The name of the dial plan configured on the SBC to which the numbers are uploaded.</p> <p>By default, when numbers are added in the Customer portal:</p> <ul style="list-style-type: none"> ■ For OC Essential customers, numbers are uploaded to OCDialplan. ■ For OC Pro customers, numbers are uploaded to CustDialPlan.
Name	The Short Name of the customer to whom the numbers are configured.
Prefix	The list of phone numbers to upload.
Tag	The Online PSTN gateway customer sub domain.

For example in the following figure, 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. CustDialPlan and RegisteredUsers are default dial plans and 'Teams' is as custom dial plan.

LifeCycle Management

Manage Templates

Online Voice Routing

Unassigned Number Range

Reserved Numbers

Audit

Queued Changes

M365 Configuration

Site Locations

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.

Search...

Delete

UndoDelete

Drag a column header and drop it here to group by that column

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

10

data items per page

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
```

sbc-scenario7 Cleanup

The **sbc-scenario7Cleanup** script does the following:

- Removes IP Group for both the Carrier and Teams legs that matches the Customer Id..
- 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
```

add-ipx-user

The **add-ipx-user** script is triggered during the Onboarding wizard. It applies the following configuration on the SBC device that is configured to connect calls to the customer site location:

- Configures a new dial plan rule in both the CustDialPlan and in the RegisteredUsers Dial Plan with the extension of the PBX user and assigns the tag of the Online PSTN Gateway sub domain.
- Configures a registered IP-PBX user and extensions to specific site location and configures connection to specific SBC.
- Configures SBC User Information for registering a user to an external registrar server If the device registers on behalf of users and the users don't perform registration:
 - Local User value which is the user name with the appended name of the IP-PBX host.
 - IP-PBX Username
 - IP-PBX User Password
 - Associates an IP-Group Teams leg, any SIP request destined to the user is routed to the Proxy Set associated with this IP Group.

```
# Registration of new PBX extensions
```

```
# GUIDELINES for the CSV file uploaded in UMP to add PBX extensions to this tenant
```

```
# the field "LocalUserName" should have the extension e.g. 2345
```

```
# the field "PbxExtension" should also have that syntax. e.g. 4002
```

```
# the field "OnlineVoiceRoutingPolicy" should have the PBX SIP domain. e.g. ac3cx.elastix.com or the IP address used by the PBX in the from header for calls towards an extension
```

```
configure voip
```

```
# Create
```

```
# if create has a value then the below will run
```



```
# leave the value empty to ignore this section
```

```
{{#if PbxUser.create}}
```

```
sbc dial-plan where name "CustDialPlan"
```

```
dial-plan-rule new
```

```
name "{{SBC.SbcSiteName}}"
```

```
prefix "{{sbcEscape PbxUser.LocalUserName}}\{{sbcEscape PbxUser.Pbxhost}}"
```

```
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}}.{{PbxUser.Pbxhost}}"
```

```
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.LocalUserName}}.{{PbxUser.Pbxhost}}"
```

```
activate
```

```
exit
```

```
dial-plan-rule new
```

```
name "{{SBC.SbcSiteName}}"
```

```
prefix "{{sbcEscape PbxUser.LocalUserName}}\{{sbcEscape  
PbxUser.Pbxhost}}"
```

```
tag "{{PbxUser.LocalUserName}}.{{PbxUser.Pbxhost}}"
```

```
activate
```

```
exit
```

```
dial-plan-rule new
```

```
name "{{SBC.SbcSiteName}}"
```

```
prefix "pb{{sbcEscape PbxUser.LocalUserName}}\{{sbcEscape  
PbxUser.Pbxhost}}"
```

```
tag "{{PbxUser.E164}}"
```

```
activate
```

```
exit
```

```
exit
```

```
{{/if }}
```

```
#Delete
```

```
# if delete has a value then the below will run
```

```
# leave the value empty to ignore this section
```

```
{{#if PbxUser.delete}}
```

```
sbc dial-plan where name "CustDialPlan"
```

```
no dial-plan-rule where prefix "{{sbcEscape PbxUser.LocalUserName}}\  
{{sbcEscape PbxUser.Pbxhost}}"
```

```
no dial-plan-rule where prefix "+{{sbcEscape PbxUser.E164}}"
```

```
exit
```

```
sip-definition proxy-and-registration
```

```
no user-info sbc-user-info where local-user "{{PbxUser.LocalUserName}}".
{{PbxUser.Pbxhost}}"
```

```
exit
```

```
sbc dial-plan where name "RegisteredUsers"
```

```
no dial-plan-rule where prefix "+{{sbcEscape PbxUser.E164}}"
```

```
no dial-plan-rule where prefix "{{sbcEscape PbxUser.LocalUserName}}\.".
{{sbcEscape PbxUser.Pbxhost}}"
```

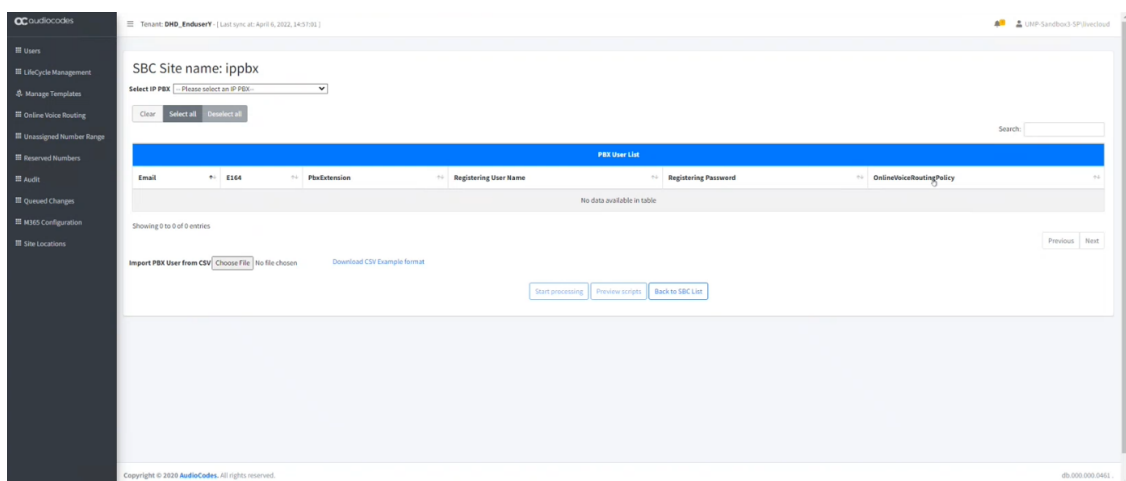
```
no dial-plan-rule where prefix "pb{{sbcEscape PbxUser.LocalUserName}}\.".
{{sbcEscape PbxUser.Pbxhost}}"
```

```
exit
```

```
{{/if }}
```

```
do write
```

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



sbcr-remove-prefix

The **sbcr-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
```

M365 Template Scenarios

The default M365 Onboarding scripts M365 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).

ID	Scenario Script	Description	Script Type	Customer Variables
5461210	Default M365 Onboarding script.	Default M365 Onboarding script.	M365Onboarding (3)	Default M365 Tenant Onboarding Script on the next page
5461211	Default M365 Cleanup.	Default M365 Onboarding cleanup script.	M365Cleanup (4)	Default M365 Tenant Cleanup Script

ID	Scenario Script	Description	Script Type	Customer Variables
				on page 193
5461212	Default M365 Location-based Routing script.	Default script for onboarding M365 Location-based routing customers.	M365Onboarding (3)  This value is disabled by default. Manually set to 3 for enabling the Location-based routing feature.	M365 Onboarding with Location-based Routing on page 194
5461213	M365 onboarding with LBR and custom networks.	Custom script for configuring Location-based routing.	M365Onboarding (3)  This value is disabled by default. Manually set to 3 for enabling the Location-based routing feature.	M365 onboarding with Location-Based Routing and Custom Networks on page 201

Default M365 Tenant Onboarding Script

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

```
# Add PSTN Usage record Unrestricted if not exists
```

```
if(Get-CsOnlinePstnUsage | Where-Object Usage -  
NotContains "Unrestricted")
```

```

{

    Set-CsOnlinePstnUsage -Identity Global -Usage @
{Add="Unrestricted"};

}

# Add Online Voice Route Unrestricted if not exists, else add
additional PSTN Gateway to the OnlinePstnGatewayList if there is a new PSTN
Gateway

if(Get-CsOnlineVoiceRoute | Where-Object {$_.Identity -
eq "Unrestricted"})

{

    Write-host "The CsOnlineVoiceRoute named Unrestricted
already exists."

    if(Get-CsOnlineVoiceRoute -Identity "Unrestricted" | Where-
Object {$_.OnlinePstnGatewayList -NotContains ""})

    {

        Write-host "A new PSTN Gateway is added to the the
OnlinePstnGatewayList."

        Set-CsOnlineVoiceRoute -Identity "Unrestricted" -
OnlinePstnGatewayList @{add=""}

    }

}else {

    Write-host "The CsOnlineVoiceRoute named Unrestricted does
not exist, creating one."

    New-CsOnlineVoiceRoute -Identity "Unrestricted" -
NumberPattern ".*" -OnlinePstnGatewayList @{add=""} -Priority 1 -
OnlinePstnUsages @{add="Unrestricted"};

```

```
}  
  
  
  
# Add Voice Routing Policy Unrestricted if not exists  
  
  
if(Get-CsOnlineVoiceRoutingPolicy | Where-Object {$_.Identity -  
like "Tag:Unrestricted"})  
  
{  
  
    continue  
  
}else {  
  
    New-CsOnlineVoiceRoutingPolicy -Identity "Unrestricted" -  
OnlinePstnUsages "Unrestricted";  
  
}  
  
  
# End of M365 onboarding script  
  
;
```



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

Default M365 Tenant Cleanup Script

The default M365 Tenant Cleanup script is shown below.



This script is hard-coded and is not included in the SQL database.


```
# Begin of Microsoft cleanup script
```

```
# Remove the PSTN Gateway from the CsOnlineVoiceRoutes
```

```
Get-CsOnlineVoiceRoute | Where-Object {$_.OnlinePstnGatewayList -like "  
{{SBC.OnlinePstnGateway}}"} | ForEach-Object {Set-CsOnlineVoiceRoute -  
Identity $_.Identity -OnlinePstnGatewayList @{remove="  
{{SBC.OnlinePstnGateway}}"}}
```

```
#Remove CsOnlineVoiceRoutes when OnlinePstnGatewayList is empty
```

```
Get-CsOnlineVoiceRoute | Where-Object {$_.OnlinePstnGatewayList.count -eq 0}  
| Remove-CsOnlineVoiceRoute
```

```
# End of M365 cleanup script;
```



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

M365 Onboarding with Location-based Routing

The M365 Location-based Routing script is shown below. Variables highlighted in orange should be changed according to customer deployment.

```
# Begin of Microsoft onboarding script
```

```
# Addition for Location based routing
```

```
# Script variables
```

```
[String]$OnlinePstnGateway="{{SBC.OnlinePstnGateway}}"
```

```
[String]$CustomerId="{{SBC.SbcSiteName}}"
```

```
# PSTN Gateway Variables
```

```
[Int]$SipSignalingPort=5061
```

```
[Int]$MaxConcurrentSessions=100
```

```
# Add Network region if not exists
```

```
if(Get-CsTenantNetworkRegion | Where-Object {$_.Identity -  
eq "India"})
```

```
{
```

```
continue
```

```
}else {
```

```
New-CsTenantNetworkRegion -NetworkRegionID "India";
```

```
}

# Add Network Site if not exists

if(Get-CsTenantNetworkSite | Where-Object {$_.Identity -like "{{SBC.SbcSiteName}}"})

{

    continue

}

else {

    New-CsTenantNetworkSite -NetworkSiteID "{{SBC.SbcSiteName}}" -NetworkRegionID "India" -EnableLocationBasedRouting $true -Description "Default Site created by AudioCodes LiveCloud";

}

# Add example subnet to the network site

if(Get-CsTenantNetworkSubnet | Where-Object {$_.Identity -like "169.254.0.0"})

{

    continue

}

else {

    New-CsTenantNetworkSubnet -SubnetID "169.254.0.0" -MaskBits "16" -NetworkSiteID "{{SBC.SbcSiteName}}" -Description "Example subnet set by AudioCodes LiveCloud";
```

```
}

# Add example trusted IP address

if(Get-CsTenantTrustedIPAddress | Where-Object {$_.Identity -
like "169.254.0.1"})

{

    continue

}else {

    New-CsTenantTrustedIPAddress -IPAddress 169.254.0.1 -
MaskBits 32 -Description "Example Trusted IP Address set by AudioCodes
LiveCloud";

}

# Add OnlinePSTNGateway

if(Get-CsOnlinePSTNGateway | Where-Object {$_.Identity -like "
{{SBC.OnlinePstnGateway}}"})

{

    continue

}else {

# The line below might require customization based on the
```

customer needs, like a change in the SipSignalingPort or attributes needs to be added like MaxConcurrentSessions

```
New-CsOnlinePstnGateway -Fqdn "{{SBC.OnlinePstnGateway}}" -Enabled $true -SipSignalingPort
$SipSignalingPort -ForwardCallHistory $True -ForwardPai $True -MediaBypass
$True -MaxConcurrentSessions $MaxConcurrentSessions -GatewaySiteLbrEnabled
$true -GatewaySiteID "{{SBC.SbcSiteName}}";
```

```
}
```

```
# Create CallingPolicy named UMPPreventTollBypass
```

```
if(Get-CsTeamsCallingPolicy | Where-Object {$_.Identity -
like "Tag:UMPPreventTollBypass"})
```

```
{
```

```
continue
```

```
}else {
```

```
New-CsTeamsCallingPolicy -Identity
"UMPPreventTollBypass" -AllowCallForwardingToPhone $True -Description "Allow
Teams calling, preventing toll bypass" -PreventTollBypass $True;
```

```
}
```

```
# End addition for Location based routing
```

```

# From original onboarding script

# Add PSTN Usage record Unrestricted if not exists

if(Get-CsOnlinePstnUsage | Where-Object Usage -
NotContains "Unrestricted")

{

    Set-CsOnlinePstnUsage -Identity Global -Usage @
{Add="Unrestricted"};

}

# Add Online Voice Route Unrestricted if not exists, else add
additional PSTN Gateway to the OnlinePstnGatewayList if there is a new PSTN
Gateway

if(Get-CsOnlineVoiceRoute | Where-Object {$_.Identity -
eq "Unrestricted"})

{

    Write-host "The CsOnlineVoiceRoute named Unrestricted
already exists."

    if(Get-CsOnlineVoiceRoute -Identity "Unrestricted" |
Where-Object {$_.OnlinePstnGatewayList -NotContains "
{{SBC.OnlinePstnGateway}}"})

    {

        Write-host "A new PSTN Gateway is added to the the
OnlinePstnGatewayList."
    }
}

```

```

        Set-CsOnlineVoiceRoute -Identity "Unrestricted" -
OnlinePstnGatewayList @{add="{{SBC.OnlinePstnGateway}}"}

    }

}

}else {

    Write-host "The CsOnlineVoiceRoute named Unrestricted
does not exist, creating one."

    New-CsOnlineVoiceRoute -Identity "Unrestricted" -
NumberPattern ".*" -OnlinePstnGatewayList @{add="{{SBC.OnlinePstnGateway}}"}
-Priority 1 -OnlinePstnUsages @{add="Unrestricted"};

}

}

}

}

}

# Add Voice Routing Policy Unrestricted if not exists

if(Get-CsOnlineVoiceRoutingPolicy | Where-Object {$_.Identity -
like "Tag:Unrestricted"})

{

    continue

}

}else {

    New-CsOnlineVoiceRoutingPolicy -Identity "Unrestricted"
-OnlinePstnUsages "Unrestricted";

}

}

}

}

}

# End of M365 onboarding script

```

```
;
```

M365 onboarding with Location-Based Routing and Custom Networks

The **M365 onboarding with LBR and Custom Networks** is shown below. Variables highlighted in orange should be changed according to customer deployment. The custom script arguments used in this script are:

- IP-Network
- IP-SubnetBits
- Trusted-IP-Network
- Trusted-IP-SubnetBits

bypass

```
# Begin of Microsoft onboarding script
```

```
# Addition for Location based routing
```

```
# Script variables
```

```
[String]$OnlinePstnGateway="{{SBC.OnlinePstnGateway}}"
```

```
[String]$CustomerId="{{SBC.SbcSiteName}}"
```

```
[String]$IPNetwork="{{CustomVar.IP-Network}}"
```

```
[String]$IPSubnet="{{CustomVar.IP-SubnetBits}}"
```

```
[String]$TrustedIPNetwork="{{CustomVar.Trusted-IP-Network}}"
```



```
[String]$TrustedIPSubnet="{CustomVar.Trusted-IP-SubnetBits}"

# PSTN Gateway Variables

[Int]$SipSignalingPort=5061

[Int]$MaxConcurrentSessions=100

# Add Network region if not exists

if(Get-CsTenantNetworkRegion | Where-Object {$_.Identity -eq "India"})
{
    continue
}
else {
    New-CsTenantNetworkRegion -NetworkRegionID "India";
}

# Add Network Site if not exists

if(Get-CsTenantNetworkSite | Where-Object {$_.Identity -like "{SBC.SbcSiteName}"})
```

```

{

    continue

}else {

    New-CsTenantNetworkSite -NetworkSiteID "
    {{SBC.SbcSiteName}}" -NetworkRegionID "India" -EnableLocationBasedRouting
    $true -Description "Default Site created by AudioCodes LiveCloud";

}

# Add example subnet to the network site

if(Get-CsTenantNetworkSubnet | Where-Object {$_.Identity -like "
    {{CustomVar.IP-Network}}"})
{

    continue

}else {

    New-CsTenantNetworkSubnet -SubnetID "{{CustomVar.IP-
    Network}}" -MaskBits "{{CustomVar.IP-SubnetBits}}" -NetworkSiteID "
    {{SBC.SbcSiteName}}" -Description "Subnet set by AudioCodes LiveCloud";

}

# Add example trusted IP address

if(Get-CsTenantTrustedIPAddress | Where-Object {$_.Identity -
    like "{{CustomVar.Trusted-IP-Network}}"})

```

```

{
    continue
}
else {
    New-CsTenantTrustedIPAddress -IPAddress "
    {{CustomVar.Trusted-IP-Network}}" -MaskBits "{{CustomVar.Trusted-IP-
    SubnetBits}}" -Description "Trusted IP Address set by AudioCodes LiveCloud";
}

# Add OnlinePSTNGateway

if(Get-CsOnlinePSTNGateway | Where-Object {$_.Identity -like "
    {{SBC.OfflinePstnGateway}}")
{
    continue
}
else {
    # The line below might require customization based on the
    customer needs, like a change in the SipSignalingPort or attributes needs to
    be added like MaxConcurrentSessions

    New-CsOnlinePstnGateway -Fqdn "
    {{SBC.OfflinePstnGateway}}" -Enabled $true -SipSignalingPort
    $SipSignalingPort -ForwardCallHistory $True -ForwardPai $True -MediaBypass
    $True -MaxConcurrentSessions $MaxConcurrentSessions -GatewaySiteLbrEnabled
    $true -GatewaySiteID "{{SBC.SbcSiteName}}" ;
}

```

```
# Create CallingPolicy named UMPPreventTollBypass

    if(Get-CsTeamsCallingPolicy | Where-Object {$_.Identity -
like "Tag:UMPPreventTollBypass"})

    {

        continue

    }else {

        New-CsTeamsCallingPolicy -Identity
"UMPPreventTollBypass" -AllowCallForwardingToPhone $True -Description "Allow
Teams calling, preventing toll bypass" -PreventTollBypass $True;

    }

# End addition for Location based routing


# From original onboarding script


# Add PSTN Usage record Unrestricted if not exists

    if(Get-CsOnlinePstnUsage | Where-Object Usage -
NotContains "Unrestricted")
```

```

{

    Set-CsOnlinePstnUsage -Identity Global -Usage @
{Add="Unrestricted"};

}

# Add Online Voice Route Unrestricted if not exists, else add
additional PSTN Gateway to the OnlinePstnGatewayList if there is a new PSTN
Gateway

if(Get-CsOnlineVoiceRoute | Where-Object {$_.Identity -
eq "Unrestricted"})

{

    Write-host "The CsOnlineVoiceRoute named Unrestricted
already exists."

    if(Get-CsOnlineVoiceRoute -Identity "Unrestricted" |
Where-Object {$_.OnlinePstnGatewayList -NotContains "
{{SBC.OnlinePstnGateway}}"})

    {

        Write-host "A new PSTN Gateway is added to the the
OnlinePstnGatewayList."

        Set-CsOnlineVoiceRoute -Identity "Unrestricted" -
OnlinePstnGatewayList @{add="{{SBC.OnlinePstnGateway}}"}

    }

}

}else {

    Write-host "The CsOnlineVoiceRoute named Unrestricted
does not exist, creating one."

    New-CsOnlineVoiceRoute -Identity "Unrestricted" -
NumberPattern ".*" -OnlinePstnGatewayList @{add="{{SBC.OnlinePstnGateway}}"}

```

```
-Priority 1 -OnlinePstnUsages @{add="Unrestricted"};

}

# Add Voice Routing Policy Unrestricted if not exists

if(Get-CsOnlineVoiceRoutingPolicy | Where-Object {$_.Identity -
like "Tag:Unrestricted"})
{
    continue
}
else {
    New-CsOnlineVoiceRoutingPolicy -Identity "Unrestricted"
-OnlinePstnUsages "Unrestricted";
}

# End of M365 onboarding script

;
```

When this script is selected in the Onboarding wizard, the Customer Variables pane opens.

1 M365 Tenant
2 M365
3 Voice Route
×

☒ **Configure M365 default routing**

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

Online PSTN Gateway

M365 Onboarding Script

M365 Cleanup Script

Customer Variables	Value
IP-Network	<input type="text"/>
IP-SubnetBits	<input type="text"/>
Trusted-IP-Network	<input type="text"/>
Trusted-IP-SubnetBits	<input type="text"/>

Back
Next

Configure the variables as described in the table below.

Customer Variables	Values
IP-Network	Network IPv4 IP address
IP-SubnetBits	For example, 24.
Trusted-IP-Network	Trusted IP address range
Trusted-IP-SubnetBits	IP subnetBits for this range (32 if only a single IP address)

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.

Variable	Description
{{CustomerId}}	The Short Customer Name.
{{CustomerId}}-t	Teams trunk
{{CustomerId}}-c	Carrier trunk

Variable	Description
{{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.
{{this.Name}}	Used to indicate the customer's shortname.
{{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.

Variable	Description
{{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.

Customer 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.

Id	Script	Description	FriendlyName	ScriptType	CustomerVariables
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 c...	NULL	add-ip-pbx-user	NULL	NULL
5000	configure voip ...	NULL	sbc-add-oc-nu...	NULL	NULL
5001	configure voips...	NULL	sbc-remove-oc...	NULL	NULL
800	custom script	NULL	customscript	1	variable1,variable2
NULL	NULL	NULL	NULL	NULL	NULL

Id	Script	Description	FriendlyName	ScriptType	CustomerVariables
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 c...	NULL	add-ip-pbx-user	NULL	NULL
5000	configure voip ...	NULL	sbc-add-oc-nu...	NULL	NULL
5001	configure voips...	NULL	sbc-remove-oc...	NULL	NULL
800	configure voip ...	NULL	customscript	1	localhostname
NULL	NULL	NULL	NULL	NULL	NULL

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 in the Onboarding wizard when the script is selected.

```

SQLQuery6.sql - U...1-c\umpadmin (97)
UMP-training1-c\S...SbcScriptTemplate
SQLQuery4.sql - U...1-c\umpadmin (60)
SQLQuery3.sql - U...1-c\umpadmin (59)

ip-profile name "Teams"
local-host-name "{{CustomVar.Variable1}}"
always-use-source-addr 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.

100 % ▾

Results Messages

	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 sip...	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	OnlinePatnGateway,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

The Custom Variables defined above appear in the wizard when the IP PBX Onboarding script is selected in the wizard.

1 M365 Tenant
2 M365
3 Voice Route
✕

Onboarding Script IP PBX 📎

Cleanup Script IP PBX Cleanup 📎

Customer Variables	Value
IPPBX-proxyaddress	<input style="width: 90%;" type="text"/>
IPPBX-proxyaddress-SIPPort	<input style="width: 90%;" type="text"/>
SIP-Hostname	<input style="width: 90%;" type="text"/>

Back
Submit

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.

```

SQLQuery17.sql - U...SP/livecloud (221)  SQLQuery15.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
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-resin-name "PBX"
ip-profile-name "PBX"
sip-group-name "{{(CustomVar.SIP-Hostname)}}"
outbound-msg-manipulation set 17
msg-man-user-defined-string "{{(CustomVar.IPPBX-proxyaddress)}}"
tags "frunk={{(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 sbs-as-client
{{(if SBC.EnabledCAC)}}
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

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 its configured for a gateway or SBC call.

```

SQLQuery17.sql - U...SP...livecloud (221)
proxy enable keep alive using options
sbcp4 sip-int-name "PBX5IP"
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 "PBX5IP"
ip-profile-name "PBX5"
sip-group-name "{{(CustomerVar.SIP-msgname)}}"
outbound-msg-manipulation-set 17
authentication-mode sbc-as-client
msg-man-user-defined-string1 "{{(CustomVar.IPPBX-proxyaddress)}}"
tags "Trunk={{(SBC.OfflinePstnGateway)}}"
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.OfflinePstnGateway)}}"
always-use-source-addr enable
tags "Tenant={{(SBC.OfflinePstnGateway)}}"
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

```

Scenario Scripts Templates Page

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

➤ To manage scripts:

1. In the Multitenant Navigation pane, open the Scripts Templates page (**System > Script Templates**).
2. In the Multitenant Navigation pane, open the Scripts Templates page (**Configuration > Script Templates**).

By default, all scripts are displayed. The following filters can be applied:

- **Show M365 scripts** displays only M365 scripts.
- **Show SBC scripts** displays only SBC scripts.

ScriptName	Executed on	Related with	Has custom arguments	Has history
sbc-add-prefix	1/1/0001 12:00:00 AM		<input type="checkbox"/>	Show no history
sbc-remove-prefix	1/1/0001 12:00:00 AM		<input type="checkbox"/>	Show no history
add-ip-pbx-user	1/1/0001 12:00:00 AM		<input type="checkbox"/>	Show no history
sbc-add-oc-numbers	1/20/2022 12:31:44 PM		<input type="checkbox"/>	Show no history
sbc-remove-oc-numbers	1/19/2022 7:04:40 PM		<input type="checkbox"/>	Show no history
sbc-scenario7	1/16/2022 3:14:20 PM	sbc-scenario7Cleanup,sbc-scenario7Cleanup,sbc-scenario7Cleanup,sbc-scenario7Cleanup	<input type="checkbox"/>	Show no history
sbc-scenario7Cleanup	1/1/0001 12:00:00 AM	sbc-scenario7,sbc-scenario7,sbc-scenario7,sbc-scenario7	<input type="checkbox"/>	Show no history

Showing 1 to 8 of 7 entries

Previous 1 Next

Script Template

3. To display the contents of a specific script, select an entry and then click **Show**. The contents of the script are displayed in the Script Template pane.

The screenshot shows the UMP-365 interface with a table of scripts and a detailed view of a script template.

Scripts Table:

Id	ScriptName	Type	Executed on	Related with	Custom Arguments	History
7	sbc-scenario7	SbcOnboarding		sbc-scenario7Cleanup	<input type="checkbox"/>	Show 3 versions
900	M365 onboarding	M365Onboarding			<input type="checkbox"/>	Show 1 versions
901	M365 cleanup	M365Cleanup			<input type="checkbox"/>	Show 1 versions
700	sbc-scenario7Cleanup	SbcCleanup		sbc-scenario7	<input type="checkbox"/>	Show 3 versions
100	sbc-add-prefix				<input type="checkbox"/>	Show 3 versions
101	sbc-remove-prefix				<input type="checkbox"/>	Show 3 versions
800	customscript	SbcOnboarding			<input checked="" type="checkbox"/>	Show 1 versions
103	add-ip-pbx-user				<input type="checkbox"/>	Show 3 versions

Showing 1 to 8 of 10 entries

Previous **1** Next

Script Template:

```

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"
  
```

Script Scenario Comparison

Differences between script versions can be viewed using the compare tool in the Script Templates page.

➤ To compare scripts:

1. In the Main Tenant Navigation pane, open the Scripts Templates page (**System > Script Templates**).
2. Choose the script that you wish to compare and then click the link in the History column. For example, for sbc-scenario7 script, click the **3 versions** link.

The screen compare tool is displayed.

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

[illegible]

- Click **current**; the contents of the current version of the script are displayed in the left “Older” pane. Click **version 3**; the latest script is displayed in the right “Newer” pane.
- Scroll down to review the differences.
- Click **Clear Left** and **Clear Right** to clear the display.

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:
 - **Blue** indicates the syntax to add.
 - ~~Strikethrough~~ indicates the syntax to add.

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.RuleSBC-Phones}}

dial-plan-rule new

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

prefix "{{this.Prefix}}"

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

exit

```



```
{{/each}}
```

```
activate
```

```
exit
```

```
{{/each}}
```

```
do write
```

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
```

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.O365OnlinePSTNGatewaythis.Tag}}"

exit

{{/each}}

activate

exit

do write

```

sbc-remove-prefix

```

configure voip

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

{{#each ToRemove}}

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

{{/each}}

activate

exit

do write

```

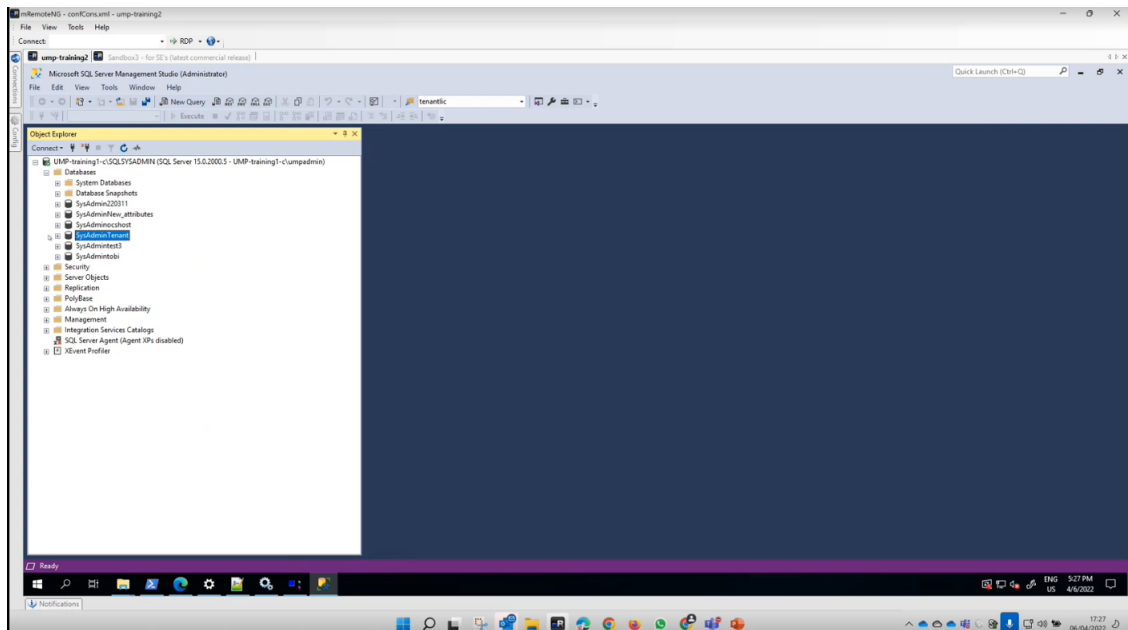
SQL DBA Script Pairing

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

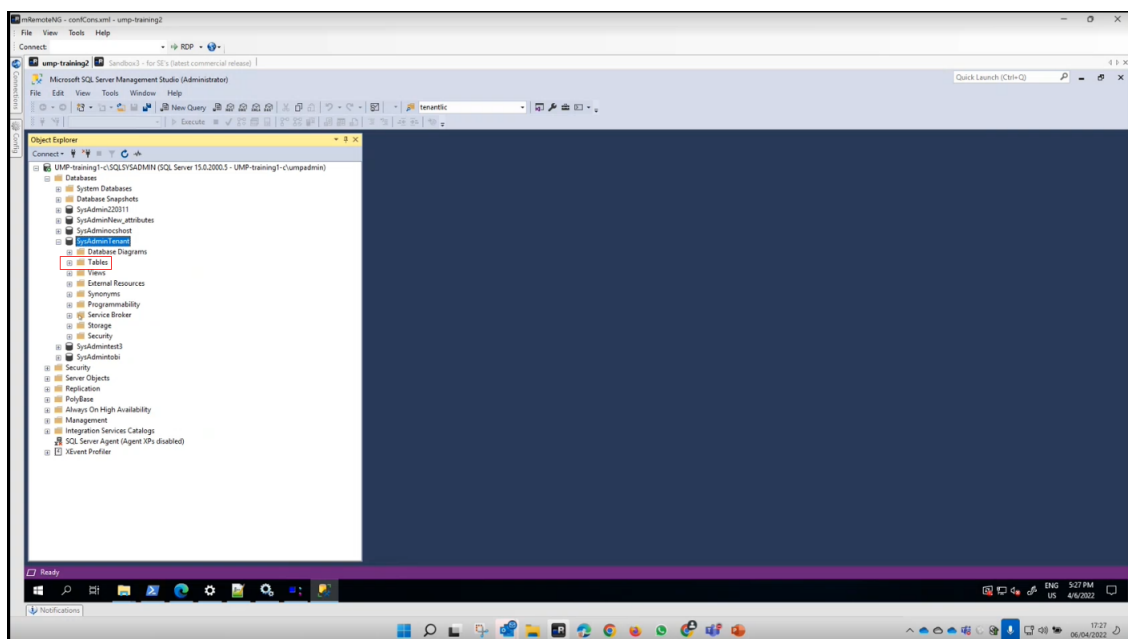
dbo.SBCScriptTemplate table.

➤ **To pair SQL DBA scripts:**

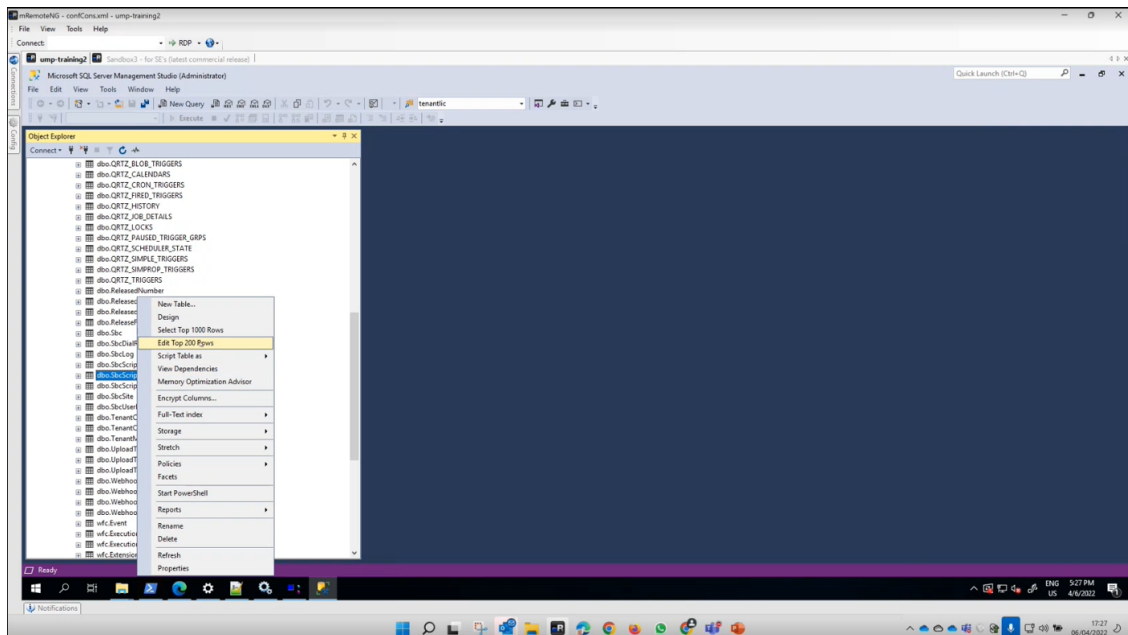
1. Open the SQL database Object Explorer.



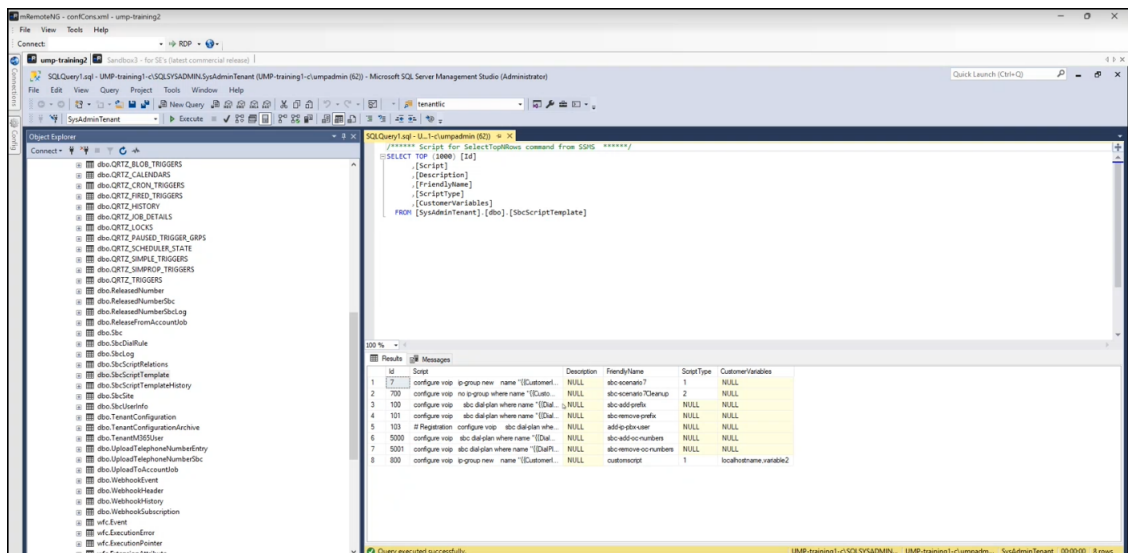
2. Select SysAdminTenant database.



3. Expand the Tables folder.

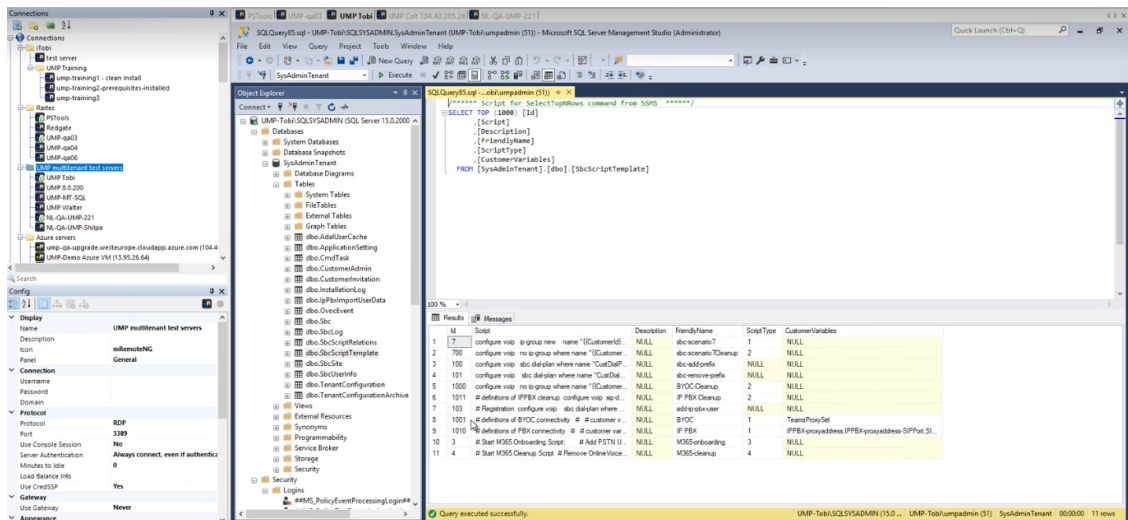


4. Select the **dbo.SBCScriptTemplate** table, right-click and select **Edit Top 200 Rows**.

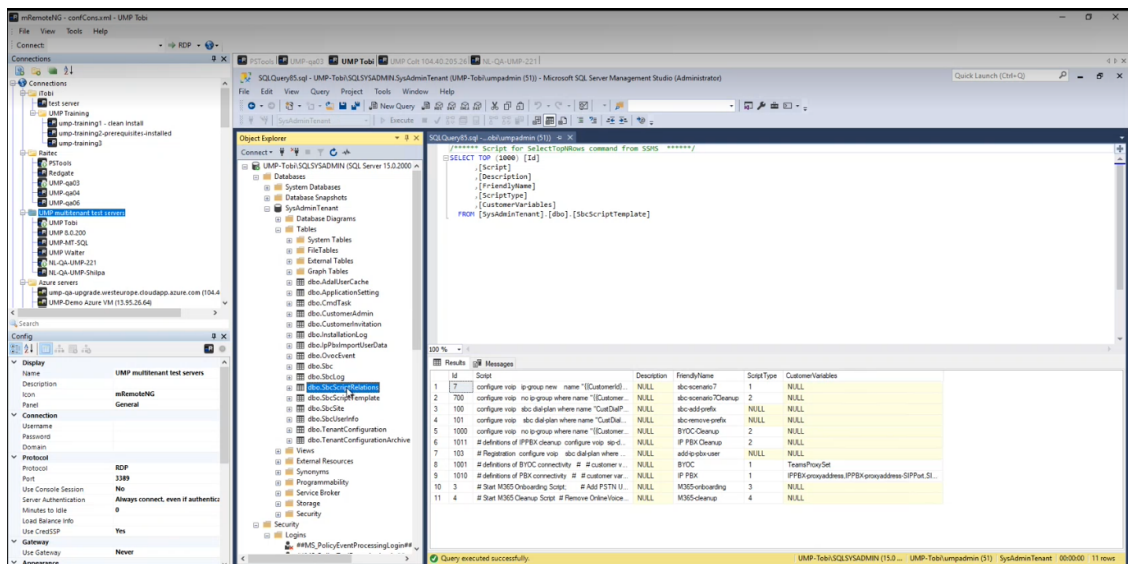


The template scenario scripts are displayed.

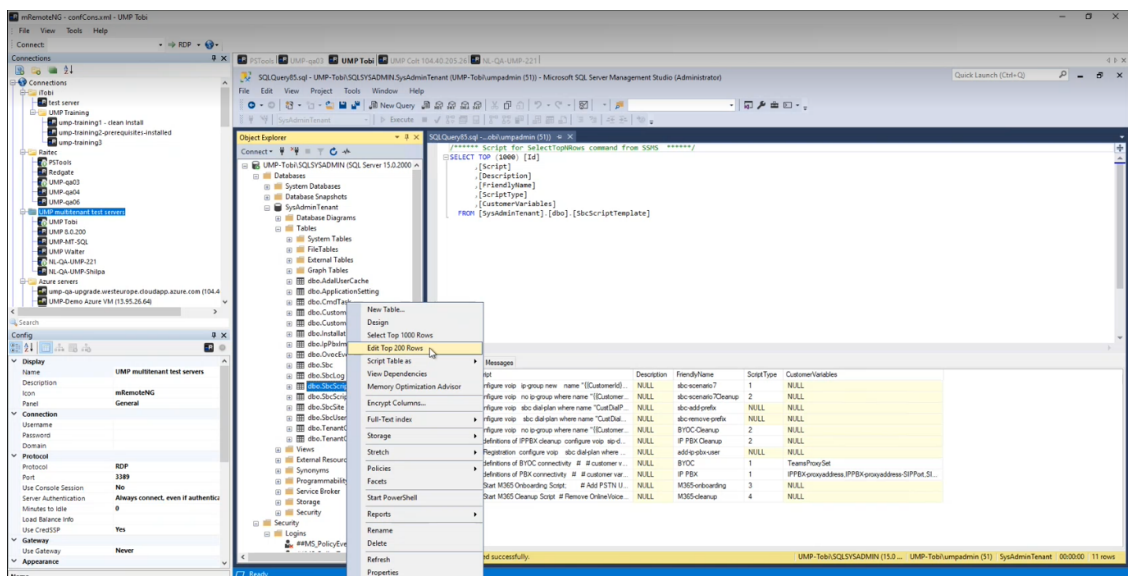
5. In the **dbo.SBCScriptTemplate** table, note the scripts that you wish to pair.



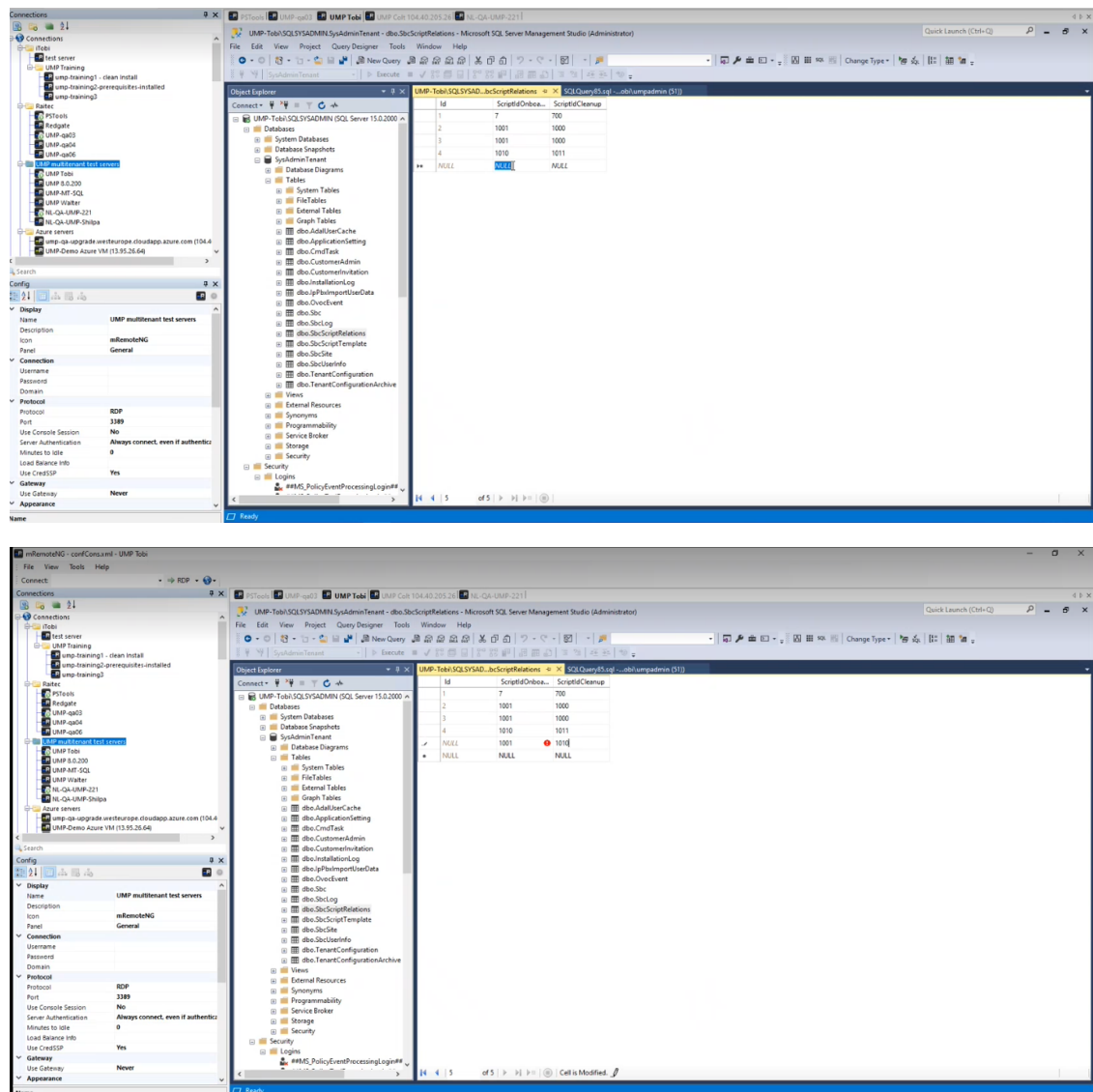
6. Right-click the dbo.SbcScriptRelations table.



7. Choose Edit Top 200 Rows.



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



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

When disabled, the Onboarding script does not check for IP Groups configured on the SBC.

The screenshot shows the Microsoft SQL Server Enterprise Manager interface. The left pane displays the 'Object Explorer' with the 'SysAdminTenant' database selected. The right pane shows the 'dbo.applicationSetting' table with columns 'id', 'Value', and 'MachineName'. The table contains various configuration settings for the application.

id	Value	MachineName
CleanupAge	10	NULL
CustomerAuthenticationPortalUrl	https://ump-impportal-staging...	NULL
CustomerInvitation.DeliveryMethod	Network	NULL
CustomerInvitation.EnabledSsl	True	NULL
CustomerInvitation.From	BMISUMPServices@audiocodes...	NULL
CustomerInvitation.Host	smtp.office365.com	NULL
CustomerInvitation.Password	Qm9ROGN0cm9uMkR0dENhQz=	NULL
CustomerInvitation.Port	587	NULL
CustomerInvitation.UserName	BMISUMPServices@audiocodes...	NULL
InstallationFolder	c:\acs	NULL
InstallationScript	c:\acs\InstallationScript\install_te...	NULL
InvitationEmail	Dear Administrator of {{Customer...	NULL
InvitationSubject	Welcome {{Customerid}} for joini...	NULL
LicenseKey	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI...	NULL
OAuthEnabled	True	NULL
OAuthHeaders	("OAuthAuthorizationHeader":"Ba...	NULL
PublicServerUrl	http://localhost	NULL
RegenerateTokensWarning	True	NULL
ServerDomain	-	NULL
ServicePassword	UMPe0112a21Q	NULL
ServiceUsername	Administrator	NULL
SourcePackage	c:\acs\SysAdminKit	NULL
SysAdminConnectionString	NULL	NULL
TeamsTokenApp.ClientId	bff3c4bb-cef4-44d3-b047-a061f6...	NULL
TeamsTokenApp.RedirectUri	https://ump-impportal-staging...	NULL
TeamsTokenApp.Secret	~v~-_Jns13aK4eKl7vcV_HQ8-jd...	NULL
TenantDir	c:\acstentants	NULL
Whitelabel	ATT	NULL
WhitelabelCustomerAuthentication	AT&T_logo.svg	NULL
SkipSslValidation	True	NULL
NULL	NULL	NULL

Managing Security Settings

This section describes the following security settings:

- [Customer Admins](#) below
- [Authentication Status](#) on page 228
- [Customer Invitations](#) below
- [UMP Service Settings](#) on page 234

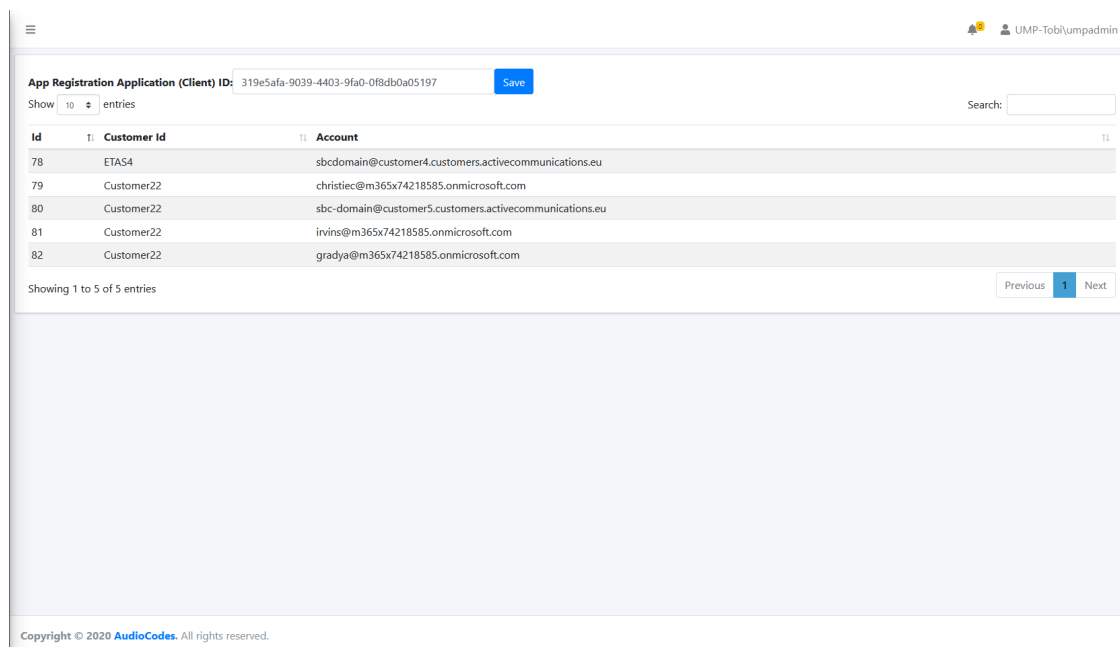
Customer Admins

The Customer Admins screen allows you to manage access for Customer administrators. Once the Application Registration is performed on the customer tenant and the Client ID is configured in this screen (see [Create Registration for Customer Administrators](#) on page 87), Customer administrators can be granted permissions to view their managed tenant (see [Initial Access to UMP-365 and Assigning Customer Admins](#) on page 425).

➤ To manage customer administrators:

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

A list of Application (Client) IDs are displayed.



The screenshot displays the 'Customer Admins' page. At the top, there is a header bar with a hamburger menu icon on the left and a user profile 'UMP-Tobi\umpadmin' on the right. Below the header, the main content area has a title 'App Registration Application (Client) ID:' followed by a text input field containing '319e5afa-9039-4403-9fa0-0f8db0a05197' and a 'Save' button. Below this, there is a 'Show' dropdown set to '10' and a search bar. The main part of the page is a table with the following data:

Id	Customer Id	Account
78	ETAS4	sbcdomain@customer4.customers.activecommunications.eu
79	Customer22	christiec@m365x74218585.onmicrosoft.com
80	Customer22	sbc-domain@customer5.customers.activecommunications.eu
81	Customer22	irvins@m365x74218585.onmicrosoft.com
82	Customer22	gradya@m365x74218585.onmicrosoft.com

At the bottom of the table, it says 'Showing 1 to 5 of 5 entries'. There are 'Previous', '1', and 'Next' navigation buttons. The footer of the page reads 'Copyright © 2020 AudioCodes. All rights reserved.'

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 [Configuring Microsoft Teams Direct Routing SBC](#) on page 86). The invitation email includes a token authentication link, details of which are displayed in the Authentication Status screen (see [Authentication Status](#) on page 228).

➤ **To monitor customer invitations:**

1. In the Multitenant 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.

Customer Invitations

Reload data Edit

Search:

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.

The table below describes the Customer Invitations parameters:

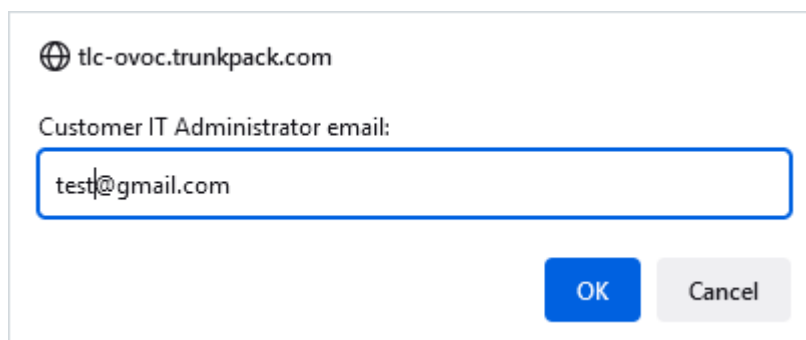
Table 27-1: Customer Invitations

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 Securing Microsoft 365 Service Provider Access on page 511)
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.

Parameter	Description
Email Invitation Sent Count	The number of retries for UMP to send the invitation email to the customer (the retry occurs per minute). The failure could be the result of the SMTP setup or due to network issues.
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



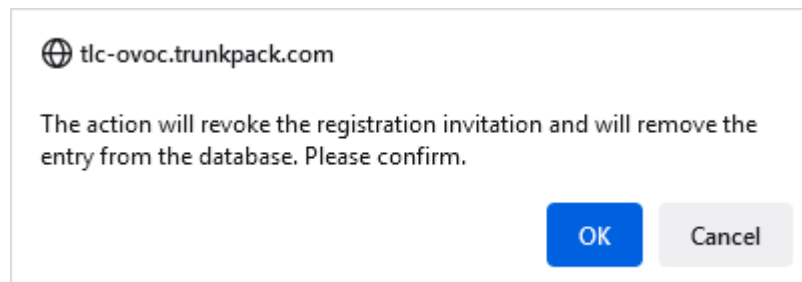
tlc-ovoc.trunkpack.com

Customer IT Administrator email:

test@gmail.com

OK Cancel

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

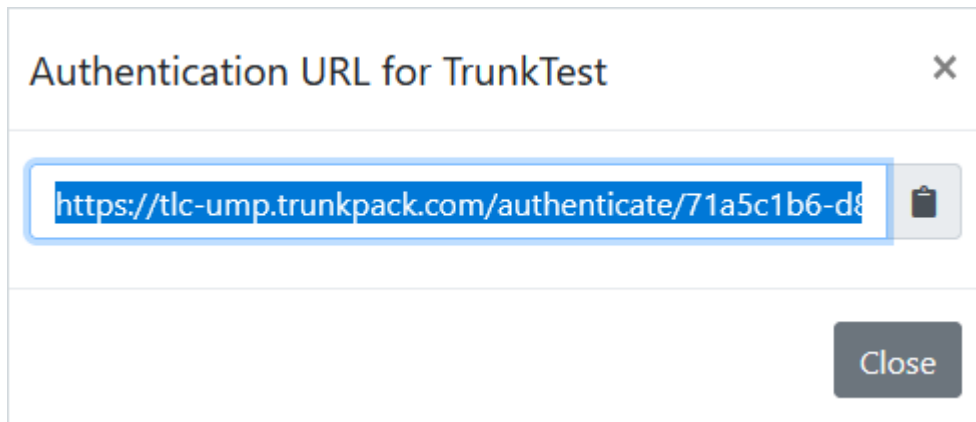


tlc-ovoc.trunkpack.com

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`



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

Authentication Status

The Authentication Status 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 that is used for the Background Replication process (see [Queued Tasks \(Background Replication\)](#)). In the Onboarding wizard (for Hosted Essentials + and Hosted Pro customers), connection to the customer's Microsoft 365 platform is secured using the following methods:

- **Username and Password:** The customer uses their existing username and password, however, in addition, the connection to M365 is secured with an access token that is claimed based on the configured user name and password. See [Switching to User Password](#) on page 525.



Customers onboarded prior to version 8.0.450 with user and password must be authenticated using token-based authentication as a result of enhanced Microsoft Security policies.

- **Switch to auth token:** This option secures the connection with M365 through a directly-claimed access token. See [Switching to Token Authentication](#) on page 519.

Using both of the above methods, the customer tenant must grant consent to the Service Provider administrator. The consent process is secured through an access token that is claimed based on the configured user name and password. The Authentication Status screen summarizes the connection status with the customer tenant's M365 platform using one of the above methods.

➤ **To manage Authorization tokens:**

1. In the Multitenant Navigation pane, open the Authentication Status page (**Security > Authentication Status**).

AuthenticationStatus
Monitor Authentication Status

Client Id
3987f05f-3b81-4d26-8bb2-4e16a5a8ce2e

Client Secret

Redirect Uri
https://tokensandbox3.finebak.com/authenticate/OAuth2Callback

Apply Changes Reset Changes

Search:

Customer Id	M365 Email	Authentication method	When Last Verified	Last Verification Status	Actions
dr8	admin@AudcDemo6.onmicrosoft.com	Token	February 7th 2023, 18:25	✓	Check Credentials Switch to password
Demo	admin@M365x08167531.onmicrosoft.com	Password	March 9th 2023, 15:38	✗	Check Credentials Switch to token
ManuelTest	admin@M365x29347113.onmicrosoft.com	Password	February 7th 2023, 18:26	✓	Check Credentials Switch to token
DemoTotSpo	admin@M365x62214376.onmicrosoft.com	Token	February 7th 2023, 18:25	✓	Check Credentials Switch to password
TRitzik	admin@M365x18234803.onmicrosoft.com	Password	February 7th 2023, 18:24	✓	Check Credentials Switch to token
testpro	admin@M365x11164675.onmicrosoft.com	Password	March 9th 2023, 11:56	✗	Check Credentials Switch to token

2. Configure the Client Id and Client Secret of the Tenant Enterprise Application Registration for Token Authentication. This registration is created in Day One Onboarding (for Hosted Essentials + and Hosted Pro customers).



If the Client Id is not configured and then the **Grant Consent** option in the Self-Service portal M365 Settings (see [Securing Microsoft 365 Service Provider Access](#) on page 511) is clicked, the following error is displayed:

1 M365 Tenant 2 M365 3 Voice Route X

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

No ClientId was specified.

Something went wrong while verifying M365 credentials!

Back Next

For example:

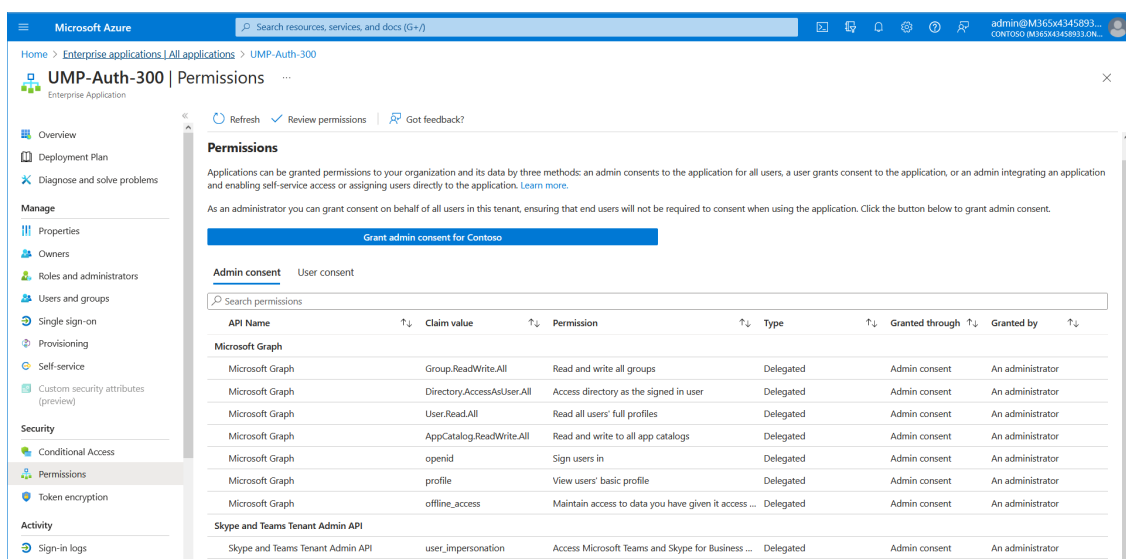
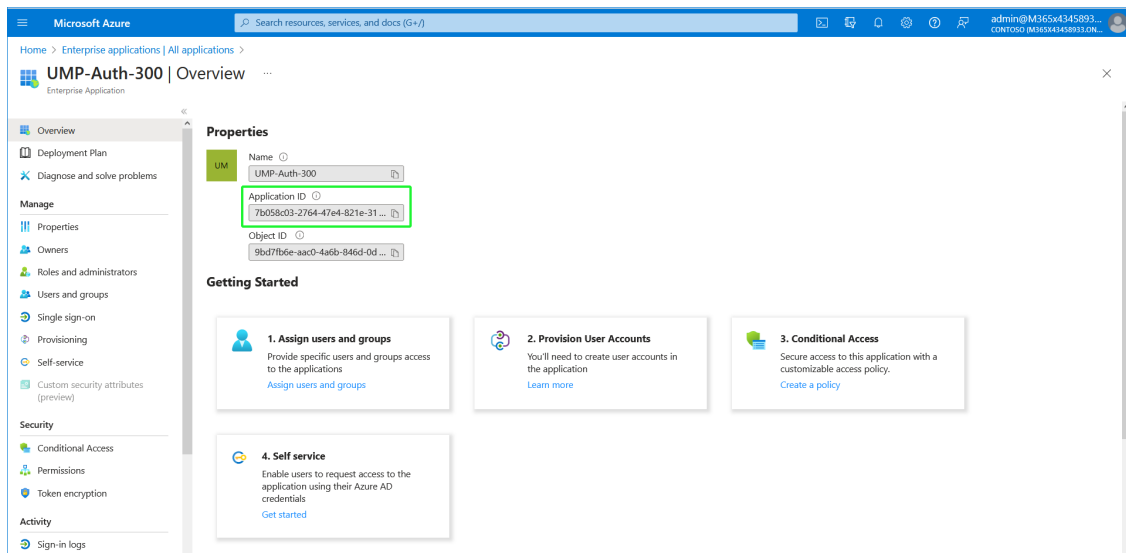
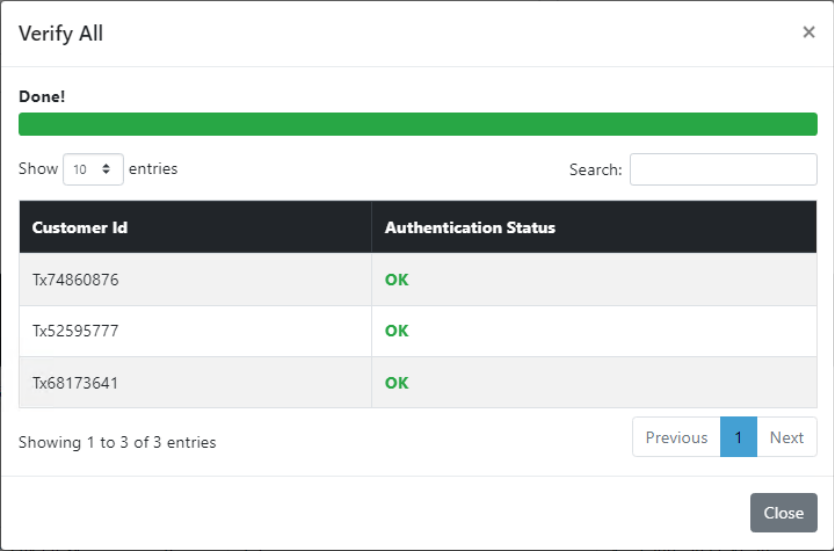
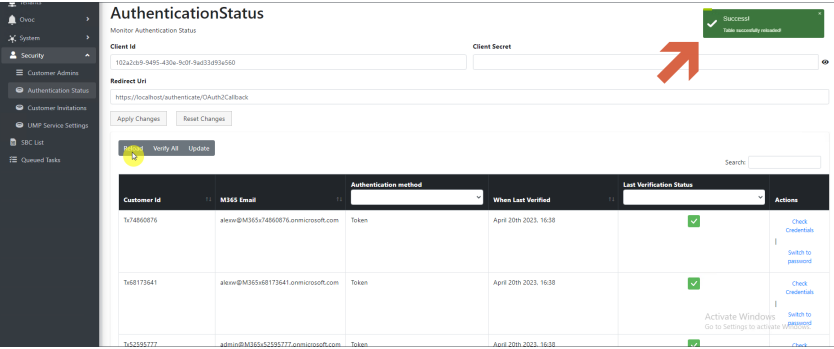



Table 27-2: Authentication Status

Field	Description
Customer Id	The Customer name.
M365 Email	The email address of the Microsoft Office 365 administrator providing consent on behalf of the customer.
Authentication Method	One of the following authentication methods: <ul style="list-style-type: none"> ■ Password (relevant for customers until version 8.0.450). For version 8.0.450 and later, all customers must be authenticated using token authentication. ■ Token authentication.
When Last	The date and time of the last verification of connection to customers'

Field	Description								
Verified	M365 platform.								
Last Verification Status	<p>Indicates one of the following verification statuses:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Never Performed <input type="checkbox"/> Successful <input type="checkbox"/> Failed <input type="checkbox"/> Token not generated 								
Update	<p>Updates for changes to Authentication method (Switch to User Password and Switch to Token). It also updates table for new customers.</p> <div> <div>Update Authentication Method</div> <div> <div>Done!</div> <div> <div>Show 10 entries</div> <div>Search:</div> </div> <table> <tr> <th>Tenant</th><th>Auth Type</th></tr> <tr> <td>Tx74860876</td><td>Token</td></tr> <tr> <td>Tx52595777</td><td>Token</td></tr> <tr> <td>Tx68173641</td><td>Token</td></tr> </table> <div> <div>Showing 1 to 3 of 3 entries</div> <div> <div>Previous</div> <div>1</div> <div>Next</div> </div> </div> <div>Close</div> </div> </div>	Tenant	Auth Type	Tx74860876	Token	Tx52595777	Token	Tx68173641	Token
Tenant	Auth Type								
Tx74860876	Token								
Tx52595777	Token								
Tx68173641	Token								
Verify All	Verifies that all claimed tokens are valid and user passwords are correct. Perform this action after 'Update' above.								

Field	Description
	
Reload All	<p>Refreshes table. Perform this action after 'Verify All'.</p> 

- Enter the Client ID and Client secret generated in [Deploy Synchronization Application](#).
- Enter the Redirect URL which consists of the IP address of the Service Provider portal. For example:
<https://finebak.domain.com/authenticate/OAuth2Callback>

Parameter	Description
Actions	<p>One of the following actions can be performed:</p> <ul style="list-style-type: none">  Check Credentials: click to verify the token. Once verified, is displayed in the Last Verification Status column. Switch to password Switch to token

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

Verify All Tokens



Done!

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

Close

Update Used By



Done!

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

Close

tlc-ovoc.trunkpack.com

Customer IT Administrator email:

test@gmail.com

OK

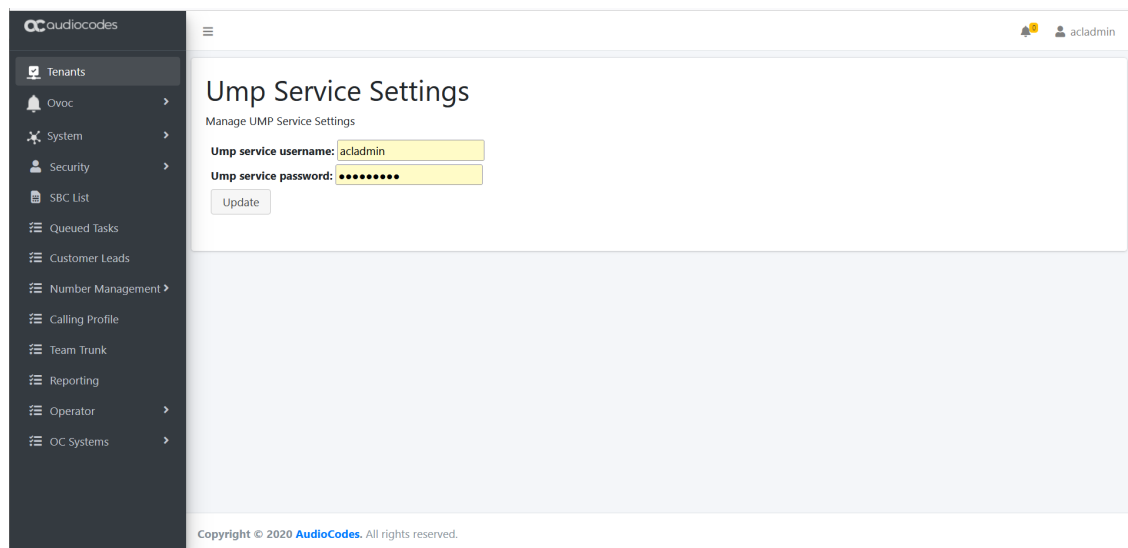
Cancel

UMP Service Settings

The UMP Service Settings for Windows server displays the SysAdmin Windows Services credentials used to install the UMP-365 (see [Creating UMP Service Account](#) on page 29).

➤ **To configure UMP Service Settings:**

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



The screenshot shows the 'Ump Service Settings' page in the AudioCodes management interface. On the left is a dark sidebar with a navigation menu including 'Tenants', 'Ovoc', 'System', 'Security', 'SBC List', 'Queued Tasks', 'Customer Leads', 'Number Management', 'Calling Profile', 'Team Trunk', 'Reporting', 'Operator', and 'OC Systems'. The main content area has a header 'Ump Service Settings' and a sub-header 'Manage UMP Service Settings'. Below this, 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 footer of the page reads 'Copyright © 2020 AudioCodes. All rights reserved.'

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

Managing SBC Devices

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

- **Add SBC Devices** on the next page: 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 SBC Site Locations** on page 237: Show a list of configured site locations that are connected to specific SBC devices.
- **Show Prefixes** on page 239: Show a list of configured number prefixes in the dialplans loaded to the managed SBC devices.
- **Download Dial Plan from Managed SBC (Import Customer)** on page 240 : Import a list of customers from the SBC.

➤ **To display list of managed SBC devices:**

1. In the Multitenant portal Navigation pane, select **SBC List**.

SBC List											
Id	Ovoc Sbc Id	Name	Ip Address	Device Fqdn	NAT Ip Addresses	Https	Gateway User	Status	Sip Users Count	Sites Count	
7	7058	EMEA SP1 SBC	10.17.0.4		40.118.70.74	False	LiveCloud	Connected	-N/A-	169	[Show Sites] [Import Customers] [Show Prefixes]
8	7613	APAC SP1 SBC	10.18.0.4		13.67.53.137	False	LiveCloud	Connected	-N/A-	25	[Show Sites] [Import Customers] [Show Prefixes]
11	53209	US SP1 SBC	20.110.187.52	sandbox3us.audiocodes.be	20.110.187.52	False	LiveCloud	Connected	-N/A-	5	[Show Sites] [Import Customers] [Show Prefixes]

The table below describes the details for each managed SBC device.

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.
NAT IP Address	NAT IP address of the SBC device.

Parameter	Description
Device FQDN	Known FQDN of the SBC device.
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.

Add SBC Devices

This section describes how to add new SBC devices to the multitenant deployment. Once added, these devices can be configured when onboarding new customers.

➤ To add a new SBC device:

1. In the Multitenant portal Navigation pane, click **SBC List**. A list of managed SBC devices is displayed.

Known SBCs

Reload From Ovoc Add New SBC

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

Copyright © 2020 AudioCodes. All rights reserved.

2. Click **Add New SBC** to add a new SBC device (the new connection is by default secured over HTTPS).

Add New SBC

Name:

SBC Name

Ip Address:

ex: 1.2.3.4

Use https: ☒

Device Fqdn:

ex: sbc.contoso.com or contoso.com

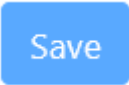
Gateway User:


Gateway Password:

Close

Save

3. Enter the name of the SBC device.
4. Enter the IP address of the SBC device.
5. Enter the Device FQDN.
6. Enter the Gateway username and password.

7. Click  to apply the changes.

8. Click  to refresh the connection between the SBC devices list and the OVOC Server.

9.

Show SBC Site Locations

You can display all site locations that are configured with an SBC device that manages calls through that site.

➤ To show site locations:

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

Known SBCs

Reload From Ovoc Add New SBC

SBC List										
Id	Ovoc Sbc Id	Name	Ip Address	Device Fqdn	NAT Ip Addresses	Https	Gateway User	Status	Sip Users Count	Sites Count
7	7058	EMEA SP1 SBC	10.17.0.4		40.118.70.74	False	LiveCloud	Connected	-N/A-	169
8	7613	APAC SP1 SBC	10.18.0.4		13.67.53.137	False	LiveCloud	Connected	-N/A-	25
11	53209	US SP1 SBC	20.110.187.52	sandbox3us.audiocodes.be	20.110.187.52	False	LiveCloud	Connected	-N/A-	5

Copyright © 2023 AudioCodes. All rights reserved.

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

SBC Site Locations

Show 10 entries Search:

Site Locations					
Site	Customer Name	Configuration	PSTN Gateway	SbcDeploymentState	M365DeploymentState
wsc	wsc	SipTrunk	customertobi.customers.activecommunications.eu	Deployed	Deployed
ETAS4	ETAS4	SipTrunk	customer4.customers.activecommunications.eu	Deployed	Deployed
Customer22	Customer22	SipTrunk	customer5.customers.activecommunications.eu	Deployed	

Showing 1 to 3 of 3 entries

Previous 1 Next

Close

The table below describes the parameters in this table.

Parameter	Description
Site	Name of the site location.
Customer Name	Customer Name
Configuration	One of the following values: <ul style="list-style-type: none"> SIP Trunk IP-PBX BYOC
PSTN Gateway	FQDN of the Online PSTN Gateway for the site location.
SBC Deployment State	Indicates that the SBC has been successfully connected to UMP-365.

Parameter	Description
M365 Deployment State	Indicates that the SBC has been successfully connected to M365.

Show Prefixes

This option lets you to view a list of configured dialplans on the selected SBC device. Each entry in the table represents a separate dial plan rule.



In UMP-365, the Dialplan name and the Dialplan rule are the same. On the SBC device, the dial plan rules defined under each dialplan are configured with unique names.

➤ To show prefixes:

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

SBC: oc1.customers.audio-code.co.il [51.137.97.95] - Prefixes ×

Refresh From Sbc

Show 10 entries

Search:

SBC Prefixes					
DialPlan ↑↓	Index ↑↓	Name ↑↓	Prefix ↑↓	Tag ↑↓	Activ ↑↓
TeamsTenants	1	Fidinam	+41589061[000-999]	4064116.cic.coltdcloudsbc.net	true
RegisteredUsers	1	M365x35880531	5755	972528545755	true
RegisteredUsers	0	M365x35880531	+972528545755	5755	true
CustDialPlan	2	M365x38076038	+5552000	M365x38076038.customers.audio-code.co.il	true
TeamsTenants	2	MKSPAMPGROUP	+4420366669[700-799]	100321906.cic.coltdcloudsbc.net	true
OCDialPlan	0	qqqqqqqqqqqqqq	+97236549877	daf09efd-f31e-41e4-a86c-bd65bf821e25	true
OCDialPlan	1	qqqqqqqqqqqqqq	+97299999998	daf09efd-f31e-41e4-a86c-bd65bf821e25	true

Showing 1 to 7 of 7 entries

Previous

1

Next

Close

The table below describes the parameters in this screen.

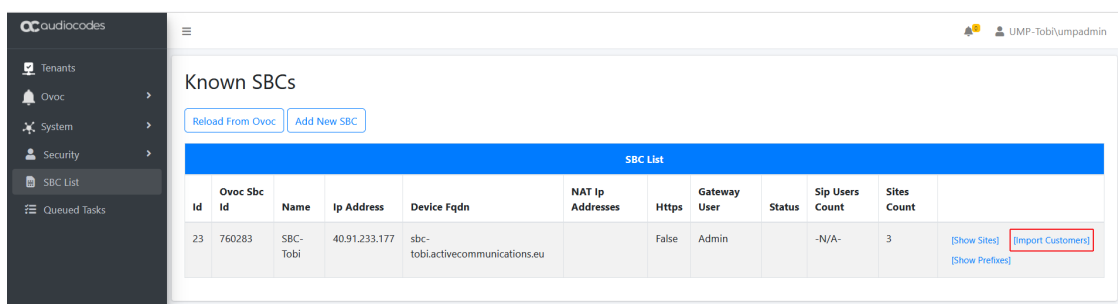
Parameter	Description
Dial Plan	Name of the Dial plan
Index	SBC index
Name	Name of the Live Cloud server instance.
Prefix	Configured phone prefix
Tag	One of the following: <div> <div></div> Tenant ID </div> <div> <div></div> IP Group Name </div>
Active	

Download Dial Plan from Managed SBC (Import Customer)

This option enables you to upload preexisting dial plans from a managed SBC device. A new customer is automatically created in the process. During this process, UMP-365 queries the uniqueness of the Dialplan rule name with the matching derived Trunk FQDN or Azure Tenant ID of the customer. Once imported, the customer shortname inherits the Dialplan rule name.

➤ To upload dial plan from an SBC:

1. In the SBC List, click **Import Customers**.



The screenshot shows the UMP-365 web interface. On the left is a sidebar with navigation options: Tenants, Ovoc, System, Security, SBC List (selected), and Queued Tasks. The main area is titled 'Known SBCs' and contains buttons for 'Reload From Ovoc' and 'Add New SBC'. Below these is a table titled 'SBC List' with the following columns: Id, Ovoc Sbc Id, Name, Ip Address, Device Fqdn, NAT Ip Addresses, Https, Gateway User, Status, Sip Users Count, Sites Count, and two action links: [Show Sites] and [Import Customers] (highlighted with a red box). The table contains one row with the following data: Id: 23, Ovoc Sbc Id: 760283, Name: SBC-Tobi, Ip Address: 40.91.233.177, Device Fqdn: sbc-tobi.activecommunications.eu, NAT Ip Addresses: (empty), Https: False, Gateway User: Admin, Status: -N/A-, Sip Users Count: 3, Sites Count: 3.

A list of customers are displayed.



Customers that have already been imported to UMP-365 are not displayed, unless the matching tag FQDN PSTN Gateway/Customer Azure Tenant ID are different. In this case, both rules are imported and added to the same customer.

Import Customers from SBC
×

SBC Cleanup Script
IPPBX-Cleanup.

Show
10
entries
Search:

oc1.customers.audio-code.co.il [51.137.97.95]			
SBC Customer Name ↑↓	FQDN PSTN Gateway ↑↓	Customer Full Name ↑↓	↑↓
Audio00codeOC1	daf09efd-f31e-41e4-a86c-bd65bf821e25	Audio00codeOC1	[Import]
Audio00codeOC2	daf09efd-f31e-41e4-a86c-bd65bf821e25	Audio00codeOC2	[Import]
Audio00codeOC3	223b8b5c-f255-4f59-af6d-422f6548d7ed	Audio00codeOC3	[Import]
Fidinam	4064116.cic.coltdcloudsbc.net	Fidinam	[Import]
MKSPAMPGROUP	100321906.cic.coltdcloudsbc.net	MKSPAMPGROUP	[Import]

Showing 1 to 5 of 5 entries
Previous
1
Next

Close

- Click the **Import** button adjacent to the customer that you wish to import.

The customer is imported.

Import Customers from SBC

SBC Cleanup Script IPPBX-Cleanup.Show 10 entriesSearch:

oc1.customers.audio-code.co.il [51.137.97.95]			
SBC Customer Name ↑↓	FQDN PSTN Gateway ↑↓	Customer Full Name ↑↓	↑↓
Audio00codeOC1	daf09efd-f31e-41e4-a86c-bd65bf821e25	<input type="text" value="Audio00codeOC1"/>	[Import]
Audio00codeOC2	daf09efd-f31e-41e4-a86c-bd65bf821e25	<input type="text" value="Audio00codeOC2"/>	[Import]
Audio00codeOC3	223b8b5c-f255-4f59-af6d-422f6548d7ed	<input type="text" value="Audio00codeOC3"/>	[Import]
Fidinam	4064116.cic.coltdcloudsbc.net	<input type="text" value="Fidinam"/>	[Imported]
MKSPAMPGROUP	100321906.cic.coltdcloudsbc.net	<input type="text" value="MKSPAMPGROUP"/>	[Import]

Showing 1 to 5 of 5 entries

Previous 1 NextClose

Once a specific dial plan is uploaded, it is removed from the list. However, with the exception where two DialPlan rules are created with the same name however with different tag values. In the example below, two DialPlan rules have been created with the name "BradTrunk", however the tag values are different. In this case, both of the rules are displayed in the Import Customer screen.

ccaudiocodes SETUP MONITOR TROUBLESHOOT Save Reset Actions brad@hivosp.org

oc1.customers IP NETWORK SIGNALING & MEDIA ADMINISTRATION Entry parameter value

SIP Interfaces (3)
Media Routes (1)
Proxy Sets (6)
IP Groups (17)
Voice AI Connectors (0)
CODERS & PROFILES
SBC
Classification (5)
Routing
Routing Policies (1)
IP-to-IP Routing (7)
Alternative Reasons Set (0)
IP Group Set (0)
Manipulation
SBC General Settings
Call Admission Control Profile (4)
User Information (1)
Malicious Signature (14)
External Media Source (0)
Teams SIP Devices (0)
SIP DEFINITIONS
Accounts (3)
SIP Definitions General Settings
Message Structure
Transport Settings
Proxy & Registration
Priority and Emergency
Call Setup Rules (20)
Least Cost Routing
Dial Plan (4)
Push Notification Servers (0)

Dial Plan (#0) > Dial Plan Rule (5)

INDEX	NAME	PREFIX	TAG
0	BradTrunk	+972900	M365x34456789.customers.corp.com
1	BradTrunk	+972904	M365x34499893.siptrunk.corp.com
2	M365x38078058	+9725000	M365x38078058.customers.audio-code.co.il
492	M365x3580531	9755	M365x3580531.customers.audio-code.co.il
493	M365x3580531	+972538545755	M365x3580531.customers.audio-code.co.il

#1[BradTrunk] Edit

GENERAL

Name * BradTrunk

Prefix * +972904

Tag * M365x34499893.siptrunk.corp.com

Import Customers from SBC

SBC Cleanup Script IPPBX-Cleanup.

Show 10 entries

Search:

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

SBC Customer Name ↑↓	FQDN PSTN Gateway ↑↓	Customer Full Name ↑↓	↑↓
Audio00codeOC1	daf09efd-f31e-41e4-a86c-bd65bf821e25	Audio00codeOC1	[Import]
Audio00codeOC2	daf09efd-f31e-41e4-a86c-bd65bf821e25	Audio00codeOC2	[Import]
Audio00codeOC3	223b8b5c-f255-4f59-af6d-422f6548d7ed	Audio00codeOC3	[Import]
BradTrunk	M365x34456789.customers.corp.com	BradTrunk	[Import]
BradTrunk	M365x34499893.siptrunk.corp.com	BradTrunk	[Import]
MKSPAMPGROUP	100321906.cic.colttcloudsbc.net	MKSPAMPGROUP	[Import]

Showing 1 to 6 of 6 entries

Previous

1

Next

Close

Queued Tasks

You can view the status of all cmdlets executed by the Background replication process which synchronizes the User Management Pack™ 365 SP Edition database with the customer Microsoft 365 platform as a result of actions performed in the Customer portal.

➤ **To view a list of queued tasks:**

1. In the Multitenant portal Navigation pane, click **Queued Tasks**.

Id	Customer	Cmd Type	State	Retries	When Executed	Execution Result	Next Execution Minutes	Was Successful	When Created
3285972	zabupart	Sync all	Queued	10			Now		10-12-2023, 19:43
3285971	zabupart	Sync psq	Queued	10			Now		10-12-2023, 19:43
3285970	zabupart	Sync lcmAz	Queued	10			Now		10-12-2023, 19:43
3285969	zabupart	Sync azgm	Queued	10			Now		10-12-2023, 19:43
3285968	zabupart	Sync azg	Queued	10			Now		10-12-2023, 19:43
3285967	TeamContoso	Sync all	Queued	10			Now		10-12-2023, 19:43
3285966	TeamContoso	Sync psq	Queued	10			Now		10-12-2023, 19:43

The table below describes the details for each task.

Parameter	Description
Queue Entry Id	Indicates the Id in the database queue.
Customer Name	Name of the customer to whom the action is applied.
Cmd Type	<p>The command type applied. One of the following values:</p> <ul style="list-style-type: none"> ■ Sync: Synchronization as a result of customer update actions. ■ CleanupSbc: Sbc Cleanup script run on the customer ■ O365Cleanup: O365 Cleanup script run on the customer ■ O365Initialization: O365 Initialization for new customer ■ TenantRemove: Customer tenant is deleted ■ SbcUpdatePrefixes: Telephone Prefixes have been added or removed

Parameter	Description
	<p>for customer</p> <ul style="list-style-type: none"> ■ TenantUpgrade: Customer tenant is upgraded to Pro or Essentials + or Hosted Pro or OC Essentials + and OC Pro. ■ IpPbxImport: A list of IPPbx users is imported. ■ Upgrade License: Number of licensed users has been changed. ■ OcNumberCleanup: OcNumberCleanup script is run. ■ SBCInit: Initial connection is established with the SBC device.
State	<p>One of the following values:</p> <ul style="list-style-type: none"> ■ Queued: Task is in the waiting queue for processing. ■ Reserved: Task has been reserved for processing. ■ Executing: Task is currently being executed. ■ FinishSuccess: Task has been completed successfully. ■ FinishFailure: Task has not been completed successfully. ■ Queue Postponed due to customer upgrade: Task has been postponed because the customer is currently upgrading to either Hosted Essentials+ or Hosted Pro. ■ Draft: The customer creation is still in progress
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.

Managing the Replication Cycle

Until version 8.0.450, the replication process was executed per hour for all tenants running on the UMP-365 instance. From this version, a CacheSync mechanism synchronizes cached data for individual tenants according to a timer value. This value QuickReplicationCycleDelay(default-five minutes) is set in the dbo.ApplicationSetting file. For example, numbers are assigned to customers for a specific tenant and Enterprise Voice is enabled. In the Queued Changes screen, two new entries are added. If after five minutes, no new updates are executed on this tenant, these actions are queued and processed. The timer mechanism is launched and monitored by the SysAdmin.Watchdog. The number of processes that can run simultaneously is set in the dbo.ApplicationSetting file by the MaxDegreeOfParallelism parameter.

Each executable has its own log directory (found in - C:\acs\tenants\{tenantName}\logs). The following table describes the replication processes.

Process	Description
SysAdmin.QuickReplicationCycleWorker	Process managing the quick cycle replication process.
CacheSync	<ul style="list-style-type: none"> ■ Downloads users, groups and group membership using MSGraph. ■ Downloads users, groups and group membership using CacheSyncAzAd via MSGraph. ■ Downloads all the CsOnlineUsers using CacheSyncV2. ■ Downloads all the Teams user policies using MSTeams module via PowerShell.
SysAdminTenantSvc (Orchestrator)	<p>This service is the main service of UMP. It controls many operations. For example, it schedules and maintains the auto-replication cycles for all the customers, it sends information to the SysAdminTenant Database, etc.</p> <p>To run a manual test, stop the SysAdminTenantSvc. Note that when the SysAdminTenantSvc is restarted, it queues the replication for all the customers on this server.</p>
SysAdmin.UMP.Watchdog	Manages the quick replication cycle timer mechanism. The replication is executed only when there are no new requests within the five minute interval.

Process	Description
SysAdmin.UMP.SyncAcquiredNumber	Used by Operator Connect (OC) for updating the Assignment Status column in the Number Management table in the self-service portal. It is run every 5 minutes.

Part V

Onboarding a new Tenant

29 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.

30 Onboarding Prerequisites

Before Onboarding customers, see the following prerequisites:

- [Register End Customer Tenant DNS Sub domains](#) below
- [End Customer Prerequisites](#) on page 263

Register End Customer Tenant DNS Sub domains

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

- **Fully Automatic process (DNS Hosting Provider resides on Azure):** The creation of the DNS sub domain including the creation of the TEXT and A-record is fully automated using the Onboarding Wizard. This setup requires configuration on the Multitenant portal (see [Setting up Fully Automatic DNS Provisioning](#) on page 70).
- **Two-step process (DNS Hosting Provider does not reside on Azure):** For this option the Onboarding process requires end customer interaction to consent to the creation of a TEXT record for validating their sub domain and an A-record for IP address translation to the FQDN of the SBC device used to manage their voice calling (see [Setup Two-step Provisioning](#) below).
- **Manual process (DNS Hosting Provider resides on Azure):** The DNS sub domain is created manually (see [Manual Provisioning](#) on page 252). This method is used for Hosted Essentials customers.

At least one of the following licenses should be available on the customer tenant for PSTN Trunk activation (activating the Customer domain): Office 365 or E5 Office 365 E1 / E3 license with Microsoft Teams Phone Standard.



- The Customer 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:
 - ✓ Microsoft 365 E5
 - ✓ Any Microsoft 365 Plan (for example, E1 or E3) with Microsoft Teams Phone Standard licenses
- The SQL database can be configured to support other license types upon request sent to AudioCodes Professional Services.

Setup Two-step Provisioning

Two-step provisioning adds the new customer sub domain 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 sub domain and adds it under the **Custom** domains on Azure. This method requires the creation of a sub domain on the DNS hosting

platform which must be then be configured on the UMP-365 Main Tenant interface in the DNS sub domain Mapping table.

➤ **Do the following:**

1. Open the customer DNS hosting platform and choose the desired sub domain.

Record Name	Type	Value	TTL	Action
NL-QA-UMP-221.activecommunications.eu	A	20.93.133.186	14400	X
officewebapps.activecommunications.eu	A	84.53.66.60	86400	X
ProTokenCust1.activecommunications.eu	A	23.97.197.54	14400	X
qa.activecommunications.eu	A	51.124.43.46	14400	X
sbc-tobi.activecommunications.eu	A	40.91.233.177	14400	X
sip.activecommunications.eu	A	84.53.66.61	86400	X
ump-access.activecommunications.eu	A	51.138.73.35	14400	X
ump-walter.activecommunications.eu	A	52.178.102.123	14400	X
wac.activecommunications.eu	A	84.53.66.60	86400	X
autodiscover.activecommunications.eu	CNAME	autodiscover.outlook.com	86400	X
transfer.activecommunications.eu	CNAME	acs-transfer.azureedge.net	3600	X
ump-tobi.activecommunications.eu	CNAME	ump-tobi.westeurope.cloudapp.azure.com	14400	X
www.activecommunications.eu	CNAME	www.audiocodes.com	86400	X
activecommunications.eu	MX	100 2007.activecommunications.eu	86400	X
activecommunications.eu	MX	50 activecommunications.eu.mail.protection.outlook.com	86400	X

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

System > DNS API Configuration

Tenant Id:

Client Id:

Client Secret:

Subscription Id:

Resource Group Name:

Dns Zone:

Apply Changes Reset Changes

Name	Sbc	FQDN	Ip Address		
Please enter a valid Name	51.124.68.108_SBC	customers.audiocodes.be	13.80.148.30		
Add	Reset Fqdn	Resolve Address			
#	Name	SbcId	Fqdn	Ip Address	Edit
11	APAC	1	pa.activecommunications.eu	13.80.148.30	Edit
12	EMEA	2	ea.activecommunications.eu	23.97.197.41	Edit
13	DEMOBRAD	3	qa.activecommunications.eu	51.124.43.46	Edit

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.

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.

Once the above configuration has been completed, the Onboarding wizard can be used to provision the DNS sub domains using the Two-step method (see [Two-step DNS Provisioning](#) on page 411).

Manual Provisioning

The manual provisioning of the Azure DNS is used predominantly for Hosted Essentials customers. It involves manual configuration on customer sites including the following actions:

- Registration of the customer sub domain on the Customer tenant (see [Registering Customer Tenant Subdomain](#) below).
- Adding a new record of the Customer Subdomain in the DNS Zone of the Service Provider tenant .
- Activation of the domain by activating a M365 user license on the customer tenant (see [Activating the Customer Domain](#) on page 258).

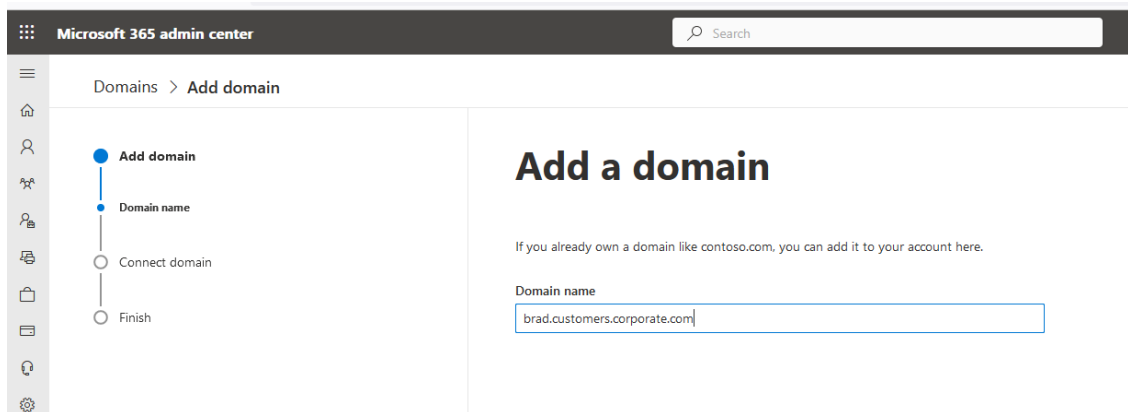
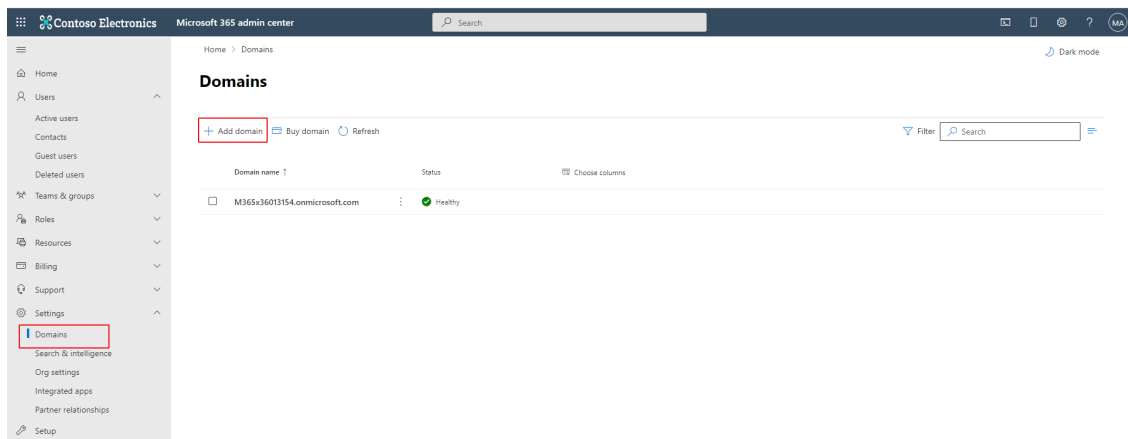
Registering Customer Tenant Subdomain

The registration of the customer Subdomain is performed in the Customer Microsoft 365 admin center and in the Service Provider tenant DNS Zone:

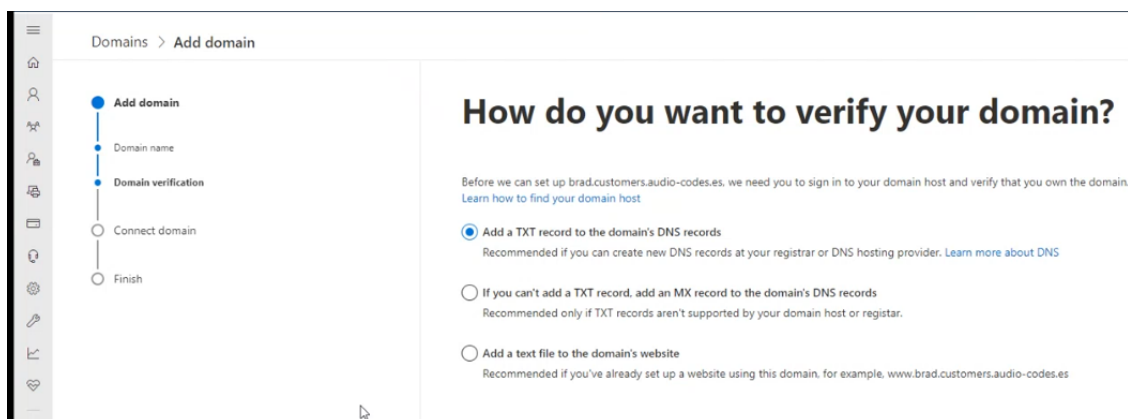
- The customer must generate a TXT record to validate with the Service Provider domain and an A-record to translate the customer site SBC shortname (configured in the Onboarding wizard) to its IP address and FQDN.
- The Service Provider must add the new record in the DNS Zone.

➤ To register a sub domain for customer tenant:

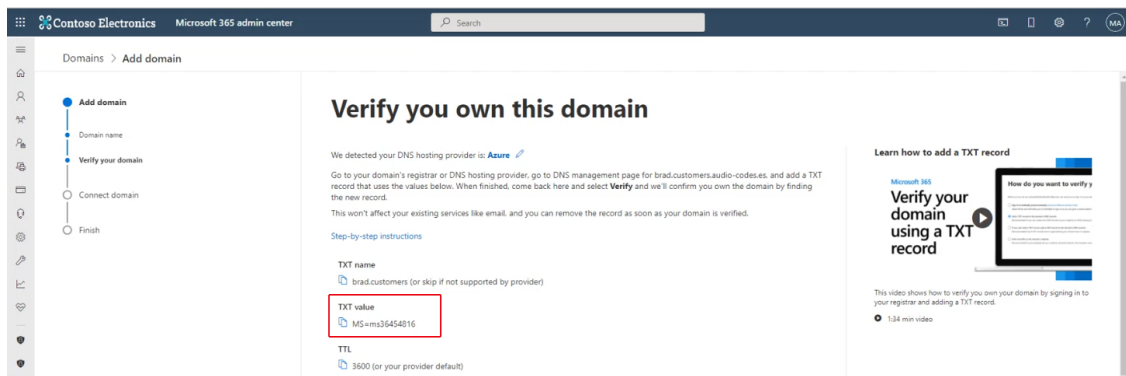
1. Login to the Microsoft 365 admin center with customer Tenant Admin permissions.
2. In the Navigation pane, select **Settings > Domains** and then click **Add a Domain**.



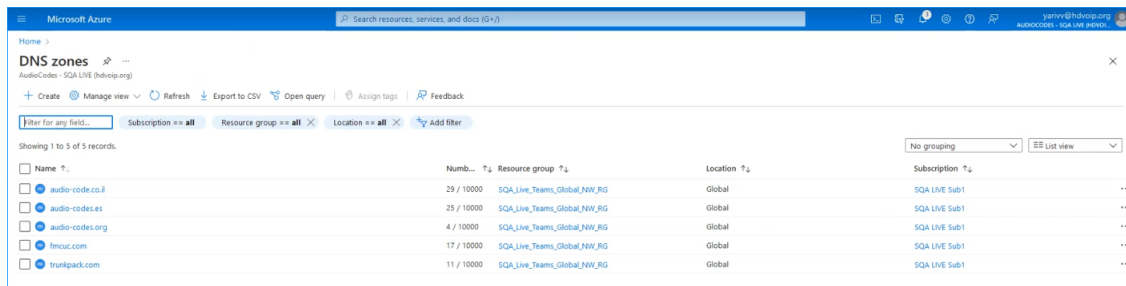
3. Enter the name for the customer subdomain e.g. brad.customers.corporate.com
4. Click **Use this domain**.



5. Select the “Add a TXT record to the domain’s DNS records” check box.



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



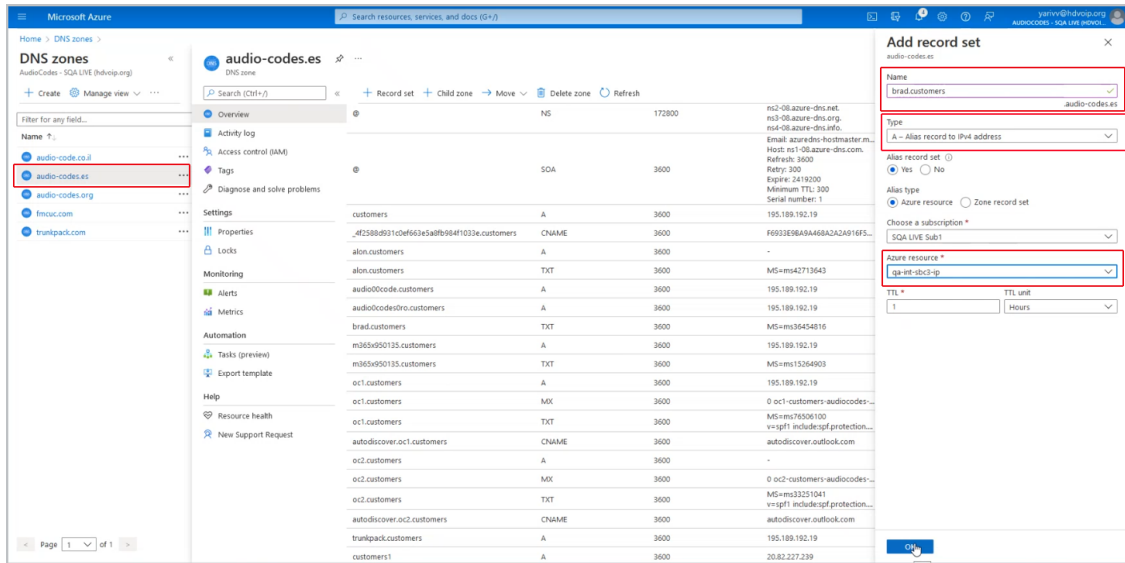
9. Select the relevant Service Provider Operator tenant DNS zone domain e.g. audio-codes.es and then add a record set for the customer's sub domain:
 - Enter the name of the customer domain.
 - In the Type drop-down list, select **TXT – Text** record type.
 - In the Value field, enter the TXT value that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

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.

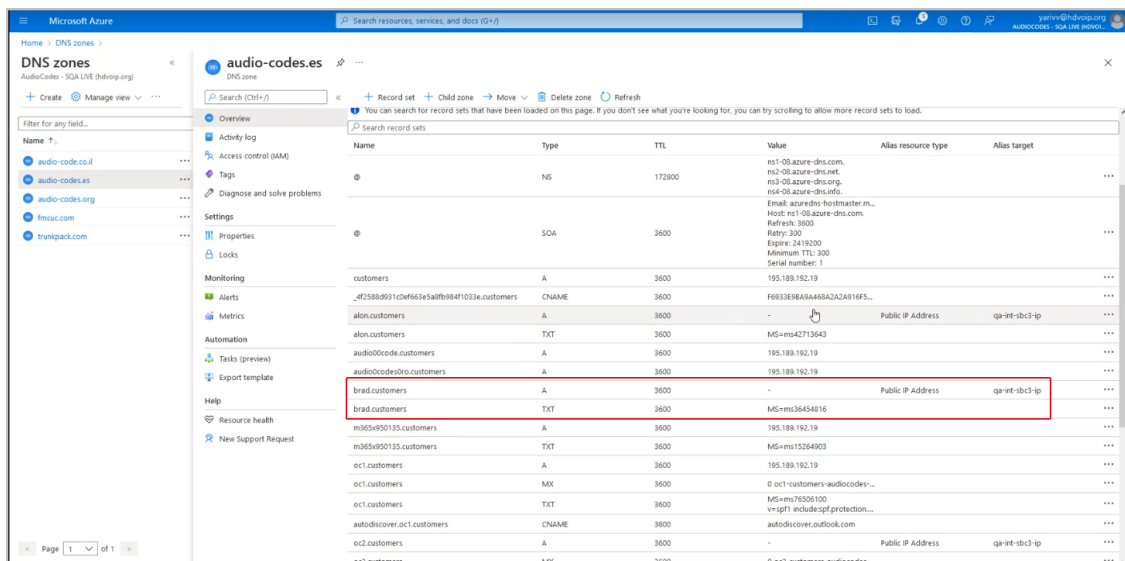
- Click **OK**.



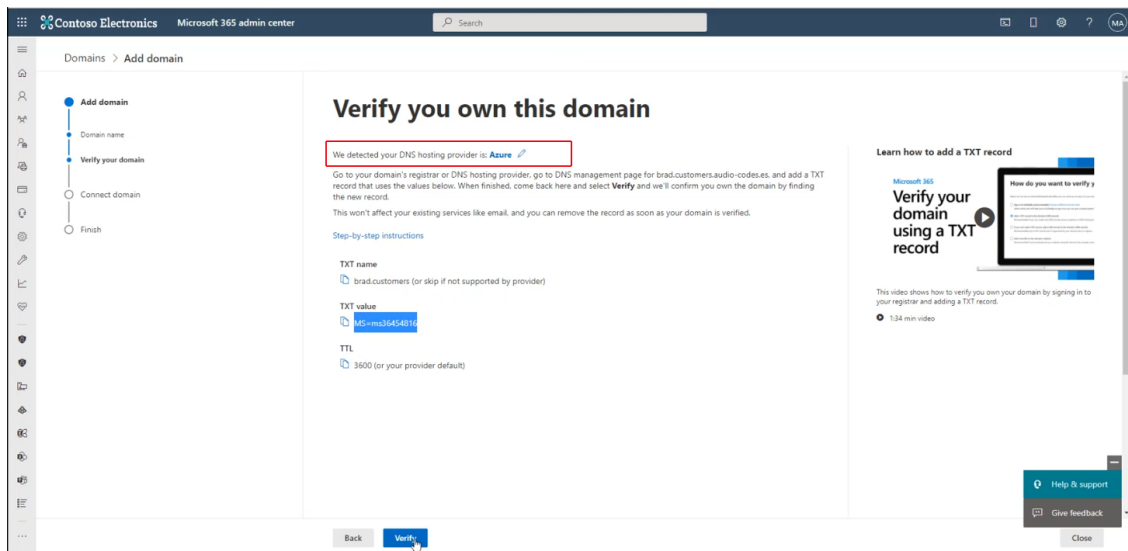
The following confirmation prompt is displayed.



The following figure displays the newly added records.

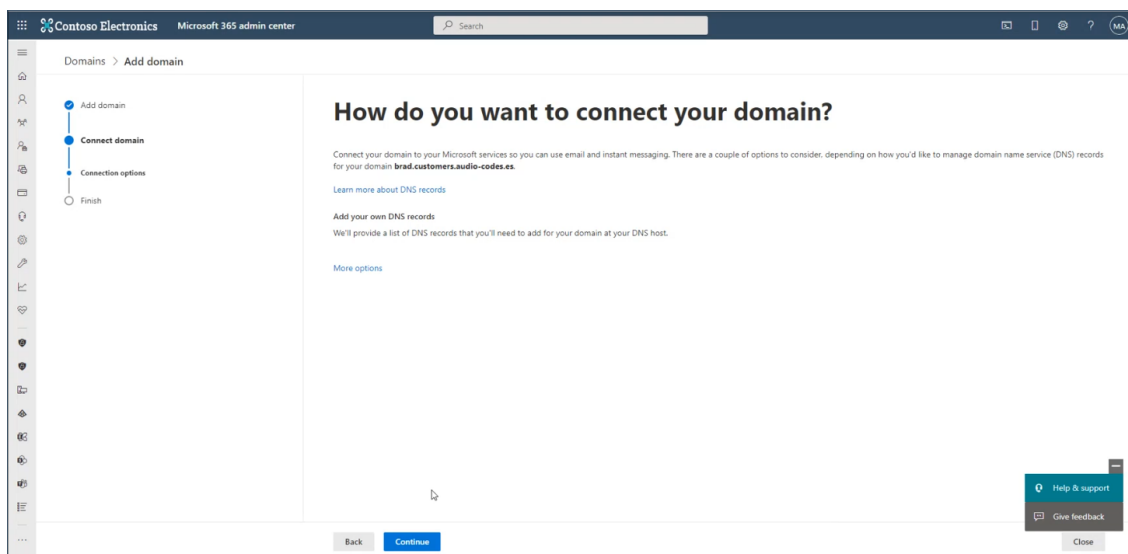


- Return to the Customer tenant Microsoft 365 admin center. Notice that the system has detected that the DNS hosting provider is on Azure.

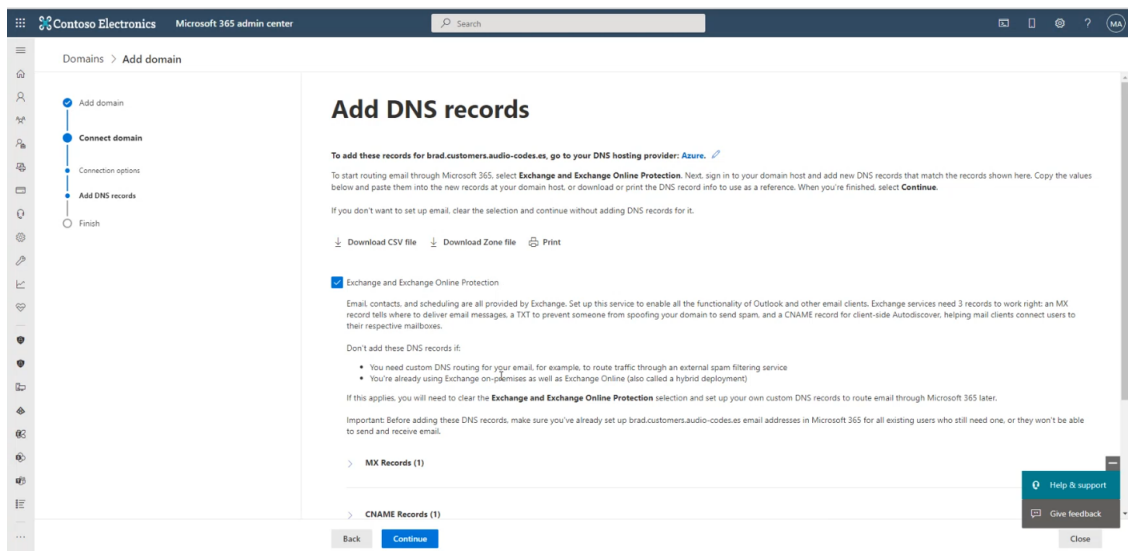


12. Click **Verify**.

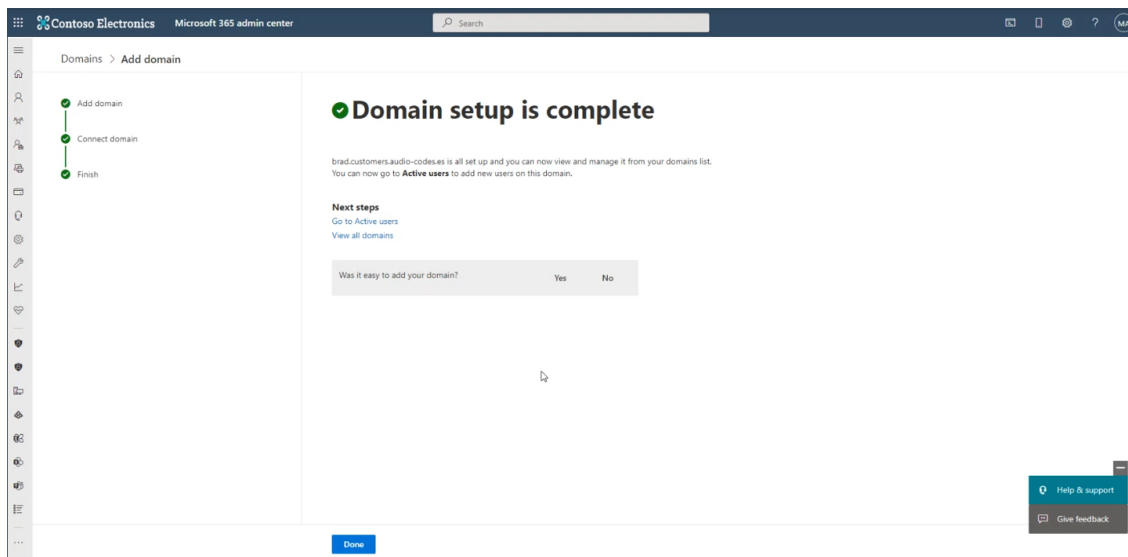
The customer's domain i.e. the Service Provider Operator domain audio-codes.es is verified.



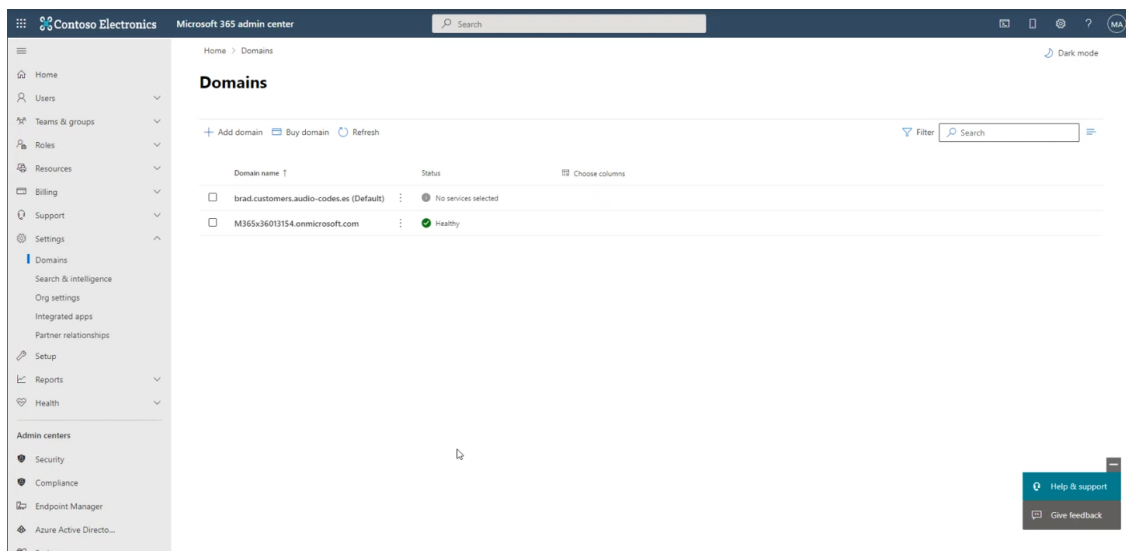
13. Click **Continue**.



14. Deselect the **Exchange and Exchange Online Protection** check box, and then click **Continue**.



15. Click **Done**.



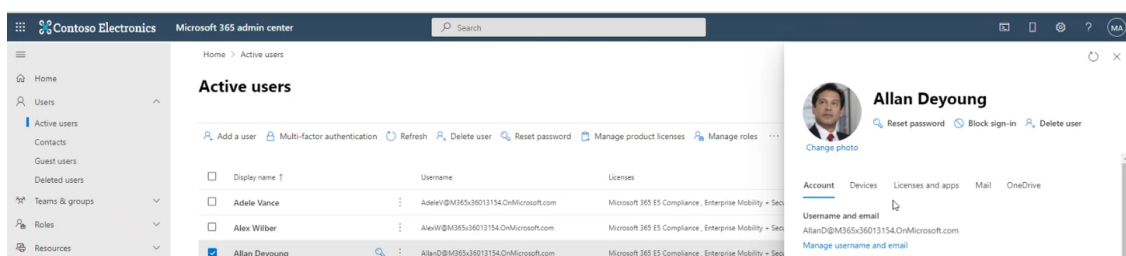
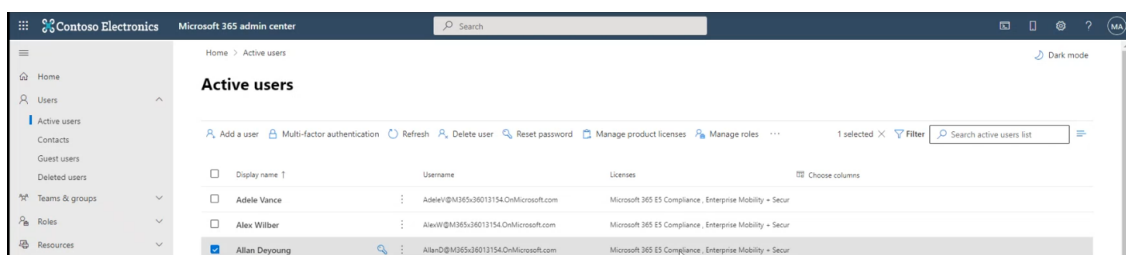
Activating the Customer Domain

Activate the new domain by adding a licensed user with a Phone System license to your new sub domain. The license can be revoked after the domain activation (this may take up to 24 hours). One of the following license types must be made available and then assigned to the Domain account:

- Office 365 E5
- Office 365 E1 / E3 with “Microsoft Teams Phone Standard

➤ To activate the customer domain:

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.



3. Select the **License and apps** tab.

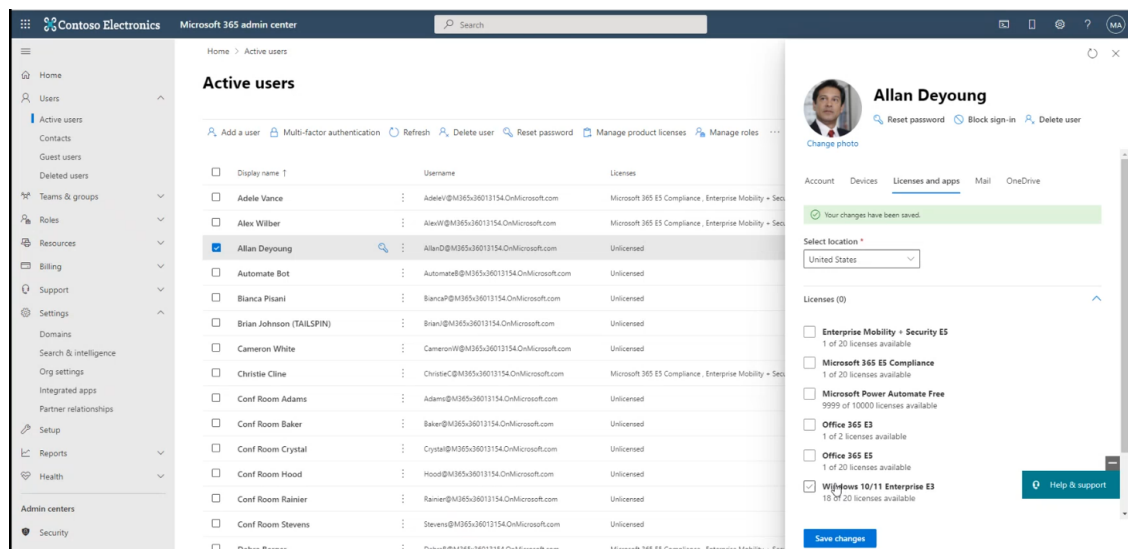
The first screenshot shows the 'Active users' page in the Microsoft 365 admin center. The user 'Allan Deyoung' is selected, and the 'Licenses and apps' tab is highlighted in the user profile sidebar.

The second screenshot shows the 'Licenses and apps' page for Allan Deyoung. The 'Licenses (3)' section shows three licenses assigned: 'Enterprise Mobility + Security E3', 'Microsoft 365 E3 Compliance', and 'Microsoft Power Automate Free'. The 'Save changes' button is visible at the bottom.

The third screenshot shows the 'Licenses and apps' page for Allan Deyoung after all licenses have been deselected. The 'Licenses (0)' section shows no licenses assigned. The 'Save changes' button is visible at the bottom.

4. Deselect all active licenses and then click **Save changes**.

A confirmation is displayed.



A free license is now available for assignment.

5. Add a new user. For example, 'LiveCloud DNS' and associate it to your new Domain. In the example below, the new domain is 'BradDRTest.sandbox3.audiocodes.be', and then click **Next**.

Add a user

Basics

Set up the basics

To get started, fill out some basic information about who you're adding as a user.

First name: UMPDNS Last name: [Empty]

Display name: UMPDNS

Username: UMPDNS Domain: M365x35340067.onmicrosoft.com

☒ Automatically create a password

☒ Require this user to change their password when they first sign in

☐ Send password in email upon completion

Next **Cancel**

6. Assign one of the product license types described above for the new user, and then click **Next**.

Add a user

Basics
Product licenses
Optional settings
Finish

Assign product licenses

Assign the licenses you'd like this user to have.

Select location *

United States

Licenses (2) *

- ☒ Assign user a product license
 - ☒ **Enterprise Mobility + Security E5**
2 of 20 licenses available
 - ☐ **Microsoft 365 E5 Compliance**
3 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 Microsoft 365 until you assign a product license.

Apps (70)

Back Next Cancel

7. Configure Optional Settings as required, and then click **Next**.

Contoso Electronics Microsoft 365 admin center

Home > Active users > Add a user

Active users

Add a user

Basics
Product licenses
Optional settings
Finish

Optional settings

You can choose what role you'd like to assign for this user, and fill in additional profile information.

Roles (User: no administration access)

Profile info

Back Next Cancel

Help & support

8. Click **Finish** adding.

Add a user

- Basics
- Product licenses
- Optional settings
- Finish**

Review and finish

Assigned Settings
Review all the info and settings for this user before you finish adding them.

Display and username
UMPDNS
UMPDNS@M365x35340067.onmicrosoft.com
[Edit](#)

Password
Type: Auto-generated
[Edit](#)

Product licenses
Location: United States
Licenses: Enterprise Mobility + Security E5
Apps: Microsoft 365 Audit Platform, Microsoft Defender for Identity, Microsoft Defender for Cloud Apps, 7 more
[Edit](#)

Roles (default)
User (no admin center access)
[Edit](#)

Profile info
[Edit](#)

[Back](#) [Finish adding](#) [Cancel](#)

9. Click **Close**; the new user is created and associated with the new domain.

Add a user

- Basics
- Product licenses
- Optional settings
- Finish**

UMPDNS added to active users

UMPDNS will now appear in your list of active users.

User details
Display name: UMPDNS
Username: UMPDNS@M365x35340067.onmicrosoft.com
Password: Zt59434

Licenses bought
None

Licenses assigned
Enterprise Mobility + Security E5

Save these user settings as a template?

User templates allow you to quickly add similar users in the future by saving a set of shared settings such as domain, password, product licenses, and roles.

[Review settings for this user template](#)

Name your template *

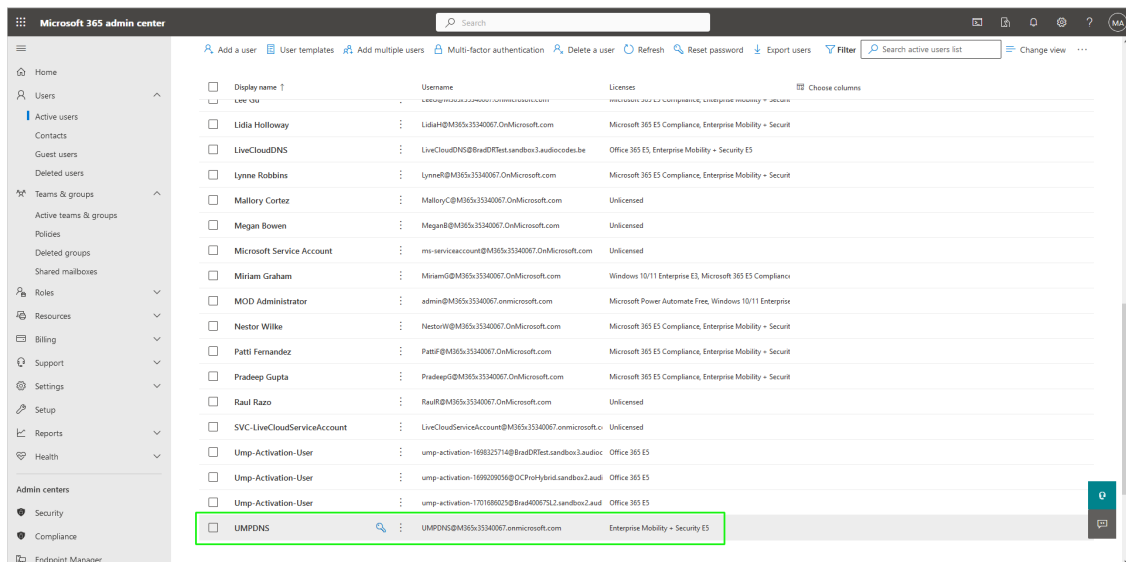
Example: FTE Senior Engineer, New York

Add a description (recommended)

Example: Template for full-time senior engineers in New York office

[Close](#)

The details of the new user are displayed.



End Customer Prerequisites

Customers must prepare their environment for the Token authentication process and DNS record creation which is part of the customer Onboarding procedure:

- Verify that at least one M365 license is available (see [Verify License Availability](#) below)
- Create a Service account to be used for Onboarding and Background Synchronization (see [Create Customer Administrator Service Account](#) on page 265)
- Configure additional Security settings (see [Configure Additional Security Settings](#) on page 274)
- Provide consent to Service Provider to access M365 platform (see [Request Consent from End Customer](#) on page 364)

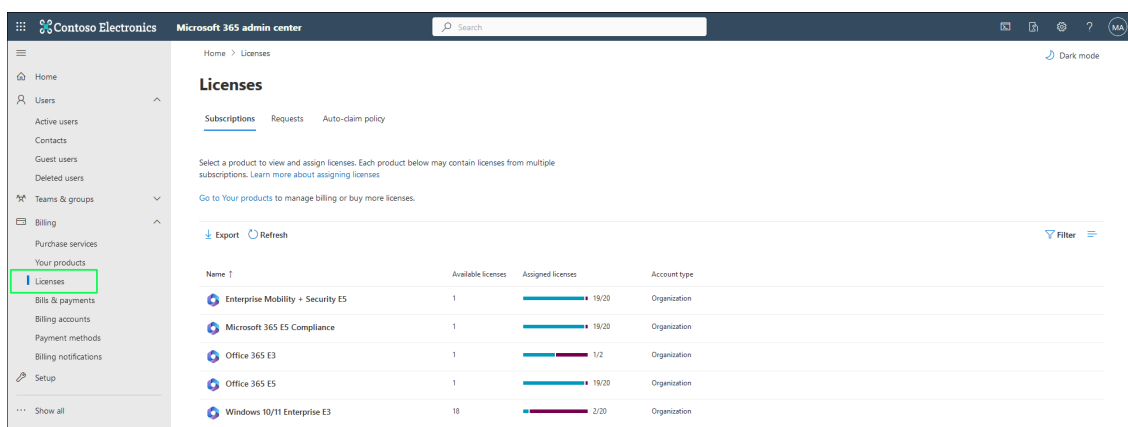
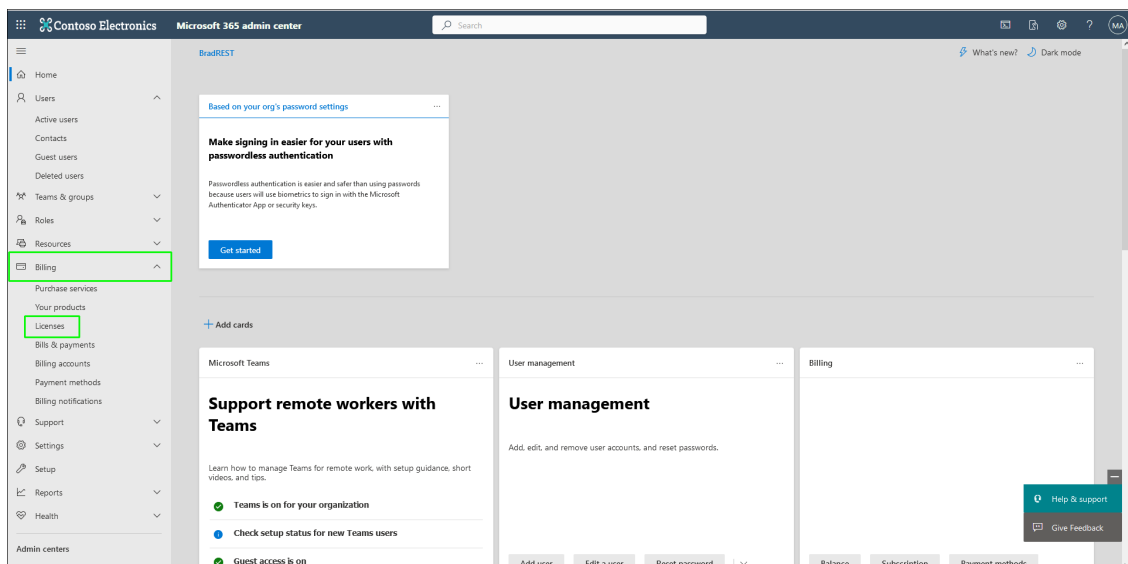
Verify License Availability

An M365 license is required for activating the PSTN trunk (customer sub domain). When the new customer is added, a unique User Management Pack™ 365 SP Edition portal URL is created for the customer with their own sub domain name (based on Customer Short Name defined in the Onboarding). This sub domain is configured on the Service Provider's DNS server. Activation of the sub domain requires an available M365 license which is applied during the Onboarding as part of the Automatic DNS provisioning process (see [Onboarding Customers](#) on page 282). You must verify that you have at least one of the following licenses available:

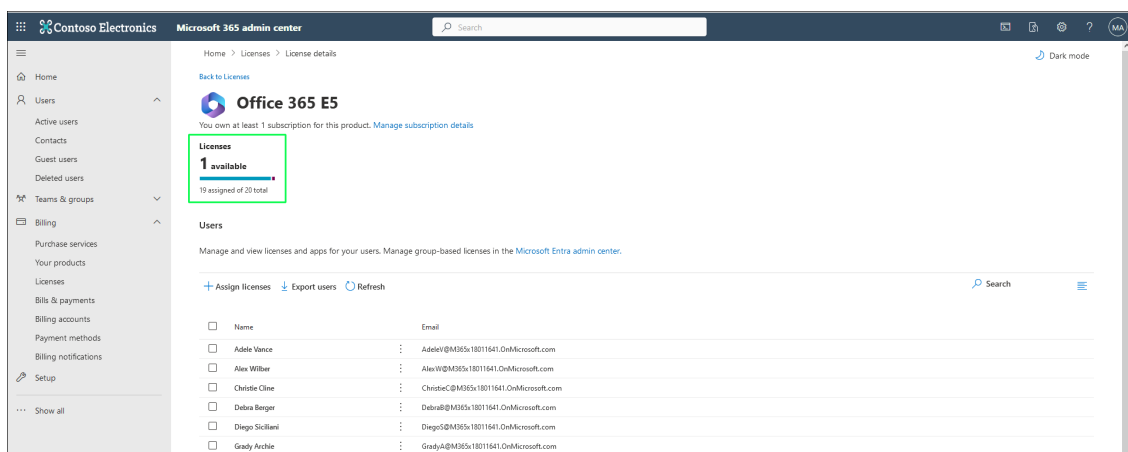
- Office 365 E5
- Office 365 E1 / E3 with "Microsoft Teams Phone Standard"

➤ To verify license availability:

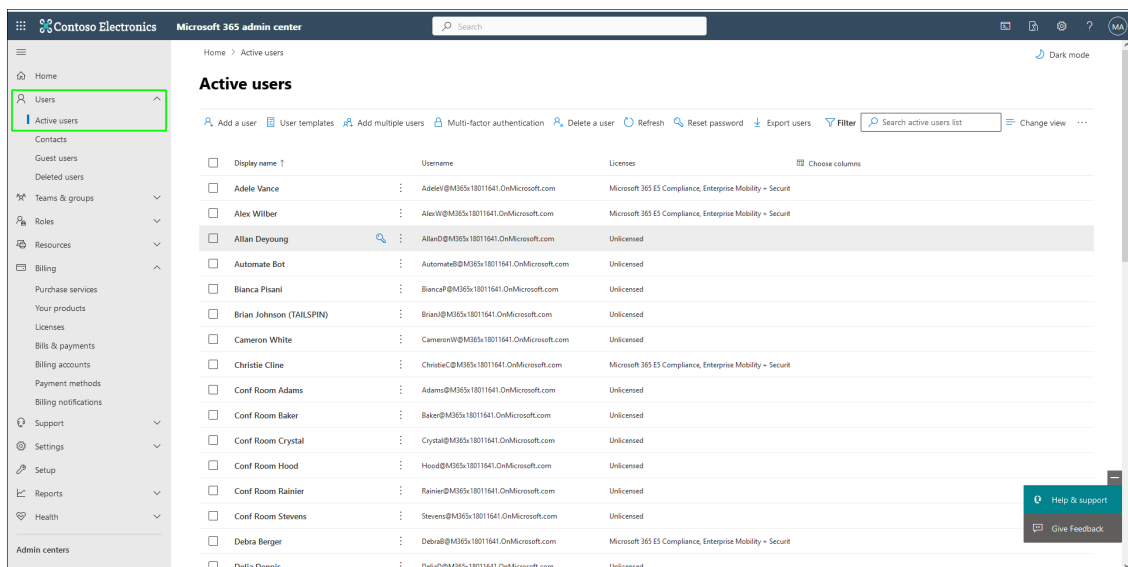
1. Open the Microsoft Admin portal with Global permissions (<https://admin.microsoft.com>).
2. In the Navigation pane, select **Billing > Licenses**.



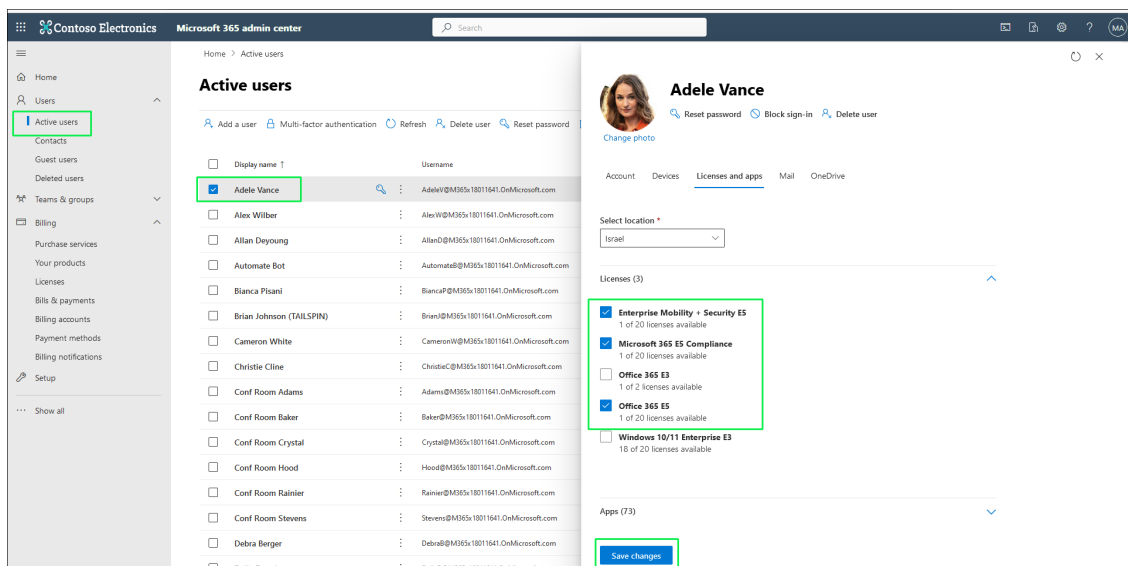
3. Verify that there is at least 1 license is available.



4. If a license is not available, in the Navigation pane, select Users > Active Users.



5. Select any existing Domain user, disable all active licenses for this user and then click **Save changes**.



Create Customer Administrator Service Account

This procedure describes how to create a M365 user to use as the User Management Pack™ 365 SP Edition Service account for customer Onboarding and database synchronization instead of using the default Global admin. User Management Pack™ 365 SP Edition requires an M365 User account to connect to the customer's M365 platform. The credentials for this account must be provided during the Onboarding process. User Management Pack™ 365 SP Edition can then perform sync actions, such as configuration of M365 Voice Routing templates and for retrieving updates from the M365 platform e.g. when new employees are added to the Active Directory. This connection is secured using Token authentication which is established using the credentials of this account.



Microsoft enforces Token authentication for connecting to M365. This user does not require a license.

➤ **To create M365 account:**

1. Log in to M365 Admin platform with Customer Admin permissions: <https://admin.microsoft.com/>.
2. In the Navigation pane, select **Active Users** and then click **Add a user**.

The screenshot shows the Microsoft 365 Admin Center interface. The left navigation pane has 'Active users' highlighted. The main area shows a table of active users with columns for Display name, Username, and Licenses. Below the table, the 'Add a user' form is displayed, showing the 'Basics' tab selected. The form fields include First name, Last name, Display name, Username, and Domains. The 'Username' field is populated with 'UMP365ServiceAccount' and the 'Domains' dropdown is set to 'M365x35340067.onmicrosoft.com'. The 'Automatically create a password' and 'Require this user to change their password when they first sign in' checkboxes are checked.

Display name	Username	Licenses
Adele Vance	Adelev@M365x18011641.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Security
Alex Wilber	AlexW@M365x18011641.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Security
Allan Deyoung	AllanD@M365x18011641.OnMicrosoft.com	Unlicensed

Add a user

Basics

Set up the basics

To get started, fill out some basic information about who you're adding as a user.

First name: UMP365ServiceAccount

Last name:

Display name *: UMP365ServiceAccount

Username *: UMP365ServiceAccount

Domains: @ M365x35340067.onmicrosoft.com

☒ Automatically create a password

☒ Require this user to change their password when they first sign in

☐ Send password in email upon completion

Next **Cancel**

3. Enter the details of the Service account, and then click **Next**.

The screenshot shows the 'Add a user' wizard in the Microsoft 365 admin center. The 'Product licenses' step is active. On the left, a progress bar shows 'Basics' completed, 'Product licenses' in progress, and 'Optional settings' and 'Finish' pending. The main area is titled 'Assign product licenses' with the instruction 'Assign the licenses you'd like this user to have.' Below this is a 'Select location' dropdown set to 'United States' and a 'Licenses (0)' section. Under 'Licenses (0)', there are several options with checkboxes: 'Enterprise Mobility + Security E5' (2 of 20 licenses available), 'Microsoft 365 E5 Compliance' (3 of 20 licenses available), 'Microsoft Power Automate Free' (9999 of 10000 licenses available), 'Office 365 E3' (1 of 2 licenses available), 'Office 365 E5' (with a note about trial subscription), and 'Windows 10/11 Enterprise E3' (18 of 20 licenses available). At the bottom of this list is the option 'Create user without product license (not recommended)' which is selected with a radio button. A note below it states: 'They may have limited or no access to Microsoft 365 until you assign a product license.' At the bottom of the wizard are 'Back', 'Next', and 'Cancel' buttons.

4. Click the **Create user without product license** and then click **Next**.

The screenshot shows the 'Add a user' wizard in the Microsoft 365 admin center, now at the 'Optional settings' step. The progress bar on the left shows 'Basics' and 'Product licenses' completed, 'Optional settings' in progress, and 'Finish' pending. The main area is titled 'Optional settings' with the instruction 'You can choose what role you'd like to assign for this user, and fill in additional profile information.' Below this are two dropdown menus: 'Roles (User: no administration access)' and 'Profile Info'. At the bottom of the wizard are 'Back', 'Next', and 'Cancel' buttons.

5. Configure Optional Settings if required, and then click **Next**.

Add a user

- Basics
- Product licenses
- Optional settings
- Finish**

Review and finish

Assigned Settings
Review all the info and settings for this user before you finish adding them.

Display and username
UMP365ServiceAccount
UMP365ServiceAccount@M365x35340067.onmicrosoft.com
[Edit](#)

Password
Type: Auto-generated
[Edit](#)

Product licenses
Create user without product license.

Roles (default)
User (no admin center access)
[Edit](#)

Profile info
[Edit](#)

[Back](#)
[Finish adding](#)
[Cancel](#)

6. Click **Finish adding**.

Add a user

- Basics
- Product licenses
- Optional settings
- Finish**

UMP365ServiceAccount added to active users

UMP365ServiceAccount will now appear in your list of active users.

User details
Display name: UMP365ServiceAccount
Username: UMP365ServiceAccount@M365x35340067.onmicrosoft.com
Password: M@198504107438uy

Licenses bought
None

Licenses assigned
None

Save these user settings as a template?

User templates allow you to quickly add similar users in the future by saving a set of shared settings such as domain, password, product licenses, and roles.

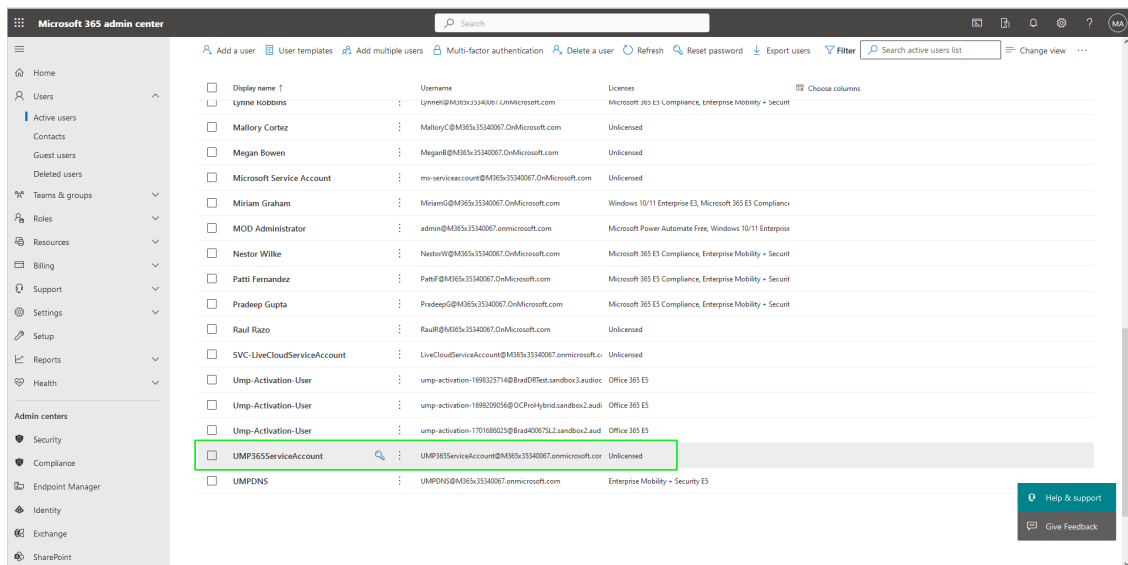
[Review settings for this user template](#)

Name your template *

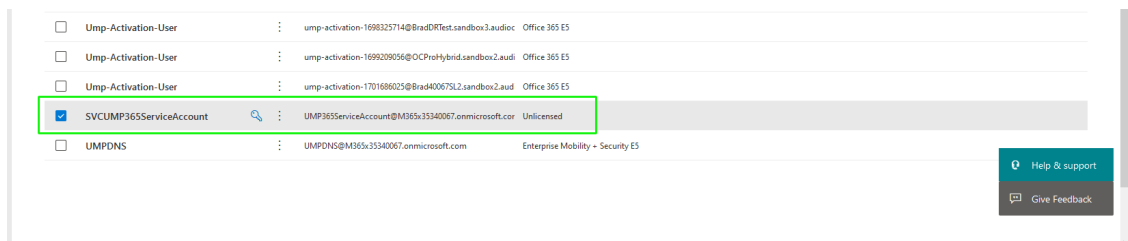
Add a description (recommended)

[Close](#)

7. Click **Close**. The new user is added.



8. Optional: Its recommended to add the "svc" to the username to distinguish your service account from your regular users.



Assign Administrator Roles to IT Administrator

The following Administrative roles must be granted to the customer Global IT administrator who grants consent to the Service Provider operator to connect to the customer Microsoft 365 platform for performing Background synchronization:

- Application Administrator (used for Token Authentication)
- Skype for Business Admin (Mandatory)
- Teams Communications Administrator (Mandatory)

For Fully Automatic DNS provisioning, the following roles must also be configured:

- Domain Name Administrator (for Txt and A-record generation)
- User Administrator (for creating the User Management Pack™ 365 SP EditionM365 Activation user)



- If you don't wish to configure the 'Application Administrator' permission, then you will be prompted to provide consent when running the Token Authentication wizard (see [Secure Token Connection with Service Account Credentials](#) on page 311).
- Skype for Business and Teams Communication roles are mandatory roles.
- User Admin and Domain Name Admin are only required if you are using Fully Automatic DNS provisioning of the customer sub domain during the Onboarding process.
- 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. Open the Azure Active Directory.
3. In the Users screen, choose the user who will have the role to grant consent in the organization.

Microsoft Azure portal showing the 'Users | All users' page. The page lists two users: 'mike o'brian' and 'TeamsITUser'. The 'TeamsITUser' is highlighted with a red circle.

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.com		
TeamsITUser	TeamsITUser@ocshost.o...	Member	No	Yes	OCSHOST.onmicrosoft.com		

Microsoft Azure portal showing the 'TeamsITUser | Profile' page. The 'Assigned roles' tab is selected and highlighted with a red box.

TeamsITUser
TeamsITUser@ocshost.onmicrosoft.com

User Sign-ins: 0

Group memberships: 0

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

Microsoft Azure portal showing the 'TeamsITUser | Assigned roles' page. The 'Add assignments' button is highlighted with a red box.

Administrative roles
Administrative roles can be used to grant access to Azure AD and other Microsoft services. [Learn more](#)

Search by name or description

Role	Description	Resource Name	Resource Type	Assignment Path	Type
No directory roles assigned.					

5. Click **Add assignments**.

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](#)

Search by name or description + Add filters

<input checked="" type="checkbox"/>	Application administrator	Can create and manage all aspects of app registrations and enterprise apps.
<input type="checkbox"/>	Application developer	Can create application registrations independent of the 'Users can register applications' setting.
<input type="checkbox"/>	Attack payload author	Can create attack payloads that an administrator can initiate later.
<input type="checkbox"/>	Attack simulation administrator	Can create and manage all aspects of attack simulation campaigns.
<input type="checkbox"/>	Attribute assignment administrator	Assign custom security attribute keys and values to supported Azure AD objects.
<input type="checkbox"/>	Attribute assignment reader	Read custom security attribute keys and values for supported Azure AD objects.
<input type="checkbox"/>	Attribute definition administrator	Define and manage the definition of custom security attributes.
<input type="checkbox"/>	Attribute definition reader	Read the definition of custom security attributes.
<input type="checkbox"/>	Authentication administrator	Has access to view, set, and reset authentication method information for any non-admin user.
<input type="checkbox"/>	Authentication policy administrator	Can create and manage all aspects of authentication methods and password protection policies.
<input type="checkbox"/>	Azure AD joined device local administrator	Users assigned to this role are added to the local administrators

Add

6. Add role “Application administrator”.

7. Add role “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.
-------------------------------------	----------------------------------	---

8. Add role “Teams communications administrator”.

Directory roles

↑ Sort

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

teams + Add filters

<input type="checkbox"/>	Teams administrator	Can manage the Microsoft Teams service.
<input checked="" 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.

9. Add role Domain Name Administrator.

Directory roles

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

Domain Name + Add filters

Role	Description
<input checked="" type="checkbox"/> Domain Name Administrator	Can manage domain names in cloud and on-premises.

Directory roles

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

User Administrator + Add filters

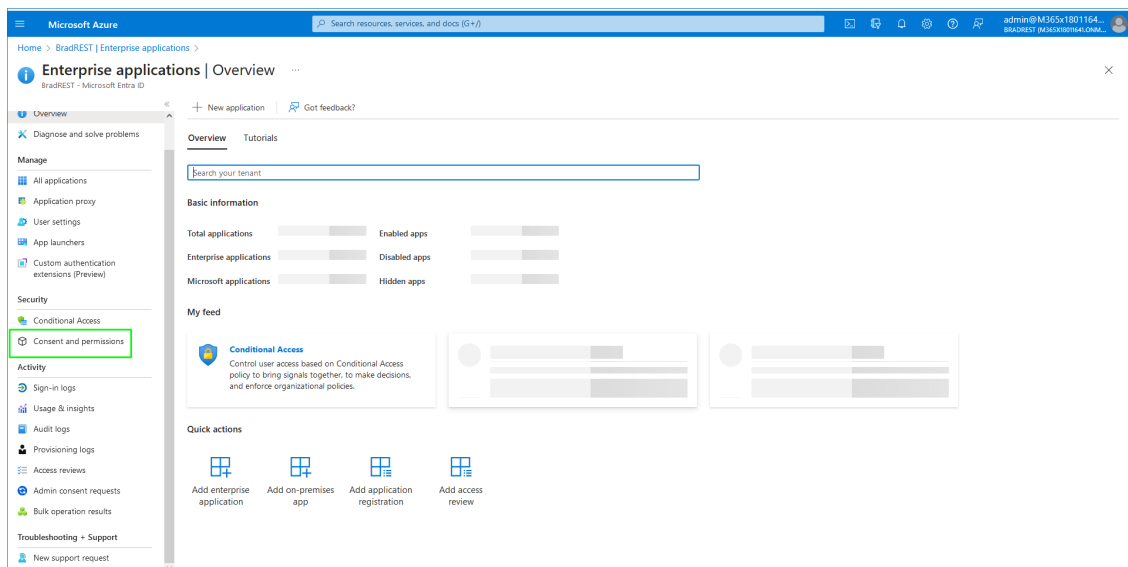
Role	Description
<input type="checkbox"/> Extended Directory User Administrator	Manage all aspects of external user profiles in the extended directory for Teams.
<input checked="" type="checkbox"/> User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.

The following screen displays all added admin roles.

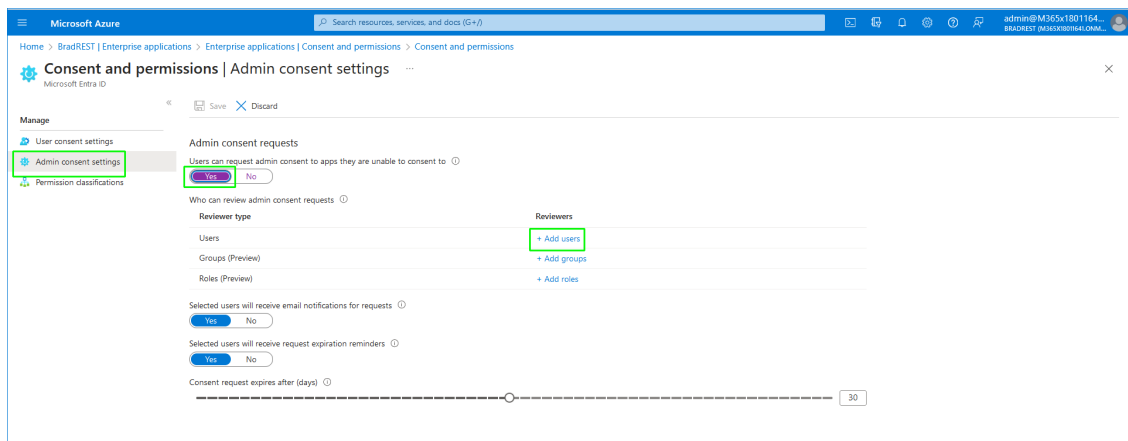
Administrative roles							
Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more							
Search by name or description		Add filters					
Role	Description	Resource Name	Resource Type	Assignment Path	Type		
<input type="checkbox"/> Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	Directory	Organization	Direct	Built-in		
<input type="checkbox"/> Domain Name Administrator	Can manage domain names in cloud and on-premises.	Directory	Organization	Direct	Built-in		
<input type="checkbox"/> Skype for Business Administrator	Can manage all aspects of the Skype for Business product.	Directory	Organization	Direct	Built-in		
<input type="checkbox"/> Teams Communications Administrator	Can manage calling and meetings features within the Microsoft Teams service.	Directory	Organization	Direct	Built-in		
<input type="checkbox"/> User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	Directory	Organization	Direct	Built-in		

10. The added User should be able to use "admin consent workflow" as an administrator (by default granted to the Global admin only):

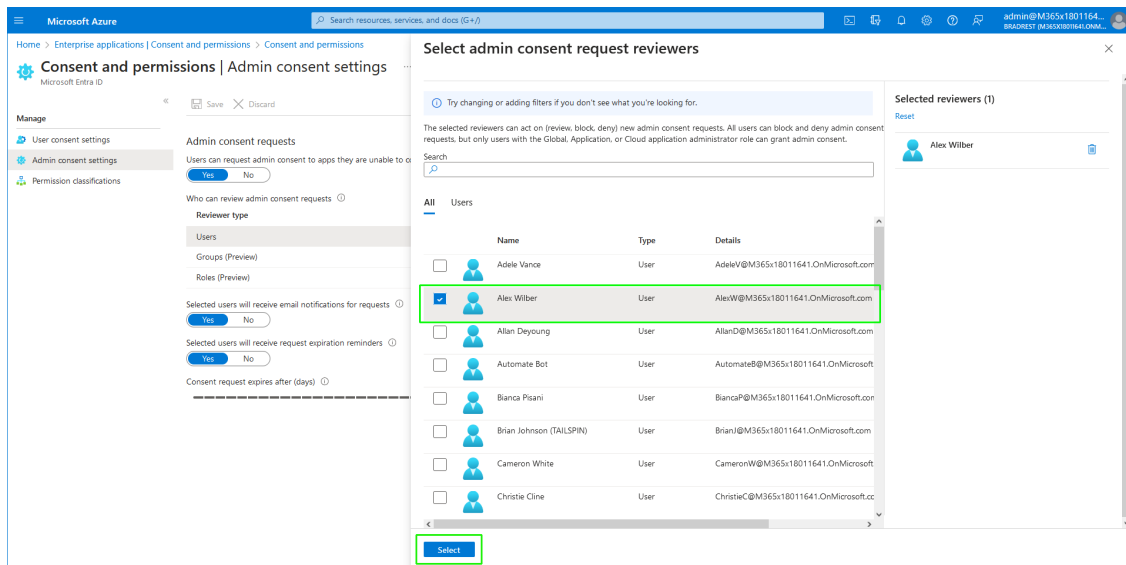
- a. Open the Enterprise Application and then in the Navigation pane, select **Consent and permissions**.



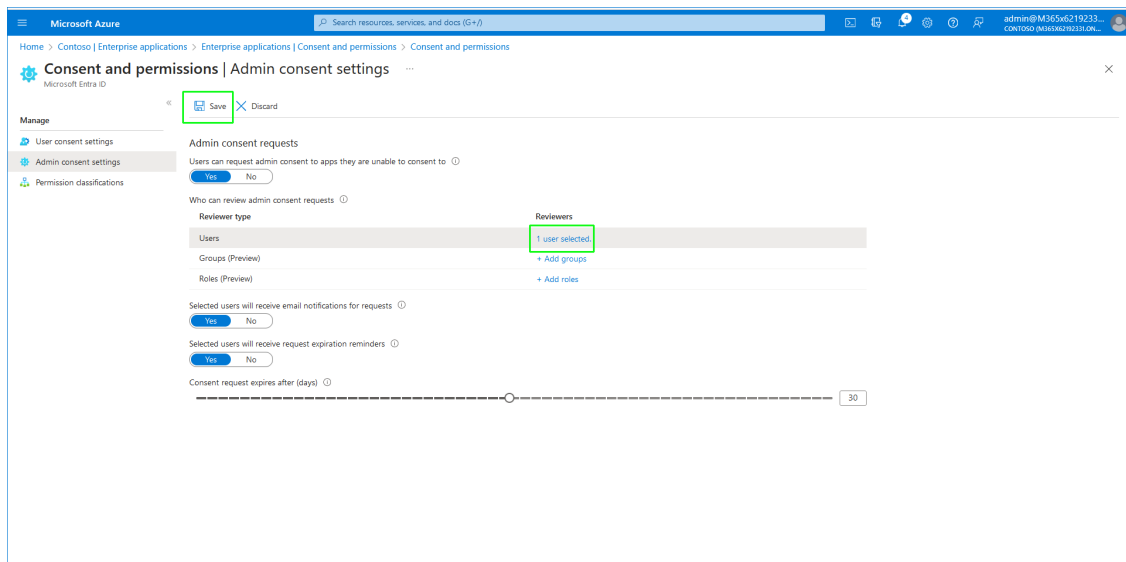
- b. Select the **Admin consent settings** tab.
- c. Select **Yes** for allowing users to request admin consents.



- d. Click **Add users**.



- e. Select the user of the Service account that you just added. The user is added.



11. Click **Save**.

Configure Additional Security Settings

It is highly recommended to implement the following security actions on the M365 platform prior to Onboarding:

- Exclude UMP Service account for all company Conditional access rules.
- Secure M365 with PIM (Privileged Identity Management).
- Ensure M365 authentication is performed using MFA.
- Provide Admin consent to the 'Enterprise application' that is used for the Background replication.

➤ **Do the following:**

1. Login to the Microsoft Entra admin center with Global Admin permissions.
2. The User Management Pack™ 365 SP Edition Service account should be excluded for all enterprise Conditional access rules according to Microsoft best practices by following Microsoft documentation: "How to create an exclusion group in a Conditional Access policy". See example figure below showing user exclusion for a conditional access rule.

Microsoft Azure

Home > Conditional Access | Overview >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

ExclusionPolicy ✓

Assignments

Users ⓘ

All users included and specific users excluded

Target resources ⓘ

No target resources selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

Include **Exclude**

Select the users and groups to exempt from the policy

☐ Guest or external users ⓘ

☐ Directory roles ⓘ

☒ Users and groups

Select excluded users and groups

1 user, 1 group

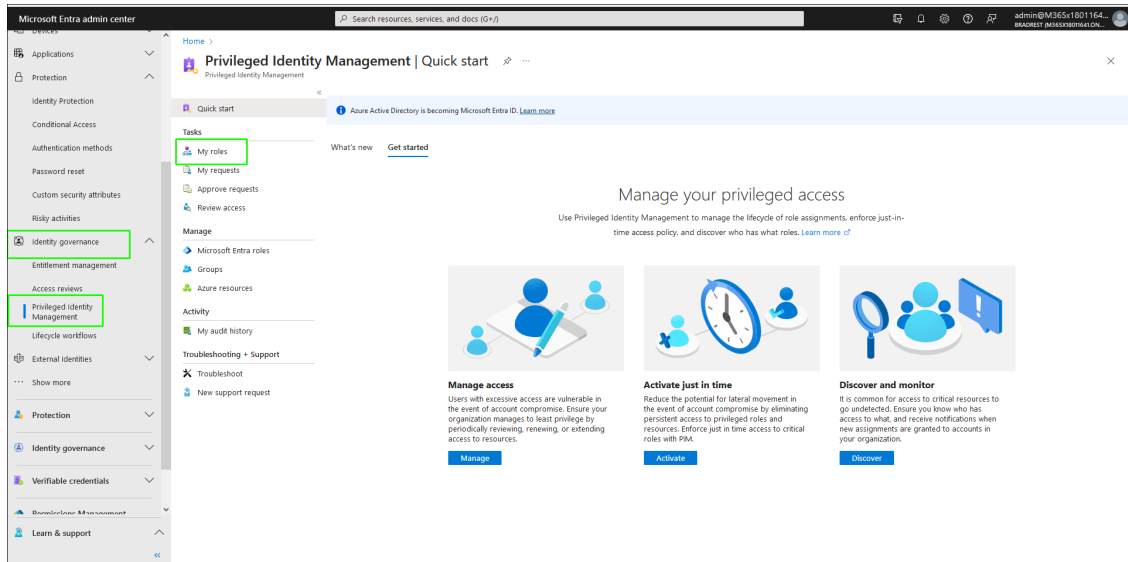
EX	ExclusionGroup	...
MA	MOD Administrator admin@M365x65686504.onm...	...

Enable policy

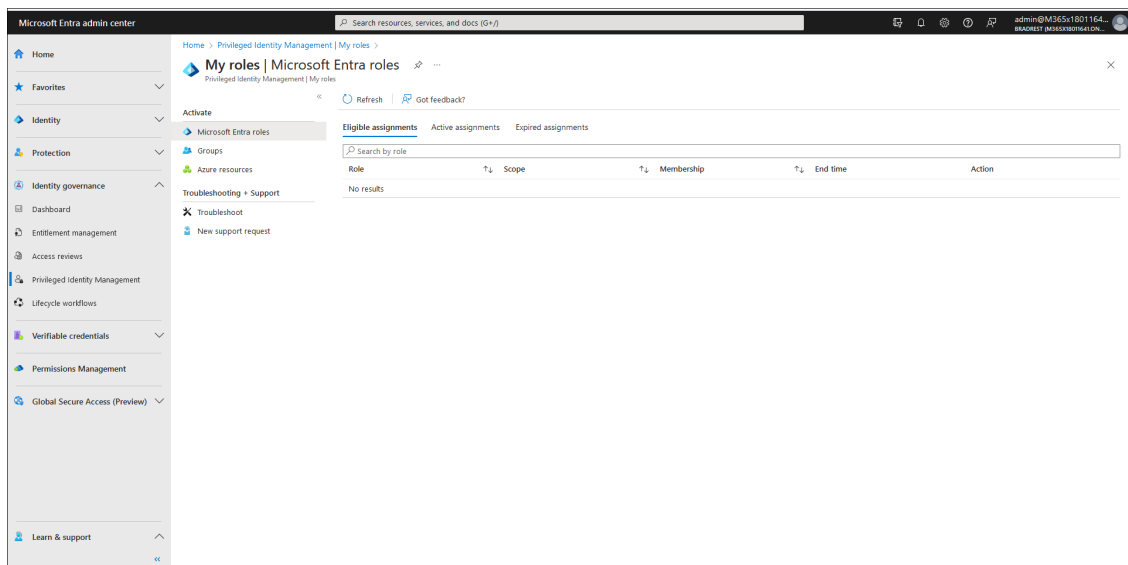
Report-only On Off

Create

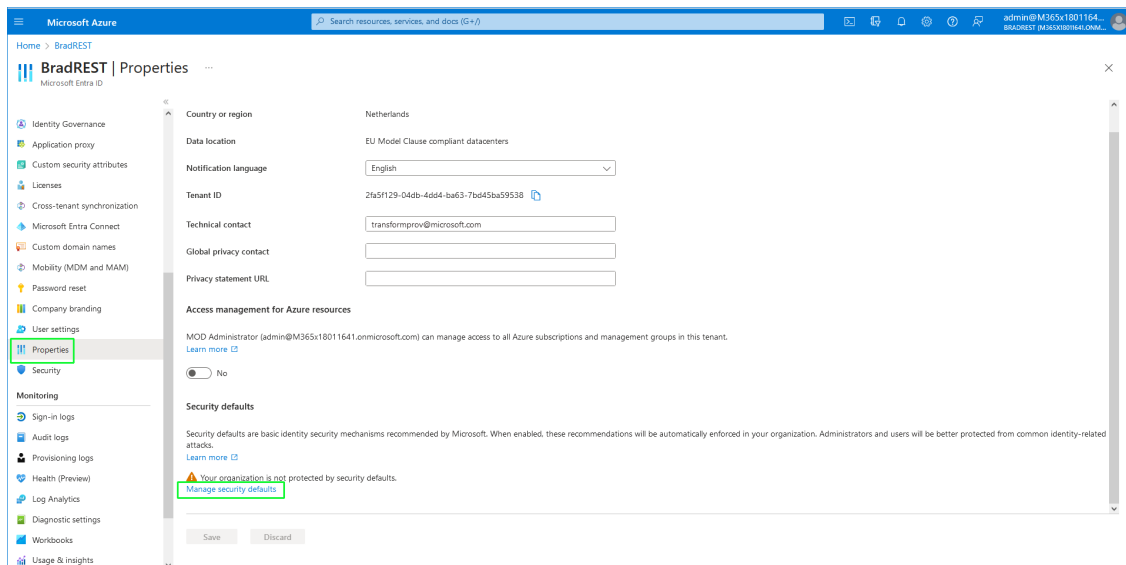
3. Verify that the M365 is secured with PIM (Privileged Identity Management), and ensure access for the Global user or Service Account to be used by User Management Pack™ 365 SP Edition. In addition, remove any rule related to PIM:
 - a. In the Navigation pane, select **Identity > Identity governance > Privileged Identity Management > My roles**.



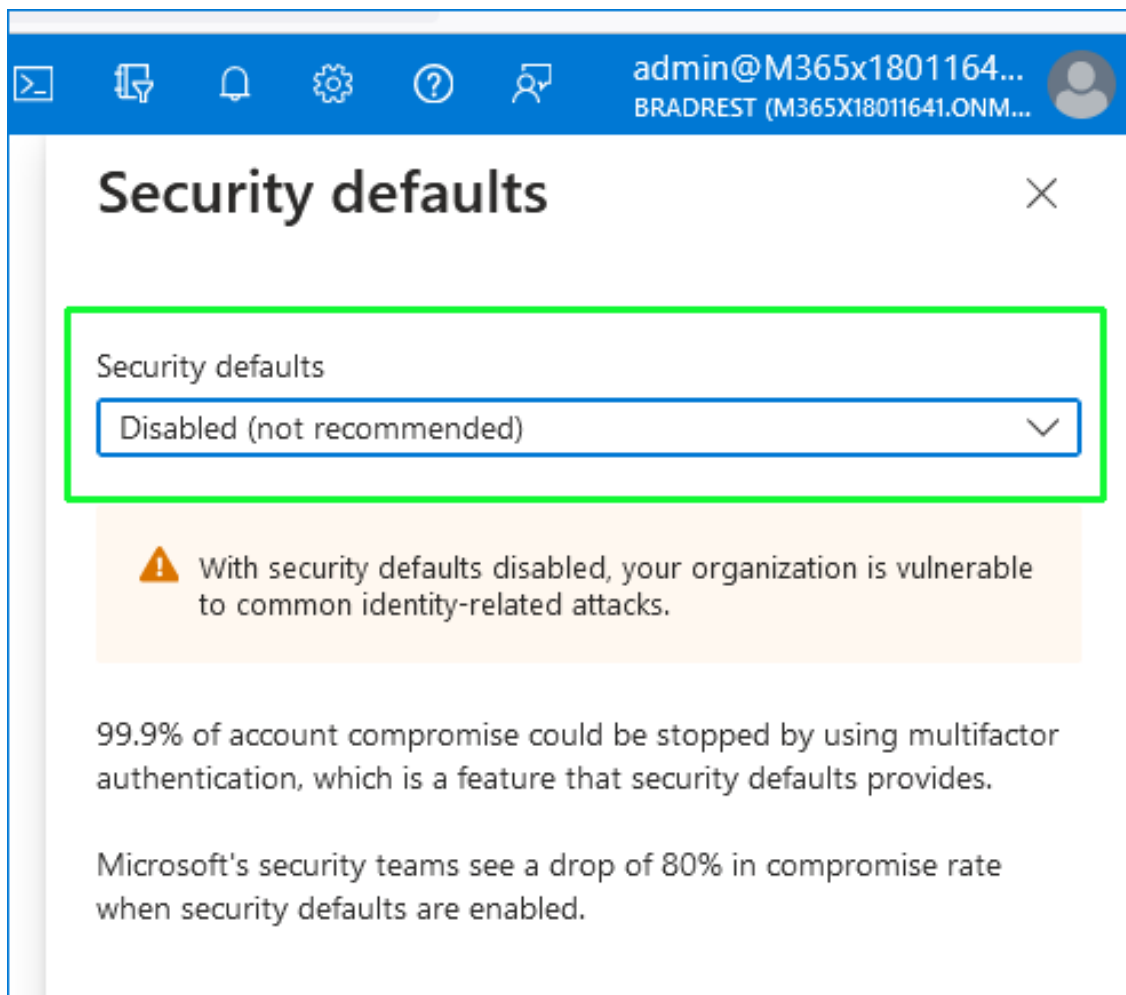
- b. Ensure that there are no active roles.



4. Ensure M365 authentication is performed using MFA (Multi-factor authentication) and not using plain user and password:
 - a. Open the Azure Active Directory portal.
 - b. In the Navigation pane, select **Properties**.
 - c. Select **Manage security defaults**.



- d. Ensure that Security defaults is set to **Disabled**.



Security defaults



Security defaults

Disabled



With security defaults disabled, your organization is vulnerable to common identity-related attacks.

99.9% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.

Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.

Reason for disabling *

This feedback will be used to improve Microsoft products and services. [View privacy statement](#)

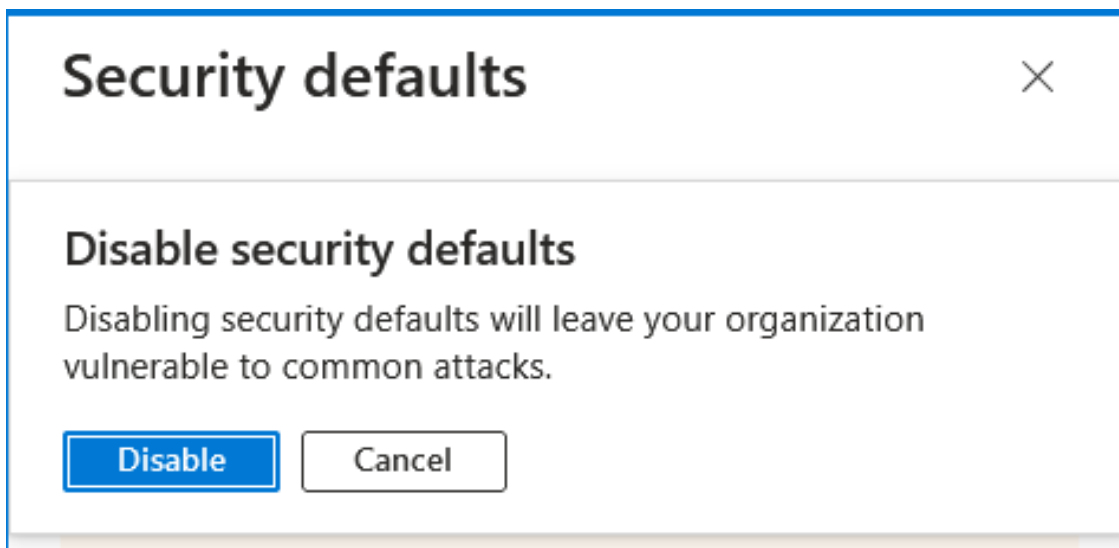
- ☐ My organization is using Conditional Access
- ☐ My organization is unable to use apps/devices
- ☒ Too many sign-in multifactor authentication challenges



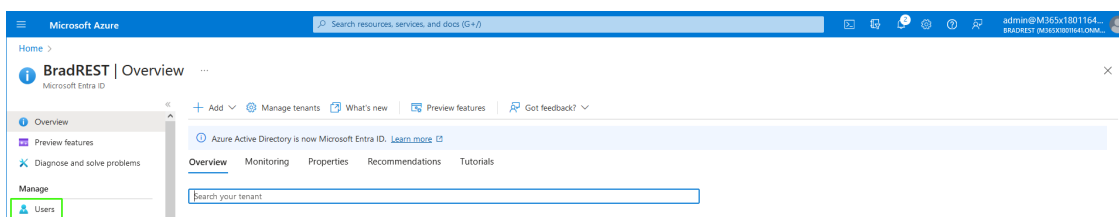
We recommend having separate accounts for administration and standard productivity tasks to significantly reduce the number of times your admins are prompted for multifactor authentication. [Learn more](#)

- ☐ Too many multifactor authentication sign-up requests
- ☐ Other

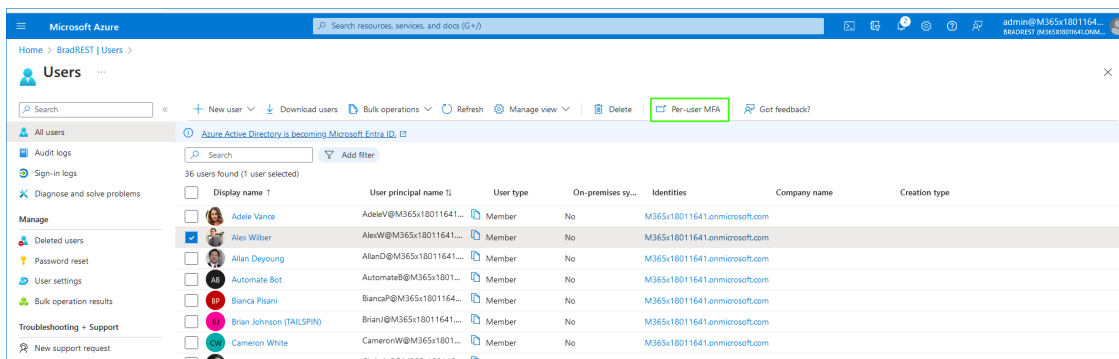
- e. Select a reason for disabling and then click **Save**.



- Perform action per user:
 - i. In the Navigation pane, select **Users**.



- ii. Select any user and then click **Per-user MFA**.



CONTOSO demo admin@M365x18011641.onmicrosoft.com | ?

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to license other users.](#)
Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users Multi-Factor Auth status: Any bulk update

<input type="checkbox"/>	DISPLAY NAME ^	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	Adele Vance	AdeleV@M365x18011641.OnMicrosoft.com	Disabled
<input checked="" type="checkbox"/>	Alex Wilber	AlexW@M365x18011641.OnMicrosoft.com	Disabled
<input type="checkbox"/>	Allan Deyoung	AllanD@M365x18011641.OnMicrosoft.com	Disabled
<input type="checkbox"/>	Automate Bot	AutomateB@M365x18011641.OnMicrosoft.com	Disabled
<input type="checkbox"/>	Bianca Pisani	BiancaP@M365x18011641.OnMicrosoft.com	Disabled
<input type="checkbox"/>	Brian Johnson (TAILSPIN)	BrianJ@M365x18011641.OnMicrosoft.com	Disabled

Alex Wilber

AlexW@M365x18011641.OnMicrosoft.com
9256 Towne Center Dr, Suite 400
+1 858 555 0110

quick steps

Enable

[Manage user settings](#)

iii. Select any user and then select **Enable** to enable MFA.

5. Provide Admin consent to the 'Enterprise application' that will be used for the Background replication (see [Deploy Synchronization Application](#) on page 91). This prerequisite is optional:

- In the Microsoft Entra admin center portal or Azure portal, navigate to **Applications > Enterprise applications > Permissions**.
- Click "grant admin consent for <CustomerTenant>".

Microsoft Entra admin center

Search resources, services, and docs (G+)

admin@M365x18011641.onmicrosoft.com

Home > Enterprise applications > All applications > Sandbox2-UMP-Token

Sandbox2-UMP-Token | Permissions

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Self-service

Custom security attributes

Security

Conditional Access

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Troubleshooting & Support

New support request

Permissions

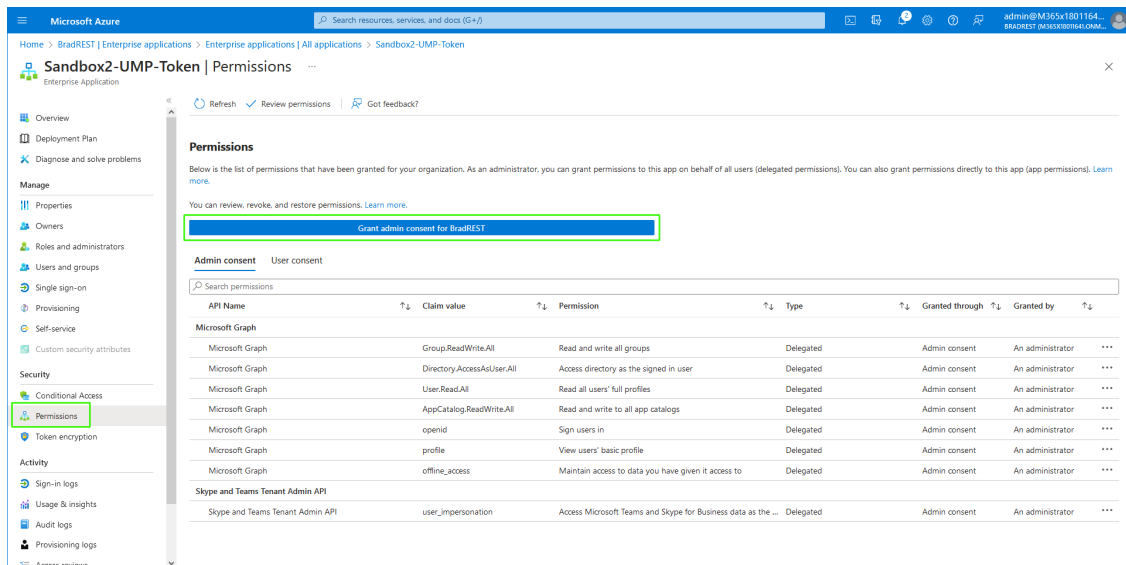
Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). [Learn more.](#)

You can review, revoke, and restore permissions. [Learn more.](#)

Grant admin consent for BroadEST

Admin consent User consent

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph	Group.ReadWrite.All	Read and write all groups	Delegated	Admin consent	An administrator
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed in user	Delegated	Admin consent	An administrator
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated	Admin consent	An administrator
Microsoft Graph	AppCatalog.ReadWrite.All	Read and write to all app catalogs	Delegated	Admin consent	An administrator
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	Admin consent	An administrator
Skype and Teams Tenant Admin API	user_impersonation	Access Microsoft Teams and Skype for Business da...	Delegated	Admin consent	An administrator



Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). [Learn more.](#)

You can review, revoke, and restore permissions. [Learn more.](#)

Grant admin consent for BradREST

Admin consent | User consent

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by	
Microsoft Graph						
Microsoft Graph	Group.ReadWrite.All	Read and write all groups	Delegated	Admin consent	An administrator	...
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed in user	Delegated	Admin consent	An administrator	...
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated	Admin consent	An administrator	...
Microsoft Graph	AppCatalog.ReadWrite.All	Read and write to all app catalogs	Delegated	Admin consent	An administrator	...
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator	...
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator	...
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	Admin consent	An administrator	...
Skype and Teams Tenant Admin API						
Skype and Teams Tenant Admin API	user_impersonation	Access Microsoft Teams and Skype for Business data as the ...	Delegated	Admin consent	An administrator	...



For any change in Enterprise application roles, make sure admin consent is applied.

31 Onboarding Customers

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

- Hosted Essentials (see [Onboarding with Hosted Essentials](#) below)
- Hosted Essentials + (see [Onboarding with Hosted Essentials +](#) on page 290)
- Hosted Pro (see [Onboarding with Hosted Pro](#) on page 361)

Onboarding with Hosted Essentials

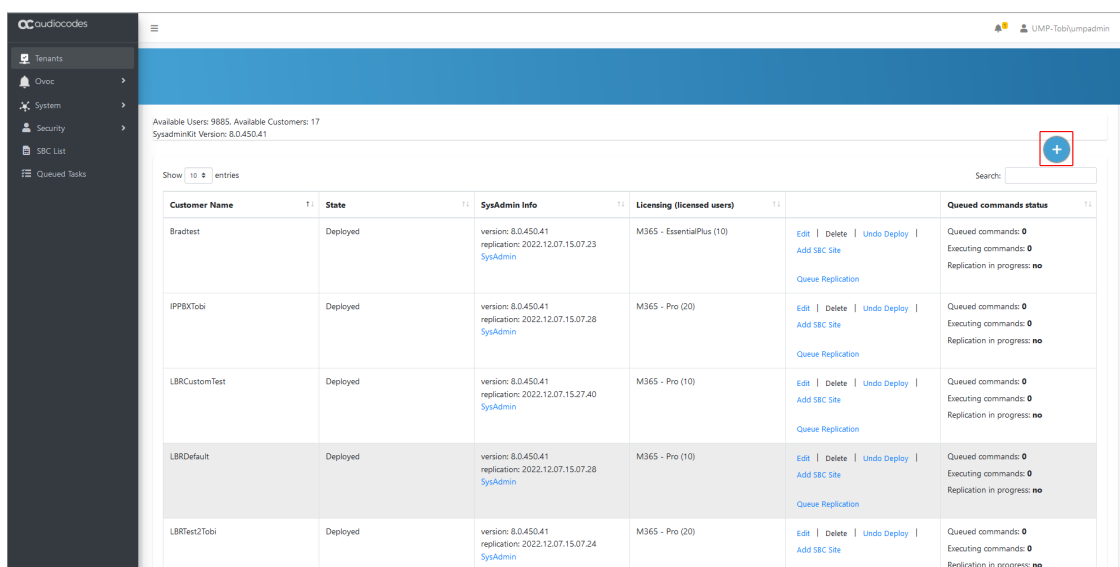
This section describes how to onboard new customers with “Hosted Essentials” licenses.



Connecting calls for Hosted Essentials customers requires the manual configuration of an SBC and Voice Routes in the Service Provider Teams admin center (see [Setting Up Hosted Essentials Customer](#) on page 288). For Hosted Essentials Plus customers and Hosted Pro customers, these entities are configured during the onboarding.

- To onboard a new “Hosted Essentials” customer:

1. In the Tenants page, click .



The screenshot shows the 'Tenants' page in the OCaudiocodes interface. The left sidebar contains navigation links: Tenants, Choc, System, Security, SBC List, and Queued Tasks. The main content area displays a table of tenants. Above the table, it states 'Available Users: 9885, Available Customers: 17' and 'SysAdminKit Version: 8.0.450.41'. A search bar is located at the top right of the table. A red box highlights a plus icon in the top right corner of the table area, indicating where to click to add a new tenant.

Customer Name	State	SysAdmin Info	Licensing (licensed users)	Queued commands status
Bradtest	Deployed	version: 8.0.450.41 replication: 2022.12.07.15.07.23 SysAdmin	M365 - EssentialPlus (10) Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
IPPBXTobi	Deployed	version: 8.0.450.41 replication: 2022.12.07.15.07.28 SysAdmin	M365 - Pro (20) Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
LBRCustomTest	Deployed	version: 8.0.450.41 replication: 2022.12.07.15.27.40 SysAdmin	M365 - Pro (10) Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
LBRCDefault	Deployed	version: 8.0.450.41 replication: 2022.12.07.15.07.28 SysAdmin	M365 - Pro (10) Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
LBRTTest2Tobi	Deployed	version: 8.0.450.41 replication: 2022.12.07.15.07.24 SysAdmin	M365 - Pro (20) Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no

The screenshot shows the 'live Cloud' dashboard with the 'CUSTOMERS' tab selected. A table of customers is displayed, including details like 'Full Name', 'Name', 'Service Type', 'Status', 'Deploy Status', 'License Type', 'Users Count', and 'Enabled'. A 'Customer Actions' dropdown menu is open, showing options such as 'Direct Routing', 'Compliance Recording', 'Zoom', and 'Operator Connect'. The 'Add Customer' option is highlighted. On the right, a 'Details' panel shows information for 'audiocodesru', including 'NAME', 'STATUS', 'DEPLOY STATUS', 'FULL NAME', 'SERVICE TYPE', 'LICENSE TYPE', 'AZURE TENANT ID', 'IS ENABLED', 'TOTAL NUMBER OF DIDS', 'USED DIDS', 'UNUSED DIDS', 'TENANT', and 'ACTIVE ALARMS'.

The 'SELECT TENANT' dialog box is shown. It has a title 'SELECT TENANT' and a dropdown menu labeled 'Tenant' with 'Provider1' selected. There are 'Close' and 'Select' buttons at the bottom right.

2.

- From the drop-down, select the desired tenant and then click **Select**.

The Onboarding interface opens.

The Onboarding interface is shown. It has a progress bar at the top with three steps: '1 M365 Tenant', '2 M365', and '3 Voice Route'. Below the progress bar, there are two large buttons: 'Add New Customer' and 'Pending Customers (2)'. At the bottom, there is a 'Reset' button and a session expiration timer showing 'Session expires in: 09:49'.

3.

3. Click Add New Customer.

The screenshot shows a multi-step form for adding a new customer. The header indicates the current step is '2 M365'. The form contains the following fields and options:

- Full Customer Name:** Text input field containing 'EssentialTrunk'.
- Short Customer Name:** Text input field containing 'EssentialTrunk'.
- License Type:** Three radio button options:
• ☒ Hosted Essential
• ☐ Hosted Essentials+
• ☐ Hosted Pro

Navigation buttons at the bottom right: 'Back' and 'Next'.

4.

4. Enter Full Customer M365 Tenant Name – Free Text.
5. Enter 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
6. Select the **Hosted Essential** License Type.

1 M365 Tenant

2 M365

3 Voice Route

×

Customer:

EssentialTrunk

☒ Configure SBC

Sbc Site Name

EssentialTrunk

Online PSTN Gateway

Online PstrnGateway

Sbc Configuration:

☒ Sip Trunk
☐ BYOC

Region

Select an SBC from list

Carrier

Select a Carrier from list

☐ Carrier Registration

☐ Enable Cac

Back

Next

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

Table 31-1: 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 Register End Customer Tenant DNS Sub domains on page 250).</p>
SBC Configuration	<p>Select one of the following SBC configuration modes:</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> SIP Trunk <input checked="" type="checkbox"/> BYOC
Region	Select the required SBC device according to site location IP address.
Carrier	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).

O365 Setting	Description
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.

1 M365 Tenant
2 M365
3 Voice Route
×

SBC number prefixes

No file selected.

+

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

1 M365 Tenant
2 M365
3 Voice Route
X

SBC number prefixes

Browse... pbxexample.csv pbxexample.csv

New Number prefix +

Back Next

1 M365 Tenant
2 M365
3 Voice Route
X

SBC number prefixes

Browse... No file selected.

New Number prefix +

314 X

Back Next



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

1 M365 Tenant
2 M365
3 Voice Route
X



SBC Onboarding Script sbc-scenario7

SBC Cleanup Script sbc-scenario7Cleanup

Customer Variables	Value

Back Submit

9. Configure SBC scripts:

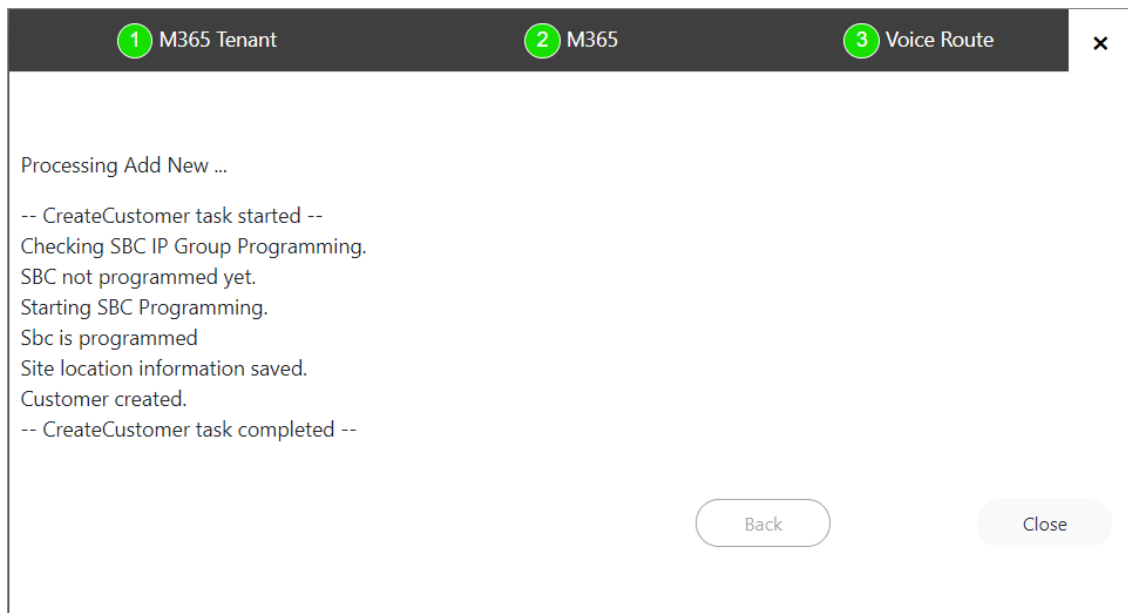
- Click the  to edit the SBC Onboarding Script file. This is a Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Custom Variables.
- Click the  to edit the SBC Cleanup Script file. Each SBC Onboarding script file has a corresponding Cleanup 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 [Customer Variables](#) on page 210.

Submit

10. When you have completed the configuration, click

The following screen is displayed:



Setting Up Hosted Essentials Customer

Connecting calls for Hosted Essentials customers requires the manual configuration of an SBC and Voice Routes.

➤ Do the following:

1. Login to the Service Provider Teams admin center.
2. In the Navigation pane,. select **Voice > Direct Routing**.
3. Click **Add** to add a new SBC device.

Direct Routing

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

Direct Routing summary

0	0	--
Total SBCs	Voice routes	SBCs with issues

SBCs Voice routes

[+ Add](#) [Edit](#) [Delete](#) 0 item

✓ SBC	Network effectiveness ⓘ	Average call duration ⓘ	TLS connectivity status ⓘ	SIP Options status ⓘ	Concurrent calls capacity ⓘ	Enabled ⓘ

- Enter the FQDN of the SBC device and configure the other parameters (refer to the relevant SBC User's Manual).

Direct Routing \ Add SBC

Add an FQDN for the SBC

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

Add a description so you know why it was created

SBC settings

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

Enabled	<input type="radio"/> Off
SIP signaling port	5067
Send SIP options ⓘ	<input checked="" type="checkbox"/> On
Forward call history	<input type="radio"/> Off
Forward P-Asserted-Identity (PAI) header ⓘ	<input type="radio"/> Off
Concurrent call capacity	24
Fallover response codes	408, 503, 504
Fallover time (seconds) ⓘ	10
SBC supports PIDF/LO for emergency calls	<input type="radio"/> Off

Location based routing and media optimization

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

The SBC is added.

Direct Routing

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

Direct Routing summary

1	0	0
Total SBCs	Voice routes	SBCs with issues

SBCs Voice routes

[+ Add](#) [Edit](#) [Delete](#) 1 item

✓ SBC	Network effectiveness ⓘ	Average call duration ⓘ	TLS connectivity status ⓘ	SIP Options status ⓘ	Concurrent calls capacity ⓘ	Enabled ⓘ
sandbox1b.audiocodes.be	ⓘ 0%	0 seconds (0)	ⓘ Inactive	⚠ Warning	Within limits	<input checked="" type="checkbox"/> On

- Add the required Voice Routes.

LocalRoute

Description

Priority: 1

Dialed number pattern: ^(\+1[0-9]{10})\$

SBCs enrolled

Select which SBCs you want calls to route to. All SBCs that you add will be tried in a random order. [Learn more](#)

You haven't selected any SBCs yet.

[Add SBCs](#)

PSTN usage records

The voice routing policy is linked to a voice route using the PSTN usage records below. You can add existing PSTN usage records, change the order in which the voice routing should be processed, and assign the policy to users. [Learn more](#)

You haven't selected any PSTN usage records yet.

[Add PSTN usage records](#)

[Save](#) [Cancel](#)

Direct Routing

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

[Manage PSTN usage records](#)

Direct Routing summary

1 Total SBCs, 2 Voice routes, 0 SBCs with issues

Voice routes

✓	Voice route	Priority	Description	Dialed number pattern	PSTN usage	SBCs enrolled
	LocalRoute	1		^(\\+1[0-9]{10})\$		
	Unrestricted	2		.	Unrestricted	NewVoice.customers.audiooc

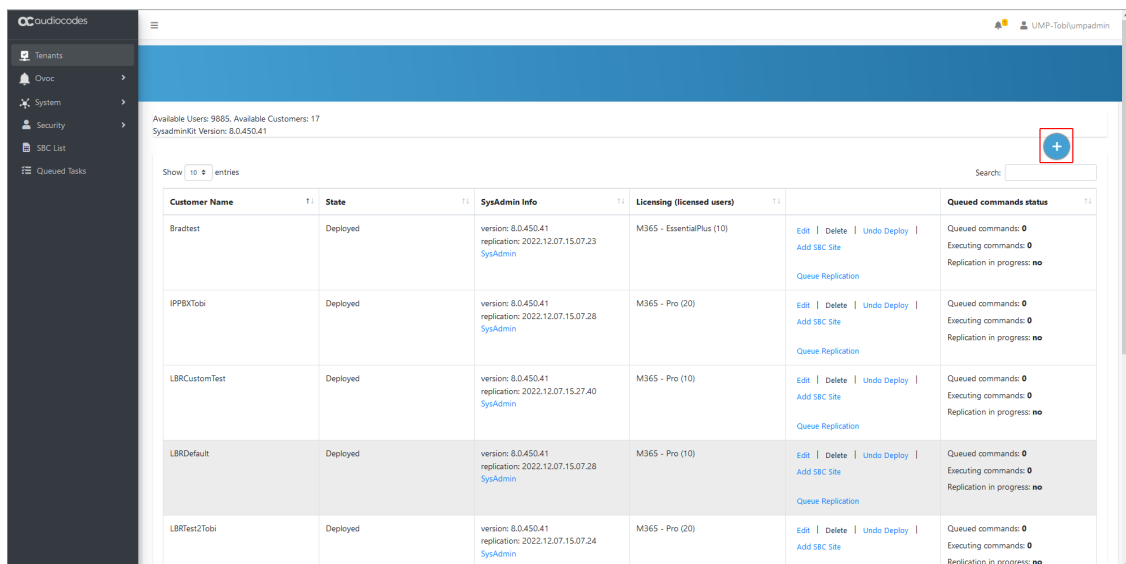
Onboarding with Hosted Essentials +

This section describes how to onboard Hosted Essentials + customers. At the start of the Onboarding wizard, consent must be requested from the customer administrator to access their M365 platform. The following Onboarding flows can be run:

- [Onboarding with both M365 Default Routing and SBC Configuration](#) on page 333
- [Onboarding with only SBC Configuration](#) on page 356

➤ To onboard Hosted Essentials + customers:

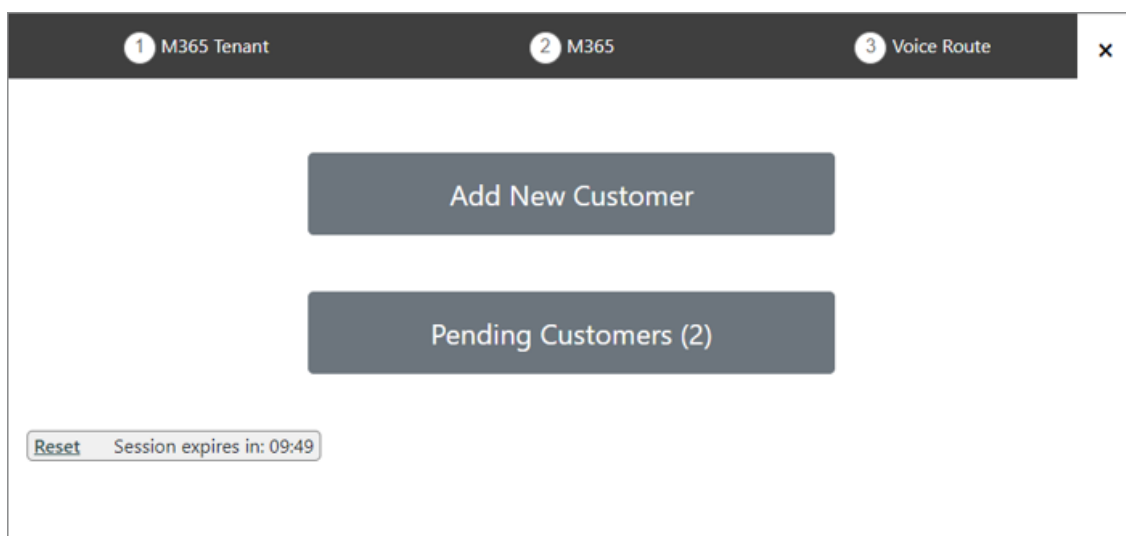
1. In the Tenants page, click  .



Available Users: 9885, Available Customers: 17
SysadminKit Version: 8.0.450.41

Show 10 entries

Customer Name	State	SysAdmin Info	Licensing (licensed users)		Queued commands status
Bractest	Deployed	version: 8.0.450.41 replication: 2022.12.07.15.07.23 SysAdmin	M365 - EssentialPlus (10)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
IPPBXTobi	Deployed	version: 8.0.450.41 replication: 2022.12.07.15.07.28 SysAdmin	M365 - Pro (20)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
LBRCustomTest	Deployed	version: 8.0.450.41 replication: 2022.12.07.15.27.40 SysAdmin	M365 - Pro (10)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
LBRCDefault	Deployed	version: 8.0.450.41 replication: 2022.12.07.15.07.28 SysAdmin	M365 - Pro (10)	Edit Delete Undo Deploy Add SBC Site Queue Replication	Queued commands: 0 Executing commands: 0 Replication in progress: no
LBRTes2Tobi	Deployed	version: 8.0.450.41 replication: 2022.12.07.15.07.24 SysAdmin	M365 - Pro (20)	Edit Delete Undo Deploy Add SBC Site	Queued commands: 0 Executing commands: 0 Replication in progress: no



1 M365 Tenant 2 M365 3 Voice Route X

Add New Customer

Pending Customers (2)

Reset Session expires in: 09:49

2. Click **Add New Customer**.

1 M365 Tenant 2 M365 3 Voice Route X

Full Customer Name

HostedPlus

Short Customer Name

HostedPlus

License Type

☐ Hosted Essential ☒ Hosted Essentials+ ☐ Hosted Pro

Licensed Users

M365 Authentication

☐ Send link to customer IT administrator for authentication:

☒ Use M365admin account with known password

M365 User Name M365 Password

Back Next

3. Enter Full Customer M365 Tenant Name – Free Text.
4. Enter 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. Proceed to [Request Consent from End Customer](#) on page 364.

1 M365 Tenant 2 M365 3 Voice Route

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

Back Next

If the following error is displayed, press [Ctrl] F in the browser to clear the cache and then try again. on the next try you will get the authentication process where you will have to consent for the permissions.

Validating credentials, please wait! On succesfull authentication the wizard will continue.
The administrator has not consented to use the application!
Something went wrong while verifying M365 credentials!

Back Next

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

1 M365 Tenant 2 M365 3 Voice Route

Customer **BasicPlus**

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 31-2: Microsoft 365 Settings

M365 Setting	Description
M365	Customer Tenant original Microsoft 365 domain prior to applying vanity

M365 Setting	Description
Domain (Override Admin Domain)	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 User Management Pack™ 365 SP Edition Channel/Customer Portal (Optional). When this option is used, Single Sign-on support with the customer Azure AD is provided.

1 M365 Tenant
2 M365
3 Voice Route
x

☐ **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** ; the wizard creates default M365 routing in the customer tenant based on the derived trunk model for service providers. In addition, you can automatically configure the DNS server to create a PSTN gateway and customer domain. See [Onboarding with both M365 Default Routing and SBC Configuration](#) on page 333.
- Click **Next** and proceed to [Onboarding with only SBC Configuration](#) on page 356.

Request Consent from End Customer

If the customer purchased a Hosted Essentials Plus or Hosted Pro license then they must grant consent to the Service Provider or Channel administrator for accessing their M365 platform. The consent is secured using Token authentication between the User Management Pack™ 365 SP Edition platform and the customer M365 tenant platform. Once the Token connection is securely established, the customer administrator account credentials can be used to create the new customer and thereafter for synchronizing the User Management Pack™ 365 SP Edition database with the M365 platform. The customer administrator must consent to the following:

- Access Microsoft Teams and Skype for Business data as the signed in user.
- Read and write all groups.
- Access directory as the signed in user.
- Read all users' full profiles.
- Read and write to all app catalogs.
- Maintain access to data that you have provided access.

The Token Invitation wizard is used for establishing the Token connection with the customer M365 platform. This wizard is run at the beginning of the Onboarding wizard. The Token Invitation wizard can be run using the following methods:

- Sending email link directly to customer IT administrator including a link to the Token Invitation wizard.
- Using M365 account credentials (username and password) received from the customer administrator.

The Token connection can be secured using either the 'Global' admin permissions or the permissions of the Customer admin Service account (see [Create Customer Administrator Service Account](#) on page 265). See the following:

- [Onboarding with Default Global Admin](#) below
- [Onboarding with Tenant-Defined Service Account](#) on page 311

Onboarding with Default Global Admin

The following methods can be used to secure the Token connection with the customer M365 platform using customer default Global admin account:

- Use username and password of the Global admin account ([Secure Token Connection with Global Admin Credentials](#) on page 365).
- Send email link directly to Global admin ([Secure Token Connection with Email Link \(Global Admin\)](#) on page 299).

Secure Token Connection with Global Admin Credentials

You can secure the Token connection with the customer M365 platform using the provided credentials of the customer Global admin account.



Ensure that the Global admin has been assigned the required roles (see [Assign Administrator Roles to IT Administrator](#) on page 269).

➤ Do the following:

1. In the Onboarding wizard click **Add New Customer**.

The screenshot shows a dark header bar with three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. Below the header, there are two large buttons: "Add New Customer" and "Pending Customers (2)". At the bottom left, there is a "Reset" link and a session expiration timer: "Session expires in: 09:49".

2. Select **Use M365admin account with known password**.

The screenshot shows the configuration screen for the M365 Tenant. It has the same header as the previous screen. The form includes:

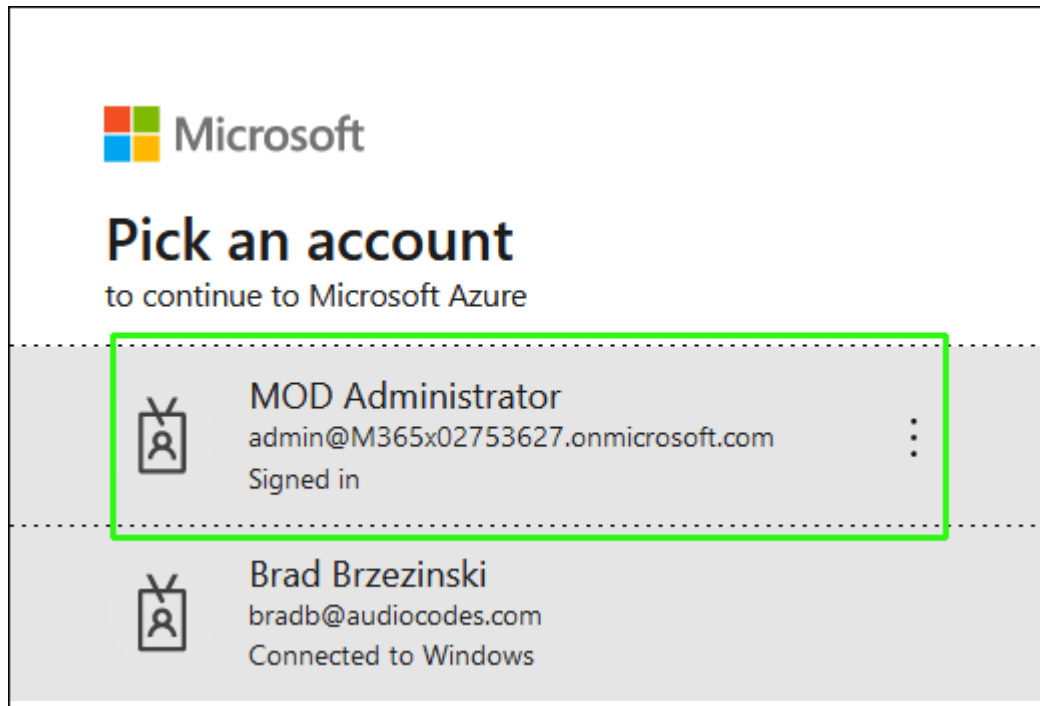
- Full Customer Name:** A text field containing "GlobalBasic".
- Short Customer Name:** A text field containing "GlobalBasic".
- License Type:** Three radio buttons: "Hosted Essential", "Hosted Essentials+", and "Hosted Pro" (which is selected). To the right is a dropdown menu showing "10".
- M365 Authentication:** Two radio buttons: "Send link to customer IT administrator for authentication:" and "Use M365admin account with known password" (which is selected).
- Authentication Fields:** Below the selected radio button, there is a text field containing "admin@M365x02753627.onmicrosoft.com" and a password field with masked characters and an eye icon to toggle visibility.
- Navigation:** "Back" and "Next" buttons at the bottom right.

3. Enter the Global Admin username and password provided by the customer.

The screenshot shows an instruction screen for the M365 Tenant. It has the same header. The content includes:

- A link: "Click [here](#) to start the authentication process."
- A message: "The Wizard will continue after consent is granted."
- Navigation:** "Back" and "Next" buttons at the bottom right.

4. Click **here** to start the authentication process.



5. Choose the customer tenant Global Admin account.



The customer Tenant account must have Global Admin permissions, otherwise the “Consent on behalf of the organization” check box does not appear.



admin@m365x02753627.onmicrosoft.com

Permissions requested

Sandbox2-UMP-Token
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to
- ☒ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement.

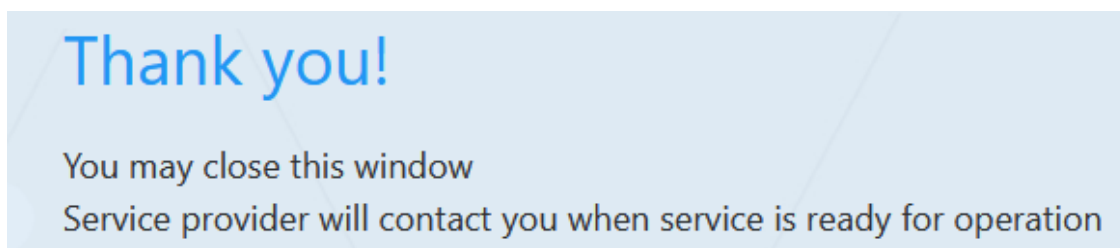
The publisher has not provided links to their terms for you to review. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept

- Click **Consent on behalf of your organization**, and then click **Accept**.



- Click **Pending Customers** to monitor the process of the request. Verify that Status is shown as **Authentication Complete** (see also [Pending Requests](#) on page 381).
- Likewise, open the Multitenant interface and navigate to **Security > Customer Invitations**. Verify that Device Authenticated is shown as **true**.
- Open the newly created Token registration on the Azure portal for the customer tenant (Enterprise Applications > <Token-Registration-Name>).
- In the Navigation pane, select **Permissions**. Note the added permissions for the new Enterprise application.

The screenshot shows the 'Permissions' page for the 'Sandbox2-UMP-Token' application in the Microsoft Azure portal. The page displays a list of permissions granted to the application, categorized into 'Admin consent' and 'User consent'. The 'Admin consent' section is currently selected, showing a table of permissions.

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph	Group.ReadWrite.All	Read and write all groups	Delegated	Admin consent	An administrator
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed in user	Delegated	Admin consent	An administrator
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated	Admin consent	An administrator
Microsoft Graph	AppCatalog.ReadWrite.All	Read and write to all app catalogs	Delegated	Admin consent	An administrator
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	Admin consent	An administrator
Skype and Teams Tenant Admin API	user_impersonation	Access Microsoft Teams and Skype for Business data as the ...	Delegated	Admin consent	An administrator

- Continue the Onboarding wizard, see [Onboarding with Hosted Pro](#) on page 361 or [Onboarding with Hosted Essentials +](#) on page 290.

Secure Token Connection with Email Link (Global Admin)

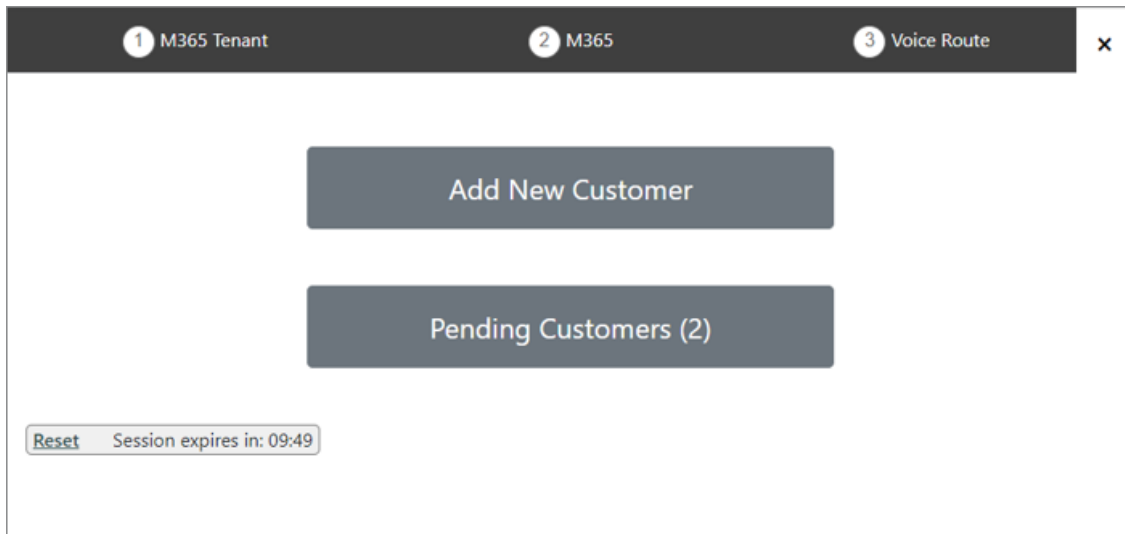
You can secure the Token connection with the customer M365 platform by sending an email to the customer Global admin with a link to trigger the Token Authentication Invitation wizard



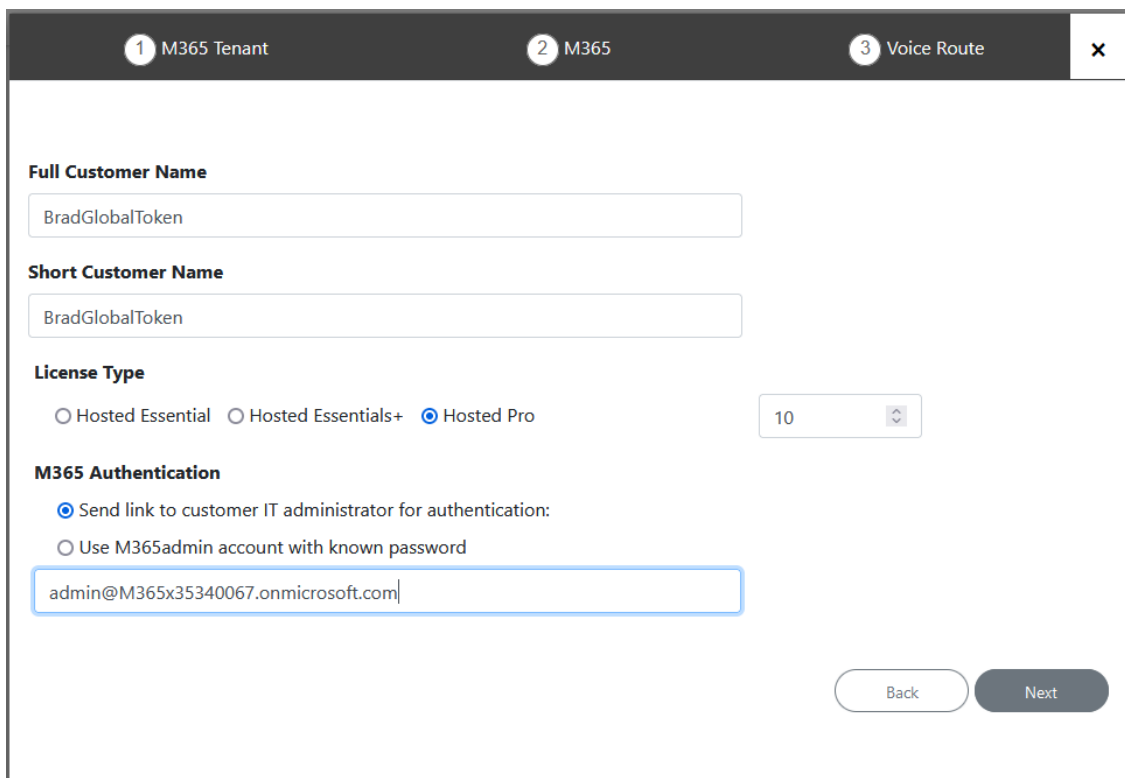
Ensure that the customer tenant has been assigned the required roles (see [Assign Administrator Roles to IT Administrator](#) on page 269).

➤ **Do the following:**

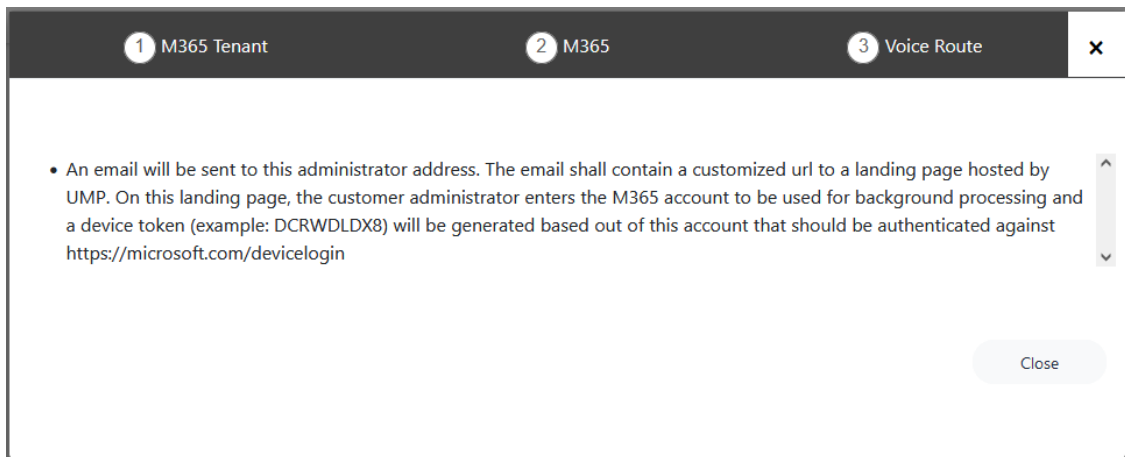
1. In the Onboarding wizard, click **Add New Customer**.



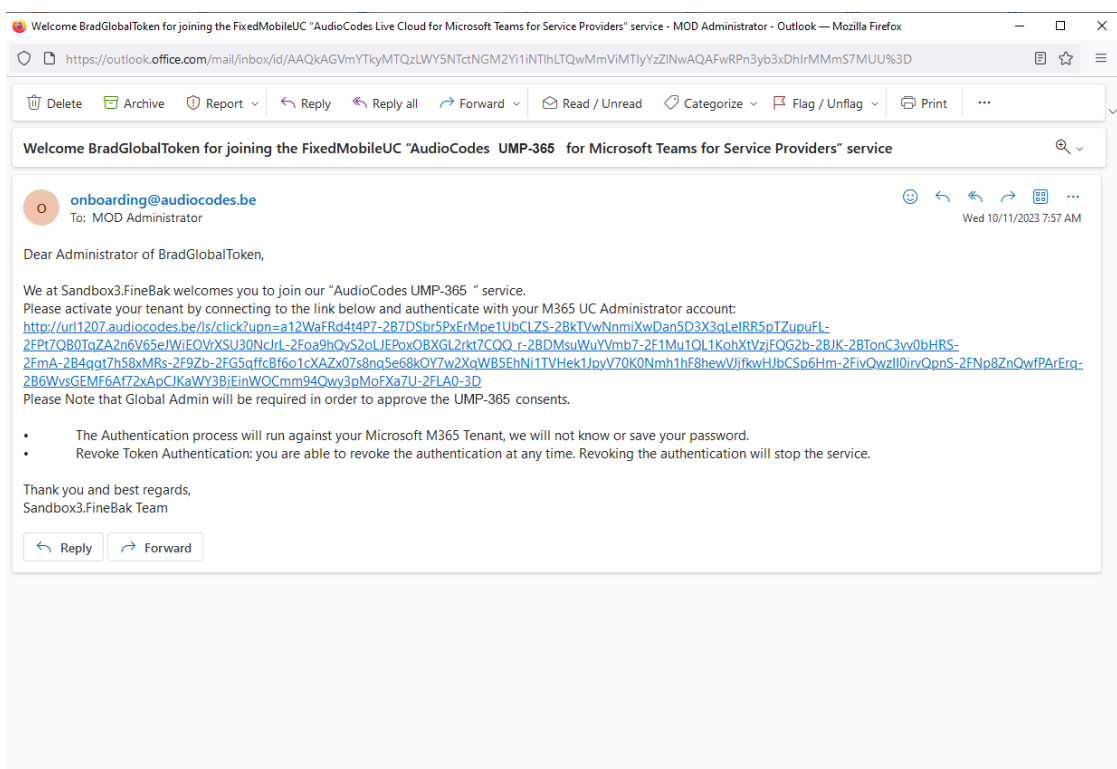
2. Enter the Full and Short Customer Names
3. Select either the **Hosted Essentials +** or **Hosted Pro** License type.
4. Set the number of required licenses.
5. Select the **Send link to customer IT administrator for authentication link**.



6. Enter the email address of the Customer tenant Global administrator, and then click **Next**. An email is sent to the customer administrator, and the following information message is displayed.

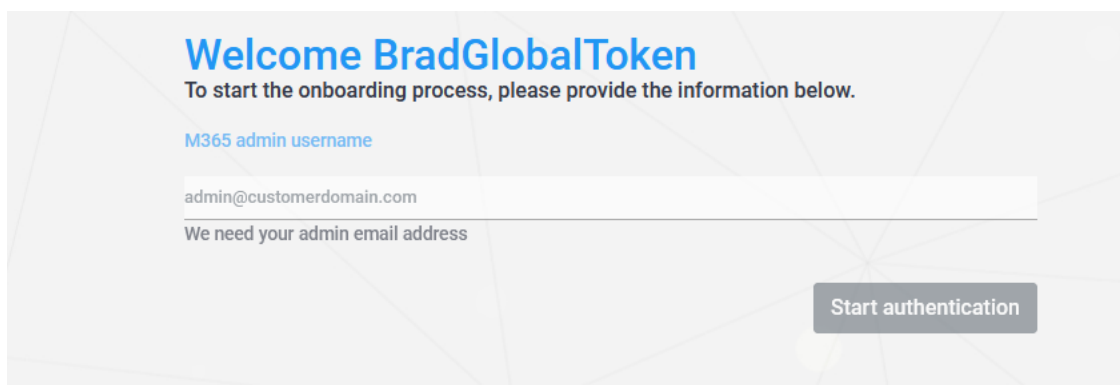


7. Open the email of the Customer tenant Service Account administrator.



If mail has not been received, open the Multitenant interface and navigate to **Security > Customer Invitations**. Search for the relevant token and validate that Email Sent is 'True'. In addition, check the email settings (see [Configuring Email Settings](#) on page 69).

8. Click the link sent in the e-mail as shown in the example above. The Token Invitation Wizard Welcome screen is displayed.



Welcome BradGlobalToken

To start the onboarding process, please provide the information below.

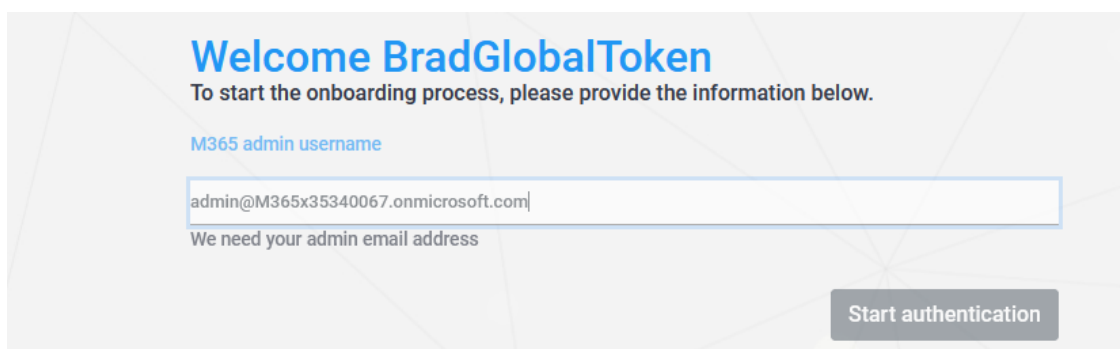
M365 admin username

admin@customerdomain.com

We need your admin email address

Start authentication

9. Enter the credentials of the Global Admin user, and then click **Start authentication**.



Welcome BradGlobalToken

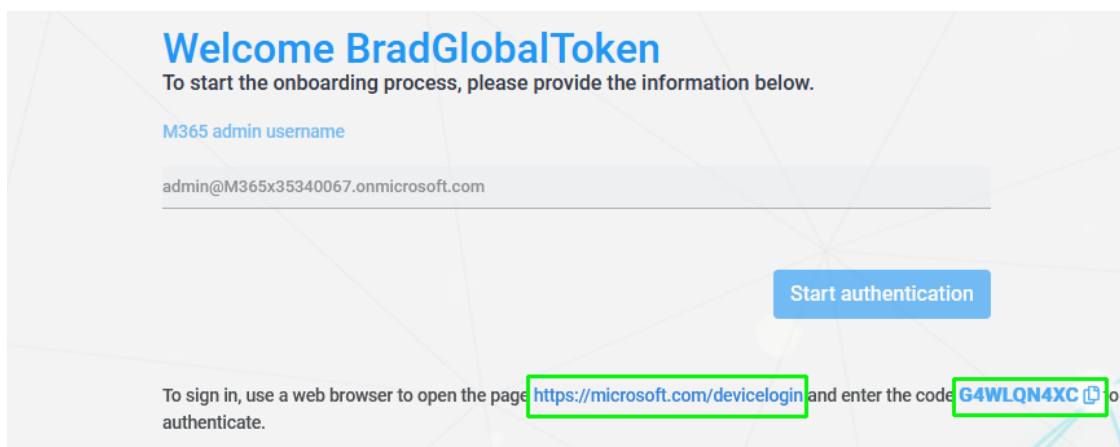
To start the onboarding process, please provide the information below.

M365 admin username

admin@M365x35340067.onmicrosoft.com

We need your admin email address

Start authentication



Welcome BradGlobalToken

To start the onboarding process, please provide the information below.

M365 admin username


admin@M365x35340067.onmicrosoft.com

We need your admin email address

Start authentication

To sign in, use a web browser to open the page <https://microsoft.com/devicelogin> and enter the code **G4WLQN4XC** to authenticate.

10. Copy the code at the bottom of the screen and then click the Web browser link.



Enter code

Enter the code displayed on your app or device.

G4WLQN4XC

Next

11. Paste the code and then click **Next**.



Pick an account

You're signing in to **LiveCloud-Token-UMP** on another device located in **Netherlands**. If it's not you, close this page.



MOD Administrator

admin@M365x35340067.onmicrosoft.com

Signed in



Christie Cline

ChristieC@M365x62192331.OnMicrosoft.com

Signed in



MOD Administrator

admin@M365x62192331.onmicrosoft.com

Signed in



MOD Administrator

admin@M365x18011641.onmicrosoft.com

Signed in



Alex Wilber

AlexW@M365x02753627.OnMicrosoft.com

Signed in



Use another account

Back

12. Choose the customer tenant Global admin account, and then click **Next**.



admin@m365x35340067.onmicrosoft.com

Permissions requested

LiveCloud-Token-UMP
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to

☒ **Consent on behalf of your organization**

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>.

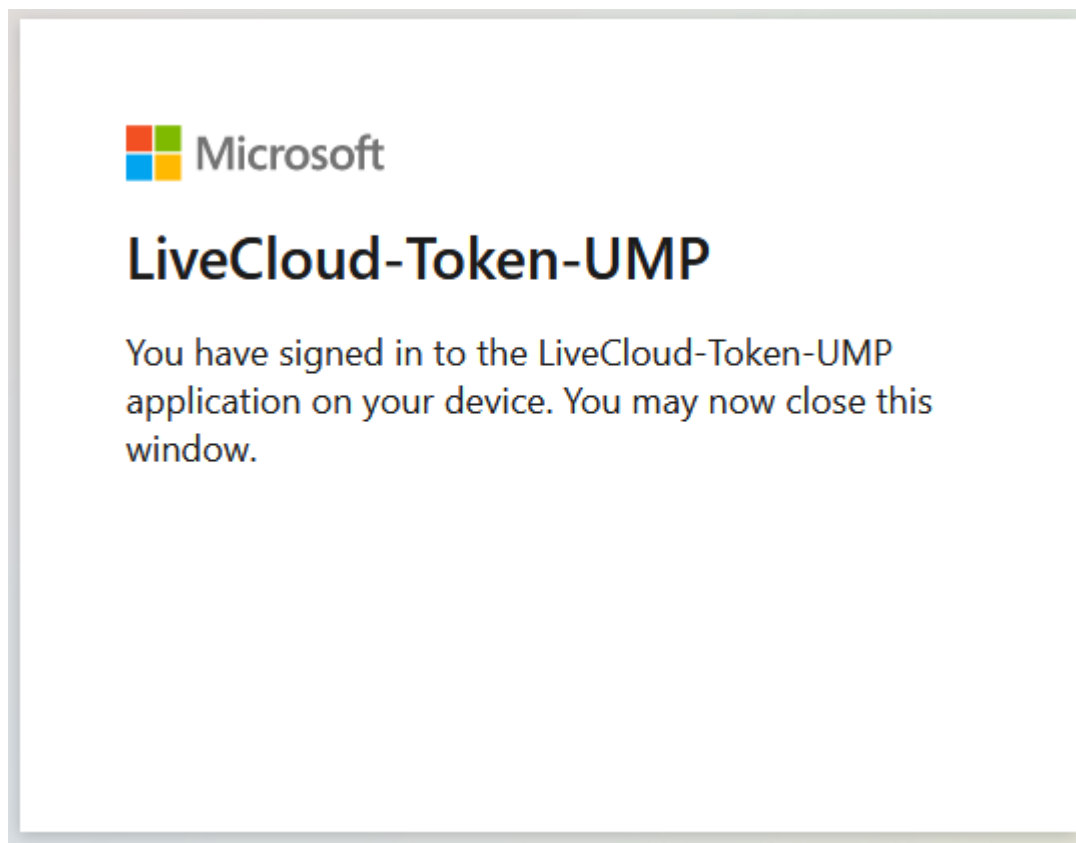
Important: Only accept if you trust the publisher and if you downloaded this app from a store or website you trust. Microsoft is not involved in licensing this app to you.

Does this app look suspicious? [Report it here](#)

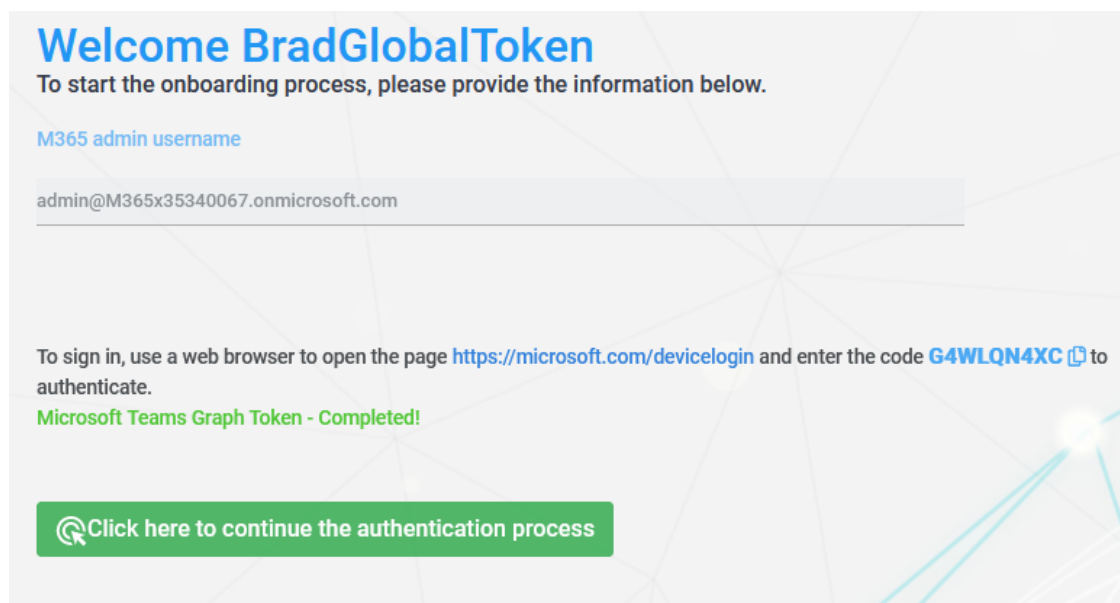
Cancel

Accept

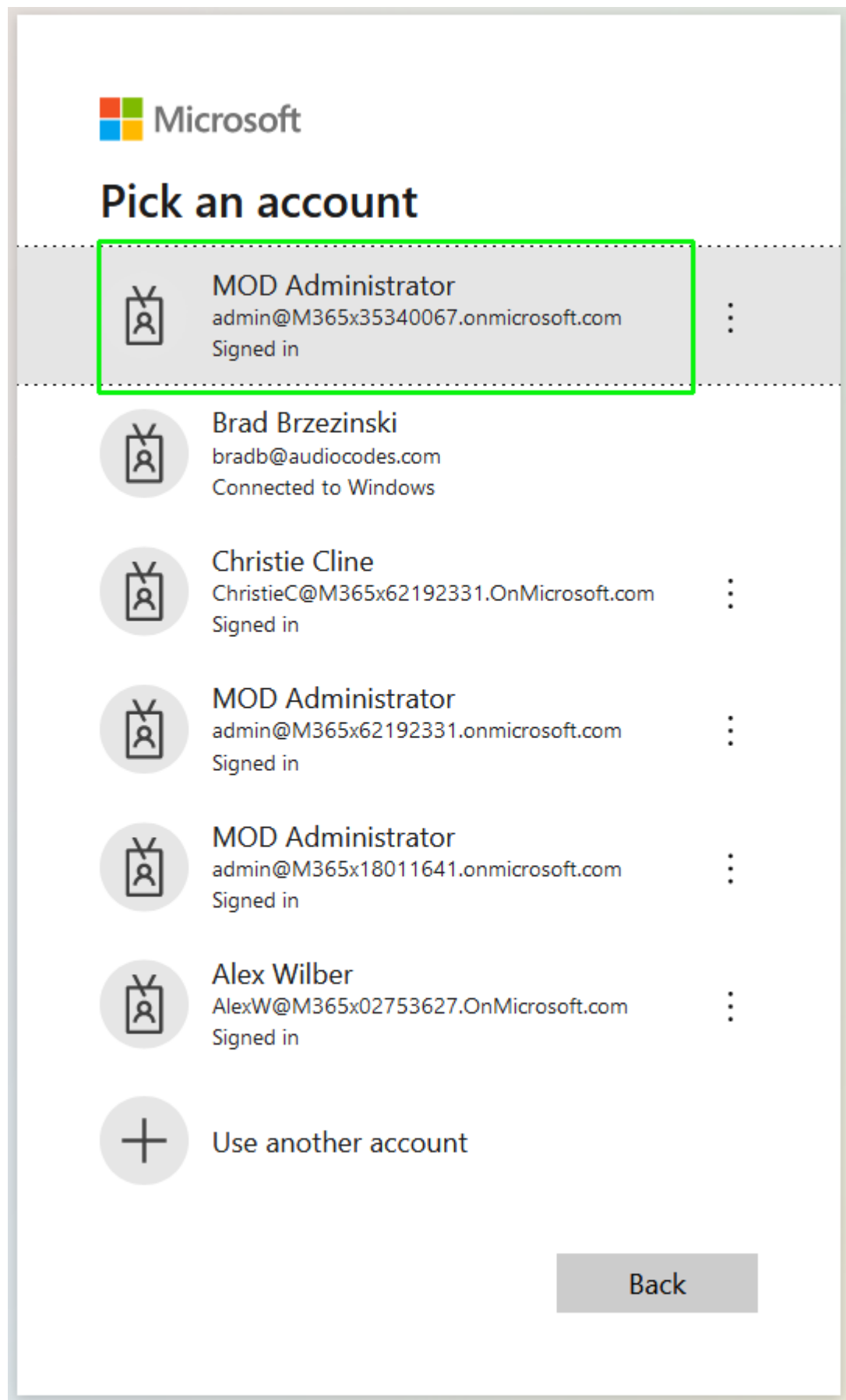
13. Select **Consent on behalf of your organization** check box, and then click **Accept**.



14. Close the Information window.



15. Click **Click here to continue the authentication process** link.



16. Choose the customer tenant Global admin account.



admin@m365x35340067.onmicrosoft.com

Permissions requested

LiveCloud-Token-UMP
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to

☒ **Consent on behalf of your organization**

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement.

The publisher has not provided links to their terms for you to review. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

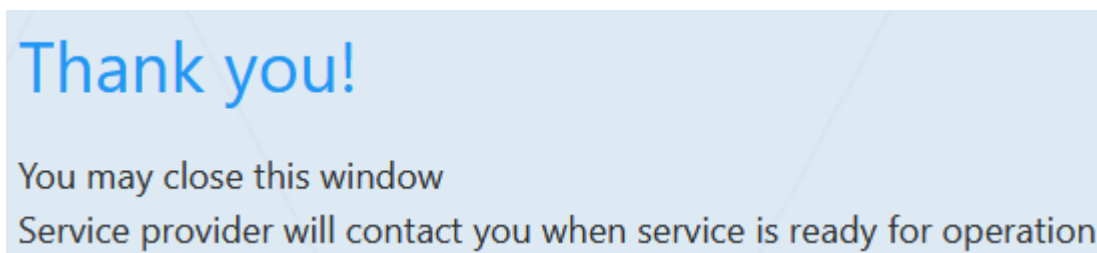
Does this app look suspicious? [Report it here](#)

Cancel

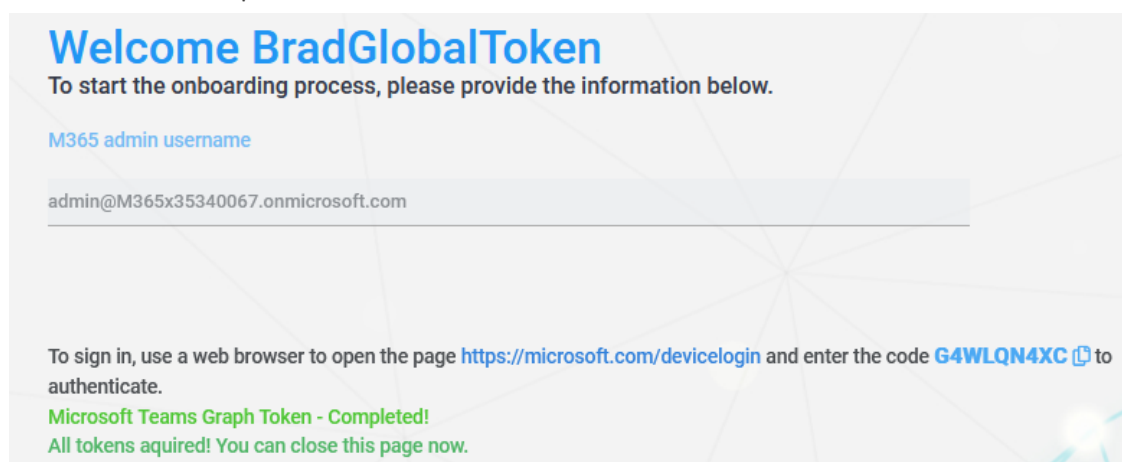
Accept

17. Select the **Consent on behalf of your organization** check box, and then click **Accept**.

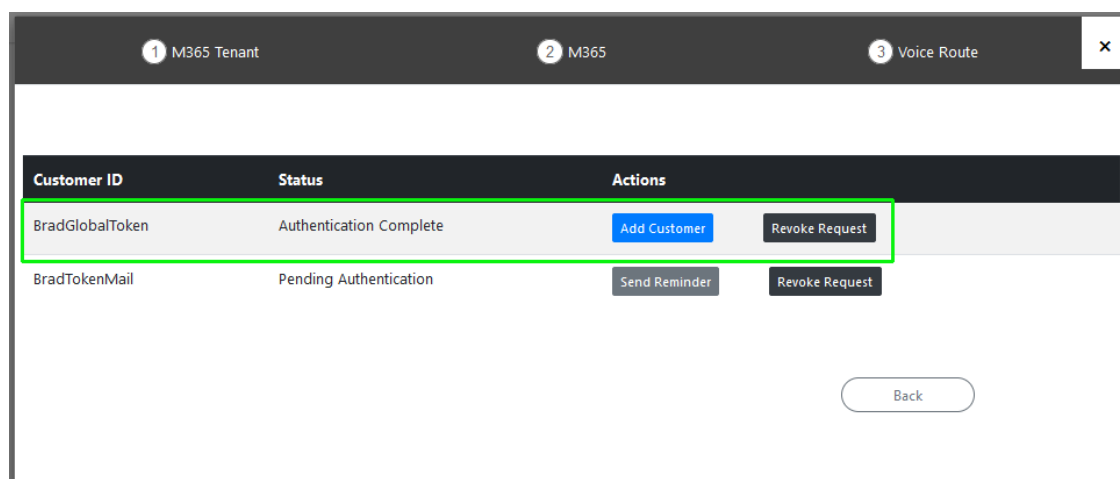
At the end of the process, the following information message is displayed.



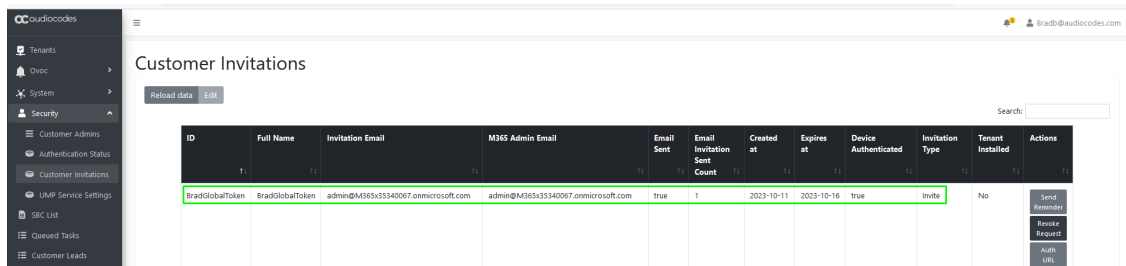
The following message also confirms the successful completion of the Token Authentication process.



18. Click **Pending Customers** to monitor the process of the request. Verify that Status is shown as **Authentication Complete** (see also [Pending Requests](#) on page 381).

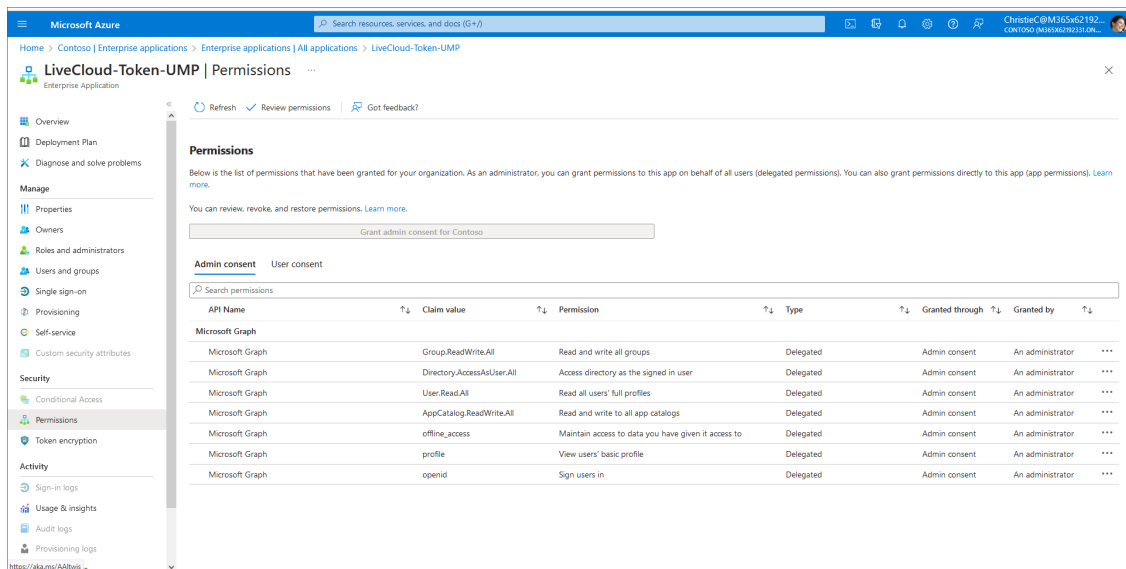


19. Likewise, open the Multitenant interface and navigate to **Security > Customer Invitations**. Verify that Device Authenticated is shown as **true**.



20. Open the newly created Token registration on the Azure portal for the customer tenant (Enterprise Applications > <Token-Registration-Name>).

21. In the Navigation pane, select **Permissions**. Note the added permissions for the new Enterprise application.



22. Resume the wizard process (see [Onboarding with Hosted Essentials +](#) on page 290 or [Onboarding with Hosted Pro](#) on page 361).

Onboarding with Tenant-Defined Service Account

The following methods can be used to secure the Token connection with the customer M365 platform Service Account ([Create Customer Administrator Service Account](#) on page 265:

- Use username and password of the Service account ([Secure Token Connection with Service Account Credentials](#) below).
- Send email link directly to Service account administrator ([Secure Token Connection with Service Account Credentials](#) below).

Secure Token Connection with Service Account Credentials

You can secure the Token connection with the customerM365 platform using the provided credentials of the customerService account (see [Create Customer Administrator Service Account](#) on page 265.



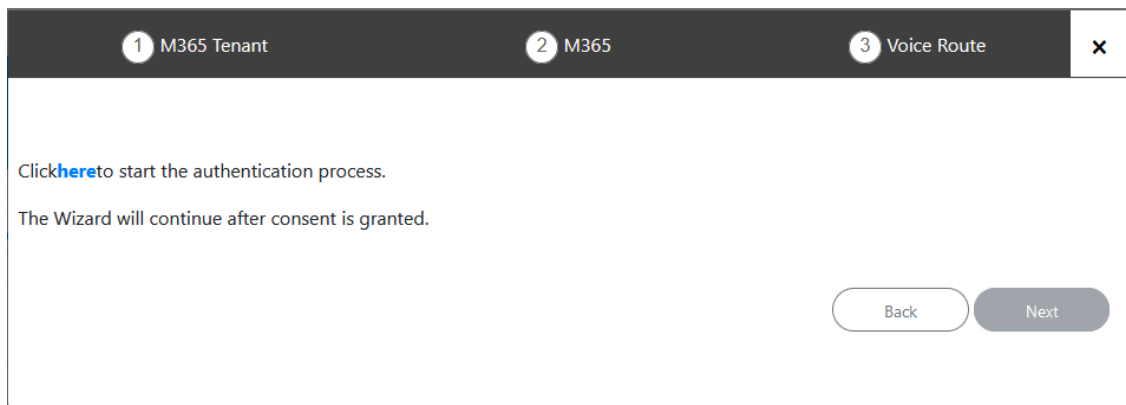
Ensure that the customer tenant has been assigned the required roles (see [Assign Administrator Roles to IT Administrator](#) on page 269).

➤ **Do the following:**

1. In the Onboarding wizard click **Add New Customer**.

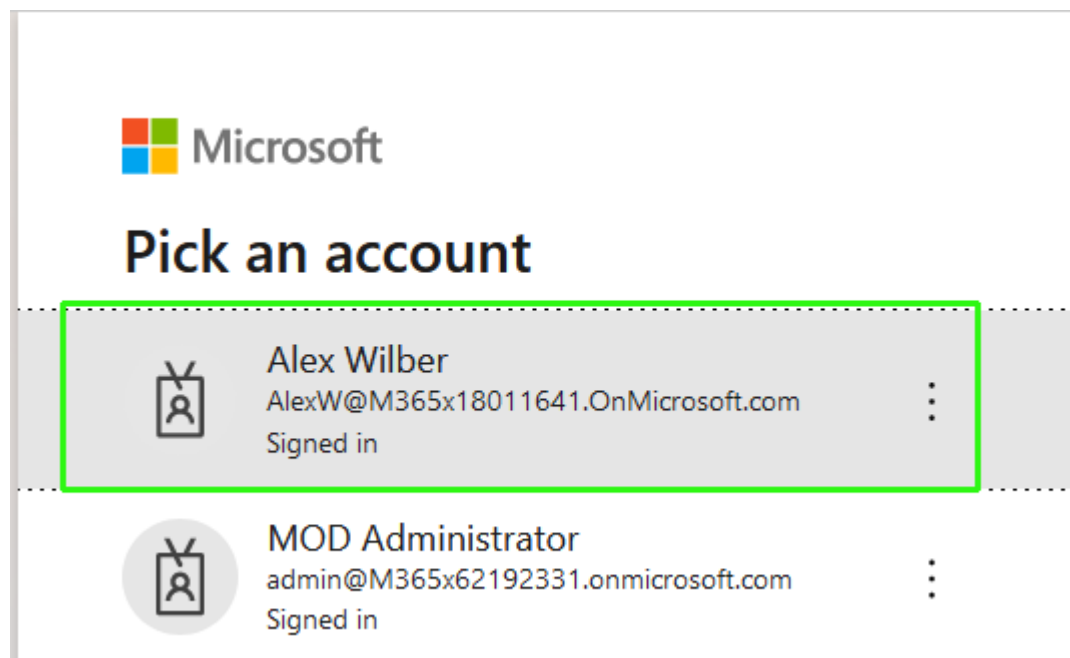
2. Enter the Full and Short Customer Names.
3. Select either the **Hosted Essentials +** or **Hosted Pro** License type.
4. Set the number of required licenses.
5. Select **Use M365admin account with known password**.

6. Enter the tenant-defined Service account defined Admin username and password provided by the customer (see [Create Customer Administrator Service Account](#) on page 265).




The screenshot shows a wizard interface with a dark header bar containing three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. The main content area has the text: "Click [here](#) to start the authentication process." and "The Wizard will continue after consent is granted." At the bottom right, there are two buttons: "Back" and "Next".

7. Click **here** to start the authentication process.



8. Choose the Customer Service account (see [Create Customer Administrator Service Account](#) on page 265).

 **CONTOSO** demo

alexw@m365x18011641.onmicrosoft.com

Approval required

unverified

This app requires your admin's approval to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to

Enter justification for requesting this app

[Sign in with another account](#)

Does this app look suspicious? [Report it here](#)

CancelRequest approval

Contoso

9. Enter justification for requesting approval from the Global admin and then click **Request Approval**.



alexw@m365x18011641.onmicrosoft.com

Approval required

unverified

This app requires your admin's approval to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to

New UMP-365 customer|



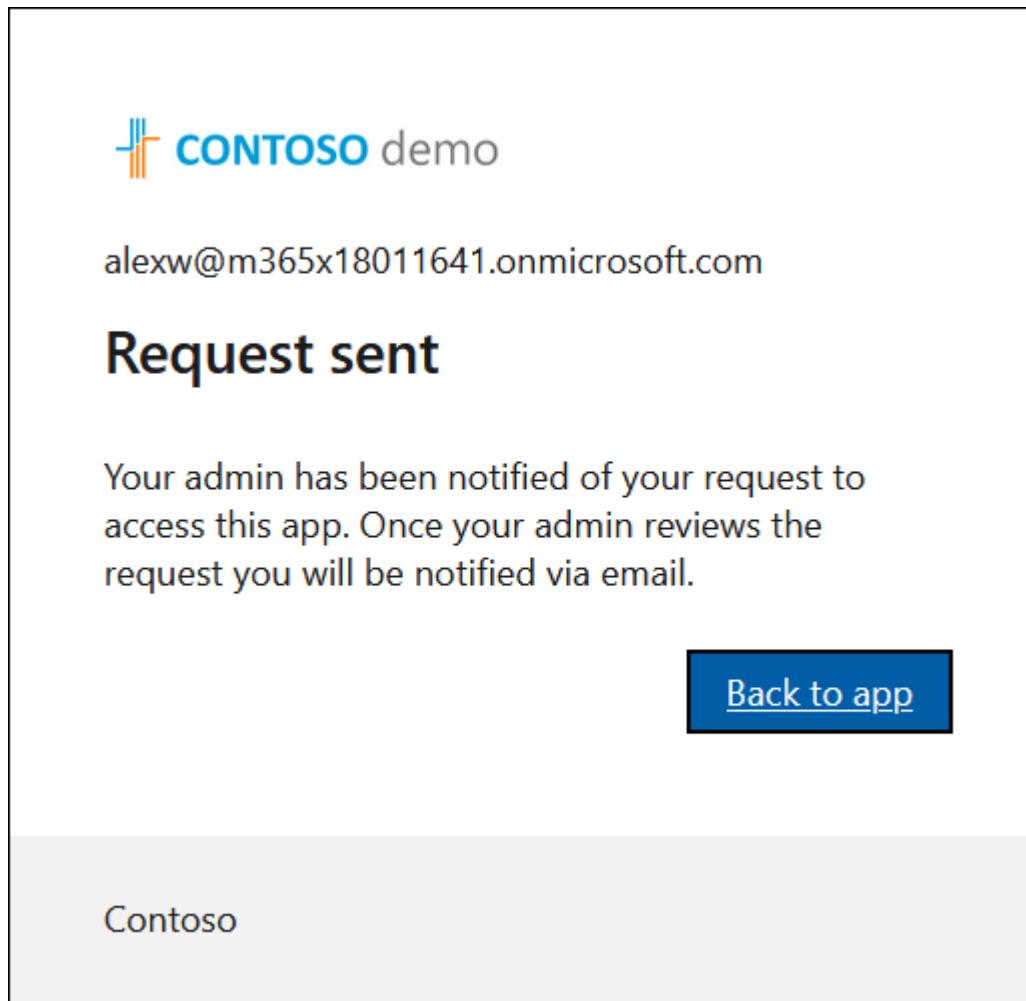
[Sign in with another account](#)

Does this app look suspicious? [Report it here](#)

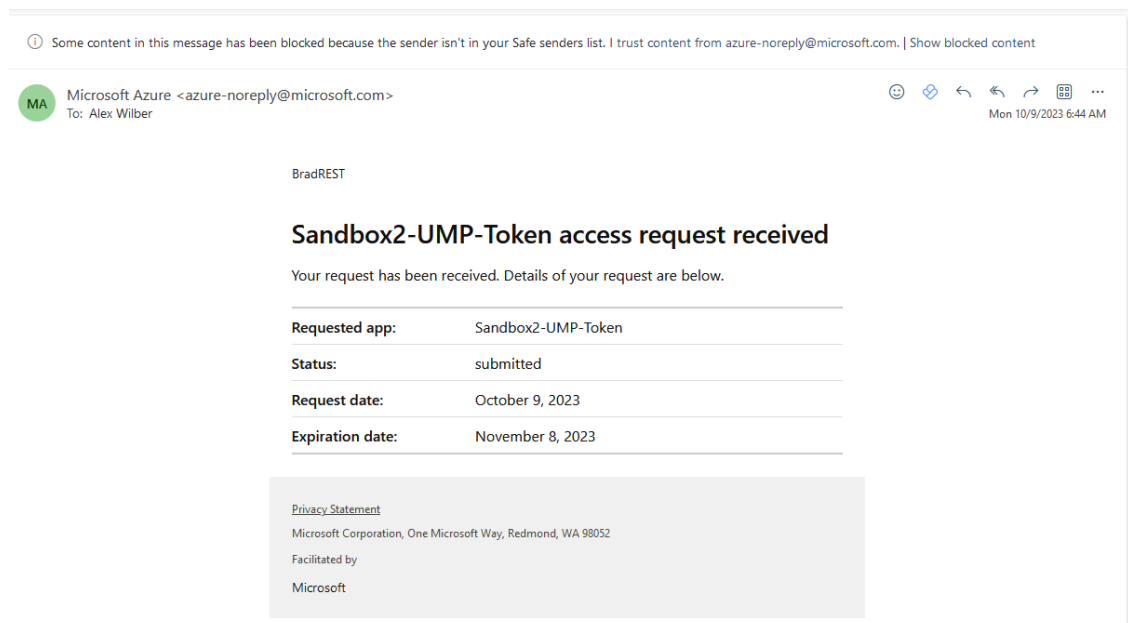
Cancel

Request approval

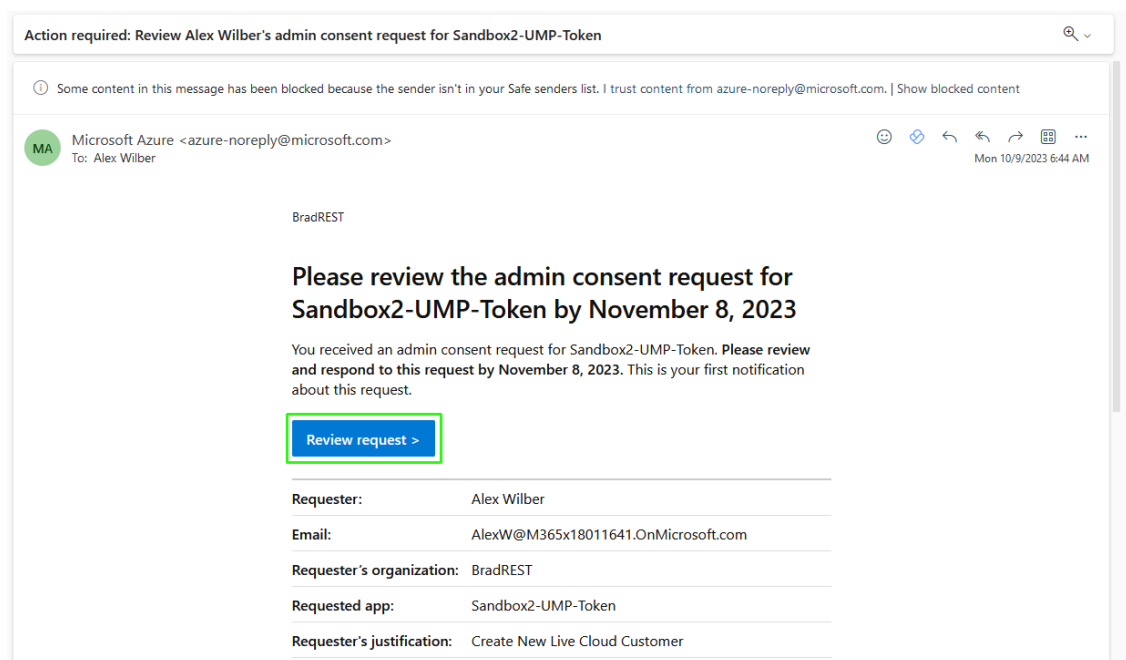
Contoso



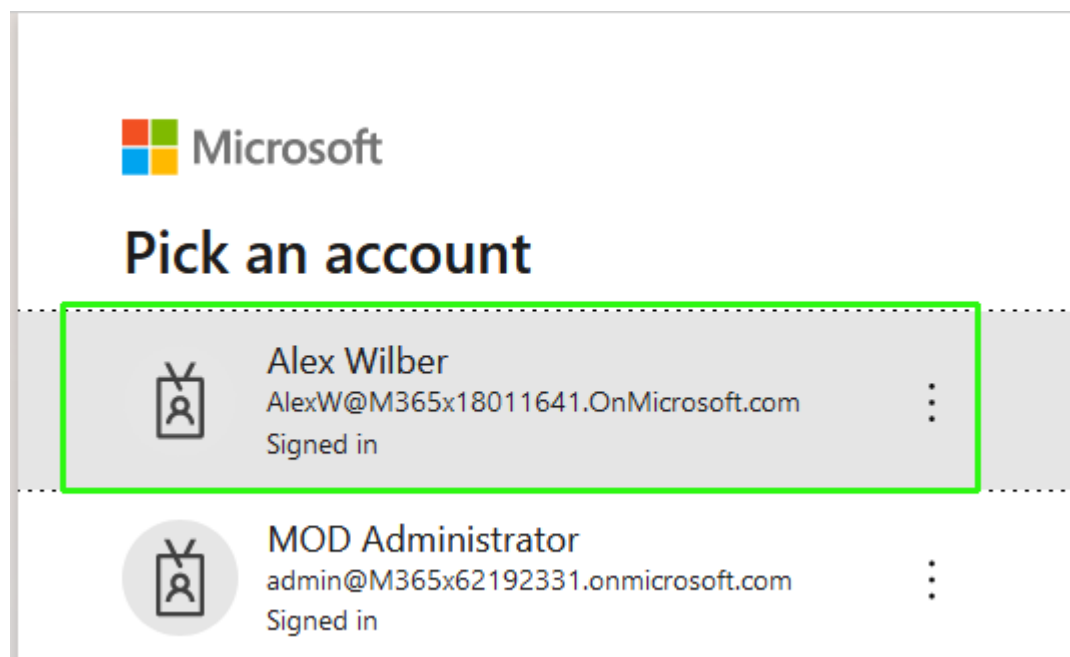
10. Open the email of the Service account. View the example mail message below indicating the request to access the Customer tenant M365 platform.



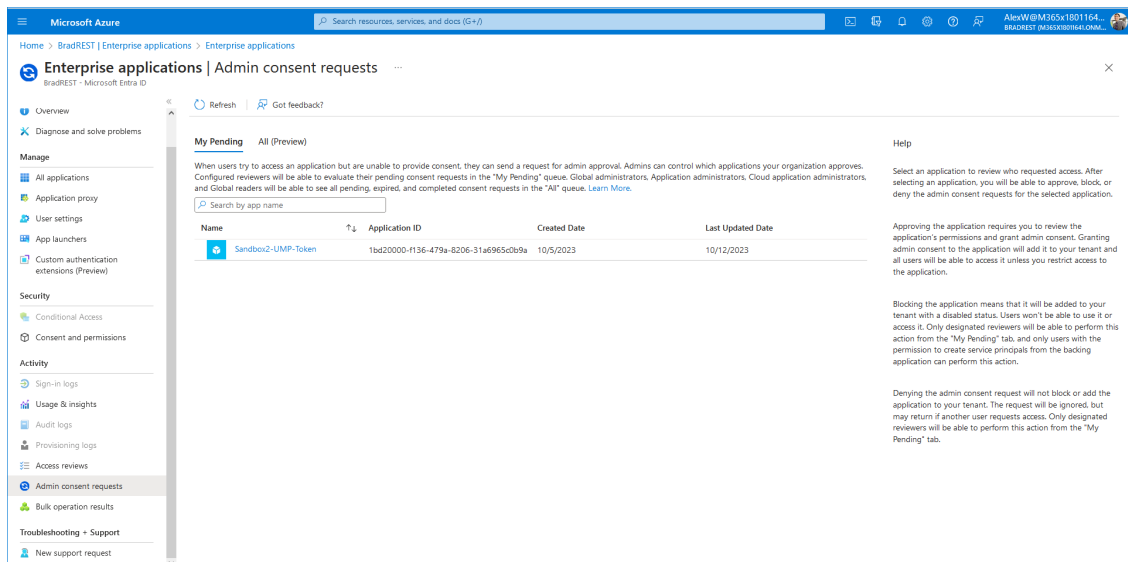
11. Another mail is then received requesting to review the admin consent request. Click **Review request**.



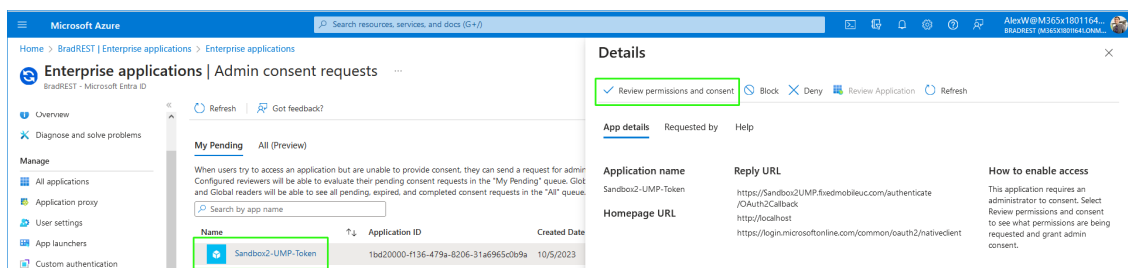
12. Choose the credentials of the Service account.



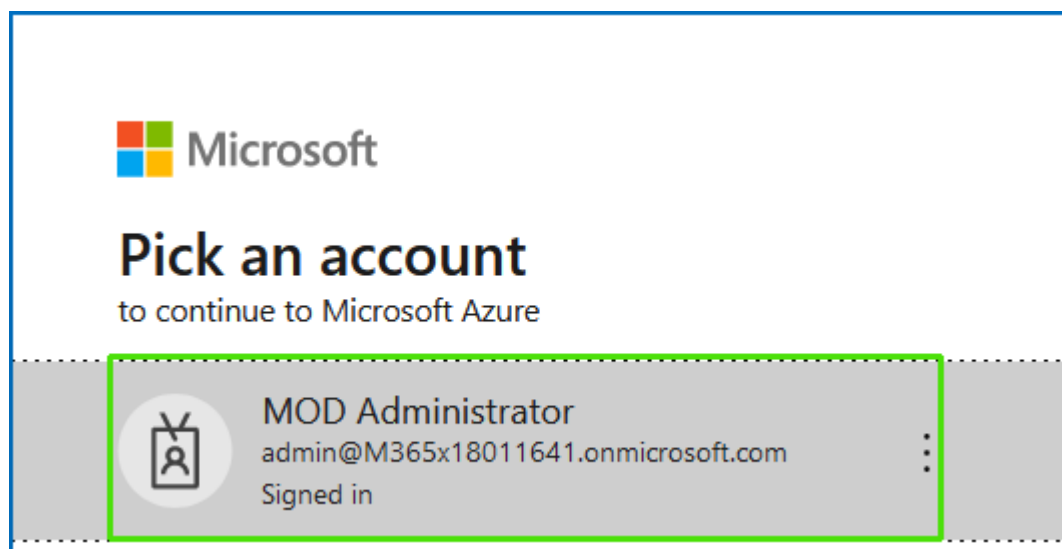
The Admin Consent request requiring Global Admin approval is displayed.



13. Select the request and then click **Review permissions and consent**.



14. Choose the Global admin account of the customer tenant, select the **Consent on behalf of your organization** check box, and then click **Accept**.





admin@m365x18011641.onmicrosoft.com

Permissions requested

Sandbox2-UMP-Token
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to
- ☒ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

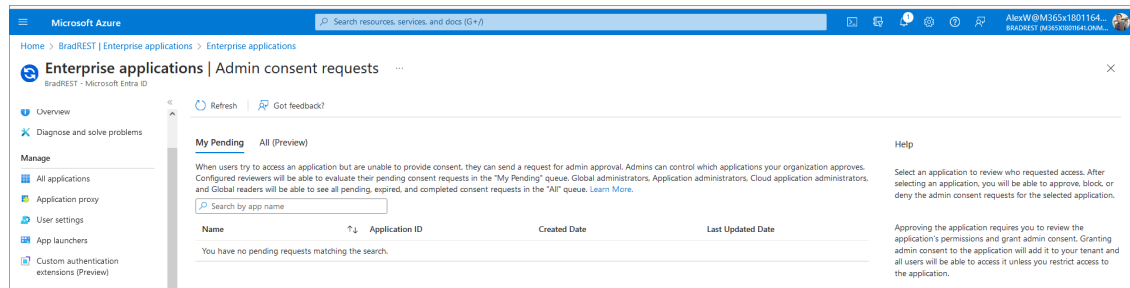
Cancel

Accept

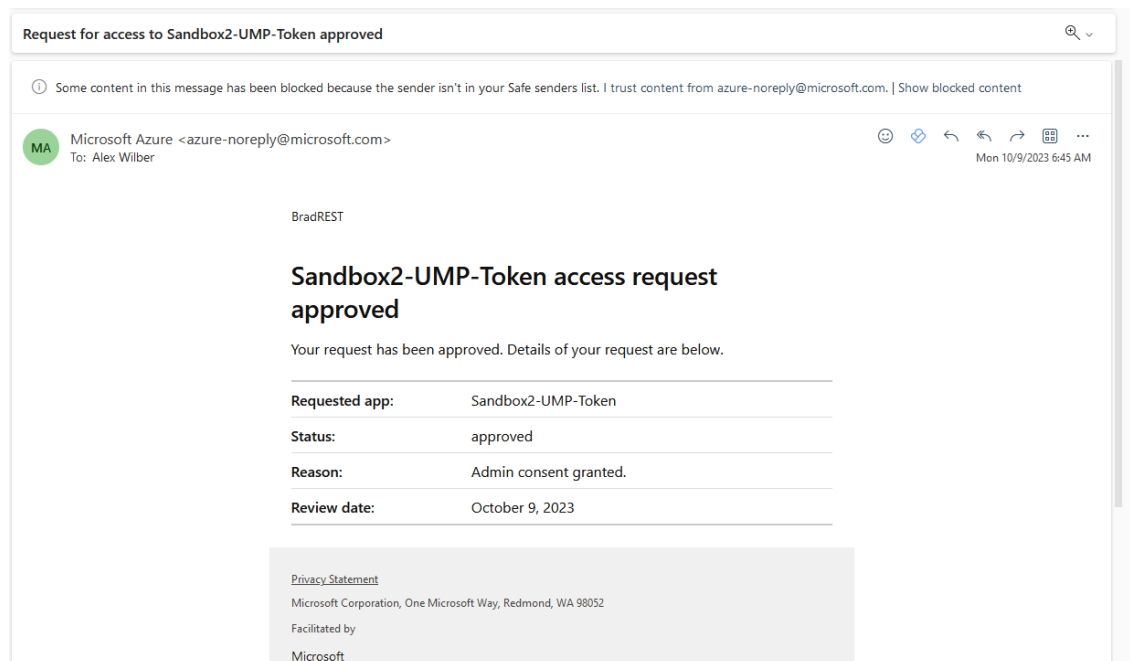


For more information, see <https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent>.

15. Once approved, all entries under **My Pending** are removed.



In addition, the following confirmation email is received by the customer administrator when the request is approved.

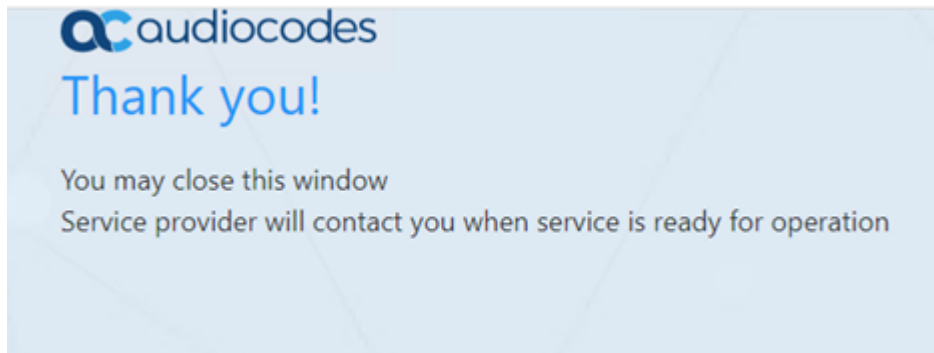


16. The Token authentication process is complete, close the window.

Thank you!

You may close this window

Service provider will contact you when service is ready for operation



17. Click **Pending Customers** to monitor the process of the request (see [Pending Requests](#) on page 381). Verify that Status is shown as **Authentication Complete**.
18. Likewise, open the Multitenant interface and navigate to **Security > Customer Invitations**. Verify that Device Authenticated is shown as **true**.
19. Open the newly created Token registration on the Azure portal for the customer tenant (Enterprise Applications > <Token-Registration-Name>).
20. In the Navigation pane, select **Permissions**. Note the added permissions for the new Enterprise application.

Permissions

Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). [Learn more.](#)

You can review, revoke, and restore permissions. [Learn more.](#)

[Grant admin consent for BradREST](#)

Admin consent **User consent**

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph					
Microsoft Graph	Group.ReadWrite.All	Read and write all groups	Delegated	Admin consent	An administrator
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed in user	Delegated	Admin consent	An administrator
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated	Admin consent	An administrator
Microsoft Graph	AppCatalog.ReadWrite.All	Read and write to all app catalogs	Delegated	Admin consent	An administrator
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	Admin consent	An administrator
Skype and Teams Tenant Admin API					
Skype and Teams Tenant Admin API	user_impersonation	Access Microsoft Teams and Skype for Business data as the ...	Delegated	Admin consent	An administrator

21. Resume the wizard process (see [Onboarding with Hosted Essentials +](#) on page 290 or [Onboarding with Hosted Pro](#) on page 361).

Grant Consent using only Token-based Authentication (Service Account)

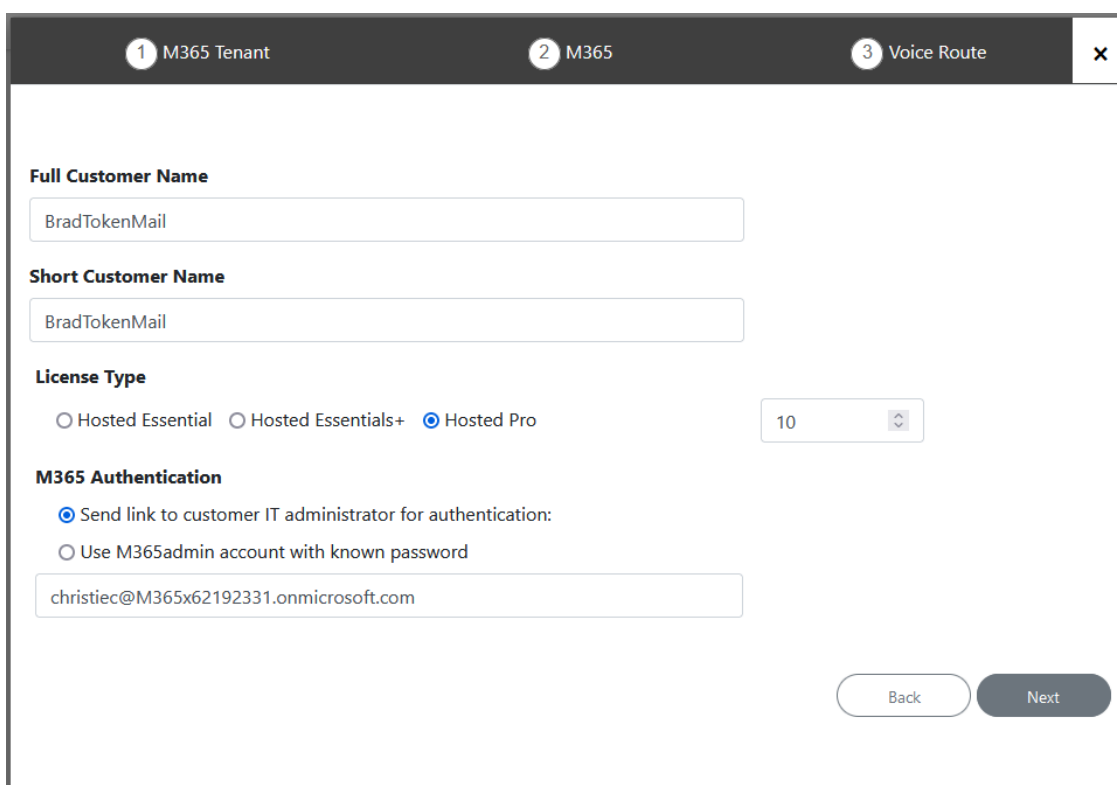
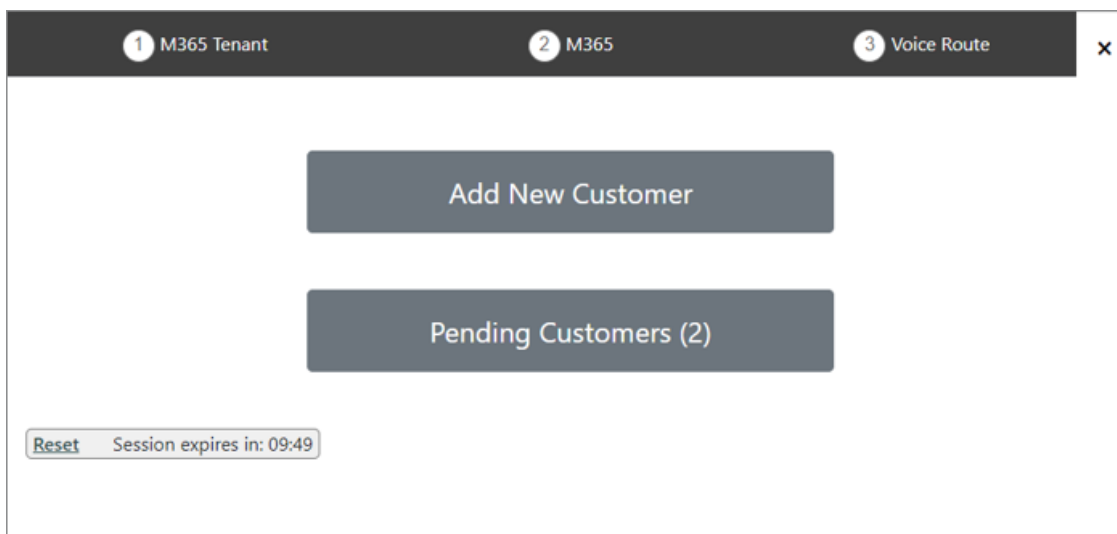
You can secure the Token connection with the customer M365 platform by sending an email to the customer Service Account with a link to trigger the Token Authentication Invitation wizard.



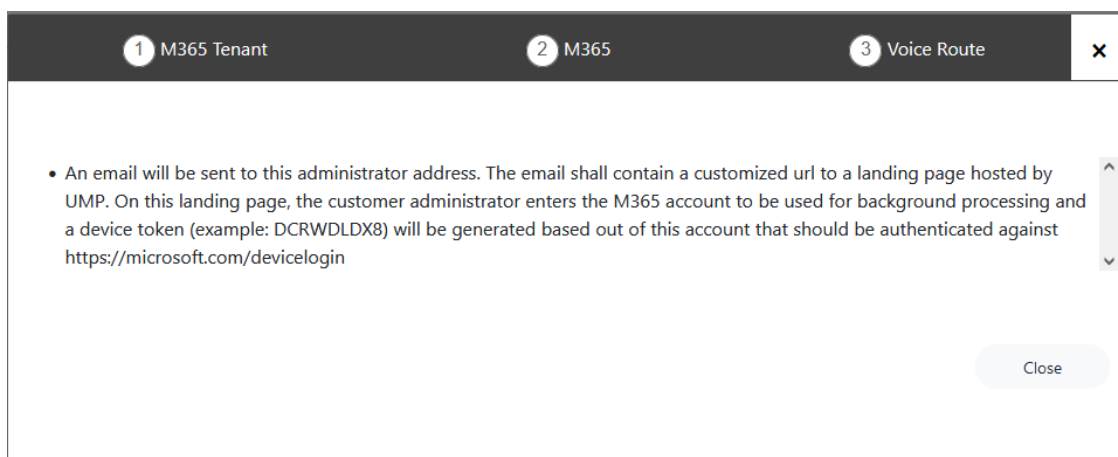
Ensure that the customer tenant Admin has been assigned the required roles (see [Assign Administrator Roles to IT Administrator](#) on page 269).

➤ **Do the following:**

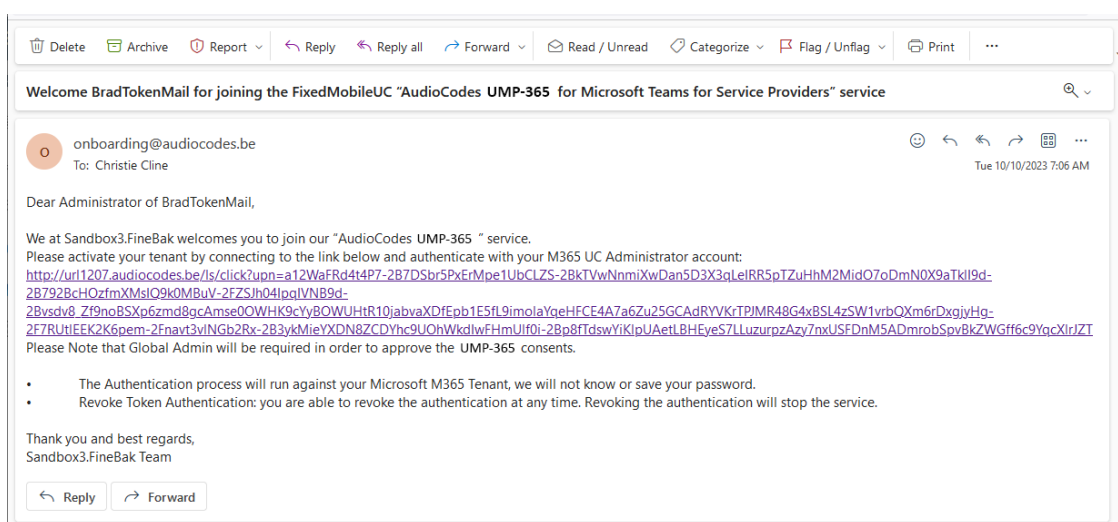
1. In the Onboarding wizard click **Add New Customer**.



2. Enter the Full and Short Customer Names.
3. Select either the **Hosted Essentials +** or **Hosted Pro** License type.
4. Set the number of required licenses.
5. Select the **Send link to customer IT administrator for authentication link**.
6. Enter the email address of the Customer administrator Service account, and then click **Next**. An email is sent to the customer administrator, and the following information message is displayed.



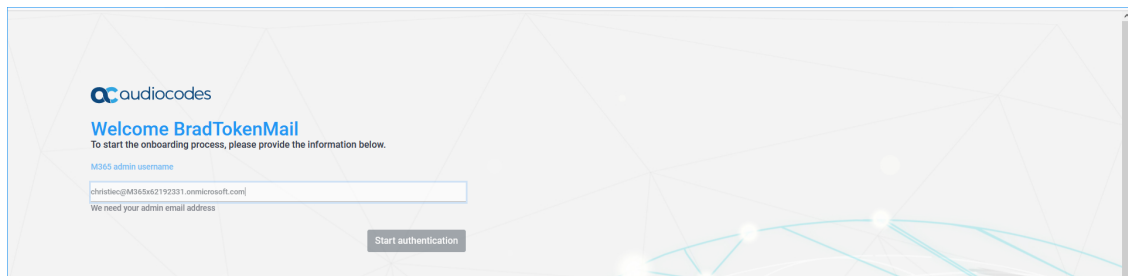
7. Open the email of Customer tenant Service account administrator.



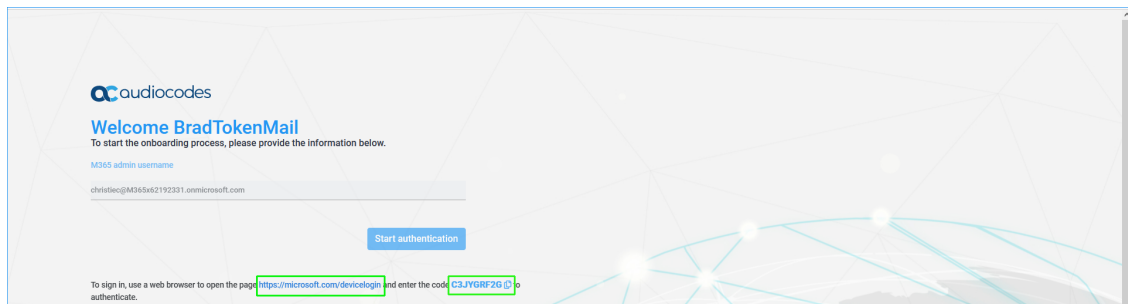
If a email has not been received, open the Multitenant interface and navigate to **Security > Customer Invitations**. Search for the relevant token and validate that Email Sent is 'True'. In addition, check the email settings (see [Configuring Email Settings](#) on page 69).

ID	Full Name	Invitation Email	M365 Admin Email	Email Sent	Email Invitation Sent Count	Created at	Expires at	Device Authenticated	Invitation Type	Tenant Installed	Actions
BradTokenMail	BradTokenMail	christie@audiocodes.be	christie@audiocodes.be	true	1	2023-10-10	2023-10-13		Invite	No	Send Invitation Revoke Request Auth Info

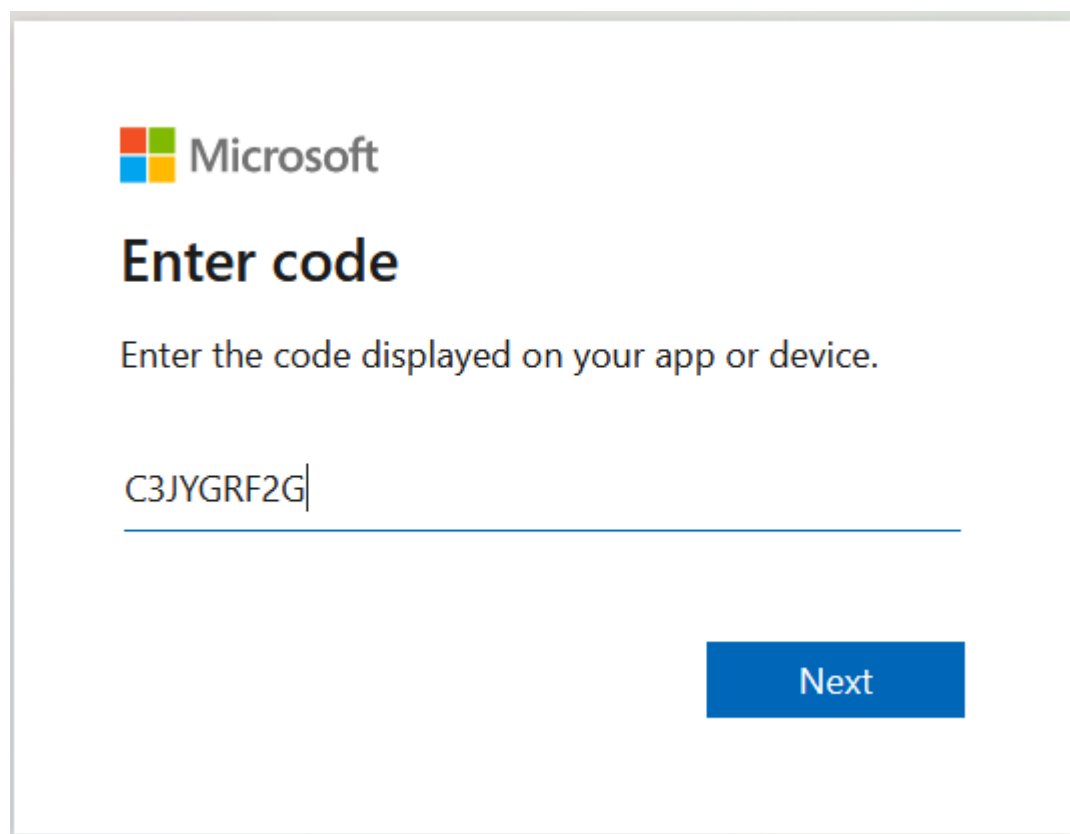
8. Click the link sent in the e-mail as shown in the example above. The Token Invitation Wizard Welcome screen is displayed.



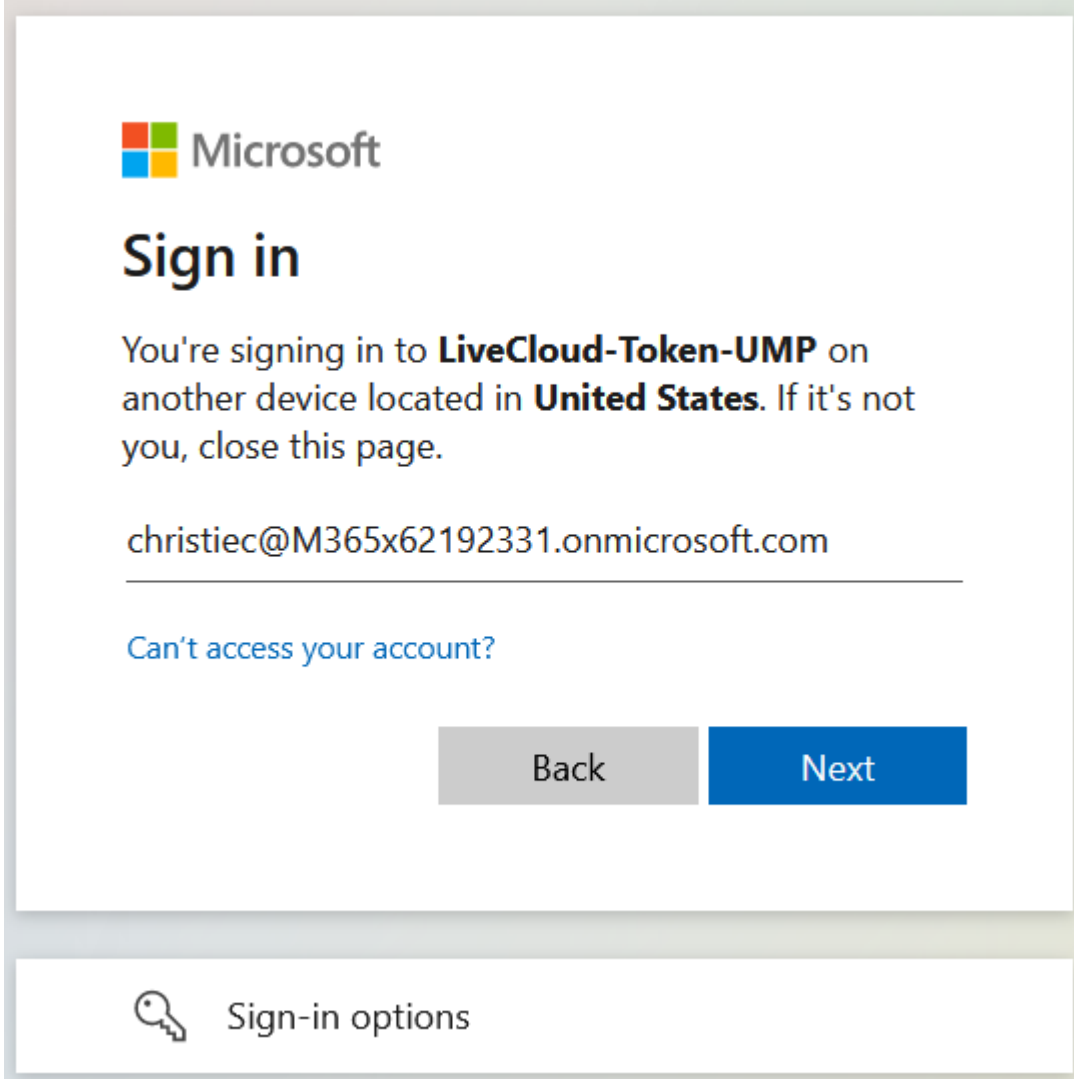
9. Enter the credentials of the customer Service account, and then click **Start authentication**.



10. Copy the code at the bottom of the screen and then click the Web browser link.



11. Paste the code and then click **Next**.



The image shows a Microsoft sign-in interface. At the top is the Microsoft logo. Below it is the heading "Sign in". A message states: "You're signing in to **LiveCloud-Token-UMP** on another device located in **United States**. If it's not you, close this page." Below this message is a text input field containing the email address "christiec@M365x62192331.onmicrosoft.com". Under the input field is a link that says "Can't access your account?". At the bottom right are two buttons: a grey "Back" button and a blue "Next" button. At the bottom left is a link icon (a key) followed by the text "Sign-in options".

Microsoft


Sign in

You're signing in to **LiveCloud-Token-UMP** on another device located in **United States**. If it's not you, close this page.


christiec@M365x62192331.onmicrosoft.com

[Can't access your account?](#)

[Back](#) [Next](#)

 [Sign-in options](#)

12. Enter the credentials of the customer tenant administrator Service account, and then click **Next**.

 **CONTOSO** demo

christiec@m365x62192331.onmicrosoft.com

Approval required

unverified

This app requires your admin's approval to:

- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to

New UMP-365 customer

[Sign in with another account](#)

Does this app look suspicious? [Report it here](#)

CancelRequest approval

Contoso

13. Enter the reason for Sign-in request and then click **Request approval**.



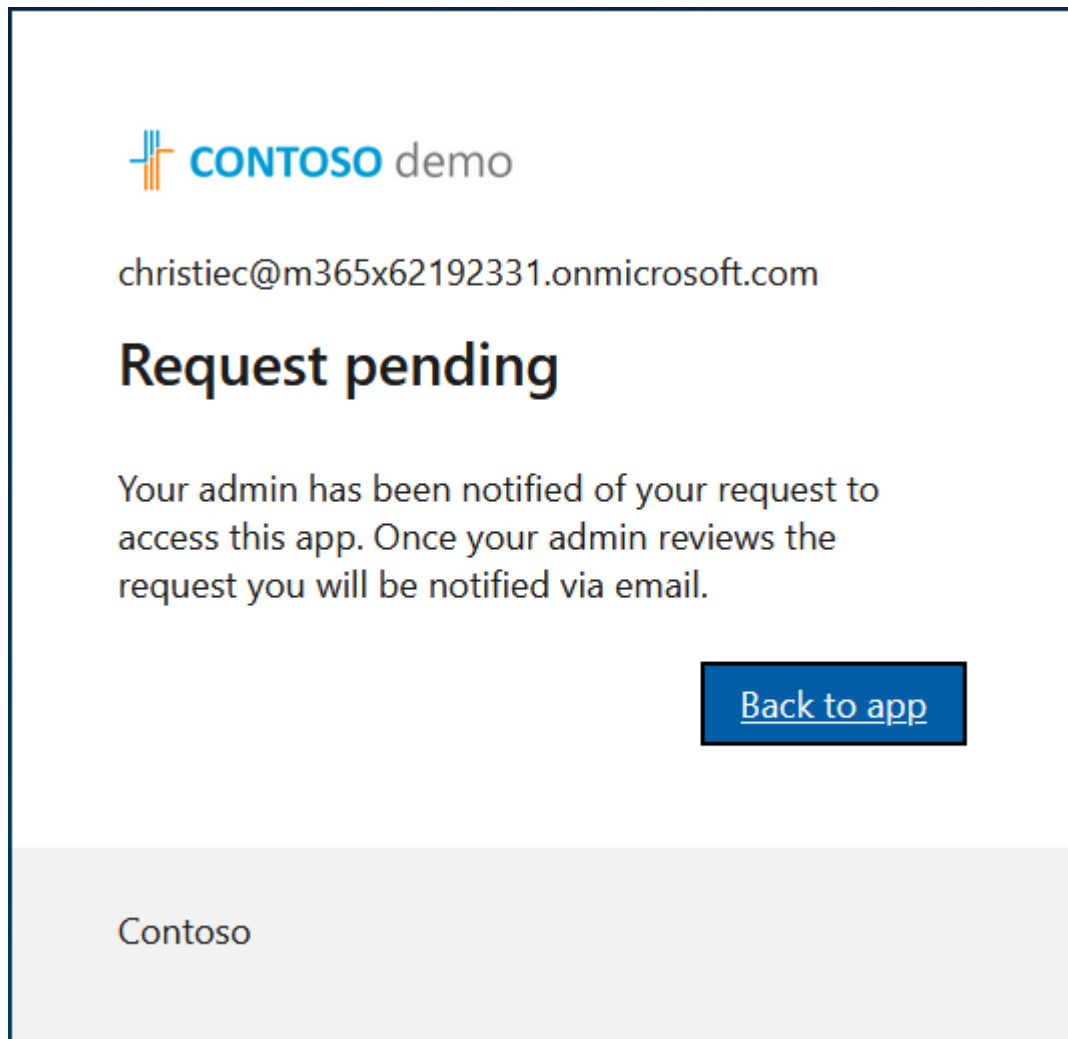
christiec@m365x62192331.onmicrosoft.com

Request sent

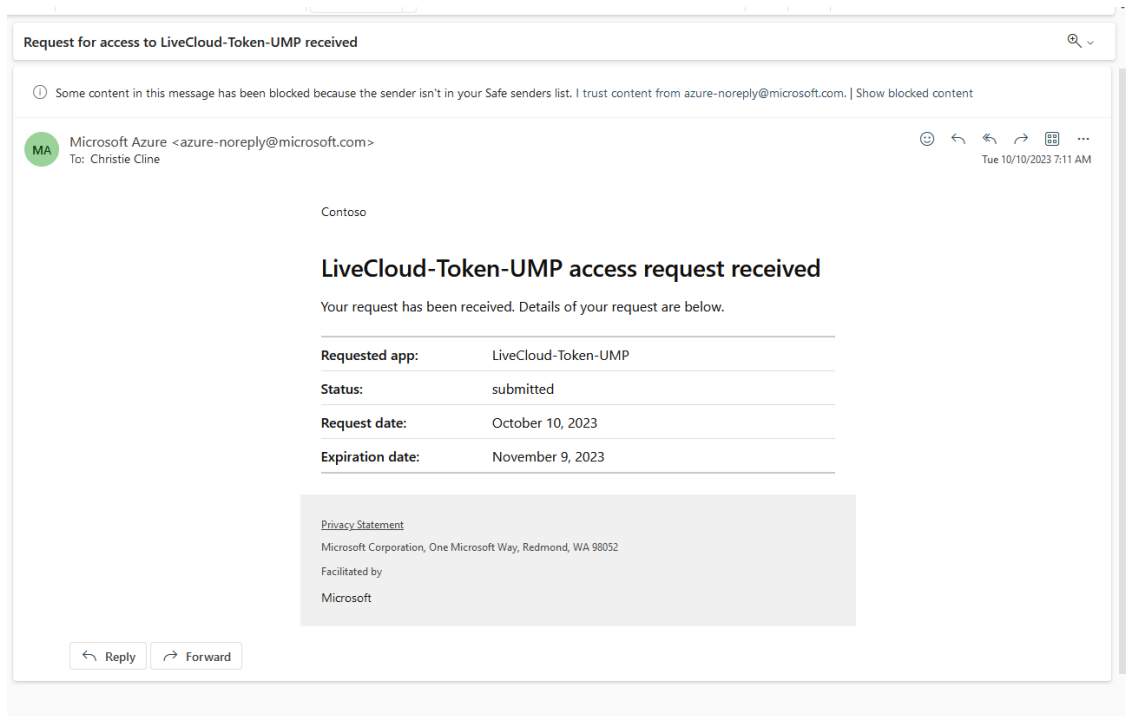
Your admin has been notified of your request to access this app. Once your admin reviews the request you will be notified via email.

[Back to app](#)

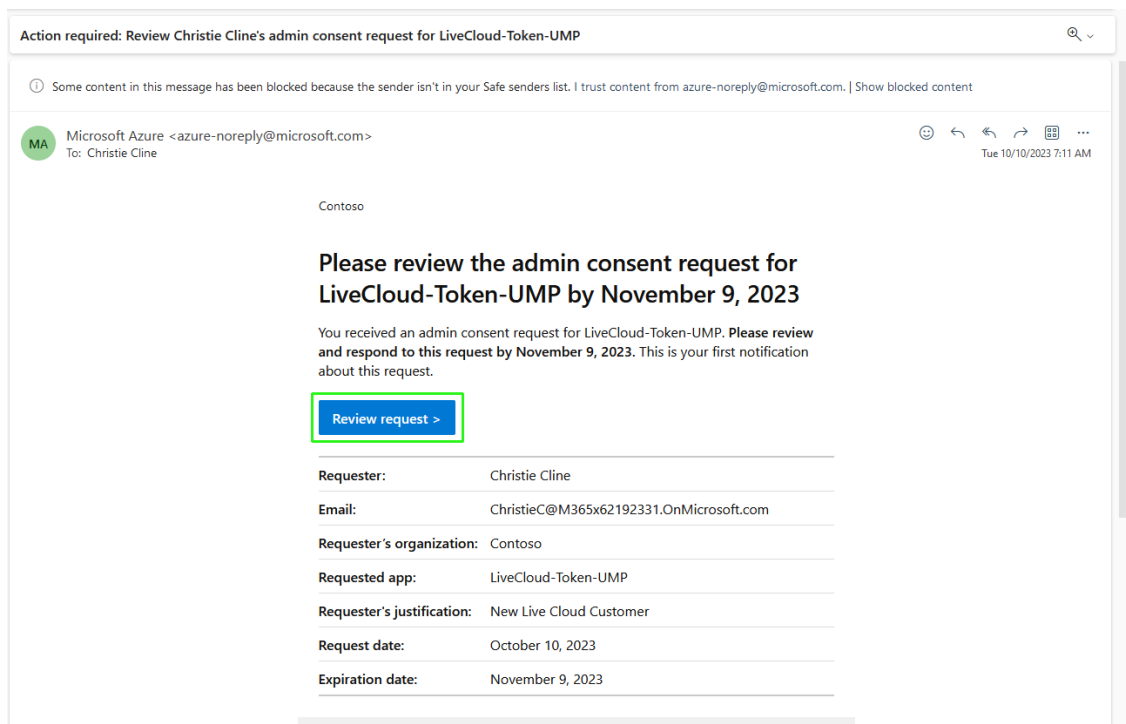
Contoso



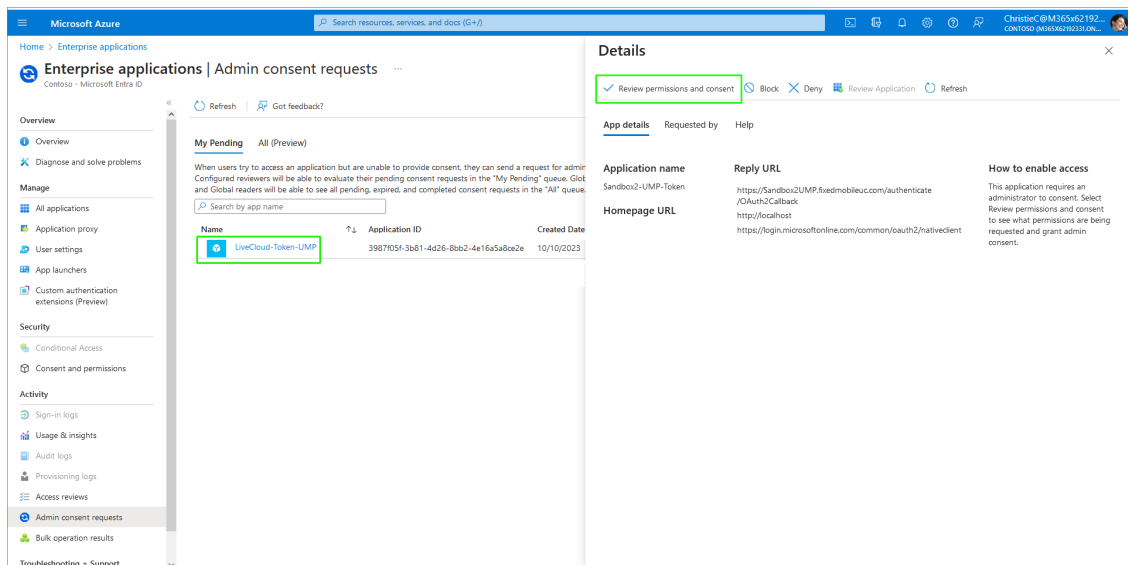
14. Open the email of the customer Service account. View the example mail message below indicating the request to access the Customer tenant M365 platform.



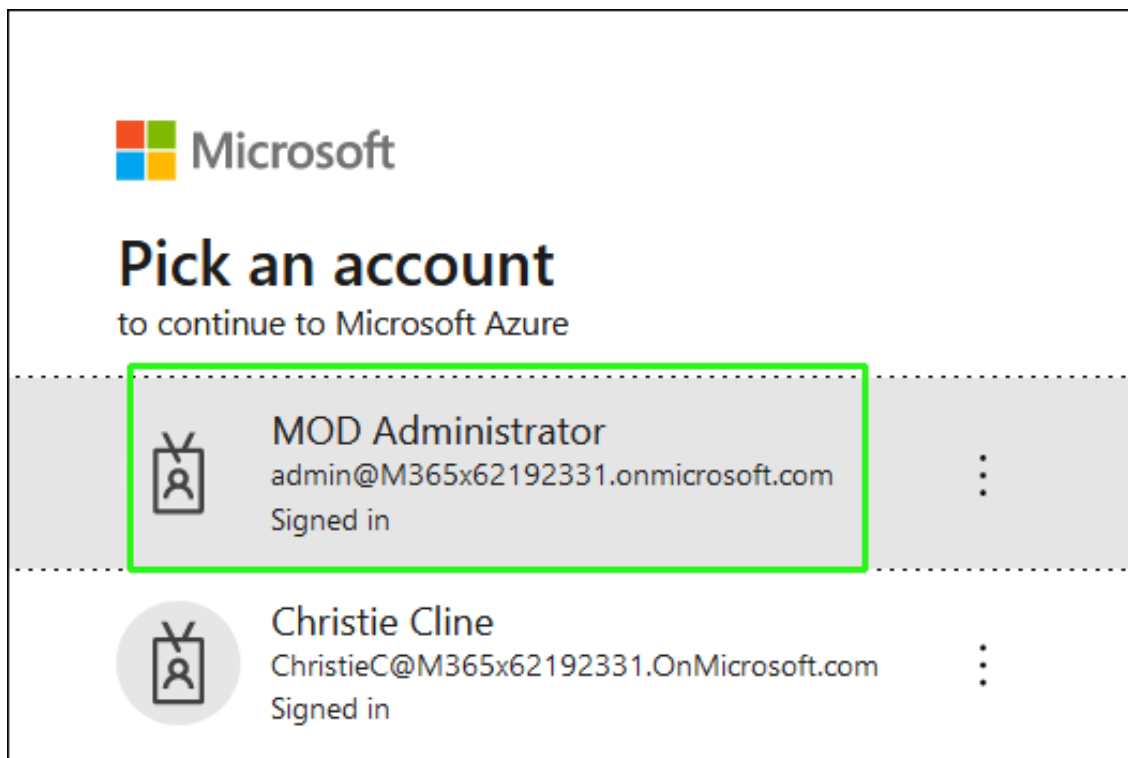
15. Another mail is then received requesting to review the admin consent request. Click **Review request**.



The list of Admin Consent requests requiring Admin approval are displayed.



16. Select the relevant token request and then click **Review permissions and consent**.





admin@M365x62192331.onmicrosoft.com

Permissions requested

Sandbox2-UMP-Token

unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to
- ☒ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

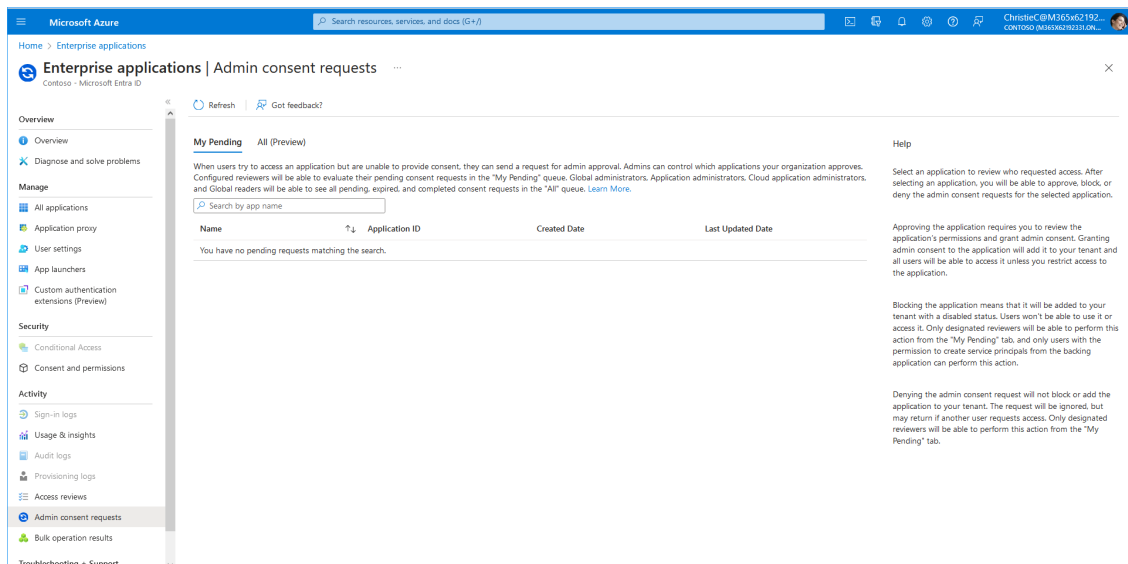
Cancel

Accept

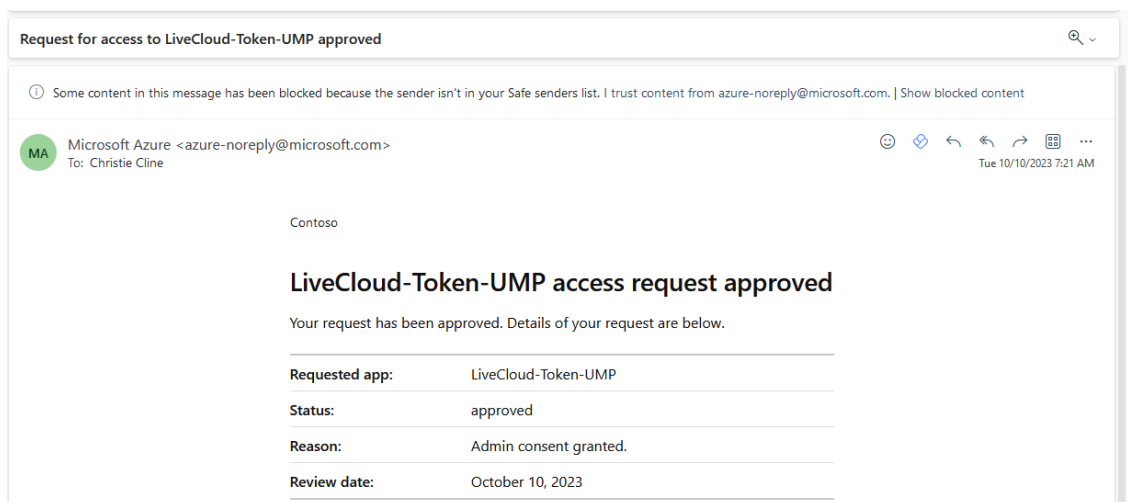


For more information, see <https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/grant-admin-consent>.

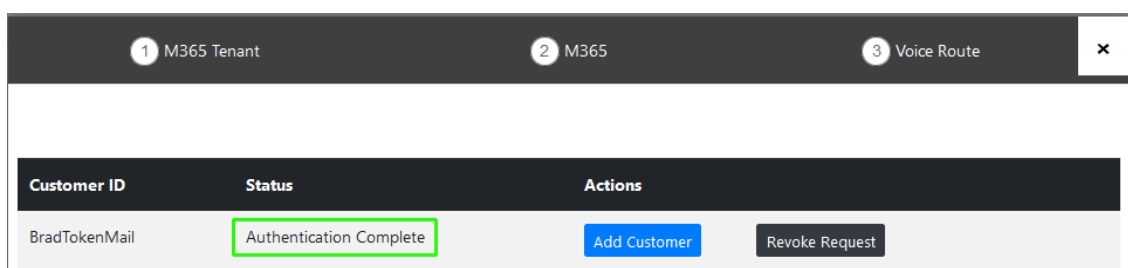
17. Choose the Global admin account of the customer tenant. Once approved, all entries under **My Pending** are removed.



In addition, the customer administrator receives an email similar to the following when the request is approved.



18. Click **Pending Customers** to monitor the process of the request (see [Pending Requests](#) on page 381). Verify that Status is shown as **Authentication Complete**.



19. Likewise, open the Multitenant interface and navigate to **Security > Customer Invitations**. Verify that Device Authenticated is shown as **true**.

ID	Full Name	Invitation Email	M365 Admin Email	Email Sent	Email Invitation Sent Count	Created at	Expires at	Device Authenticated	Invitation Type	Tenant Installed	Actions
BradGlobalToken	BradGlobalToken	admin@M365x35340067.onmicrosoft.com	admin@M365x35340067.onmicrosoft.com	true	1	2023-10-11	2023-10-16	true	Invite	No	Send Reminder Revoke Request Auth URL
BradTokenMail	BradTokenMail	christie@M365x62192331.onmicrosoft.com		true	1	2023-10-10	2023-10-15	true	Invite	No	Send Reminder Revoke Request Auth URL

20. Open the newly created Token registration on the Azure portal for the customer tenant (Enterprise Applications > <Token-Registration-Name>).
21. In the Navigation pane, select **Permissions**. Note the added permissions for the new Enterprise application.

The screenshot shows the 'Permissions' page for the 'LiveCloud-Token-UMP' Enterprise Application in the Microsoft Azure portal. The page lists several permissions granted to the application, including 'Group.ReadWrite.All', 'Directory.AccessAsUser.All', 'User.Read.All', 'AppCatalog.ReadWrite.All', 'offline_access', 'profile', and 'openid'. Each permission is associated with a 'Microsoft Graph' API and is granted through 'Admin consent' by an administrator.

22. Continue the Onboarding wizard , see [Onboarding with Hosted Pro](#) on page 361 or [Onboarding with Hosted Essentials +](#) on page 290.

Onboarding with both M365 Default Routing and SBC Configuration

This section describes how to onboard new customers by applying the default M365 Onboarding script. This option also allows you to automatically configure the customer DNS domain as part of the Onboarding script. Once M365 has been configured, the wizard continues with the SBC configuration.

➤ To onboard with M365 default routing:

1. Select option **Configure M365 default routing**, the following screen is displayed:

1 M365 Tenant
2 M365
3 Voice Route
✕

☒ **Configure M365 default routing**

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

Online PSTN Gateway

M365 Onboarding Script

M365 Cleanup Script



Customer Variables	Value

Back
Next

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

Table 31-3: M365 Default Routing

O365 Setting	Description
Click here to Provision M365 Domain and DNS Automatically	Support for automatic and semi-automatic DNS provisioning (see Setting up Fully Automatic DNS Provisioning on page 70 and Setup Two-step Provisioning on page 250 respectively).
Region/Country	The customer SBC region sub domain name (see Configure DNS API on page 82).
IP Address	Preconfigured IP address of the region SBC (see Configure DNS API on page 82).
SBC	Preconfigured FQDN of the region SBC (see Configure DNS API on page 82).
Domain Name	Preconfigured domain name of the DNS (A-record) (see Creating A Records for SBC Devices on page 74).
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.

O365 Setting	Description
Other Configuration	
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 Register End Customer Tenant DNS Sub domains on page 250).</p>
M365 Onboarding Script	<p>Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Customer Variables.</p> <p>Click the  to edit the Onboarding script file. For example, when a service provider needs a separate registration per customer tenant. See Default M365 Tenant Onboarding Script on page 191.</p>
M365 Cleanup Script	<p>Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Customer Variables.</p> <p>Click the  to edit the Cleanup script file. See Default M365 Tenant Cleanup Script on page 193.</p>
Customer Variables	<p>Script variables can be customized and loaded to the M365 Onboarding and Cleanup scripts. See Customer Variables on page 210.</p>

The wizard continues with the SBC configuration.

1 M365 Tenant

2 M365

3 Voice Route

X

Customer: HostedPlus

☒ **Configure SBC**

Sbc Site Name

Online PSTN Gateway

Sbc Configuration: ☒ Sip Trunk ☐ IP PBX ☐ BYOC

Region

Carrier

☐ **Carrier Registration**

☐ **Enable Cac**

Back

Next

Sbc Configuration: ☒ Sip Trunk ☐ IP PBX ☐ BYOC

Region

Carrier

☒ **Carrier Registration**

☒ **Enable Cac**

Back

Next

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

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
ddswfdsds

SIPMain
O365Host

☒ Enable Cac

1 session
1 session
5 sessions
10 sessions
20 sessions
1000 sessions

Back
Next

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

Table 31-4: 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 Register End Customer Tenant DNS Sub domains on page 250).</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: SIP Trunk used by Service Provider. ■ IP-PBX-Service Provider IP-PBX ■ BYOC (Bring-Your-Own-Carrier) for integrating customer SIP Trunk services that are different to the SIP Trunk service used by their Service Provider.
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.

O365 Setting	Description
	<ul style="list-style-type: none"> ■ 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.

4. Click **Next**, the Wizard continues with the configuration of the SBC Number Prefixes. For initial setup, a Dialplan file must be preconfigured on the SBC or IP-PBX. For Second day management, SBC prefixes can later be imported (see [Manage SBC Prefixes](#) on page 533).

The screenshot shows a configuration wizard with three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. The current step is 2 M365. The main area is titled 'SBC number prefixes' and contains a 'Browse...' button with the text 'No file selected.' Below this is a text input field labeled 'New Number prefix' with a green plus icon to its right. At the bottom right are 'Back' and 'Next' buttons.

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

Table 31-5: Define Prefixes

Setting	Description
Update from CSV	Browse to load a CSV file containing a range of telephone prefixes.

Setting	Description
Telephone Number Prefix	Enter a specific telephone number prefix.

1 M365 Tenant
2 M365
3 Voice Route

SBC number prefixes

Browse... pbxexample.csv pbxexample.csv

New Number prefix +

Back Next

1 M365 Tenant
2 M365
3 Voice Route

SBC number prefixes

Browse... No file selected.

New Number prefix +

314 X

Back Next

1 M365 Tenant
2 M365
3 Voice Route



SBC Onboarding Script sbc-scenario7

SBC Cleanup Script sbc-scenario7Cleanup

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

Back Submit

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 [Managing Onboarding Script Templates](#) on page 170.

7. When you have completed the configuration, click

Submit

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

Fully Automatic DNS Provisioning

This section describes how to automatically create the DNS record using the Onboarding wizard (see [Two-step DNS Provisioning](#) on page 411).

1. Click **Here to Provision M365 Domain and DNS Automatically**.

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

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

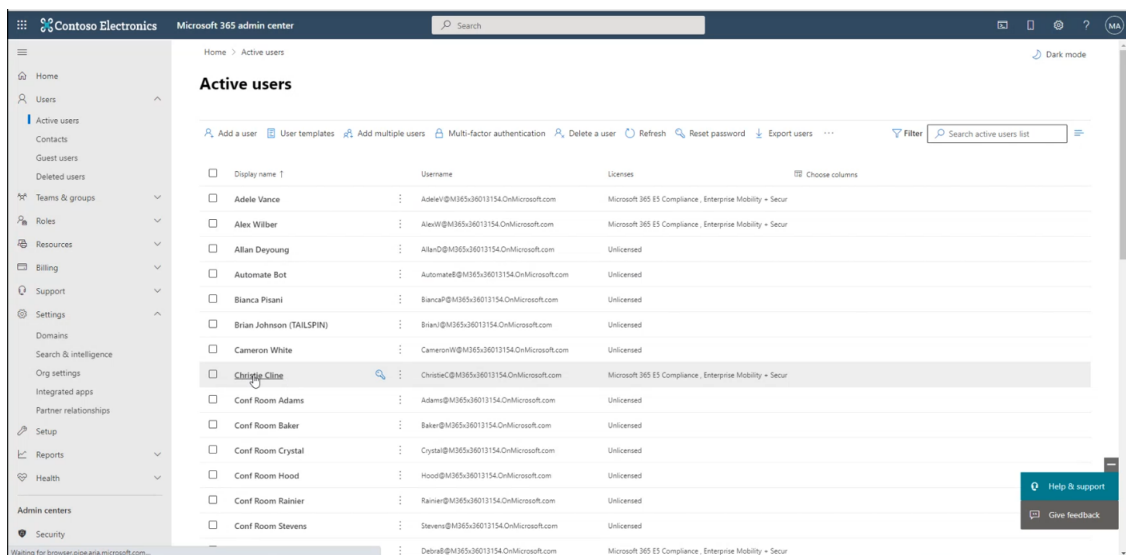
License Plan

Reload

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

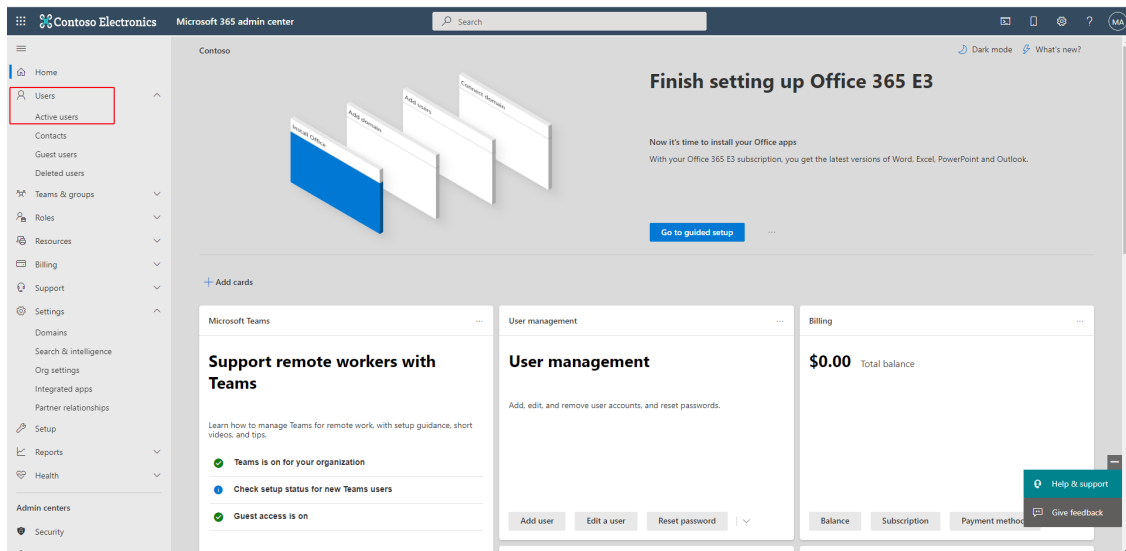
Back
Next

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



3. Open the Microsoft 365 admin center for the customer tenant.

4. In the Navigation pane, select **Users** > **Active users**.



5. Select any licensed user.

The screenshot shows the Microsoft 365 admin center interface. On the left is a navigation pane with options like Home, Users, Teams & groups, Roles, Resources, Billing, Support, Settings, Domains, Search & intelligence, Org settings, Integrated apps, Partner relationships, Setup, Reports, Health, Admin centers, Security, and Compliance. The main area is titled 'Active users' and contains a table of users. The user 'Christie Cline' is selected, and her profile card is visible on the right.

Display name	Username	Licenses
Adele Vance	AdeleV@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Security
Alex Wilber	AlexW@M365x36013154.OnMicrosoft.com	Microsoft 365 E5 Compliance, Enterprise Mobility + Security
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	Microsoft 365 E5 Compliance, Enterprise Mobility + Security
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 + Security

This screenshot shows the 'Licenses and apps' page for the user 'Christie Cline'. The page displays a list of available licenses and the current assignment. The 'Office 365 E5' license is currently assigned to the user.

License	Available
Enterprise Mobility + Security E5	1 of 20 licenses available
Microsoft 365 E5 Compliance	2 of 20 licenses available
Microsoft Power Automate Free	9999 of 10000 licenses available
Office 365 E3	1 of 2 licenses available
Office 365 E5	1 of 20 licenses available
Windows 10/11 Enterprise E3	18 of 20 licenses available

This screenshot shows the 'Licenses and apps' page for the user 'Christie Cline' after the 'Office 365 E5' license has been deselected. The 'Office 365 E5' license is now shown as 'Unlicensed' in the table, and the 'Save changes' button is visible at the bottom.

License	Available
Enterprise Mobility + Security E5	1 of 20 licenses available
Microsoft 365 E5 Compliance	2 of 20 licenses available
Microsoft Power Automate Free	9999 of 10000 licenses available
Office 365 E3	1 of 2 licenses available
Office 365 E5	1 of 20 licenses available
Windows 10/11 Enterprise E3	18 of 20 licenses available

6. 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

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

Reload

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

BackNext

7. 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 following figure, the OFFICE 365 E5 license is 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.

1 M365 Tenant

2 M365

3 Voice Route

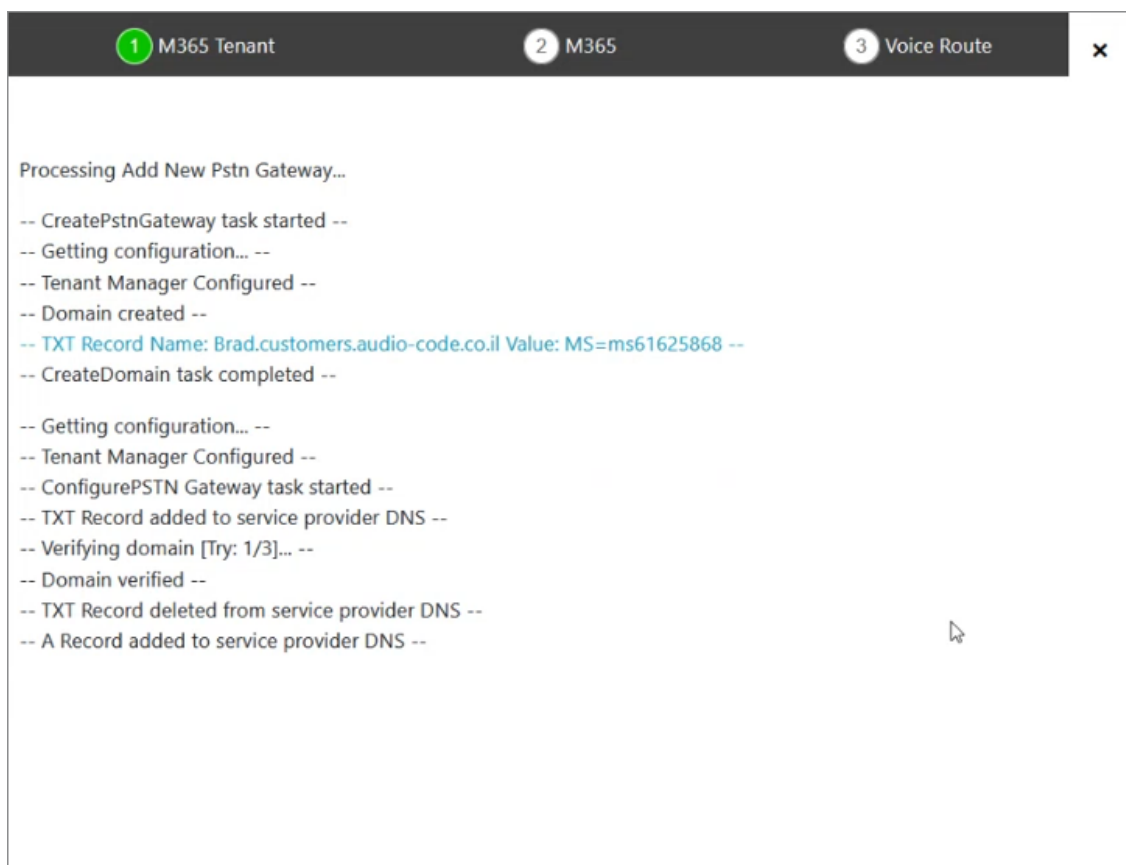
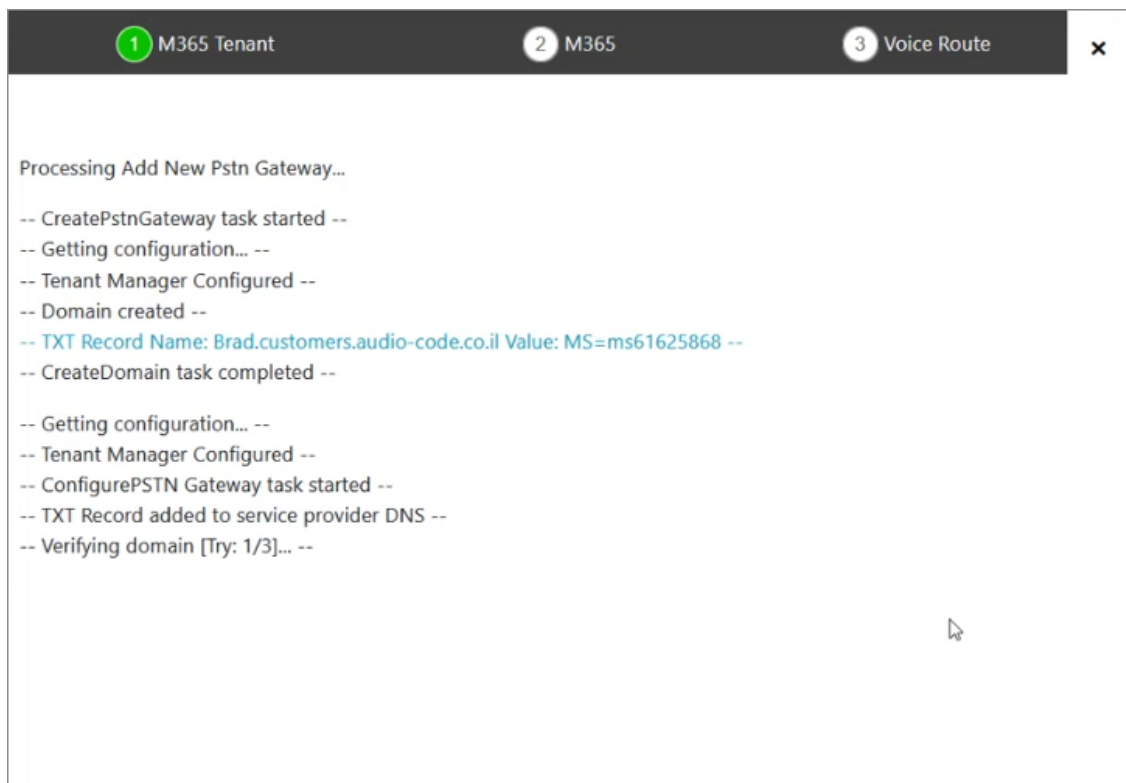
✕

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.



1 M365 Tenant
2 M365
3 Voice Route

Processing Add New Pstn Gateway...

```
-- CreatePstnGateway task started --
-- Getting configuration... --
-- Tenant Manager Configured --
-- Domain created --
-- TXT Record Name: Brad.customers.audio-code.co.il Value: MS=ms61625868 --
-- CreateDomain task completed --

-- Getting configuration... --
-- Tenant Manager Configured --
-- ConfigurePSTN Gateway task started --
-- TXT Record added to service provider DNS --
-- Verifying domain [Try: 1/3]... --
-- Domain verified --
-- TXT Record deleted from service provider DNS --
-- A Record added to service provider DNS --
-- User created with OFFICE 365 E5 license--
-- Verify and Configure Domain task completed --
```

[Back to M365 Scripts](#)


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

1 M365 Tenant
2 M365
3 Voice Route

☒ **Configure M365 default routing**

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

Online PSTN Gateway

M365 Onboarding Script 

M365 Cleanup Script

Customer Variables	Value

Back Next

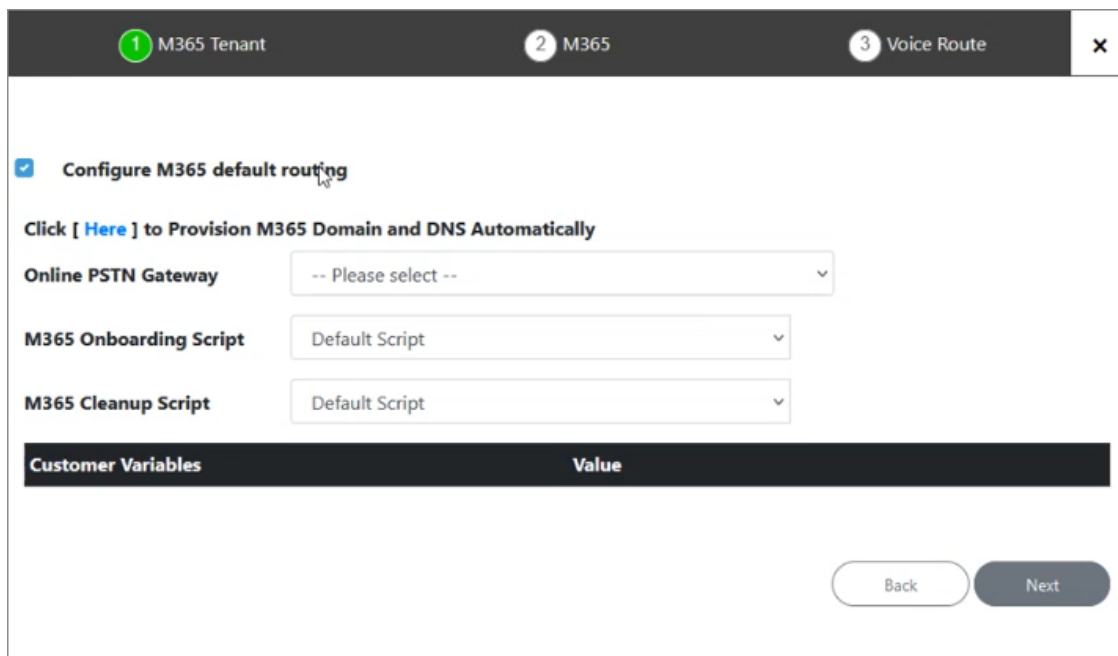
- Complete the Onboarding wizard as described in [Onboarding with both M365 Default Routing and SBC Configuration](#) on page 333.

Two-step DNS Provisioning

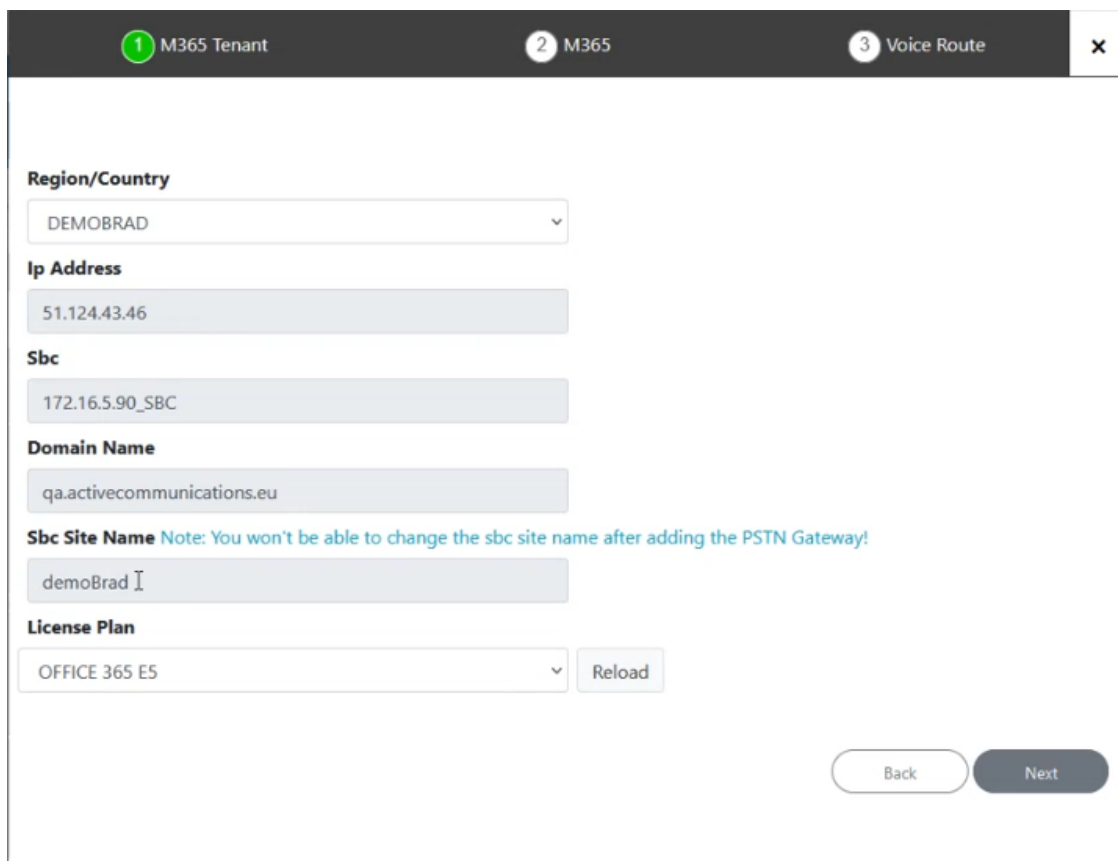
This procedure describes how to run the Onboarding Wizard to provision a DNS subdomain using the two-step method.

➤ Do the following:

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



The screenshot shows the 'M365 Tenant' step of the Onboarding Wizard. The progress bar at the top indicates three steps: 1. M365 Tenant (active), 2. M365, and 3. Voice Route. A checkbox labeled 'Configure M365 default routing' is checked. Below it, a link says 'Click [Here] to Provision M365 Domain and DNS Automatically'. There are three dropdown menus: 'Online PSTN Gateway' (set to '-- Please select --'), 'M365 Onboarding Script' (set to 'Default Script'), and 'M365 Cleanup Script' (set to 'Default Script'). Below these is a table with two columns: 'Customer Variables' and 'Value'. At the bottom right are 'Back' and 'Next' buttons.



The screenshot shows the 'M365' step of the Onboarding Wizard. The progress bar at the top indicates three steps: 1. M365 Tenant, 2. M365 (active), and 3. Voice Route. The form contains several fields: 'Region/Country' (dropdown set to 'DEMOBRAD'), 'Ip Address' (text field with '51.124.43.46'), 'Sbc' (text field with '172.16.5.90_SBC'), 'Domain Name' (text field with 'qa.activecommunications.eu'), 'Sbc Site Name' (text field with 'demoBrad'), and 'License Plan' (dropdown set to 'OFFICE 365 E5'). A note next to 'Sbc Site Name' says 'Note: You won't be able to change the sbc site name after adding the PSTN Gateway!'. A 'Reload' button is next to the 'License Plan' dropdown. At the bottom right are 'Back' and 'Next' buttons.

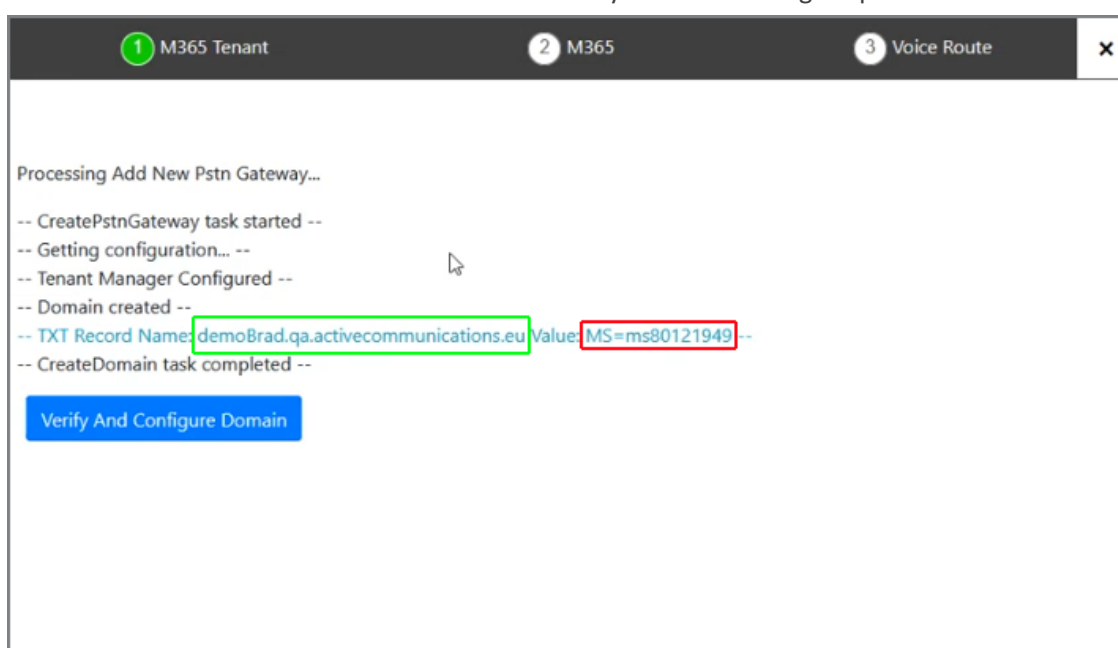
2. From the Region/Country drop-down, select the newly created region e.g. DEMOBRAD that you added in [Registering DNS Application \(Service Provider Tenant\)](#) on page 70.
3. Select the configured License Plan of the user e.g. Office 365 E5.



The Microsoft Office 365 Phone System user license should be preloaded as described in Section Activating the Providers Domain. 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.



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

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	dfcqn053hxy30pzf6dbmqj5fgqz5mp	14400	X
f4h.EMEA.activecommunications.eu	TXT	MS=ms40644176	14400	X
SBC-SIPTTrunk.activecommunications.eu	A	82.79.139.25	3600	X
SBC-SIPTTrunk.activecommunications.eu	TXT	MS=ms14688467	3600	X
<small>NEUWE RECORDS</small>				
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!

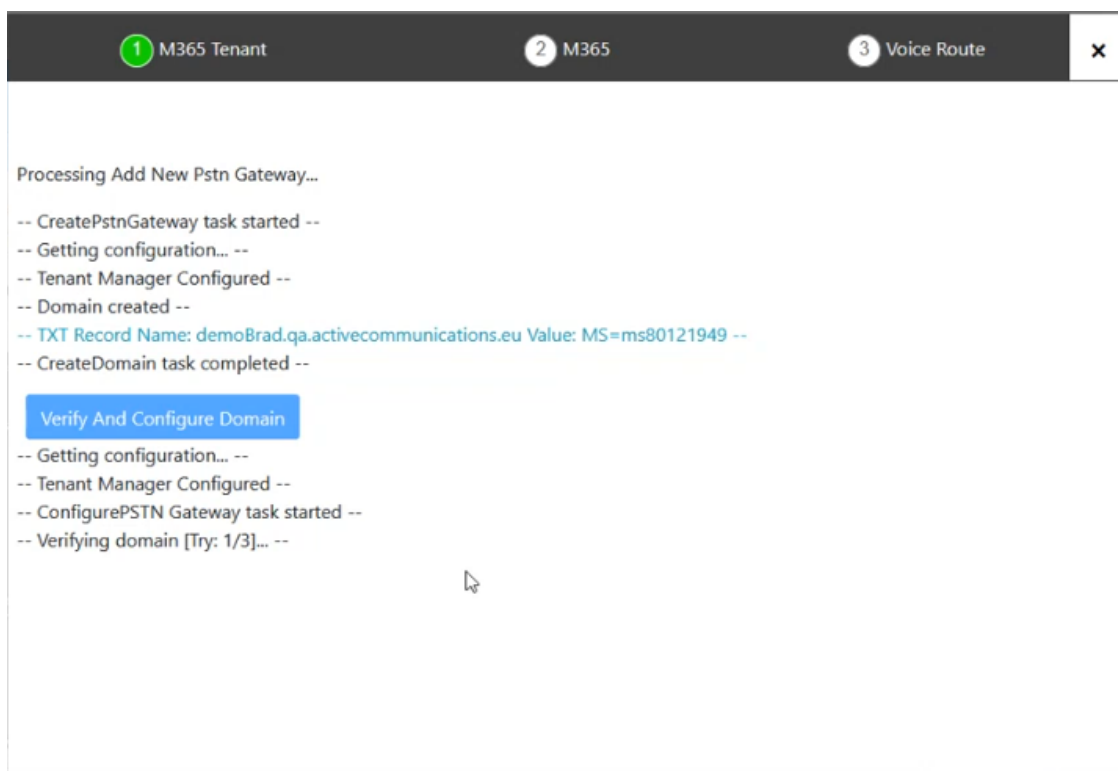
1 M365 Tenant
2 M365
3 Voice Route
X

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 --
```

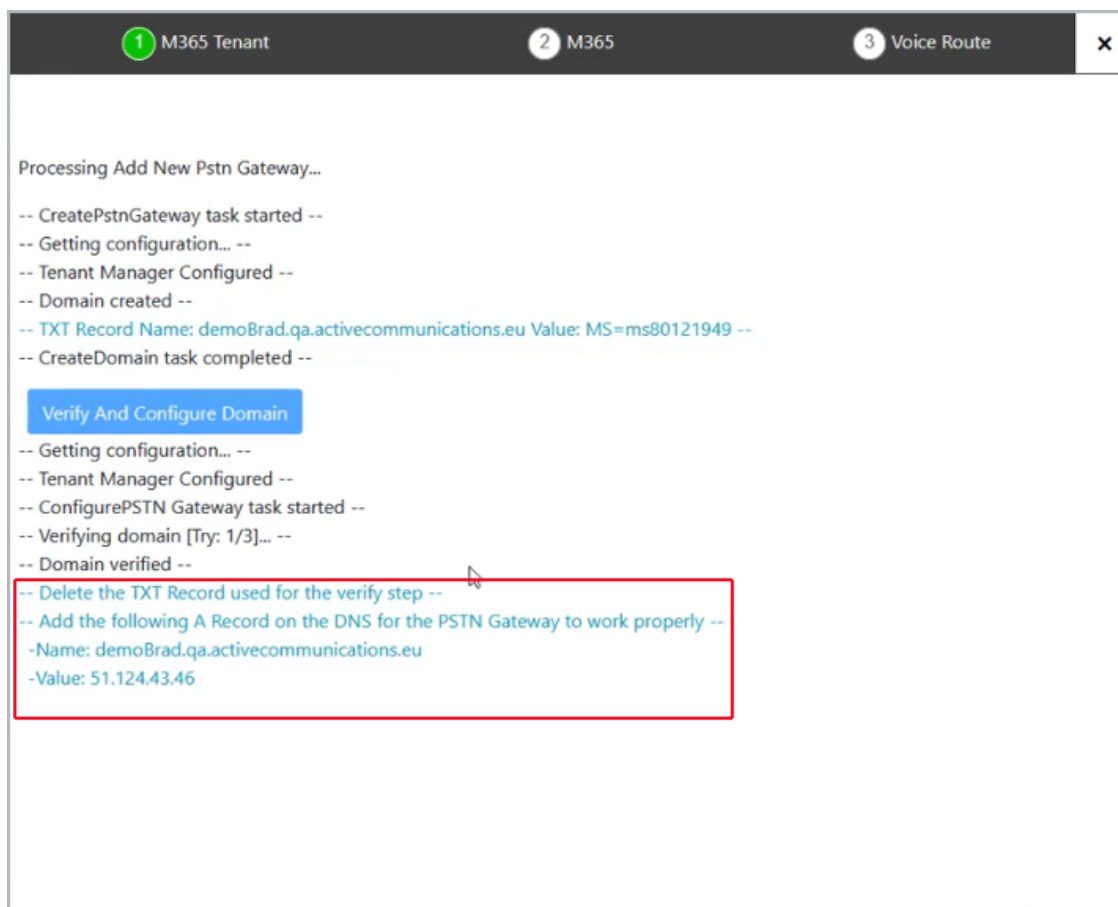
Verify And Configure Domain

6. Click **Verify and Configure Domain**.

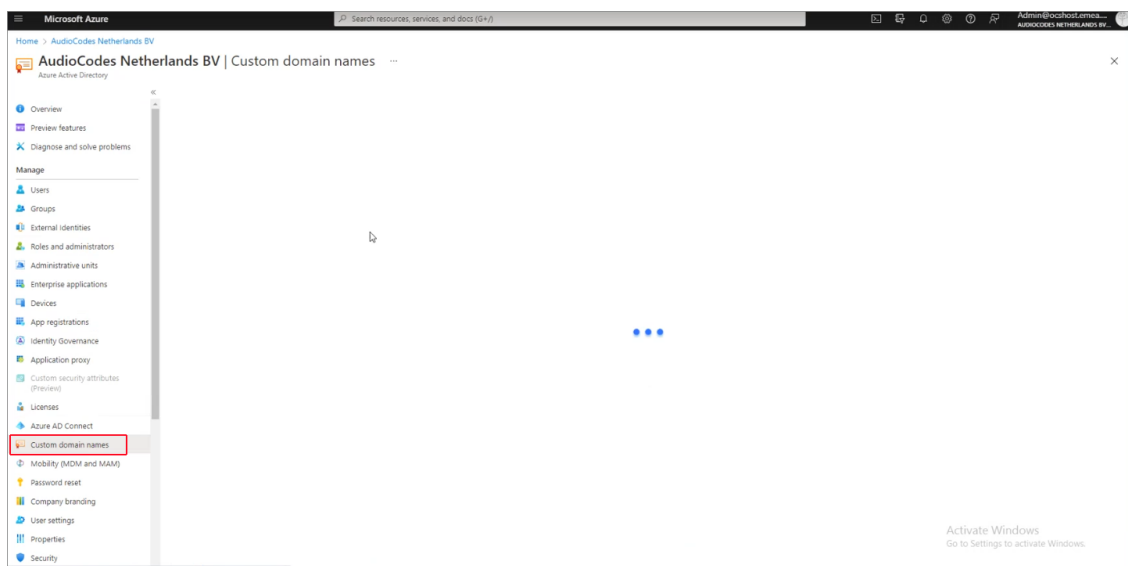


The verification process may take several tries to complete.

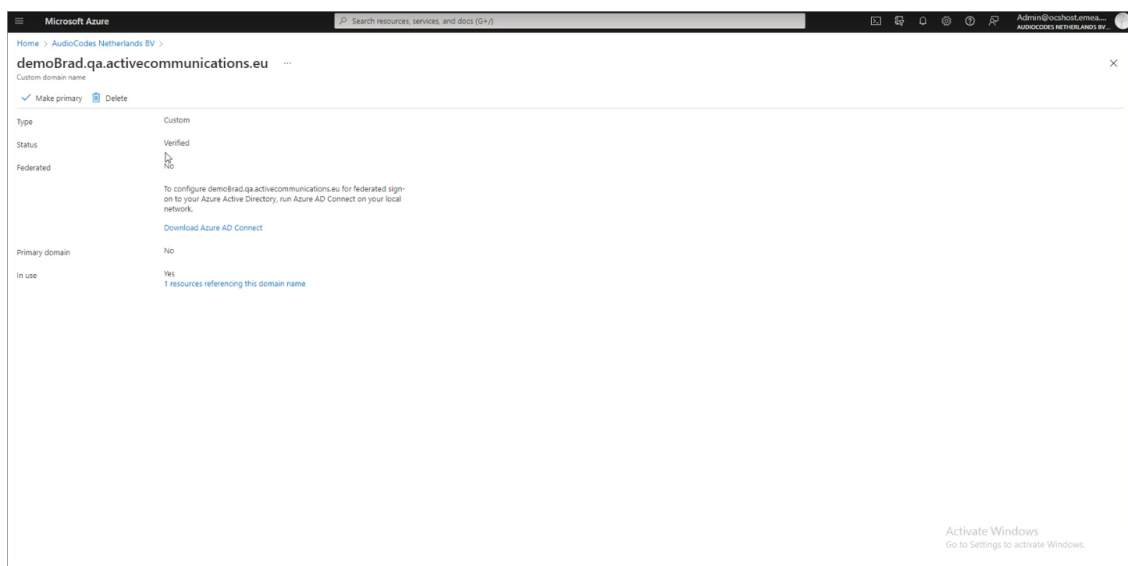
7. You are prompted to configure an A Record on the DNS Hosting platform.



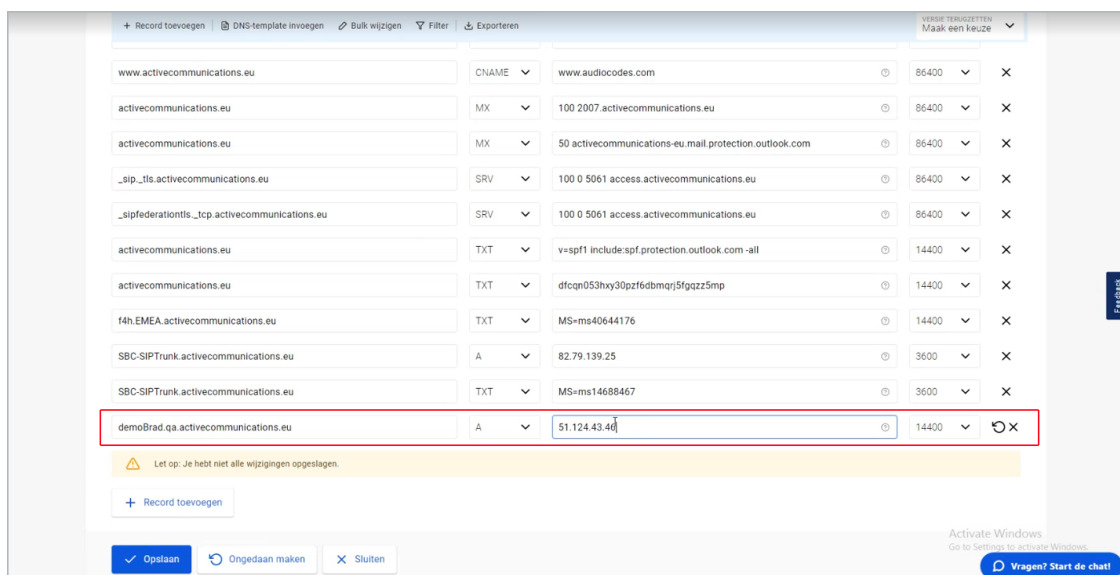
8. Open the customer Azure portal, and then in the Navigation pane, select **Custom domain names**.



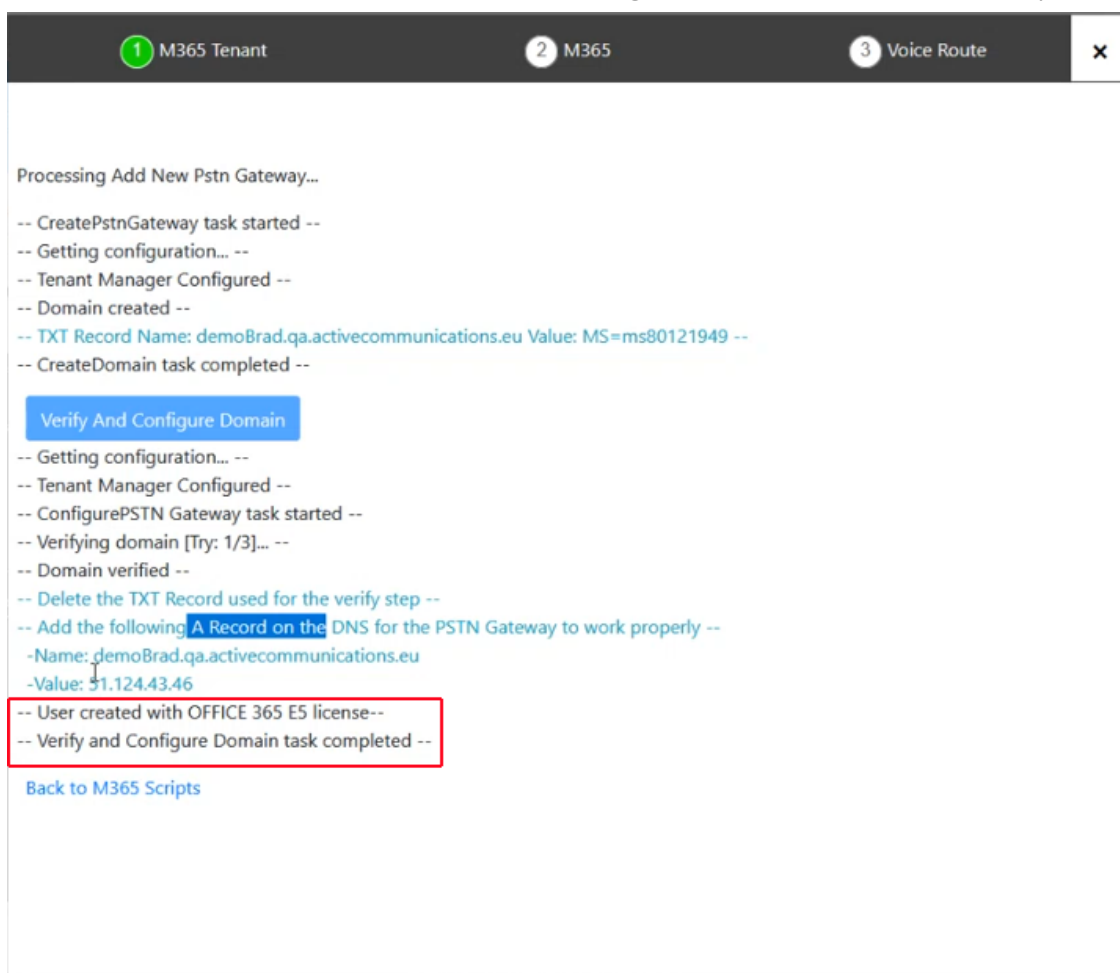
Notice the new domain that has been created.



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



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



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

The screenshot shows the 'M365 Tenant' step of the onboarding wizard. The progress bar at the top indicates three steps: 1. M365 Tenant (active), 2. M365, and 3. Voice Route. The main content area has a checkbox labeled 'Configure M365 default routing' which is checked. Below this is a link: 'Click [Here] to Provision M365 Domain and DNS Automatically'. There are three dropdown menus: 'Online PSTN Gateway' with the value 'demoBrad.qa.activecommunications.eu', 'M365 Onboarding Script' with 'Default Script', and 'M365 Cleanup Script' with 'Default Script'. Below these is a table with two columns: 'Customer Variables' and 'Value'. At the bottom right are 'Back' and 'Next' buttons.

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

11. Click **Next** to continue.

The screenshot shows the 'M365' step of the onboarding wizard. The progress bar at the top indicates three steps: 1. M365 Tenant, 2. M365 (active), and 3. Voice Route. The main content area shows the 'Customer' as 'demoBrad'. There is a checkbox labeled 'Configure SBC' which is checked. Below this are several fields: 'Sbc Site Name' with 'demoBrad', 'Online PSTN Gateway' with 'demoBrad.qa.activecommunications.eu', 'Sbc Configuration:' with radio buttons for 'Sip Trunk' (selected), 'IP PBX', and 'BYOC', 'Region' with '172.16.5.90_SBC', and 'Carrier' with a dropdown menu showing 'Select a Carrier from list'. At the bottom left are two unchecked checkboxes: 'Carrier Registration' and 'Enable Cac'. At the bottom right are 'Back' and 'Next' buttons.

12. Complete the wizard as described in Complete the Onboarding wizard as described in [Onboarding with both M365 Default Routing and SBC Configuration](#) on page 333.

Onboarding with only SBC Configuration

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

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

Back

Next

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**

Back

Next

Sbc Configuration: ☒ Sip Trunk ☐ IP PBX ☐ BYOC

Region


Carrier

☒ **Carrier Registration**

☒ **Enable Cac**

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

Table 31-6: SBC Parameters

SBC Parameter	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 Register End Customer Tenant DNS Sub domains on page 250).</p> <div>  If Default Routing is configured, then this field is automatically filled. </div>
SBC Configuration	<p>Select one of the following SBC configuration modes:</p> <ul style="list-style-type: none"> ■ SIP Trunk: SIP Trunk used by Service Provider. When this option is selected, you must select both the SBC device (see 'Region' field below) and the Service Provider Carrier SIP Trunk (see 'Carrier' field below). ■ IP-PBX: Service Provider IP-PBX. When this option is selected, you must select both the SBC device and the Service Provider Carrier SIP Trunk (see 'Region' field below). ■ BYOC: (Bring-Your-Own-Carrier) for integrating customer SIP Trunk services that are different to the SIP Trunk

SBC Parameter	Description
	service used by their Service Provider. When this option is selected, you must select both the SBC device (see 'Region' field below) and the Service Provider Carrier SIP Trunk (see 'Carrier' field below).
Region	Select the required SBC device for the site location.
Carrier: (this option is only relevant if you are connecting your Carrier to a SIP Trunk (when options SIP Trunk or BYOC are selected 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	<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.

- Click **Next**, the Wizard continues with the configuration of the SBC Number Prefixes. For initial setup, a Dialplan file must be preconfigured on the SBC or IP-PBX. For Second day management, SBC prefixes can later be imported (see [Manage SBC Prefixes](#) on page 533).

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

Table 31-7: 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.

1 M365 Tenant

2 M365

3 Voice Route

×

SBC Onboarding Script

sbcs-scenario7

▼

📄

SBC Cleanup Script

sbcs-scenario7Cleanup

▼



📄

Customer Variables	Value

Back

Submit

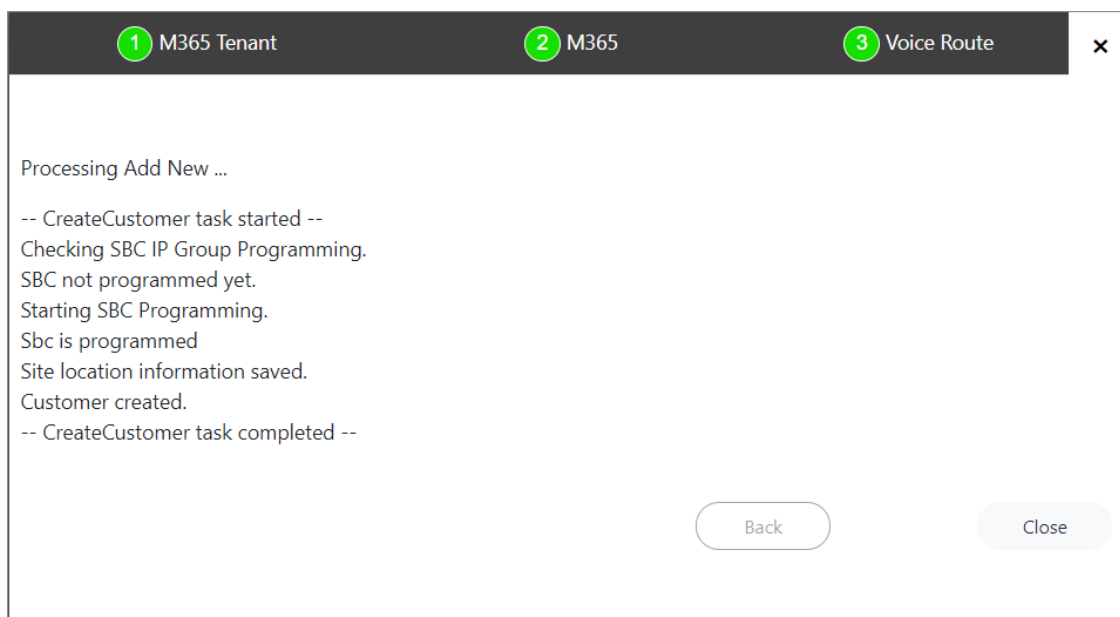
4. Configure SBC scripts:

- 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 [Customer Variables](#) on page 210.

5. When you have completed the configuration, click

Submit




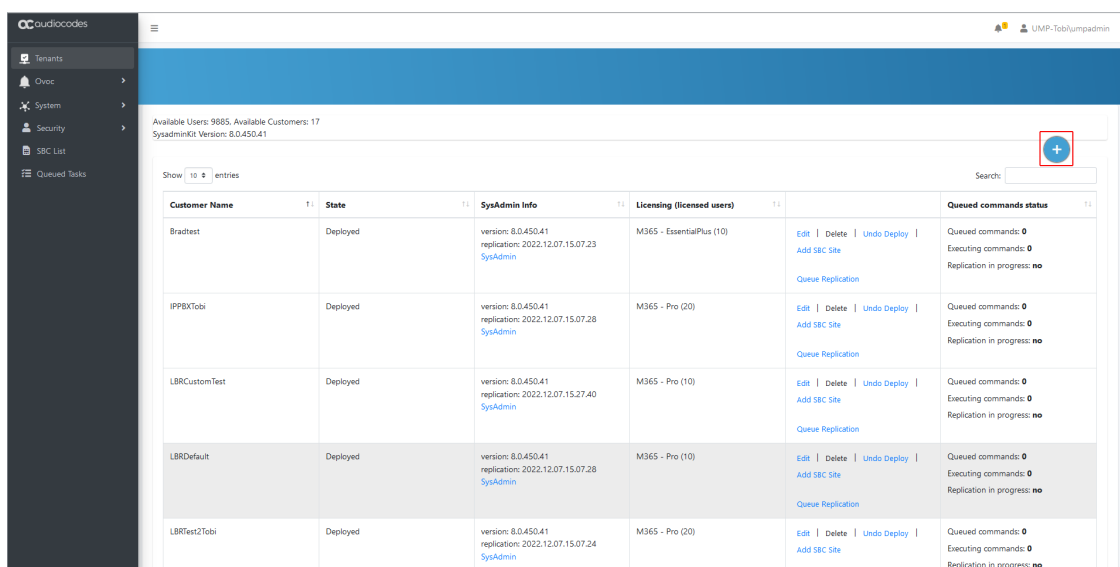
Onboarding with Hosted Pro

This section describes how to onboard Hosted Pro customers. At the start of the Onboarding wizard, consent must be requested from the customer administrator to access their M365 platform. The following Onboarding flows can be run:

- [Onboarding with both M365 Default Routing and SBC Configuration](#) on page 383
- [Onboarding with only SBC Configuration](#) on page 418

➤ **To onboard a new Hosted Pro customer:**

1. In the Tenants page, click .



The Onboarding wizard opens.

2. Click **Add New Customer**.

3. Enter Full Customer M365 Tenant Name – Free Text.
4. Enter 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. Proceed to [Request Consent from End Customer](#) on the next page.

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.

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 31-8: 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").

M365 Setting	Description
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 User Management Pack™ 365 SP Edition/Customer Portal (Optional). When this option is used, Single Sign-on support with the customer Azure AD is provided.

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** check box; 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 [Onboarding with both M365 Default Routing and SBC Configuration](#) on page 383).
- Click **Next** and proceed to [Onboarding with only SBC Configuration](#) on page 418.

Request Consent from End Customer

If the customer purchased a Hosted Essentials Plus or Hosted Pro license then they must grant consent to the Service Provider or Channel administrator for accessing their M365 platform. The consent is secured using Token authentication between the User Management Pack™ 365 SP Edition platform and the customer M365 tenant platform. Once the Token connection is securely established, the customer administrator account credentials can be used to create the new customer and thereafter for synchronizing the User Management Pack™ 365 SP Edition database with the M365 platform. The customer administrator must consent to the following:

- Access Microsoft Teams and Skype for Business data as the signed in user.
- Read and write all groups.
- Access directory as the signed in user.
- Read all users' full profiles.

- Read and write to all app catalogs.
- Maintain access to data that you have provided access.

The Token Invitation wizard is used for establishing the Token connection with the customer M365 platform. This wizard is run at the beginning of the Onboarding wizard. The Token Invitation wizard can be run using the following methods:

- Sending email link directly to customer IT administrator including a link to the Token Invitation wizard.
- Using M365 account credentials (username and password) received from the customer administrator.

The Token connection can be secured using either the 'Global' admin permissions or the permissions of the Customer admin Service account (see [Create Customer Administrator Service Account](#) on page 265). See the following:

- [Onboarding with Default Global Admin](#) on page 295
- [Onboarding with Tenant-Defined Service Account](#) on page 311

Secure Token Connection with Global Admin Credentials

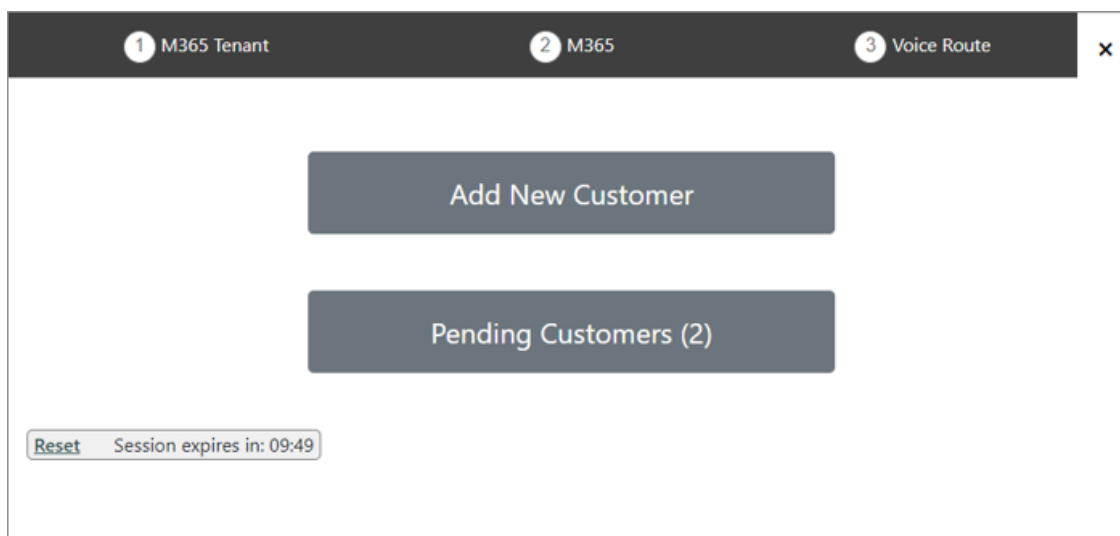
You can secure the Token connection with the customer M365 platform using the provided credentials of the customer Global admin account.



Ensure that the Global admin has been assigned the required roles (see [Assign Administrator Roles to IT Administrator](#) on page 269).

➤ Do the following:

1. In the Onboarding wizard click **Add New Customer**.



2. Select **Use M365admin account with known password**.

1 M365 Tenant

2 M365

3 Voice Route

✕

Full Customer Name

Short Customer Name

License Type
☐ Hosted Essential ☐ Hosted Essentials+ ☒ Hosted Pro

10

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

admin@M365x02753627.onmicrosoft.com

.....

Back

Next

3. Enter the Global Admin username and password provided by the customer.

1 M365 Tenant

2 M365

3 Voice Route

✕

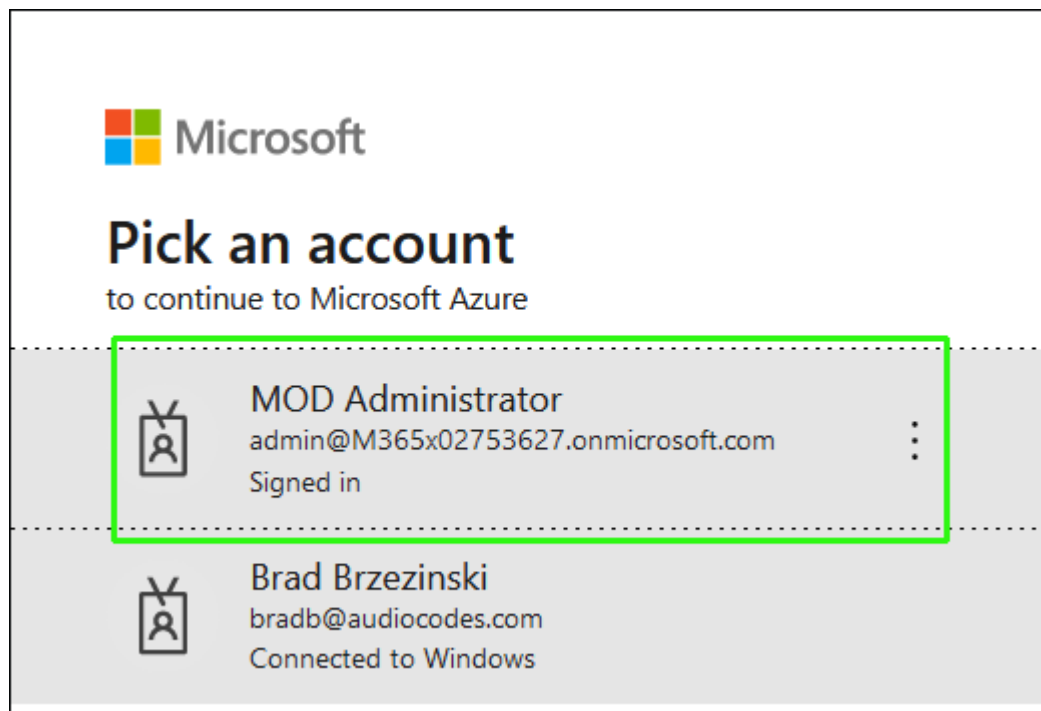
Click [here](#) to start the authentication process.

The Wizard will continue after consent is granted.

Back

Next

4. Click **here** to start the authentication process.



5. Choose the customer tenant Global Admin account.



The customer Tenant account must have Global Admin permissions, otherwise the "Consent on behalf of the organization" check box does not appear.



admin@m365x02753627.onmicrosoft.com

Permissions requested

Sandbox2-UMP-Token
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to
- ☒ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement.

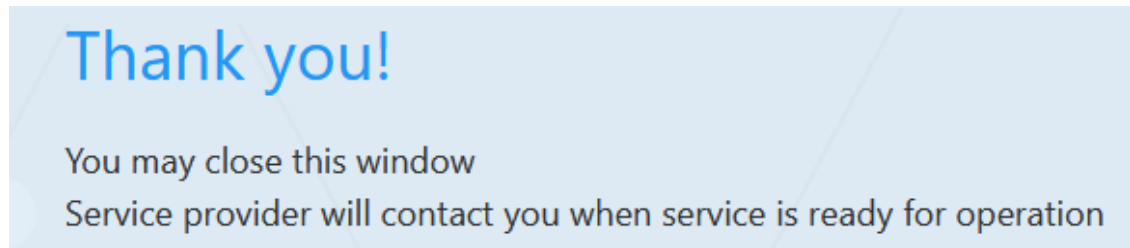
The publisher has not provided links to their terms for you to review. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

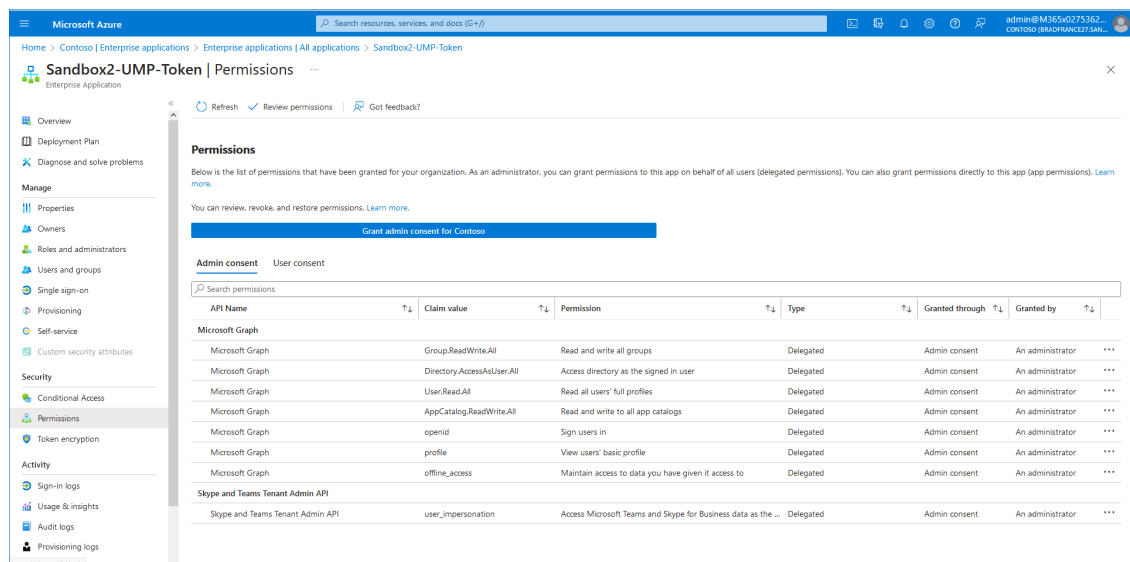
Cancel

Accept

- Click **Consent on behalf of your organization**, and then click **Accept**.



- Click **Pending Customers** to monitor the process of the request. Verify that Status is shown as **Authentication Complete** (see also [Pending Requests](#) on page 381).
- Likewise, open the Multitenant interface and navigate to **Security > Customer Invitations**. Verify that Device Authenticated is shown as **true**.
- Open the newly created Token registration on the Azure portal for the customer tenant (Enterprise Applications > <Token-Registration-Name>).
- In the Navigation pane, select **Permissions**. Note the added permissions for the new Enterprise application.



- Continue the Onboarding wizard, see [Onboarding with Hosted Pro](#) on page 361 or [Onboarding with Hosted Essentials +](#) on page 290.

Grant Consent using only Token-based Authentication (Global Admin)

You can request consent from the Customer administrators using the Token Authentication Invitation. When the token authentication requests are sent to the customer IT administrator from the Service Provider administrator, the details of the Invitation email are displayed in the Customer Invitations screen (see [Customer Invitations](#) on page 225) and the details of the authentication token are displayed in the Authentication Status screen (see [Authentication Status](#) on page 228).



The customer tenant requires the following UC admin roles (see [Assign Administrator Roles to IT Administrator](#) on page 269):

- Application Administrator
- Skype For Business Admin
- Teams Communication Administrator

➤ **To run the Token Authentication wizard:**

1. In the Onboarding wizard click **Add New Customer**.

1 M365 Tenant 2 M365 3 Voice Route x

Add New Customer

Pending Customers (2)

Reset Session expires in: 09:49

2. Select option "Send link to customer IT administrator for authentication".

1 M365 Tenant 2 M365 3 Voice Route x

Full Customer Name

BradTrunk

Short Customer Name

BradTrunk

License Type

☐ Hosted Essential ☒ Hosted Essentials+ ☐ Hosted Pro

10

M365 Authentication

☒ Send link to customer IT administrator for authentication:

☐ Use M365admin account with known password

IT Administrator email

Back Next

1 M365 Tenant
2 M365
3 Voice Route
X

Full Customer Name

BradTrunk

Short Customer Name

BradTrunk

License Type

☐ Hosted Essential
☐ Hosted Essentials+
☒ Hosted Pro

10

M365 Authentication

☒ Send link to customer IT administrator for authentication:
☐ Use M365admin account with known password

IT Administrator email

Back Next

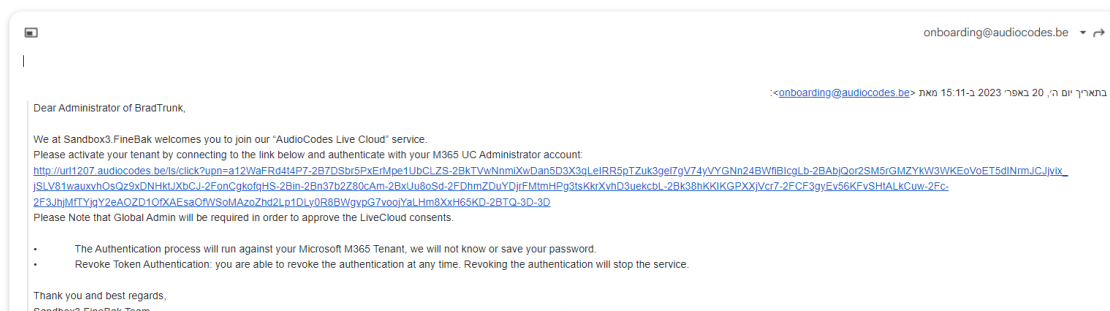
- Enter the email address of the Customer administrator with Global Admin permissions for their M365 tenant.

1 M365 Tenant
2 M365
3 Voice Route
X

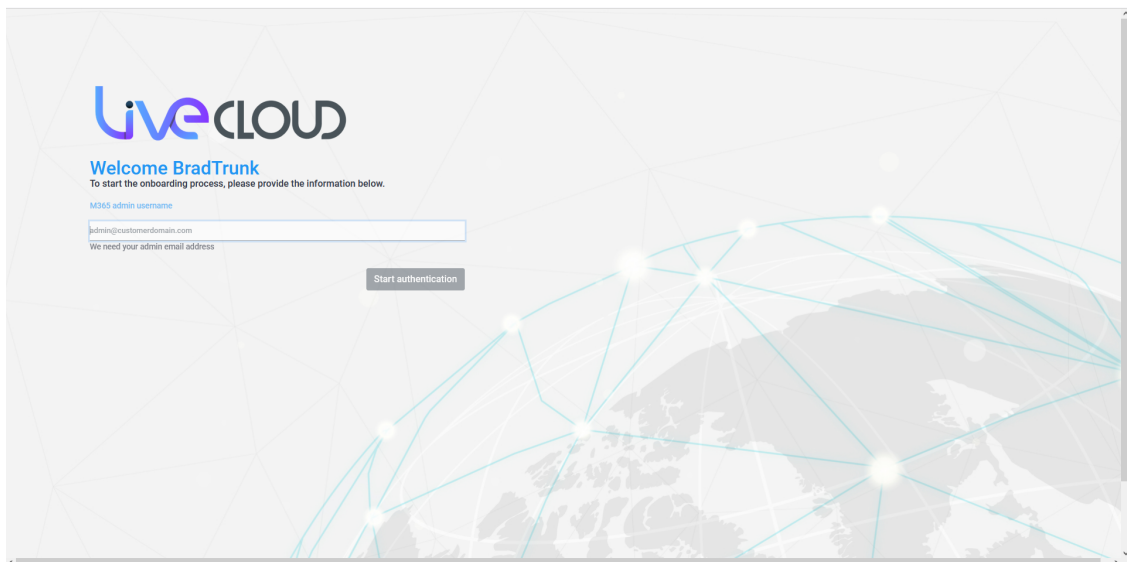
- An email will be sent to this administrator address. The email shall contain a customized url to a landing page hosted by UMP. On this landing page, the customer administrator enters the M365 account to be used for background processing and a device token (example: DCRWDLX8) will be generated based out of this account that should be authenticated against <https://microsoft.com/device/login>

Close

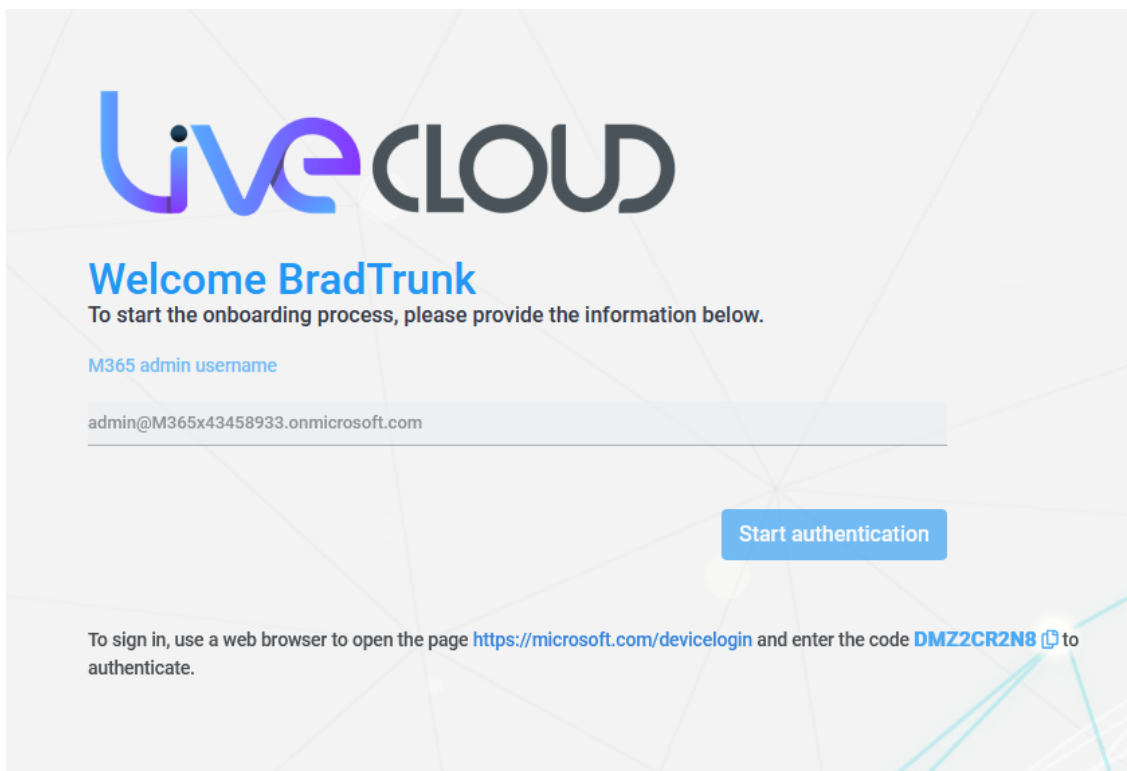
- An email similar to the following is received by the customer IT administrator.




- The customer clicks



6. The customer enters the credentials of their M365 tenant Global Administrator, and then clicks **Start authentication**.



7. The customer copies the code appearing on the bottom of the screen and then clicks **Start authentication**.



Microsoft

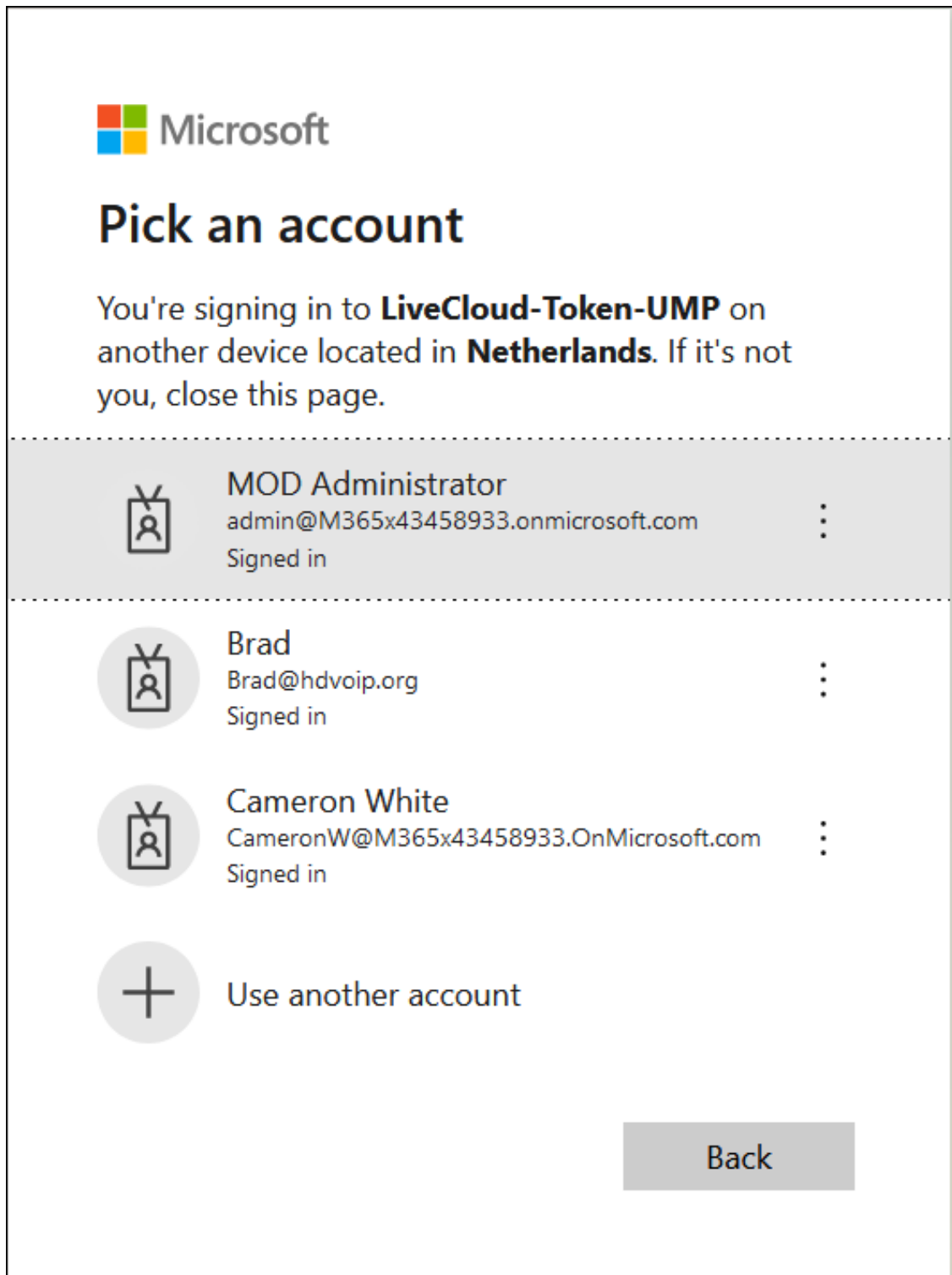
Enter code

Enter the code displayed on your app or device.

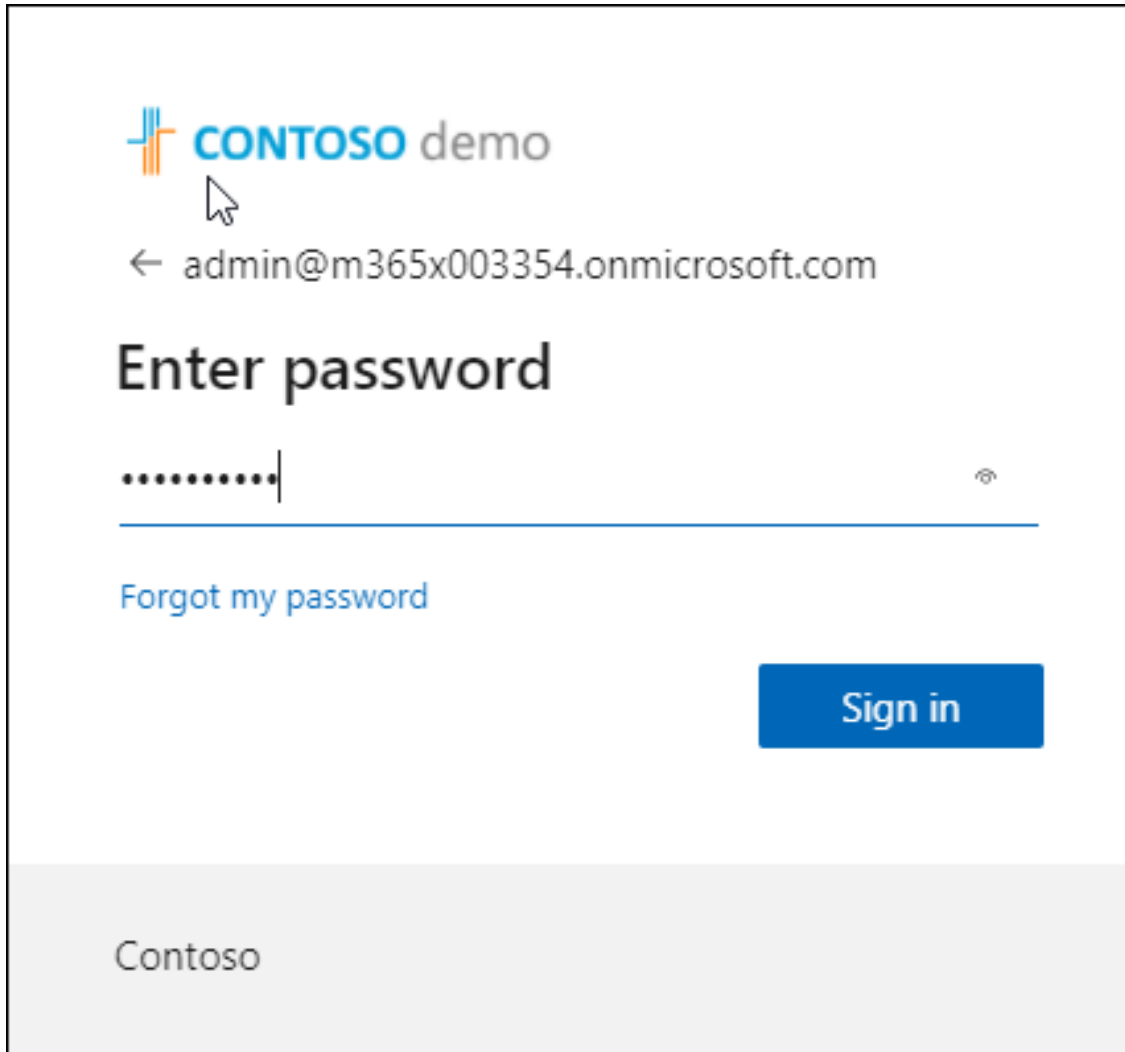
DMZ2CR2N8|


Next

8. The customer enters the code.




9. The customer enters the M365 tenant Global administrator username, and then clicks **Next**.



 **CONTOSO** demo

← admin@m365x003354.onmicrosoft.com

Enter password

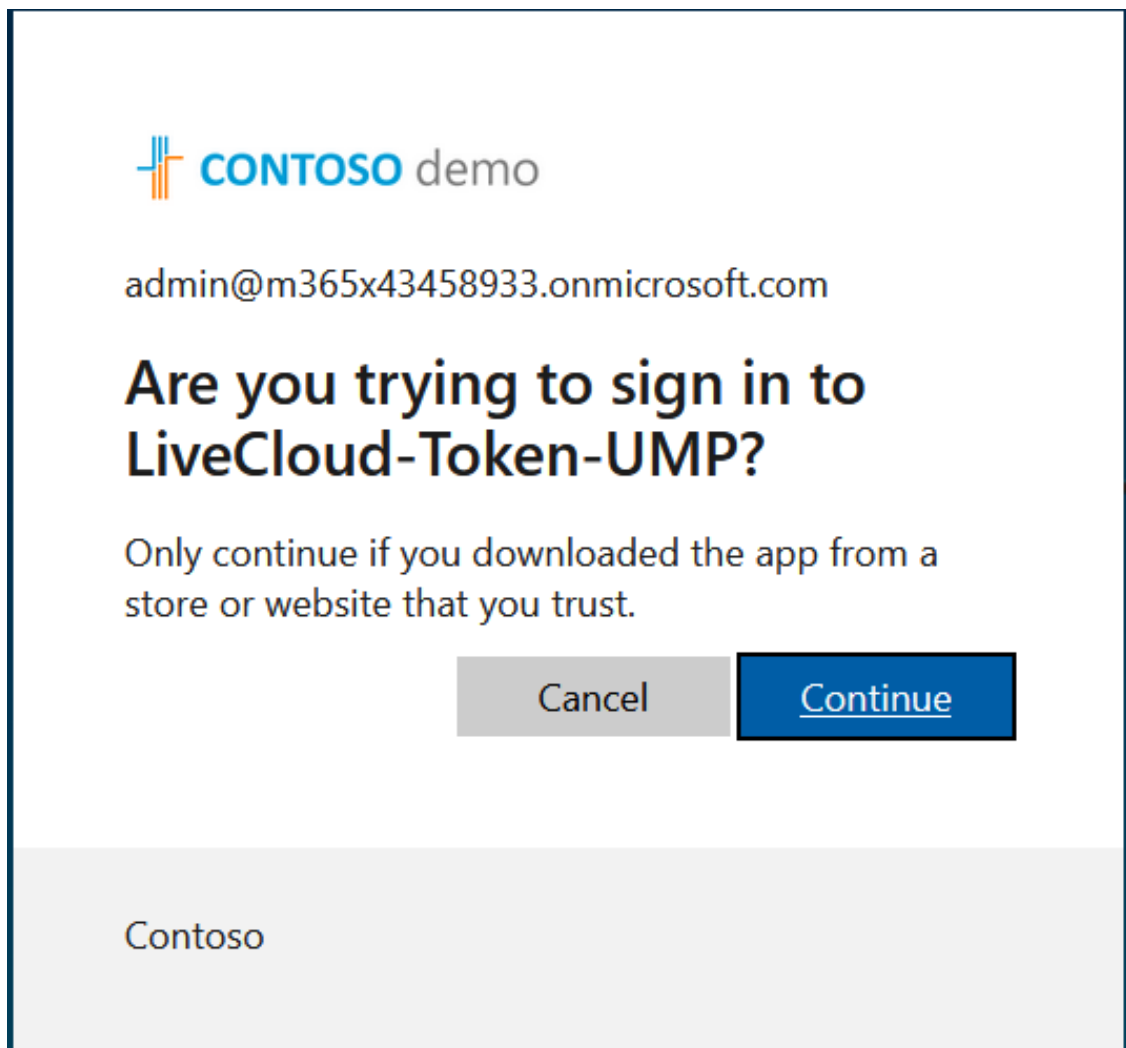
.....| 

[Forgot my password](#)

Sign in

Contoso

10. The customer enters password, and then clicks **Sign in**.



11. The customer clicks **Continue**.



admin@m365x43458933.onmicrosoft.com

Permissions requested

LiveCloud-Token-UMP
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to

☒ **Consent on behalf of your organization**

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement.

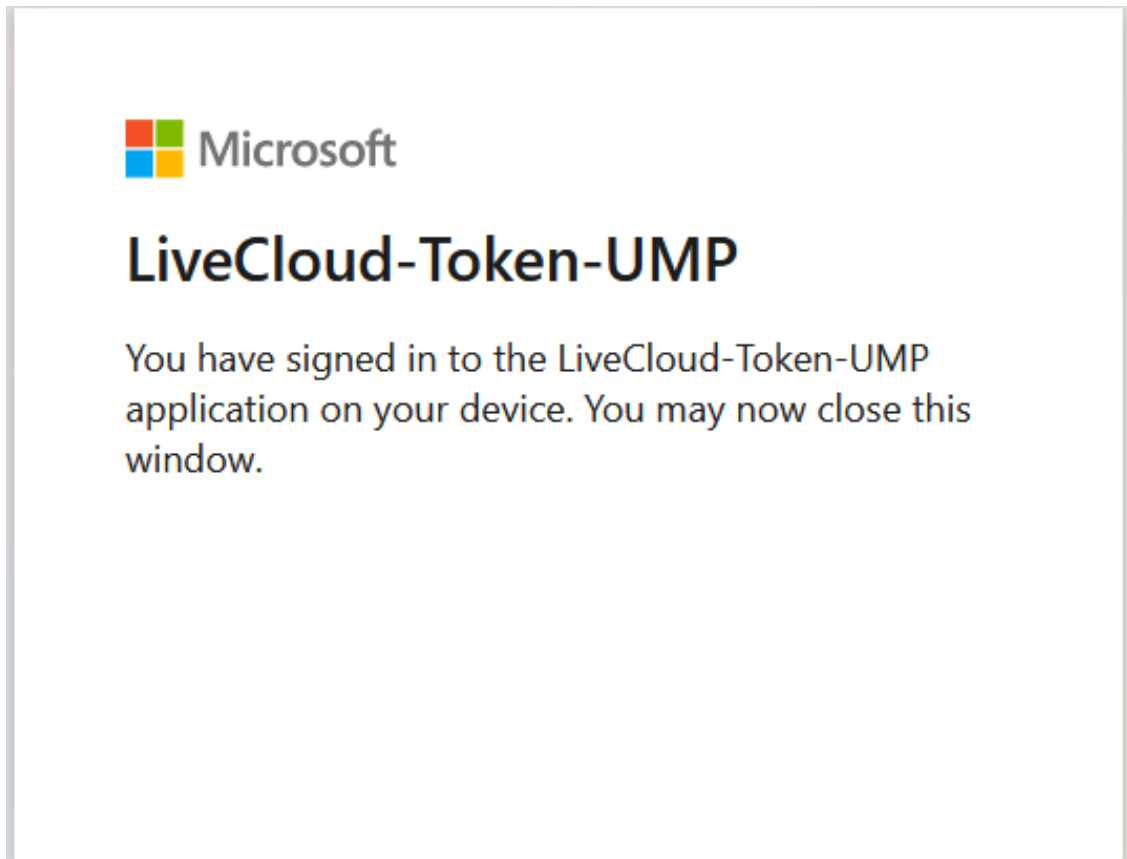
The publisher has not provided links to their terms for you to review. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

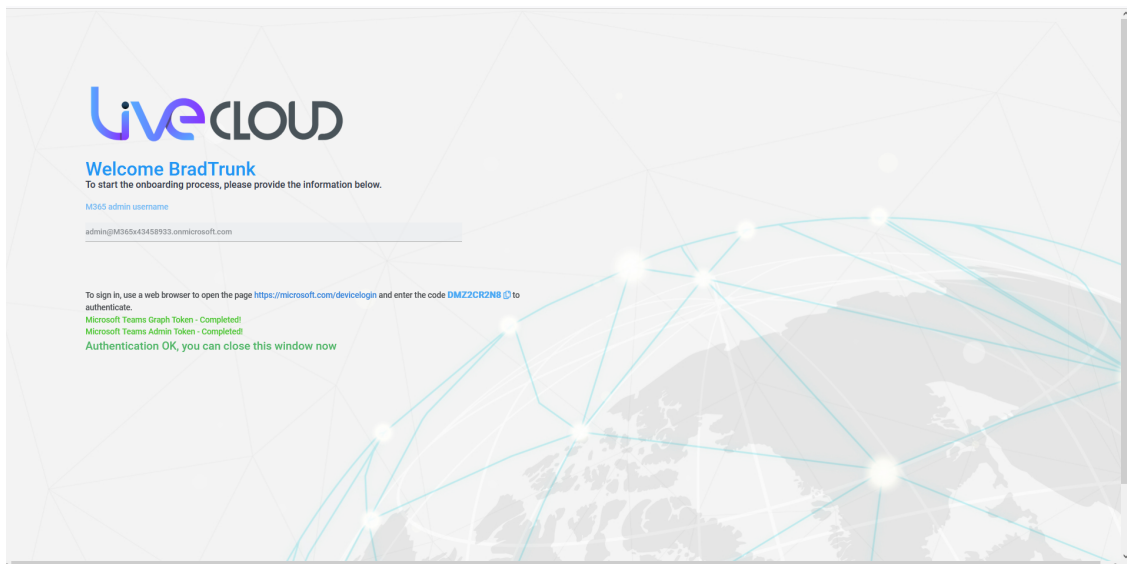
Cancel

Accept

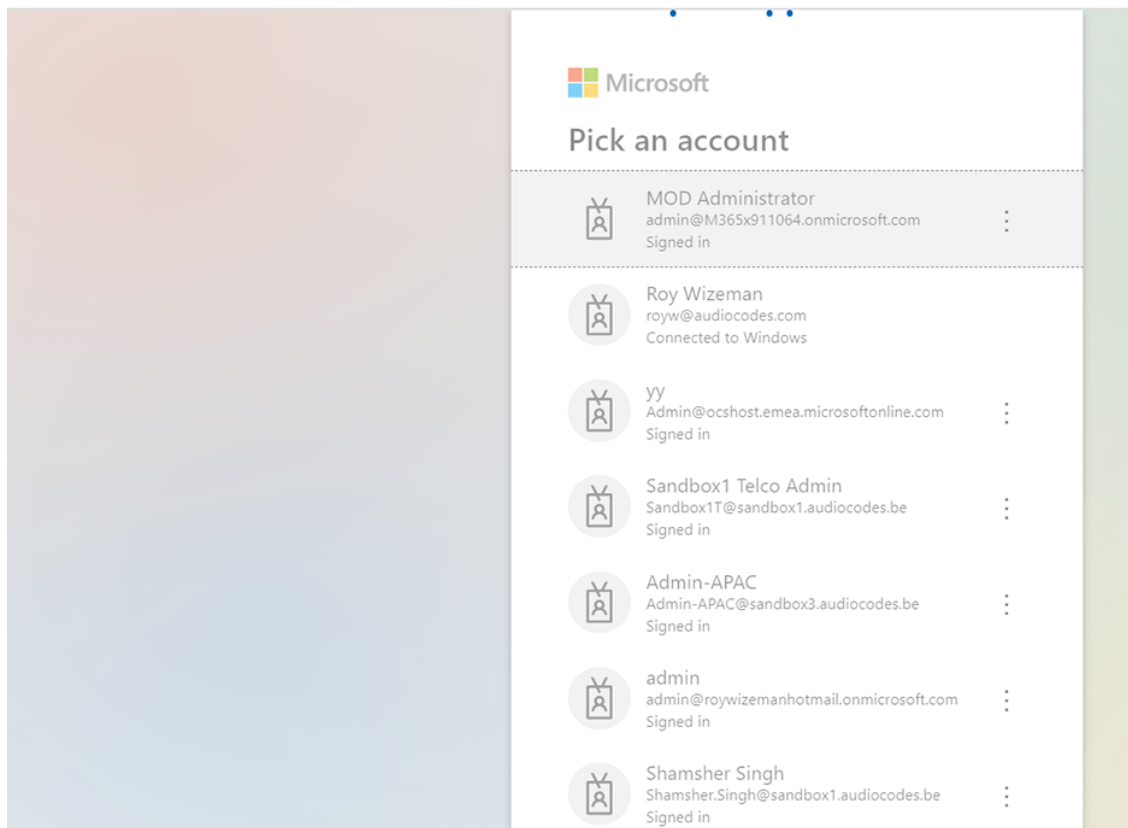
12. The customer selects **Consent on behalf of your organization** check box, and then clicks **Accept**.



13. The customer closes the Information window.



14. The customer clicks **Click here to continue the authentication process** link.



15. The customer logs in to their M365 tenant account with Global admin permissions.



admin@m365x43458933.onmicrosoft.com

Permissions requested

LiveCloud-Token-UMP
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to

☒ **Consent on behalf of your organization**

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement.

The publisher has not provided links to their terms for you to review. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

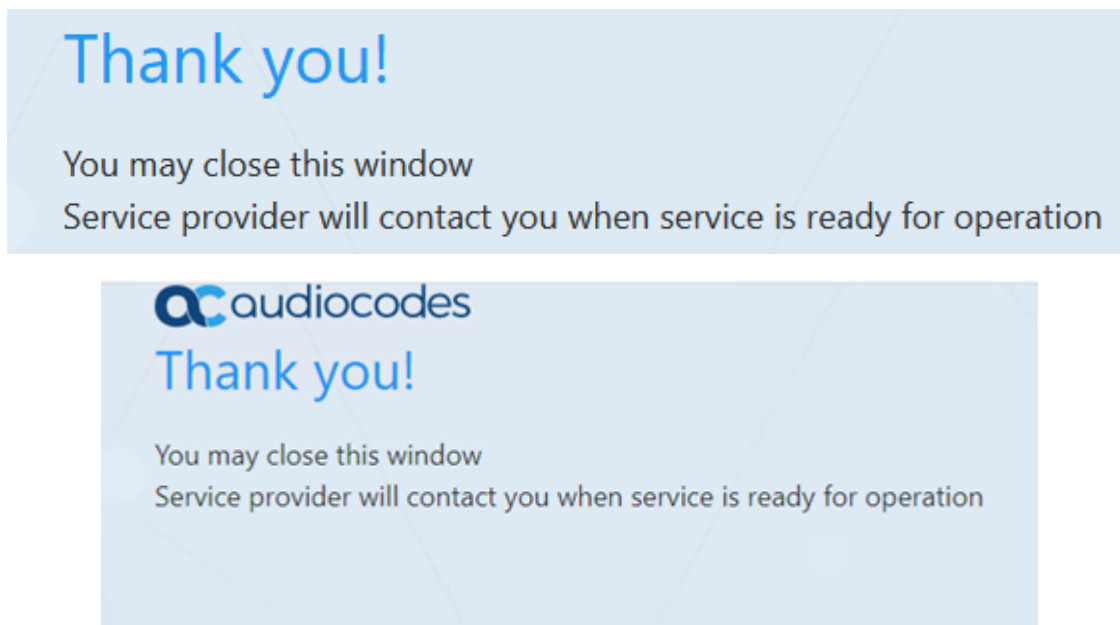
Does this app look suspicious? [Report it here](#)

Cancel

Accept

16. The customer selects **Consent on behalf of your organization** check box, and then clicks **Accept**

At the end of the process, the following screen is displayed informing the Global administrator that the service provider will complete the process.

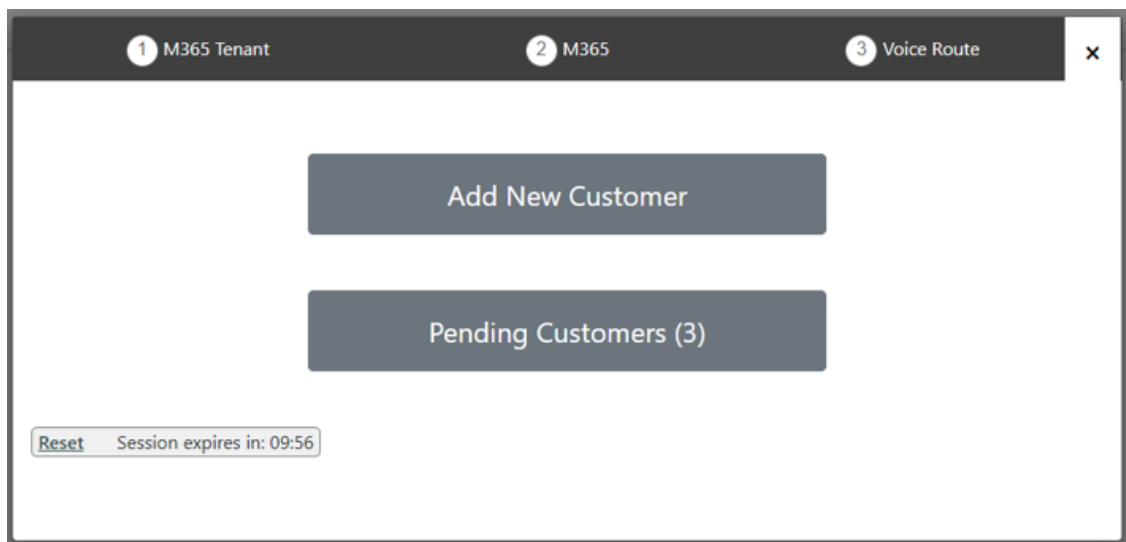


17. Click **Pending Customers** to monitor the process of the request (see [Pending Requests](#) below) and then continues the wizard process (see [Onboarding with Hosted Essentials +](#) on page 290 or [Onboarding with Hosted Pro](#) on page 361).

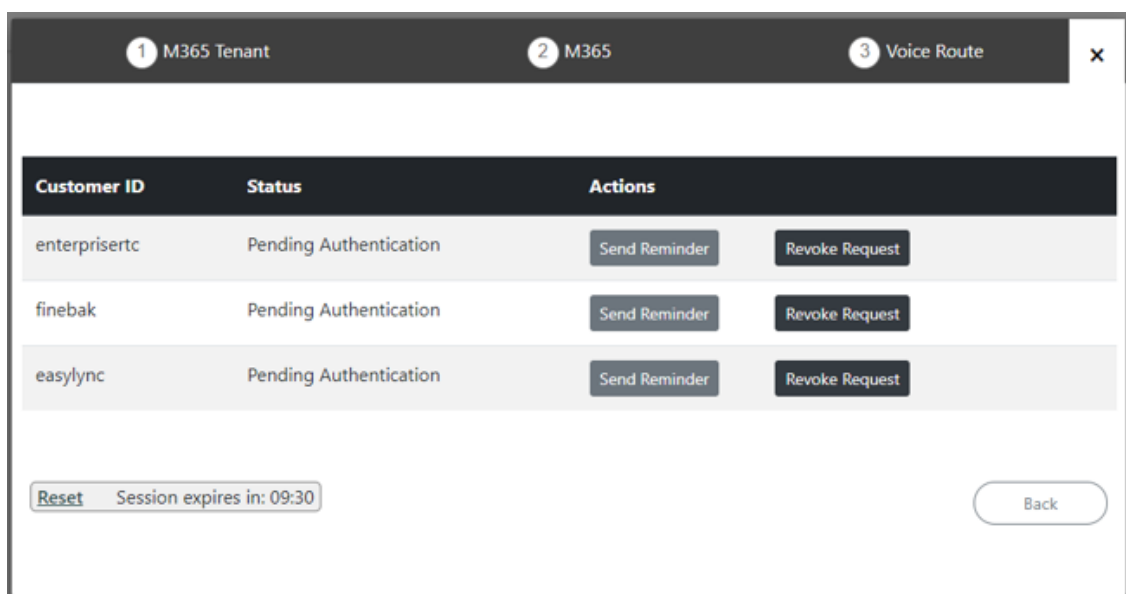
1 M365 Tenant	2 M365	3 Voice Route	x
Customer ID			
BradDemo	Authentication Complete	Add Customer	Revoke Request

Pending Requests

You can monitor the status of Pending Requests by clicking **Pending Customers**.



A list of pending authentication requests is displayed:



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.

A screenshot of a web application interface. A modal dialog box is open, titled "says", with the text "Customer IT Administrator email:". Below the text is a text input field containing "xxxx@corporate.com". The input field is highlighted with a red rectangle. To the right of the input field are two buttons: "OK" (blue) and "Cancel" (white). In the background, a table is visible with columns "Customer ID" and "Pending Authentication". The table has three rows: "enterprisertc", "finebak", and "easylync". Each row has a "Send Reminder" button and a "Revoke Request" button. At the bottom of the page, there is a "Reset" button, a session timer "Session expires in: 08:57", and a "Back" button.

- **Revoke Request:** revoke the request sent to the customer IT administrator

A screenshot of the same web application interface. A modal dialog box is open, titled "says", with the text "The action will revoke the registration invitation and will remove the entry from the database. Please confirm." Below the text are two buttons: "OK" (blue) and "Cancel" (white). The background table and buttons are the same as in the previous screenshot.

Onboarding with both M365 Default Routing and SBC Configuration

This section describes how to onboard new customers by applying the default M365 Onboarding script. This option also allows you to automatically configure the customer DNS domain as part of the Onboarding script. Once M365 has been configured, the wizard continues with the SBC configuration.

➤ To onboard with both M365 and SBC configuration:

1. Select option **Configure M365 default routing**, the following screen is displayed:

1 M365 Tenant
2 M365
3 Voice Route
×

☒ **Configure M365 default routing**

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

Online PSTN Gateway

M365 Onboarding Script

M365 Cleanup Script



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

Back
Next

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

Table 31-9: 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 Setting up Fully Automatic DNS Provisioning on page 70 and Setup Two-step Provisioning on page 250 respectively).
Region/Country	The customer SBC region subdomain name configured (see Configure DNS API on page 82).
IP Address	Preconfigured IP address of the region SBC (see Configure DNS API on page 82).
SBC	Preconfigured FQDN of the region SBC (see Configure DNS API on page 82).
Domain Name	Preconfigured domain name of the DNS (A-record) (see Creating A Records for SBC Devices on page 74).
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.

O365 Setting	Description
Other Configuration	
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 Register End Customer Tenant DNS Sub domains on page 250).</p>
M365 Onboarding Script	<p>Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Customer Variables.</p> <p>Click the  to edit the Onboarding script file. For example, when a service provider needs a separate registration per customer tenant. See Default M365 Tenant Onboarding Script on page 191.</p>
M365 Cleanup Script	<p>Preconfigured script that is prepared by AudioCodes Professional services and that can be customized by setting Customer Variables.</p> <p>Click the  to edit the Cleanup script file. See Default M365 Tenant Cleanup Script on page 193.</p>
Customer Variables	<p>Script variables can be customized and loaded to the M365 Onboarding and Cleanup scripts. See Customer Variables on page 210.</p>

The wizard continues with the SBC configuration.

1 M365 Tenant

2 M365

3 Voice Route

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

Back

Next

1 M365 Tenant

2 M365

3 Voice Route

Customer: ProTrunk

☒ **Configure SBC**

Sbc Site Name

Online PSTN Gateway

Sbc Configuration: ☒ Sip Trunk ☐ IP PBX ☐ BYOC

Region

Carrier

☐ **Carrier Registration**

☐ **Enable Cac**

Back

Next

Sbc Configuration: ☒ Sip Trunk ☐ IP PBX ☐ BYOC

Region

Carrier

☒ **Carrier Registration**

☒ **Enable Cac**

Back

Next

1 M365 Tenant

2 M365

3 Voice Route

×

Customer:

EPC

☒ Configure SBC

Sbc Site Name

EPC

Online PSTN Gateway

Online PstnGateway

Sbc Configuration:

☒ Sip Trunk ☐ BYOC

Region

52.143.14.26_SBC

Carrier

52.143.14.26_SBC

☒ Carrier Registration

Username

Password

MainLine

Hostname

☒ Enable Cac

Select an CAC Profile

Back

Next

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

Select a Carrier from list

☒ Carrier Registration

ProxySet_0
SIPTrunk
SIPTrunk1
this is a very long name deliberately_12

☒ Enable Cac

Select an CAC Profile

Back

Next

1 M365 Tenant
2 M365
3 Voice Route
✕

Customer: EPC

☒ **Configure SBC**

Sbc Site Name

Online PSTN Gateway

Sbc Configuration: ☒ Sip Trunk ☐ BYOC

Region

Carrier

☒ **Carrier Registration**

☒ **Enable Cac**

1 session

1 session

5 sessions

10 sessions

20 sessions

1000 sessions

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

Table 31-10: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"> <input checked="" type="checkbox"/> SIP Trunk: SIP Trunk used by Service Provider. <input checked="" type="checkbox"/> IP-PBX-Service Provider IP-PBX <input checked="" type="checkbox"/> BYOC (Bring-Your-Own-Carrier) for integrating customer SIP Trunk services

O365 Setting	Description
	that are different to the SIP Trunk service used by their Service Provider.
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	<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.

4. Click **Next**, the Wizard continues with the configuration of the SBC Number Prefixes. For initial setup, a Dialplan file must be preconfigured on the SBC or IP-PBX. For Second day management, SBC prefixes can later be imported (see [Manage SBC Prefixes](#) on page 533).

1 M365 Tenant 2 M365 3 Voice Route

SBC number prefixes

Browse... No file selected.

New Number prefix

Back Next

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

Table 31-11: 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.

1 M365 Tenant 2 M365 3 Voice Route

SBC number prefixes

Browse... pbxexample.csv

pbxexample.csv

New Number prefix

Back Next

1 M365 Tenant 2 M365 3 Voice Route

SBC number prefixes

Browse... No file selected.

New Number prefix

314

Back Next

1 M365 Tenant

2 M365

3 Voice Route

×

SBC Onboarding Script

sbcs-scenario7

▼

📄

SBC Cleanup Script

sbcs-scenario7Cleanup

▼



📄

Customer Variables	Value

Back

Submit

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 [Managing Onboarding Script Templates](#) on page 170.

7. When you have completed the configuration, click

Submit

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 --

BackClose

Fully Automatic DNS Provisioning

This section describes how to automatically create the DNS record using the Onboarding wizard (see [Two-step DNS Provisioning](#) on page 411).

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

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
--------------------	-------

BackNext

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

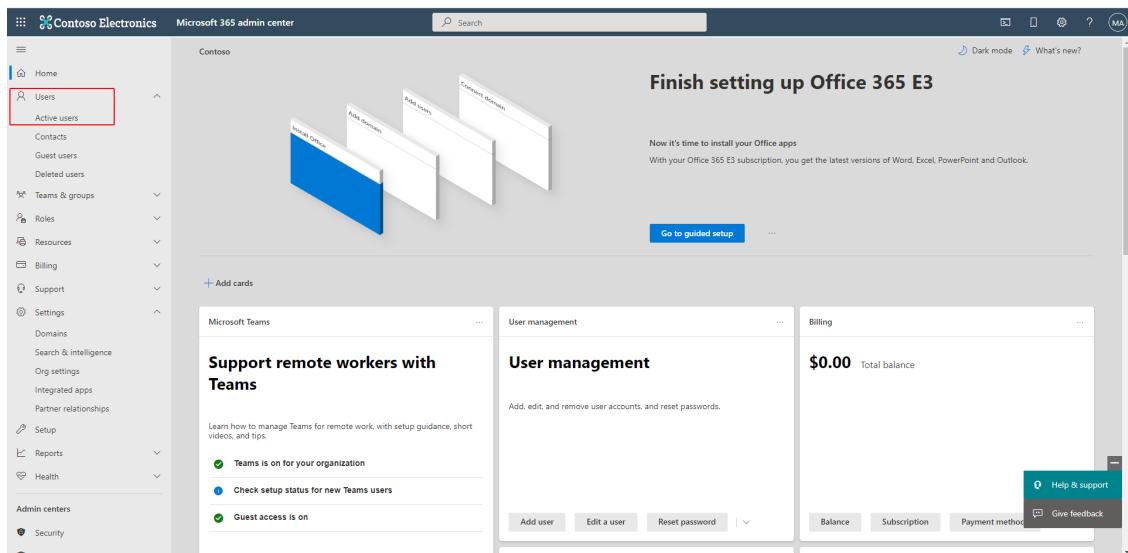
Back Next

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

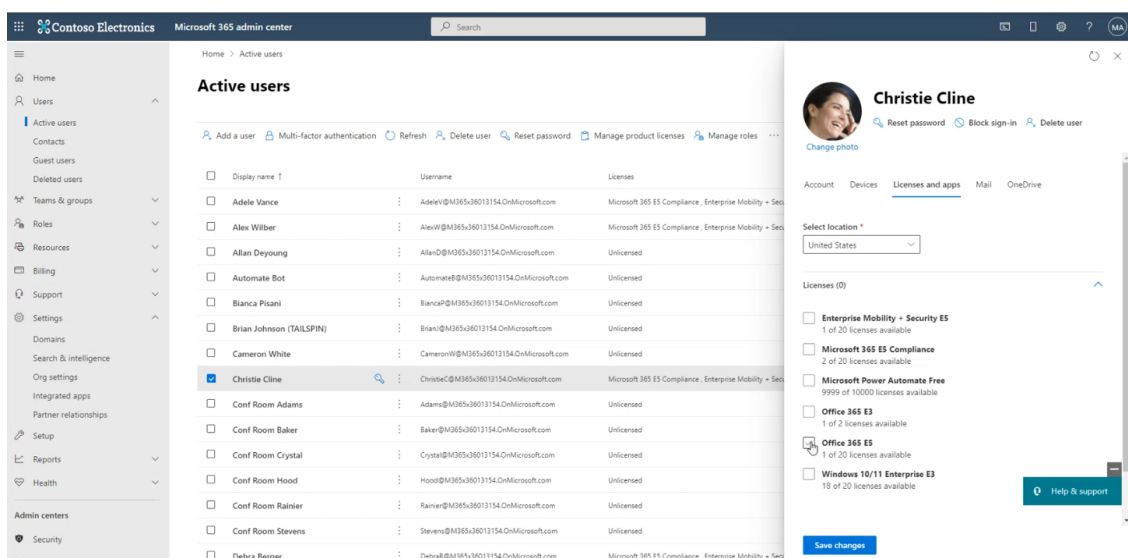
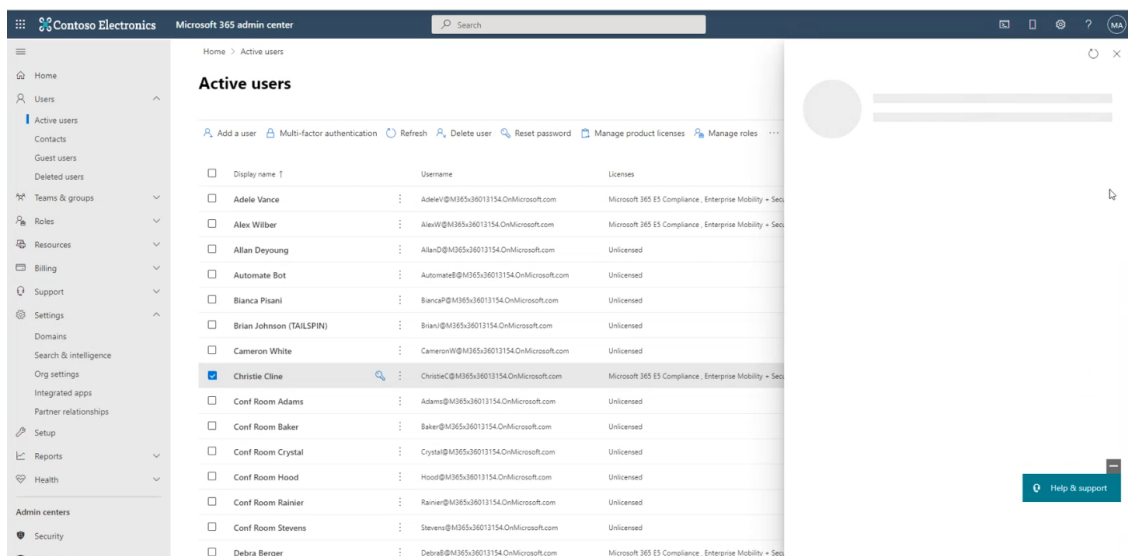
Active users

<input type="checkbox"/>	Display name	Username	Licenses
<input type="checkbox"/>	Adele Vance	AdeleV@M365x26013154.OnMicrosoft.com	Microsoft 365 E3 Compliance, Enterprise Mobility + Secur
<input type="checkbox"/>	Alex Wilber	AlexW@M365x26013154.OnMicrosoft.com	Microsoft 365 E3 Compliance, Enterprise Mobility + Secur
<input type="checkbox"/>	Allan Deyoung	AllanD@M365x26013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/>	Automate Bot	AutomateB@M365x26013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/>	Blanca Pisani	BlancaP@M365x26013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/>	Brian Johnson (TAILSPIN)	BrianJ@M365x26013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/>	Cameron White	CameronW@M365x26013154.OnMicrosoft.com	Unlicensed
<input checked="" type="checkbox"/>	Christie Cline	ChristieC@M365x26013154.OnMicrosoft.com	Microsoft 365 E3 Compliance, Enterprise Mobility + Secur
<input type="checkbox"/>	Conf Room Adams	Adams@M365x26013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/>	Conf Room Baker	Baker@M365x26013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/>	Conf Room Crystal	Crystal@M365x26013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/>	Conf Room Hood	Hood@M365x26013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/>	Conf Room Rainier	Rainier@M365x26013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/>	Conf Room Stevens	Stevens@M365x26013154.OnMicrosoft.com	Unlicensed
<input type="checkbox"/>	Debra@M365x26013154.OnMicrosoft.com	Debra@M365x26013154.OnMicrosoft.com	Microsoft 365 E3 Compliance, Enterprise Mobility + Secur

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



5. Select any licensed user.



The screenshot shows the Microsoft 365 admin center interface. On the left is a navigation pane with options like Home, Users, Teams & groups, Roles, Resources, Billing, Support, Settings, Domains, Search & intelligence, Org settings, Integrated apps, Partner relationships, Setup, Reports, Health, Admin centers, Security, and Compliance. The main area is titled 'Active users' and lists various users. 'Christie Cline' is selected. On the right, the 'Licenses' section for Christie Cline is displayed, showing a list of available licenses and their counts. The 'Enterprise Mobility + Security E5' license is currently assigned to the user.

6. 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

The screenshot shows the M365 Tenant configuration page. At the top, there are three tabs: '1 M365 Tenant', '2 M365', and '3 Voice Route'. The 'M365 Tenant' tab is active. The page contains several form fields: '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' (Brad), and 'License Plan'. A red error message is displayed below the 'License Plan' field: 'No License Plan Available! Make sure to free the license(s) for a plan and reload'. The 'Reload' button is highlighted.

- 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 following figure, the OFFICE 365 E5 license is loaded.

The screenshot shows a configuration window with a dark header bar containing three steps: 1 M365 Tenant (active), 2 M365, and 3 Voice Route. The main content area has the following fields:

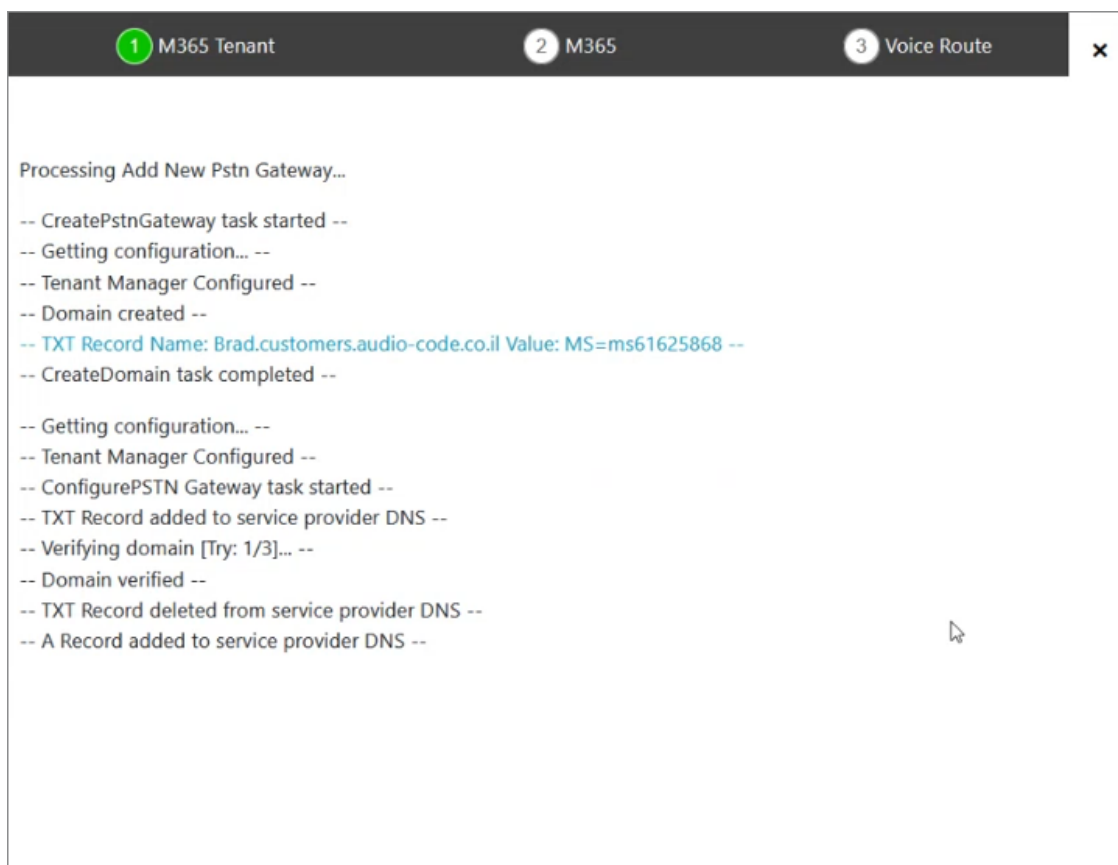
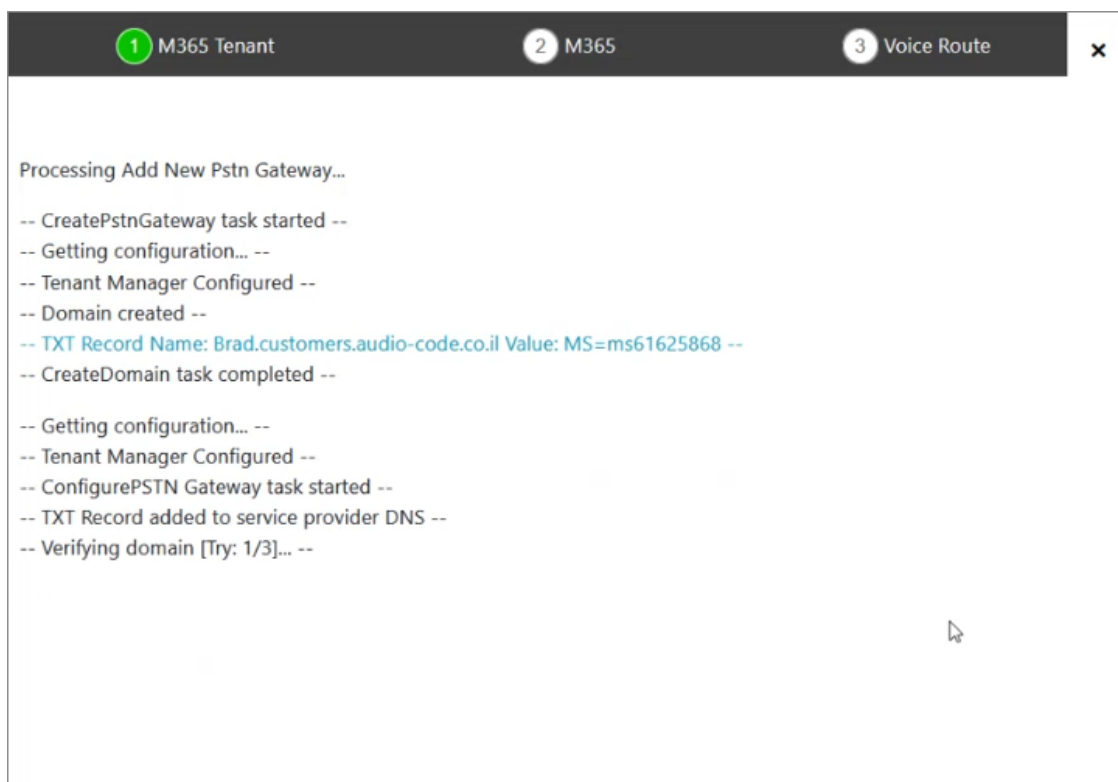
- Region/Country:** A dropdown menu showing "OC1_SBC".
- Ip Address:** A text field containing "51.137.97.95".
- Sbc:** A text field containing "oc1.customers.audio-code.co.il [51.137.97.95]".
- Domain Name:** A text field containing "customers.audio-code.co.il".
- Sbc Site Name:** A text field containing "Brad". A note next to it says: "Note: You won't be able to change the sbc site name after adding the PSTN Gateway!".
- License Plan:** A dropdown menu showing "OFFICE 365 E5".
- Buttons:** A "Reload" button is located next to the License Plan dropdown. At the bottom right, there are "Back" and "Next" buttons.

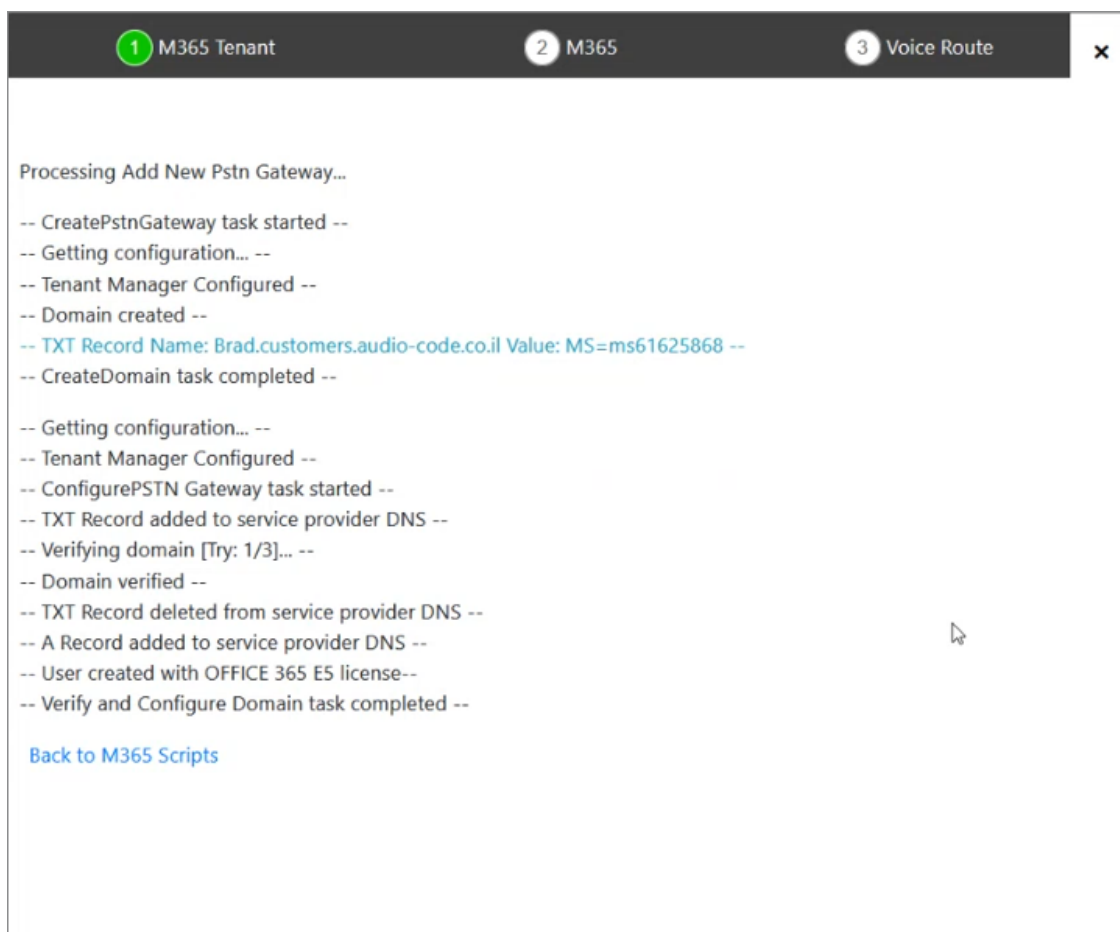
The new tenant is added.

The screenshot shows the same configuration window, but now it displays the status of the process:

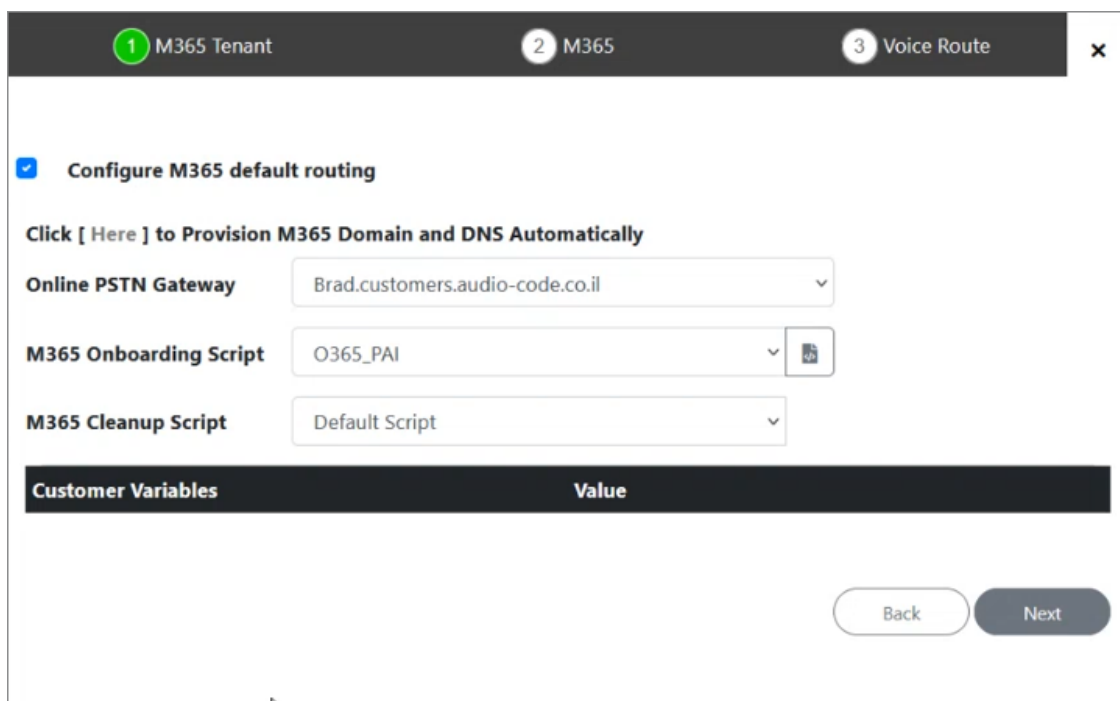
- Status:** "Processing Add New Pstn Gateway..."
- Tasks:** A list of tasks is shown: "-- CreatePstnGateway task started --", "-- Getting configuration... --", and "-- Tenant Manager Configured --".
- Buttons:** A "Back" button is located at the bottom right.

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.





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



- Complete the Onboarding wizard as described in [Onboarding with both M365 Default Routing and SBC Configuration](#) on page 333.

Onboarding with M365 Location-Based Routing

This section describes how to onboard new customers with M365 Location-based routing. This procedure includes the authentication consent process for a new customer and also the creation of a PSTN gateway and Customer domain using Fully-automatic domain provisioning.

➤ To create a new customer with Location-based routing:

1. Enter the details of the new customer.

The screenshot shows a wizard interface with a dark header bar containing three steps: '1 M365 Tenant' (highlighted with a green circle), '2 M365', and '3 Voice Route'. A close button (X) is on the right. The main content area has the following sections:

- Full Customer Name:** A text input field containing 'BradPro'.
- Short Customer Name:** A text input field containing 'BradPro'.
- License Type:** Three radio buttons: 'Hosted Essential', 'Hosted Essentials+', and 'Hosted Pro' (selected). To the right is a numeric input field with '10' and a dropdown arrow.
- M365 Authentication:** Two radio buttons: 'Send link to customer IT administrator for authentication:' and 'Use M365admin account with known password' (selected). Below these are two text input fields: 'M365 User Name' and 'M365 Password' (with an eye icon for toggling visibility).

At the bottom right are two buttons: 'Back' and 'Next'.

2. Click **Next**.

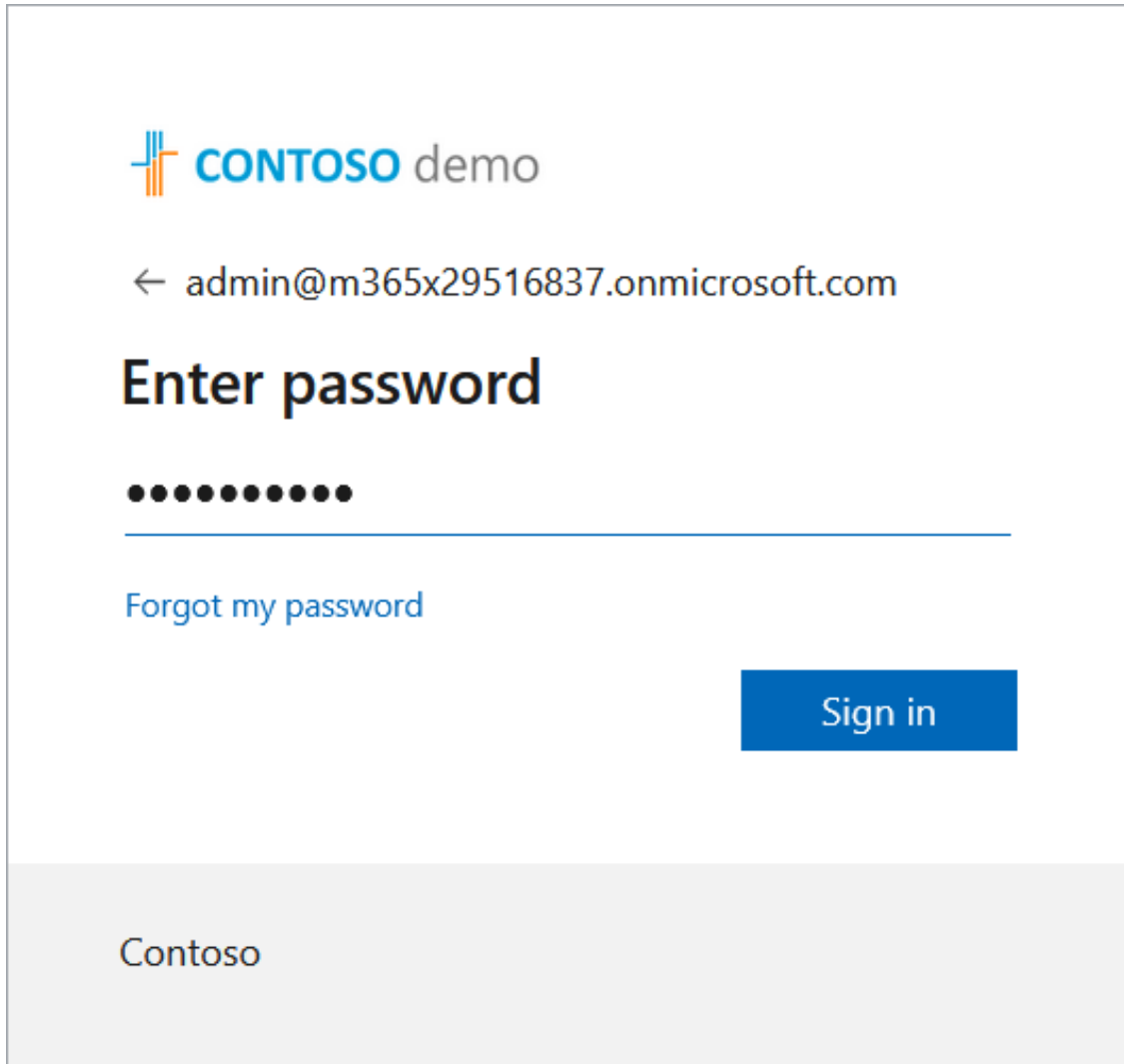
The screenshot shows the same wizard interface, but step '2 M365' is now highlighted with a green circle. The content area contains the following text:


Click [here](#) to start the authentication process.

The Wizard will continue after consent is granted.

At the bottom right are two buttons: 'Back' and 'Next'.

3. Click **here** to start the authentication process to allow the Service Provider administrator access to customer Azure tenant.



 **CONTOSO** demo

← admin@m365x29516837.onmicrosoft.com

Enter password

●●●●●●●●

[Forgot my password](#)

[Sign in](#)

Contoso

4. Enter customer tenant credentials.



admin@m365x29516837.onmicrosoft.com

Permissions requested

MSAL-Token-simplify

unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access the directory as you
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to
- ☐ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement.

The publisher has not provided links to their terms for you to review. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

Cancel

Accept



admin@m365x29516837.onmicrosoft.com

Permissions requested

MSAL-Token-simplify
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to
- ☒ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement.

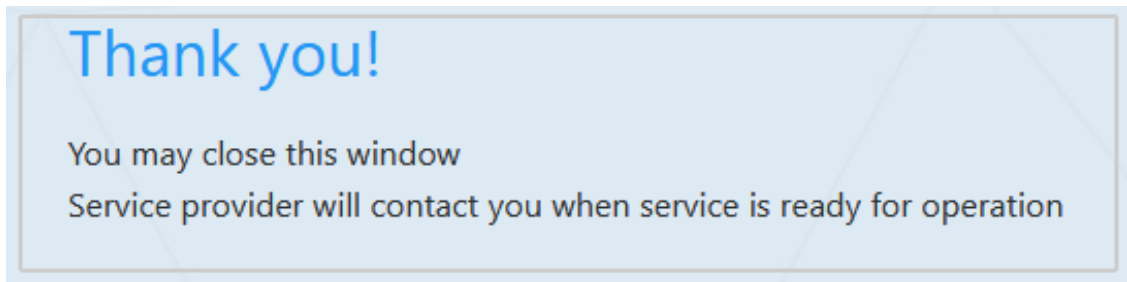
The publisher has not provided links to their terms for you to review. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

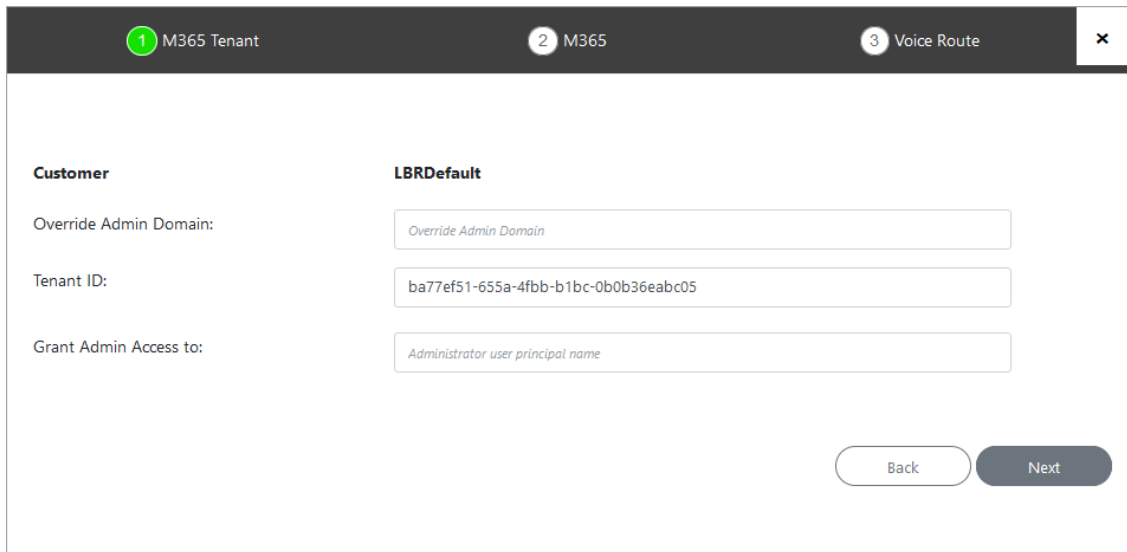
Cancel

Accept

5. Select the **Consent on behalf of your organization** check box.

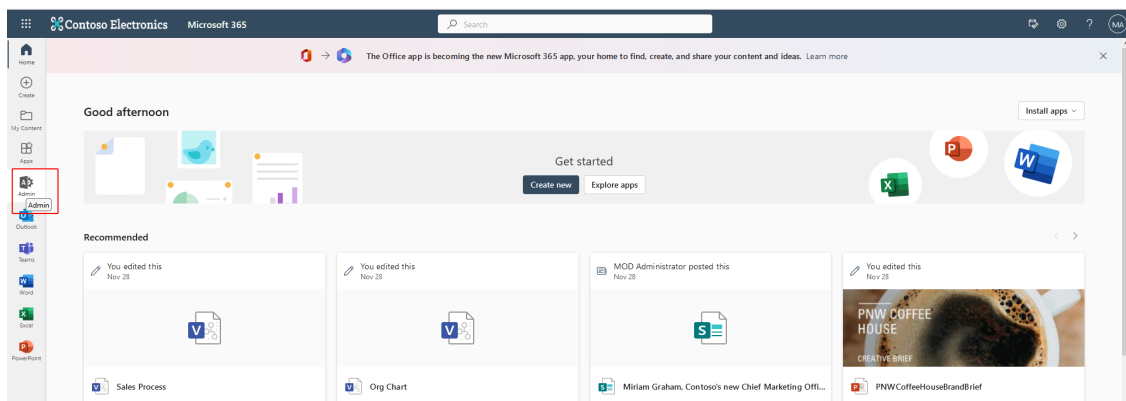


A confirmation is sent from the Service Provider tenant.

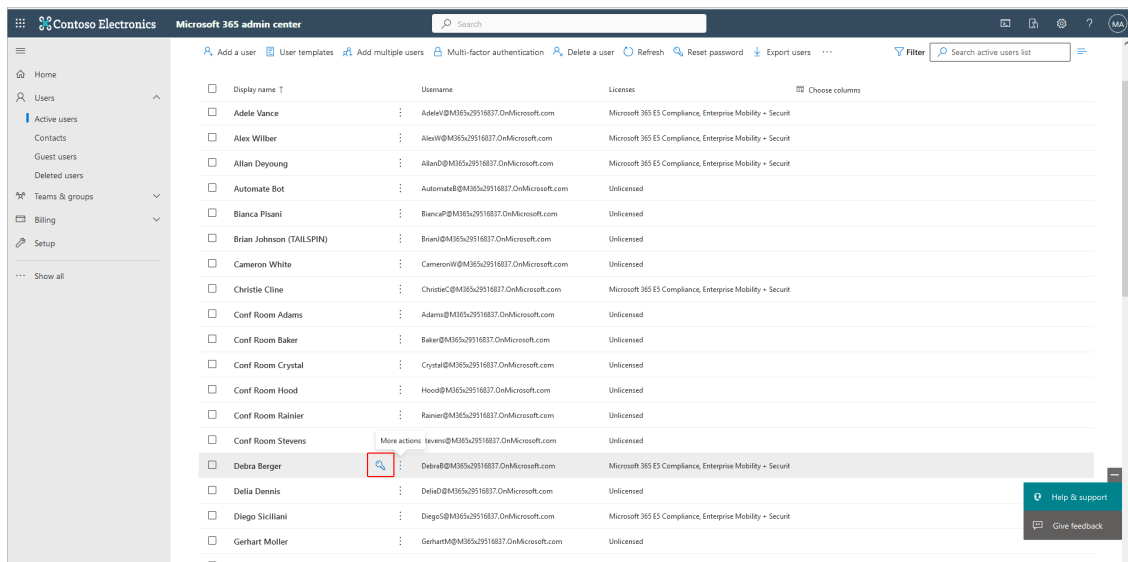
A screenshot of a software configuration window titled "M365 Tenant" (indicated by a green circle with the number 1). The window has a dark header bar with three tabs: "M365 Tenant" (active), "M365" (indicated by a green circle with the number 2), and "Voice Route" (indicated by a green circle with the number 3). A close button (X) is in the top right. The main content area is white and contains a form for "Customer" configuration. The form has a label "Customer" and a value "LBRDefault". It includes three input fields: "Override Admin Domain:" with the placeholder "Override Admin Domain", "Tenant ID:" with the value "ba77ef51-655a-4fbb-b1bc-0b0b36eabc05", and "Grant Admin Access to:" with the placeholder "Administrator user principal name". At the bottom right, there are two buttons: "Back" and "Next".

6. Configure parameter (see [Onboarding with Hosted Pro](#) on page 361).

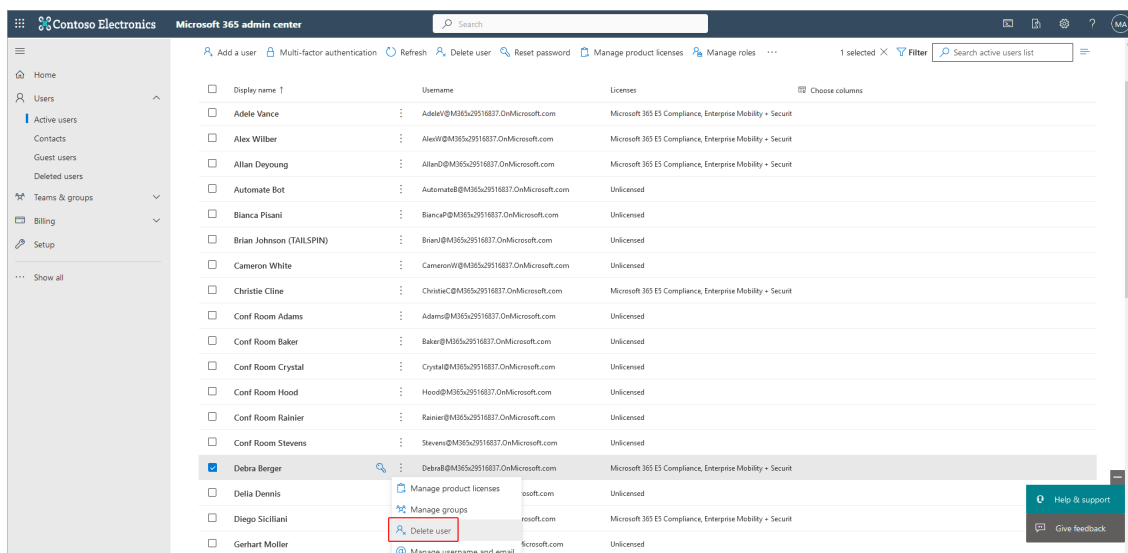
7. If the above message appears, you need to free a customer license; login to <https://www.office.com> with the credentials of the Onboarding customer.
8. In the Navigation pane, select **Admin**.



9. Select any user whose license you wish to release.



10. Right-click and choose **Delete user**.



11. Click **Delete User**.

×

Delete Debra Berger

Close

You can restore deleted users and their data, for up to 30 days after you delete them. Data on their connected devices will be removed, as well as the following:

i **Enterprise Mobility + Security E5, Office 365 E5, Microsoft 365 E5 Compliance** will be unassigned and available for other users

☐ Email aliases will be removed i
No email aliases

☐ Mailbox delegate permissions will be removed i
No mailbox delegate permissions

☐ Give another user access to Debra Berger's OneDrive files for 30 days after the user is deleted

☐ Give another user access to Debra Berger's email i

Delete user

The following confirmation is displayed.

×

Debra Berger has been deleted

You can restore deleted users, and recover their data except for calendar items and aliases, for up to 30 days from the [deleted users](#) list.

- ✓ Licenses unassigned
 - Enterprise Mobility + Security E5
 - Office 365 E5
 - Microsoft 365 E5 Compliance
- ✓ User account deleted

Close

12. Return to the wizard and click **Reload** to reload the license.

1 M365 Tenant

2 M365

3 Voice Route

×

Region/Country

Nederland

Ip Address

40.91.233.177

Sbc

SBC-Tobi

Domain Name

customers.activecommunications.eu

Sbc Site Name

Note: Modifying this will also change the customer name!

LBRCustomTest

Full Domain Name

LBRCustomTest.customers.activecommunications.eu

License Plan

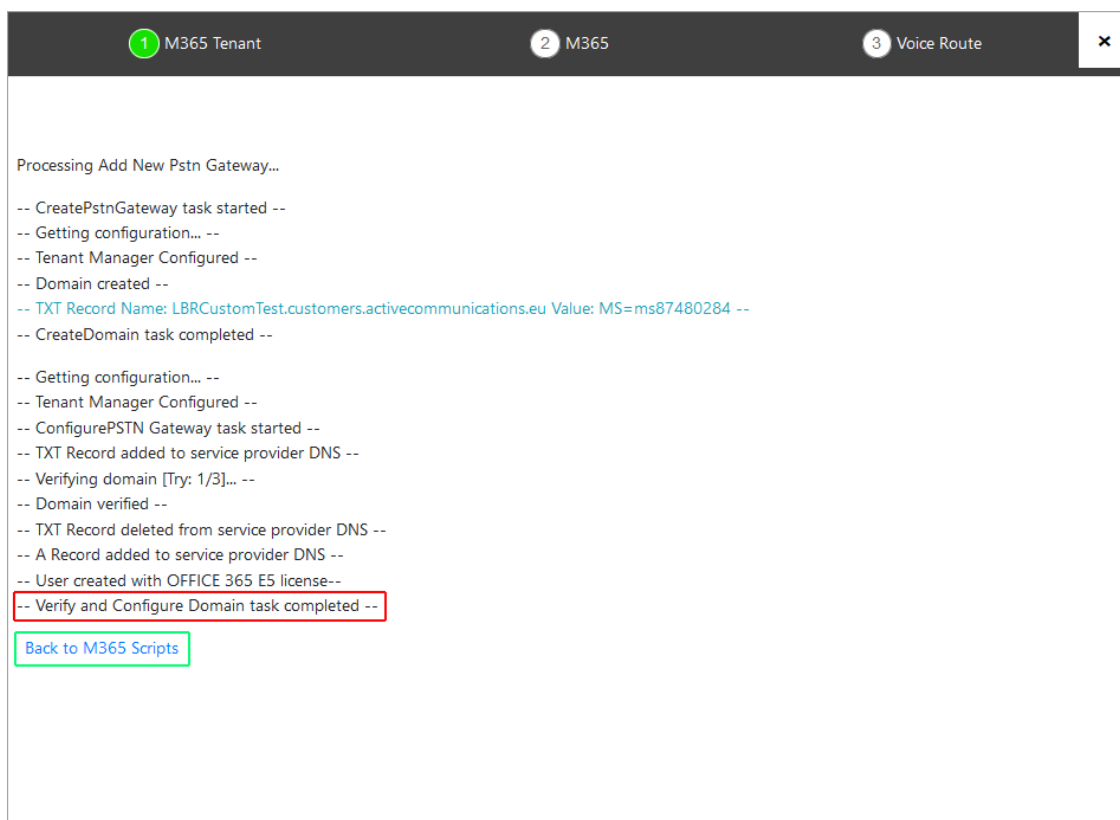
OFFICE 365 E5

Reload

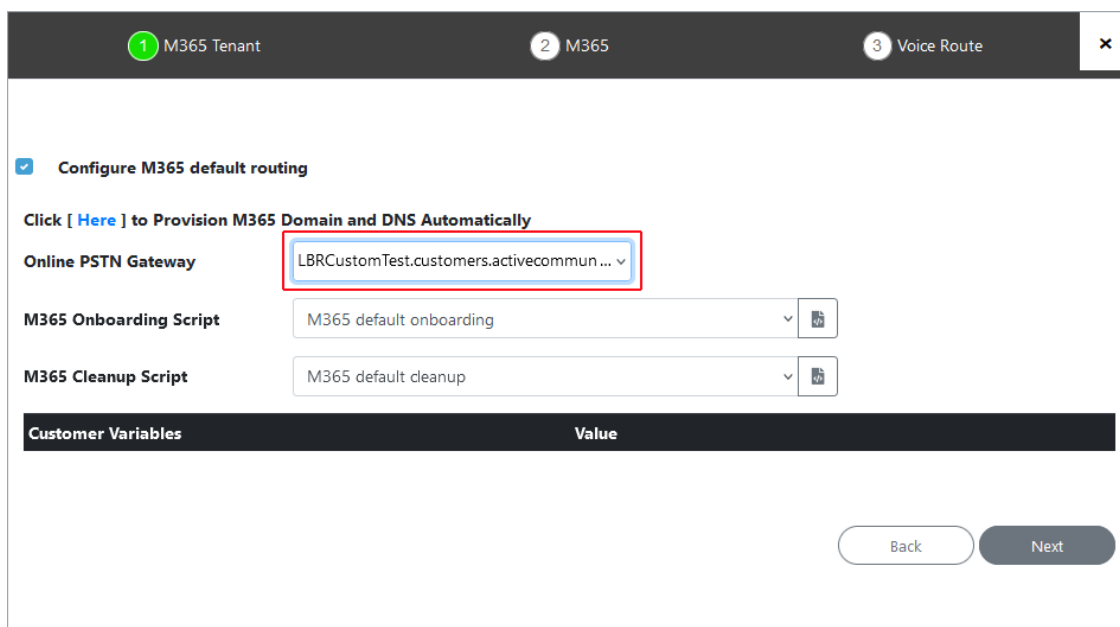
Back

Next

13. Click **Next** to continue the process of adding the PSTN gateway and DNS customer domain.



14. Once the Verify and Configure Domain task completed message is displayed, click **Back to M365 Scripts** link to return to the wizard configuration. Notice that the new PSTN gateway is displayed in the **Online PSTN Gateway** field.



15. Select one of the following scripts:

- M365 onboarding with Location-Based Routing
- M365 onboarding with Location-Based Routing and Custom Networks. For this option, the following custom variables must be configured

Customer Variable	Description
IP-Network	Internal IP address of the customer network
IP-SubnetBits	Subnet mask for the internal customer network interface
Trusted-IP-Network	Public IP address of the customer network.
Trusted-IP-Subnet-Bits	Subnet mask for the customer Public IP network interface

1 M365 Tenant
2 M365
3 Voice Route
×

☒ **Configure M365 default routing**

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

Online PSTN Gateway

M365 Onboarding Script

M365 Cleanup Script

Customer Variables	Value
IP-Network	<input type="text" value="192.168.180.0"/>
IP-SubnetBits	<input type="text" value="24"/>
Trusted-IP-Network	<input type="text" value="217.122.130.60"/>
Trusted-IP-SubnetBits	<input type="text" value="32"/>

16. Enter variable values and then click **Next**.

1 M365 Tenant
2 M365
3 Voice Route
×

Customer: **BradPro**

☐ **Configure SBC**

By selecting this check box, the wizard will automatically configure the SBC with a selectable CLI script.

17. Do one of the following:

- Configure SBC (see [Onboarding with only SBC Configuration](#) on page 418)

- Complete the wizard to create new customer (see below)

The screenshot shows a wizard window with three steps: 1 M365 Tenant, 2 M365, and 3 Voice Route. The first step is active. The main content area displays the following text:

```
Processing Add New ...
-- CreateCustomer task started --
Customer saved and queued for installation.
-- CreateCustomer task completed --
```

A "Close" button is located in the bottom right corner.

Two-step DNS Provisioning

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

➤ Do the following:

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

The screenshot shows the same wizard window, but now step 2, 'M365', is active. The main content area displays the following configuration options:

- ☒ **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

Below these options is a table with two columns: **Customer Variables** and **Value**. The table is currently empty.

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

1 M365 Tenant 2 M365 3 Voice Route

Region/Country
DEMOCRAD

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

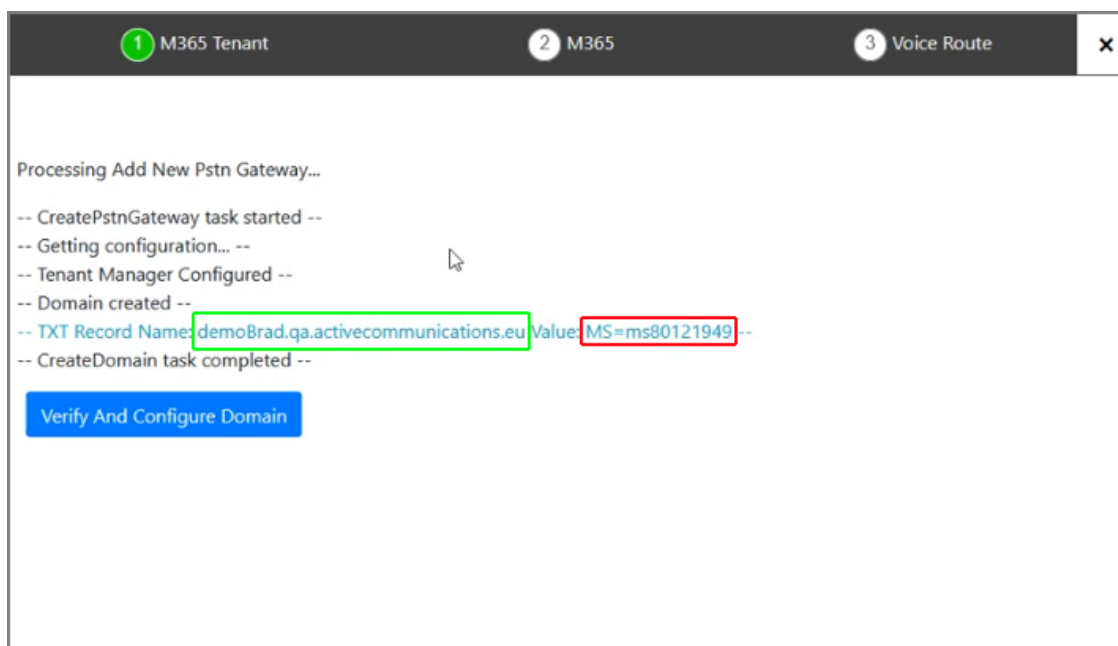
2. From the Region/Country drop-down, select the newly created region e.g. DEMOCRAD that you added in [Registering DNS Application \(Service Provider Tenant\)](#) on page 70.
3. Select the configured License Plan of the user e.g. Office 365 E5.



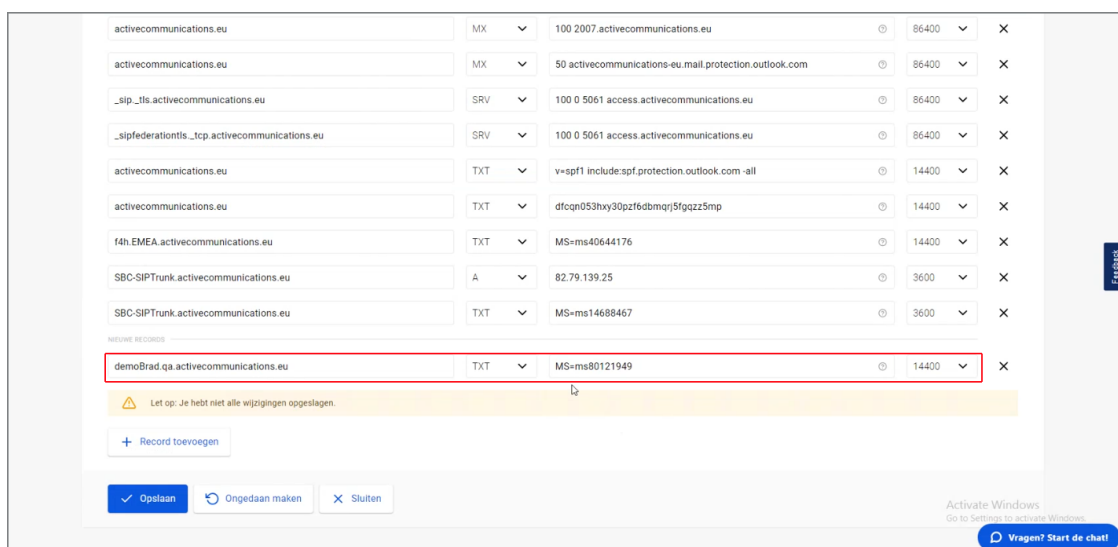
The Microsoft Office 365 Phone System user license should be preloaded as described in Section Activating the Providers Domain. If not, make a license available and then click Reload. The system is refreshed and searches for an available license for the tenant. The license plan is then loaded. The following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

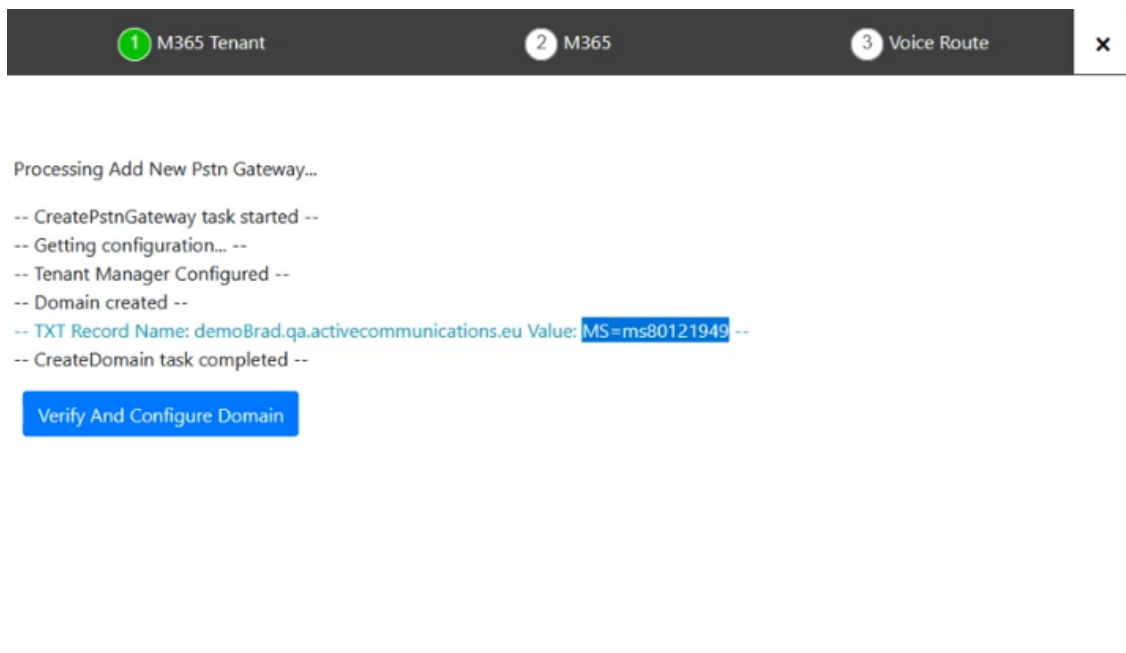
- E1 with Phone System
- E3 with Phone System
- Office 365 E5

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

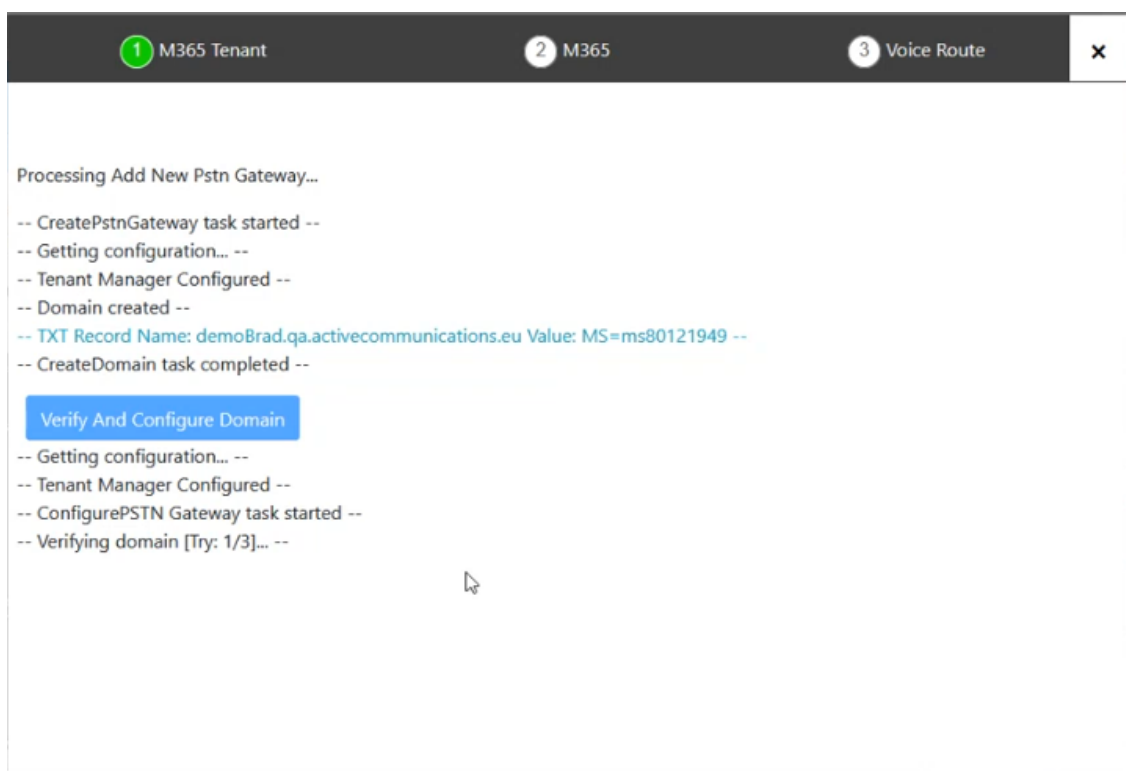


4. Copy the full record name <customername.domainname> and the TXT values to Notepad.
5. On your DNS Hosting platform, configure a new record with the values that you copied above, and then confirm .



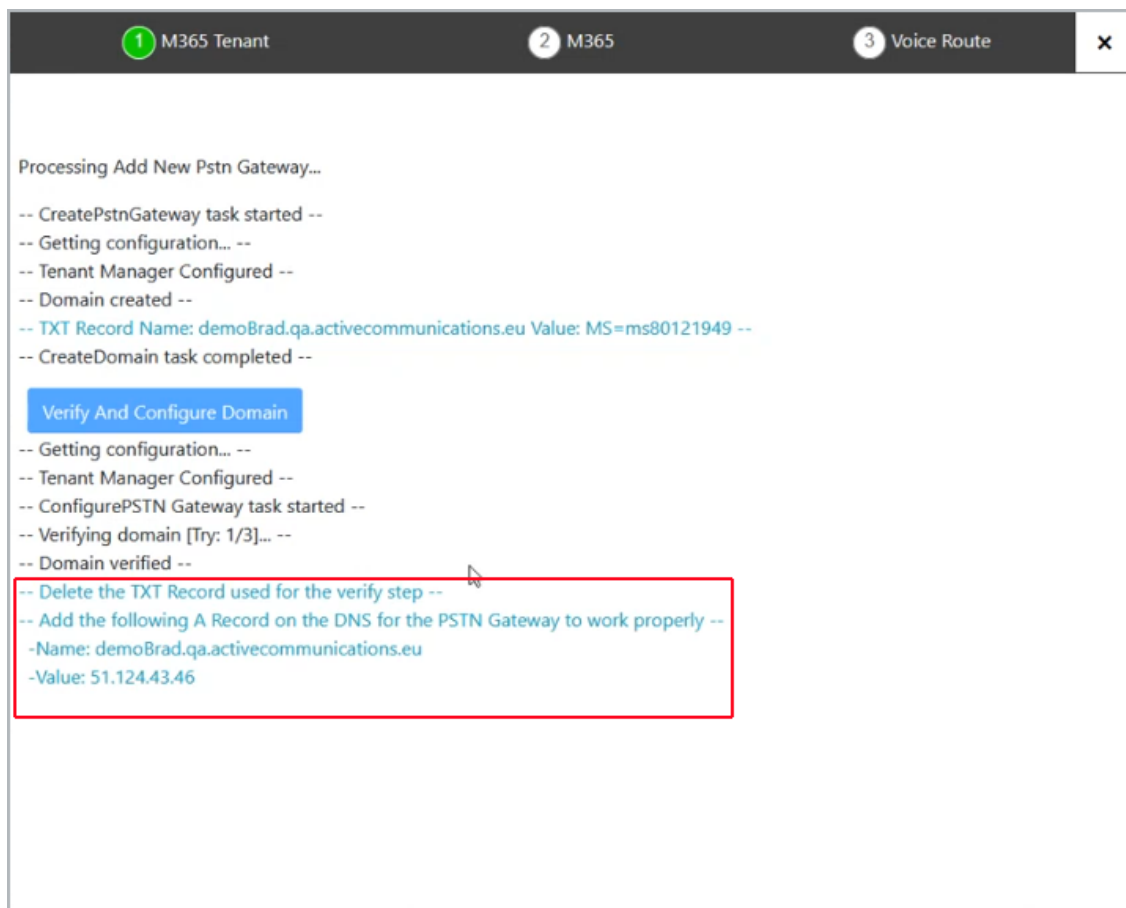


6. Click **Verify and Configure Domain**.

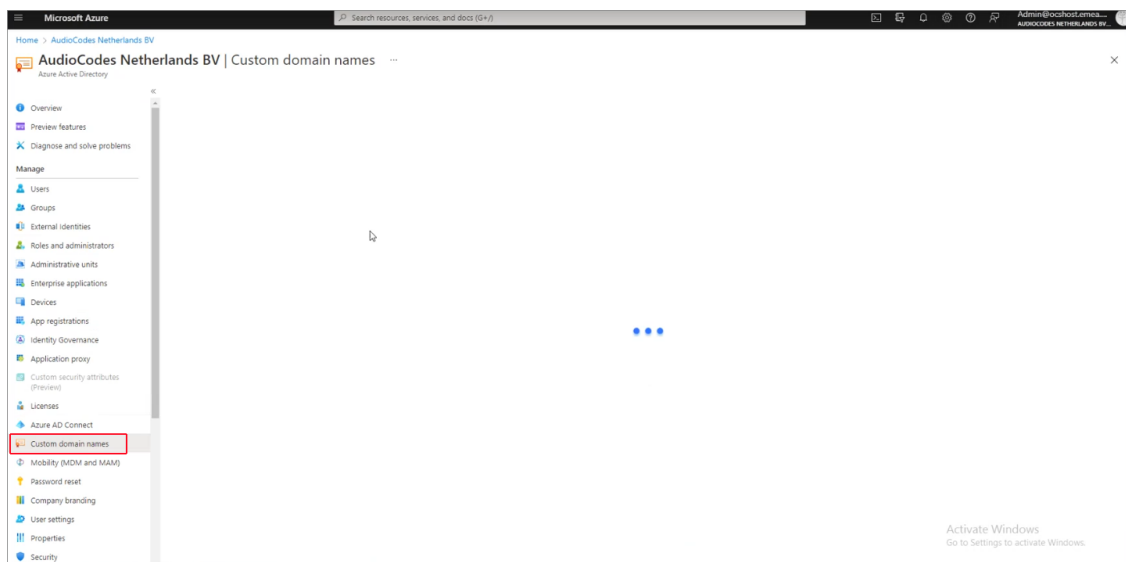


The verification process may take several tries to complete.

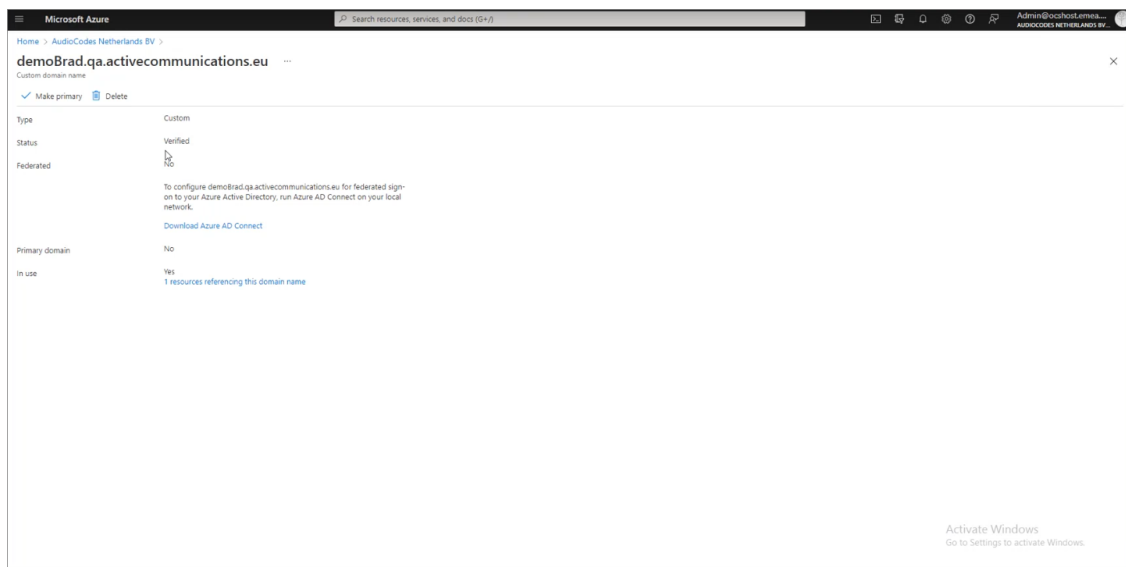
7. You are prompted to configure an A Record on the DNS Hosting platform.



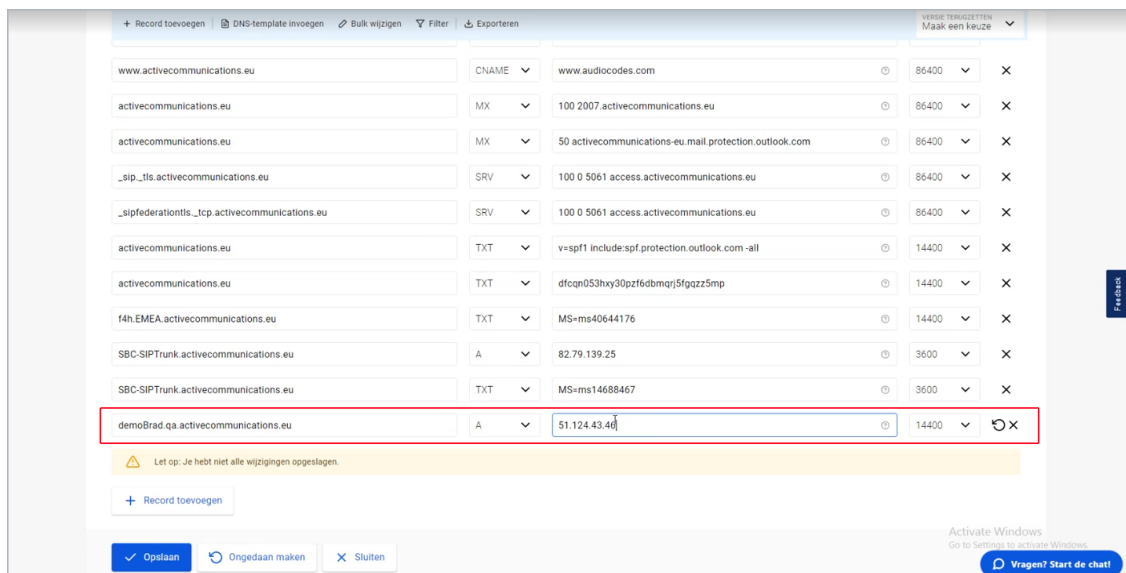
8. Open the customer Azure portal, and then in the Navigation pane, select **Custom domain names**.



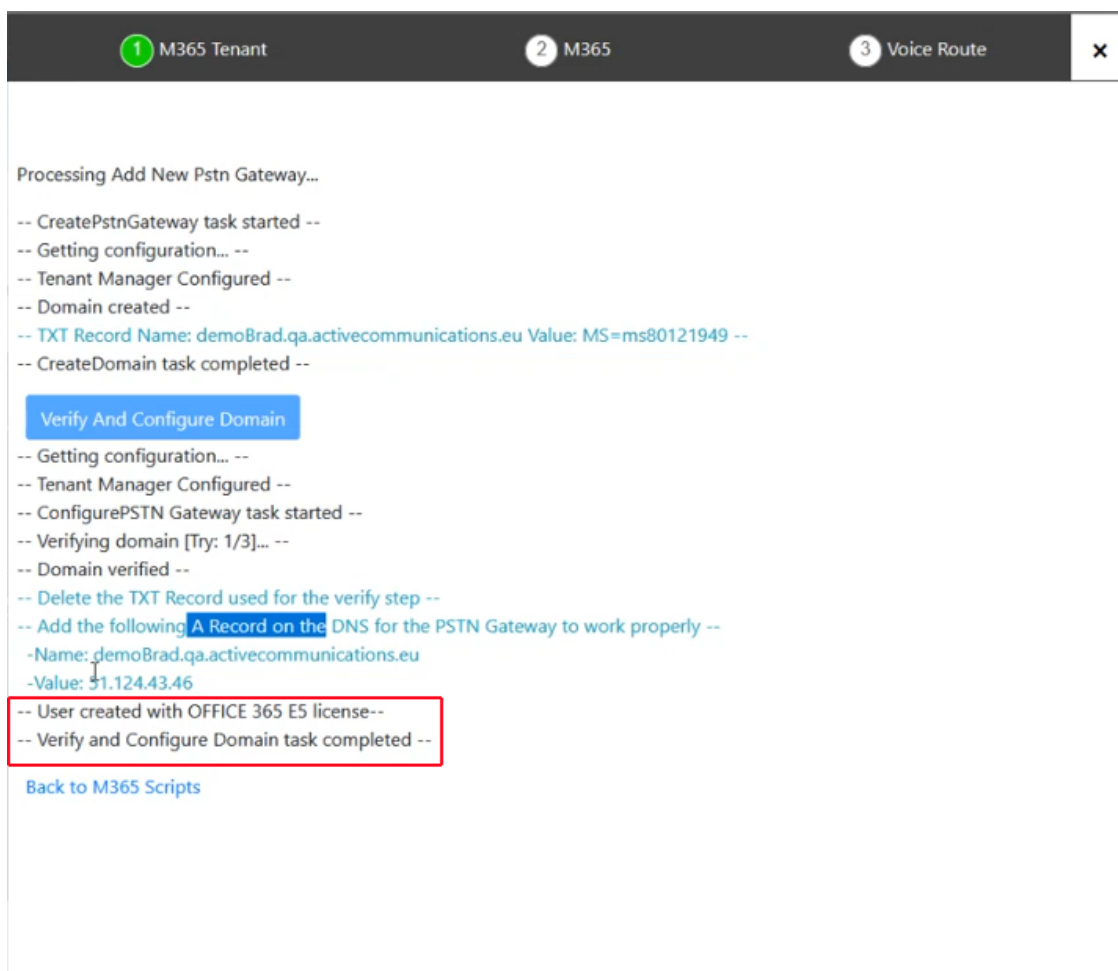
Notice the new domain that has been created.



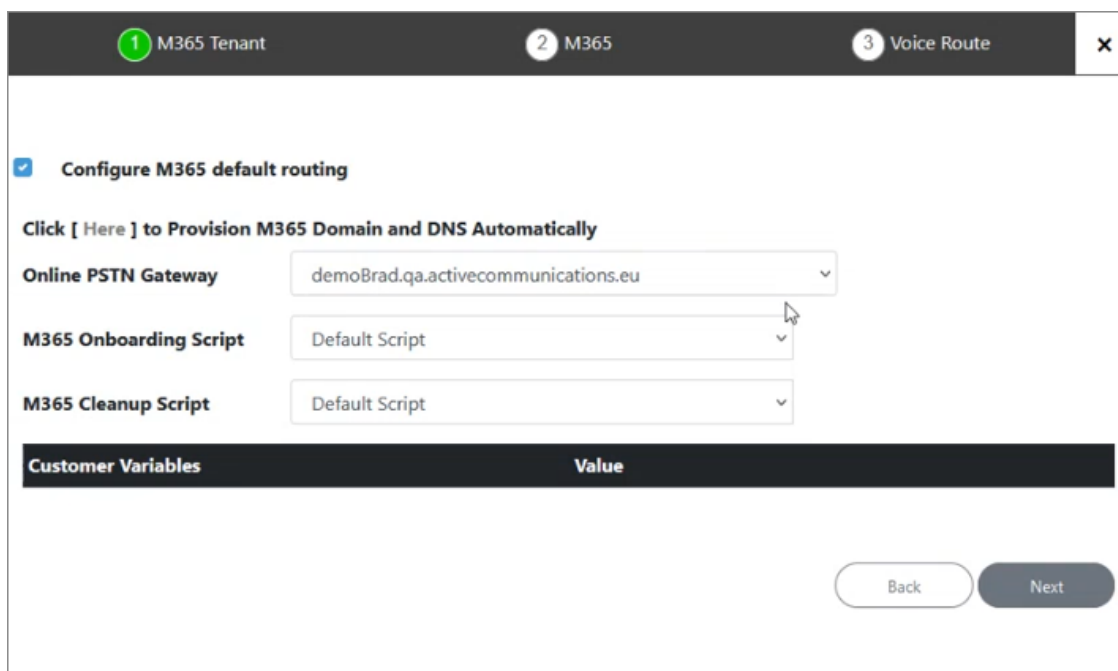
9. On the DNS Hosting platform, search for the TXT record that you create above, and then overwrite it by creating the A Record.



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



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



11. Click **Next** to continue.

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

12. Complete the wizard as described in Complete the Onboarding wizard as described in [Onboarding with both M365 Default Routing and SBC Configuration](#) on page 333.

Onboarding with only SBC Configuration

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

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

1 M365 Tenant

2 M365

3 Voice Route

X

Customer: ProTrunk

☒ **Configure SBC**

Sbc Site Name

Online PSTN Gateway

Sbc Configuration: ☒ Sip Trunk ☐ IP PBX ☐ BYOC

Region

Carrier

☐ **Carrier Registration**

☐ **Enable Cac**

Back Next

Sbc Configuration: ☒ Sip Trunk ☐ IP PBX ☐ BYOC

Region

Carrier

☒ **Carrier Registration**


☒ **Enable Cac**

Back Next

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

Table 31-12:SBC Parameters

SBC Parameter	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	Unique subdomain name per M365 Tenant (CSONlinePSTNGateway–FQDN) which represents the desired host name added for the carrier trunk.

SBC Parameter	Description
	<p>This name must be preconfigured on the M365 Tenant Domain or via DNS provisioning (see Register End Customer Tenant DNS Sub domains on page 250).</p> <div>  <p>If Default Routing is configured, then this field is automatically filled.</p> </div>
SBC Configuration	<p>Select one of the following SBC configuration modes:</p> <ul style="list-style-type: none"> ■ SIP Trunk: SIP Trunk used by Service Provider. When this option is selected, you must select both the SBC device (see 'Region' field below) and the Service Provider Carrier SIP Trunk (see 'Carrier' field below). ■ IP-PBX: Service Provider IP-PBX. When this option is selected, you must select both the SBC device and the Service Provider Carrier SIP Trunk (see 'Region' field below). ■ BYOC: (Bring-Your-Own-Carrier) for integrating customer SIP Trunk services that are different to the SIP Trunk service used by their Service Provider. When this option is selected, you must select both the SBC device (see 'Region' field below) and the Service Provider Carrier SIP Trunk (see 'Carrier' field below).
Region	Select the required SBC device for the site location.
<p>Carrier: (this option is only relevant if you are connecting your Carrier to a SIP Trunk (when options SIP Trunk or BYOC are selected 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.

SBC Parameter	Description
	<p>This appears in REGISTER From/To headers as ContactUser@HostName</p> <p>■ Host Name: Defines the Address of Record (AOR) host name. The host name appears in SIP REGISTER From/To headers as ContactUser@HostName.</p>
Enable CAC	Enable Call Admission Control (CAC). From the drop-down list, select the desired CAC Profile including the desired number of call sessions.

- Click **Next**, the Wizard continues with the configuration of the SBC Number Prefixes. For initial setup, a Dialplan file must be preconfigured on the SBC or IP-PBX. For Second day management, SBC prefixes can later be imported (see [Manage SBC Prefixes](#) on page 533).

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

Table 31-13: 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.

1 M365 Tenant
2 M365
3 Voice Route

SBC number prefixes
Browse... pbxexample.csv
pbxexample.csv

New Number prefix

Back
Next

1 M365 Tenant
2 M365
3 Voice Route

SBC number prefixes
Browse... No file selected.

New Number prefix

314

Back
Next

2 M365 Tenant
2 M365
3 Voice Route


SBC Onboarding Script
sbcs-scenario7


SBC Cleanup Script
sbcs-scenario7Cleanup

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

Back
Submit

4. 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 [Customer Variables](#) on page 210.

5. When you have completed the configuration, click

Submit

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

Part VI

Second Day Operations

32 Day Two Management using Customer Tenant Portal

This section describes Day Two Management for the Direct Routing and Operator Connect Service Types using the Customer portal. The following actions can be performed:

- [Initial Access to UMP-365 and Assigning Customer Admins](#) below
- [Customer Portal Direct Routing License Model Menus](#) on page 428
- [Provisioning with Direct Routing](#) on page 432
- [Manually Provisioning Users](#) on page 443
- [Manually Assigning Phone Numbers to Users](#) on page 443
- [Lifecycle Management](#) on page 451
- [Managing Templates](#) on page 459
- [Location-Based Routing](#) on page 471
- [Configuring Online Voice Routing](#) on page 495
- [Reserving Customer Phone Numbers](#) on page 507
- [Viewing Audit and Roll Back Historical Updates](#) on page 507
- [Monitoring M365 Replication Actions Queue](#) on page 508
- [Securing Microsoft 365 Service Provider Access](#) on page 511
- [Managing Site Locations](#) on page 530
- [Managing User Licenses](#) on page 540

Initial Access to UMP-365 and Assigning Customer Admins

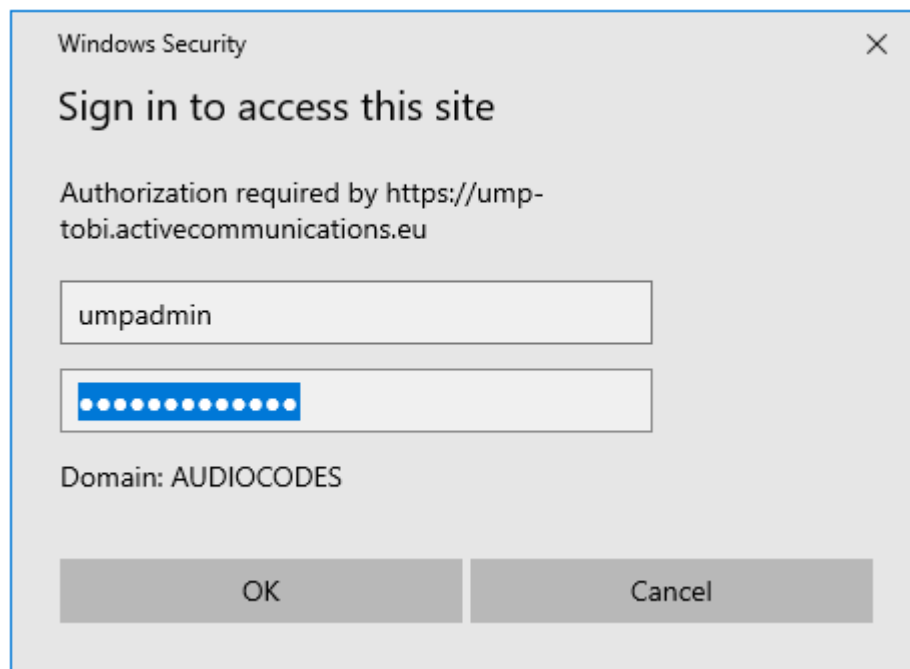
The initial login should be performed by the local administrator of service account for this server (see [Creating UMP Service Account](#) on page 29). Once logged in, navigate to the relevant customer tenant and choose any user to grant permissions as an administrator. This user administrator is then able to login to the tenant portal for this tenant.



This functionality requires an Application registration on Azure Service Provider tenant (see [Create Registration for Customer Administrators](#) on page 87).

➤ To access the customer portal:

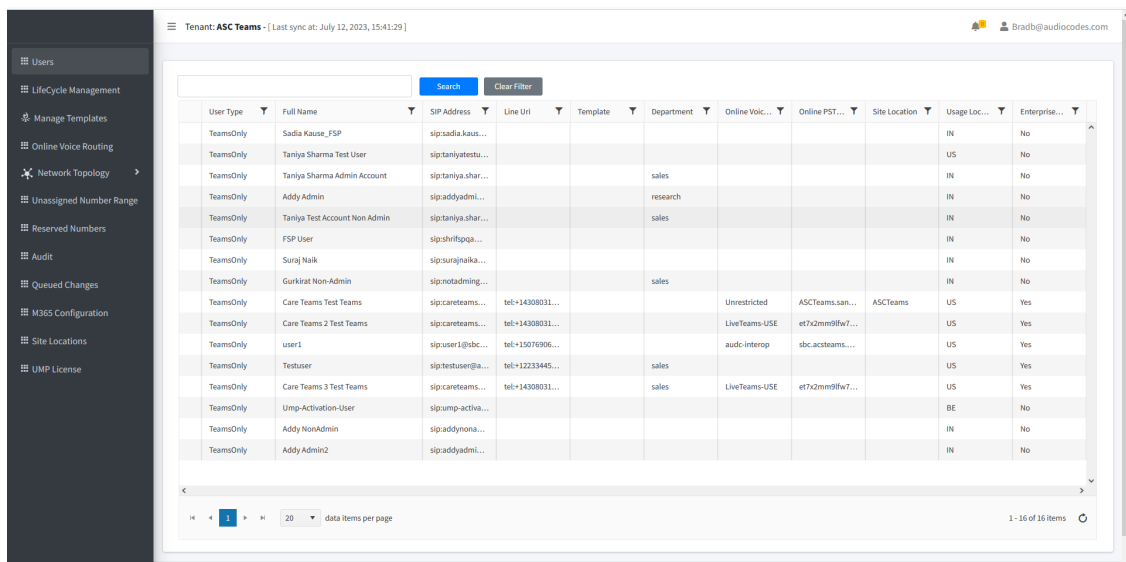
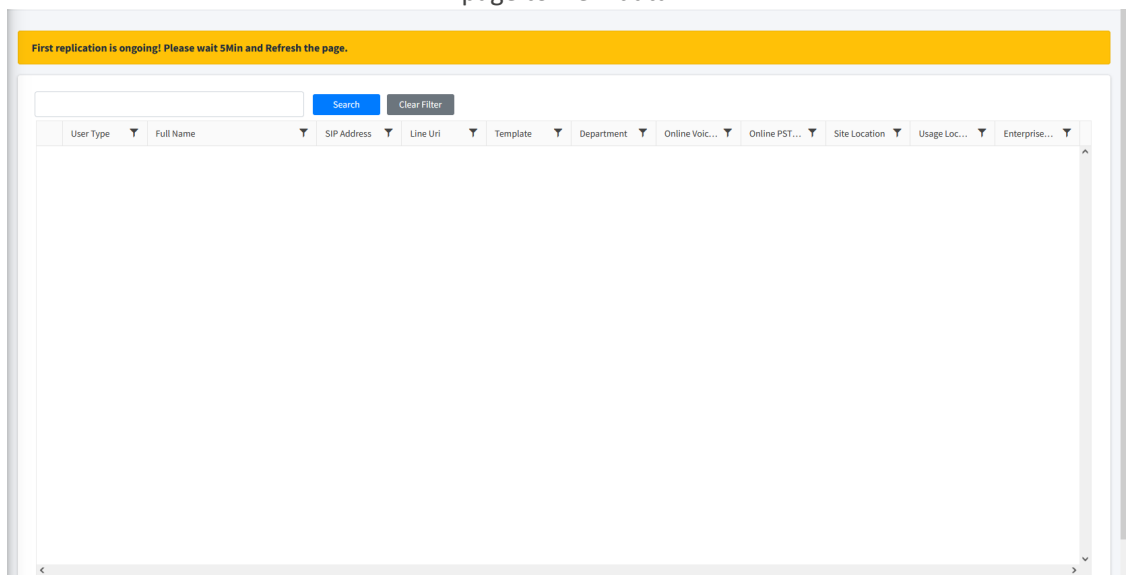
1. Login to the Multitenant portal with Service Account permissions.



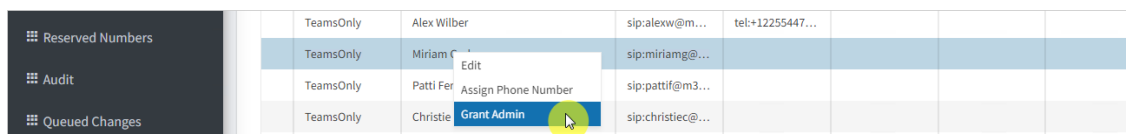
2. Click the **SysAdmin** link adjacent to the customer that you wish to edit.

Customer Name	State	SysAdmin Info	Licensing (licensed users)	Queued commands status
1 TO ALL CO LTD	Deployed	version: 8.0.450.101 replication: 2023.07.12.11.58.05 SysAdmin	M365 - Pro (10)	Queued commands: 5 Executing commands: 0 Replication in progress: no
220914	Deployed	version: 8.0.450.101 replication: 2023.07.12.11.48.48 SysAdmin	M365 - Pro (500)	Queued commands: 0 Executing commands: 1 Replication in progress: no
AdminRandD	Deployed	version: 8.0.450.101 replication: 2023.07.12.12.28.58 SysAdmin	M365 - Pro (10)	Queued commands: 0 Executing commands: 0 Replication in progress: no
Alex and sons	Deployed	version: 8.0.450.101 replication: 2023.07.12.11.56.55 SysAdmin	M365 - Pro (22)	Queued commands: 5 Executing commands: 0 Replication in progress: no
Alex MS Dynamics 365	Deployed	version: 8.0.450.101 replication: 2023.07.12.11.58.39 SysAdmin	M365 - Pro (11)	Queued commands: 5 Executing commands: 0 Replication in progress: no
Anatoly as Customer1	Deployed	version: 8.0.450.101 replication: 2023.07.12.11.49.12 SysAdmin	M365 - Pro (5)	Queued commands: 5 Executing commands: 0 Replication in progress: no
ASC Teams	Deployed	version: 8.0.450.101 replication: 2023.07.12.11.37.54 SysAdmin	M365 - Pro (10)	Queued commands: 0 Executing commands: 0 Replication in progress: no
AudCDemo4LATAM	Deployed	SysAdmin	M365 - OC Essential (0)	Queued commands: 0

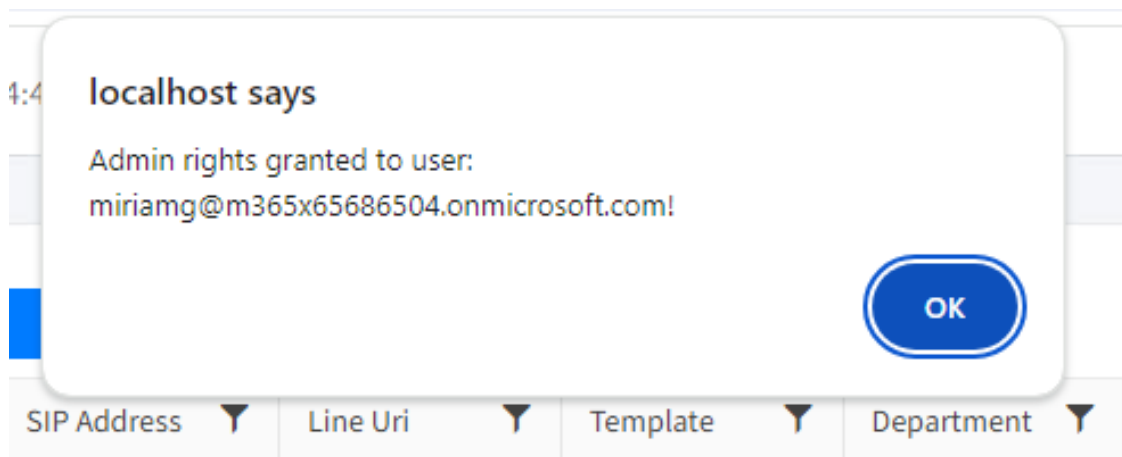
The initial replication process to retrieve tenant M365 users may take a few minutes. Refresh page to view data.



3. Select the desired user, right-click, select **Grant Admin**, and then click **OK**.

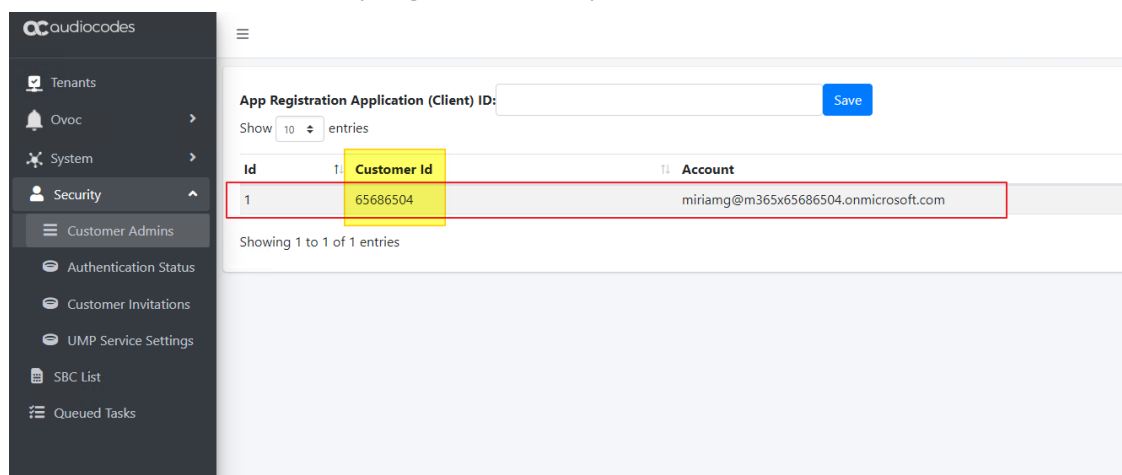


A confirmation message is displayed.



4. Open the Multitenant portal Customer Admins page (**Security > CustomerAdmins**).

Notice the user to whom you granted Admin permissions is added to the list.



5. Likewise, to revoke a user, in the right-click menu, choose **Revoke Admin**.

TeamsOnly	Alex Wilber	sip:alexw@m...	tel:+12255447...
TeamsOnly	Miriam Graham	sip:miriamg@...	
TeamsOnly	Patti Fernandez	sip:pattif@m3...	
TeamsOnly	Christie Cline	sip:christiec@...	
TeamsOnly	Johanna Lorenz	sip:johanna@...	

Customer Portal Direct Routing License Model Menus

Customers can be managed in the Customer portal according to the customer license capabilities.

- **Hosted Essentials** on the next page
- **Hosted Essentials Plus** on the next page
- **Hosted Pro** on page 430

Hosted Essentials

The following actions can be performed with Hosted Essentials license capabilities:

- Manage SBC Prefixes (see [Manage SBC Prefixes](#) on page 533)
- Manage User Management Pack™ 365 SP Edition User licenses (see [Managing User Licenses](#) on page 540)

The following figure displays a selected Hosted Essentials licensed customer in the Live Cloud portal.

The screenshot shows the Live Cloud portal interface. At the top, there are tabs for DASHBOARD, NETWORK, ALARMS, STATISTICS, CALLS, USERS, SYSTEM, and SERVICE REQUEST. Below these, there's a 'CUSTOMER' section with a table of services. The table has columns for FULL NAME, NAME, SERVICE TYPE, STATUS, DEPLOY STATUS, LICENSE TYPE, USERS COUNT, ENABLED, CAC PROFILE, CARRIER NAME, CHANNEL NAME, and TOTAL. The first row is highlighted in green, showing 'M365s57163939 Bahir test' with 'aiologicESS' as the service type and 'Essential' as the license type. To the right of the table, there's a 'CUSTOMER DETAILS' panel with a 'Details' tab. It shows the customer's name 'aiologicESS', status 'OK', and deployment status 'Deployed'. The license type is 'Essential' and the carrier name is 'SPTrunk'. The 'CUSTOMER ACTIONS' dropdown menu is open, showing options like 'Direct Routing', 'Edit Customer', and 'Delete'. The 'Direct Routing' option is selected, and the 'Edit Customer' option is highlighted.

1. From the Customer Actions drop-down menu, choose **Direct Routing > Edit Customer**. The Customer portal menu opens.

The screenshot shows the Customer portal menu. On the left, there's a sidebar with 'Site Locations' and 'UMP License'. The main area has a 'Tenant: aliquip eu pariatur' header. Below this, there's a 'Sites' tab. The 'Sites' tab shows a table with columns: Site, SBC Name, Configuration, PSTN Gateway, Sbc Deployment State, M365 Deployment State, Notes, and Actions. The first row is 'ColtTestJuly' with 'ServiceProvider1 SBC1 [40.87.31.200]' as the SBC Name. The 'Actions' column for this site shows 'Uninstall' and 'Manage Sbc Prefixes'.

Hosted Essentials Plus

The following actions can be performed with Hosted Essentials + license capabilities:

- Users (see [Manually Provisioning Users](#) on page 443)
- Assign Phone Numbers (see [Manually Assigning Phone Numbers to Users](#) on page 443)
- Manage Templates (see [LifeCycle Management](#))
- Configure Online Routing (see [Configuring Online Voice Routing](#) on page 495)
- Manage Location-based routing (see [Location-Based Routing](#) on page 471)
- View queue for tasks status and results (see [Monitoring M365 Replication Actions Queue](#) on page 508)
- Update the Microsoft 365 Settings (see [Securing Microsoft 365 Service Provider Access](#) on page 511)
- Manage Site Locations (see [Managing Site Locations](#) on page 530)

■ Manage UMP User licenses (see [Managing User Licenses](#) on page 540)

The following figure shows a selected Hosted Essentials Plus licensed customer type in the Live Cloud portal.

FILTERS	FULL NAME	NAME	SERVICE TYPE	STATUS	DEPLOY STATUS	LICENSE TYPE	USERS COUNT	ENABLED	CAC PROFILE	CARRIER NAME	CHANNEL NAME	TOTAL
ADD FILTER	AirTel End ...	012475882821	Teams: Direct Routing	●	●	Pro	0	✓		Telnyx		0
REAL TIME	220914	220914	Teams: Direct Routing	●	●	Pro	2	✓		Telnyx		1,001
	AudioCod...	acmx	Teams: Direct Routing	●	●	Pro	3	✓		Telnyx		9
	Microsoft ...	adatum	Compliance Recording	●	●	Audio & Vide...	20					
	aiLogicSDR	aiLogicSDR	Teams: Direct Routing	●	●	Pro	0	✓		SIPTrunk		0
	Alex and s...	Alex222	Teams: Direct Routing	●	●	Pro	0	✓		Telnyx		0
	AutoDem...	AutoDemo4LATAM	Teams: Operator Connect	●	●	Essential		✓				1
	AustraliaO...	AUDemo1	Teams: Direct Routing	●	●	Pro	0	✓		Movio		100
	audioDco...	audioDcode	Teams: Operator Connect	●	●	Essential		✓				1
	AudioCod...	audioCod02	Teams: Direct Routing	●	●	Essential	1	✓		Telnyx	APAC-Channel	0
	AudioCodes	AudioCodes	Teams: Operator Connect	●	●	Essential		✓				1
	AudioCod...	AudioCodes8	Teams: Operator Connect	●	●	Essential		✓				1
	AutoCod...	AutoCodesUS	Teams: Operator Connect	●	●	Essential		✓				2
	Aut Test ...	AUTest1	Teams: Direct Routing	●	●	Pro	1	✓		Movio		10
	Beneta J...	BenetaJFDemo	Teams: Direct Routing	●	●	Pro	0	✓		Telnyx		113
	BLRTesT	BLRTesT	Teams: Direct Routing	●	●	Essential	0	✓		SIPTrunk		0
	C2 Comm...	C2Comm	Teams: Direct Routing	●	●	EssentialPlus	0	✓		TPGAU01	C2Communica...	0
	Callaba	callaba	Compliance Recording	●	●	Audio & Vide...	20					
	Callaba	Callaba	Teams: Direct Routing	●	●	Pro	5	✓		SIPTrunk		5
	Candela s...	Candela	Teams: Direct Routing	●	●	Pro	1	✓		Telnyx		6
	Central Ba...	cbnigeria	Teams: Direct Routing	●	●	Pro	49	✓	5 sessions	INQ Digital	ZA Channel De...	50
	Client1	Client1	Teams: Direct Routing	●	●	Pro	0	✓		LatamSIP		1,000
	Colt Demo...	coltdemo	Teams: Direct Routing	●	●	EssentialPlus	0	✓		Telnyx	Colt-Claudia-de...	1
	customer8	customer8-ZM	Zoom: Peering	●	●	Essential		✓				1
	Customer...	CustomerTh1	Teams: Direct Routing	●	●	Pro	0	✓		SIPTrunk		0

FILTERS	FULL NAME	NAME	SERVICE TYPE	STATUS	DEPLOY STATUS	LICENSE TYPE	USERS COUNT	ENABLED	CAC PROFILE	CARRIER NAME	CHANNEL NAME	TOTAL NUMBER OF DIDS	TENANT	PROVIDERS SIDE	TEAM
ADD FILTER	BroEssen...	BroEssen1	Teams: Di...	●	●	Essential Plus	0	✓		SIPTrunk		0	AudioCodeDig	BroEssen1	
REAL TIME															

1. From the Customer Actions drop-down menu, choose **Direct Routing > Edit Customer**. The Customer portal menu opens.

User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voic...	Online PST...	Site Location	Usage Loc...	Enterprise...
TeamsOnly	Miriam Graham	sip:miriam@...				Unrestricted			GB	Yes
TeamsOnly	Christie Cline	sip:christie@...							GB	No
TeamsOnly	Lynne Robbins	sip:lynne@...							GB	No
TeamsOnly	Lidia Holloway	sip:lidia@...							GB	No
TeamsOnly	Alex Wilber	sip:alex@...							GB	No
TeamsOnly	Isalah Langer	sip:isalah@...							GB	No
TeamsOnly	Allan Deyoung	sip:allan@...							GB	No
TeamsOnly	Joni Sherman	sip:joni@...							GB	No
TeamsOnly	Irvin Sayers	sip:irvin@...							GB	No
TeamsOnly	Grady Archie	sip:grady@...							GB	No
TeamsOnly	Adela Vance	sip:adela@...							GB	No
TeamsOnly	Lee Gu	sip:lee@...							GB	No
TeamsOnly	Megan Bowen	sip:megan@...							GB	No
TeamsOnly	MOD Administrator	sip:admin@...							GB	No
TeamsOnly	Diego Siciliani	sip:diego@...							GB	No
TeamsOnly	Johanna Lorenz	sip:johanna@...							GB	No
TeamsOnly	Debra Berger	sip:debra@...							GB	No

Hosted Pro

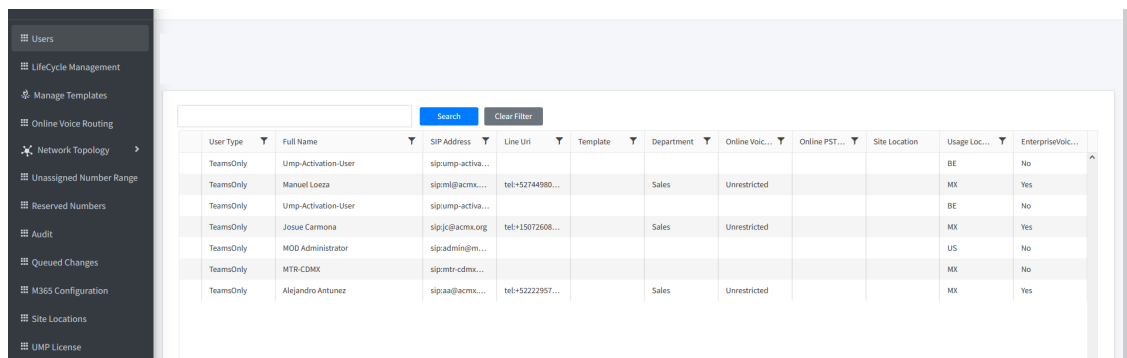
The following actions can be performed with Hosted Pro license capabilities:

- Users (see [Manually Provisioning Users](#) on page 443)
- Assign Phone Numbers (see [Manually Assigning Phone Numbers to Users](#) on page 443)
- LifeCycle Management (see [Lifecycle Management](#) on page 451)
- Manage Templates (see [Managing Templates](#) on page 459)
- LBR Network Topology (see [Location-Based Routing](#) on page 471)
- Unassigned Number Ranges (see [Managing Unassigned Number Ranges](#) on page 451)
- Reserve M365 Tenant Phone Numbers (see [Reserving Customer Phone Numbers](#) on page 507)
- Audit activities (see [Viewing Audit and Roll Back Historical Updates](#) on page 507)
- Configure Online Routing (see [Voice Routing Policy](#) on page 496)
- View queue for tasks status and results (see [Monitoring M365 Replication Actions Queue](#) on page 508)
- Update the Microsoft 365 Setting (see [Securing Microsoft 365 Service Provider Access](#) on page 511)
- Manage Site Locations (see [Managing Site Locations](#) on page 530)
- Manage UMP User Licenses (see [Managing User Licenses](#) on page 540)
- (see [Managing Templates](#) on page 459)

The following figure shows a selected Hosted Pro licensed customer in the Live Cloud portal.

The screenshot displays the 'CUSTOMERS' section of the Live Cloud portal. A table lists various customers with columns for Full Name, Name, Service Type, Status, Deploy Status, License Type, Users Count, Enabled, CAC Profile, Carrier Name, Channel Name, and Total Number of DIDs. The customer 'Benelux J. BeneluxJFDemo' is highlighted in blue. To the right, the 'CUSTOMER DETAILS' panel is open, showing information for 'Benelux J. BeneluxJFDemo', including its status (OK), deployment status (Deployed), full name, service type (Teams: Direct Routing), license type (Pro), carrier name (Telnyx), Azure tenant ID, users count (20), total number of DIDs (115), used DIDs (2), and unused DIDs (113). The 'ACTIVE ALARMS' section shows no active alarms.

1. From the Customer Actions drop-down menu, choose **Direct Routing > Edit Customer**. The Customer portal menu opens.



The screenshot shows the UMP-365 Customer Tenant Portal interface. On the left is a dark sidebar with a menu containing: Users, LifeCycle Management, Manage Templates, Online Voice Routing, Network Topology, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, Site Locations, and UMP License. The main area displays a table of users with search and filter buttons at the top. The table has columns for User Type, Full Name, SIP Address, Line Uri, Template, Department, Online Voic..., Online PST..., Site Location, Usage Loc..., and EnterpriseVoic... The data rows show various users, including 'Ump-Activation-User', 'Manuel Loeza', 'Ump-Activation-User', 'Josue Carmona', 'MOD Administrator', 'MTR-CDMX', and 'Alejandro Antunez'.

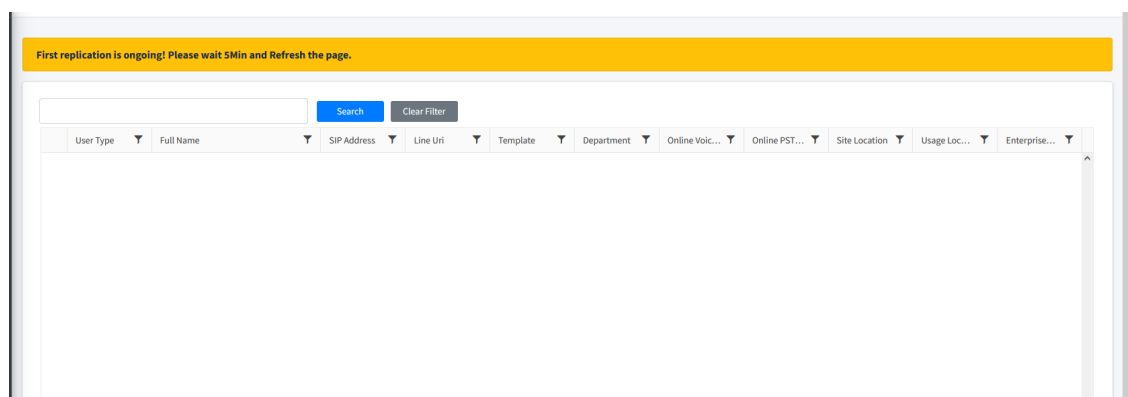
User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voic...	Online PST...	Site Location	Usage Loc...	EnterpriseVoic...
TeamsOnly	Ump-Activation-User	sipump-activa...							BE	No
TeamsOnly	Manuel Loeza	siplml@acmx...	tel:+52744980...		Sales	Unrestricted			MX	Yes
TeamsOnly	Ump-Activation-User	siplump-activa...							BE	No
TeamsOnly	Josue Carmona	sipljc@acmx.org	tel:+15072608...		Sales	Unrestricted			MX	Yes
TeamsOnly	MOD Administrator	sipladmin@m...							US	No
TeamsOnly	MTR-CDMX	siplmtr-cdmx...							MX	No
TeamsOnly	Alejandro Antunez	siplaa@acmx...	tel:+52222957...		Sales	Unrestricted			MX	Yes

Provisioning with Direct Routing

Once the new customer has been onboarded, M365 users must be applied the appropriate license and basic template configuration before they can connect calls. Users are applied basic configuration in the Onboarding scripts including a default route and default routing policy and a configured PSTN gateway for connecting calls (see figures below). Provisioning can be performed manually or automated using templates. The templates can then be applied to different user groups in the Enterprise Active Directory. The templates are mapped to Calling Policies that are mapped to Voice Routes for different site locations. The routes defined through which SBC device calls are connected to the customer or provider SIP Trunk or to the Provider IP PBX. Dial plan patterns can also be associated with the Voice Routes. The PSTN Usage maps the Voice Route to the Voice Routing Policy. You can then assign phone numbers (DIDs) and map them to Templates together with OnlineVoiceRouting and other Teams Calling policies.

➤ Do the following:

1. Open the Customer portal (see [Initial Access to UMP-365 and Assigning Customer Admins](#) on page 425) and wait for the initial replication process to complete.



User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voice Routing Policy	Online PSTN Usage	Site Location
TeamsOnly	Miriam Graham	sip:miriamg@...						
TeamsOnly	Christie Cline	sip:christiec@...						
TeamsOnly	Lynne Robbins	sip:lynner@m...						
TeamsOnly	Lidia Holloway	sip:lidiah@m3...						
TeamsOnly	Alex Wilber	sip:alexw@m3...						
TeamsOnly	Isaiah Langer	sip:isalah@m...						
TeamsOnly	Allan Deyoung	sip:alland@m...						
TeamsOnly	Joni Sherman	sip:jonis@m36...						
TeamsOnly	Irvin Sayers	sip:irvins@m3...						
TeamsOnly	Grady Archie	sip:gradya@m...						
TeamsOnly	Adele Vance	sip:adelev@m...						
TeamsOnly	Lee Gu	sip:leeg@m36...						
TeamsOnly	Megan Bowen	sip:meganb@...						
TeamsOnly	MOD Administrator	sip:admin@m...						
TeamsOnly	Diego Siciliani	sip:diegos@m...						
TeamsOnly	Johanna Lorenz	sip:johanna@...						
TeamsOnly	Debra Berger	sip:debrab@m...						

1 - 17 of 17 items

- In the Navigation pane, select **Online Voice Routing > Voice Routes** and **Voice Routing Policy**. See the default entries.

Dial Plans

Normalization Rule Templates

PSTN Gateways

PSTN Usage

Voice Routes

Voice Routing Policies

Add New Voice Route

DataCh...	Identity	Prio...	Pattern	Name	Description	PSTN Gateway List	PSTN Usage	
	Unrestricted	0	.	Unrestricted		BradDRService.sandbox2.aud locodes.be	Unrestricted	▼ ▲

Dial Plans

Normalization Rule Templates

PSTN Gateways

PSTN Usage

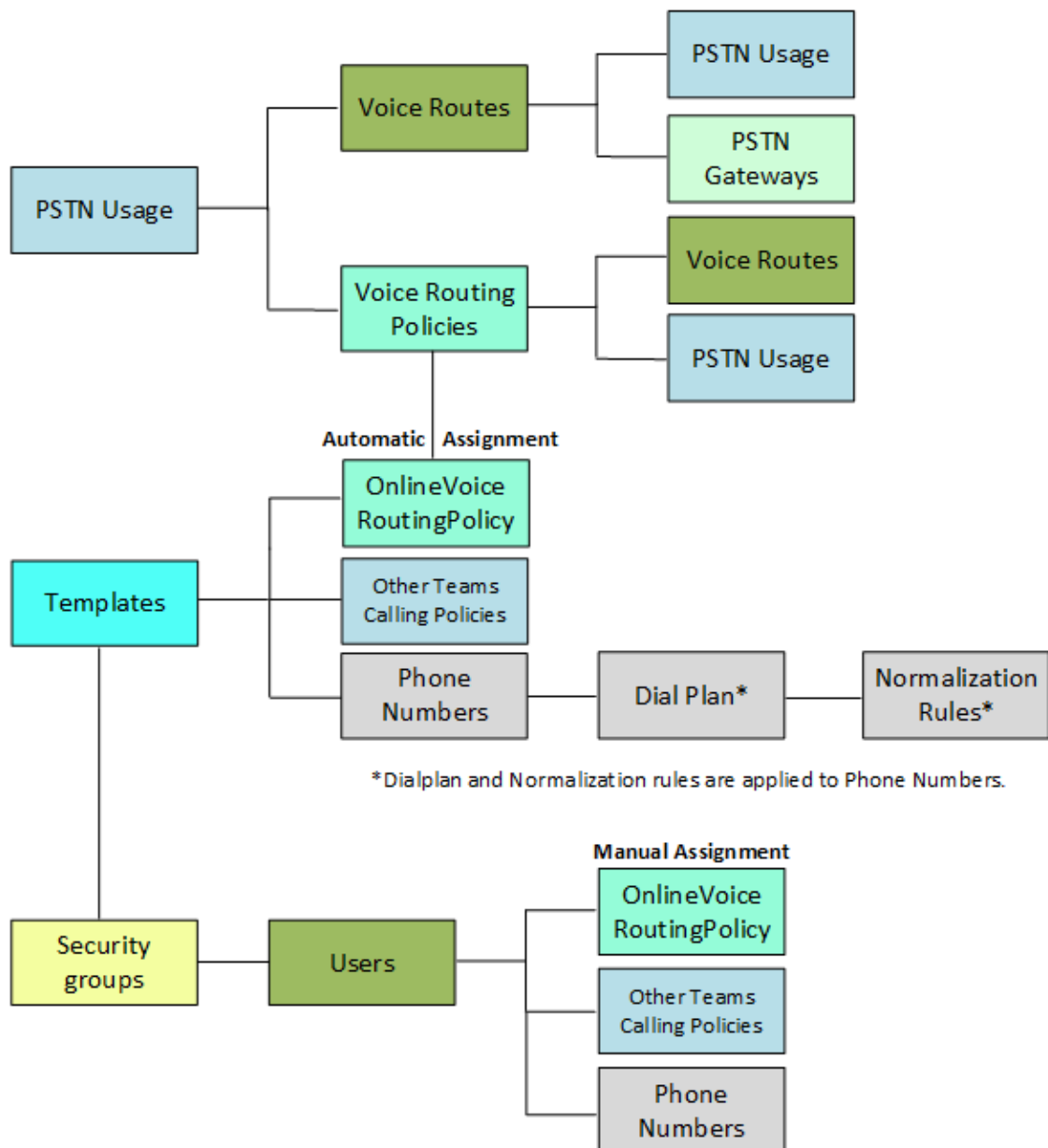
Voice Routes

Voice Routing Policies

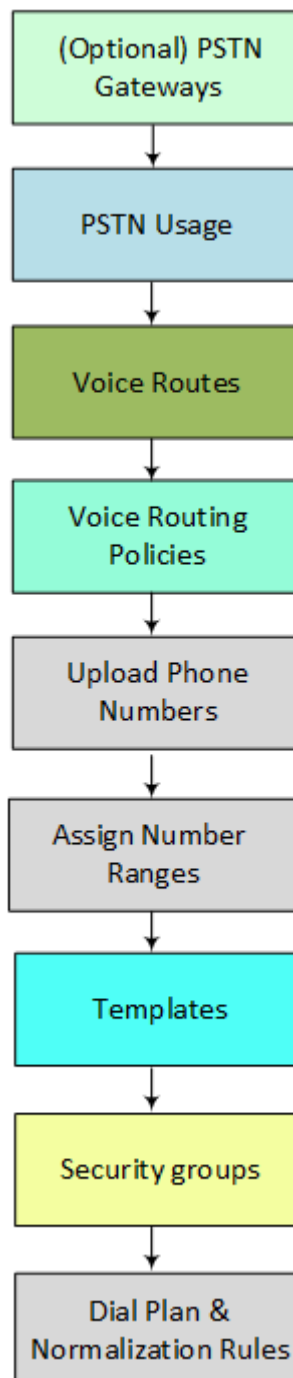
Add New Voice Routing Policy

DataChangeType	Identity	Description	PSTN Usage
	Global		
	Unrestricted		Unrestricted

The figure below illustrates the logical associations between the different Configuration entities.



The following figure outlines the step-by-step provisioning instructions:



- A subset of Teams Calling Policies are available for manual configuration. Provisioning of the full range of policies must be performed using template automation.
- During configuration, refresh the Execution queue (run **Process all**) to synchronize with the Live Cloud database (see [Monitoring M365 Replication Actions Queue](#) on page 508).

■ **PSTN Gateways:** During Onboarding you configured a PSTN Gateway (SBC device) to connect calls with Microsoft 365 using either the service provider's SIP Trunk or IP PBX or the customer SIP Trunk provider (BYOC). This gateway is defined in the User Management

Pack™ 365 SP Edition database. This option lets you configure additional BYOC devices. See [PSTN Gateways](#) on page 501.



The PSTN Gateway table does not display the PSTN gateway configured in the Onboarding; values are only displayed when added manually in Day Two.

- **PSTN Usage:** Mapping of Voice Routes to Voice Routing Policies. In the example below, separate Usages are defined for each site location. Routes and Policies data is filled when configured below. See [PSTN Usage](#) on page 495.

Manage Pstn Usage			
Identity	Routes	Policies	Last Replication
Unrestricted	Unrestricted	Unrestricted	
SiteTwo	Unrestricted,SiteTwoRoute	SiteTwoPolicy	
SiteOne	Unrestricted,SiteOneRoute	SiteOnePolicy	

- **Voice Routes:** Configure PSTN Gateways and PSTN Usage and Dialing patterns. In the example below, both sites are assigned to separate Online PSTN gateways and PSTN usages. See [Voice Route](#) on page 500.

SiteOneRoute	2	^(\+1[0-9][10])\$	SiteOneRoute	SiteOneRoute	BradDRDemo97.sandbox2.audiocodes.be	SiteOne	▼ ▲
SiteTwoRoute	3	^(\+1[0-9][10])\$	SiteTwoRoute	SiteTwoRoute	DRDemoSite2.sandbox2.audiocodes.be	SiteTwo	▼ ▲



It may take a few minutes for data to process. In the meantime, proceed to configure other entities and then return to this screen.

- **Voice Routing Policies:** Configure Voice Routes and PSTN Usage. In the example below, each site is assigned a separate policy with its respective PSTN usage. See [Voice Routing Policy](#) on page 496.

Add New Voice Routing Policy			
DataChangeType	Identity	Description	PSTN Usage
	Global		
	Unrestricted		Unrestricted
	SiteTwoPolicy	SiteTwoPolicy	SiteTwo
	SiteOnePolicy	SiteOnePolicy	SiteOne



It may take a few minutes for data to process. In the meantime, proceed to configure other entities and then return to this screen.

- **Upload Numbers:** Upload numbers to the SBC Dial plan (default CustDialPlan) with the PSTN Gateway tag for the Customer Site Location (see [Manage SBC Prefixes](#) on page 533).
- **Assign Number Ranges:** Define numbers ranges based on the uploaded numbers for automatic configuration to users in the applied templates (see [Managing Unassigned Number Ranges](#) on page 451). You can also assign numbers manually, see [Manually](#)

[Assigning Phone Numbers to Users](#) on page 443. In the example below, one range is defined for Site Location 'Napoli' and another range for Site Location 'Paris'.

<div> <div>Reload All</div> <div>Add/Edit Range</div> <div>Add/Edit Bundle</div> <div>Delete</div> </div>				
Show 10 entries			Search:	
Identity	Start of Number Range	End of Number Range	Available Numbers	Used in
Napoli	+390810902000	+390810902050	37	Napoli
Paris	+33564371500	+33564371550	51	Paris
Showing 1 to 2 of 2 entries				<div>Previous</div> <div>1</div> <div>Next</div>

- **Templates:** Configure templates including Calling Policies and Number ranges (automatic Number assignment). In the examples below, custom Online Voice Routing policies defined above are applied to each respective template. In addition, Enterprise Voice is enabled and the respective number ranges defined above are applied to each template. See [Managing Templates](#) on page 459. A subset of Calling Policies can also be applied manually to the users (see [Manually Applying M365 User Policies](#) on page 446). In the example below, respective templates are defined for Napoli and Paris.

Choose a template :

Napoli

Reload

Create

Clone as

Delete

Submit All Changes

Template Name :

Napoli

Template Id :

1

Registrar Pool :

Office365

Additional Policies

1. Onlinevoiceroutingpolicy Policy:

SiteOnePolicy

del

Enable Enterprise Voice:

☐ Do Not Configure
 ☒ Enable
 ☐ Disable

Clear Line URI:

Assign Number from :

NumberRange

NumberRange :

Napoli

NumberRange details :

From: +390810902000 to +390810902050

Use Extensions :

☐

Number Of Digits :

Choose a template :

Paris

Reload

Create

Clone as

Delete

Submit All Changes

Template Name :

Paris

Template Id :

2

Registrar Pool :

Office365

Additional Policies

1. Onlinevoiceroutingpolicy Policy:

SiteTwoPolicy

del

Enable Enterprise Voice:

☐ Do Not Configure
 ☒ Enable
 ☐ Disable

Clear Line URI:

Assign Number from :

NumberRange

NumberRange :

Paris

NumberRange details :

From: +33564371500 to +33564371550

Use Extensions :

☐

Number Of Digits :

- **Security Groups:** Assign Security Groups to templates; Azure Active Directory Organizational User Groups. In the example below, Site One is assigned to the 'Communications' Group and Site Two is assigned to the 'Design' group. The members for each group are also shown below. See [Binding Templates to Security Groups](#) on page 469. In this example, the SiteOne Napoli Template is assigned to the 'Retail' group and SiteTwo Paris Template is assigned to the SOC Team.

Add

Show 10 entries

Search:

Rank	Replication Template	Security Group	Error
1	Napoli	Retail	
2	Paris	SOC Team	

Showing 1 to 2 of 2 entries
Templates are processed by priority, the lowest rank index has the highest priority.

Previous **1** Next

- **Create Dial Plans and Assign Normalization Rules:** Create M365 Dial plans and assign Normalization rules. See [Microsoft 365 Dial Plan and Normalization Rules](#) on page 501.

Add New Normalization Rule

Name	Description	Pattern	Translation	IsInternalExtension
NapoliRule	Napoli Rule	*390810902(\d{3,})\$	+390810905\$1	false
ParisRule	Paris Rule	*33(564371501\d{3})\$	0\$1	false

Add New Plan

DataChangeType	Identity	Simple Name	Description	External Prefix	Last Replication
	Global	DefaultTenantDialPlan			
New	Napoli	Napoli	Napoli		
New	Paris	Paris	Paris		

The figure below shows the User configuration after templates have been applied:

- Users from the 'Retail' group are assigned with the Napoli template. One user from the SOC team is assigned with the Paris template.
- Online Voice Routing Policy, Online PSTN Gateway and Site Location fields are configured for each site. Note in the example below, only one user is configured for Site Two Paris.
- The Usage Location (configured in Azure) has been manually set to Italy and France (see [Set Usage Location](#) on the next page).
- Phone Numbers (DIDs) are automatically assigned to users according to the defined Number ranges with Napoli and Paris dialing prefixes.

Search Clear Filter

User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voic...	Online PSTN Gate...	Site Location	Us...	Enterprise
TeamsOnly	Pradeep Gupta	sip:pradeep@...	tel:+390810902003	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	IT	Yes
TeamsOnly	MOD Administrator	sip:admin@m3...	tel:+390810902004	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	IT	Yes
TeamsOnly	Alex Wilber	sip:alexw@m3...	tel:+390810902005	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	IT	Yes
TeamsOnly	Ump-Activation-User	sip:ump-activa...							BE	No
TeamsOnly	Ump-Activation-User	sip:ump-activa...							BE	No
TeamsOnly	Grady Archie	sip:gradya@m...	tel:+390810902006	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	US	Yes
TeamsOnly	Ump-Activation-User	sip:ump-activa...							BE	No
TeamsOnly	Ump-Activation-User	sip:ump-activa...							BE	No
TeamsOnly	Christie Cline	sip:christiec@...	tel:+390810902007	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	IT	Yes
TeamsOnly	Joni Sherman	sip:joni@m36...	tel:+390810902008	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	IT	Yes
TeamsOnly	Adele Vance	sip:adelev@m...	tel:+390810902009	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	IT	Yes
TeamsOnly	Miriam Graham	sip:miriamg@...	tel:+390810902010	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	IT	Yes
TeamsOnly	Megan Bowen	sip:meganb@...	tel:+390810902011	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	IT	Yes
TeamsOnly	Lidia Holloway	sip:ldiah@m3...	tel:+390810902012	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	IT	Yes
TeamsOnly	Allan Deyoung	sip:alland@m...	tel:+33564371500	Paris		SiteTwoPolicy	DRDemoSite2.sandbo...	DRDemoSite2	FR	Yes
TeamsOnly	Irvin Sayers	sip:irvins@m3...	tel:+390810902013	Napoli		SiteOnePolicy	BradDRDemo97.sandb...	BradDRDemo97	IT	Yes
TeamsOnly	Ump-Activation-User	sip:ump-activa...							BE	No

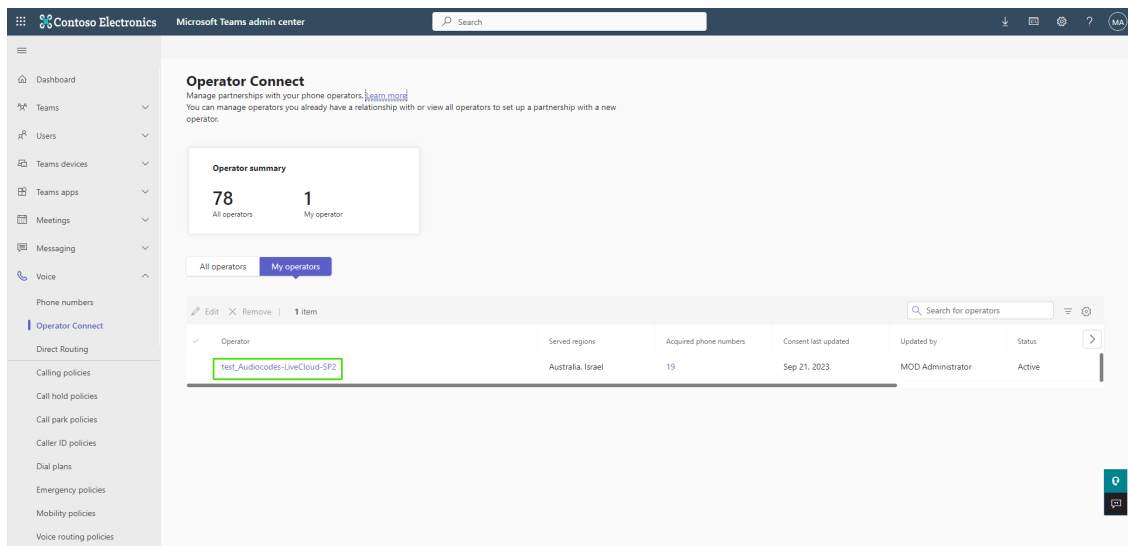
See also [Voice Routing Scenarios](#) on page 442.

Set Usage Location

Before you can add a number to a user, the users usage location must be mapped to the uploaded number country calling prefix.

➤ Do the following:

1. Click the operator. The loaded numbers are displayed. Note the countries for which you have already uploaded numbers.



Operator Connect

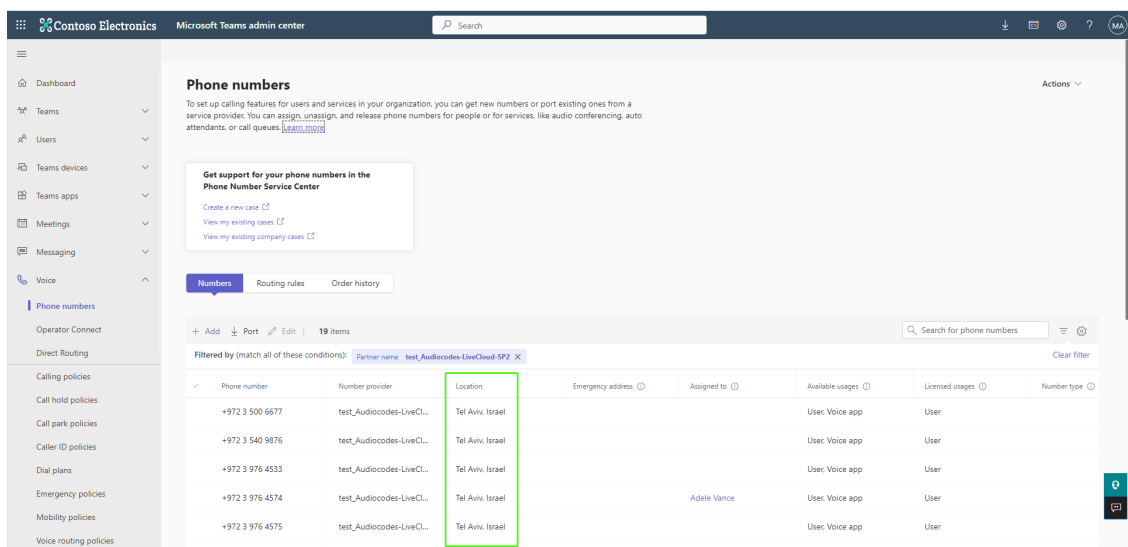
Manage partnerships with your phone operators. [Learn more](#)
You can manage operators you already have a relationship with or view all operators to set up a partnership with a new operator.

Operator summary

78 All operators 1 My operator

All operators My operators

Operator	Served regions	Acquired phone numbers	Consent last updated	Updated by	Status
test_Audiocodes-LiveCloud-SF2	Australia, Israel	19	Sep 21, 2023	MOD Administrator	Active



Phone numbers

To set up calling features for users and services in your organization, you can get new numbers or port existing ones from a service provider. You can [assign](#), [unassign](#), and release phone numbers for people or for services, like audio conferencing, auto attendants, or call queues. [Learn more](#)

Get support for your phone numbers in the Phone Number Service Center

[Create a new case](#) [View my existing cases](#) [View my existing company cases](#)

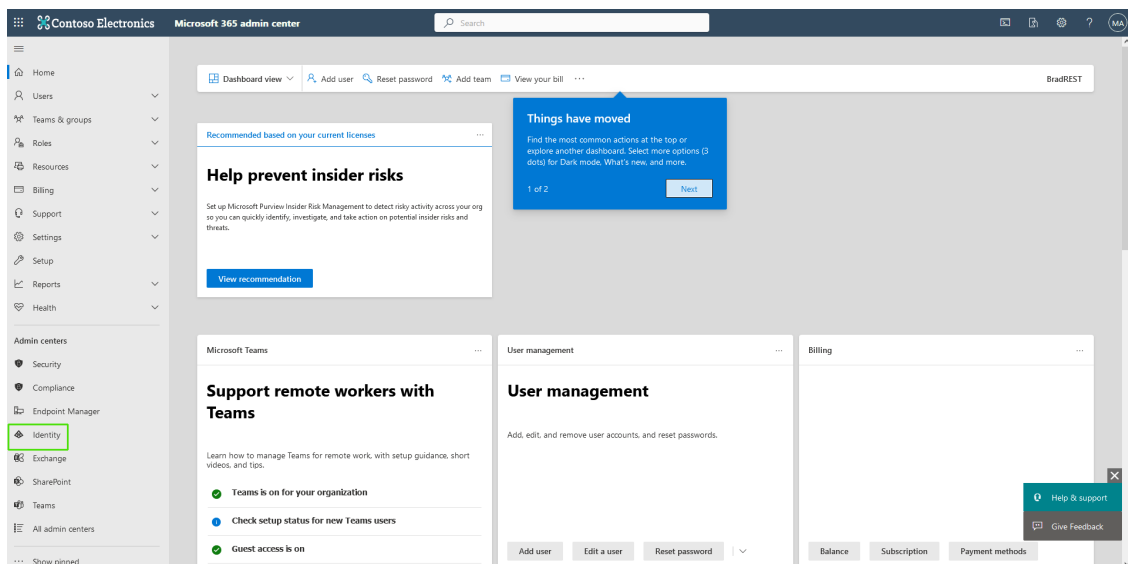
Numbers Routing rules Order history

+ Add Port Edit 19 items

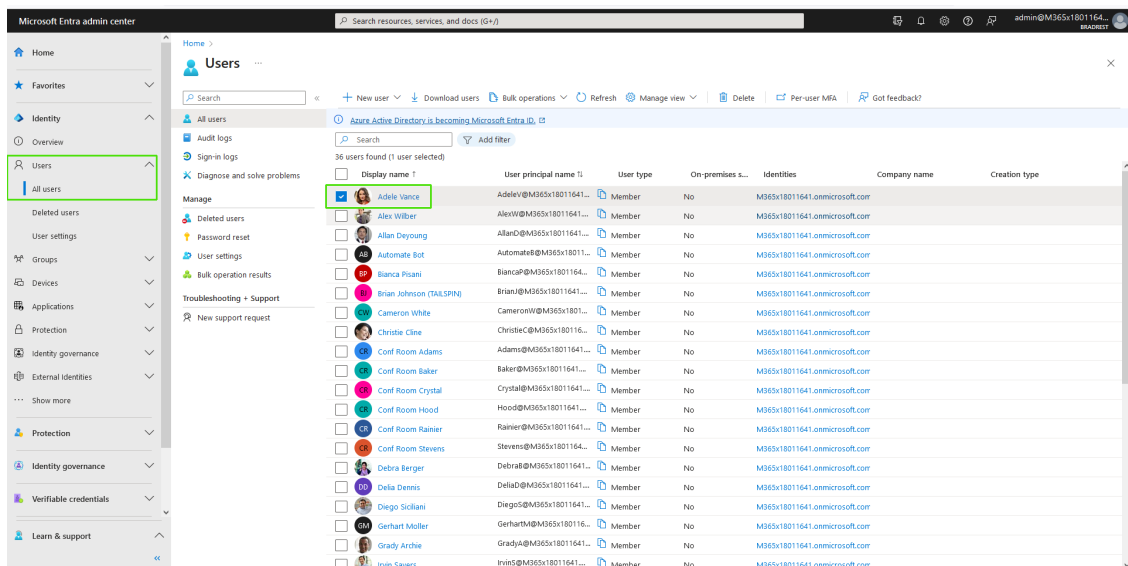
Filtered by (match all of these conditions): [Partner name test_Audiocodes-LiveCloud-SF2](#) [Clear filter](#)

Phone number	Number provider	Location	Emergency address	Assigned to	Available usages	Licensed usages	Number type
+972 3 500 6677	test_Audiocodes-LiveCL...	Tel Aviv, Israel			User: Voice app	User	
+972 3 540 9876	test_Audiocodes-LiveCL...	Tel Aviv, Israel			User: Voice app	User	
+972 3 976 4533	test_Audiocodes-LiveCL...	Tel Aviv, Israel			User: Voice app	User	
+972 3 976 4574	test_Audiocodes-LiveCL...	Tel Aviv, Israel		Adele Vance	User: Voice app	User	
+972 3 976 4575	test_Audiocodes-LiveCL...	Tel Aviv, Israel			User: Voice app	User	

2. Login to the Microsoft Entra admin center and navigate to **Identity**.



3. Select **Users** > **All users** and then select a specific user.



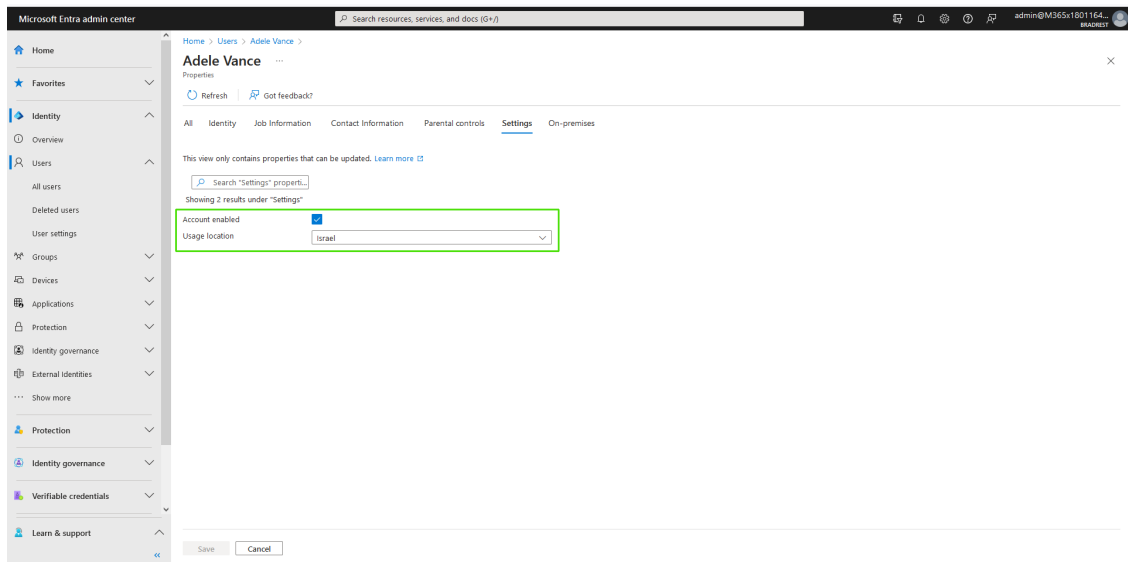
4. Select **Properties**.

The screenshot shows the Microsoft Entra admin center interface. On the left is a navigation pane with categories like Identity, Users, Groups, Devices, Applications, Protection, and Governance. The main area displays the user profile for 'Adele Vance'. The 'Properties' tab is highlighted with a green box. The profile includes a search bar, action buttons (Edit properties, Delete, Refresh, Reset password, Revoke sessions, Manage view, Got feedback?), and sections for Basic info, My Feed, and Quick actions.

5. Select Settings.

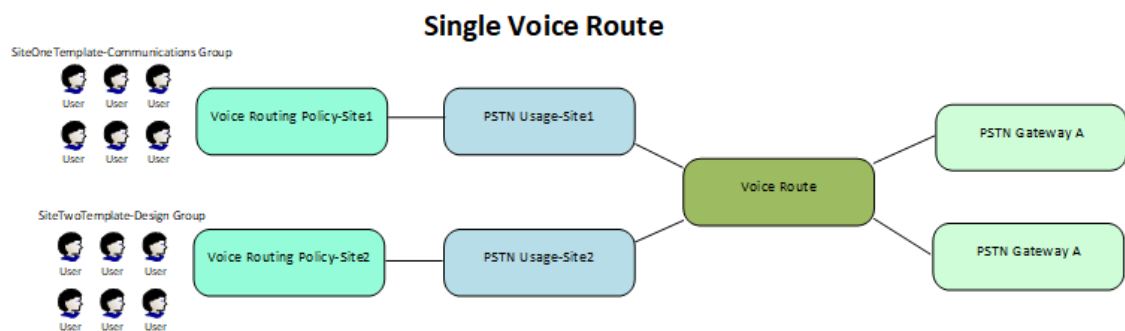
This screenshot shows the 'Properties' tab of the user profile for 'Adele Vance'. The 'Settings' link under the 'Parental controls' section is highlighted with a green box. The page is divided into two main columns: 'Identity' and 'Contact Information'. The 'Identity' column contains fields like Display name, First name, Last name, User principal name, Object ID, User type, Creation type, Created date time, Last password change date time, Invitation state, External user state change date, Assigned licenses, Password policies, Password profile, Preferred language, Sign in sessions valid from date, and Authorization info. The 'Contact Information' column contains fields like Street address, City, State or province, ZIP or postal code, Country or region, Business phone, Mobile phone, Email, Other emails, Proxy addresses, Fax number, IM addresses, Mail nickname, Parental controls, Age group, Consent provided for minor, Legal age group classification, Account enabled, Usage location, Preferred data location, and On-premises.

6. In the Usage Location drop-down, set to the country for which you wish to assign the number.

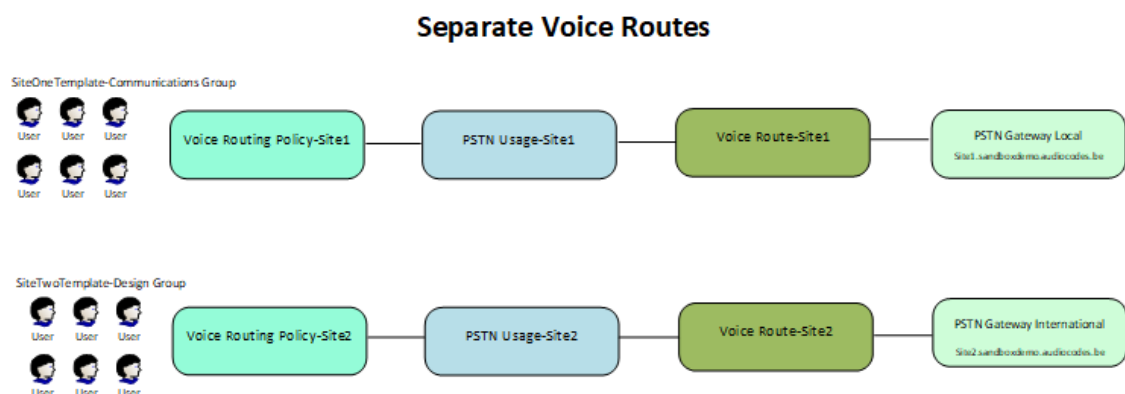


Voice Routing Scenarios

The scenario shown below illustrates both sites using the same Voice Route and PSTN Gateway (SBC device).



The scenario shown below illustrates both sites using separate Voice Routes and SBC devices.



Manually Provisioning Users

You can manually provision users with phone numbers and a subset of Calling policies. For provisioning the full set of available Teams Calling Policies, users must be provisioned through template automation.

■ [Manually Assigning Phone Numbers to Users](#) below

■ [Manually Applying M365 User Policies](#) on page 446



- Each user enabled with Enterprise Voice requires the appropriate Microsoft Phone System license (see [Microsoft Phone System Service Plan](#)).
- All assigned numbers must be configured in the relevant site location dial plan, see [Manage SBC Prefixes](#) on page 533.

Manually Assigning Phone Numbers to Users

You can manually assign phone numbers that you do not wish to be automatically assigned. Using this option, you can assign a Voice Routing Policy to the phone number. Once added, the user is assigned to a PSTN Gateway and Site Location according to the Voice Routing Policy. In this example, the user is assigned the default 'Unrestricted' policy which is associated with a PSTN Gateway sub domain configured with Automatic DNS provisioning in the customer onboarding.

Dial Plans Normalization Rule Templates PSTN Gateways PSTN Usage Voice Routes Voice Routing Policies								
Add New Voice Route								
DataC...	Identity	Prf...	Pattern	Name	Description	PSTN Gateway List	PSTN Usage	
	Unrestricted	0	*	Unrestricted		BradDRService.sandbox2.audiocodes.be	Unrestricted	▼ ▲



Hosted Essentials + and Hosted Pro customers can also assign numbers in the Line URI field in the User details (see [Manually Applying M365 User Policies](#) on page 446). Hosted Essentials customers can only assign numbers using this option.

➤ To assign a phone number:

1. In the Customer portal Users view page, select a user, right-click and choose **Assign Phone Number**.

TeamsOnly	Isalah Langer	sip:isalahl@m...	tel:+97235609010	TestTemplate3				US	Ye
TeamsOnly	Irvin Sayers	sip:irvins@m3...						US	Ye
TeamsOnly	Johanna Lorenz	sip:johanna@m...	tel:+97235609011					US	Ye
TeamsOnly	Miriam Graham	@...	tel:+97235609012	TestTemplate3				US	Ye

Assign phone to subscriber

Enter phone details without 'tel:+' (or leave empty)
to (un)assign to sip:johannal@m365x62192331.onmicrosoft.com:

Telephone Number


tel:+97235609011

☒ EnterpriseVoiceEnabled

OnlineVoiceRouting Policy

- Don't change the actual value -

- Don't change the actual value -
Global
Unrestricted

 Enterprise Voice check box is enabled automatically when you start typing the number digits.

- Start typing to enter the phone number that you wish to assign to the user, notice that tel:+ is added to the string, and then click **OK**.

Phone number format – **tel:xxxxxxxx**

The valid syntax rules are displayed in the dialog below.

Assign phone to subscriber

tel:++97 - Valid values:
The number must match the regular expression (tel:+)?([1-9]d{0,17})(;ext=[1-9]d{0,9})
'tel:+' is automatically added to the phonenumber. This means the number should begin with a digit 1 through 9.
The phone number can be up to 17 digits. The extension is optional.

- Configure the OnlineVoiceRouting Policy and click **OK**:
 - Unrestricted (default)
 - Global
 - Custom
- In the Users page, select the user.

User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voic...	Online PST...	Site Location	Usage Loc...	Enterprise...
TeamsOnly	Nestor Wilke	sip:nestorw@...	tel:+97235609...						US	Yes
TeamsOnly	Joni Sherman	sip:jonis@m36...	tel:+97235609...	TestTemplate3		Unrestricted	BradDRService...	BradDRService...	US	Yes
TeamsOnly	Lynne Robbins	sip:lynnr@m...	tel:+97235609...			Unrestricted	BradDRService...	BradDRService...	US	Yes
TeamsOnly	Christie Cline	sip:christiec@...	tel:+97235609...			Unrestricted	BradDRService...	BradDRService...	US	Yes
TeamsOnly	Alex Wilber	sip:alexw@m3...	tel:+97235609...			Unrestricted	BradDRService...	BradDRService...	US	Yes
TeamsOnly	Adele Vance	sip:adelev@m...	tel:+97235609...			Unrestricted	BradDRService...	BradDRService...	US	Yes
TeamsOnly	Grady Archie	sip:gradya@m...	tel:+97235609...						US	Yes
TeamsOnly	Ump-Activation-User	sip:ump-activa...							BE	No
TeamsOnly	Patti Fernandez	sip:pattif@m3...	tel:+97235609...	TestTemplate3		Unrestricted	BradDRService...	BradDRService...	US	Yes
TeamsOnly	Ump-Activation-User	sip:ump-activa...							BE	No
TeamsOnly	Isalah Langer	sip:isalahl@m...	tel:+97235609...	TestTemplate3					US	Yes
TeamsOnly	Irvin Sayers	sip:irvins@m3...							US	Yes
TeamsOnly	Johanna Lorenz	sip:johanna@...	tel:+97235609...			Unrestricted	BradDRService...	BradDRService...	US	Yes

Note that the user has been configured with the following:

- Online Voice Routing Policy 'Unrestricted'
- Online PSTN Gateway
- Site Location



A dedicated PSTN Gateway is not required on the customer tenant; the customer is assigned the **Derived Trunk FQDN** of the Service Provider SBC device. Unless the customer is using their own SIP Trunk provider (BYOC).

5. Right-click the user and choose **Edit**.

Edit sip:johanna@m365x62192331.onmicrosoft.com

General Pending changes Audit

Display name: Johanna Lorenz

First name: Johanna

Last name: Lorenz

SIP address: sip:johanna@m365x62192331.onmicrosoft.com

Manager:

Interpreted user type: PureOnlineTeamsOnlyUser

Location: EnterpriseVoice Enabled ☒

Policies: Tms.SBA.Policy:

Telephony: Select Number range: select number range

Teams: Online Voiceroouting Policy: Unrestricted

Tenant Dialplan: <Automatic>

Line URI: tel:+97235609011

Available nr(s):

Update Cancel

Note the highlighted configuration in the figure above:

- PureOnlineTeamsOnlyUser (configured by default).
- Enterprise Voice Enabled
- Online Voice Routing Policy
- Line URI

6. (Optional): You can optionally view the synchronized configuration for the customer tenant in their Teams admin center:

- Open the Teams Admin Center (<https://admin.teams.microsoft.com/users>):

- b. In the Navigation pane, select **Manage users**.
- c. Select the relevant user.
- d. Verify that the following policies are synchronized for the user:
 - Calling policy **Allow Calling** (Operator Connect Only)
 - Voice Routing Policy **Unrestricted**

The screenshot shows the Microsoft Teams admin center interface. On the left, the 'Users' section is expanded, and 'Manage users' is selected. The main area displays a table of policies for user Alex Wilber. The 'Calling policy' is set to 'AllowCalling' and the 'Voice routing policy' is set to 'Unrestricted'. A right-hand pane titled 'Edit policy assignment' for Alex Wilber shows the same settings.

- e. Under the **Account** tab, view the Coexistence mode is set to **Teams only**.

The screenshot shows the 'Account' tab for user Alex Wilber. The 'General information' section shows the user's profile. The 'Audio Conferencing' section shows settings for audio conferencing. The 'Teams upgrade settings' section shows the 'Coexistence mode' set to 'Teams only'. The 'Avatar profile' section shows no avatar profiles found.

Manually Applying M365 User Policies

M365 Teams Calling policies can be applied to users. A subset of these policies can be applied in the Users page. Applying the full list of policies must be done using templates and then assigning these templates to Security Groups including the managed users (see [Managing Templates](#) on page 459).

➤ **To edit user policies:**

1. In the Customer portal Users page, select a user and right-click **Edit** to edit User policies.

The screenshot shows the 'Users' page in the Customer portal. A table lists users with columns: User Ty, Full Name, SIP Add, Line Un, Templ, Depart, Online, Site Loc, Usage, and Enterpri. The 'auto4 user' row is selected, and a right-click context menu is displayed with options: Edit, Assign Phone Number, and Grant Admin.


The screenshot shows the 'Users' page in the Customer portal. A table lists users with columns: User Type, Full Name, SIP Address, Line Un, Template, Department, Online Voic, Online PST, Site Location, Usage Loc, and Enterprise. The 'Christie Cline' row is selected, and a right-click context menu is displayed with options: Edit and Assign Phone Number.

The following figure shows an example user policy.

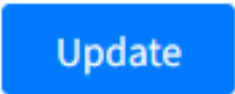
The screenshot shows the user policy configuration page for 'Christie Cline'. The page has three tabs: General, Pending changes, and Audit. The 'General' tab is active, showing fields for Display name, First name, Last name, SIP address, Manager, and Interpreted user type. The 'Location' tab shows fields for City, Department, Postal code, Street address, Company, Office, State or Province, and Usage location. The 'Policies' tab is also visible.

Parameter	Description
Display Name	Display Name in Microsoft 365 and Customer portal.
First Name	First Name of M365 user.

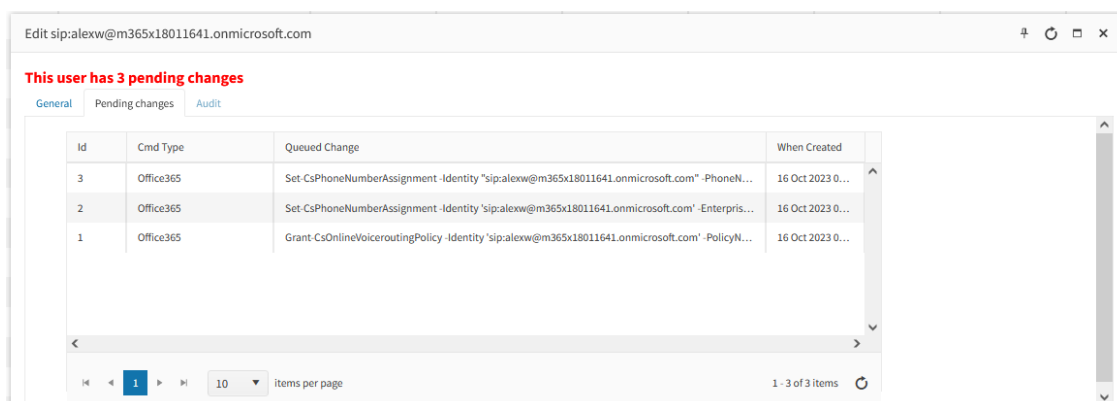
Parameter	Description
Last Name	Surname of M365 user.
SIP address	SIP URL of M365 user.
Manager	Manager in charge of M365 user
Interpreted User Type	Teams Only
DirSync Enabled	Directory Sync Enabled
Location	
City	City of user location.
Department	Active Directory department of user.
Postal Code	Postal Code
Street Address	Street address of the user work location.
Company	Name of the user's employment enterprise.
Office	Office address
State or Province	State or Province (relevant for countries with states or provinces).
Usage location	Country for which Enterprise calling is enabled.
Policies	
Broadcast Meeting Policy	Broadcast meeting policy govern broadcast-specific functionality. In addition, the settings of the conferencing policy assigned to the user producing the broadcast also general conferencing settings that are also relevant for broadcast meetings.
Client Policy	Client policies are used by Skype for Business Server to manage the client-related settings that are managed by the administrators. For example, if Skype for Business automatically saves transcripts of instant messaging sessions.
Conferencing Policy	Conferencing policy determines the features and capabilities that can be used in a conference as well as in a broadcast meeting; this includes everything from whether or not the conference can include IP audio and video to the maximum number of people who can attend a meeting.

Parameter	Description
Mobility Policy	Mobility policies determine whether or not a user can use Skype for Business Mobile. These policies include the ability to make and receive phone calls on mobile phone by using their work phone number instead of their mobile phone number.
External Access Policy	<p>External access policies determine whether or not users can do the following:</p> <ul style="list-style-type: none"> Communicate with users with Session Initiation Protocol (SIP) accounts with a federated organization Communicate with users who are using custom applications built with Azure Communication Services (ACS) Access Skype for Business Server over the Internet, without having to log on to your internal network. Communicate with users who have SIP accounts with a public instant messaging (IM) provider such as Skype.
Telephony	
Enterprisevoice Enabled	Enables users to make and receive calls.
Tms.SBA.Policy	Assign Teams Branch Survivability policy to user.
Select Numberrange	Enables configuration of number ranges.
Online Voicerouting Policy	Applies Online Voice Routing policy. Default "Unrestricted" created by the Onboarding script.
Tenant Dialplan	Numbers added are automatically applied to the tenant dialplan.
Line URI	<p>User assigned phone number.</p> <div>  <p>This configuration can also be performed using the Assign Phone Number right-click option (see Manually Assigning Phone Numbers to Users on page 443); for Hosted Essentials customers, numbers can only be assigned using this right-click option.</p> </div>
Available nr (s)	
Teams	
Tms. Calling Policy	Teams Calling Policy controls which calling and call forwarding features are available to users in Microsoft Teams.

Parameter	Description
Tms. Messaging Policy	Teams Messaging policies control which chat and channel messaging features are available to users (owners and members) in Microsoft Teams.
Tms.Vid.Int.serv.Pol	
Tms. Meeting Policy	Teams Meeting Policy enables administrators to control the type of meetings that users can create or the features that they can access while in a meeting.
Tms. Upgrade Policy	

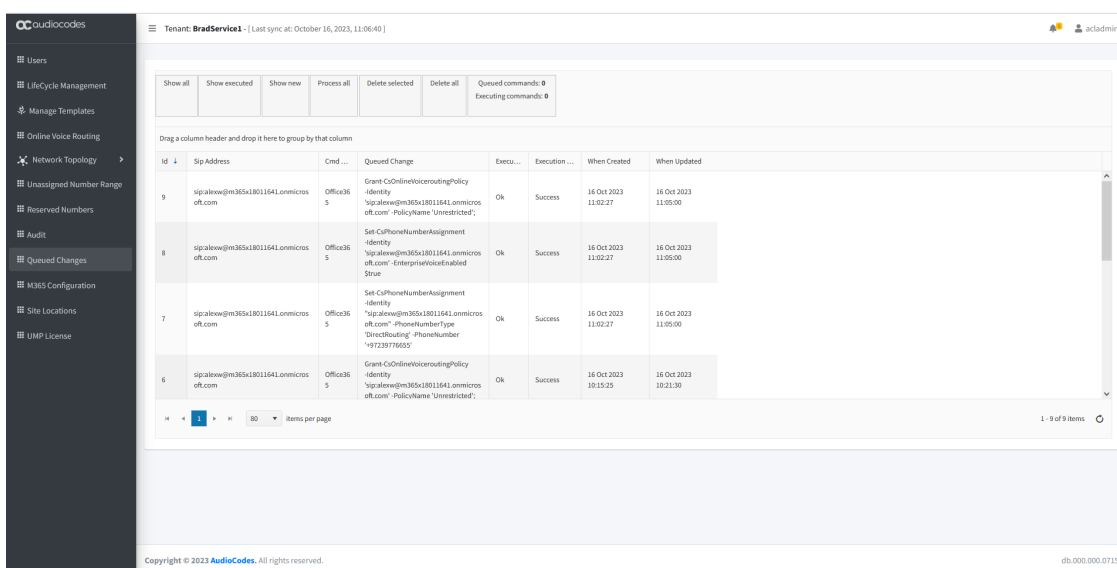


- Perform the required modifications and then click **Update**.
- Select the **Pending changes** tab. Updates are displayed.



Id	Cmd Type	Queued Change	When Created
3	Office365	Set-CsPhoneNumberAssignment -Identity "sip:alexw@m365x18011641.onmicrosoft.com" -PhoneN...	16 Oct 2023 0...
2	Office365	Set-CsPhoneNumberAssignment -Identity "sip:alexw@m365x18011641.onmicrosoft.com" -Enterpris...	16 Oct 2023 0...
1	Office365	Grant-CsOnlineVoicerooutingPolicy -Identity "sip:alexw@m365x18011641.onmicrosoft.com" -PolicyN...	16 Oct 2023 0...

- In the Navigation pane, select **Queued Changes**. View the above changes in the Synchronization queue.



Id	Sip Address	Cmd ...	Queued Change	Execu...	Execution ...	When Created	When Updated
9	sip:alexw@m365x18011641.onmicros...	Office365	Grant-CsOnlineVoicerooutingPolicy -Identity "sip:alexw@m365x18011641.onmicros...	Ok	Success	16 Oct 2023 11:02:27	16 Oct 2023 11:05:00
8	sip:alexw@m365x18011641.onmicros...	Office365	Set-CsPhoneNumberAssignment -Identity "sip:alexw@m365x18011641.onmicros...	Ok	Success	16 Oct 2023 11:02:27	16 Oct 2023 11:05:00
7	sip:alexw@m365x18011641.onmicros...	Office365	Set-CsPhoneNumberAssignment -Identity "sip:alexw@m365x18011641.onmicros...	Ok	Success	16 Oct 2023 11:02:27	16 Oct 2023 11:05:00
6	sip:alexw@m365x18011641.onmicros...	Office365	Grant-CsOnlineVoicerooutingPolicy -Identity "sip:alexw@m365x18011641.onmicros...	Ok	Success	16 Oct 2023 10:15:25	16 Oct 2023 10:21:30

5. Return to the Users screen, notice that the User has been updated.

The screenshot shows the 'Users' screen in the AudioCodes UMP-365 interface. The left sidebar contains navigation options: Users, Lifecycle Management, Manage Templates, Online Voice Routing, Network Topology, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, Site Locations, and UMP License. The main area displays a table of users for Tenant: BradService1. The table has columns: User Type, Full Name, SIP Address, Line UI, Template, Department, Online Voice R..., Online PSTN G..., Site Location, Usage Location, and EnterpriseVoic... The first user, Alex Wilber, is highlighted with a green border. Below the table, there is a pagination bar showing '1 - 20 of 20 Items'.

User Type	Full Name	SIP Address	Line UI	Template	Department	Online Voice R...	Online PSTN G...	Site Location	Usage Location	EnterpriseVoic...
TeamsOnly	Alex Wilber	sipalexw@m365...	tel-197239776655		Marketing	Unrestricted			NL	Yes
TeamsOnly	Christie Cline	sipchristiec@m3...			Sales				NL	No
TeamsOnly	Nestor Wilke	sipnestorw@m36...			Operations				NL	No
TeamsOnly	Ump-Activation User	sipump-activatio...							BE	No
TeamsOnly	Patti Fernandez	sippatti@m365...			Executive Manage...				NL	No
TeamsOnly	Joni Sherman	sipjonis@m365...			Legal				NL	No
TeamsOnly	Miriam Graham	sipmiriam@m3...			Sales & Marketing				NL	No
TeamsOnly	Irvin Sayers	sipirvins@m365...			R&D				NL	No
TeamsOnly	Pradeep Gupta	sippradeep@m...			Finance				NL	No
TeamsOnly	Lidia Holloway	siplidiah@m365...			Engineering				NL	No
TeamsOnly	Lee Gu	sipleegu@m365...			Manufacturing				NL	No
TeamsOnly	Grady Archie	sipgrady@m365...			R&D				NL	No
TeamsOnly	Isiah Langer	sipisiah@m365...			Sales				NL	No
TeamsOnly	MDO Administrator	sipadmin@m365...							NL	No
TeamsOnly	Lynne Robbins	siplynner@m365...			Retail				NL	No
TeamsOnly	Adelle Vance	sipadelle@m365...	tel-197239764574		Retail				IL	Yes
TeamsOnly	Debra Berger	sipdebrab@m36...			Executive Manage...				NL	No

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 the following three components. It is critical to configure the components in the ordershown below 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 (see [Managing Unassigned Number Ranges](#) below).
2. Configure templates, holding policies and telephony settings (see [Managing Templates](#) on page 459).
3. Configure Lifecycle management and bind templates to security groups (see [Binding Templates to Security Groups](#) on page 469).

Managing Unassigned Number Ranges

The Unassigned Number Range allows an operator administrator to define ranges with numbers that belong to their Customer tenant. Unassigned Number Ranges are used in Lifecycle Management to automatically assign telephone numbers to M365 tenant users upon creation of the tenant in the Onboarding process. You can configure a range of phone numbers to be automatically assigned to new users. For example, new employees start working at a

specific location and once connected to the network are automatically assigned a phone number.



Unlike policies (or Phone) is not enforced / or changed during the lifecycle scheduled policy replication.

➤ **Do the following:**

1. In the Customer portal Navigation pane, select **Unassigned Number Range**.

Identity	Start of Number Range	End of Number Range	Available Numbers	Used in
newRange	1000	1999	1000	
newRange1	1000	1100	101	
newRange2	1099	1200	102	
Test (newRange)			1000	

A dialog appears from where you can provide a number range name as well as set a limit of for the desired phone numbers.

Add/Edit Range

2. Click **Add/Edit Range** to add a new number range.

Add new range

Please enter the requested data

Identity
New Branch

NumberRangeStart
2000

NumberRangeEnd
2200

OK Cancel

3. Select the Identity Name and the Number Range.
4. Click **OK**.

The new number range is displayed.

Identity	Start of Number Range	End of Number Range	Available Numbers	Used In
New Branch	2000	2200	201	
newRange	1000	1999	1000	
newRange1	1000	1100	101	
newRange2	1099	1200	102	
Test (newRange)			1000	

Showing 1 to 5 of 5 entries 1 row selected

Previous 1 Next

tel:+2000 tel:+2001 tel:+2002 tel:+2003 tel:+2004 tel:+2005 tel:+2006 tel:+2007 tel:+2008 tel:+2009 tel:+2010
tel:+2011 tel:+2012 tel:+2013 tel:+2014 tel:+2015 tel:+2016 tel:+2017 tel:+2018 tel:+2019 tel:+2020 tel:+2021
tel:+2022 tel:+2023 tel:+2024 tel:+2025 tel:+2026 tel:+2027 tel:+2028 tel:+2029 tel:+2030 tel:+2031 tel:+2032
tel:+2033 tel:+2034 tel:+2035 tel:+2036 tel:+2037 tel:+2038 tel:+2039 tel:+2040 tel:+2041 tel:+2042 tel:+2043
tel:+2044 tel:+2045 tel:+2046 tel:+2047 tel:+2048 tel:+2049 tel:+2050 tel:+2051 tel:+2052 tel:+2053 tel:+2054

5. Select the new entry to view all available extensions in the range.
6. Right-click an extension, and then enter name of a M365 user to assign the phone extension.

Assign subscriber to phone [X]

Enter online subscriber to assign to tel:+2000:

Subscriber to assign

OK Cancel

Assign subscriber to phone [X]

Enter online subscriber to assign to tel:+2000:

Subscriber to assign

OK Cancel

7. Once you have assigned the number, go to the Users page to view the assignment of the number (see [Manually Provisioning Users](#) on page 443).

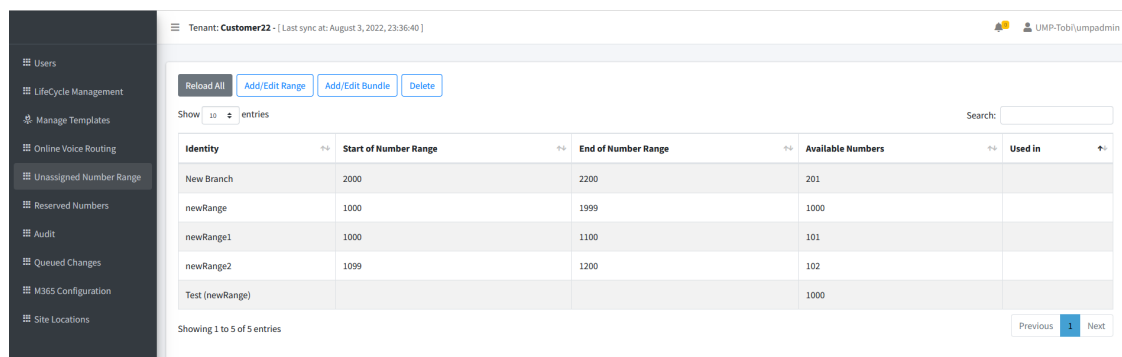
Creating a Bundle

A bundle is a collection of one or more number ranges that are defined in [Managing Unassigned Number Ranges](#) on page 451.

➤ To create a bundle:

Add/Edit Bundle

1. Click



The screenshot shows the UMP-365 interface with the 'Add/Edit Bundle' button highlighted in the top navigation bar. The main content area displays a table of number ranges.

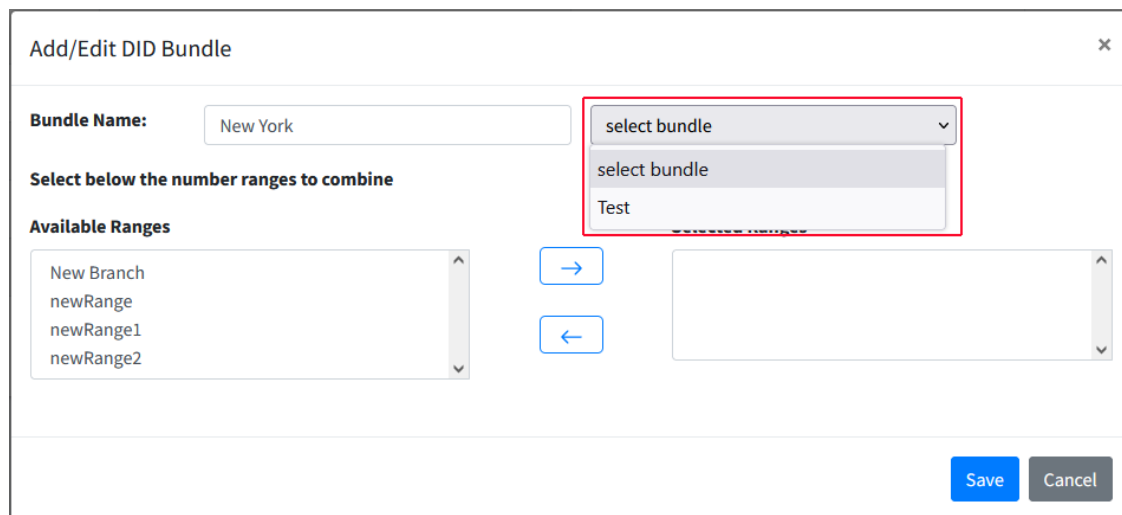
Identity	Start of Number Range	End of Number Range	Available Numbers	Used in
New Branch	2000	2200	201	
newRange	1000	1999	1000	
newRange1	1000	1100	101	
newRange2	1099	1200	102	
Test (newRange)			1000	

Showing 1 to 5 of 5 entries

A new popup window open, enter the Bundle Name.




If you want the new NumberRanges to be part of a previously created bundle, select the desired bundle from the drop-down list.



The screenshot shows the 'Add/Edit DID Bundle' popup window. It includes a 'Bundle Name' field with the value 'New York'. Below it, there is a section titled 'Select below the number ranges to combine' with an 'Available Ranges' list containing 'New Branch', 'newRange', 'newRange1', and 'newRange2'. A dropdown menu is open, showing 'select bundle' and 'Test'. At the bottom, there are 'Save' and 'Cancel' buttons.

Number ranges are displayed in the lower left in Available Ranges pane. Select the desired

number range (only one range can be selected at the same time) then click the  to move it to the Selected Ranges pane.

Add/Edit DID Bundle

Bundle Name:

New York

select bundle

Select below the number ranges to combine

Available Ranges

newRange

newRange2

→

←

Selected Ranges


New Branch

newRange1

Save

Cancel

Save

- Click . The Unassigned Number Ranges page opens displaying the newly created bundle. In the example below, the Bundle name "New York" includes the "New Branch" and "newRange" number ranges. The "Available Numbers" column indicates the sum of the total available numbers for the two number ranges defined in the bundle.

Tenant: **Customer22** - [Last sync at: August 3, 2022, 23:36:40]

UMP-Tobi/umpadmin

Users

LifeCycle Management

Manage Templates

Online Voice Routing

Unassigned Number Range

Reserved Numbers

Audit

Queued Changes

M365 Configuration

Site Locations

Reload All

Add/Edit Range

Add/Edit Bundle

Delete

Show 10 entries

Search:

Identity	Start of Number Range	End of Number Range	Available Numbers	Used in
New Branch	2000	2200	201	
New York (New Branch,newRange)			1201	
newRange	1000	1999	1000	
newRange1	1000	1100	101	
newRange2	1099	1200	102	
Test (newRange)			1000	

Showing 1 to 6 of 6 entries 1 row selected

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

tel:+1025

tel:+1026

tel:+1027

tel:+1028

tel:+1029

tel:+1030

tel:+1031

tel:+1032

tel:+1033

tel:+1034

tel:+1035

tel:+1036

tel:+1037

tel:+1038

tel:+1039

tel:+1040

tel:+1041

tel:+1042

tel:+1043

tel:+1044

tel:+1045

tel:+1046

tel:+1047

tel:+1048

tel:+1049



It is possible for one or more phone numbers to be part of more than one number range in the bundle. For example, if the first phone in Number Range B starts with the last phone number defined in Number Range A. The bundle to which the two number ranges are assigned treats 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 of the number ranges even though the same phone number is common to both of the ranges (see example in the following figure).

Add Reload Add/Edit Bundle

Show 10 entries Search:

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
Reload Previous 1 Next

[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](#)
[tel:+1120](#) [tel:+1121](#) [tel:+1122](#) [tel:+1123](#)

Editing a Bundle

Editing a bundle allows you to add another number range, remove the number range from the bundle or change the name of the bundle.

➤ To edit a bundle:

1. In the table on the **Unassigned Number Ranges** page, select the desired bundle, right-click and then choose **Edit**.

Add/Edit DID Bundle

Bundle Name: New York New York

Select below the number ranges to combine

Available Ranges
newRange1
newRange2

Selected Ranges
New Branch
newRange

Save Cancel

Save

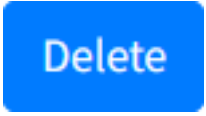
2. Modify the ranges as required and then click **Save**.

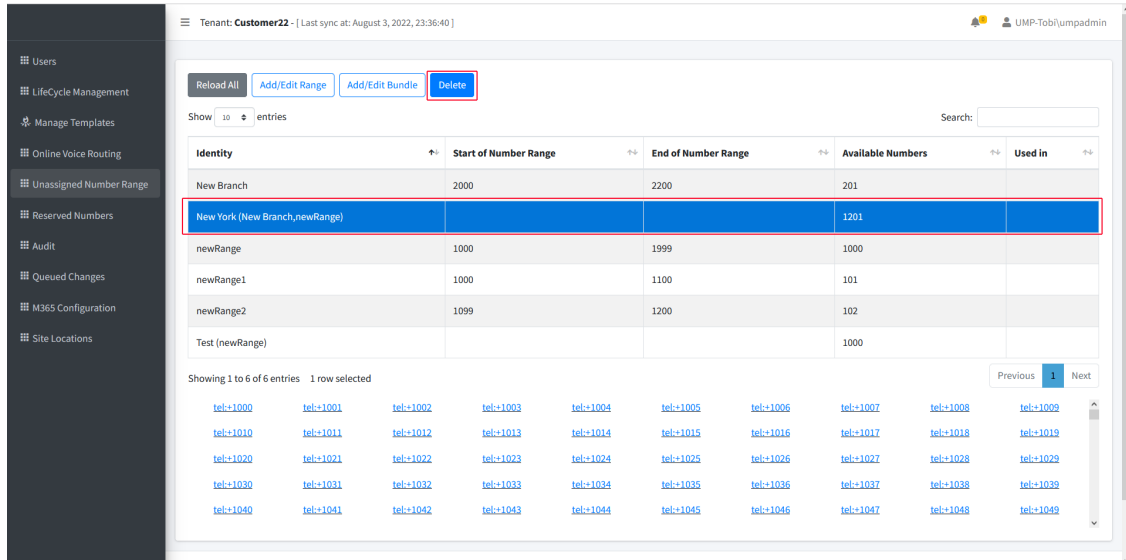
Deleting a Bundle

This section describes how to delete a bundle.

➤ **To delete a bundle:**

1. On the **Unassigned Number Ranges** page select the desired bundle, right-click and then

choose .



Tenant: **Customer22** - [Last sync at: August 3, 2022, 23:36:40]

Reload All Add/Edit Range Add/Edit Bundle **Delete**

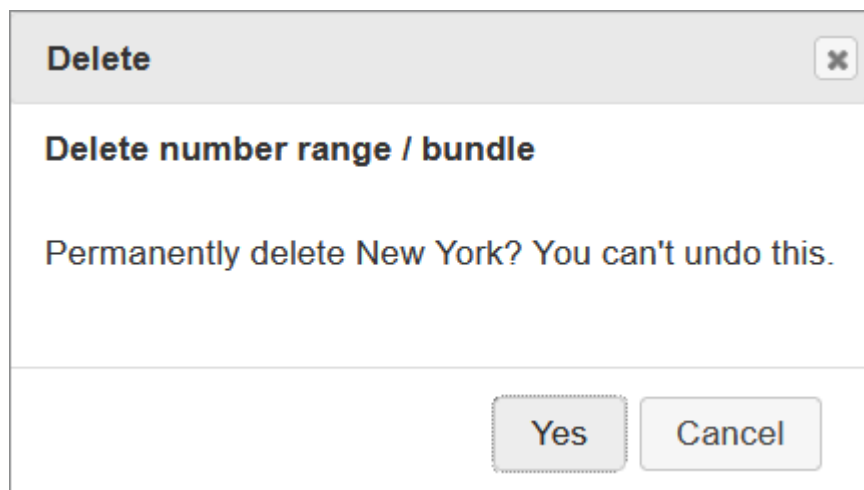
Show 10 entries Search:

Identity	Start of Number Range	End of Number Range	Available Numbers	Used in
New Branch	2000	2200	201	
New York (New Branch,newRange)			1201	
newRange	1000	1999	1000	
newRange1	1000	1100	101	
newRange2	1099	1200	102	
Test (newRange)			1000	

Showing 1 to 6 of 6 entries 1 row selected

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 tel:+1025 tel:+1026 tel:+1027 tel:+1028 tel:+1029
tel:+1030 tel:+1031 tel:+1032 tel:+1033 tel:+1034 tel:+1035 tel:+1036 tel:+1037 tel:+1038 tel:+1039
tel:+1040 tel:+1041 tel:+1042 tel:+1043 tel:+1044 tel:+1045 tel:+1046 tel:+1047 tel:+1048 tel:+1049



Delete

Delete number range / bundle

Permanently delete New York? You can't undo this.

Yes Cancel

2. Click **Yes** to confirm deletion.

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 UnassignedNumberRanges page next to the bundle and the number ranges in UsedIn column.

Add Reload Add/Edit Bundle

Show 10 entries Search:

Identity	NumberRangeStart	NumberRangeEnd	NumbersAvailable	Used in
MsPhoneSystem(EMEA-NL-ALL-FL_AL)			11	
Bundle One (Range1,Range2)			203	Template T1
Range1	1000	1100	101	Template T1
Range2	1099	1200	102	Template T1

Showing 1 to 4 of 4 entries

Reload Previous 1 Next

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.

Tenant: Zagotinous Kirilis - [Last sync at] localhost says
This bundle is in use: Template T1
Deletion denied. OK

WIN-05B27UQKV7K\Administrator

Add Reload Add/Edit Bundle

Show 10 entries Search:

Identity	NumberRangeStart	NumberRangeEnd	NumbersAvailable	Used in
MsPhoneSystem(EMEA-NL-ALL-FL_AL)			11	
Bundle One (Range1,Range2)			203	Template T1
Range1		1100	101	Template T1
Range2	1099	1200	102	Template T1

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

To resolve this issue, firstly its necessary to delete the template which 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:

1. In the Multitenant portal Navigation pane, select **Manage Templates**.
2. From the Choose a template drop-down, select the template to delete and confirm.
3. Click **Delete**.

Choose a template: Test Reload Create Clone as Delete Submit All Changes

Template Name: Test

Template Id: 1

Registrar Pool: Office365

Additional Policies: Add Policy

Enable Enterprise Voice: ☒ Do Not Configure ☐ Enable ☐ Disable

Delete confirmation

Delete template

Permanently delete template Test? You can't undo this.

Yes Cancel



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 adjacent to the bundle or number ranges in the table UnassignedNumberRange page.

[Add](#)
[Reload](#)
[Add/Edit Bundle](#)

Show entries Search:

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
[Reload](#)
[Previous](#)
[1](#)
[Next](#)

Managing Templates

Templates are created to automate policies and number assignment for users and can be assigned to Azure AD security groups in LifeCycle management.

➤ To manage templates:

1. In the Customer portal Navigation pane, select **Manage Templates**.

Tenant: **Customer22** | Last sync at: July 20, 2022, 15:33:59

UMP-Tobi\umpadmin

- Users
- LifeCycle Management
- Manage Templates**
- Online Voice Routing
- Unassigned Number Range
- Reserved Numbers
- Audit
- Queued Changes
- M365 Configuration
- Site Locations

Choose a template: BG clone [Reload](#) [Create](#) [Clone as](#) [Delete](#) [Submit All Changes](#)

Template Name: BG clone

Template Id: 3

Registrar Pool:
Office365

Additional Policies
Teamsapppermission [Add Policy](#)

Enable Enterprise Voice: ☐ Do Not Configure ☒ Enable ☐ Disable

Clear Line URI: ☐

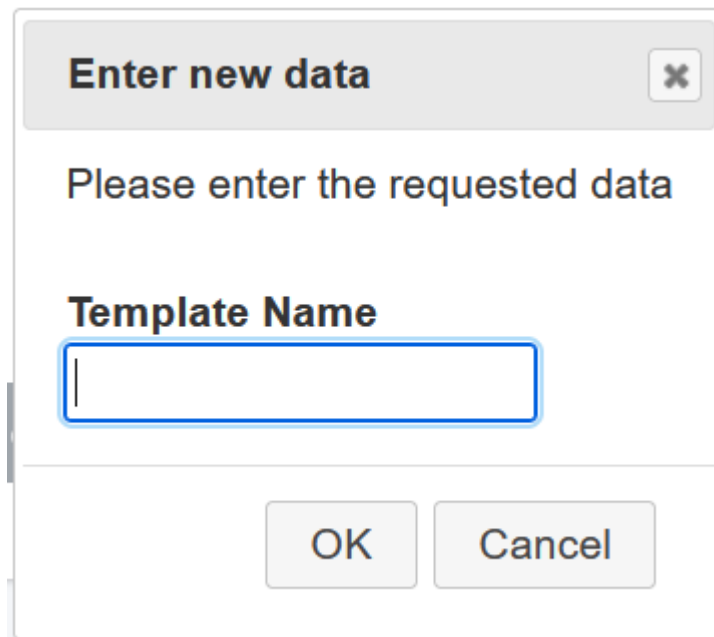
Assign Number from:

NumberRange:

NumberRange details:
Use Extensions:
Number Of Digits:


➤ To create a new template, do the following:

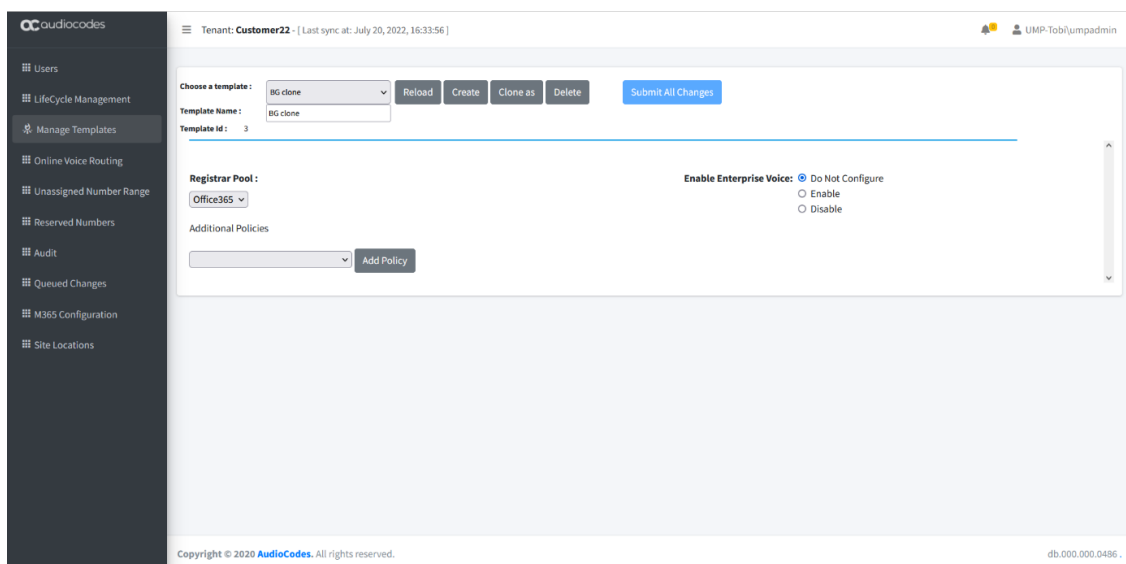
1. From the template drop-down list, select Create. A new template is created with a random number (e.g. New-Template).
2. In the Selected Template box, enter the desired name.



A modal dialog box titled "Enter new data" with a close button (X) in the top right corner. The text "Please enter the requested data" is displayed. Below it, the label "Template Name" is followed by a text input field. At the bottom, there are two buttons: "OK" and "Cancel".

3. Complete the Policy and Telephony settings section, and then select the policies you wish to assign.
4. From the Additional Policies drop-down list, select the desired Teams Policies, and then

click 



A screenshot of the AudioCodes Customer Tenant Portal interface. The left sidebar shows a navigation menu with options: Users, Lifecycle Management, Manage Templates (selected), Online Voice Routing, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, and Site Locations. The main content area shows the configuration for a template named "BG clone" (Template ID: 3). It includes fields for "Registrar Pool" (set to "Office365") and "Enable Enterprise Voice" (set to "Do Not Configure"). There is an "Additional Policies" dropdown menu with an "Add Policy" button. The top of the page shows the tenant name "Customer22" and the user "UMP-TobiJumadmin". The footer contains the copyright notice "Copyright © 2020 AudioCodes. All rights reserved." and the identifier "db.000.000.0486".

The screenshots show the 'Manage Templates' interface for Tenant: Customer22. The top screenshot shows the initial configuration with 'Enable Enterprise Voice' set to 'Do Not Configure'. The bottom screenshot shows the 'Additional Policies' section expanded, with 'CallingLineIdentity' policy added and 'Enable Enterprise Voice' set to 'Enable'.

5. Select the Policy Value for the selected policies. In the example above, the value is <Automatic>.
6. 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.

Table 32-1: Enterprise Voice Phone Number Configuration

Parameter	Description
Assign Number From	Assign a phone number using one of the following range definitions: <ul style="list-style-type: none"> ■ Phone ■ Home ■ Mobile

Parameter	Description
	<ul style="list-style-type: none"> ■ Number Range ■ IpPhone ■ File
Number Range	Configures one of the predefined number ranges configured in Section Managing Unassigned Number Ranges on page 451. This parameter is displayed when “Number Range” is displayed above.
Use Extensions	Determines whether extensions are configured.
Number of Digits	Configures the number of digits of the extension. This parameter is displayed when the “Use Extensions” checkbox is selected.

The screenshot shows the AudioCodes Customer Tenant Portal interface. The sidebar on the left contains navigation links: Users, Lifecycle Management, Manage Templates (highlighted), Online Voice Routing, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, and Site Locations. The main content area is titled 'Tenant: Customer22 - [Last sync at: July 20, 2022, 16:33:56]'. It features a 'Choose a template' dropdown set to 'BG clone', with buttons for 'Reload', 'Create', 'Clone as', 'Delete', and 'Submit All Changes'. Below this, the 'Template Name' is 'BG clone' and 'Template ID' is '3'. The 'Registrar Pool' is set to 'Office365'. There are sections for 'Additional Policies' and '1. CallingLineIdentity Policy' with a dropdown set to '<Automatic>' and a 'del' button. On the right, 'Enable Enterprise Voice' has radio buttons for 'Do Not Configure', 'Enable' (selected), and 'Disable'. Below that is a 'Clear Line URI' checkbox. Further down, 'Assign Number from' is a dropdown, and 'NumberRange details' includes 'Use Extensions' and 'Number Of Digits' fields. The footer shows 'Copyright © 2020 AudioCodes. All rights reserved.' and a user ID 'db.000.000.0486'.



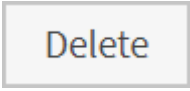
7. When you have completed the configuration, click

Submit All Changes



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:**

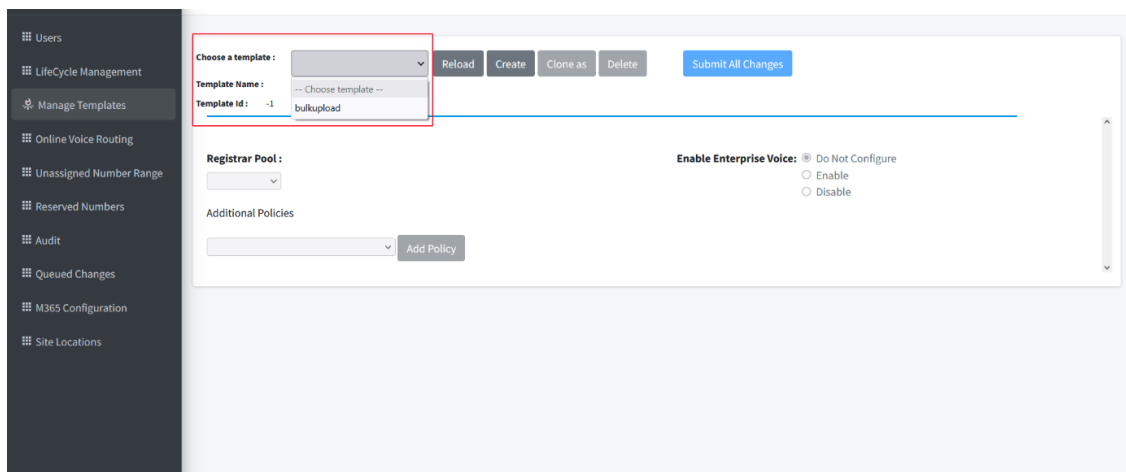
- Click  to reload an existing template.
- Click  to clone an existing template.
- Click  to delete an existing template.

Upload M365 Users from File and Attach to Template

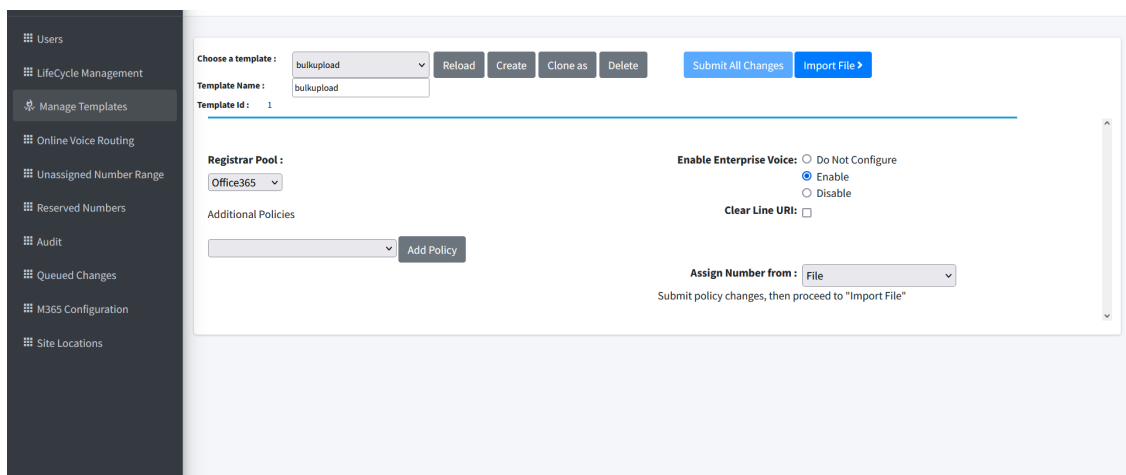
This section describes how to upload a list of M365 users from an external file and attach them to a specific template.

➤ **To import a bulk template from a CSV file:**

1. From the template drop-down list, choose a template to import.



The screenshot shows the 'Manage Templates' interface. On the left is a sidebar with navigation links: Users, LifeCycle Management, Manage Templates (selected), Online Voice Routing, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, and Site Locations. The main content area has a header with 'Choose a template:' dropdown, 'Reload', 'Create', 'Clone as', 'Delete', and 'Submit All Changes' buttons. Below this, the 'Template Name' is 'bulkupload' and 'Template Id' is '-1'. The 'Registrar Pool' is set to 'Office365'. The 'Enable Enterprise Voice' section has three radio buttons: 'Do Not Configure' (selected), 'Enable', and 'Disable'. There is also an 'Add Policy' button.



The screenshot shows the 'Manage Templates' interface after selecting a template. The 'Choose a template:' dropdown is now closed, and 'bulkupload' is selected. The 'Template Name' is 'bulkupload' and 'Template Id' is '1'. The 'Registrar Pool' is set to 'Office365'. The 'Enable Enterprise Voice' section has three radio buttons: 'Do Not Configure', 'Enable' (selected), and 'Disable'. The 'Clear Line URI' checkbox is checked. The 'Assign Number from' dropdown is set to 'File'. The 'Submit policy changes, then proceed to "Import File"' button is visible.

2. From the Add Policy drop-down, select the desired policy.
3. **Enable Enterprise Voice.**

4. From the Assign Number from drop-down, select **File**.

The screenshot shows the UMP-365 interface for a tenant named 'Customer22'. The left sidebar contains a menu with options: Users, LifeCycle Management, Manage Templates (selected), Online Voice Routing, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, and Site Locations. The main content area has a header with 'Tenant: Customer22 - [Last sync at: August 16, 2022, 11:38:56]' and a user profile 'UMP-Tobi\umpadmin'. Below the header, there are buttons for 'Choose a template', 'Reload', 'Create', 'Clone as', 'Delete', 'Submit All Changes', and 'Import File >'. The 'Template Name' is 'BG clone' and the 'Template Id' is '3'. The 'Registrar Pool' is 'Office365'. The 'Enable Enterprise Voice' section has radio buttons for 'Do Not Configure', 'Enable' (selected), and 'Disable'. The 'Clear Line URI' checkbox is unchecked. The 'Assign Number from' dropdown is set to 'File'. Below this, it says 'Submit policy changes, then proceed to "Import File"'.

5. Click **Submit All Changes**. The **Import File >** button is enabled. This action is required whenever a change is made to a policy.

Import File >

6. Click **Import File >** to import a template file.

The screenshot shows the UMP-365 interface for a tenant named 'Customer22'. The left sidebar contains a menu with options: Users, LifeCycle Management, Manage Templates (selected), Online Voice Routing, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, and Site Locations. The main content area has a header with 'Tenant: Customer22 - [Last sync at: August 16, 2022, 11:38:56]' and a user profile 'UMP-Tobi\umpadmin'. Below the header, there are buttons for 'New', 'Edit', 'Delete', 'Import CSV' (highlighted with a red box), 'Export CSV', 'Select all', 'Deselect all', and 'Apply Template'. The 'Template Name' is 'BG clone' and the 'Template Id' is '3'. The 'Registrar Pool' is 'Office365'. The 'Enable Enterprise Voice' section has radio buttons for 'Do Not Configure', 'Enable' (selected), and 'Disable'. The 'Clear Line URI' checkbox is unchecked. The 'Assign Number from' dropdown is set to 'File'. Below this, it says 'Submit policy changes, then proceed to "Import File"'.

7. Click **Import CSV**. The Import file dialog is displayed.

CSV file import

CSV file:

Choose file...

Drag and drop a file here to upload

The file to import should be in the following format:

sip:christiec@m365x74218585.onmicrosoft.com,+18585550111

sip:irvins@m365x74218585.onmicrosoft.com,+13095550101

sip:gradya@m365x74218585.onmicrosoft.com,+13095550104

sip:alexw@m365x74218585.onmicrosoft.com,+18585550110

8. Choose a file to import.

Map CSV fields

Select the CSV column you want to use the data from for each field.

Sip address

▼

Number

▼

Import 5 records

9. Optionally select the CSV column to apply to the SIP address and Number fields.

10. Select **Import <number of records> records**.

Users

LifeCycle Management

Manage Templates

Online Voice Routing

Unassigned Number Range

Reserved Numbers

Audit

Queued Changes

M365 Configuration

Site Locations

New

Edit

Delete

Import CSV

Export CSV

Select all

Deselect all

Apply Template

Search:

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

Previous

1

Next

Apply Template

11. Select all records and then click

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	

The following confirmation is displayed.

The operation is now completed. You can view the cmdlets in the Queued Changes menu (see [Monitoring M365 Replication Actions Queue](#) on page 508).



A validation check is conducted to verify whether a user already has a preexisting policy in the Managed Template. In this case, the cmdlet is not populated in the Queued Changes for this user, thereby avoiding the loading of redundant cmdlets to the replication queue.

Export CSV

You can export a CSV file containing a list of entries.

➤ To export a CSV file:

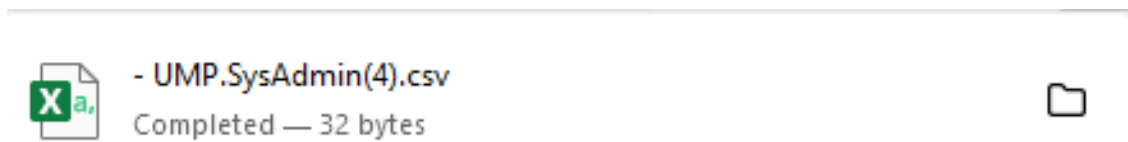
1. From the template drop-down list, choose a template to import.

2. Enable Enterprise Voice.
3. From the Assign Number from drop-down, select **File**.

Import File >

4. Click **Import File >** to import a template file.

5. Click **Export CSV** to export a list of existing entries.



Create New Entry Manually

You can create a new template entry manually.

➤ **To create a new entry:**

1. Click **New**.

A screenshot of a 'Create new entry' dialog box. The dialog has a title bar with the text 'Create new entry' and a close button (X). Inside the dialog, there are two input fields. The first is labeled 'Sip address:' and contains the text '9242520.OnMicrosoft.com'. The second is labeled 'Number:' and contains the text 'tel:+4812341'. At the bottom right of the dialog is a 'Create' button.

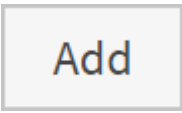
2. Enter the user SIP URI and telephone and then click **Create**.

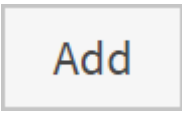
Binding Templates to Security Groups

This section describes how to assign the templates created in [Managing Templates](#) on page 459 to Microsoft 365 Security Groups. The Security groups are used for granting access to Microsoft 365 resources for users with identical or similar organization profiles in the Enterprise network.

➤ **To assign templates to security groups:**

1. In the Customer portal Navigation pane, select **Lifecycle Management**. A list of the assignments of templates to security groups is displayed.

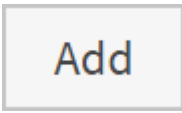


2. Click  to assign a Template to a Security Group.


Rank	Replication Template	Security Group	Error
1	TempleRun	SG_Auto11-20	
2	t1	SG_Auto11-20	
3	t2	user24_1	

Showing 1 to 3 of 3 entries 1 row selected
 Templates are processed by priority, the lowest rank index has the highest priority.

Previous 1 Next

2. Click  to assign a Template to a Security Group.



4. Click .

Add new

Security Group (min 1 char):

group102 ✕

group103 ✕

group104 ✕

group105 ✕

✕


Template:

t1

Close

Save

3. In the Add new screen, select one or more Security Groups and select a Security Template to apply. If multiple Security Groups are selected, the template is only assigned to group members belonging to all security groups (A logical AND function is performed on all groups specified).

4. Click .

Users
LifeCycle Management
Manage Templates
Online Voice Routing
Unassigned Number Range
Reserved Numbers
Audit
Queued Changes
O365 Configuration

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

- The new binding with the replication template assigned to multiple security groups is assigned Rank “4” in the previous figure. 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.

Location-Based Routing

Location-Based Routing restricts toll bypass for a Teams user based on their configured policy and geographic location when connecting to the PSTN network. Location-Based Routing is applied to the configured network region topology, site, and subnet. When toll bypass is restricted for a specific location, you associate an IP subnet and PSTN gateway for this location to a network site. When the Teams user policy is enabled for Location-Based Routing, a call takes place between the user and the PSTN network and the user is located at a site where Location-Based Routing restrictions are applied, then toll bypass is restricted for this user.

A user’s location is determined by the IP subnet of the connected Teams endpoints. If a user has multiple Teams clients located at different sites, Location-Based Routing enforces each client’s routing separately, depending on the location of the Teams endpoints:

- The Teams user must be enabled for Location-Based Routing in the user's Teams Calling policy.
- The Teams user’s endpoint network site location must be enabled for Location-Based Routing.
- The PSTN gateway passing the call must be enabled for Location-Based Routing.

For transfer scenarios, the route of the PSTN call is based on the routing settings of the person transferring the call, and on the Location-Based Routing settings of the Teams user to whom the call is being transferred.

For conferencing and group call scenarios, whether a Teams user for whom toll bypass is restricted is or has been part of the call.

For outbound PSTN calls, the message appears in the call window: Call not allowed due to your organization's settings.

For inbound PSTN calls, the call is routed based on the called Teams user's unanswered call forwarding settings, typically to voicemail. If the Teams user doesn't have unanswered call settings configured, the call disconnects.



- This feature is relevant for Hosted Pro and OC Pro licenses.
- You must enable Location-based routing scripts for implementing this feature (see [M365 Template Scenarios](#) on page 190).

The script executes the same commands from [Default M365 Tenant Onboarding Script](#) on page 191 and in addition executes the following actions:

- Adds a region (if not already preconfigured in the DNS subdomain).
- Enables Location-based routing for the region
- Adds a network site either using preconfigured networking parameters or custom variables configured in the Onboarding wizard (as described above).
- Adds Online PSTN Gateway
- Configures PSTN gateway including SIP Signaling port, Max Concurrent sessions, ForwardCallHistory, ForwardPai
- Enables Location-based routing on the PSTN Gateway
- Creates Teams Calling policy with UMPPreventTollBypass feature enabled (Allow Teams calling, preventing toll bypass).

Location-Based Routing Configuration

The Onboarding wizard applies Location-based routing using the following scripts:

- M365 Onboarding script "M365 onboarding with Location Based Routing" (see [M365 Onboarding with Location-based Routing](#) on page 194: Default networking settings (hard-coded values) are applied by the script. Otherwise, this entry is for example purposes only.



Contact AudioCodes Professional Services to configure custom values for this script.

- M365 Onboarding script "M365 onboarding with Location-Based Routing and Custom Networks" (see [M365 onboarding with Location-Based Routing and Custom Networks](#) on page 201): Customers configure networking parameters.

Additional sites can be configured using one of the following methods:

- Using the Customer portal, see [Adding Network Sites](#) below and [Adding Trusted Sites](#) on page 478.
- Using the Teams admin center, see [Configure Network Topology in Microsoft Teams](#) on page 481.

User policies must be changed to prevent Toll Bypass as described in [Change Users Policies to Prevent Toll Bypass \(mandatory\)](#) on page 487.

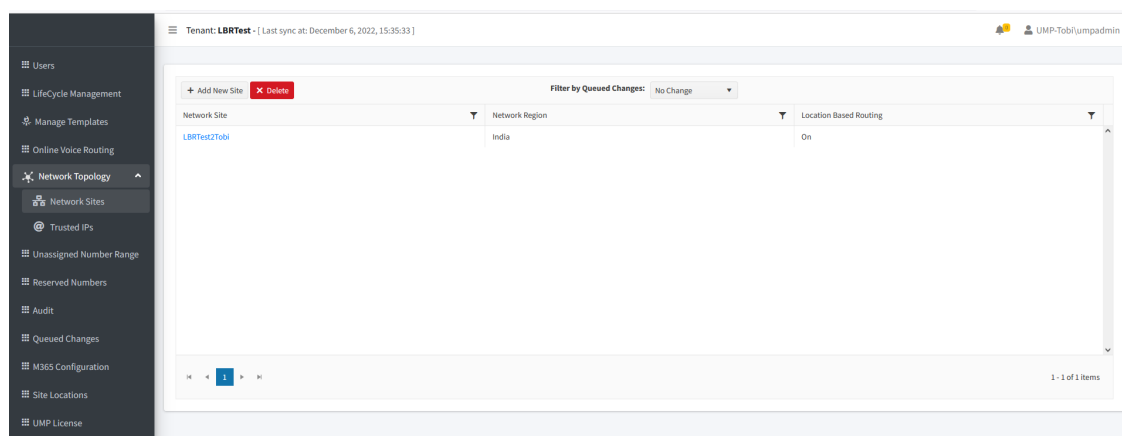
Adding Network Sites

You can add network sites that you wish to manage Location Based Routing for each relevant network region.

➤ To add a new network site:

1. In the Customer portal Navigation pane, open the Network Sites page (**Network Topology > Network sites**).

The following screen displays the **default** entry **LBRTes2Tobi** created during the Onboarding wizard, the default M365 Location-Based routing script was applied. This entry may be a preconfigured customer value or otherwise an example entry. It cannot be edited (only deleted or the subnet mask may be modified).



2. Select the default entry and double-click it.

Site Name:
LBRCustomTest

Description:
Default Site

Network Region:
India Manage Regions

☒ **Location based routing**

Network roaming policy:

Emergency calling policy:

Emergency call routing policy:

+ Add New Record Filter by Queued Changes: No Change

Subnet	Description	Network Range	
192.168.178.0 (Queued: New)	Default site	0	Edit Delete

3. Click **Edit** to update the subnet mask.

Site Name:
LBRCDefault

Description:
Default Site created by AudioCodes LiveCloud

Network Region:
India Manage Regions

☒ **Location based routing**

Network roaming policy:

Emergency calling policy:

Emergency call routing policy:

+ Add New Record Filter by Queued Changes: No Change

Subnet	Description	Network Range	
192.254.0.0	Example subnet set by AudioCodes LiveCloud	16	Update Cancel

4. Update the Network Range (subnet mask) and then click **Update**.

➤ **To add a new site:**

1. Click **Add New Record**.

Tenant: LBRDefault - [Last sync at: December 8, 2022, 15:08:39]

Filter by Queued Changes: No Change

Network Site	Network Region	Location Based Routing
LBRDefault	India	On

1 - 1 of 1 items

Copyright © 2022 Audiocodes. All rights reserved. db.000.000.0571.

Tenant: LBRDefault - [Last sync at: December 8, 2022, 15:08:39]

Site Name:

Description:

Network Region: -- No Region-- Manage Regions

☐ Location based routing

Network roaming policy: Global (Org-wide default)

Emergency calling policy: Global (Org-wide default)

Emergency call routing policy: Global (Org-wide default)

Save

Copyright © 2022 Audiocodes. All rights reserved. db.000.000.0571.

2. Configure new site according to the table below.

Parameter	Description
Site Name	Name of the site.
Description	Short site description.
Network Region	List of regions to assign to the site. Click Manage Regions to add new regions (see Adding Network Regions on the next page).
Location based routing	Enables Location-based routing feature.
Network Roaming Policy	Preconfigured Microsoft Network Roaming policies.

Parameter	Description
Emergency Calling Policy	Preconfigured Microsoft Emergency Calling policies.
Emergency Call Routing Policy	Preconfigured Microsoft Emergency Call Routing policies.

Tenant: LBRDefault - [Last sync at: December 8, 2022, 15:08:39]

Site Name: Shanghai

Description: Shanghai Logistics Center

Network Region: China [Manage Regions](#)

☐ Location based routing

Network roaming policy: Global (Org-wide default)

Emergency calling policy: Global (Org-wide default)

Emergency call routing policy: Global (Org-wide default)

[Save](#)

Copyright © 2022 AudioCodes. All rights reserved. db.000.000.0571.

3. Click **Save** to save the new site.

Tenant: LBRDefault - [Last sync at: December 8, 2022, 15:08:39]

[Add New Site](#) [Delete](#) Filter by Queued Changes: No Change

Network Site	Network Region	Location Based Routing
LBRDefault	India	On
Shanghai (Queued: New)	China	On

1 - 2 of 2 items

Copyright © 2022 AudioCodes. All rights reserved. db.000.000.0571.

Adding Network Regions

You can manage the network regions for applying the Location Based Routing. Each region consists of sites (see [Adding Network Sites](#) on page 473).

➤ **To add a network region:**

1. In the Network Sites page, click **Manage Regions**.

CCaudioCodes

Tenant: IPPBXToBI - [Last sync at: December 6, 2022, 09:08:14]

UMP-Tobi/umpadmin

Site Name:

Description:

Network Region: --No Region-- [Manage Regions](#)

☐ Location based routing

Network roaming policy: Global (Org-wide default)

Emergency calling policy: Global (Org-wide default)

Emergency call routing policy: Global (Org-wide default)

[Save](#)

Copyright © 2022 AudioCodes. All rights reserved. db.000.000.0571.

Manage Regions

Region List:

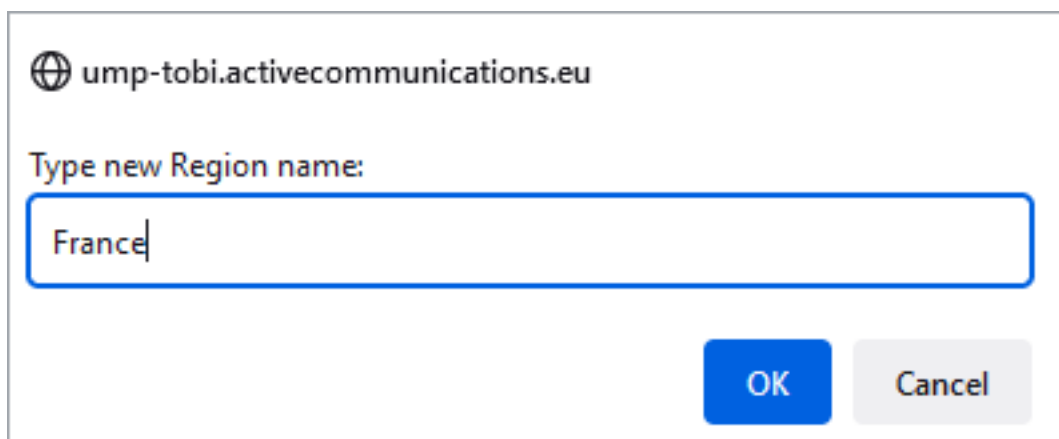
Holland

Benelux

[New Region](#) [Delete Region](#)

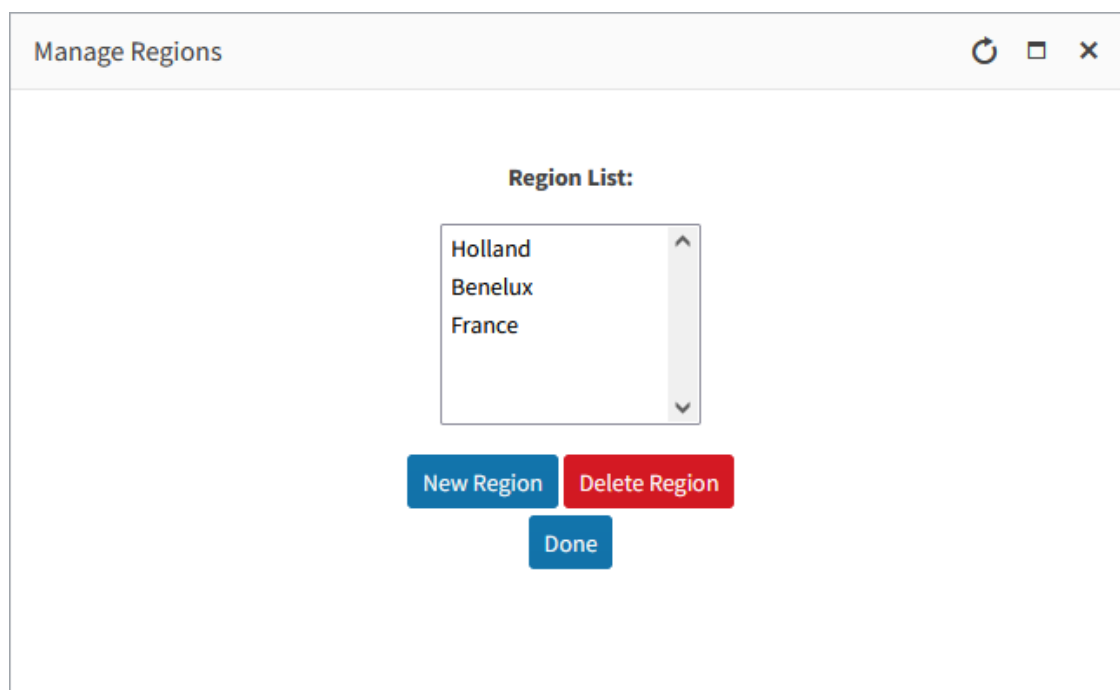
[Done](#)

2. Click **New Region**.



The dialog box has a title bar with a globe icon and the text "ump-tobi.activecommunications.eu". Below the title bar, the text "Type new Region name:" is followed by a text input field containing the word "France". At the bottom right of the dialog box are two buttons: "OK" (blue) and "Cancel" (gray).

3. Enter the name of the new region and then click **OK**.



The "Manage Regions" window has a title bar with a refresh icon, a maximize icon, and a close icon. The main content area is titled "Region List:" and contains a list box with the following items: "Holland", "Benelux", and "France". Below the list box are three buttons: "New Region" (blue), "Delete Region" (red), and "Done" (blue).

Adding Trusted Sites

Trusted Public IP addresses must be configured for allowing NAT translated internal IP addresses for all site locations..

➤ To add Trusted sites:

1. In the Customer portal Navigation pane, open the Trusted IPs page (**Network Topology > Trusted IPs**).

The following screen displays the **default** entry **Trusted IP Address set by AudioCodes LiveCloud** created when during the Onboarding wizard, the default M365 Location-Based routing script was applied. This entry may be a preconfigured customer value or otherwise an example entry. It cannot be edited (only deleted or the subnet mask may be modified).

The screenshot shows the AudioCodes UMP-365 interface. On the left is a dark sidebar with a menu including Users, Lifecycle Management, Manage Templates, Online Voice Routing, Network Topology (expanded), Network Sites, Trusted IPs (selected), Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, Site Locations, and UMP License. The main content area is titled 'Tenant: LBRDefault - [Last sync at: December 7, 2022, 18:19:29]'. It features a table with columns: Trusted IP, Description, and Network Range. A single row is visible with '109.254.0.1' in the Trusted IP column, 'Example Trusted IP Address set by AudioCodes LiveCloud' in the Description column, and '32' in the Network Range column. To the right of the row are 'Edit' and 'Delete' icons. Above the table is a filter dropdown set to 'No Change'. A red box highlights the '+ Add New Record' button in the top left of the table area. At the bottom right of the table area, it says '1 - 1 of 1 Items'. The footer contains 'Copyright © 2022 AudioCodes. All rights reserved.' and 'db.000.000.0571'.

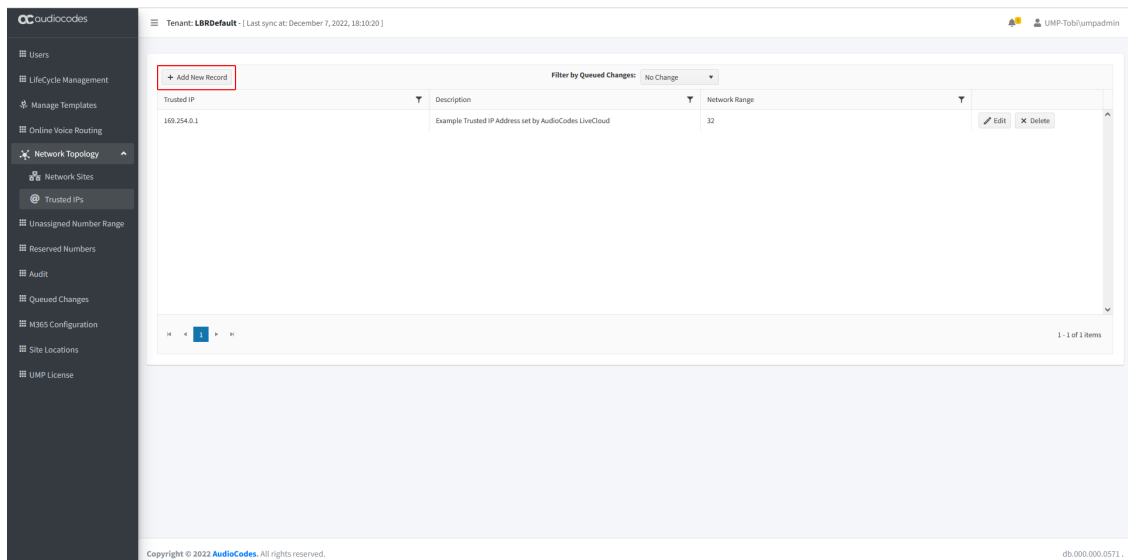
2. Select the default entry and double-click it.

This screenshot shows the same interface as the previous one, but the first row of the 'Trusted IPs' table is now selected with a blue highlight. The 'Update' button (a blue checkmark icon) is now visible to the right of the 'Delete' button. The 'Add New Record' button is no longer highlighted. All other elements, including the sidebar, filters, and footer, remain the same.

3. In the Network Range field, update the subnet mask as required.

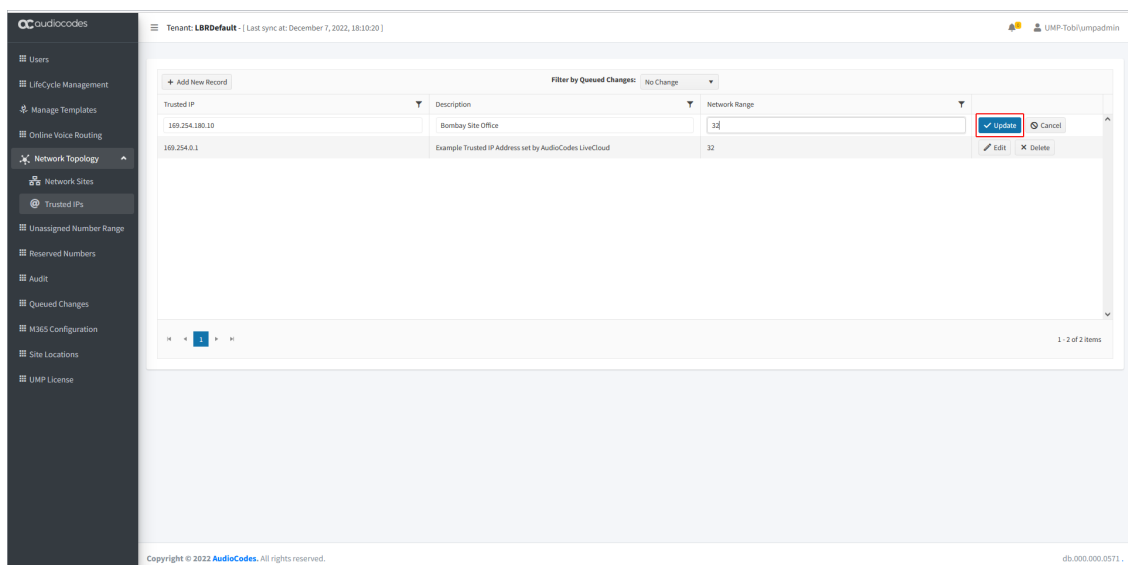
➤ **To add a new record:**

1. Click **Add New Record** to add a new Trusted IP site.



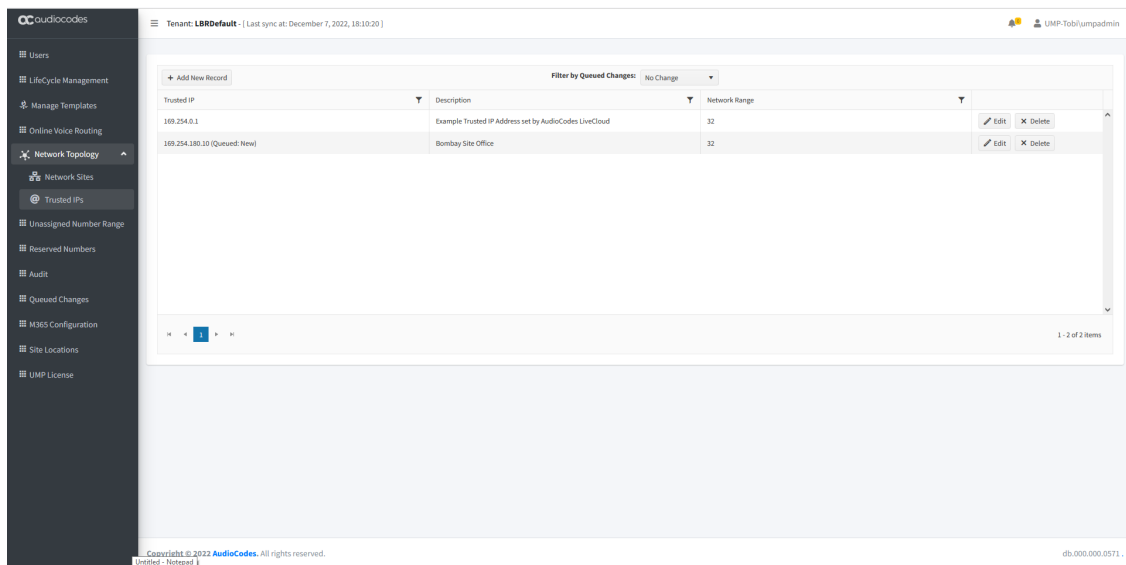
The screenshot shows the 'Trusted IPs' configuration page in the AudioCodes UMP-365 Tenant Portal. The left sidebar contains navigation options: Users, Lifecycle Management, Manage Templates, Online Voice Routing, Network Topology (selected), Network Sites, Trusted IPs, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, Site Locations, and UMP License. The main content area displays a table with columns: Trusted IP, Description, and Network Range. A red box highlights the '+ Add New Record' button. The table contains one record with Trusted IP 109.254.0.1, Description 'Example Trusted IP Address set by AudioCodes LiveCloud', and Network Range 32. The bottom right corner shows '1 - 1 of 1 Items'.

2. Enter the Public IP address of the site, a short description and the Network Range (subnet mask) and then click **Update**.



The screenshot shows the 'Trusted IPs' configuration page after adding a new record. The 'Update' button is highlighted with a red box. The table now contains two records: one with Trusted IP 109.254.180.10, Description 'Bombay Site Office', and Network Range 32; and another with Trusted IP 109.254.0.1, Description 'Example Trusted IP Address set by AudioCodes LiveCloud', and Network Range 32. The bottom right corner shows '1 - 2 of 2 Items'.

The new site is added.



You can filter this screen according to the following criteria:

- No Change
- Edit
- New
- Delete
- Failed

Configure Network Topology in Microsoft Teams

You can optionally configure network topology in the Microsoft Teams admin center instead of using the Multitenant portal:

- [Location-Based Network Sites](#) below
- [Location-Based Trusted Sites](#) on page 484



All updates on Microsoft Teams are synchronized to User Management Pack™ 365 SP Edition.

Location-Based Network Sites

This section describes how to configure new subnets in the Microsoft Teams admin center.

➤ To create a network site:

1. Login to the Teams admin with customer tenant credentials.
2. In the Navigation pane, select **Locations > Network Topology**.

Manage users

You can manage Audio Conferencing settings, policies, phone numbers, and other features for people in your organization. Go to [Admin center > Users](#) to manage other user settings such as adding or deleting users, changing passwords, and assigning licenses. [Learn more](#)

Search for a user

✓	Display name	Username	Phone number	Location	Policies assigned	Directory status	Audio Conferencing	Phone System
	MOD Administrator	admin@M365x12380949.o...		Netherlands	View policies	Online	On	On
	MOD Administrator	admin@M365x12380949.o...		Netherlands	View policies	Online	On	On
	Microsoft Service Account	ms-serviceaccount@M365...		Netherlands	View policies	Unlicensed	Off	Off
	Joni Sherman	JoniS@M365x12380949.O...		Netherlands	View policies	Online	On	On
	Patti Fernandez	PattiF@M365x12380949.O...		Netherlands	View policies	Online	On	On
	Alex Wilber	AlexW@M365x12380949...		Netherlands	View policies	Online	On	On
	Debra Berger	DebraB@M365x12380949...	+31 36 546 1241	Netherlands	View policies	Online	On	On
	Allan Deyoung	AllanD@M365x12380949...		Netherlands	View policies	Online	On	On
	Christie Cline	ChristieC@M365x1238094...		Netherlands	View policies	Online	On	On
	Nestor Wilke	NestorW@M365x1238094...		Netherlands	View policies	Online	On	On
	Johanna Lorenz	JohannaL@M365x1238094...		Netherlands	View policies	Online	On	On
	Adele Vance	AdeleV@M365x12380949...		Netherlands	View policies	Online	On	On

Network topology

You can use network topology to define the network regions, sites, and subnets that are used to determine the emergency call routing and calling policies that are to be used for a given location. [Learn more](#)

Network topology summary

- 1 Network site
- 1 Trusted IP
- 1 Roaming policy

Network sites | Trusted IPs | Roaming policies

[+ Add](#) [Edit](#) [Delete](#) | 1 item

Search

✓	Network site	Description	Network region	Location based routing	Emergency calling policy	Emergency call routing policy	Network roaming policy	Subnets
	LBRTest2Tobi	Default Site created by Au...	India	On	Global (Org-wide default)	Global (Org-wide default)	Global (Org-wide default)	1

3. Click **Add** to add a new subnet.

Network topology | Add a name for your network site

Add a name for your network site

Description

+ Add network region

Location based routing ☐ Off

Network roaming policy

Emergency calling policy

Emergency call routing policy

Subnets

A network subnet defines a segment of the IP network that contains the addresses of one or more endpoints. Each subnet must be associated with an emergency location, and the subnet ID must match the client network ID. [Learn more](#)

You haven't added any subnets in this network site yet.

[Add subnets](#)

[Save](#) [Cancel](#)

Add

Each subnet must be associated with a specific network site. A client's location is determined based on the network subnet and the associated network site. You can associate multiple subnets with the same network site but you can't associate multiple sites with the same subnet.

IP version

IPv4

IP address

192.168.1.0

Network range ⓘ

24

Description

Test range Amsterdam

Apply

Cancel

4. Select your IP version IP4/IPv6.
5. Enter the IP address.
6. Enter the network range (subnet mask).
7. Enter a short description.
8. Click **Apply**.

Location-Based Trusted Sites

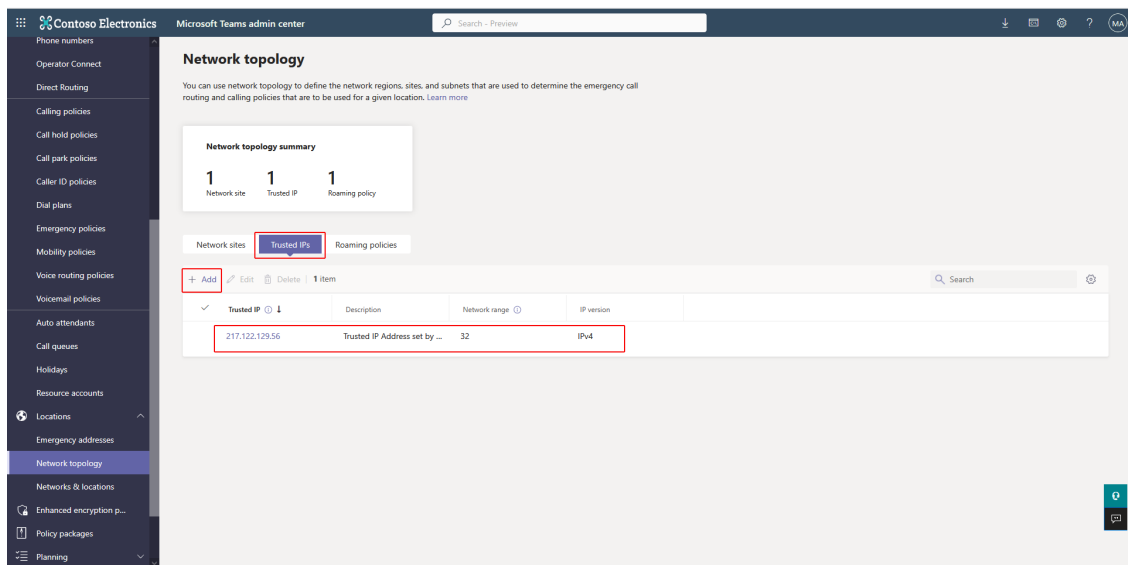
This section describes how to configure new trusted sites in the Teams admin center. Trusted IP addresses must be configured for allowing NAT translated internal IP addresses for all site locations.



Once added, the Trusted IP address cannot be modified (you can delete it or change the subnet mask/Network range).

➤ To configure Trusted IPs:

1. Click the **Trusted IPs** tab and then click **Add**.



The screenshot shows the Microsoft Teams admin center interface for 'Contoso Electronics'. The left sidebar contains a navigation menu with various settings categories. The main content area is titled 'Network topology' and includes a summary section and a table of trusted IP addresses.

Network topology summary

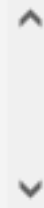
Network site	Trusted IP	Roaming policy
1	1	1

Trusted IPs

Trusted IP	Description	Network range	IP version
217.122.129.56	Trusted IP Address set by ...	32	IPv4

Add trusted IP address

Enter the number of bits that are used to determine the network range or ID. You can also figure out the number of bits needed here if you have the subnet mask.



IP version

IPv4



IP address

85.53.66.66

Network range ⓘ

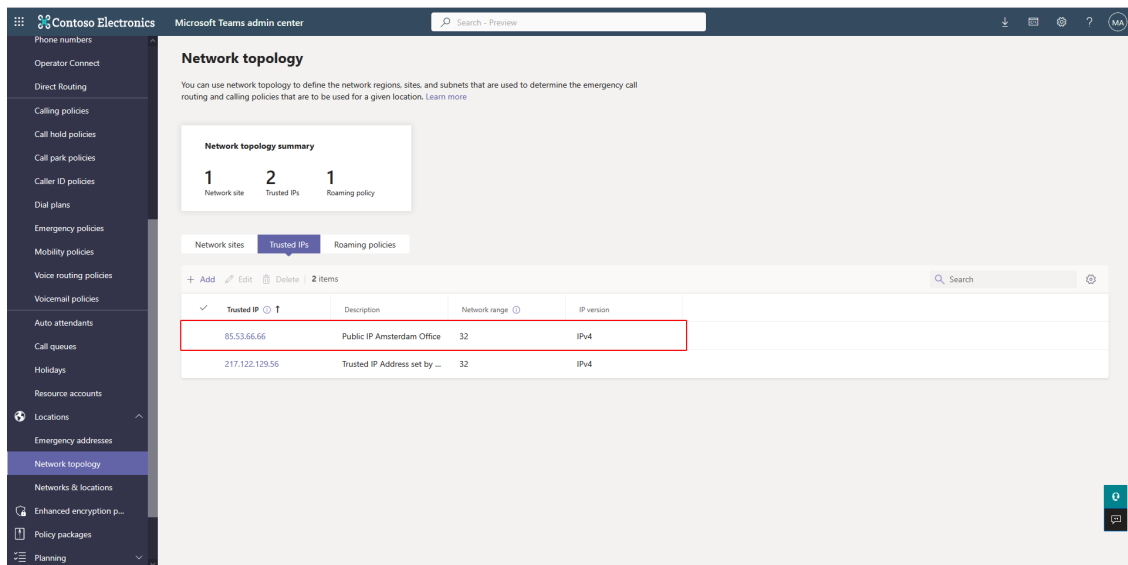
32

Description

Public IP Amsterdam Office

2. Select your IP version IP4/IPv6.
3. Enter the Public IP address.
4. Enter the network range (subnet mask).
5. Give the subnet a description.
6. Click **Apply**.

A public IP (range) is added.



Change Users Policies to Prevent Toll Bypass (mandatory)

User policies can be configured using one of the following methods:

- **Configure User Policy Manually** below
- **Configure User Policy Automatically** on page 490

Configure User Policy Manually

You can manually change the policies of the users to set them for calling with Enterprise Voice and to prevent Toll Bypass.

➤ To change user policies:

1. In the Navigation pane, select **Users > Manage users**.

Manage users

You can manage Audio Conferencing settings, policies, phone numbers, and other features for people in your organization. Go to [Admin center > Users](#) to manage other user settings such as adding or deleting users, changing passwords, and assigning licenses. [Learn more](#)

[Edit settings](#)

✓	Display name	Username	Phone number	Location	Policies assigned	Directory status	Audio Conferencing	Phone system
	MOD Administrator	admin@M365x12380949.o...		Netherlands	View policies	Online	On	On
	Microsoft Service Account	ms-serviceaccount@M365...		Netherlands	View policies	Unlicensed	Off	Off
	Joni Sherman	JoniS@M365x12380949.O...		Netherlands	View policies	Online	On	On
	Patti Fernandez	PattiF@M365x12380949.O...		Netherlands	View policies	Online	On	On
	Alex Wilber	AlexW@M365x12380949...		Netherlands	View policies	Online	On	On
	Debra Berger	DebraB@M365x12380949...	+31 36 546 1241	Netherlands	View policies	Online	On	On
	Allan Deyoung	AllanD@M365x12380949...		Netherlands	View policies	Online	On	On
	Christie Cline	ChristieC@M365x1238094...		Netherlands	View policies	Online	On	On
	Nestor Wilke	NestorW@M365x1238094...		Netherlands	View policies	Online	On	On
	Johanna Lorenz	JohannaL@M365x1238094...		Netherlands	View policies	Online	On	On
	Adele Vance	AdeleV@M365x12380949...		Netherlands	View policies	Online	On	On
	Isaiah Langer	IsaiahL@M365x12380949...		Netherlands	View policies	Online	On	On

Manage users

You can manage Audio Conferencing settings, policies, phone numbers, and other features for people in your organization. Go to [Admin center > Users](#) to manage other user settings such as adding or deleting users, changing passwords, and assigning licenses. [Learn more](#)

[Edit settings](#)

✓	Display name	Username	Phone number	Location	Policies assigned	Directory status	Audio Conferencing	Phone system
	MOD Administrator	admin@M365x12380949.o...		Netherlands	View policies	Online	On	On
	Microsoft Service Account	ms-serviceaccount@M365...		Netherlands	View policies	Unlicensed	Off	Off
	Joni Sherman	JoniS@M365x12380949.O...		Netherlands	View policies	Online	On	On
	Patti Fernandez	PattiF@M365x12380949.O...		Netherlands	View policies	Online	On	On
✓	Alex Wilber	AlexW@M365x12380949...		Netherlands	View policies	Online	On	On
	Debra Berger	DebraB@M365x12380949...	+31 36 546 1241	Netherlands	View policies	Online	On	On
	Allan Deyoung	AllanD@M365x12380949...		Netherlands	View policies	Online	On	On
	Christie Cline	ChristieC@M365x1238094...		Netherlands	View policies	Online	On	On
	Nestor Wilke	NestorW@M365x1238094...		Netherlands	View policies	Online	On	On
	Johanna Lorenz	JohannaL@M365x1238094...		Netherlands	View policies	Online	On	On
	Adele Vance	AdeleV@M365x12380949...		Netherlands	View policies	Online	On	On
	Isaiah Langer	IsaiahL@M365x12380949...		Netherlands	View policies	Online	On	On

2. Select a user and then click **Edit Settings**.

Edit settings

You can assign these policies to one or more people in your organization at the same time.

[Learn more](#)

Keep existing policy

App setup policy

Keep existing policy

Call park policy

Keep existing policy

Calling policy

UMPPreventTollBypass

Caller ID policy

Keep existing policy

Teams policy

Keep existing policy

Update policy

Keep existing policy

Emergency calling policy

Keep existing policy

Emergency call routing policy


Keep existing policy

Dial plan

Keep existing policy

Voice routing policy

Add/Edit Range

2. Click  to add a new number range.
3. Create the desired number range.

Edit

✕

Edit number range: LBR

NumberRangeStart

39026784000|

NumberRangeEnd

39026784500

OK

Cancel

Tenant: IPPBX-Tobi - [Last sync at: December 5, 2022, 16:07:32]
 UMP:Tobijumpadin

Reload All

Add/Edit Range

Add/Edit Bundle

Delete

Show
entries

Search:

Identity	Start of Number Range	End of Number Range	Available Numbers	Used In
LBR	39026784000	39026784500	501	
test	1000	1999	1000	

Showing 1 to 2 of 2 entries 1 row selected

Previous
1
Next

tel+39026784000
tel+39026784001
tel+39026784002
tel+39026784003
tel+39026784004
tel+39026784005
tel+39026784006
tel+39026784007
tel+39026784008
tel+39026784009
tel+39026784010

tel+39026784011
tel+39026784012
tel+39026784013
tel+39026784014
tel+39026784015
tel+39026784016
tel+39026784017
tel+39026784018
tel+39026784019
tel+39026784020
tel+39026784021

tel+39026784022
tel+39026784023
tel+39026784024
tel+39026784025
tel+39026784026
tel+39026784027
tel+39026784028
tel+39026784029
tel+39026784030
tel+39026784031
tel+39026784032

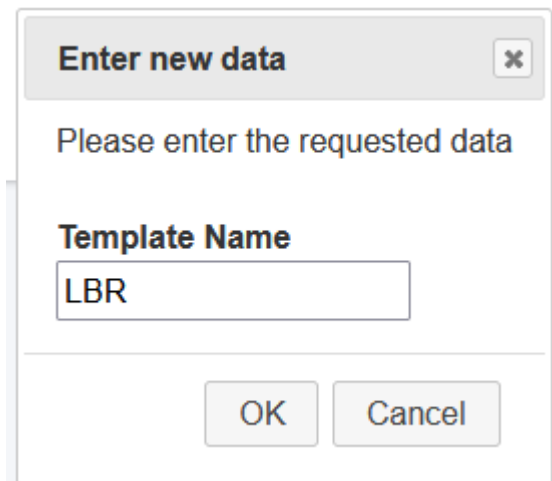
tel+39026784033
tel+39026784034
tel+39026784035
tel+39026784036
tel+39026784037
tel+39026784038
tel+39026784039
tel+39026784040
tel+39026784041
tel+39026784042
tel+39026784043

tel+39026784044
tel+39026784045
tel+39026784046
tel+39026784047
tel+39026784048
tel+39026784049
tel+39026784050
tel+39026784051
tel+39026784052
tel+39026784053
tel+39026784054

4. In the Multitenant portal Navigation pane, select **Manage Templates**.

Create

5. Click  to create a new template.



Enter new data [X]

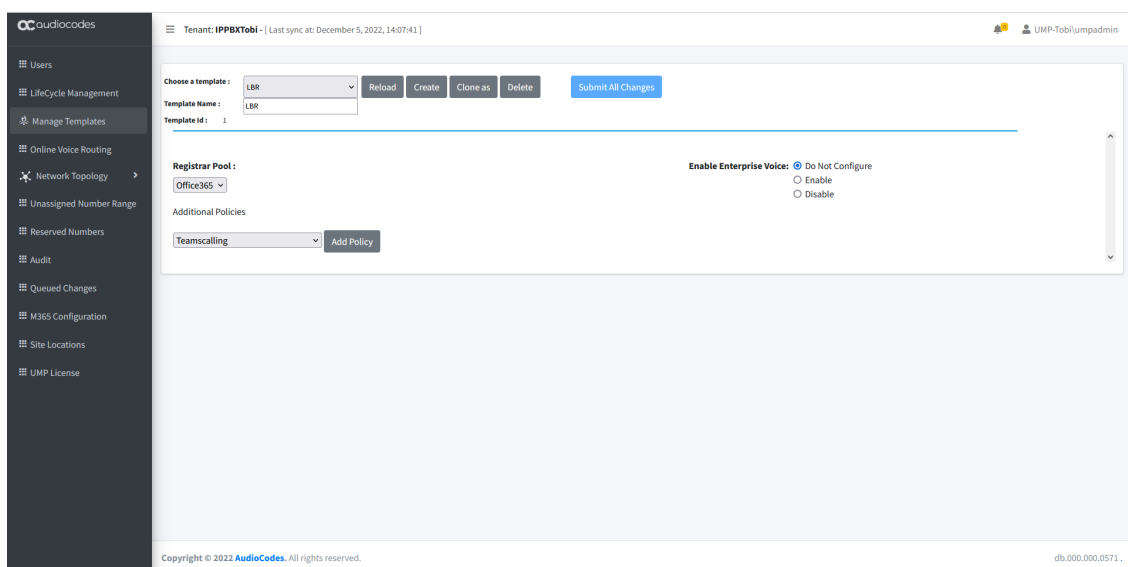
Please enter the requested data

Template Name

LBR

OK Cancel

6. Select **Teamscalling** and then click **Add Policy**.



AudioCodes

Tenant: IPPBXTobi - [Last sync at: December 5, 2022, 14:07:41]

UMP-Tobi/umpadmin

Choose a template: LBR [Reload] [Create] [Clone as] [Delete] [Submit All Changes]

Template Name: LBR

Template Id: 1

Registrar Pool: Office365

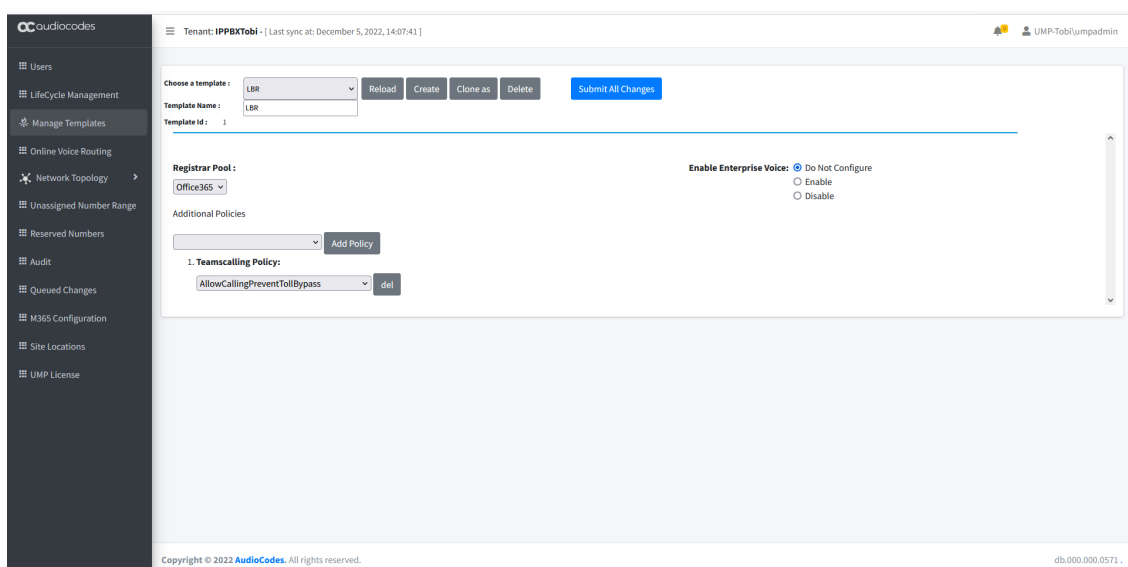
Enable Enterprise Voice: ☒ Do Not Configure ☐ Enable ☐ Disable

Additional Policies

Teamscalling [Add Policy]

Copyright © 2022 AudioCodes. All rights reserved. db.000.000.0571.

7. Click **Add Policy**.



AudioCodes

Tenant: IPPBXTobi - [Last sync at: December 5, 2022, 14:07:41]

UMP-Tobi/umpadmin

Choose a template: LBR [Reload] [Create] [Clone as] [Delete] [Submit All Changes]

Template Name: LBR

Template Id: 1

Registrar Pool: Office365

Enable Enterprise Voice: ☒ Do Not Configure ☐ Enable ☐ Disable

Additional Policies

1. Teamscalling Policy: AllowCallingPreventTollBypass [del]

Copyright © 2022 AudioCodes. All rights reserved. db.000.000.0571.

8. From the drop-down list, select **AllowCallingPreventTollBypass**.

9. Click **Add Policy**.

10. From the drop-down list, select **Onlinevoiceroutingpolicy**.

CCaudiocodes

Tenant: IPPEXTobi - [Last sync at: December 5, 2022, 14:07:41]

UMP-Tobi\umpadmin

Choose a template: LBR [Reload] [Create] [Clone as] [Delete] [Submit All Changes]

Template Name: LBR

Template Id: 1

Registrar Pool: Office365

Enable Enterprise Voice: ☒ Do Not Configure
☐ Enable
☐ Disable

Additional Policies

Onlinevoiceroutingpolicy [Add Policy]

1. Teamscalling Policy:
 AllowCallingPreventTollBypass [del]

Copyright © 2022 AudioCodes. All rights reserved. db.000.000.0571

11. Click **Add Policy**.

CCaudiocodes

Tenant: IPPEXTobi - [Last sync at: December 5, 2022, 16:07:32]

UMP-Tobi\umpadmin

Choose a template: LBR [Reload] [Create] [Clone as] [Delete] [Submit All Changes]

Template Name: LBR

Template Id: 1

Registrar Pool: Office365

Enable Enterprise Voice: ☒ Do Not Configure
☐ Enable
☐ Disable

Clear Line URI: ☐

Assign Number from: NumberRange

NumberRange: LBR

NumberRange details: From: 39026784000 to 39026784500

Use Extensions: ☐

Number Of Digits:

Additional Policies

Onlinevoiceroutingpolicy [Add Policy]

2. Onlinevoiceroutingpolicy Policy:
 Unrestricted [del]

1. Teamscalling Policy:
 AllowCallingPreventTollBypass [del]

Copyright © 2022 AudioCodes. All rights reserved. db.000.000.0571

12. From the drop-down list, select **Unrestricted**.

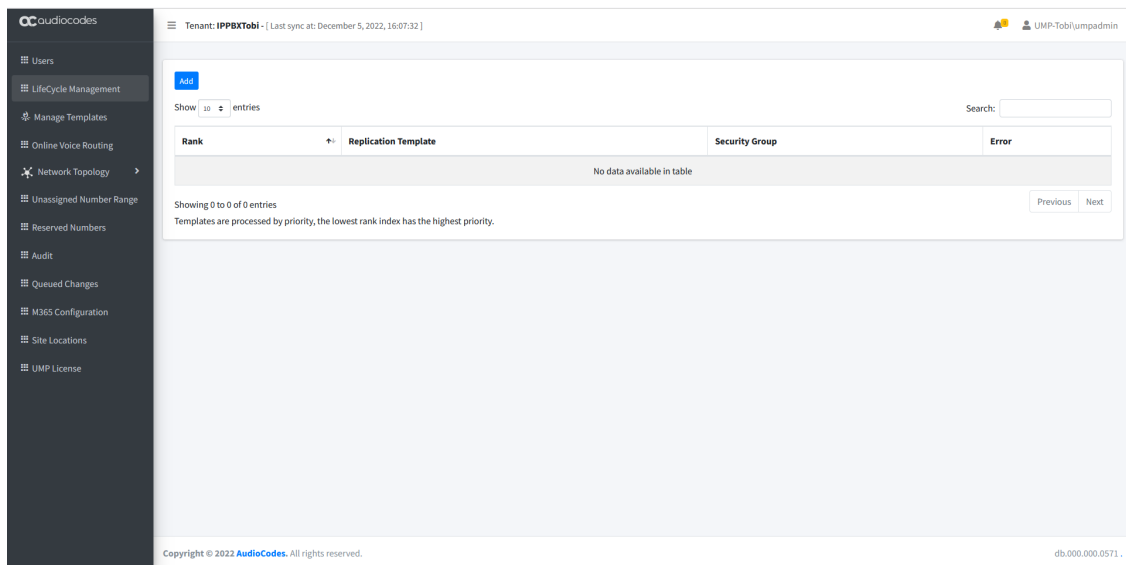
13. Enable Enterprise Voice for the users.

14. Assign number from **NumberRange**.

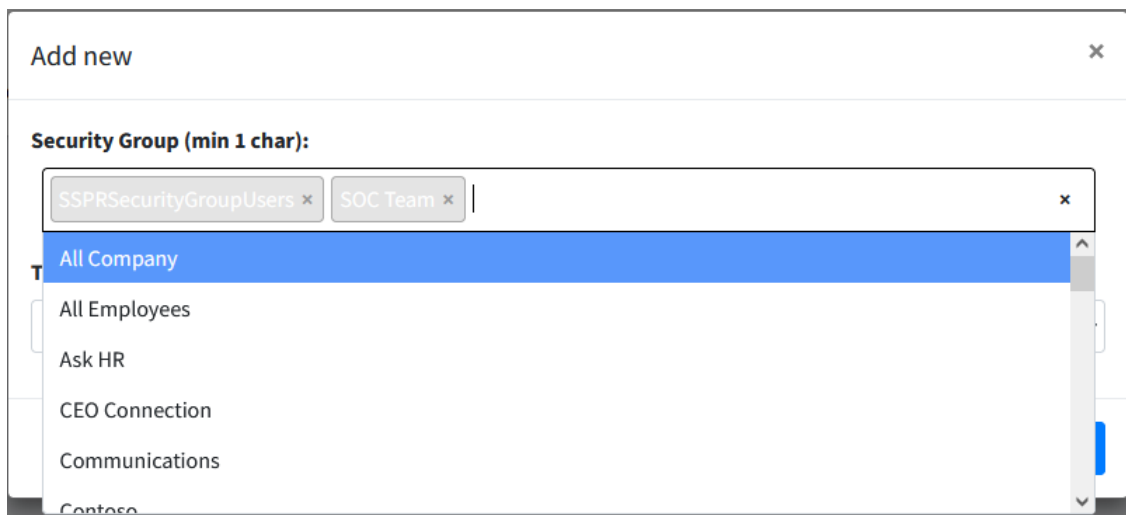
15. Select the range that you created for this Template above.

16. Click **Submit All Changes**.

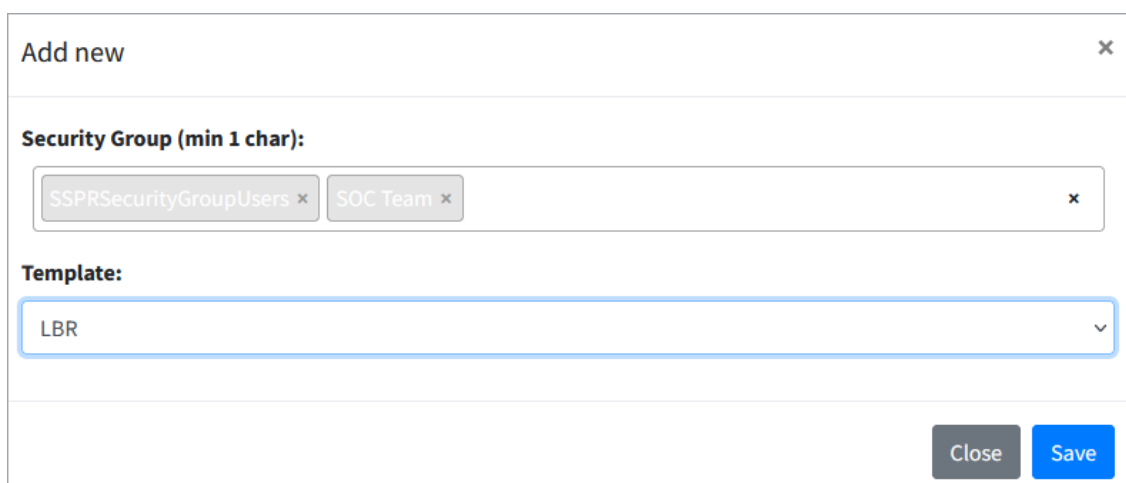
17. In the Navigation pane, select **LifeCycle management**.



18. Click **Add** to add a new mapping.



19. Select the desired security group.

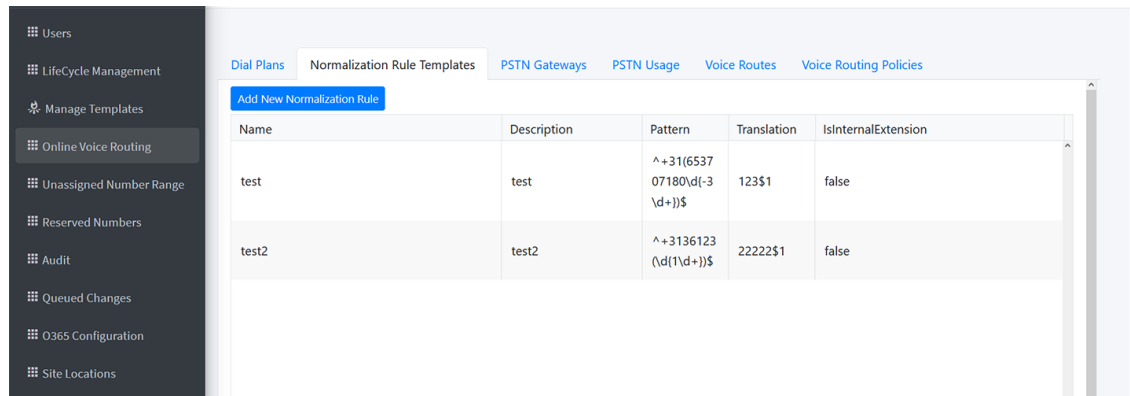


20. Apply the new template that you created above and then click **Save**. Changes and users are now automatically synchronized on each synchronization (every 60 minutes).

Configuring Online Voice Routing

The M365 default Onboarding script creates a default Online Voice Routing 'Unrestricted' and default Voice Route 'Unrestricted' (see [Default M365 Tenant Onboarding Script](#) on page 191). You can customize this policy and create additional policies according to site requirements.

1. In the Customer portal Navigation pane, select **Online Voice Routing**.

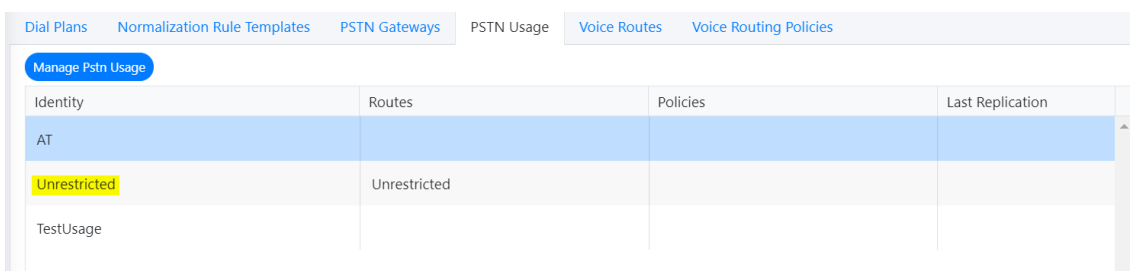


The Online Voice Routing screen allows you to define Customer M365 Tenant Voice Routing policies:

- Voice Routing Policies (see [Voice Routing Policy](#) on the next page)
- Voice Route (see [Voice Route](#) on page 500)
- PSTN Usage (see [PSTN Usage](#) below)
- PSTN Gateways (see [PSTN Gateways](#) on page 501)
- Normalization Rule Template (see [Microsoft 365 Dial Plan and Normalization Rules](#) on page 501)
- Dial Plan (see [Microsoft 365 Dial Plan and Normalization Rules](#) on page 501)

PSTN Usage

A container for voice routes and PSTN usages can be shared in different voice routing policies.



- Select the **Manage Pstn Usage** button to manage the PSTN Usage (Add/Edit/Delete).

Manage PSTN Usage

Manage PSTN Usage

Identity:

Usage List:

Unrestricted

New Usage

Delete Usage

Update PSTN Usage

Voice Routing Policy

A container for PSTN Usages can be assigned to a user or to multiple users.

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				

See the following:

- [Add Voice Routing Policy](#) on the next page
- [Edit Voice Routing Policy](#) on the next page
- [Delete Voice Routing Policy](#) on page 498

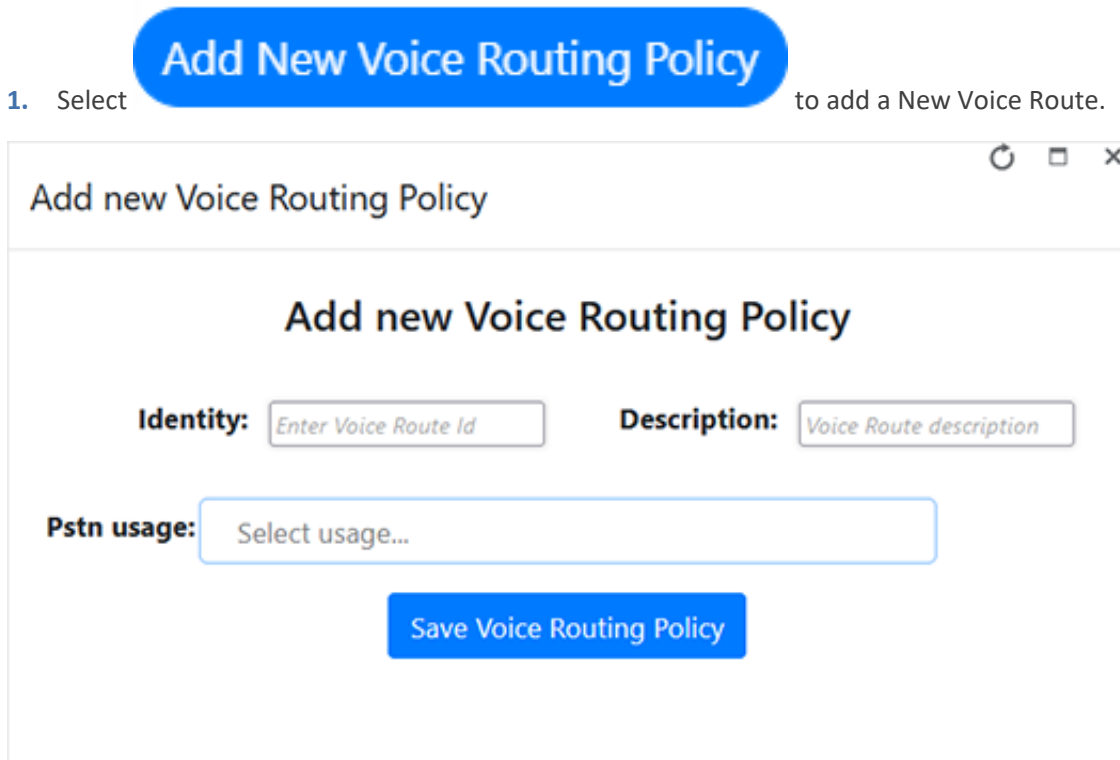
- [Apply Routing Policy to Security Group](#) on page 499

Add Voice Routing Policy

This section describes how to add a Voice Routing Policy.

- To add a voice routing policy:

1. Select **Add New Voice Routing Policy** to add a New Voice Route.



2. In the Identity field, enter the Voice Route Id.
3. In the Description field, enter a short description.
4. In the Pstn usage field, enter the Pstn usage configured in [PSTN Usage](#) on page 495.

5. Click **Save Voice Routing Policy** to save the new settings.

Edit Voice Routing Policy

This section describes how to edit a Voice Routing Policy.

- To edit Voice Routing Policy, do the following:

1. Select a Voice Routing policy.
2. Right-click and choose **Edit Voice Routing Policy**.

Add New Voice Routing Policy			
DataChangeT...	Identity	Description	PSTN Usage
	Global		
	Unrestr...		Unrestricted
	12	Skill 1	Unrestricted

Apply this Policy to Security Group
 Edit Voice Routing Policy
 Delete Voice Routing Policy
 Cancel changes

Edit Voice Routing Policy

Edit Voice Routing Policy

Identity:
Description:

3. Enter a text description and configure the PSTN usage.
4. Click **Update Voice Routing Policy** to apply the changes.

Delete Voice Routing Policy

This section describes 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.

Are you sure you want to delete the Voice Routing Policy?

OK

Cancel

Apply Routing Policy to Security Group

This section describes how to apply a Routing Policy to a Security Group.

➤ **To apply a routing policy to a security group:**

1. Select a Voice Routing policy.
2. Right-click and select **Apply Policy To Group**.

Apply Policy To Group

Security Group (min 1 char):

Select an option

- All Company
- All Employees
- Ask HR
- CEO Connection
- Communications
- Contoso

Apply Policy To Group

Security Group (min 1 char):

Ask HR

Close

Apply

- From the drop-down list, select a Security Group and then click **Apply**.

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. 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 when multiple routes to the same destination exist. Voice Routing Policies are assigned to subscribers, allowing them to reach certain destinations based on the PSTN Usage record that is assigned within the policy.

Dial Plans

Normalization Rule Templates

PSTN Gateways

PSTN Usage

Voice Routes

Voice Routing Policies

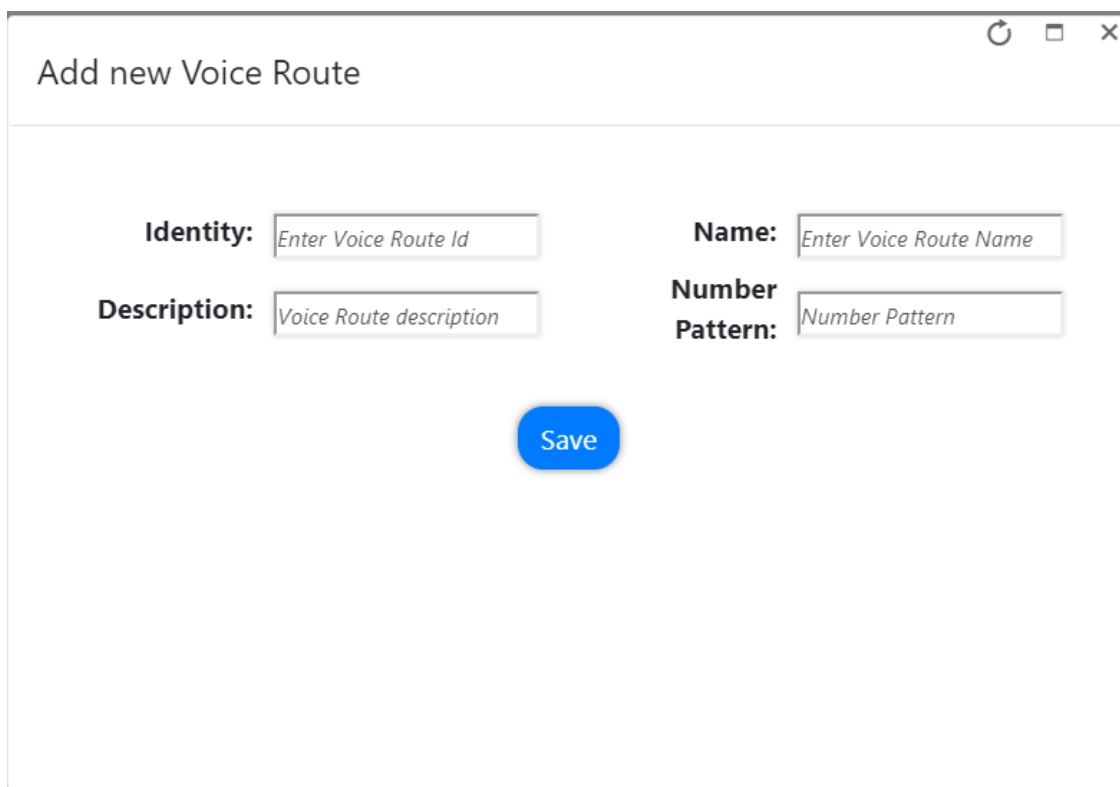
Add New Voice Route

Dat...	Identity	P...	Pattern	Name	Description	Pattern	PSTN Gateway...	PSTN Usage	
	LocalRoute	0	^(\+1[0-9]{10})\$	LocalRoute		^(\+1[0-9]{10})\$			<div><div>▼▲</div></div>
	Unrestricted	1	.*	Unrestricted		.*	audiocodes-be.customers.audiocodes.be	Unrestricted	<div><div>▼▲</div></div>

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.



The screenshot shows a web application window titled "Add new Voice Route". The window has standard browser controls (refresh, maximize, close) in the top right corner. The form contains four input fields arranged in a 2x2 grid:

- Identity:** Input field with placeholder text "Enter Voice Route Id".
- Name:** Input field with placeholder text "Enter Voice Route Name".
- Description:** Input field with placeholder text "Voice Route description".
- Number Pattern:** Input field with placeholder text "Number Pattern".

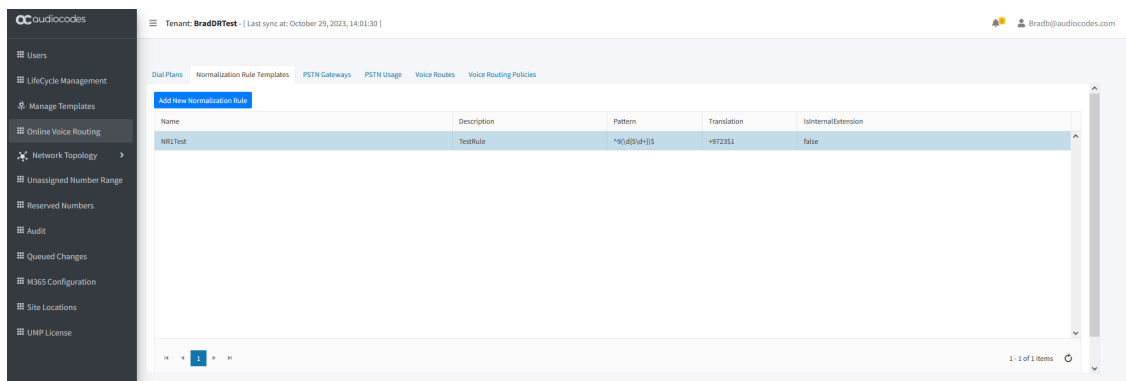
Below the input fields is a blue "Save" button.

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.

Microsoft 365 Dial Plan and 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 from Microsoft 365.



➤ **To create a new normalization rule:**

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.

Add new Normalization Rule

Add new Normalization Rule

Name:

Description:

Starting digits:

Length:

Digits to remove:

Digits to add:

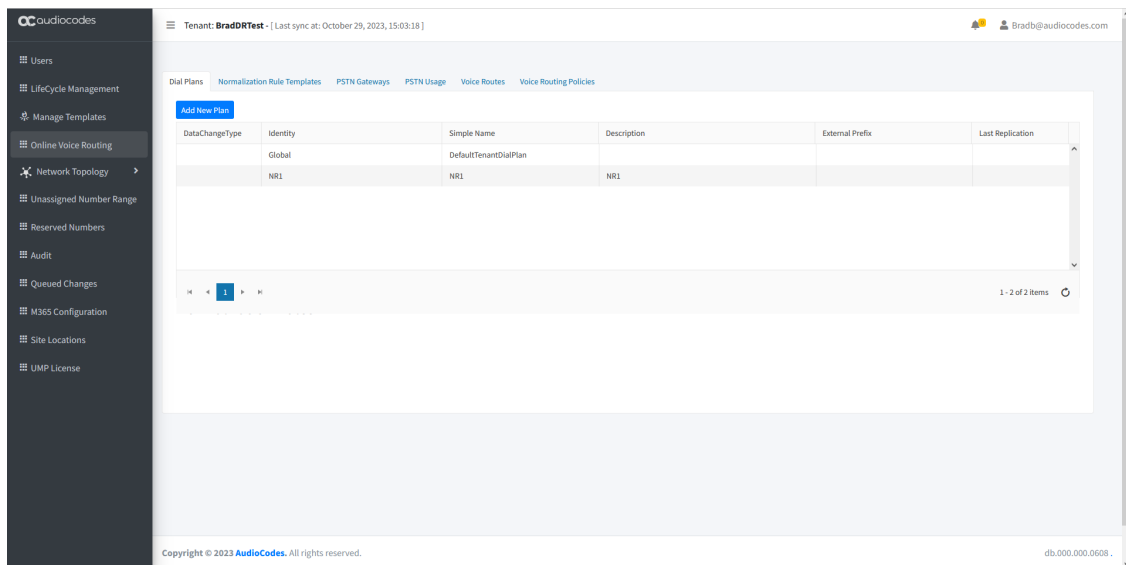
Pattern:

Translation:

IsInternalExtension: ☐

Save Normalization Rule

3. 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.



- To add Normalization Rules to a new dial plan:

Add New Plan

1. Click to add a new dial plan.

Add new Dial Plan

Add new Dial Plan

Identity:
Simple name:

Description:
External Access Prefix:

Normalization Rules

Select a Rule:

Name	Pattern	Translation	IsIn...

Save

2. Enter the relevant information, select the Normalization rules that you wish to assign to the dial plan, and then click **Save**.

Add new Dial Plan

Add new Dial Plan

Identity:
Simple name:

Description:
External Access Prefix:

Normalization Rules

Select a Rule:

Name	Name	Pattern	Translation
	NR1Test	$^9(\backslash d\{5\backslash d+\})\$$	+9723\$1
	AustRule	$^(\backslash d\{5,\})\$$	613\$1

Add new Dial Plan

Add new Dial Plan

Identity:
Simple name:

Description:
External Access Prefix:

Normalization Rules

Select a Rule:

Name	Pattern	Translation	IsIn...	
NR1Test	$^9(\backslash d\{5\backslash d+\})\$$	+9723\$1	false	

Save

If multiple rules exist, you can change their order of priority by either using the green arrow



buttons or by dragging-and-dropping, by placing one rule above or below another.

Add new Dial Plan

Add new Dial Plan

Identity:

Description:

Simple name:

External Access Prefix:

Normalization Rules

Select a Rule: AustRule

Name	Pattern	Translation	IsIn...	
AustRule	^\d{5,})\$	+613\$1	false	
NR1Test	^9(\d{5\d+})\$	+9723\$1	false	

Save

➤ To add Normalization rules to an existing dial plan:

1. Select the relevant dial plan.
2. Right-click the selection and then select **Edit**.

Dial Plans
Normalization Rule Templates
PSTN Gateways
PSTN Usage
Voice Routes
Voice Routing Policies

Add New Plan

DataChangeType	Identity	Simple Name	Description	External Prefix	Last Replication
	Global	DefaultTenantDialPlan			
	NR1	NR1	NR1		

Edit
Delete
Cancel changes

1
1 - 2 of 2 items

3. In the Edit Dial Plan dialog, select the Normalization Rules that you wish to assign to the dial plan., and then click **Save**.

Edit Dial Plan




Edit Dial Plan

Identity:
Simple name:

Description:
External Access Prefix:



Normalization Rules

Select a Rule:

Name	Pattern	Translation	IsIn...	
NR1Test	$\wedge 9(\backslash d\{5\backslash d+\})\$$	+9723\$1		  

Save

If multiple rules exist, you can change their order of priority by either using the green arrow

buttons   or by dragging-and-dropping, by placing one rule above or below another.

Add new Dial Plan







Add new Dial Plan

Identity:
Simple name:

Description:
External Access Prefix:

Normalization Rules

Select a Rule:

Name	Pattern	Translation	IsIn...	
AustRule	$\wedge(\backslash d\{5,\})\$$	+613\$1	false	  
NR1Test	$\wedge 9(\backslash d\{5\backslash d+\})\$$	+9723\$1	false	  

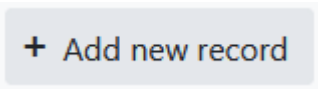
Save

Reserving Customer Phone Numbers

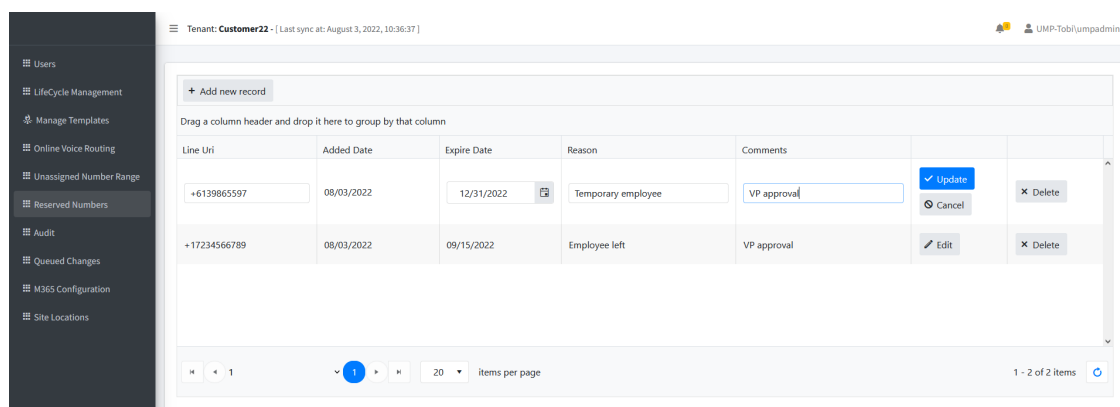
You can reserve a phone number from the DID Range to assign to a specific user. When the phone number is reserved, it is not prevented from allocation in the automatic assignment. This functionality can be used when you wish to reserve the number for future use.

➤ To configure a reserved number range:

1. In the Customer portal Navigation pane, select **Reserved Numbers**. The reserved numbers are displayed.

2. Click  to add a new record.

3. Add the required fields and click  to add the new record.







Tenant: **Customer22** - [Last sync at: August 3, 2022, 10:36:37]

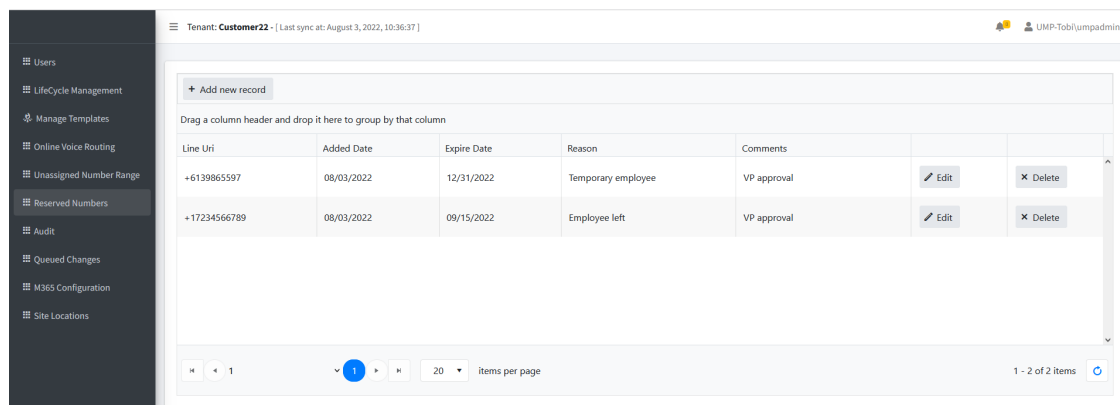
UMP-Tobi\umpadmin

+ Add new record

Drag a column header and drop it here to group by that column

Line Uri	Added Date	Expire Date	Reason	Comments		
+6139865597	08/03/2022	12/31/2022	Temporary employee	VP approval		
+17234566789	08/03/2022	09/15/2022	Employee left	VP approval		

1 - 2 of 2 items







Tenant: **Customer22** - [Last sync at: August 3, 2022, 10:36:37]

UMP-Tobi\umpadmin

+ Add new record

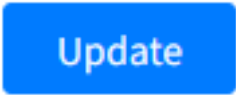
Drag a column header and drop it here to group by that column

Line Uri	Added Date	Expire Date	Reason	Comments		
+6139865597	08/03/2022	12/31/2022	Temporary employee	VP approval		
+17234566789	08/03/2022	09/15/2022	Employee left	VP approval		

1 - 2 of 2 items

Viewing Audit and Roll Back Historical Updates

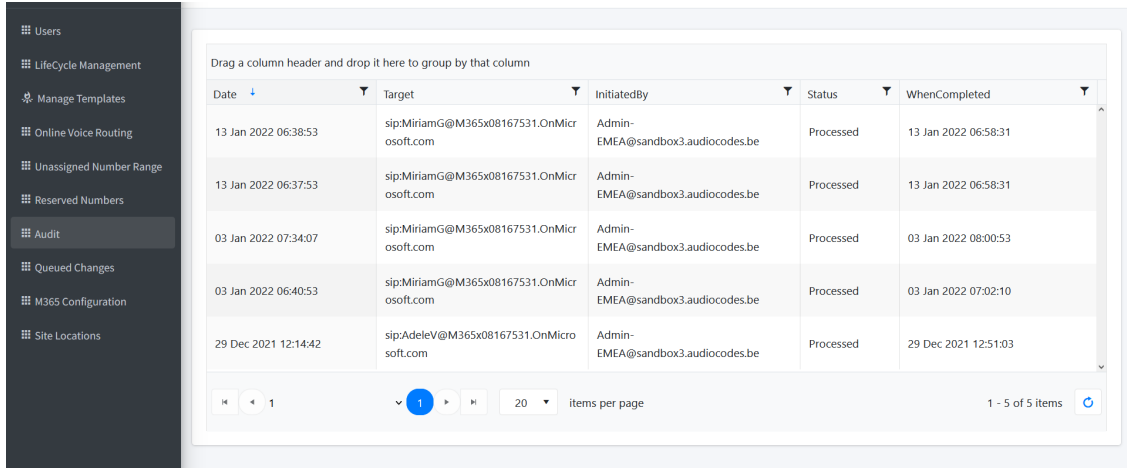
User Management Pack™ 365 SP Edition Customer Portal includes tracking for changes made by administrators. Under Audit, all changes performed are shown and can be reverted by right clicking a line. If multiple changes were performed in one action, a list of the changes, where the appropriate change can be selected. Select the entry for the change that you wish to



rollback and click  to roll back to the previous value.

➤ **To view audit history and perform rollback:**

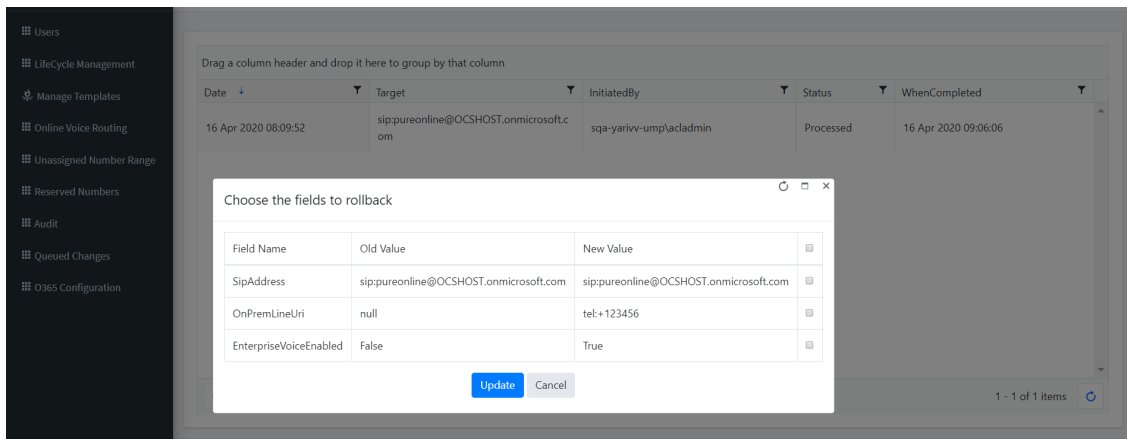
1. In the Customer portal Navigation pane, select **Audit**. The Audit History is displayed.



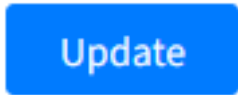
Date	Target	InitiatedBy	Status	WhenCompleted
13 Jan 2022 06:38:53	sip:MiriamG@M365x08167531.OnMicrosoft.com	Admin-EMEA@sandbox3.audiocodes.be	Processed	13 Jan 2022 06:58:31
13 Jan 2022 06:37:53	sip:MiriamG@M365x08167531.OnMicrosoft.com	Admin-EMEA@sandbox3.audiocodes.be	Processed	13 Jan 2022 06:58:31
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

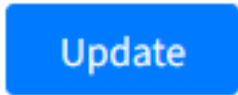


2. Right-click an entry, and then click  to undo the policy update for the selected user.



Field Name	Old Value	New Value
SipAddress	sip:pureonline@OCSTHOST.onmicrosoft.com	sip:pureonline@OCSTHOST.onmicrosoft.com
OnPremLineUri	null	tel:+123456
EnterpriseVoiceEnabled	False	True



3. Choose the specific fields that you want to rollback and then click .

Monitoring M365 Replication Actions Queue

You can view the a list of all actions processed by User Management Pack™ 365 SP Edition including those that have been executed and those in waiting. Queued tasks are executed by

the Background Replication process.

➤ **To view queued changes:**

1. In the Customer portal Navigation pane, select **Queued Changes**. A list of updates is displayed.

Id...	SipAddress	Cmd ...	Queued Change	Execu...	Execution...	When Created	When Updated
5538	sip:DiegoS@M365x08167531.O nMicrosoft.com	Office 365	Grant-CsTeamsappSetupPolicy -PolicyName \$null -Identity 'sip:DiegoS@M365x08167531. OnMicrosoft.com';	New	-	18 Jan 2022 20:52:41	-
5537	sip:DiegoS@M365x08167531.O nMicrosoft.com	Office 365	Grant-CsTeamsSurvivableBranchAppli ancePolicy -Identity 'sip:DiegoS@M365x08167531. OnMicrosoft.com' -PolicyName \$null;	New	-	18 Jan 2022 20:52:41	-
5536	sip:DiegoS@M365x08167531.O nMicrosoft.com	Office 365	Grant-CsTeamscomplianceRecordingP olicy -PolicyName \$null -Identity	New	-	18 Jan 2022 20:52:41	-

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.

Id	SipAddress	Cmd ...	Queued Change	Execu...	Execution...	When Created...	When Update...
76	sip:auto24@audio-codes.co.il	Office3 65	Grant- CsOnlineVoiceroutingPolicy -Identity 'sip:auto24@audio- codes.co.il' -PolicyName 'Unrestricted';	Ok	-	22 Mar 2021 14:44:00	22 Mar 2021 14:44:14
75	sip:auto24@audio-codes.co.il	Office3 65	Grant- CsOnlineVoiceroutingPolicy -Identity 'sip:auto24@audio- codes.co.il' -PolicyName 'Unrestricted';			21 Mar 2021 21:17:06	21 Mar 2021 21:17:23
74	sip:auto24@audio-codes.co.il	Office3 65	Grant- CsOnlineVoiceroutingPolicy -Identity 'sip:auto24@audio- codes.co.il' -PolicyName 'Unrestricted';	Ok	-	21 Mar 2021 18:17:05	21 Mar 2021 18:17:22

The table below describes the details for each task.

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

Parameter	Description
	example, Cleanup SBC or tenant remove.
State	<p>One of the following:</p> <ul style="list-style-type: none"> ■ Queued: Task is in the waiting queue for processing. ■ Reserved: Task has been reserved for processing. ■ Executing: Task is currently being executed. ■ Finish Success: Task has been completed successfully. ■ Finish Failure: Task has not been completed successfully. ■ Queue Postponed: Queue has been postponed because the customer is currently upgrading to either Hosted Essentials+ or Hosted Pro. ■ Draft: The customer creation is still in progress.
Retries	Indicates the number of retry attempts to process the task.
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.

The table below describes the Toolbar.

Show all	Show executed	Show new	Process all	Delete selected	Delete all	Queued commands: unknown Executing commands: unknown
----------	---------------	----------	-------------	-----------------	------------	---

Action	Description
Show All	Displays all queue jobs including both executed and non-executed.
Show Executed	Displays all executed queue jobs.

Action	Description
Show New	Displays the latest queue jobs.
Process All	Process all jobs in the queue.
Delete Selected	Deletes selected queue jobs.
Delete All	Delete all queue actions.
Queued Commands (Read-only)	Lists the number of commands that are in the queue waiting to be processed.
Executing Commands (Read-only)	Lists the number of commands that are currently executing.

Securing Microsoft 365 Service Provider Access

The Microsoft 365 Settings screen configures the Service Provider access to the customer's Microsoft 365 platform. Access is required by the Service Provider for initial onboarding and for Day Two management. Access is secured using token-based authentication. The token is generated upon customer consent to access their Microsoft 365 platform. In Day One Onboarding, customers are onboarded either by providing their username and password to the Service Provider or by Token authentication only triggered by an email link sent to the Customer administrator (see [Request Consent from End Customer](#) on page 364). In Day Two, the authentication method can be changed as follows:

- **Username and Password:** Using this option, the connection is secured using both the provided username and password and a Microsoft Graph access token that is claimed based on the configured user name and password. For implementing this option, select the **Grant Consent** option in the Microsoft 365 Settings screen (see [Grant Consent](#) on page 514). This option is relevant for the following scenarios:
 - Customers onboarded prior to version 8.0.450 with M365 user and password authentication must upgrade to use Token based authentication as a result of enhanced Microsoft Security policies.
 - Customers decide to switch from Token-based authentication to Password-based authentication (see [Switching to User Password](#) on page 525), then they must **Grant Consent** again to generate a **new** token based on the username and password.
- **Token-only:** Using this option, the connection is secured using only Token-based authentication (see [Switching to Token Authentication](#) on page 519). This is the **recommended** method.

Server-side GetCsOnlineUser filters can be configured in the UMP-365 database to enhance database performance. For example, a global corporation has 50,000 worldwide users and a

filter is configured to only retrieve users in the Italy office e.g. 5000 users. See [Get-CsOnlineUser \(Microsoft Teams PowerShell\)](#) on the next page.

➤ **To configure Microsoft 365 settings:**


1. In the Customer portal Navigation pane, select **M365 Configuration**.

The screenshot displays the 'Microsoft 365 Settings' configuration page. On the left is a navigation pane with options like LifeCycle Management, Manage Templates, Online Voice Routing, Network Topology, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration (selected), Site Locations, and UMP License. The main content area has a teal header 'Microsoft 365 Settings' and a status bar 'Last Authentication Status: Never Performed.' Below this are input fields for 'User Name' (containing 'admin@M365x12380949.onmicrosoft.com'), 'Password (Password already set)', and 'Confirm password'. A 'Validate Authentication' section contains three buttons: 'Save Microsoft365 settings', 'Switch to auth token', and 'Grant Consent'. At the bottom, there is a 'CsOnlineUser Filter' section with a large text area and 'Save Filters' and 'Clear Filters' buttons.

2. Configuration the Microsoft 365 credentials as described in the table below.

Table 32-2: Microsoft 365 Settings

Parameter	Description
Username	Microsoft 365 UC Admin User that was configured for the Background Replication Processing (see Configuring Microsoft Teams Direct Routing SBC on page 86)
Password	Microsoft 365 UC Admin Password.
Validate Authentication	Validates the user credentials.
Save Office 365 settings	Saves the settings updated in this screen.
Switch to auth token	Enables customer authentication by sending link to customer IT administrator for authentication (see Switching to Token Authentication on page 519).
Grant Consent	Enables customer to automatically grant consent to Service Provider administrator.

Parameter	Description
	 For using this feature, Ensure that the Client Id of the Token Authentication Registration is configured in the Authentication Status screen (see Authentication Status on page 228).
Filters	Get-CsOnlineUser: Get-CsOnlineUser (Microsoft Teams PowerShell) below

Get-CsOnlineUser (Microsoft Teams PowerShell)

Get-CsOnlineUser PowerShell queries can be applied directly in the UMP-365 database. Filter statement rules are enforced according to Teams PowerShell Modules version 3.0 or later. Filters are defined in the dbo.ApplicationSettings table. See examples in the table below. For more information, see [Get-CsOnlineUser](#).

Table 32-3: Get-CsOnlineUser Filters

MS-SQL ID	MS-SQL Value (PowerShell Command Line Syntax)	Action
O365CsOnlineUsersFilter	<pre>Department -eq 'Marketing'</pre>	Retrieves users for a specific department
O365CsOnlineUsersFilter	<pre>AssignedPlan -eq 'MCOEV' -and Country -eq 'France'</pre>	Retrieves users for specific Microsoft Service Plan in specific country.
O365CsOnlineUsersFilter	<pre>Identity "sip:brad@finebak.com"</pre>	Retrieves a specific user.
O365CsOnlineUsersFilter	<pre>UsageLocation -eq 'Rotterdam' "</pre>	Filter only online users who have been assigned the per-user archiving policy

MS-SQL ID	MS-SQL Value (PowerShell Command Line Syntax)	Action
O365CsOnlineUsersFilter	<div>LineURI -eq "tel:+1234"</div> <div>LineURI -eq "tel:+1234,ext:"</div> <div>LineURI -eq "1234"</div>	Retrieves information for user accounts that have been assigned a specific phone number.
O365CsOnlineUsersFilter	EnterpriseVoiceEnabled -eq \$True'	Retrieve only users enabled with Enterprise Voice.
O365CsOnlineUsersFilter	UsageLocation -eq 'Rotterdam' "	Retrieve users for a specific location.

The screenshot displays the SQL Server Enterprise Manager interface. On the left, the Object Explorer shows the database structure, with 'SysAdminjvmdach' and 'dbo.ApplicationSetting' highlighted. The main pane shows the results of a SQL query, which includes a table with two columns: 'Id' and 'Value'. The row corresponding to 'O365.CsOnlineUsersFilter' is highlighted, showing the value 'Department -eq 'Marketing''.

Grant Consent

The **Grant Consent** option enables you to implement Token-based authentication based on existing user name and password. A permission request is sent to the customer "Global" administrator to access the customer Microsoft 365 platform.

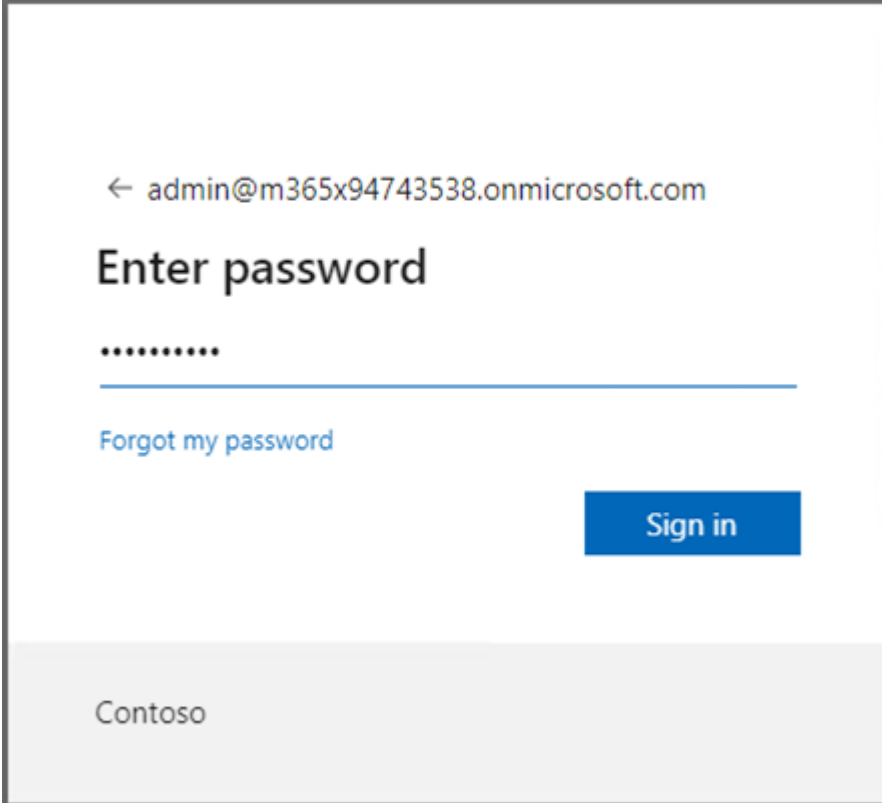


Customers onboarded prior to version 8.0.450 with M365 user and password authentication must upgrade to use Token based authentication as a result of enhanced Microsoft Security policies.

➤ **To secure Token-based connection with Grant Consent:**

1. In the Customer portal Navigation pane, select **M365 Configuration**.

2. Click **Grant Consent**.




The screenshot shows a web interface for signing into a Microsoft 365 tenant. At the top, there is a back arrow and the email address 'admin@m365x94743538.onmicrosoft.com'. Below this is the heading 'Enter password'. A password field is shown with eight dots. Underneath the password field is a blue link that says 'Forgot my password'. To the right of the password field is a blue button labeled 'Sign in'. At the bottom of the page, the word 'Contoso' is displayed in a light gray bar.

- a. Enter customer IT Administrator credentials with "Global" Admin permissions.



The M365 User Account must have "Global" Admin permissions, otherwise the "Consent on behalf of the organization" check box does not appear.



admin@m365x94743538.onmicrosoft.com

Permissions requested

Warrick_Token_Background_Replication
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to
- ☒ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

CancelAccept

- b. Click "Consent on behalf of your organization" and then click **Accept**.

Once the process has completed successfully, the following confirmation is displayed:

Thank you!

You may close this window

Service provider will contact you when service is ready for operation

audiocodes Thank you!

You may close this window

Service provider will contact you when service is ready for operation

Microsoft Azure

Home > Contoso > Enterprise applications > Enterprise applications | All applications > Warrick_Token_Background_Replication

Warrick_Token_Background_Replication | Permissions

Overview Deployment Plan Diagnose and solve problems Manage Properties Owners Roles and administrators Users and groups Single sign-on Provisioning Self-service Custom security attributes (Preview) Security Conditional Access Permissions Token encryption Activity Sign-in logs Usage & insights Audit logs Provisioning logs Access reviews Troubleshooting + Support

Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application. [Learn more](#).

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

[Grant admin consent for Contoso](#)

Admin consent User consent

Search permissions

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph					
Microsoft Graph	Group.ReadWrite.All	Read and write all groups	Delegated	Admin consent	An administrator
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed in user	Delegated	Admin consent	An administrator
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated	Admin consent	An administrator
Microsoft Graph	AppCatalog.ReadWrite.All	Read and write to all app catalogs	Delegated	Admin consent	An administrator
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	Admin consent	An administrator
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Skype and Teams Tenant Admin API					
Skype and Teams Tenant Admin API	user_impersonation	Access Microsoft Teams and Skype for Business data as the signed in user	Delegated	Admin consent	An administrator

Microsoft Azure

Home > Contoso > Enterprise applications > Enterprise applications

Enterprise applications | All applications

Overview Overview Diagnose and solve problems Manage All applications Application proxy User settings App launchers Custom authentication extensions (Preview) Security Conditional Access Consent and permissions Activity Sign-in logs Usage & insights Audit logs Provisioning logs Access reviews Admin consent requests Bulk operation results Troubleshooting + Support New support request

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

Application type == Enterprise Applications Application ID starts with Add filters

1 application found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status
Warrick_Token_Background_Replicat...	e4c42766-9690-45c4-89ad-e4ee9545931	102a2c19-9495-430e-9cdf-9ad33d93e560		4/19/2023	-

Switching to Token Authentication

Customer consent for securing Service Provider access to their Microsoft 365 platform can be secured using **only** Microsoft Graph Token-based authentication.



This is recommended method for securing connection to Microsoft 365.

➤ **To switch to token authentication:**

1. In the Customer portal Navigation pane, select **Microsoft 365 Settings**.
2. Click **Validate Authentication** to ensure current token is valid. Last Authentication Status: Successful is displayed.

3. In the **Microsoft 365 Settings** screen, click **Switch to auth token**.

The following dialog is displayed.

4. Enter the email address of the customer administrator to whom you wish to send the invitation.

The following confirmation screen is displayed showing the invitation sent to the customer IT administrator from the Service Provider IT administrator.

Microsoft 365 Settings

Tenant has open invitation.

User Name
admin@M365x74218585.onmicrosoft.com

There is at least one Authentication Invitation sent to test@gmail.com, please go to customer portal as stated in the email or click [here](#).

Switch to user/pwd Resend invitation

Save Microsoft365 settings

- In the Main Tenant interface, open the Customer Invitations screen (see [Customer Invitations](#) on page 225) View the Customer Invitation sent to the email address entered above.

Customer Invitations

Reload data Edit

Search:

ID	Full Name	Invitation Email	M365 Admin Email	Email Sent	Email Invitation Sent Count	Created at	Expires at	Device Authenticated	Tenant Installed	Actions
20220823	20220823	test@gmail.com	admin@M365x74218585.onmicrosoft.com	true	1	2022-08-29	2022-09-03		Yes	Send Reminder Revoke Request Auth URL

Showing 1 to 1 of 1 entries

Previous 1 Next

An email similar to the following is sent to the customer administrator.

<onboarding@audiocodes.be> בתאריך: 24 באפריל 2023, 18:13

Dear Administrator of BradSIP,

We at Sandbox3.FineBak welcomes you to join our "AudioCodes Live Cloud" service.

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

http://url1207.audiocodes.be/ls/click?on=a12WafR444P7.2B7DSb5PxErMoe1UbCLZS.2BkTVwInmXwDap5D33qLeRR5p7ZuQRBqJIDwChScjKnlXdtGMMKIPX.2FF3UFVBEKEDCHIAMZDzhnrOkKYuum9xudKobc2py_JSLV81wauxhQzQz3qQH4HXCL.2FonCqkofH5.2BmleXrgQH7NmITNB0T86eR.2Bof35teoWaxVUQqRBp8ApoXaATCHAq8.2B##af-2BEEhGCoDX.2Bxmgy5wQxcB9DAAdAnyQJ42lrmS9GTOMDVGradmyG8xPDrexbtIws7gq7pXSCdDEC8FWcolbnGUs4Fdc5RlkXvS.2BQz65.2FB9C28y9hsWz8kCHIElmt5.2BcaFqA.3D

Please Note that Global Admin will be required in order to approve the LiveCloud consents.

- 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,

Sandbox3.FineBak Team

- Click the link sent in the mail to start the authentication process.

Welcome BradSIP

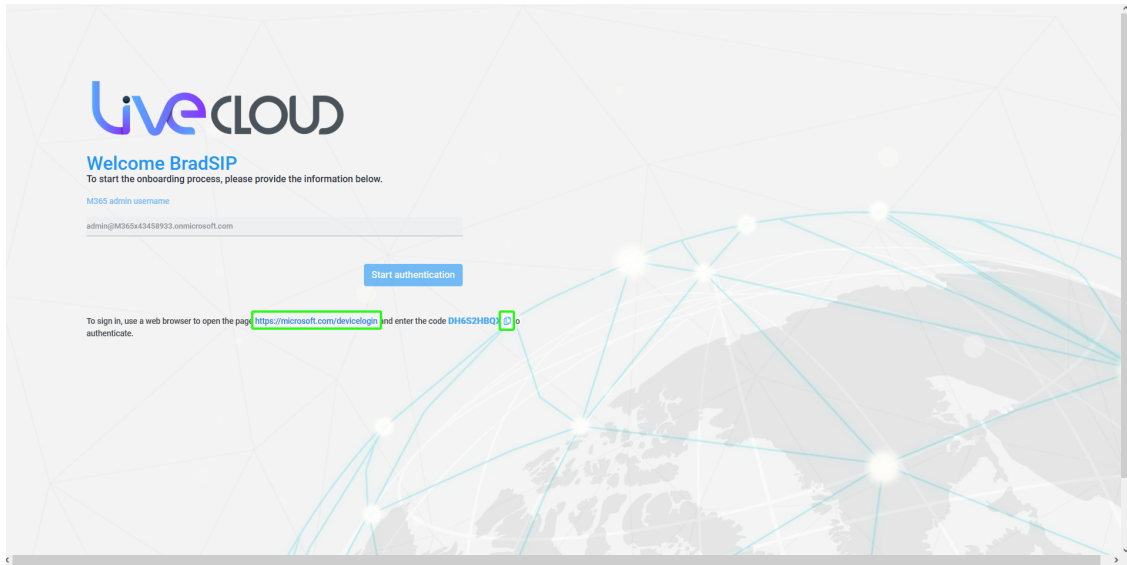
To start the onboarding process, please provide the information below.

M365 admin username

admin@M365x43489933.onmicrosoft.com

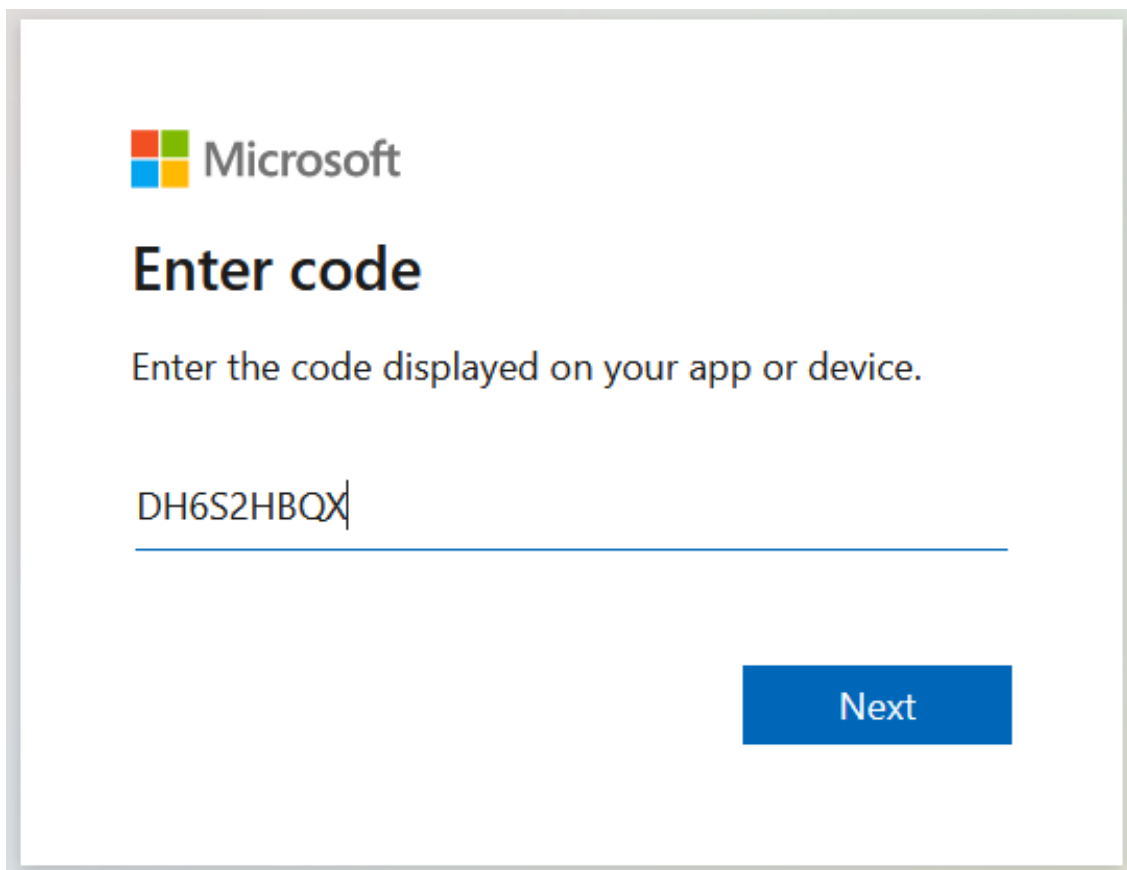
Start authentication

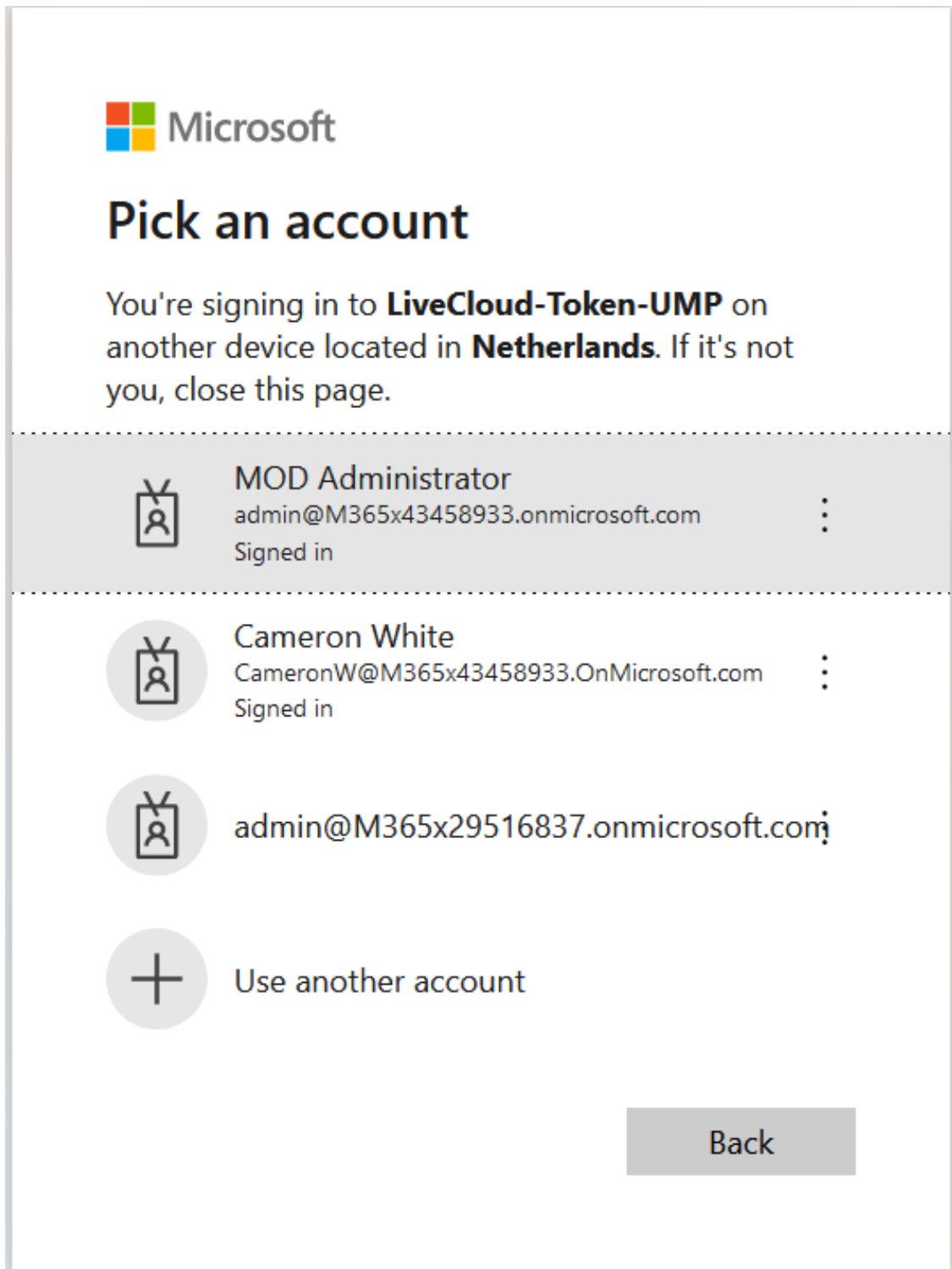
7. Click **Start authentication**.



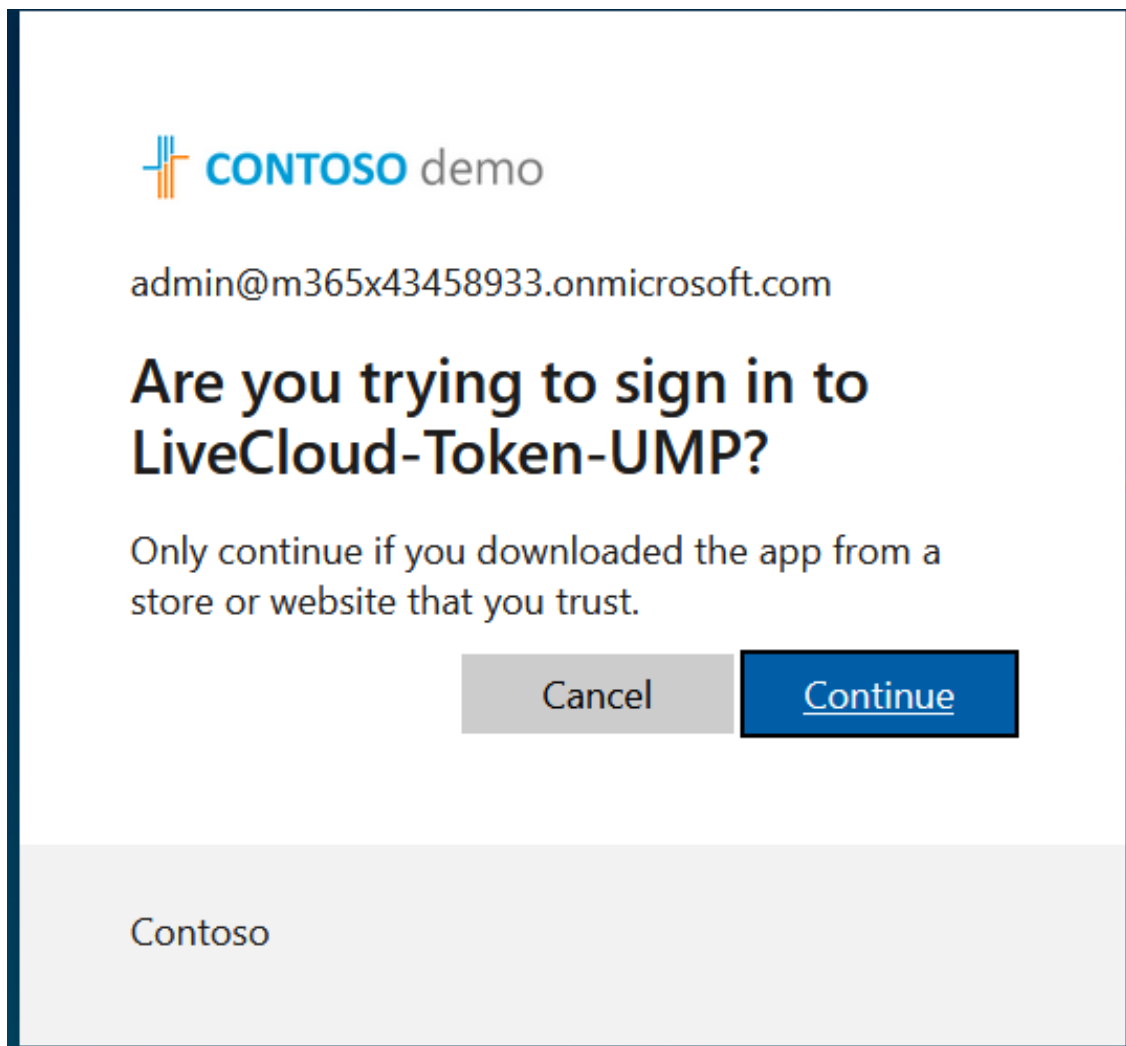
8. Copy the displayed code to clipboard.

9. Open the web browser link shown below the **Start authentication** button.

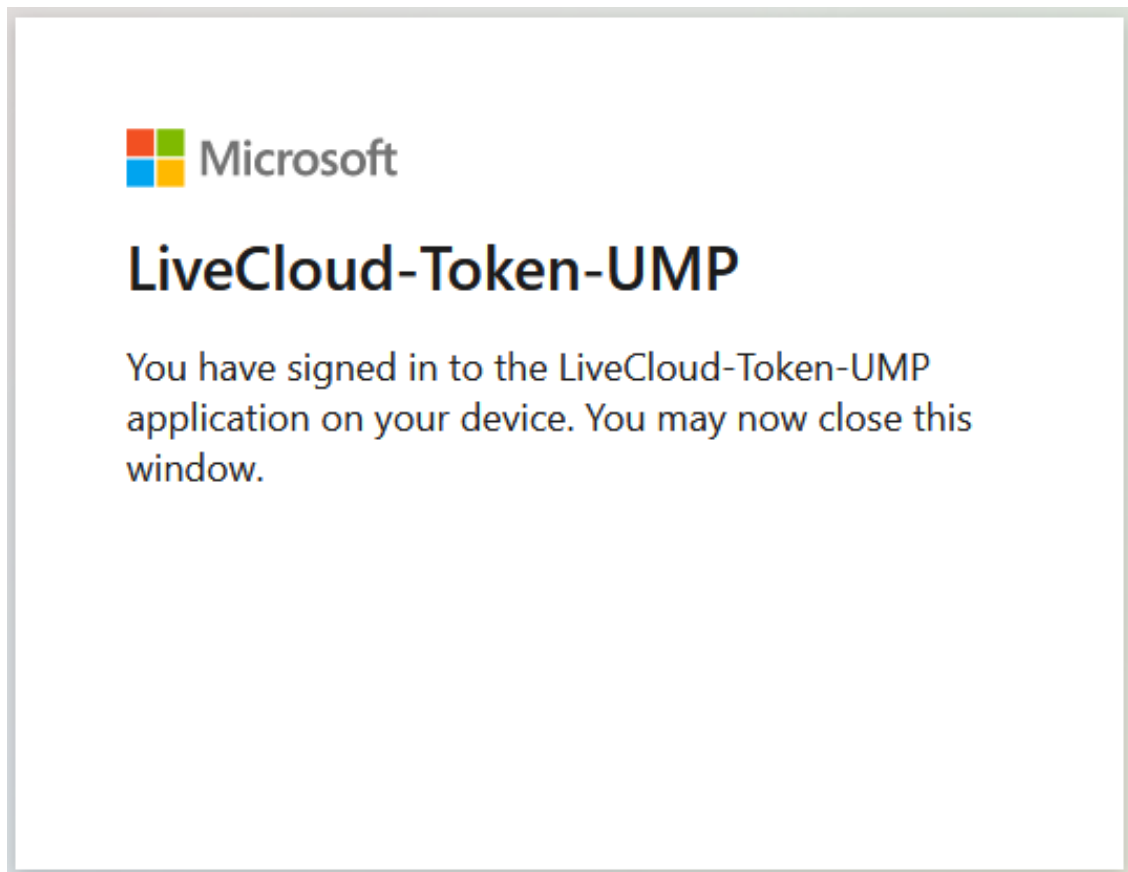




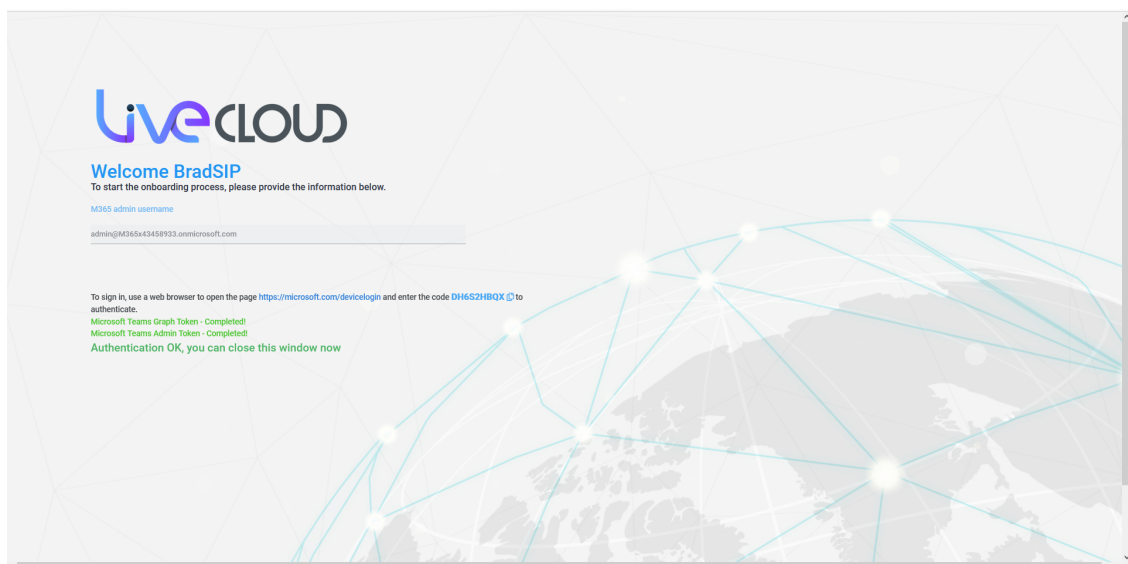
10. Choose the account of the customer tenant administrator with "Global" permissions.



11. Click **Continue**.



12. Close the above window. The confirmation of the completion of the authentication process is displayed.



13. Close the above window.
14. Return to the **Microsoft 365 Settings** screen. Note that "Authentication Status: Successful" is displayed and that the **Switch to user/pwd** button is displayed.

Microsoft 365 Settings

Last Authentication Status: Successful.

User Name
 admin@M365x43458933.onmicrosoft.com

The customer is configured to use Authentication Token, password is not needed.

Validate Authentication

Save Microsoft365 settings: **Switch to user/pwd**

QOE Integration with Microsoft Teams

Azure Application Id

Azure Application Password

Save QOE Integration settings

CsOnlineUser Filter

15. In the Main Tenant interface, open the Customer Invitations screen (see [Customer Invitations](#) on page 225, view the "Created at" and "Expires at" of the claimed token.

Customer Invitations

Reload data Edit

Search:

ID	Full Name	Invitation Email	M365 Admin Email	Email Sent	Email Invitation Sent Count	Created at	Expires at	Device Authenticated	Invitation Type	Tenant Installed
BradConnect	BradConnect	Brconnect@gmail.com		true	1	2023-04-24	2023-04-29		Invite	No
BradSIP	BradSIP	BradSIP@gmail.com	admin@M365x43458933.onmicrosoft.com	true	1	2023-04-24	2023-04-29	true	Request	No
BradTrunk2	BradTrunk2	BradTrunk2@gmail.com		true	1	2023-04-20	2023-04-25		Invite	No
SinhaCnslt	Ranjan Consulting	acenterprise.demo1@gmail.com	admin@M365x434560539.onmicrosoft.com	true	1	2023-04-19	2023-04-24	true	Invite	No

Switching to User Password

This section describes how to switch from Token authentication to user and password authentication. Once the new username and password are defined and validated, consent must be granted to the Service Provider administrator for the implementation of token-based authentication. The token is claimed based on the configured user name and password.

➤ To switch to user name and password:

1. In the Customer portal Navigation pane, select **Microsoft 365 Settings**.
2. Click **Validate Authentication** to ensure the current Token is valid. Last Authentication Status: Successful is displayed.

OC audiocodes

Tenant: TxM365x74860876 - [Last sync at: April 20, 2023, 16:44:32]

WIN-RPC33131A7D\Administrator

Microsoft 365 Settings

Last Authentication Status: Successful.

User Name

alexw@M365x74860876.onmicrosoft.com

The customer is configured to use Authentication Token, password is not needed.

Validate Authentication

Save Microsoft365 settings

Switch to user/pwd

CoOnlineUser Filter

3. Click **Switch to user/pwd**.

4. Enter the desired user name and password and confirm password.

OC audiocodes

Tenant: TxM365x74860876 - [Last sync at: April 20, 2023, 16:44:32]

WIN-RPC33131A7D\Administrator

Microsoft 365 Settings

Last Authentication Status: Successful.

User Name

alexw@M365x74860876.onmicrosoft.com

Password (Password not set)

Confirm password

Validate Authentication

Save Microsoft365 settings

Switch to auth token

Grant Consent

OC audiocodes

Tenant: TxM365x74860876 - [Last sync at: April 20, 2023, 16:44:32]

WIN-RPC33131A7D\Administrator

Microsoft 365 Settings

Last Authentication Status: In Progress.

User Name

alexw@M365x74860876.onmicrosoft.com

Password (Password not set)

Confirm password

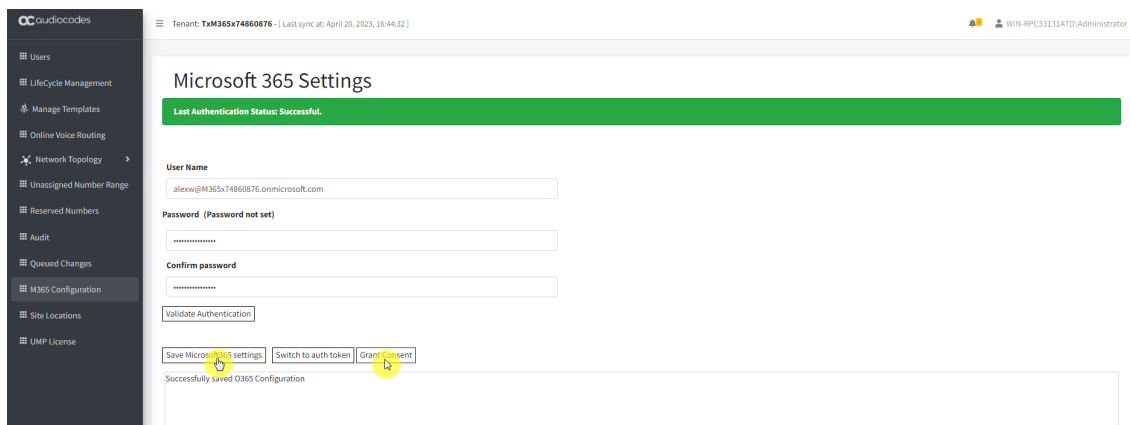
Validate Authentication

Save Microsoft365 settings

Switch to auth token

Grant Consent

5. Click **Validate Authentication**.



Microsoft 365 Settings

Last Authentication Status: Successful.

User Name
alexw@M365x74860876.onmicrosoft.com

Password (Password not set)
.....

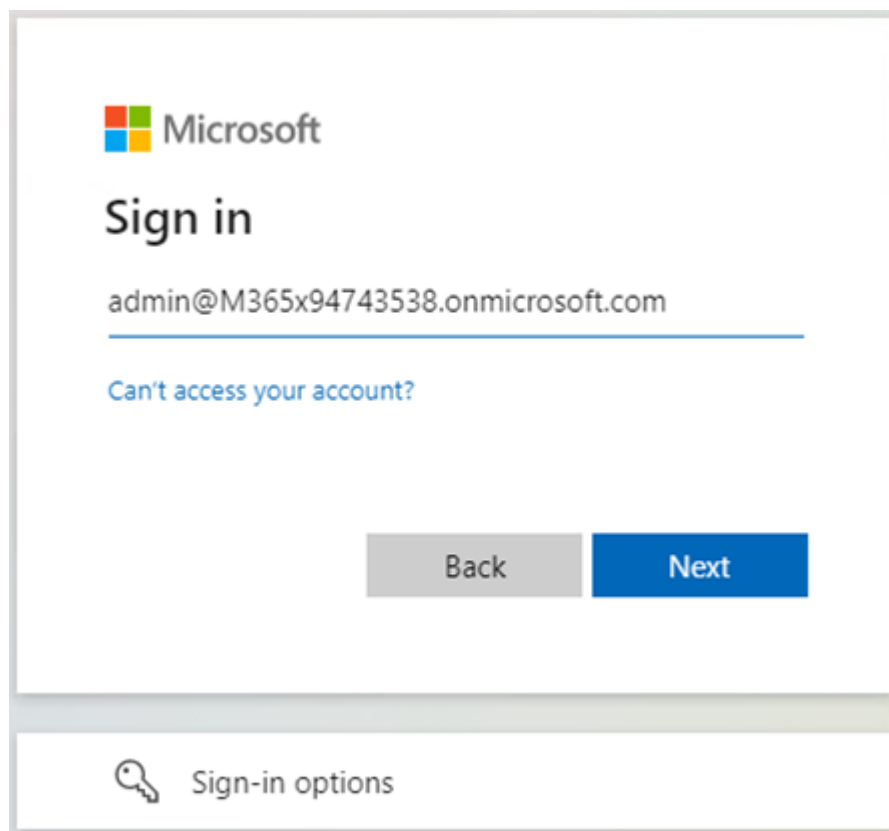
Confirm password
.....

Validate Authentication

Save Microsoft 365 settings | Switch to auth token | Grant Consent

Successfully saved O365 Configuration

6. Click **Save Microsoft 365 Settings** and then click **Grant Consent**.



Microsoft

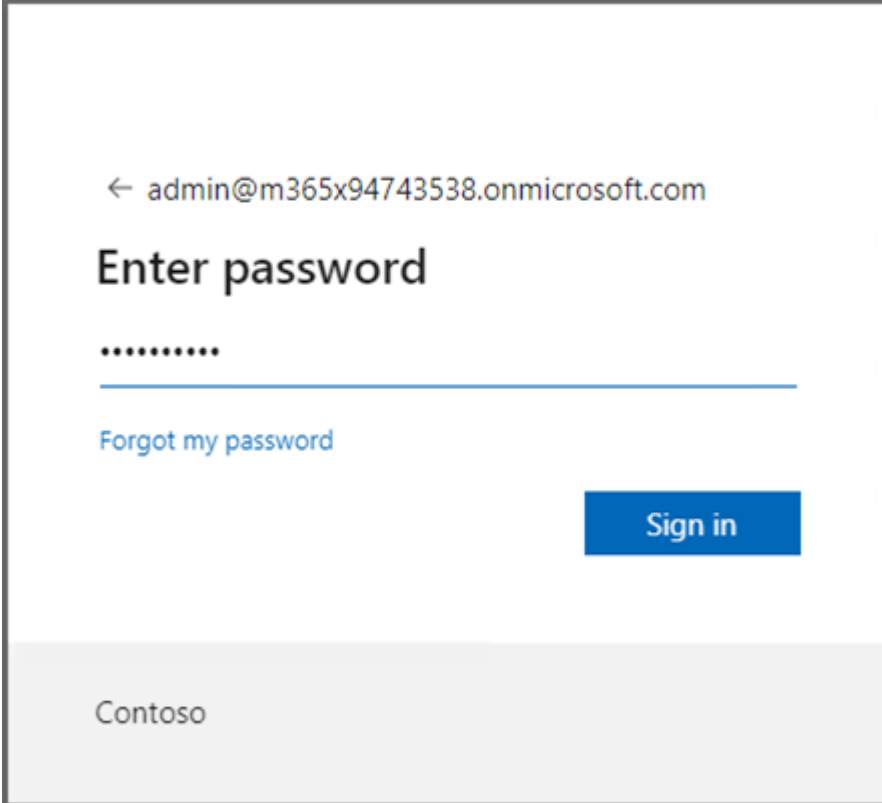
Sign in

admin@M365x94743538.onmicrosoft.com

Can't access your account?

Back Next

Sign-in options




The screenshot shows a web interface for signing into a Microsoft 365 tenant. At the top, there is a back arrow and the email address 'admin@m365x94743538.onmicrosoft.com'. Below this is the heading 'Enter password'. A password field is shown with eight dots. Underneath the password field is a blue link that says 'Forgot my password'. To the right of the password field is a blue button labeled 'Sign in'. At the bottom of the page, the word 'Contoso' is displayed in a light gray bar.

- a. Enter customer IT Administrator credentials with Global Admin permissions.



The M365 User Account must have Global Admin permissions, otherwise the “Consent on behalf of the organization” check box does not appear.



admin@m365x94743538.onmicrosoft.com

Permissions requested

Warrick_Token_Background_Replication
unverified

This app may be risky. Only continue if you trust this app. [Learn more](#)

This app would like to:

- ✓ Access Microsoft Teams and Skype for Business data as the signed in user
- ✓ Read and write all groups
- ✓ Access directory as the signed in user
- ✓ Read all users' full profiles
- ✓ Read and write to all app catalogs
- ✓ Maintain access to data you have given it access to
- ☒ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

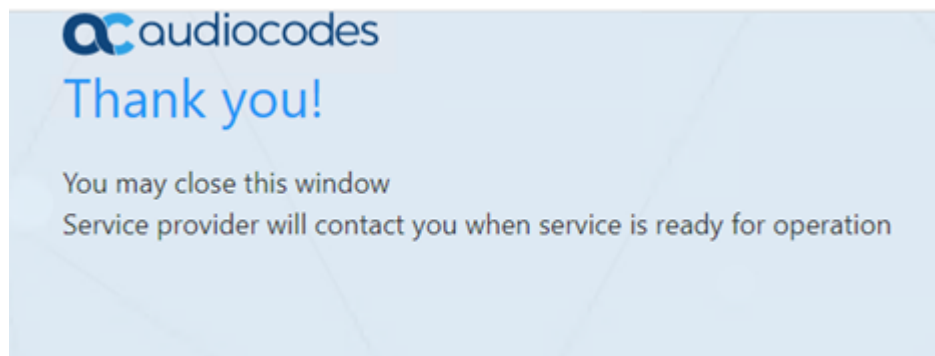
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

CancelAccept

- b. Click "Consent on behalf of your organization" and then click **Accept**.

Once the process has completed successfully, the following confirmation is displayed:



Microsoft Azure

Home > Contoso > Enterprise applications > Enterprise applications | All applications > Warrick_Token_Background_Replication

Warrick_Token_Background_Replication | Permissions

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Self-service

Custom security attributes (preview)

Security

Conditional Access

Permissions

Token encryption

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Troubleshooting + Support

Permissions

Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application. [Learn more.](#)

As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

Grant admin consent for Contoso

Admin consent

User consent

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph	Group.ReadWrite.All	Read and write all groups	Delegated	Admin consent	An administrator
Microsoft Graph	DirectoryAccessAsUser.All	Access directory as the signed in user	Delegated	Admin consent	An administrator
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated	Admin consent	An administrator
Microsoft Graph	AppCatalog.ReadWrite.All	Read and write to all app catalogs	Delegated	Admin consent	An administrator
Microsoft Graph	offline_access	Maintain access to data you have given it access to	Delegated	Admin consent	An administrator
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Skype and Teams Tenant Admin API					
Skype and Teams Tenant Admin API	user_impersonation	Access Microsoft Teams and Skype for Business data as the signed in user	Delegated	Admin consent	An administrator

Microsoft Azure

Home > Contoso > Enterprise applications > Enterprise applications

Enterprise applications | All applications

Overview

Diagnose and solve problems

Manage

All applications

Application proxy

User settings

App launchers

Custom authentication extensions (Preview)

Security

Conditional Access

Consent and permissions

Activity

Sign-in logs

Usage & insights

Audit logs

Provisioning logs

Access reviews

Admin consent requests

Bulk operation results

Troubleshooting + Support

New support request

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider. The list of applications that are maintained by your organization are in [application registrations](#).

1 application found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status
Warrick_Token_Background_Replication	e4c42766-a690-45c4-b9ad-e4eeff545931	102a2cb9-9495-430e-9c0f-9ad33693e560		4/19/2023	-

Managing Site Locations

You can add additional site locations connecting to the same or different SBC and manage the dial plans for those sites:

- Onboard additional SBC devices for new sites (see [Add SBC Site Locations](#) on the next page)
- Add and edit SBC prefixes (see [Manage SBC Prefixes](#) on page 533)

- Import PBX users (see [Import IP-PBX Users](#) on page 538)

➤ **To manage site locations:**

1. In the Multitenant portal Navigation pane, click **Site Locations**.

The table below describes the site location parameters.

Table 32-4: Site Locations

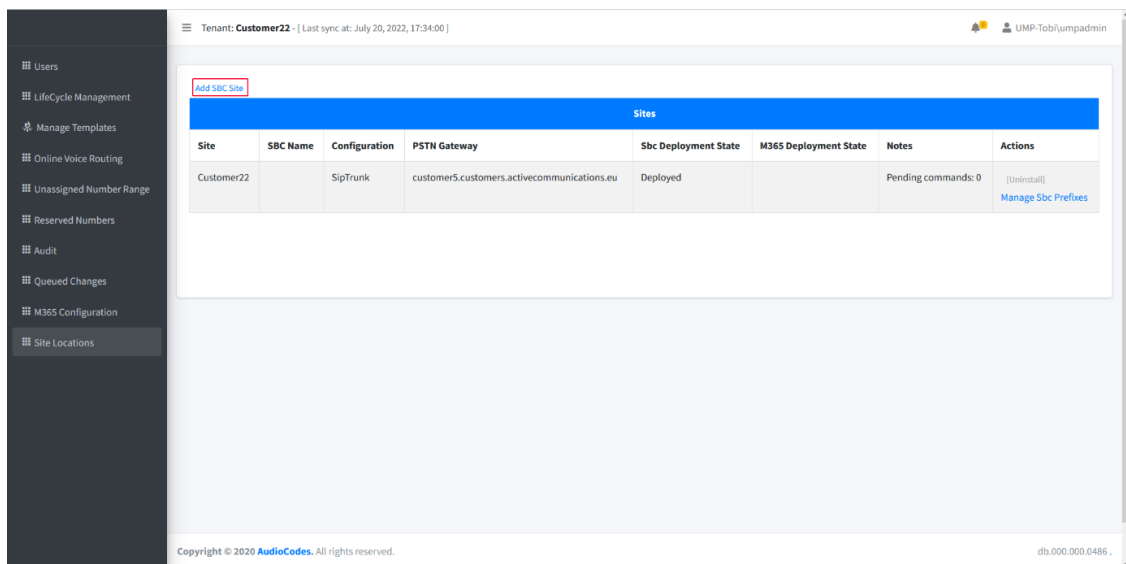
Parameter	Description
Site	FQDN of the site location.
SIP Address	IP address of the site location.
Configuration	Configuration type e.g. SIP Trunk (how is this field filled)
PSTN Gateway	PSTN Online Gateway
SbcDeploymentState	Indicates the SBC deployment state.
M365DeploymentState	Indicates the M365 deployment state.
Notes	Lists commands yet to be executed.
Actions	<p>The following actions can be performed:</p> <ul style="list-style-type: none"> ■ Add SBC Site ■ Configure SBC Prefixes ■ Import PBX users

Add SBC Site Locations

This option provides the ability to 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. In the Customer portal Navigation pane, select **Site Locations**.
2. Click **Add SBC Site** to connect an SBC device deployed in a specific site.



The screenshot shows the 'Add SBC Site' button highlighted in red. Below it is a table titled 'Sites' with the following data:

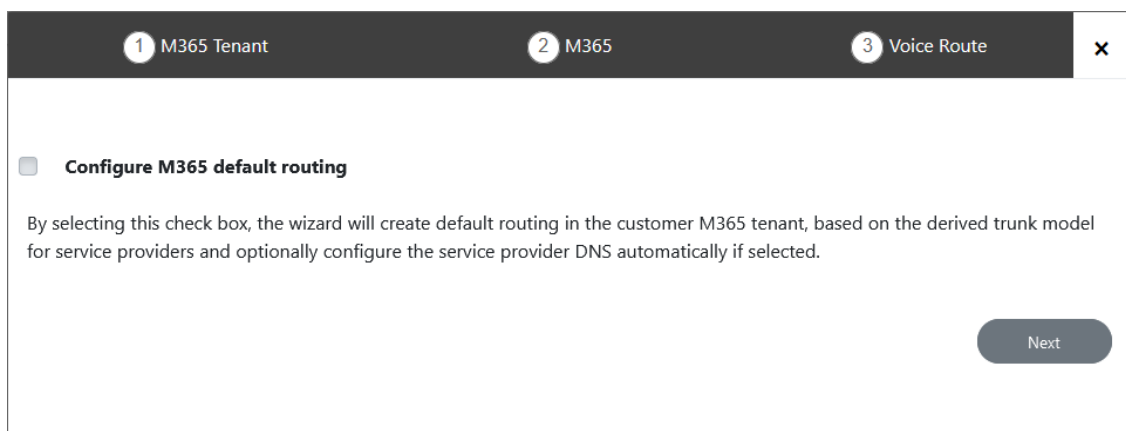
Site	SBC Name	Configuration	PSTN Gateway	Sbc Deployment State	M365 Deployment State	Notes	Actions
Customer22		SipTrunk	customer5.customers.activecommunications.eu	Deployed		Pending commands: 0	[Uninstall] Manage Sbc Prefixes

Copyright © 2020 AudioCodes. All rights reserved. db.000.000.0486



The screenshot shows the 'ADD NEW SITE PRESS NEXT' screen. The 'Next' button is visible in the bottom right corner.

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



The screenshot shows the 'Configure M365 default routing' screen. The 'Next' button is visible in the bottom right corner.

4. See [Onboarding Customers](#) on page 282 to complete the Onboarding process.
5. Once onboarded, verify that the new location is deployed.

Add SBC Site							
Sites							
Site	SBC Name	Configuration	PSTN Gateway	Sbc Deployment State	M365 Deployment State	Notes	Actions
Bradinvent78	qa-att-sbc1.customers.audio-codes.org[20.71.165.0]	SipTrunk	BradIM478Site1.customers.audio-codes.org	Deployed	Deployed	Pending commands: 0	[uninstall] Manage Sbc Prefixes
Cust78SBCSite2	qa-att-sbc2.customers.audio-codes.org[20.229.217.60]	SipTrunk	Cust78SBCSite2.customers.audio-codes.org	Deployed	Deployed	Pending commands: 0	[uninstall] Manage Sbc Prefixes

Manage SBC Prefixes

This section describes how to configure SBC dialplans for specific sites. SBC prefixes can be configured manually or can be imported from a file. A tag can be applied to each entry to associate the prefixes to a specific SBC site location. The dialplan rule does not have a unique name and instead inherits the name of the configured dialplan e.g. 'CustDialPlan'. In the CLI script, the shortname of the customer is used to match the prefix to the customer tenant and in the Dialplan configured on the SBC device, the Dial plan rule name inherits this shortname.

➤ To configure SBC dial plans:

1. Choose the site for which you wish to configure SBC prefixes, and then click **Manage SBC Prefixes**.

Add SBC Site							
Sites							
Site	SBC Name	Configuration	PSTN Gateway	Sbc Deployment State	M365 Deployment State	Notes	Actions
220914	EMEA SP1 SBC	SipTrunk	customers.activecommunications.eu	Deployed		Pending commands: 0	[uninstall] Manage Sbc Prefixes

Tenant: 220914 - [Last sync at: September 5, 2023, 15:52:32]

SBC: 7 - Location: 220914

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

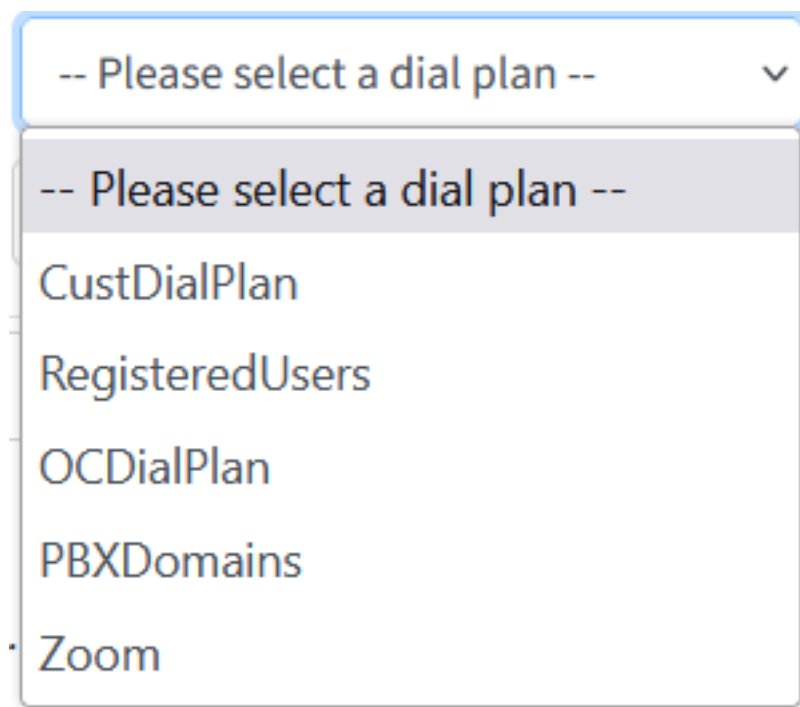
Prefixes shown below are from cache. Press **Reload** to refresh them from SBC.

Dial Plan Name	Prefix	Tag
<input type="checkbox"/> CustDialPlan	+31365461234	eu-lab-sbc.activecommunications.eu

1 - 1 of 1 items

Save

- From the Select Dial Plan drop-down, select the required dialplan. The following default dialplans can be selected:



- **CustDialPlan:** Default Dialplan for the Direct Routing customers
- **RegisteredUsers:** Dialplan used for managing IP-PBX users when an IP-PBX is configured in the Onboarding Wizard.
- **OCDialPlan:** Default Operator Connect dialing plan
- **PBXDomains:** Dialplan used for managing PBX domain customers
- **Zoom:** Dialplan used for managing Zoom customers

SBC: 2 - Location: Cellcomsiptrunk

Add additional prefixes / number ranges

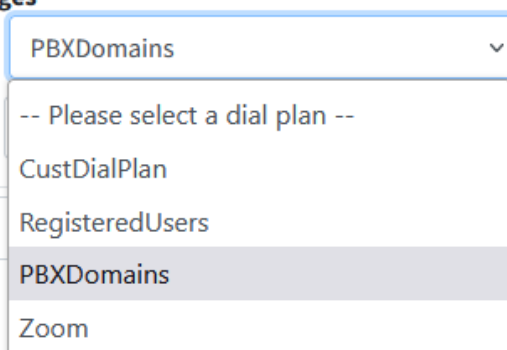
Select Dial Plan

Telephone Number Prefix

Upload from single file

Current prefixes

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



Browse

3. In the Tag/PSTN Gateway field, enter the tag 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).

Tag / PSTN Gateway

ai0logics.onmicrosoft.com
ai-logics.com


This tag may be one of the following values:

- ◆ The derived Trunk FQDN of the SBC device. Used predominantly for **Direct Routing** customers.
- ◆ The Tenant's Azure subscription ID. Used predominantly for **Operator Connect** customers.



The dialplan rule does not have a unique name and instead inherits the name of the configured dialplan 'CustDialPlan'. In the CLI script, the shortname of the customer is used to match the prefix to the customer tenant and in the Dialplan configured on the SBC device, the Dial plan rule name inherits this shortname.

4. 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 (see [Upload Dial plan to SBC](#) on the next page).

SBC: 2 - Location: aiLog

Add additional prefixes / number ranges

Select Dial Plan: CustDialPlan Tag / PSTN Gateway: ai0logics.onmicrosoft.com

Telephone Number Prefix: New Number prefix

Upload from single file: Choose file Browse

Current prefixes

Prefiles 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
<input type="checkbox"/> CustDialPlan	+564654546	ai0logics.onmicrosoft.com
<input type="checkbox"/> CustDialPlan	+972	ai0logics.onmicrosoft.com

1 - 2 of 2 items



5. Click  to apply configuration.
6. Click **Reload** to refresh the list of prefixes with the SBC device.

Current prefixes

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

Upload Dial plan to SBC

You can upload dial plans to an SBC device from an external file (*.csv). You can create the file using any text-based editor such as Notepad or Microsoft Excel. The file must be saved with the *.csv file name extension. Once imported to the UMP-365, the dial plan is also synchronized to update the Dial Plan table on the SBC device. This enables customers to manage dial plan rules directly from the UMP-365 (without the need to configure the dial plans on the SBC device).

➤ To download dial plan to SBC:

1. Configure the file in the format shown below:

```
[dialPlanName],[prefix],[tag]
```

where:

- **DialPlanName:** Name of the dial plan. This name must appear for each entry in the dial plan.
- **Prefix:** Source or destination number prefix.
- **Tag:** Result of the user categorization and can be used as matching characteristics for routing and outbound manipulation. See tag types in [Manage SBC Prefixes](#) on page 533.

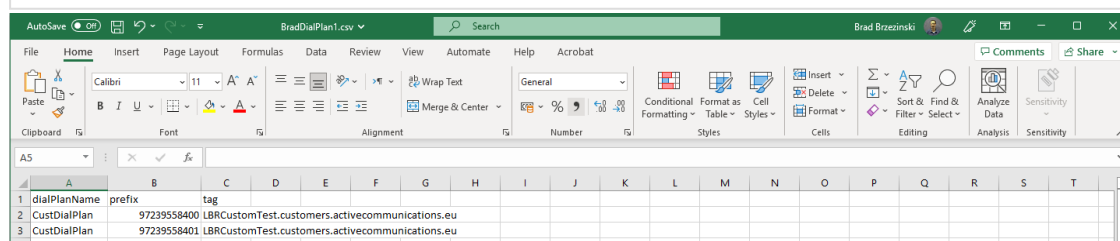
```
dialPlanName,prefix,tag
```

```
CustDialPlan,+9729004567,trnkpck01DR.customers.audiocodes.es
```

```
CustDialPlan,+9729004568,trnkpck01DR.customers.audiocodes.es
```

```
CustDialPlan,+9729004569,trnkpck01DR.customers.audiocodes.es
```

```
CustDialPlan,+9729004570,trnkpck01DR.customers.audiocodes.es
```



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	dialPlanName	prefix	tag																	
2	CustDialPlan	97239558400	LBRCustomTest.customers.activecommunications.eu																	
3	CustDialPlan	97239558401	LBRCustomTest.customers.activecommunications.eu																	
4																				

A range of numbers can be displayed as follows:

```
CustDialPlan, 551136184[4000-9999]
```



When importing a CSV file, its recommended to open the file in a text editor to ensure that the file syntax is correct (as shown in the example above). Also ensure that there are no empty lines in the file.

2. Click Browse and choose the file that you configured above.

The new entries are displayed in the lower pane.

Dial Plan Name	Prefix	Tag
<input type="checkbox"/> CustDialPlan	+123456789112345001	trnkpck01DR.customers.audio-codes.es
<input type="checkbox"/> CustDialPlan	+123456789112345002	trnkpck01DR.customers.audio-codes.es
<input type="checkbox"/> CustDialPlan	+123456789112345003	trnkpck01DR.customers.audio-codes.es
<input type="checkbox"/> CustDialPlan	+123456789112345004	trnkpck01DR.customers.audio-codes.es

Once the dialplan is imported, the new entries are displayed in the Dialplan on the SBC device with the rule name inheriting the Short Customer Name. In the example above, the customer shortname is “dr_cust_maxxch”.

INDEX	NAME	PREFIX	TAG
0	dr_cust_2_maxch	+123456789112345001	trnkpck01DR.customers.audio-codes.es
1	dr_cust_2_maxch	+123456789112345002	trnkpck01DR.customers.audio-codes.es
2	dr_cust_2_maxch	+123456789112345003	trnkpck01DR.customers.audio-codes.es
3	dr_cust_2_maxch	+123456789112345004	trnkpck01DR.customers.audio-codes.es
4	dr_cust_2_maxch	+123456789112345005	trnkpck01DR.customers.audio-codes.es
5	dr_cust_2_maxch	+123456789112345006	trnkpck01DR.customers.audio-codes.es
6	dr_cust_2_maxch	+123456789112345007	trnkpck01DR.customers.audio-codes.es
7	dr_cust_2_maxch	+123456789112345008	trnkpck01DR.customers.audio-codes.es
8	dr_cust_2_maxch	+123456789112345009	trnkpck01DR.customers.audio-codes.es
9	dr_cust_2_maxch	+123456789112345010	trnkpck01DR.customers.audio-codes.es

#0[dr_cust_2_maxch]

GENERAL	
Name	dr_cust_2_maxch
Prefix	+123456789112345001
Tag	trnkpck01DR.customers.audio-codes.es

Import IP-PBX Users

You can import a file containing a list of IP-PBX users which updates the GW User Information table on the SBC device. The users must be configured in comma-separated value (CSV) or txt file format. You can create the file using any standard text-based editor such as Notepad, or alternatively a CSV-based program such as Microsoft Excel. The file can have any filename extension (e.g., .csv or .txt).



- This feature is available for Hosted Pro licenses only.
- The imported file overwrites the existing IP-PBX user list.

➤ To 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

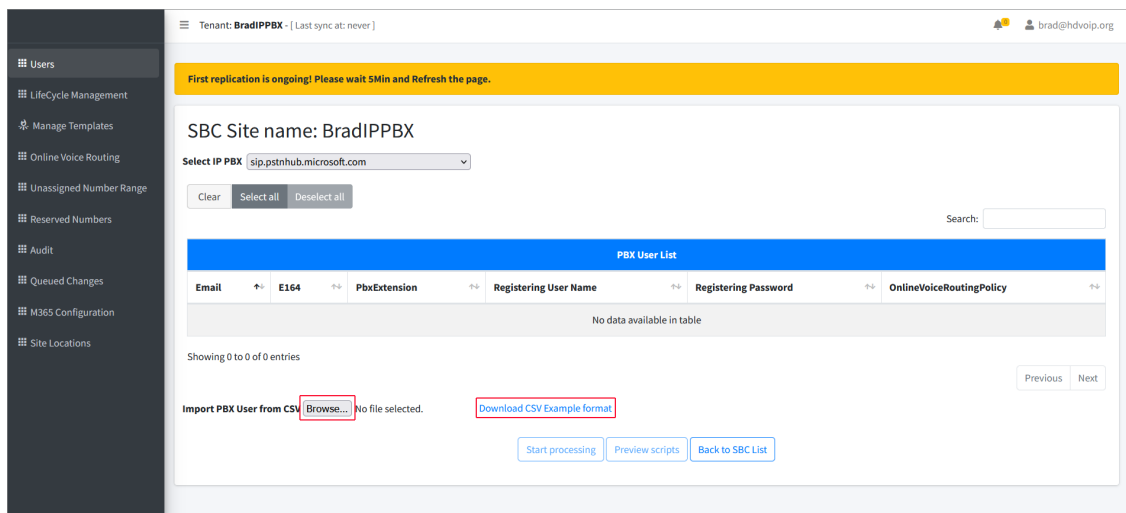
Search:

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

1. Click **Import Pbx Users**.
2. From the Select IP PBX drop-down list, select an IP-PBX to apply.



- Click the **Browse** button adjacent to the Import PBX Users from CSV link. Click **Download CSV Example format** to download an example CSV template file including the correct syntax. See example below.

Email,E164,PbxExtension,LocalUserName,RegisteringUserName,RegisteringPassword,OnlineVoiceRoutingPolicy

AlexW@M365x289401.OnMicrosoft.com,191912,222,anca1,anca2,***,Unrestricted

rani@audio-codes.biz,34000,rani,rani,****,,

bradb@audio-codes.biz,40736376,9898,Bradb,Bradb,****,,

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1																			
2	Email	E164	PbxExtension	LocalUserName	RegisteringUserName	RegisteringPassword	OnlineVoiceRoutingPolicy												
3	AlexW@M365x289401.OnMicrosoft.com	191912	222	anca1	anca2	***	Unrestricted												
4	rani@audiocodes.biz	34000	223	rani	rani	****	Restricted												
5	JohnWilber@M365x290405.OnMicrosi	20000	224	john	john	***	Unrestricted												

Once imported, the list of users are displayed in the PBX User List.

The screenshot displays the 'SBC Site name: BradIPPBX' configuration page. A dropdown menu shows 'Select IP PBX' with 'sip.pstnhub.microsoft.com' selected. Below this are 'Clear', 'Select all', and 'Deselect all' buttons. A search bar is on the right. The main section is titled 'PBX User List' and contains a table with the following data:

Email	E164	PbxExtension	LocalUserName	RegisteringUserName	RegisteringPassword	OnlineVoiceRoutingPolicy
AlexW@M365x289401.OnMicrosoft.com	191912	222	anca1	anca2	***	Unrestricted
bradb@audio-codes.biz	40736376	9898	Bradb	Bradb	*****	
rani@audio-codes.biz	34000		rani	rani	****	

Below the table, it says 'Showing 1 to 3 of 3 entries'. At the bottom, there is an 'Import PBX User from CSV' section with a 'Browse...' button and a link to 'ImportIPPBXUser.csv'. A 'Download CSV Example format' link is also present. Navigation buttons 'Previous', '1', and 'Next' are at the bottom right. At the very bottom, there are buttons for 'Start processing', 'Preview scripts', and 'Back to SBC List'.

Managing User Licenses

The UMP-365 User License screen in the Multitenant portal monitors the currently assigned user licenses for each tenant based on their purchased available license pool. Customers are then billed for license usage based on the aggregated data attributed to the configuration actions performed in Day Two upon the managed users. The following factors are used in the license calculation. (see details in table below):

- Managed Users-Direct Routing
- Managed Users-Operator Connect
- *Managed Users-By Template
- *Managed Users-By User Interface
- *Managed Service Numbers



For those factors indicated with *, Global settings can be configured by Sysadmin in the Multitenant portal (see [Configuring Global License Settings](#) on page 168).

➤ To manage user licenses:

1. In the Customer portal Navigation pane, select **UMP License**.

UMP Customer License - Audit

Last 3 months [Get History](#)

License Calculation Time	Currently Licensed	Managed Users - Direct Routing -	Managed Users - Operator Connect -	Managed Users - By Template -	Managed Users - User Interface -	Managed Service Numbers	Total Monitored Users
25 Oct 2023 03:06	19	0	0 (0)	15 (15)	3 (16)	1 (1)	20

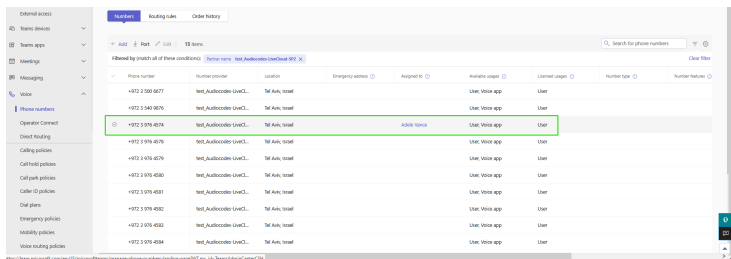
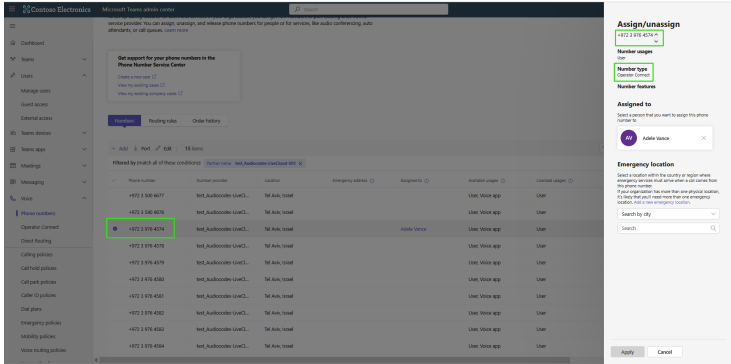
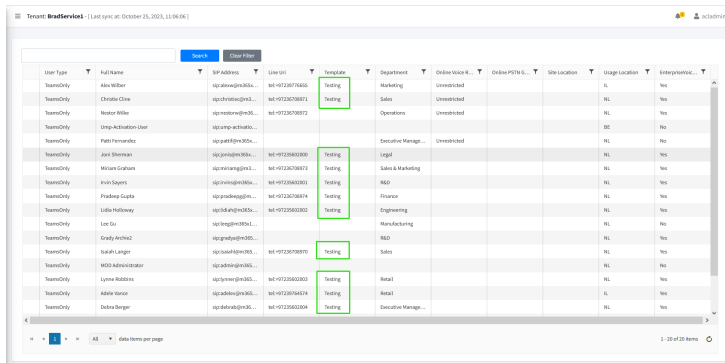
1 - 1 of 1 items

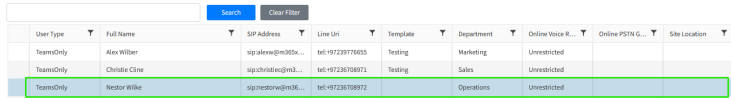
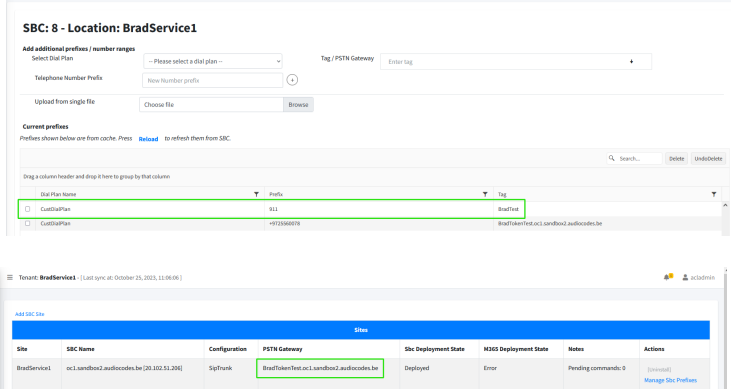

* n1 (n2): n1 items included in Currently Licensed (n2 items qualified for license)
 ** [n/a] equal to not applicable

2. Refer to the table below for descriptions.

License Factor	Description	Priority
Acquired Licenses	Number of licenses purchased by customer and configured in Onboarding wizard.	-
Currently Licensed	<ul style="list-style-type: none"> License factors are derived from one of the following configuration actions: 	-
Managed Users-Direct Routing	<p>Total number of users configured with Direct Routing numbers with the following conditions:</p> <ul style="list-style-type: none"> Enterprise Voice enabled Online Voice Routing Policy assigned Online PSTN Gateway assigned Site Location assigned 	1

Full Name	SIP Address	Line URI	Template	Department	Online Voice R...	Online PSTN Gateway	Site Location	Usage Location	EnterpriseWor...
Johanna Lorenzo	vip.jlorenzo@ms...			Engineering			US		No
Joni Sherman	vip.jonshe@ms...		vip onboarding	Legal			US		No
Pradeep Gupta	vip.pragu@ms...			Finance			US		No
Michael Graham	vip.micgra@ms...		vip onboarding	Sales & Marketing			US		No
Debra Berger	vip.deb@ms...		vip onboarding	Executive Manage...			US		No
Diego Sanchez	vip.diesan@ms...		vip onboarding	HR			US		No
WCD Administrator	vip.wcd@ms...						US		No
Lian Gu	vip.liangu@ms...			Manufacturing			US		No
Charles Chow	vip.chchow@ms...			Sales			US		No
UMP Activation User	vip.ump-activat...						BE		No
Grady Archer	vip.gradar@ms...			HRD			US		No
Adrian Vance	vip.adrian@ms... net +13032546827			Retail	unrestricted	myemobile.landback.audiocodes.be	myemobile	US	No
Irvin Sapers	vip.irvin@ms...			HRD			US		No
Lynne Robbins	vip.lynn@ms...			Retail			US		No
Wagen Dixon	vip.wagend@ms... net +13032312203			Marketing	unrestricted	myemobile.landback.audiocodes.be	myemobile	US	No
Pauli Fernandez	vip.paulif@ms...		vip onboarding	Executive Manage...			US		No
UMP Activation User	vip.ump-activat...						BE		No

License Factor	Description	Priority
	<p>License Calculation Time: 25 Oct 2023 09:29</p> <p>Refresh Licenses</p> <p>Acquired Licenses: 25</p> <p>Currently Licensed: 10</p> <ul style="list-style-type: none"> Managed Users - Direct Routing: 2 (Enterprise voice enabled Direct Routing users in M365 using the LiveCloud configured PSTN Gateway) Managed Users - By Template: 7 (users configured in Lifecycle Management groups) Managed Users - User Interface: 1 (other individual changes to a user) Managed Service Numbers: 0 (such as fax numbers in SBC) <p>Total Monitored Users: 20</p>	
Managed Users-Operator Connect	<p>Total number of users configured with Operator Connect numbers with the following conditions:</p> <ul style="list-style-type: none"> Number is assigned to user (in Teams admin center).  	2
*Managed Users-By Template	<p>Total number of users assigned to M365 templates (see Managing Templates on page 459). In the example below, users are associated with the template 'Testing'</p> 	3

License Factor	Description	Priority
*Managed Users-By User Interface	<p>Total number of users with User properties updated using this interface (see Manually Provisioning Users on page 443). In the example below, the user is configured with a Line Uri and Online Voice Routing Policy. Note that the user is not configured with a template, Online PSTN Gateway and Site Location.</p> 	4
*Managed Service Numbers	<p>Total number of users configured with numbers that are tagged to a PSTN Gateway that is different to the PSTN gateway that is associated with the Site Location SBC. These numbers may be typically Service numbers such as those configured for Fax IVR or Emergency numbers. In the example below, the tag BradTest is mapped to the 911 prefix, however, the actual tag of the PSTN Gateway for the site location is 'BradTokenTest.oc1.sandbox2.audiocodes.be'.</p> 	5
Total Monitored Users	<p>Total number of users on the M365 customer tenant who are synchronized with User Management Pack™ 365 SP Edition.</p> <div>  <p>The customer is only billed for licensed users and not for monitored users.</p> </div>	
Refresh Licenses	Select this option after performing any of the above described license factor configurations or after clicking the Apply license factors option.	
Apply license factors	Select this option after changing the License Factors (Customer):	

License Factor	Description	Priority
	<ul style="list-style-type: none"> Managed Users-By Template Managed Users-By User Interface Managed Service Numbers <p>See Customizing Global License Factors on the next page for details.</p>	

In the following example, an enterprise has purchased **50** licenses. The IT administrator then allocates license with the following composition:

- **6** license factor due to Direct Routing configuration
- **4** license factor due to Template configuration
- **10** license factors due to User interface configuration
- **2** license factor due to configured Service numbers
- **20** Monitored Users

In this case, there are a total of **22** users with licenses assigned, leaving **28** available licenses:

Acquired Licenses= **50**

—

Currently Licensed= **22**

Remaining licenses=**28**

The user license usage calculation is derived from a single factor to prevent double counting. If a user is configured for more than one of the license factor categories, then the license is calculated based on the factor with the highest priority (see priorities listed above). License values are displayed in the format **n1 (n2)** where the value shown outside the brackets reflects the actual **calculated** value and the value inside the brackets, reflects the actual **configured** value.

For example, 'Managed Users-User Interface shows 10 (18) implying that there are 10 users with the license calculated with this factor and another 8 users (18-10) who have User Interface configuration; however, for these other 8 users, the license is calculated based on other factors with higher priority i.e. with 'By Template' and 'Direct Routing' licenses.

The screenshot displays the AxiomClouds UMP-365 Customer Tenant Portal interface. The left sidebar contains navigation links: Users, Lifecycle Management, Manage Templates, Online Voice Routing, Network Topology, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, M365 Configuration, Site Locations, and UMP License (selected). The main content area shows the tenant name 'BradDRService' and a 'Last sync at: November 16, 2023, 11:12:58'.

License Calculation Time: 16 Nov 2023 09:11
[Refresh Licenses](#)

Acquired Licenses: 50

Currently Licensed: 22

- Managed Users - Direct Routing: 6 (Enterprise voice enabled Direct Routing users in M365 using the LiveCloud configured PSTN Gateway)
- Managed Users - By Template: 4 (users configured in Lifecycle Management groups)
- Managed Users - User Interface: 10 (other individual changes to a user)
- Managed Service Numbers: 2 (such as fax numbers in SBC)

Total Monitored Users: 20

License Factors (Customer):

- ☒ Managed Users - By Template
- ☒ Managed Users - By User Interface
- ☒ Managed Service Numbers

[Apply license factors](#)

Note: License billing is based on the local configured License Factors. If you want to restore to default, [click here](#).

UMP Customer License - Audit

Last 3 months [Get History](#)

License Calculation Time	Currently Licensed	Managed Users - Direct Routing -	Managed Users - Operator Connect -	Managed Users - By Template -	Managed Users - User Interface -	Managed Service Numbers	Total Monitored Users
16 Nov 2023 11:11	22	6	0 (0)	4 (5)	10 (16)	2 (2)	20
01 Nov 2023 01:55	1	1	0 (0)	0 (0) [n/a]	0 (1)	0 (0)	20

Customizing Global License Factors

This option lets you determine whether the following License Factors are used in the license calculation. The default settings for this configuration is set by SysAdmin (see [Configuring Global License Settings](#) on page 168). You can customize which license factors are used in the license calculation:

- ☒ Managed Users-By Template
- ☒ Managed Users-By User Interface
- ☒ Managed Service Numbers

If the customer, changes the configuration i.e. deselects any of the check boxes, then only those factors are used in the license calculation. Note that the data in the table is updated accordingly. In the example below, the default Global settings have been updated by excluding the 'Managed Users- By User Interface' factor. As a result, its not used in the calculation i.e. 0 (16) is displayed, where '0' indicates that no license values are incremented to the license and '16' indicates the actual configuration attributed to this factor. You can restore the Global Settings by selecting **click here** link. Once clicked, note that the 'Managed Users- By User Interface' indicates 16 (16) and the corresponding value is displayed in the 'Currently Licensed' list. In addition, notice that the factor 'Managed Users - By Template' now displays the value '0' in the Currently Licensed list and in the table 0 (16).

OCaudiocodes Tenant: **BradService1** - [Last sync at: October 24, 2023, 18:20:45]

License Calculation Time: 24 Oct 2023 03:26

[Refresh Licenses](#)

Acquired Licenses: 50

Currently Licensed: 15

- Managed Users - Direct Routing: 0 (Enterprise voice enabled Direct Routing users in M365 using the LiveCloud configured PSTN Gateway)
- Managed Users - By Template: 15 (users configured in Lifecycle Management groups)
- Managed Users - User Interface: 0 (other individual changes to a user)
- Managed Service Numbers: 0 (such as fax numbers in SBC)

Total Monitored Users: 20

License Factors (Customer):

- ☒ Managed Users - By Template
- ☐ Managed Users - By User Interface
- ☒ Managed Service Numbers

[Apply license factors](#)

Note: License billing is based on the local configured License Factors.
If you want to restore to default [click here](#)

UMP Customer License - Audit

Last 3 months [Get History](#)

License Calculation Time	Currently Licensed	Managed Users - Direct Routing -	Managed Users - Operator Connect -	Managed Users - By Template -	Managed Users - User Interface -	Managed Service Numbers	Total Monitored Users
24 Oct 2023 06:26	15	0	0 (0)	15 (15)	0 (0) (n/a)	0 (0)	20

1 - 1 of 1 items

*n1 (n2): n1 items included in CurrentlyLicensed (n2 items qualified for license)
** (n/a) equal to not applicable

OCaudiocodes Tenant: **BradService1** - [Last sync at: October 24, 2023, 18:29:37]

License Calculation Time: 24 Oct 2023 03:37

[Refresh Licenses](#)

Acquired Licenses: 50

Currently Licensed: 17

- Managed Users - Direct Routing: 0 (Enterprise voice enabled Direct Routing users in M365 using the LiveCloud configured PSTN Gateway)
- Managed Users - By Template: 0 (users configured in Lifecycle Management groups)
- Managed Users - User Interface: 16 (other individual changes to a user)
- Managed Service Numbers: 1 (such as fax numbers in SBC)

Total Monitored Users: 20

License Factors (Global):

- ☐ Managed Users - By Template
- ☒ Managed Users - By User Interface
- ☒ Managed Service Numbers

[Apply license factors](#)

Note: By default License billing is based on the globally configured License Factors.

UMP Customer License - Audit

Last 3 months [Get History](#)

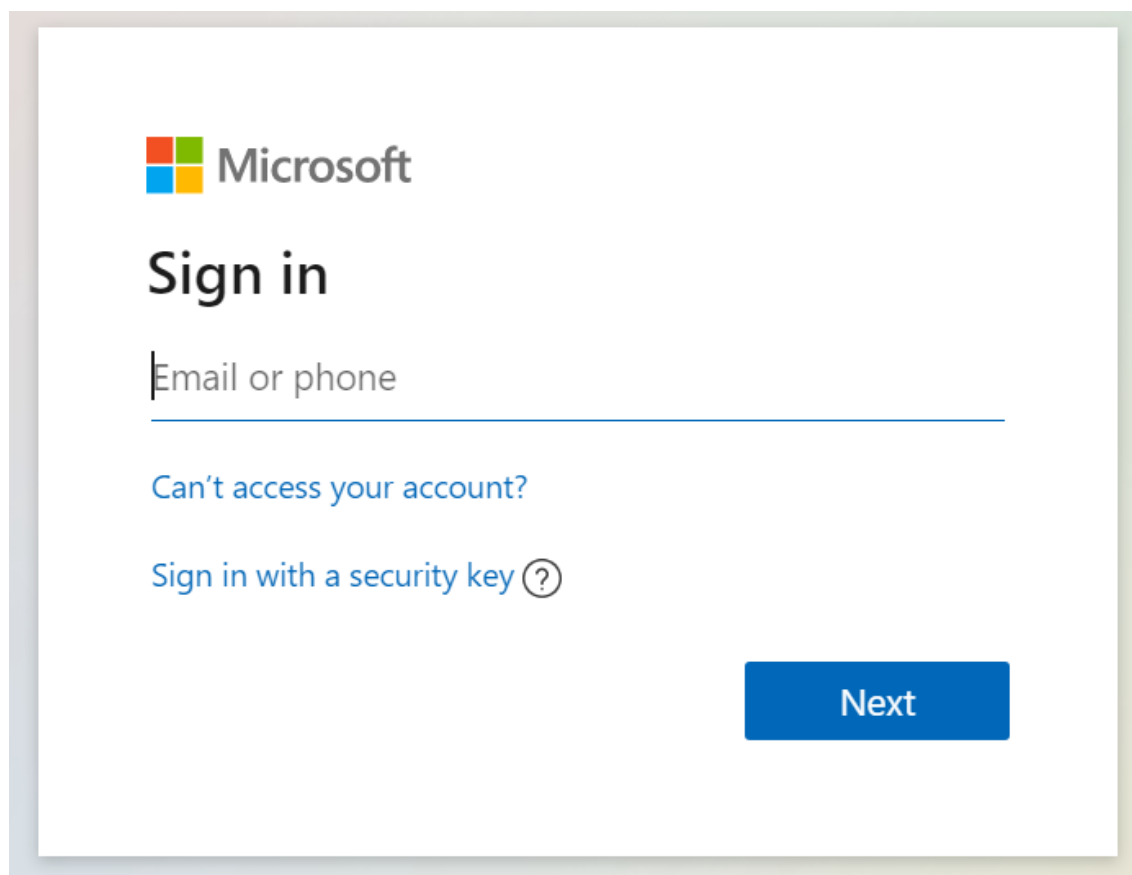
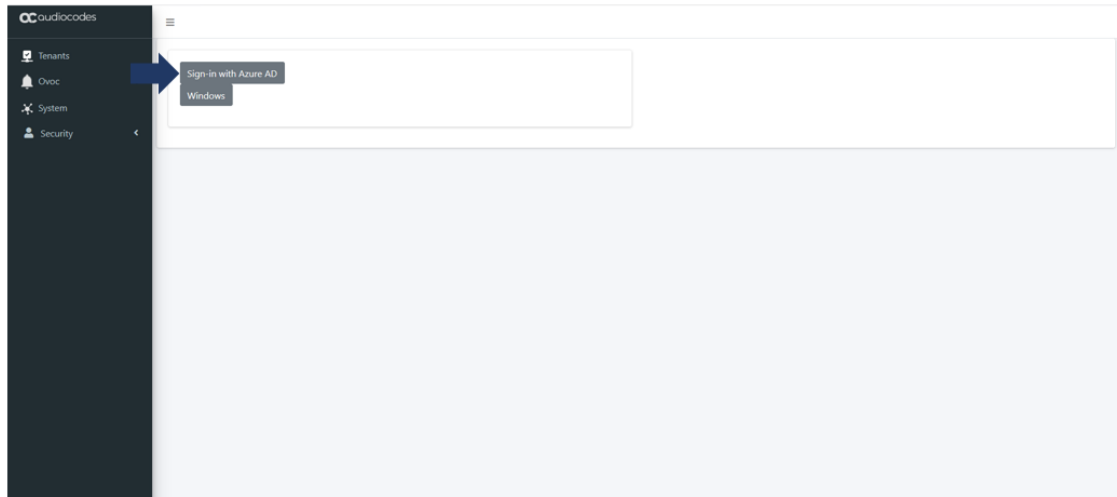
License Calculation Time	Currently Licensed	Managed Users - Direct Routing -	Managed Users - Operator Connect -	Managed Users - By Template -	Managed Users - User Interface -	Managed Service Numbers	Total Monitored Users
24 Oct 2023 06:37	17	0	0 (0)	0 (0) (n/a)	16 (16)	1 (1)	20

1 - 1 of 1 items

*n1 (n2): n1 items included in CurrentlyLicensed (n2 items qualified for license)
** (n/a) equal to not applicable

33 Multitier Admin Access

Providers can create an additional layer of support by granting 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), the list of customers that the provider has granted them access to manage is displayed.



List of customers for AudioCodes EMEA Channel

[enterpricertc](#)[TalkMail](#)[easylync](#)[finebak](#)[Logout](#)

audioCodes

Tenant: **Customer22** - [Last sync at: August 7, 2022, 15:37:24]

UMP-Tobi/umpadmin

Search Clear Filter

User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voice	Online PST	Site Location	Usage Loca	EnterpriseV...
TeamsOnly	Christie Cline	sip:christie...	tel:+18585...	BG	Sales				NL	Yes
TeamsOnly	Ivin Sayers	sip:ivins...	tel:+13095...	BG	R&D				NL	Yes
TeamsOnly	SBC Domain	sip:sbc-do...				Unrestricted			NL	No
TeamsOnly	Grady Archie	sip:gradya...	tel:+13095...	BG	R&D	Unrestricted			NL	Yes
TeamsOnly	Alex Wilber	sip:alexw...	tel:+18585...	BG	Marketing				NL	Yes
TeamsOnly	Patti Fernandez	sip:pattif...	tel:+15025...	BG	Executive ...				NL	Yes
TeamsOnly	Allan Deyoung	sip:alland...	tel:+12625...	BG	IT				NL	Yes
TeamsOnly	Nestor Wilke	sip:nestor...	tel:+12065...	BG	Operations				NL	Yes
TeamsOnly	Megan Bowen	sip:megan...	tel:+14125...	BG	Marketing				NL	Yes
TeamsOnly	MOD Administrator	sip:admin...		BG					NL	Yes
TeamsOnly	Miriam Graham	sip:miriam...	tel:+18585...	BG	Sales & M...				NL	Yes
TeamsOnly	Adele Vance	sip:adelev...	tel:+14255...	BG	Retail				NL	Yes

1 - 14 of 14 items

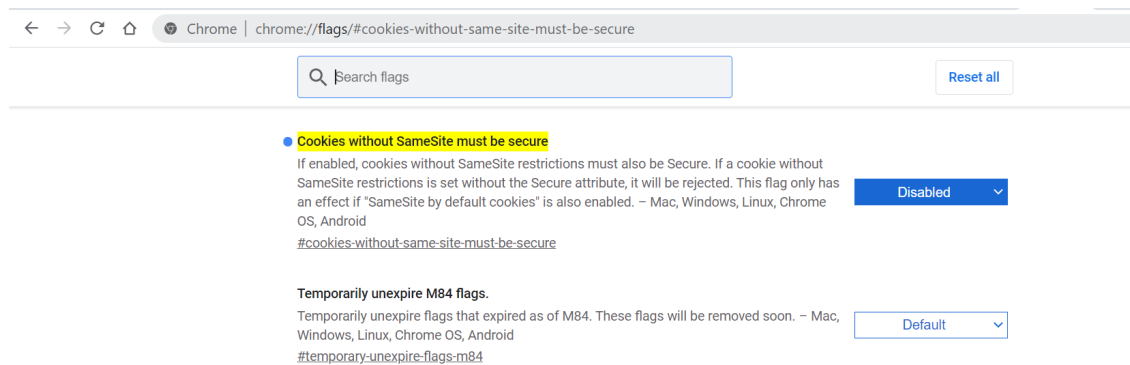
34 Browser Settings- IETF Same Site Cookie Attribute

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:

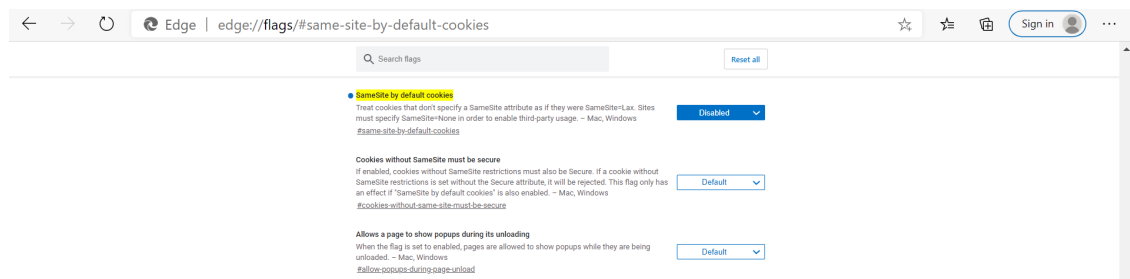
■ Chrome:

- Go to: "chrome://flags/#cookies-without-same-site-must-be-secure"
- Disable option "Cookies without SameSite must be secure"
- Restart Chrome.



■ Edge:

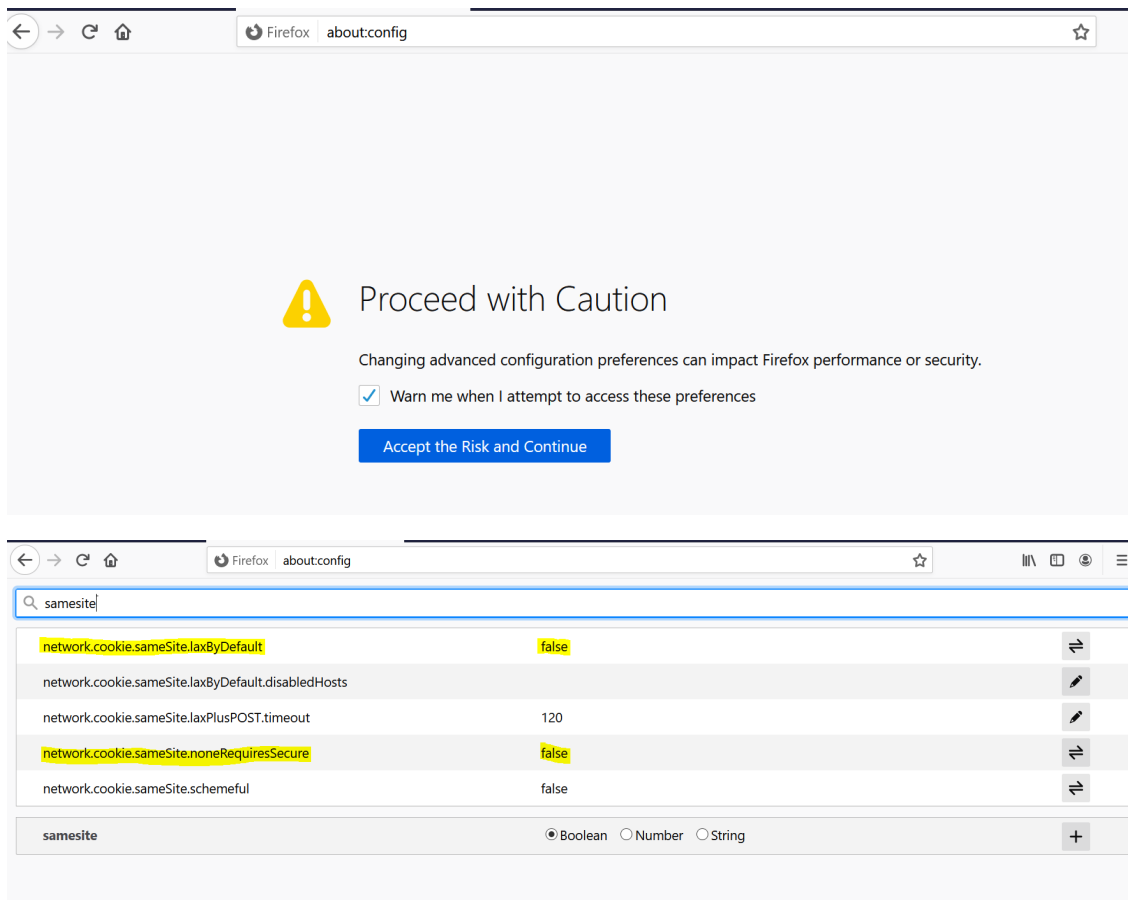
- Go to: "edge://flags/#same-site-by-default-cookies"
- Disable option "SameSite by default cookies"
- Restart Edge.



■ Firefox: (works in any version past 75):

- In the URL bar, navigate to **about:config**. (accept the warning prompt, if shown).
- Type SameSite into the "Search Preference Name" bar.
- Set `network.cookie.sameSite.laxByDefault` to **false** using the toggle icon.

- d. Set `network.cookie.sameSite.noneRequiresSecure` to **false** using the toggle icon.
- e. Restart Firefox.



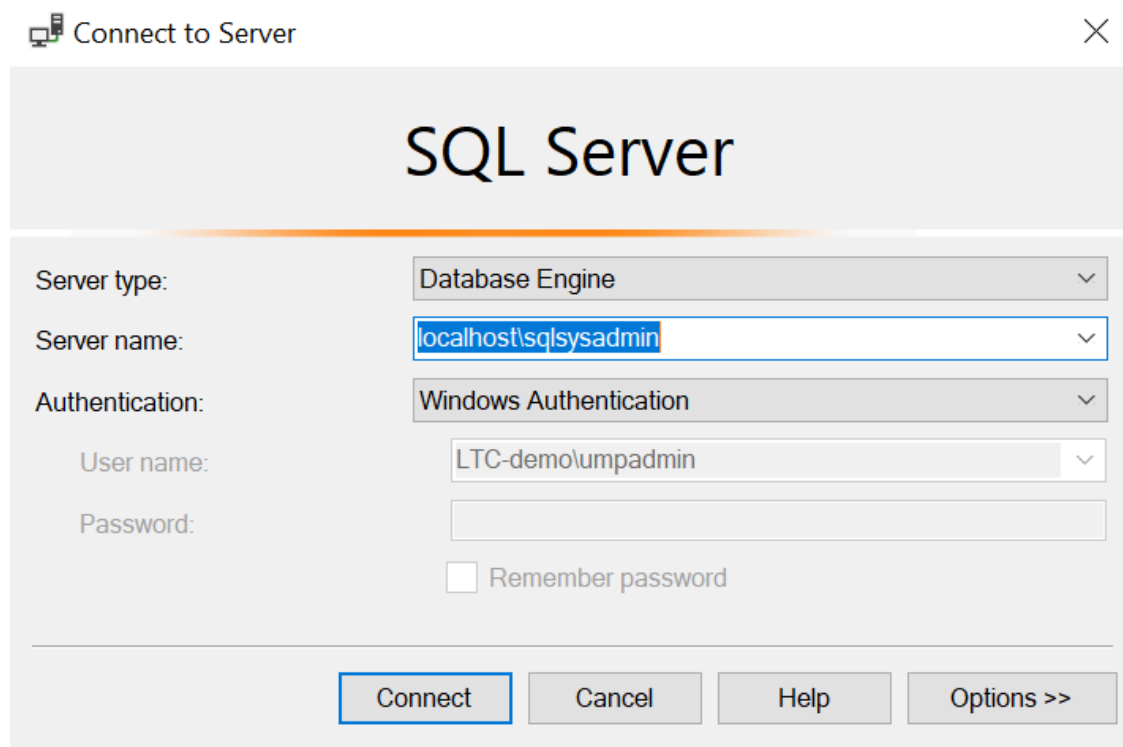
Public Customer/ Channel Url Portal requires a secure connection (HTTPS) as a default Mandatory requirement. Channel and Customer Admin do not need to edit the browser setting IETF SameSite cookie attribute.

35 Backup the Customer Tenant Database

This section describes how to back up the customer tenant database.

➤ **To back up the customer tenant database:**

1. Start the Microsoft SQL Server Management Studio.



Connect to Server

SQL Server

Server type: Database Engine

Server name: localhost\sqlsysadmin

Authentication: Windows Authentication

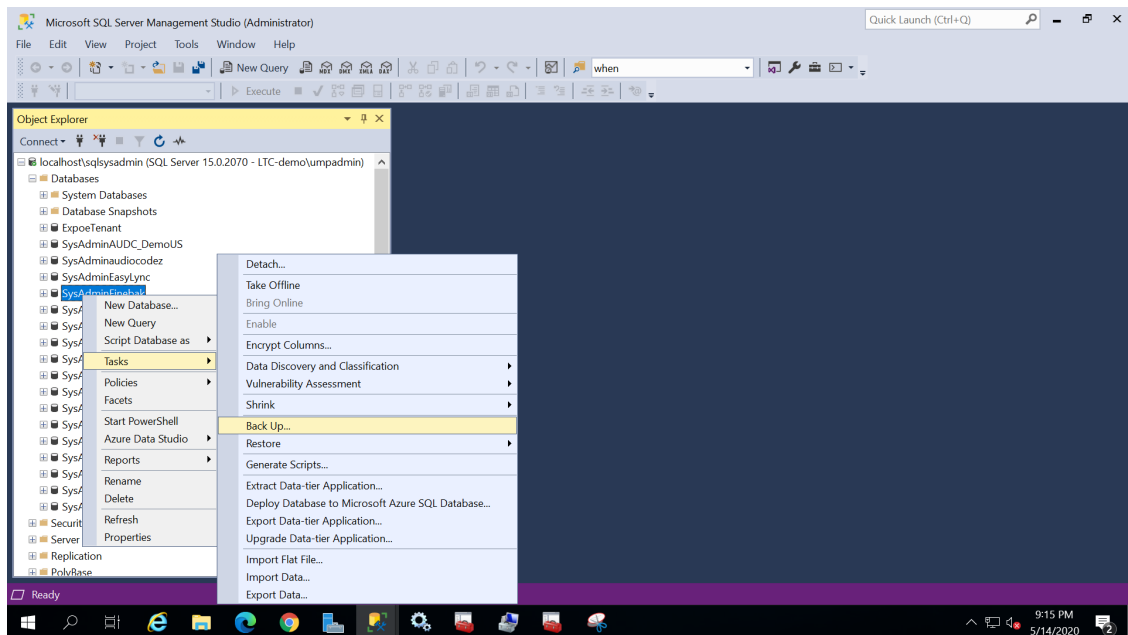
User name: LTC-demo\umpadmin

Password:

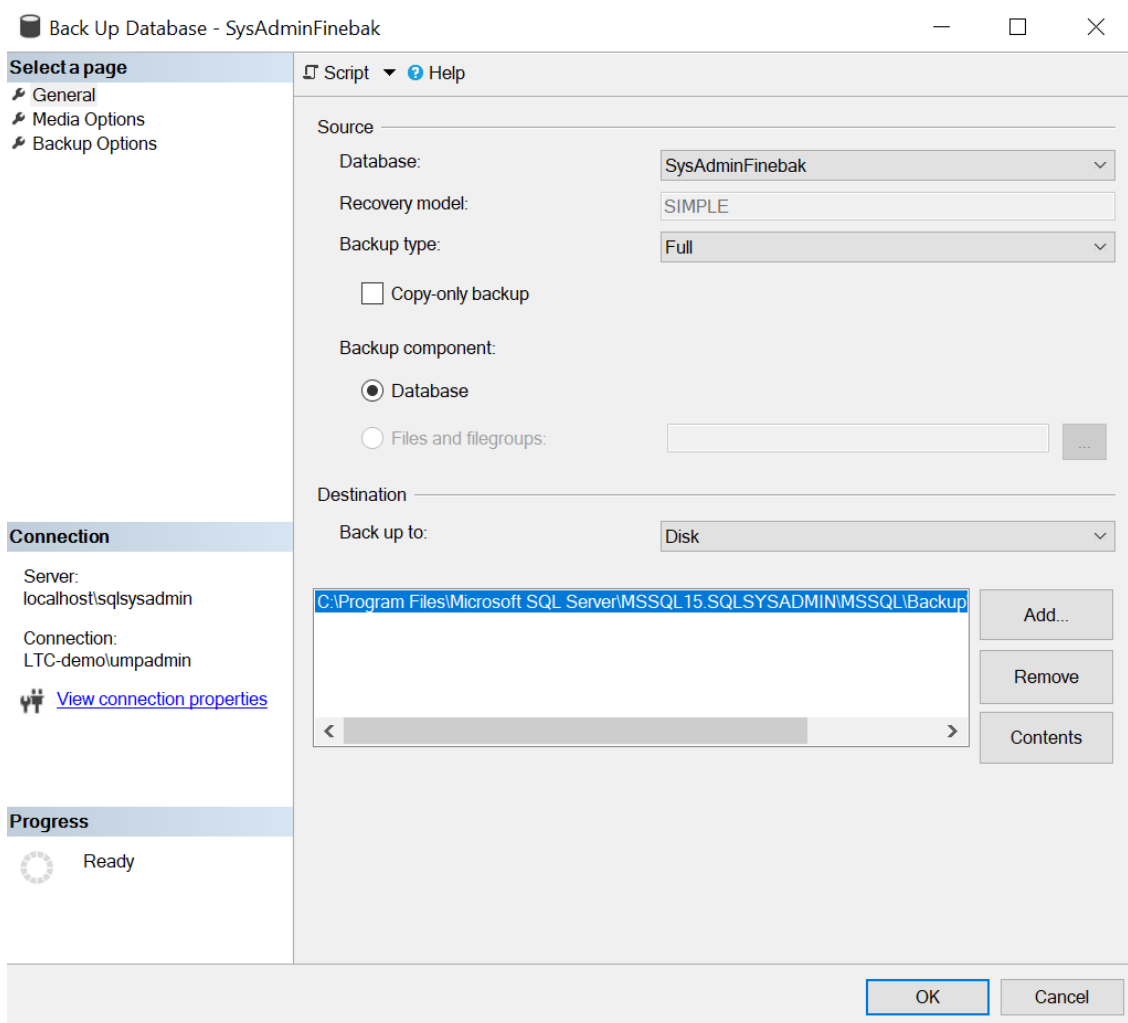
☐ Remember password

Connect Cancel Help Options >>

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.



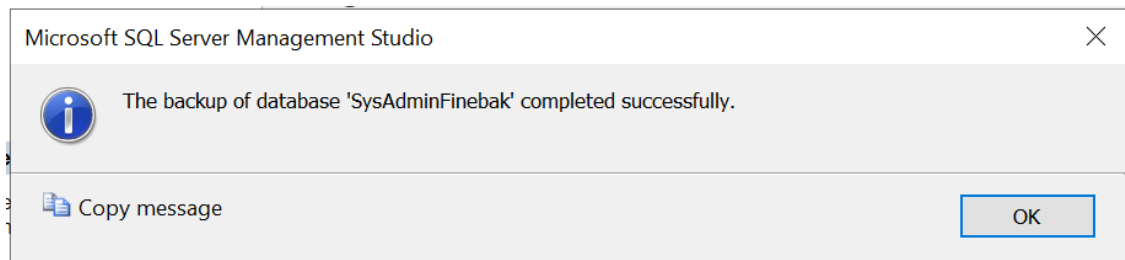
5. Right-click and select the Destination.





Save the backup on a separate disk to the SQL database.

6. Select the 'Destination' and then click **OK**.

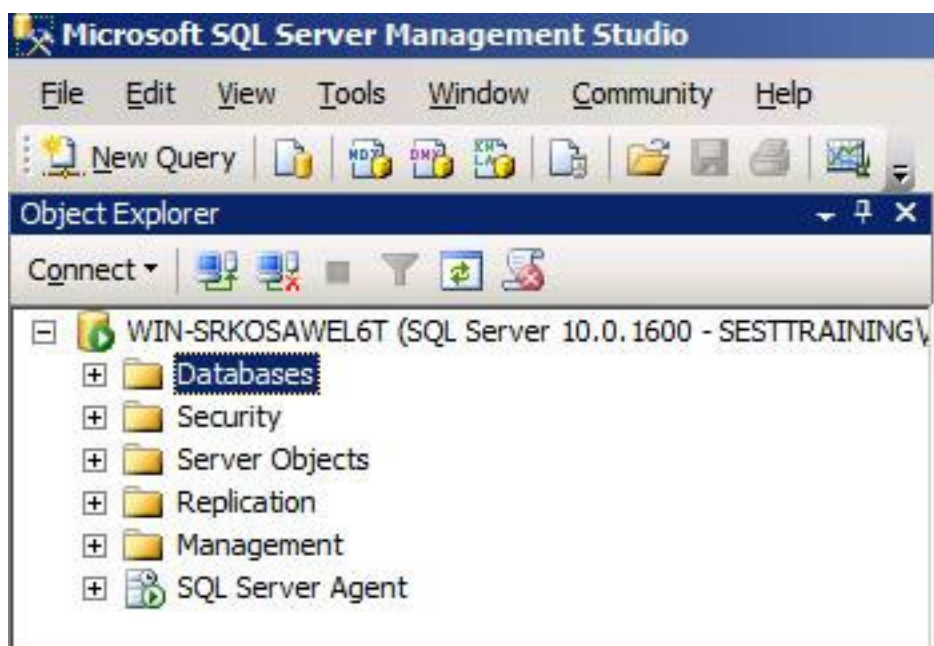


36 Restore the Customer Tenant Database

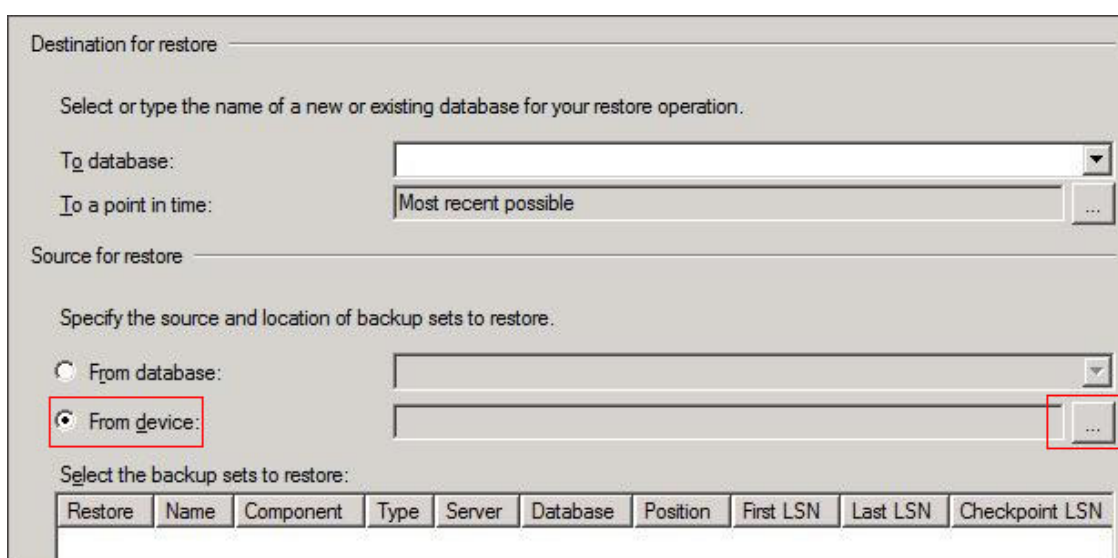
This section describes how to restore the customer tenant database.

➤ **To restore the database, do the following:**

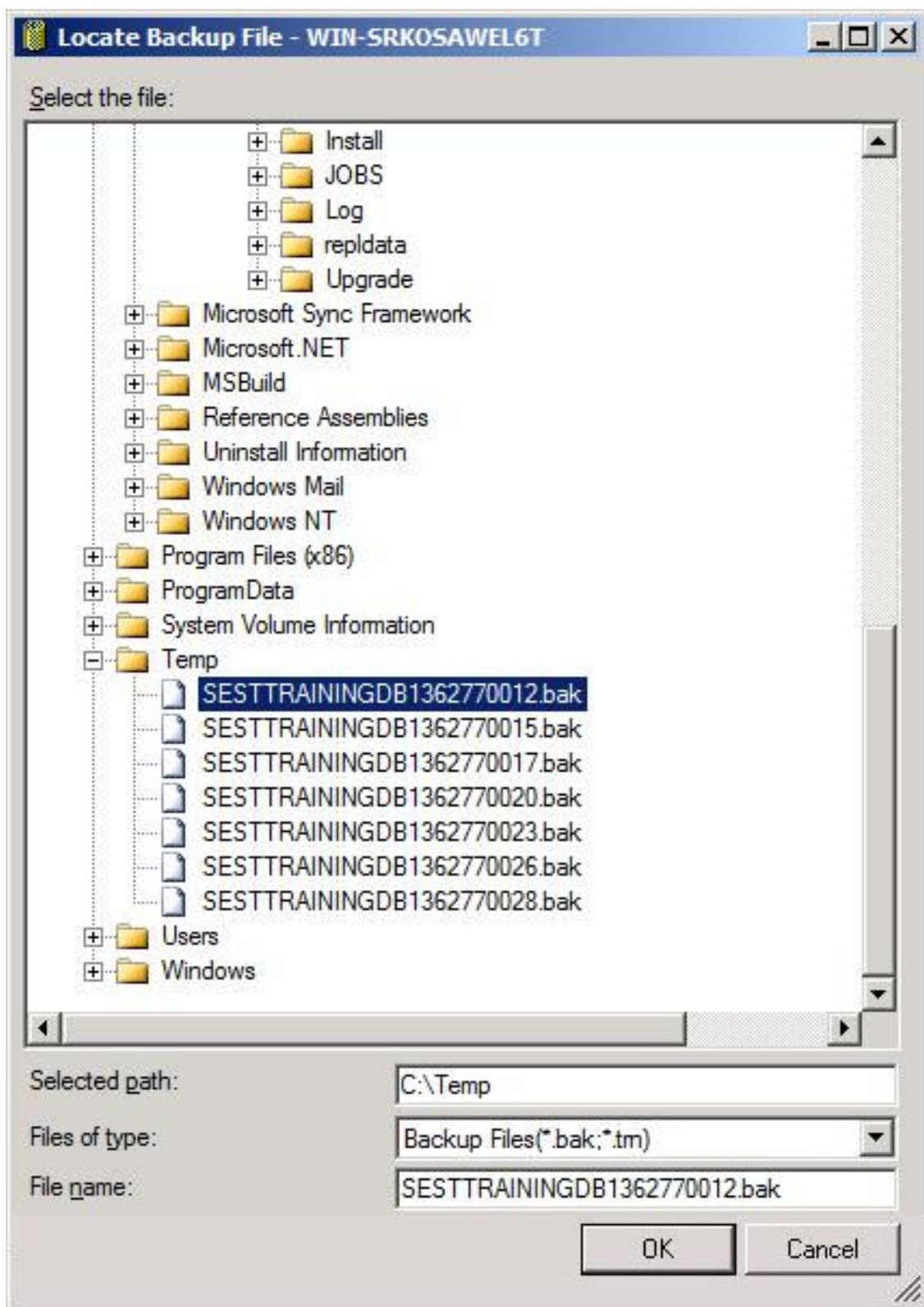
1. Open Microsoft SQL Server Management Studio and navigate to **Databases**.



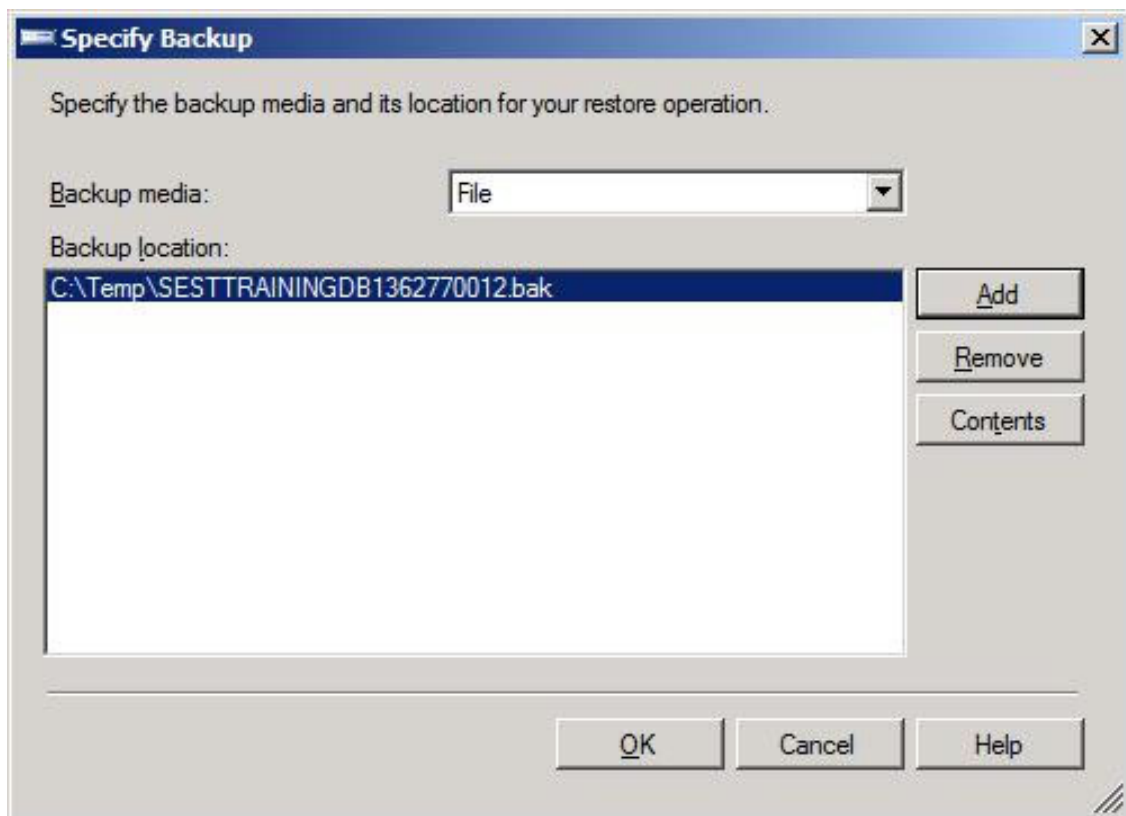
2. Right-click Databases and click **Restore Database**. In the screen section 'Source for restore', select From Device and then click the **browse** button:



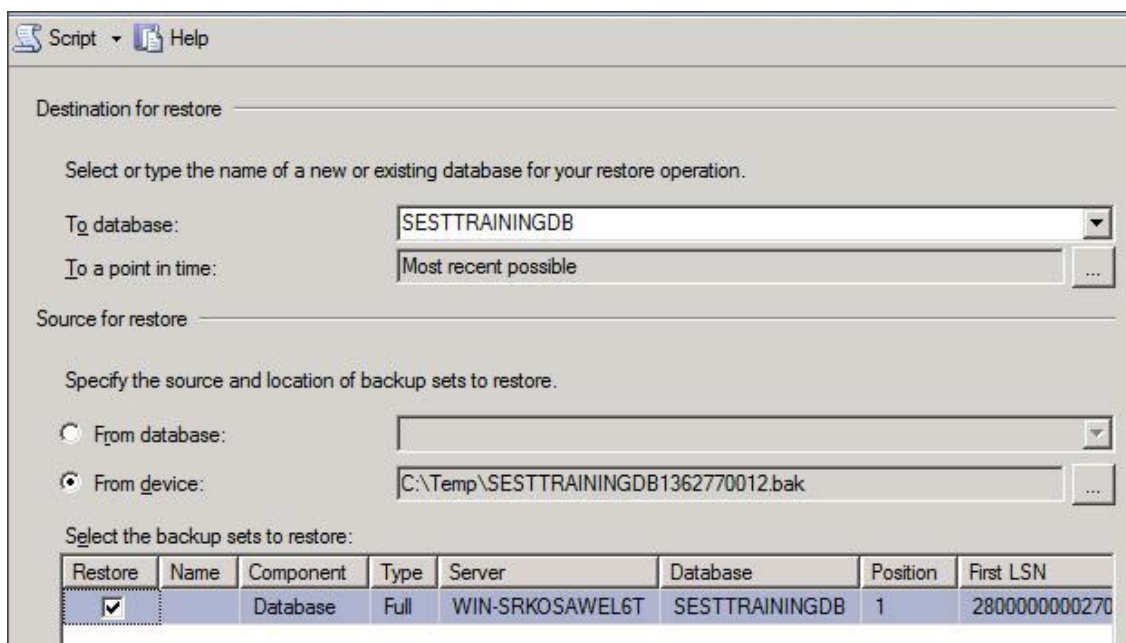
3. Click **Add** in the Specify Backup window. Browse to the location of your recently restored files. Choose the full backup file which should be the first backup file in the list:



4. Click **OK**; the Specify Backup window is displayed.

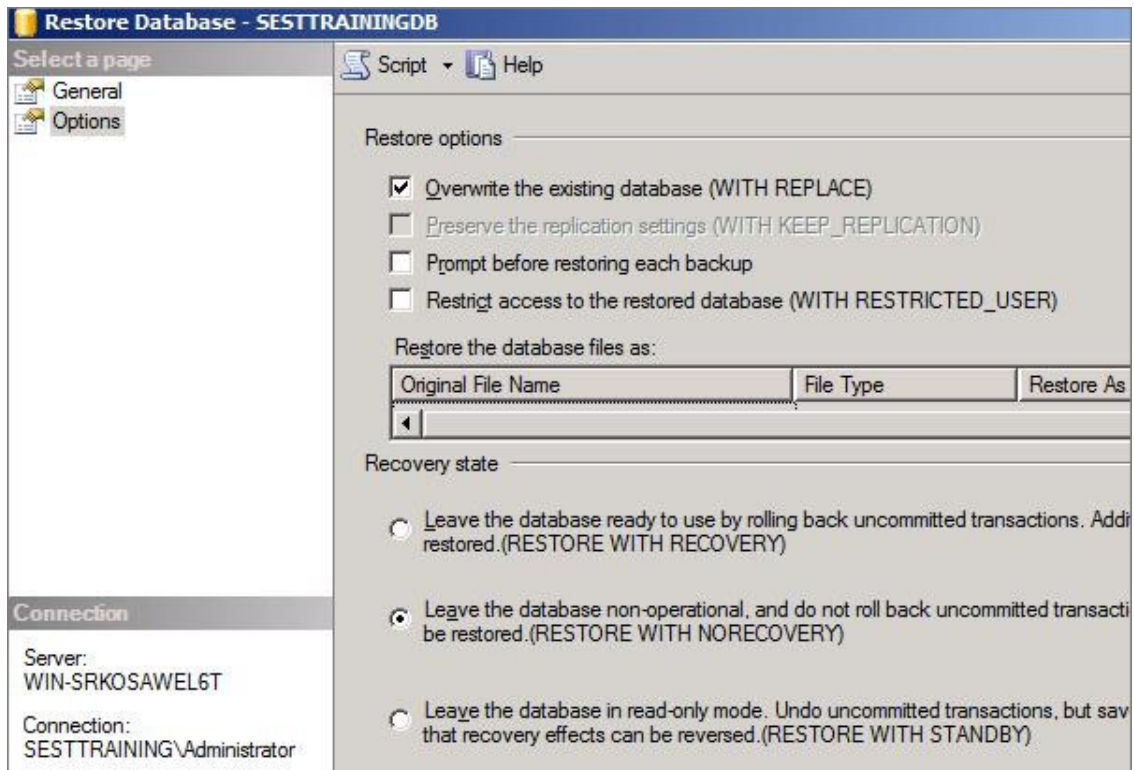


5. Click **OK**.
6. In the screen section 'Destination for restore', select the database to which you want to restore, and then in the 'Select the backup sets to restore' section of the screen, select the backup file you selected above.



7. In the left pane, click **Options**, and then select the following:

- In the Restore options' section, select Overwrite the existing database (WITH REPLACE) and leave the other options unselected.
- 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):



8. Click **OK** to 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. Proceed to 'Restoring to a Point-in-Time'.

Restoring to a Point in Time

This procedure describes how to restore the last incremental file containing the point-in-time.

➤ Do the following:

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 then 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:

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

6. 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.
7. Select a specific date and time and choose the date and time to which to restore:

Point in time restore

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

8. 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.

9. 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):

Restore Database - SESTTRAININGDB

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 can be restored. (RESTORE WITH RECOVERY)
- ☐ Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be 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: SESTTRAINING\Administrator

10. Click **OK** to perform the restore. the restored database is displayed with only those changes up to the specified point-in-time.

37 AudioCodes SfB2Teams Migration Tool

This section describes the SfB2Teams application 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:

- Prerequisite App registration configuration
- SfB2Teams Application
- 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



The solution consumes Migration Service User license (per users).

This chapter includes the following:

- [Installing the Prerequisites](#) below
- [Create and Register the Azure App](#) on the next page
- [Running SfB2Teams Application](#) on page 566
- [ARM Auto Call Routing to Teams](#) on page 569

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 [Installing the Prerequisites](#) above)

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
- Install Skype Online PowerShell by running “6 - SkypeOnlinePowerShell.Exe”.
- 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>).

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.

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...](#)

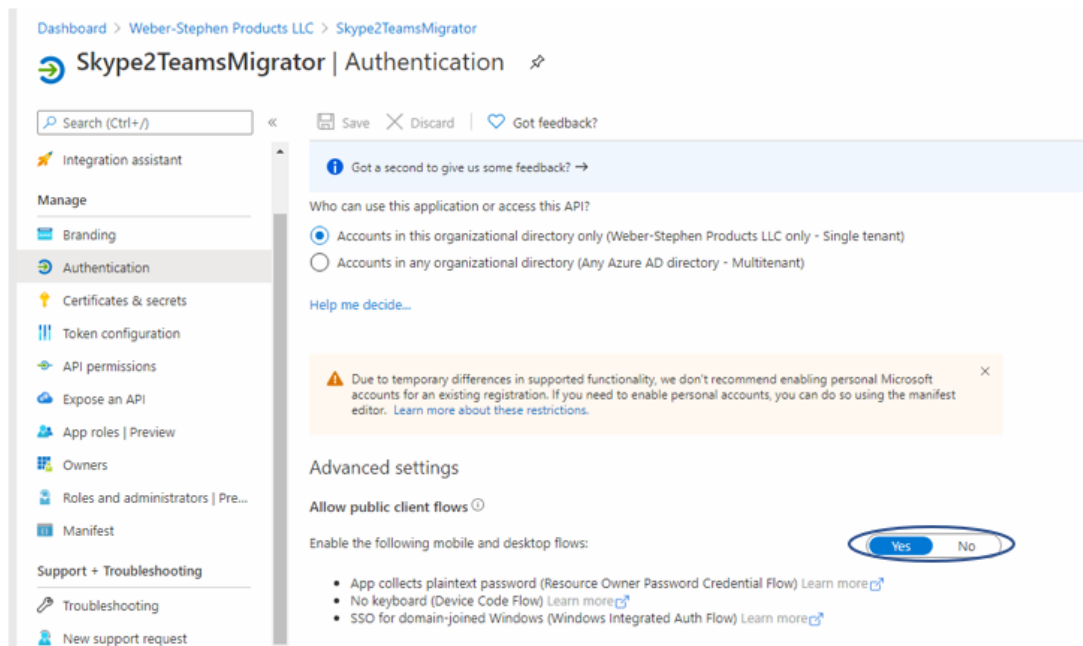
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

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

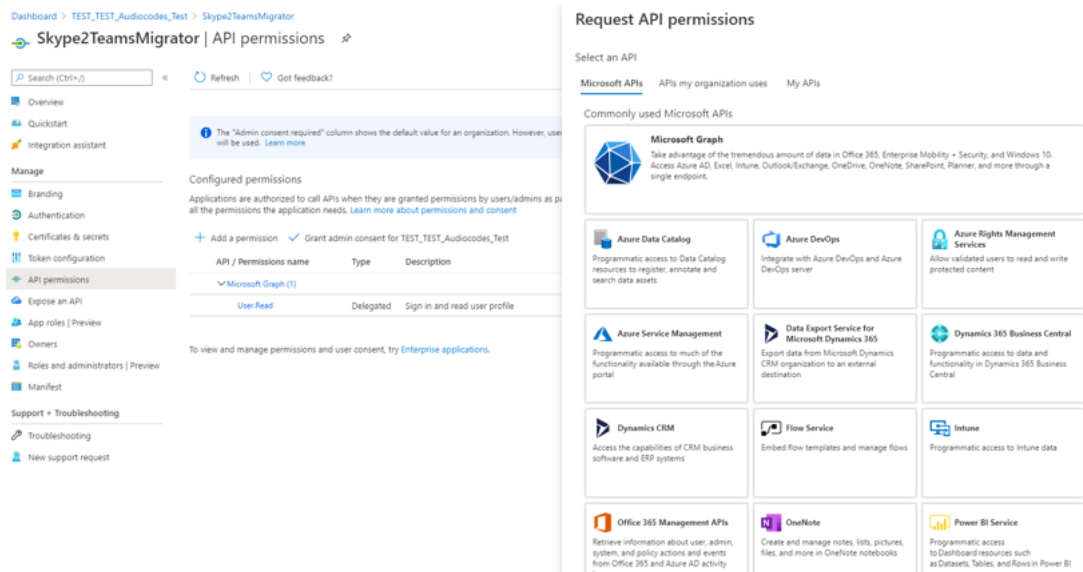
By proceeding, you agree to the [Microsoft Platform Policies](#)

Register



4. In the Navigation pane, select **API Permissions**.


5. Click Add a permission and then select the **Microsoft Graph** tab.



6. Select **Delegated Permission**.

Request API permissions

[← All APIs](#)


Microsoft Graph
<https://graph.microsoft.com/>
[Docs](#)

What type of permissions does your application require?


Delegated permissions


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





Application permissions

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

Select permissions [expand all](#)

 Start typing a reply url to filter these results

 The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
<p>Openid permissions</p>	
<input type="checkbox"/> email  View users' email address	No
<input type="checkbox"/> offline_access  Maintain access to data you have given it access to	No
<input type="checkbox"/> openid  Sign users in	No
<input type="checkbox"/> profile  View users' basic profile	No
<p>> AccessReview</p>	

7. Select the following Delegation Permissions:

- Openid permissions:
 - ◆ offline_access
 - ◆ openid
 - ◆ profile
- Directory:
 - ◆ Directory.AccessAsUser.All
 - ◆ Directory.Read.All
- User:
 - ◆ User.Read
 - ◆ User.ReadBasic.All

Dashboard > TEST_TEST_AudioCodes_Test > Skype2TeamsMigrator

Skype2TeamsMigrator | API permissions

Search (Ctrl+F) Refresh Got feedback?

You are editing permission(s) to your application, users will have to consent even if they've already consented. Learn more

The "Admin consent required" column shows the default value for an organization. However, users will be prompted to grant consent if the application is not configured for admin consent. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as per all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for TEST_TEST_AudioCodes_Test

API / Permissions name	Type	Description
Microsoft Graph (7)		
Directory.AccessAsUser.All	Delegated	Access directory as the signed-in user
Directory.Read.All	Delegated	Read directory data
offline_access	Delegated	Maintain access to data you have given it access to
openid	Delegated	Sign users in
profile	Delegated	View users' basic profile
User.Read	Delegated	Sign in and read user profile
User.ReadBasic.All	Delegated	Read all users' basic profiles

To view and manage permissions and user consent, try Enterprise applications.

Request API permissions

Microsoft Graph
https://graph.microsoft.com/ Docs

What type of permissions does your application require?

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

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

Select permissions expand all

Start typing a reply url to filter these results

Permission	Admin consent required
AccessReview	
AdministrativeUnit	
APIConnectors	
Application	
AppRoleAssignment	
ApprovalRequest	
AuditLog	
BitLockerKey	

Add permissions Discard

8. Select the "Grant admin consent for..." and then select **yes**.



If the App hasn't been granted admin consent, users are prompted to grant consent the first time they use the App.

9. Select **Application permissions**.

10. Select the following Application permissions.

Request API permissions

×

[← All APIs](#)

> TermStore

> ThreatAssessment

> ThreatIndicators

> TrustFrameworkKeySet

> UserAuthenticationMethod

> UserNotification

> UserShiftPreferences

✓ User (1)

☐

User.Export.All ⓘ
Export user's data

Yes

☐

User.Invite.All ⓘ
Invite guest users to the organization

Yes

☐

User.ManageIdentities.All ⓘ
Manage all users' identities

Yes

☒

User.Read.All ⓘ
Read all users' full profiles

Yes

☐

User.ReadWrite.All ⓘ
Read and write all users' full profiles

Yes

Add permissions

Discard

11. Review all permissions.

Dashboard > AudioCodes Netherlands BV > Skype2TeamsMigrator

Skype2TeamsMigrator | API permissions

Search (Ctrl+/) Refresh Got feedback?

Overview Quickstart Integration assistant

Manage

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

Support + Troubleshooting

- Troubleshooting
- New support request

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for AudioCodes Netherlands BV

API / Permissions name	Type	Description	Admin consent req...	Status
Microsoft Graph (B)				
DirectoryAccessAsUser	Delegated	Access directory as the signed in user	Yes	✓ Granted for AudioCodes_ ...
Directory.Read.All	Delegated	Read directory data	Yes	✓ Granted for AudioCodes_ ...
offline_access	Delegated	Maintain access to data you have given it acc...	-	✓ Granted for AudioCodes_ ...
openid	Delegated	Sign users in	-	✓ Granted for AudioCodes_ ...
profile	Delegated	View users' basic profile	-	✓ Granted for AudioCodes_ ...
User.Read	Delegated	Sign in and read user profile	-	✓ Granted for AudioCodes_ ...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for AudioCodes_ ...
User.ReadBasic.All	Delegated	Read all users' basic profiles	-	✓ Granted for AudioCodes_ ...

To view and manage permissions and user consent, try [Enterprise applications](#).

12. Copy application (client) ID and Directory (tenant) ID to notepad as they are required in the procedure in [Create and Register the Azure App](#) on page 561.

Dashboard > 1

Skype2TeamsMigrator

Search (Ctrl+/) Delete Endpoints Preview features

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions**
- Expose an API
- App roles | Preview
- Owners

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name Skype2TeamsMigrator	Supported account types My organization only
Application (client) ID f*****5	Redirect URIs Add a Redirect URI
Directory (tenant) ID 4*****5	Application ID URI Add an Application ID URI
Object ID c*****5	Managed application in local directory Skype2TeamsMigrator

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) an 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 mo](#)

Running 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.

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:

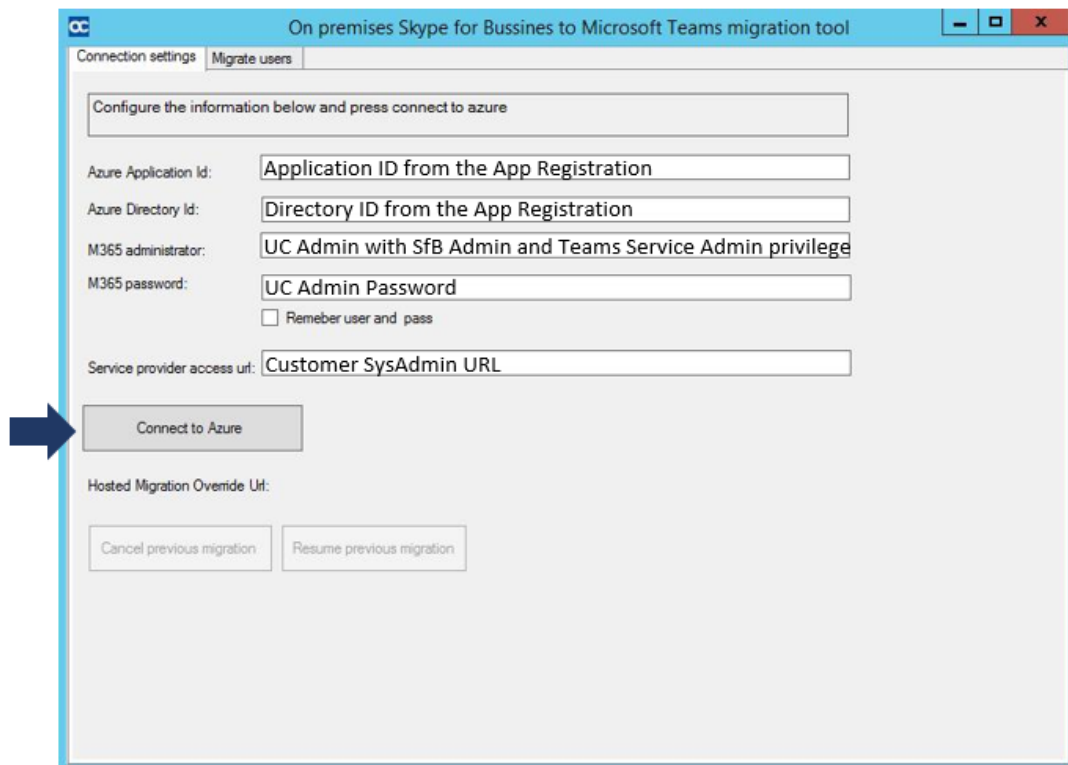
☐ Remember user and pass

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**.



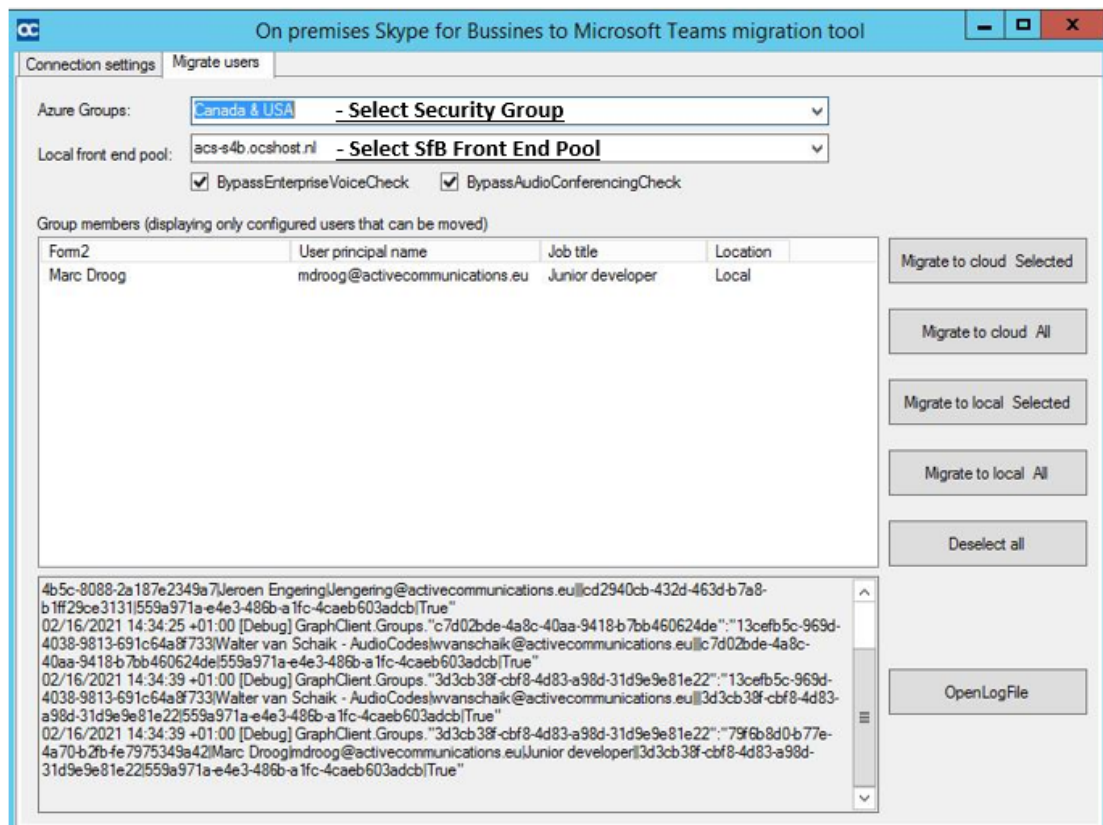
4. Migrate Users:

- **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:

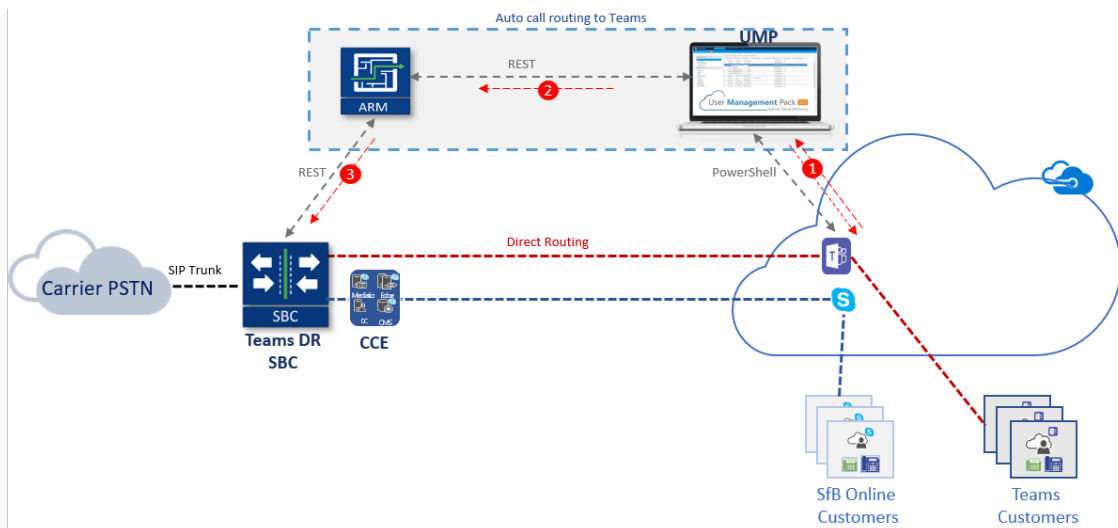
- **Migrate to Cloud Selected:** Migrate selected Users to Teams
- **Migrate to Cloud All:** Migrate all users to Teams
- **Migrate to Local Selected:** Revert Selected Users to SfB
- **Migrate to Local All:** Revert All Users to SfB
- **Deselect All:** Deselect all Users



ARM 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 (see figure below).



For more information, contact AudioCodes Professional Services.

38 Renewing Expired Tokens

When you are unable 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. The following figures show example expired token messages.

```

1 {
2   "type": "MsalThrottledUiRequiredException",
3   "error_code": "invalid_grant",
4   "error_description": "AADSTS50173: The provided grant has expired due to it being revoked, a fresh auth token
   is needed. The user might have changed or reset their password. The grant was issued on
   '2022-09-22T07:33:10.1150000Z' and the TokensValidFrom date (before which tokens are not valid) for this user
   is '2023-02-27T07:34:20.0000000Z'.\r\nTrace ID: 230af00f-209a-4e61-93a0-ed997a293000\r\nCorrelation ID:
   0ee05169-eb55-42b7-807e-650f4a80fff7\r\nTimestamp: 2023-02-27 07:57:41Z",
5   "claims": null,
6   "response_body": "{\r\n  \"error\": \"invalid_grant\",
   \"error_description\": \"AADSTS50173: The provided grant has
   expired due to it being revoked, a fresh auth token is needed. The user might have changed or reset their
   password. The grant was issued on '2022-09-22T07:33:10.1150000Z' and the TokensValidFrom date (before which
   tokens are not valid) for this user is '2023-02-27T07:34:20.0000000Z'.\r\nTrace ID:
   230af00f-209a-4e61-93a0-ed997a293000\r\nCorrelation ID: 0ee05169-eb55-42b7-807e-650f4a80fff7\r\nTimestamp:
   2023-02-27 07:57:41Z\",
   \"error_codes\": [50173],
   \"timestamp\": \"2023-02-27
   07:57:41Z\",
   \"trace_id\": \"230af00f-209a-4e61-93a0-ed997a293000\",
   \"correlation_id\": \"0ee05169-eb55-42b7-807e-650f4a80fff7\",
   \"suberror\": \"bad_token\"
   }",
7   "correlation_id": "0ee05169-eb55-42b7-807e-650f4a80fff7",
8   "sub_error": "bad_token"
9 }

```

```

1 {
2   "type": "MsalUiRequiredException",
3   "error_code": "invalid_grant",
4   "error_description": "AADSTS50078: Presented multi-factor authentication has expired due to policies
   configured by your administrator, you must refresh your multi-factor authentication to access
   '00000003-0000-0000-c000-000000000000'.\r\nTrace ID: 3b405061-31c2-4607-9ad7-d9738d870600\r\nCorrelation ID:
   d7d217f4-b082-4164-b0c1-1eb5b6f36bd0\r\nTimestamp: 2023-03-17 14:22:35Z",
5   "claims": null,
6   "response_body": "{\r\n  \"error\": \"invalid_grant\",
   \"error_description\": \"AADSTS50078: Presented multi-factor
   authentication has expired due to policies configured by your administrator, you must refresh your
   multi-factor authentication to access '00000003-0000-0000-c000-000000000000'.\r\nTrace ID:
   3b405061-31c2-4607-9ad7-d9738d870600\r\nCorrelation ID: d7d217f4-b082-4164-b0c1-1eb5b6f36bd0\r\nTimestamp:
   2023-03-17 14:22:35Z\",
   \"error_codes\": [50078],
   \"timestamp\": \"2023-03-17
   14:22:35Z\",
   \"trace_id\": \"3b405061-31c2-4607-9ad7-d9738d870600\",
   \"correlation_id\": \"d7d217f4-b082-4164-b0c1-1eb5b6f36bd0\",
   \"suberror\": \"basic_action\"
   }",
7   "correlation_id": "d7d217f4-b082-4164-b0c1-1eb5b6f36bd0",
8   "sub_error": "basic_action"
9 }

```

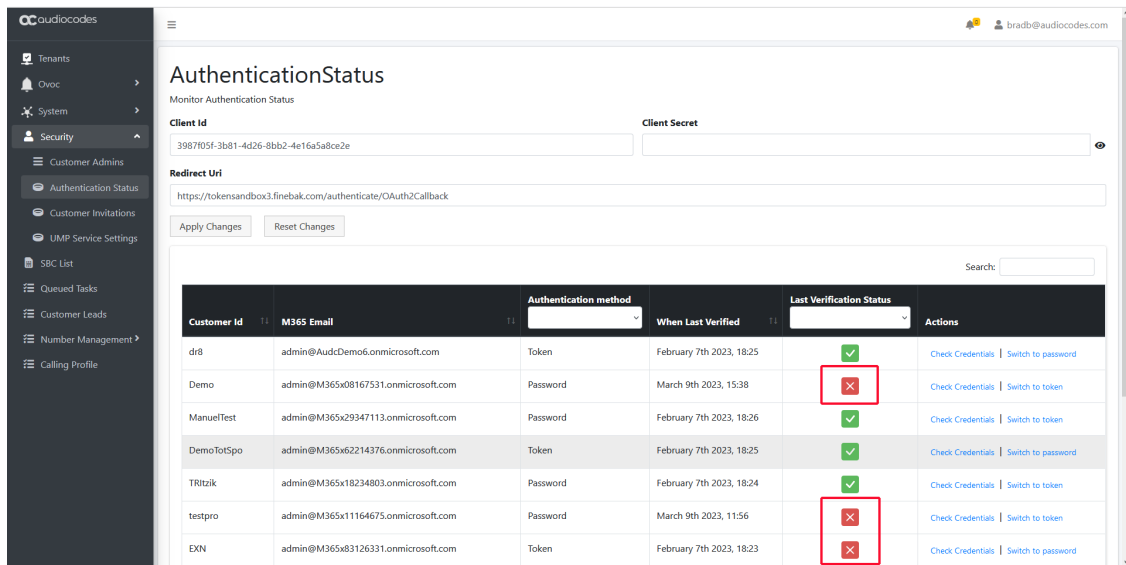
The dbo.MsalError table can be found in SQL Studio, under the SysAdminTenant database. It can be sorted by "Id desc" to view the most recent MsalErrors.

Id	Account	Error	CreatedDate	SessionId	ContextName
1	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.3053901 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
2	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
3	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
4	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
5	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
6	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
7	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
8	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
9	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
10	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
11	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
12	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:28:08.2933803 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
13	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:27:42.9057260 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
14	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:27:42.9057260 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
15	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:27:42.9057260 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
16	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:27:42.9057260 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
17	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:27:42.9057260 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
18	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:27:42.9057260 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
19	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:27:42.9057260 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens
20	adm-prod@technetprocess.com	"MsalThrottledUiRequiredException", "invalid_grant"	2023-03-17 15:27:42.9057260 -0500	630146036400297607	CoOnlineSession: PowerShell and Graph Tokens

➤ To renew expired tokens:

1. In the Multitenant interface, open the Authentication Status page (**Security** menu > **Authentication Status**) to determine which tenants have expired Tokens (see

Authentication Status on page 228).



AuthenticationStatus
Monitor Authentication Status

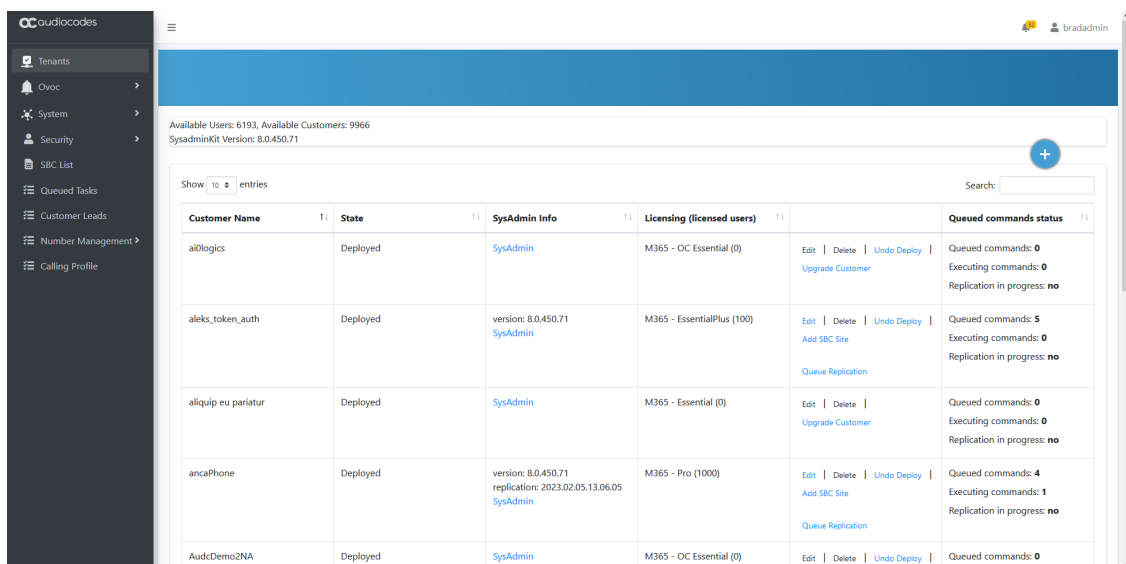
Client Id: 3987f05f-3b81-4d26-8bb2-4e16a5a8ce2e Client Secret: [Redacted]

Redirect Uri: https://tokensandbox3.finebak.com/authenticate/OAuth2Callback

Apply Changes Reset Changes

Customer Id	M365 Email	Authentication method	When Last Verified	Last Verification Status	Actions
dr8	admin@AudcDemo6.onmicrosoft.com	Token	February 7th 2023, 18:25	✓	Check Credentials Switch to password
Demo	admin@M365x08167531.onmicrosoft.com	Password	March 9th 2023, 15:38	✗	Check Credentials Switch to token
ManuelTest	admin@M365x29347113.onmicrosoft.com	Password	February 7th 2023, 18:26	✓	Check Credentials Switch to token
DemoTotSpo	admin@M365x62214376.onmicrosoft.com	Token	February 7th 2023, 18:25	✓	Check Credentials Switch to password
TRitzik	admin@M365x18234803.onmicrosoft.com	Password	February 7th 2023, 18:24	✓	Check Credentials Switch to token
testpro	admin@M365x11164675.onmicrosoft.com	Password	March 9th 2023, 11:56	✗	Check Credentials Switch to token
EXN	admin@M365x83126331.onmicrosoft.com	Token	February 7th 2023, 18:23	✗	Check Credentials Switch to password

- In the Multitenant portal Tenants screen, select the **SysAdmin** link under the tenant whose token you wish to renew.



Available Users: 6193, Available Customers: 9966
SysadminKit Version: 8.0.450.71

Show 10 entries Search:

Customer Name	State	SysAdmin Info	Licensing (licensed users)	Queued commands status
aiOlogics	Deployed	SysAdmin	M365 - OC Essential (0)	Queued commands: 0 Executing commands: 0 Replication in progress: no
aleks_token_auth	Deployed	version: 8.0.450.71 SysAdmin	M365 - EssentialPlus (100)	Queued commands: 5 Executing commands: 0 Replication in progress: no
aliquip eu pariatur	Deployed	SysAdmin	M365 - Essential (0)	Queued commands: 0 Executing commands: 0 Replication in progress: no
ancaPhone	Deployed	version: 8.0.450.71 replication: 2023.02.05.13.06.05 SysAdmin	M365 - Pro (1000)	Queued commands: 4 Executing commands: 1 Replication in progress: no
AudcDemo2NA	Deployed	SysAdmin	M365 - OC Essential (0)	Queued commands: 0

- In the Multitenant portal Navigation pane, select **M365 Configuration**.

audiocodes

Tenant: M365x72025851xTOKEN - [Last sync at: March 17, 2023, 16:24:13]

Microsoft 365 Settings

Last Authentication Status: Failed.

User Name

admin@M365x72025851.onmicrosoft.com

Password (Password not set)

Confirm password

Validate Authentication

Save Microsoft365 settings

Switch to auth token

Grant Consent

4. Click **Switch to username/password**.

audiocodes

Tenant: M365x72025851xTOKEN - [Last sync at: March 17, 2023, 16:24:13]

Microsoft 365 Settings

Last Authentication Status: Failed.

User Name

admin@M365x72025851.onmicrosoft.com

Password (Password not set)

Confirm password

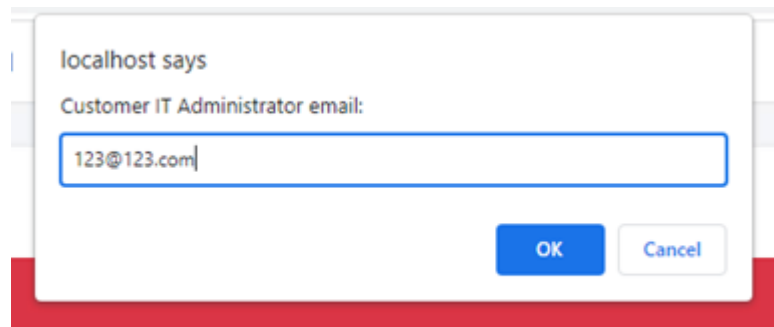
Validate Authentication

Save Microsoft365 settings

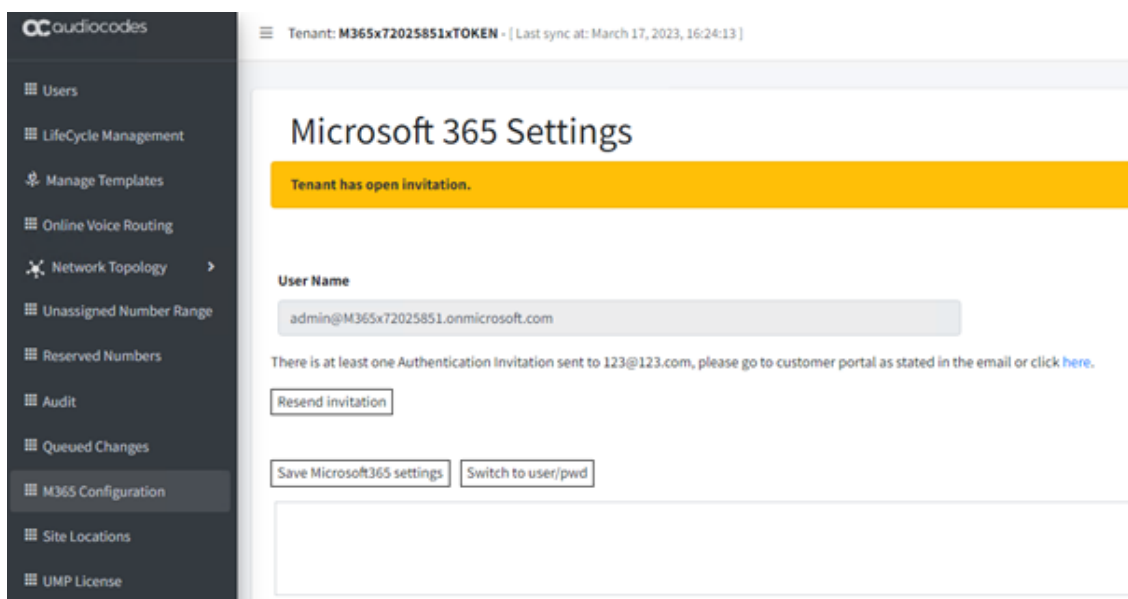
Switch to auth token

Grant Consent

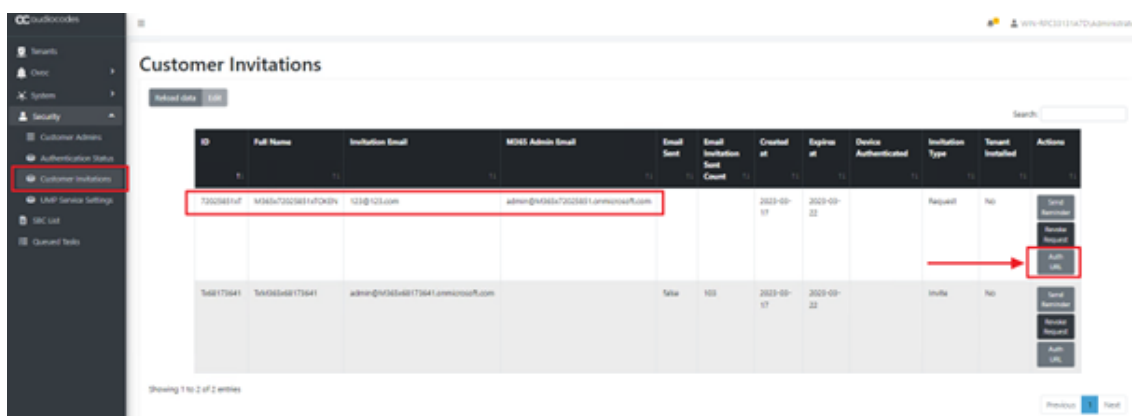
5. Click **Switch to auth token**.
6. An email pop-up window is displayed. Enter the email address to send the token invitation (this does not have to be a real email address).



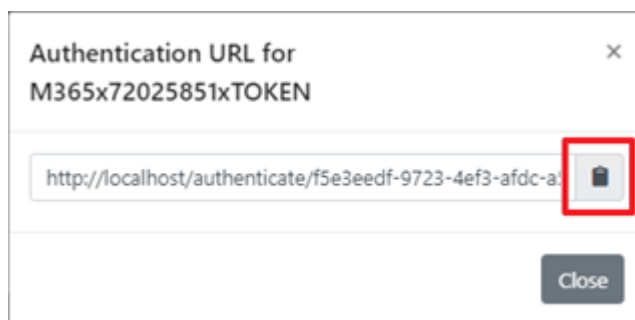
7. Click **OK** to send the invitation to the tenant.



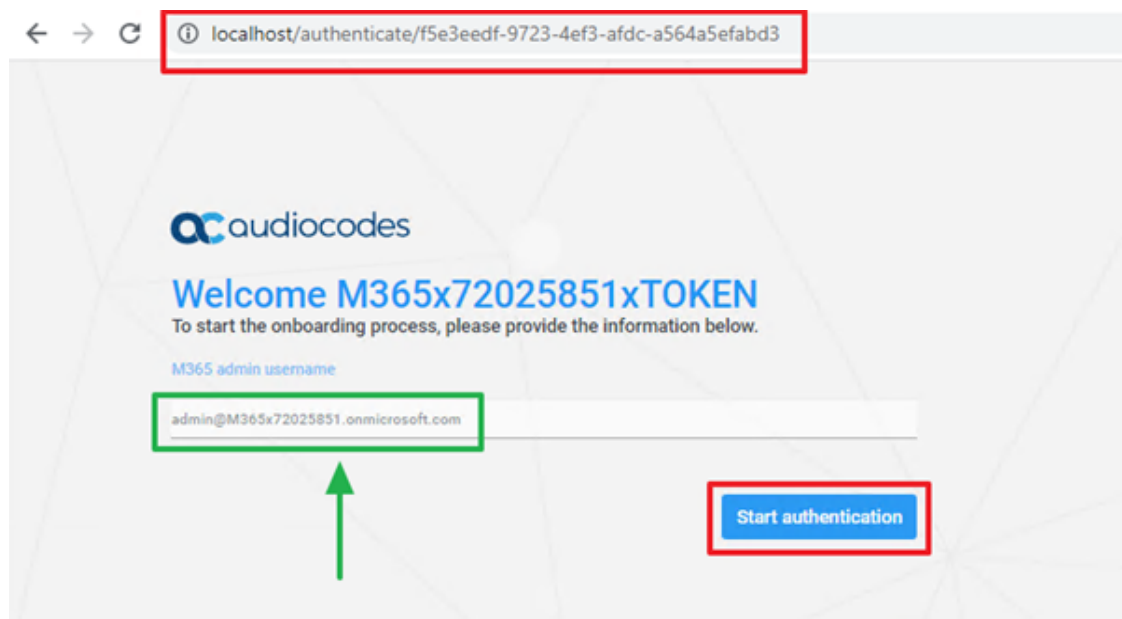
8. Navigate to the **Customer Invitations** screen (**Security** menu > **Customer Invitations**).



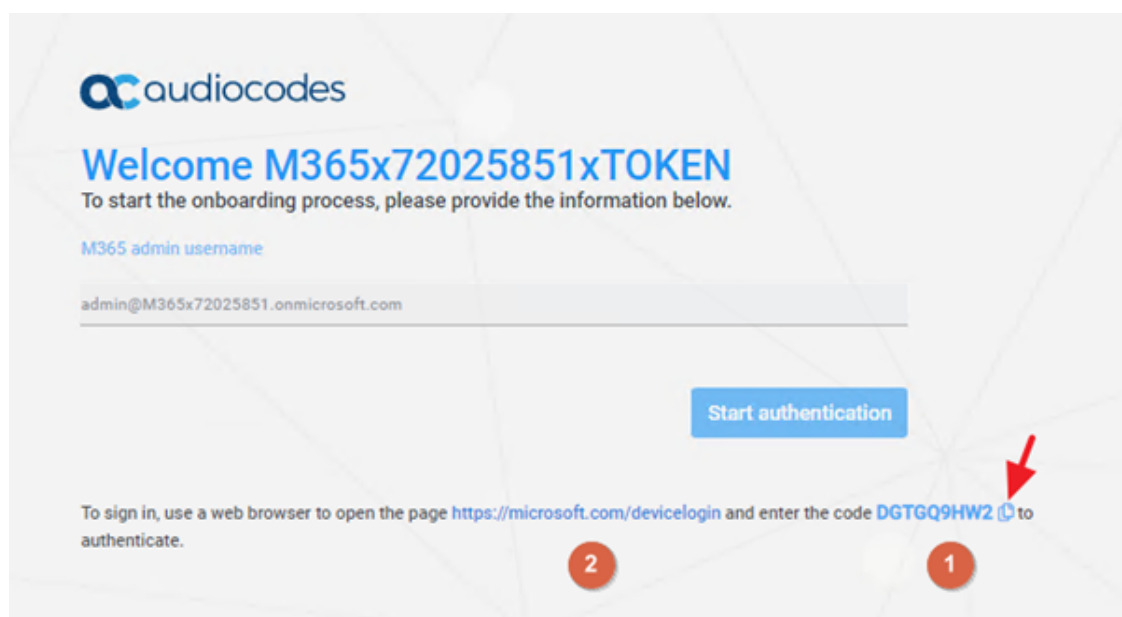
9. Click **Auth URL**.



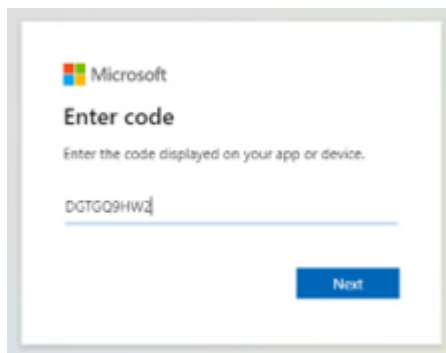
10. Click the clipboard icon to copy the link. Send the link to the customer to begin the Onboarding process. The customer can then paste the link in a new Incognito/private browser window.



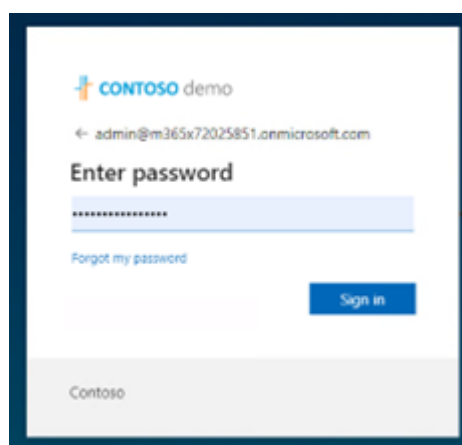
11. Ensure that the correct email is populated in the M365 admin username and then click **Start authentication**.



12. Copy the Code using the clipboard button.
13. Click the Microsoft hyperlink to start the Login Authentication process.



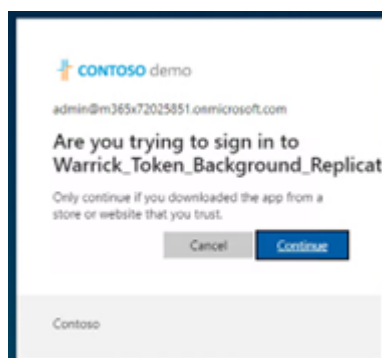
14. Paste the code you previously copied.

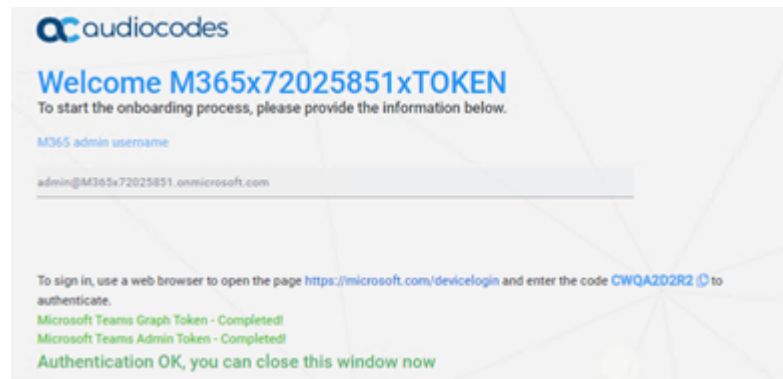
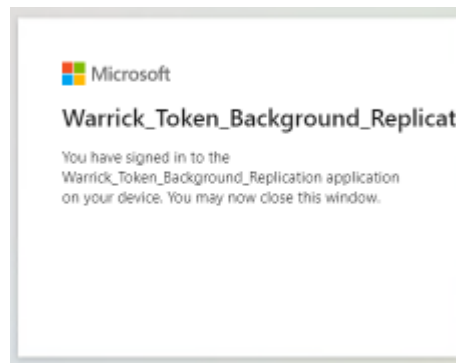


15. Enter in the credentials of the account that was loaded at the beginning of the process. This is also the account that is loaded in the M365 Settings page menu page.

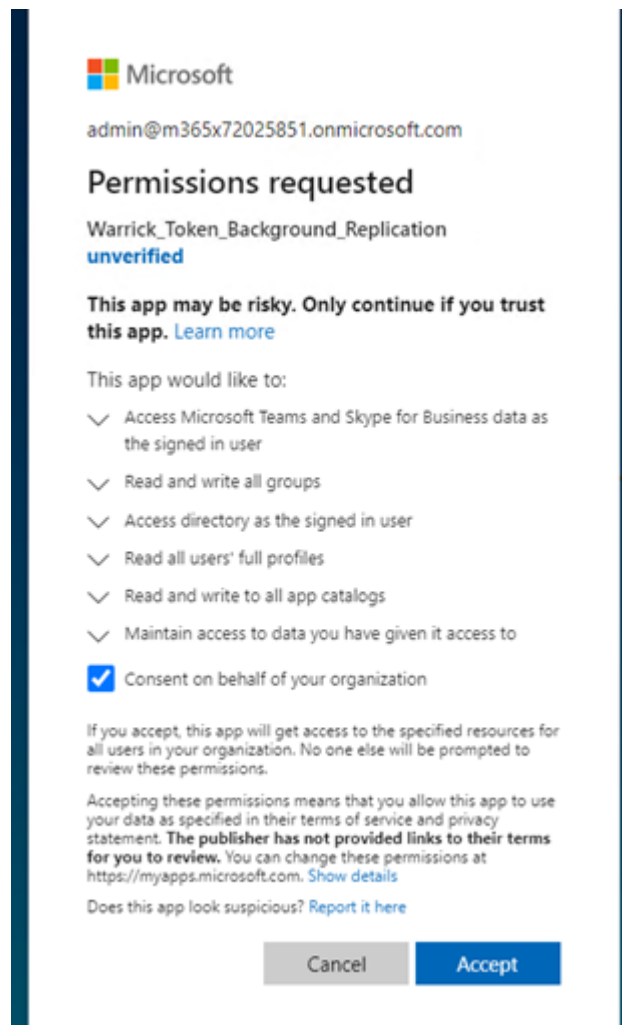


If the Enterprise Application in the customer's Azure environment was not deleted (is still present), then the below windows will appear, and the Permissions requests will not be triggered.





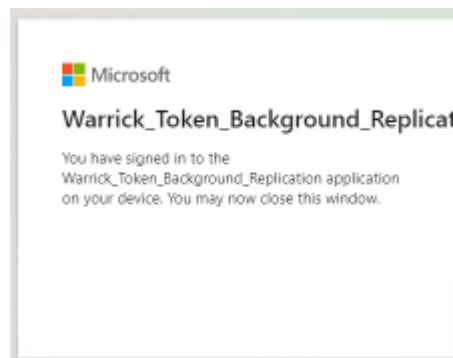
If the Enterprise Application was deleted, then the Permissions requested will appear. See below.



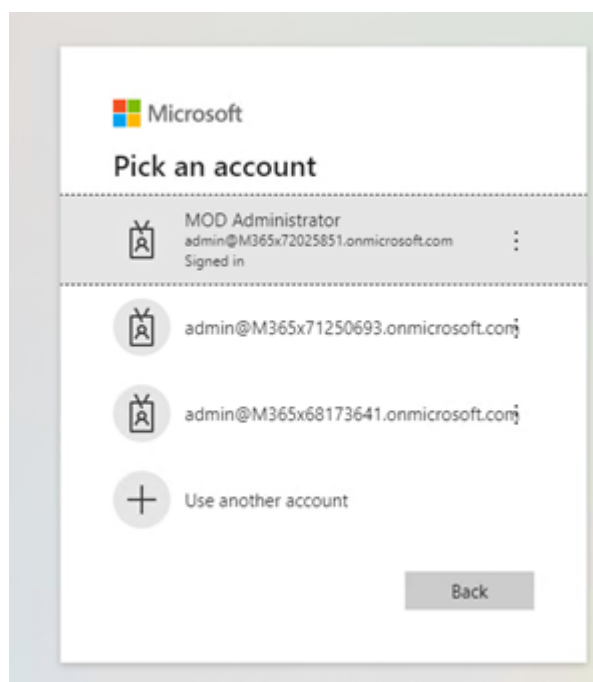
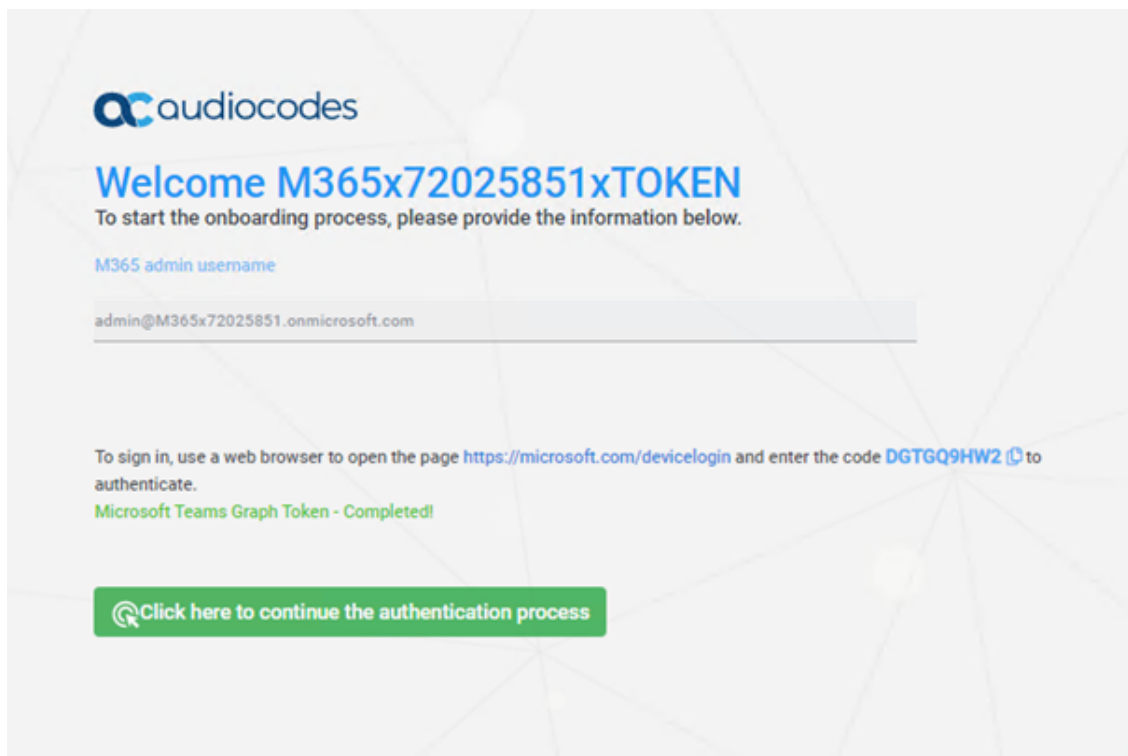
16. Click the check box **Consent on behalf of your organization**.



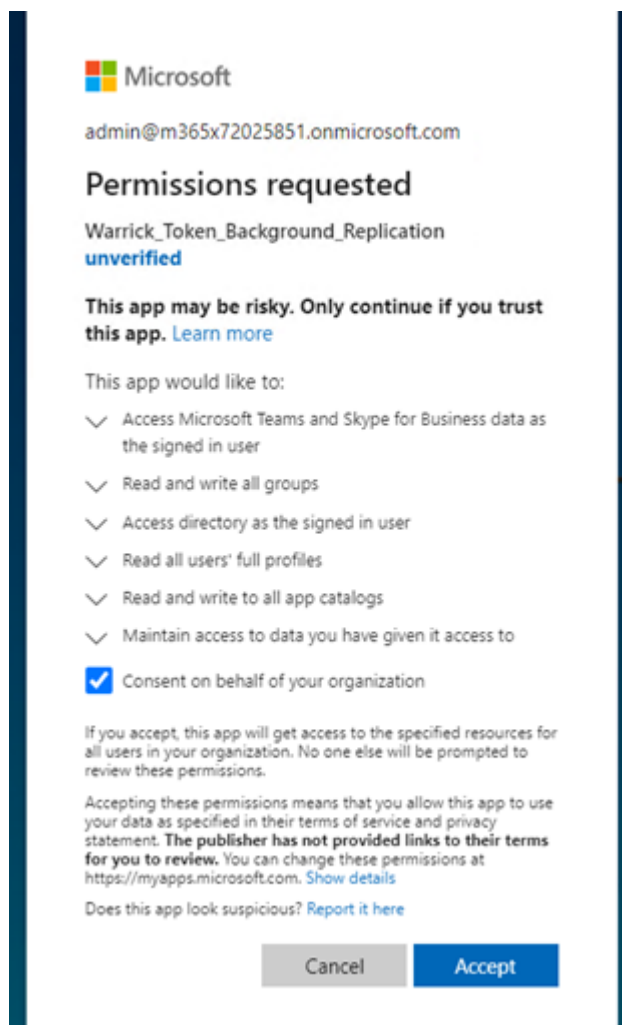
The customer account must have Global Administrator role for this check box to appear. The role can be removed after the token onboarding has completed.



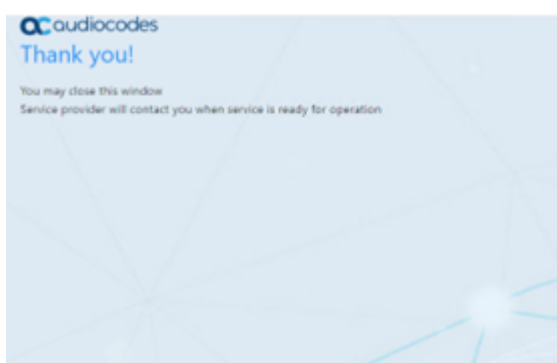
17. Click here to continue the authentication process.

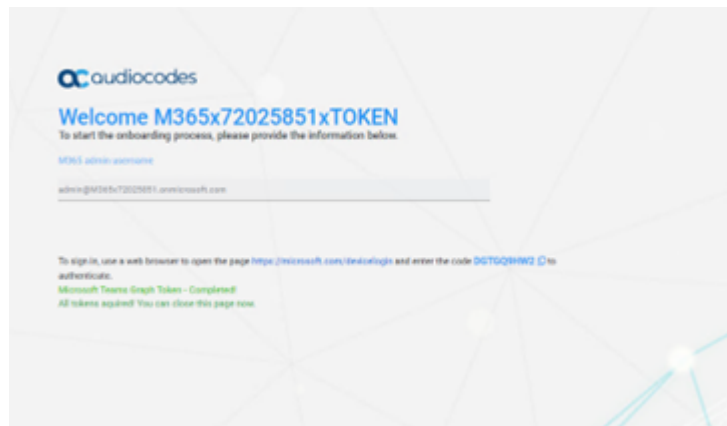


18. Sign in with the same customer IT administrator account used throughout this process.

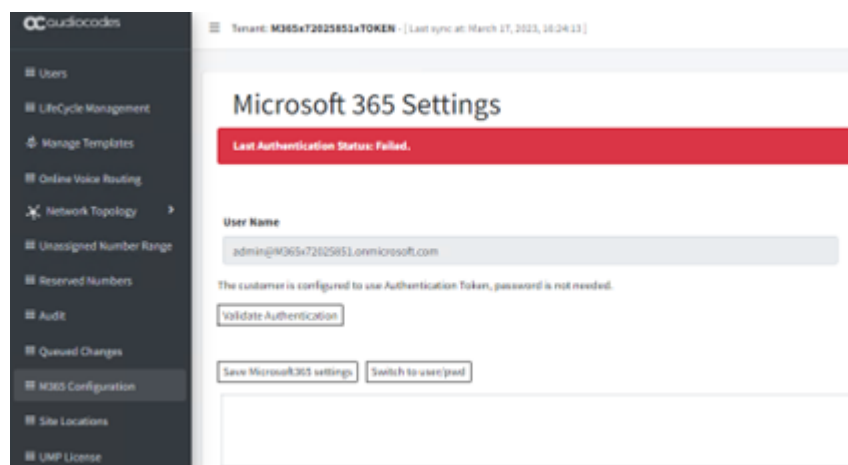


The customer account must have Global Administrator role for this check box to appear. The role can be removed after the token onboarding has completed.

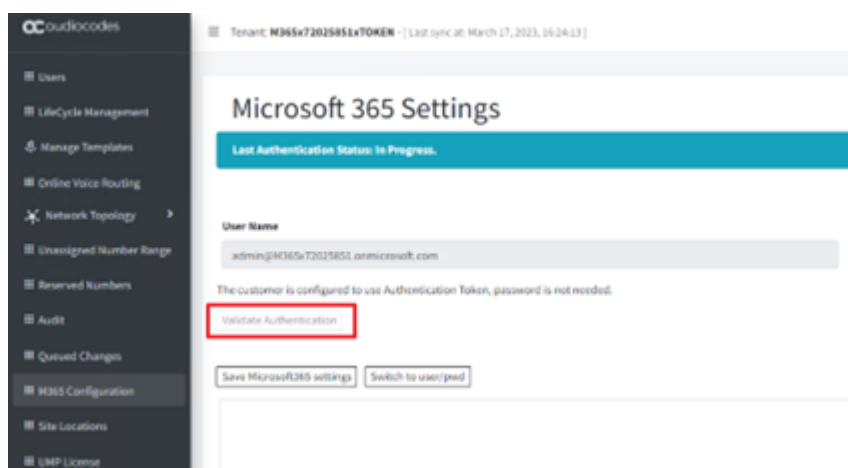




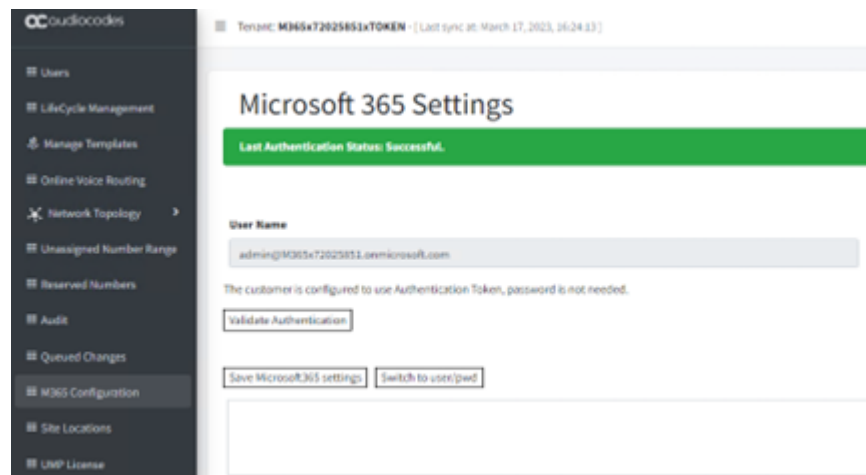
19. When you see this window, return to the original Onboarding window, you will see the “All tokens acquired! You can close this page now.”
20. Return to the M365 Configuration page.



21. Click **Validate Authentication**.



Once successfully validated, the green banner is displayed.



39 SQL Server Configuration

This section describes SQL Server configuration actions.

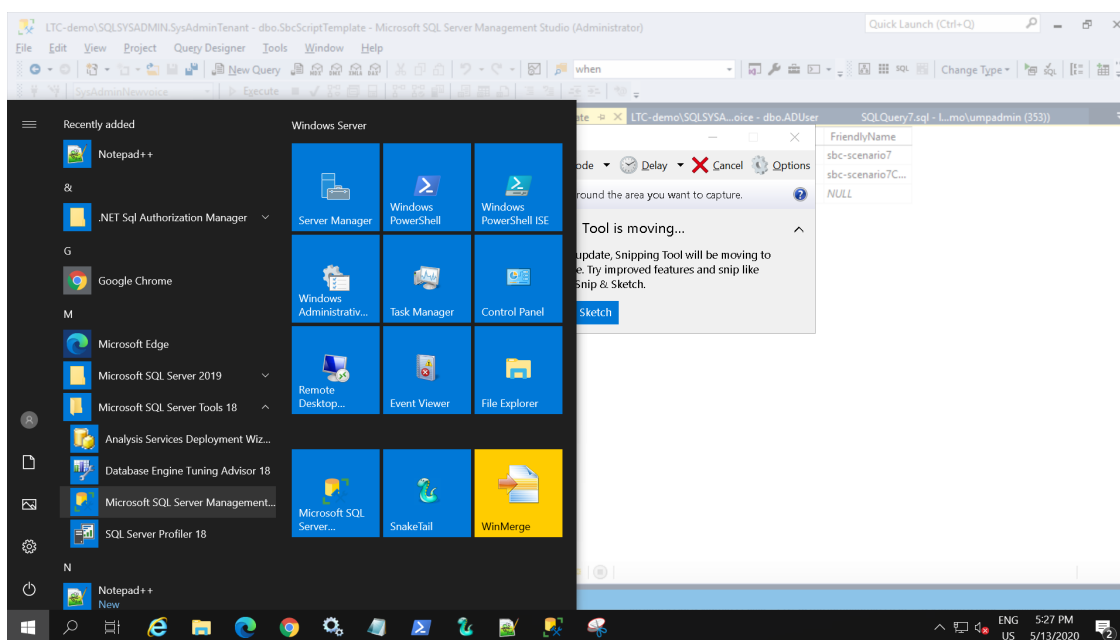
- [Setup Microsoft SQL Server for SBC](#) below
- [SQL Server Database Updates](#) on the next page
- [Optional SQL Script Updates](#) on the next page
- [Updates for Backend SQL Server](#) on page 586
- [Backup All Databases](#) on page 587
- [Configure SQL Server for Enhanced Capacity](#) on page 588

Setup Microsoft SQL Server for SBC

This section describes the setup of the Microsoft SQL server for SBC device.

➤ Do the following:

1. Run Microsoft SQL Server Management Studio.



2. Run Microsoft SQL server Management Studio.
3. Expand tables and select **SysAdminTenant** and **dbo.AppllicationSetting**, and then select Edit Top 200 Rows.
4. Add or edit the row with ID **OvocSbcInfo** to include the following 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"}}]

Id	Value	Machine...
CleanupAge	10	NULL
CustomerAuthenticationPortalUrl	https://livecloud.fixedmobileuc.com/authenticate	NULL
InstallationFolder	c:\acs	NULL
InstallScript	c:\acs\installationScript\install_tenant.ps1	NULL
InvitationEmail	Dear Administrator of {{Customerid}}, We at FixedMobileU...	NULL
InvitationSubject	Welcome {{Customerid}} for joining the FixedMobileUC "Au...	NULL
LicenseKey	eyJ0eXAiOiJV1QlCjhbGciOiJIUzI1Ni9yIj0iDdXN0b21icil6L...	NULL
OvoEnabled	True	NULL
OvoSbcInfo	[{"ipAddress":"13.80.148.30","name":"EMEA","id":10,"sbcInf...	NULL
PublicServerUrl	https://livecloud.fixedmobileuc.com	NULL
ServerDomain	.	NULL
ServicePassword	.	NULL
ServiceUsername	.	NULL
SourcePackage	c:\acs\SysAdminKit	NULL
SysAdminConnectionString	NULL	NULL
TenantDir	c:\acs\tenants	NULL
Whitelabel	AudioCodes	NULL
CustomerInvitation.UserName	apikey	NULL
CustomerInvitation.From	Support@fixedmobileuc.com	NULL
CustomerInvitation.Host	smtp.sendgrid.net	NULL
CustomerInvitation.Port	587	NULL
CustomerInvitation.EnableSsl	True	NULL
CustomerInvitation.DeliveryMethod	Network	NULL

SQL Server Database Updates

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:

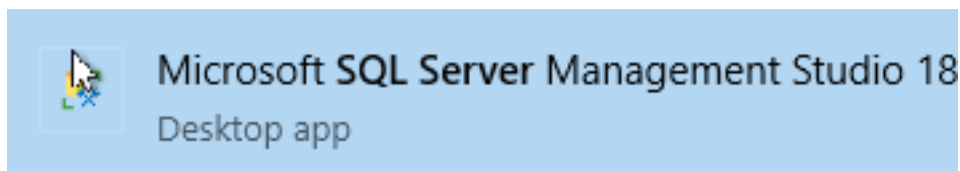
- 10.Add-columns.sql
- 20.RefreshSpf.sql

Optional SQL Script Updates

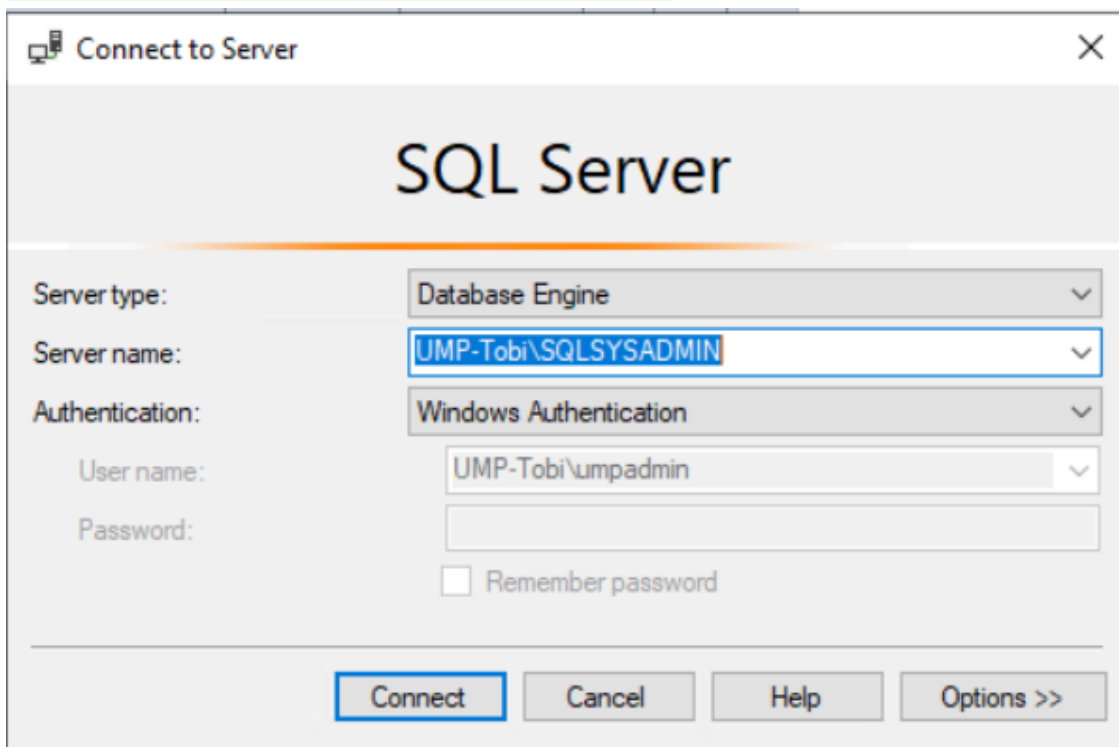
This section describes how to optionally update SQL scripts.

➤ Do the following:

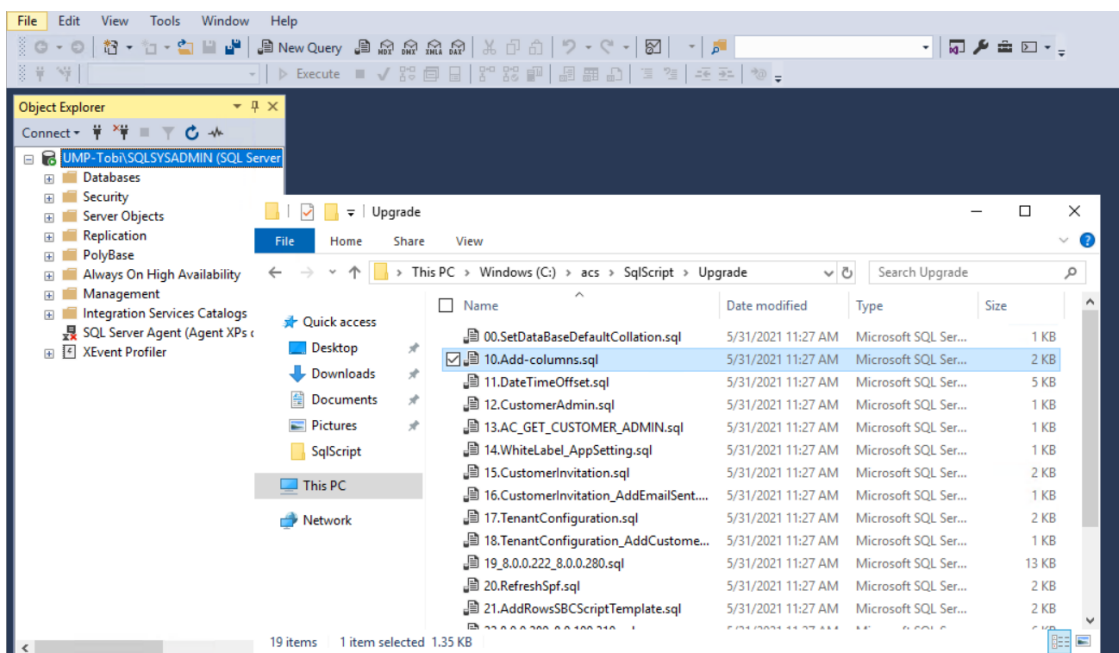
1. Connect to the SQL Server using the following credentials.



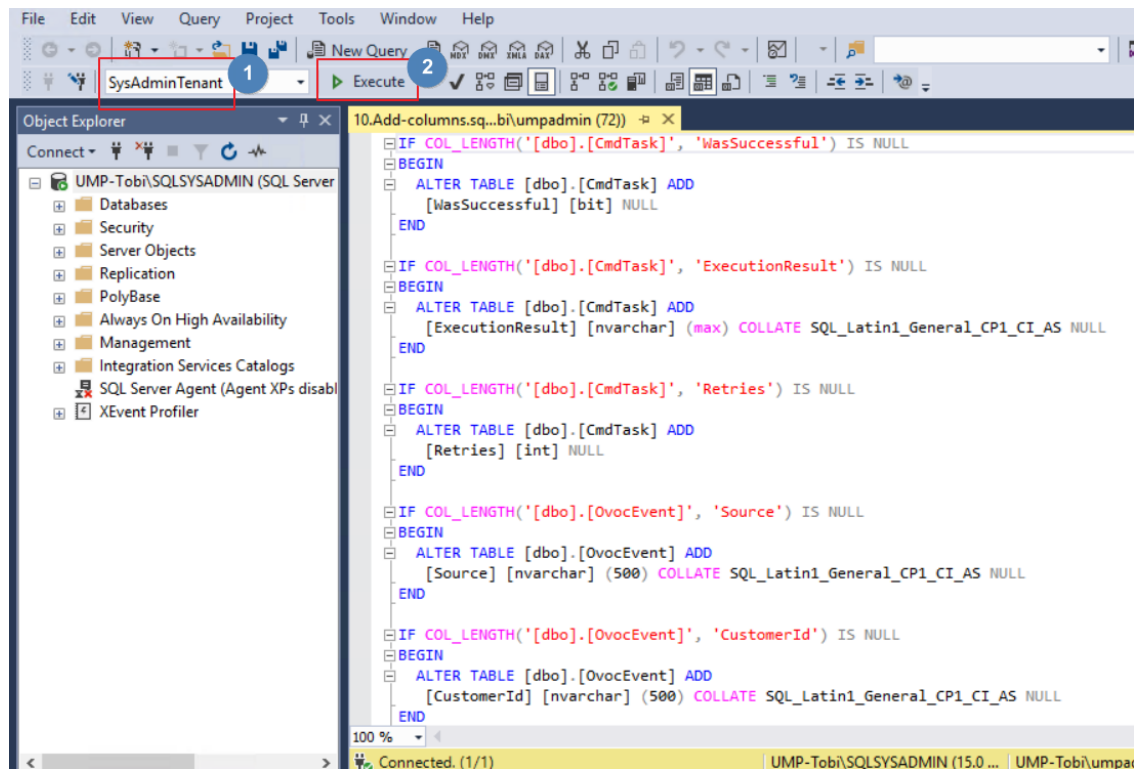
Parameter	Description
Server type	Database Engine
Server name	[servername]\SQLSYSADMIN
Authentication	Windows Authentication



2. Open the SqlScript\Upgrade directory.



3. In the Windows Explorer, select **10.Add-columns.sql** and drag and release it into the grey area in the SQL Manager Studio.



4. Make sure SysAdminTenant database is selected and then press **Execute**.
5. Repeat the above steps for “20.RefreshSpf.sql”.
6. In addition, when UMP-SP is deployed with OVOC, set the **OvocEnabled** parameter to true in the **dbo.ApplicationSetting** in the SysAdminTenant database.

Updates for Backend SQL Server

This section describes the changes required to run when customer databases are deployed on an external SQL backend server.

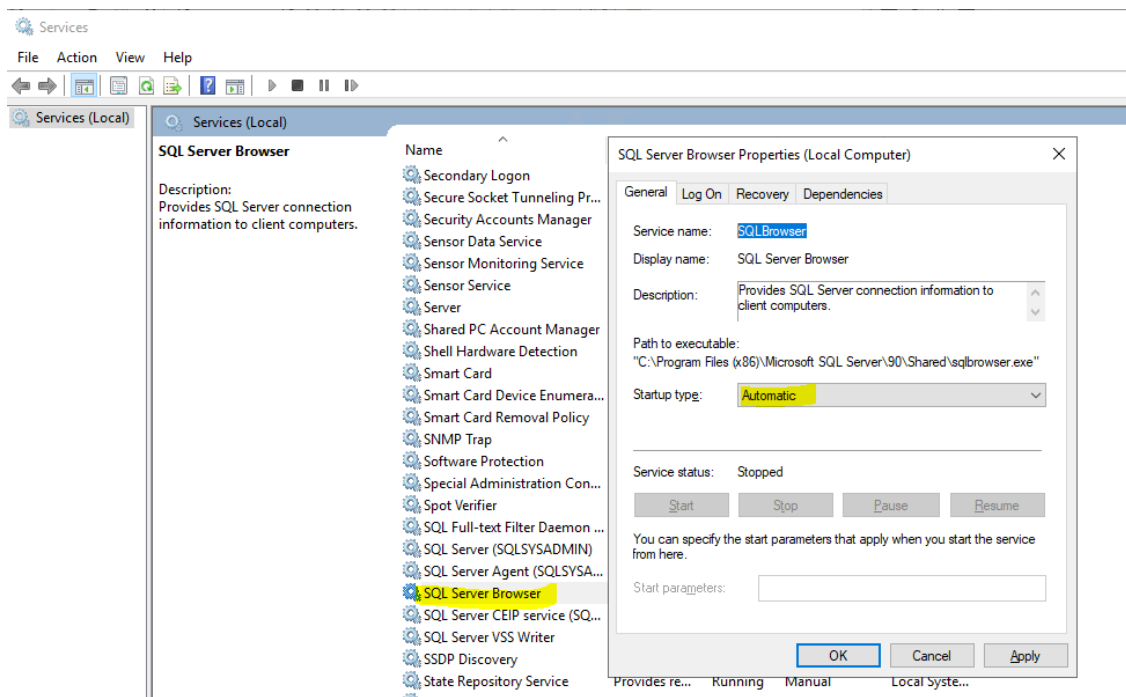


The Backend SQL server username and password must be identical to the service account used for the installation of the UMP server. Create the following directory for database backup for Wyupdates:

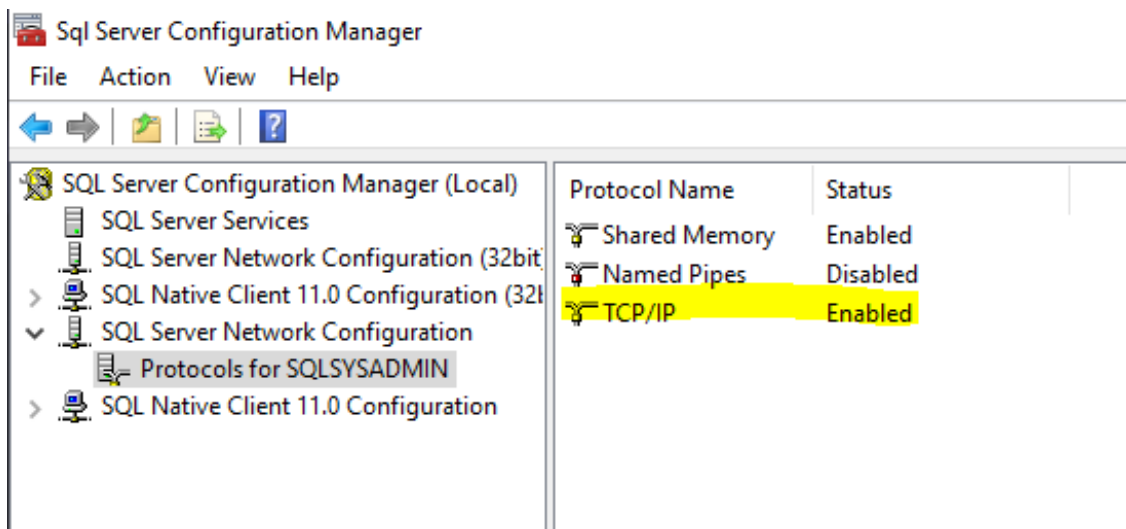
c:/acs/dbbackup/

➤ 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:



3. Enable SQL TCP/IP connection.
4. Open the Sql Server Configuration Manager (under Protocols for SQLSYSADMIN) and set TCP/IP to **Enabled**.

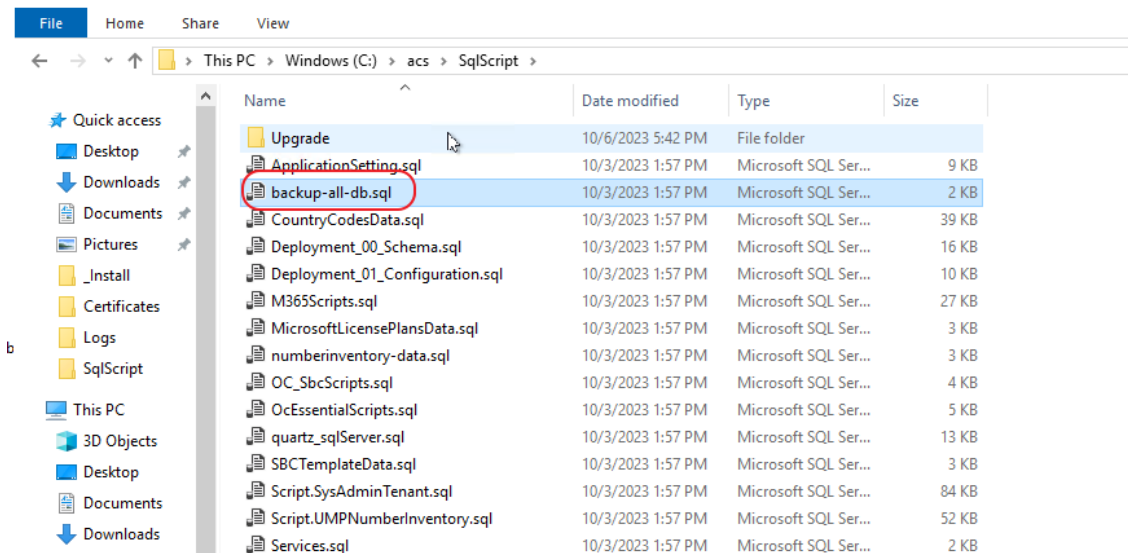


Backup All Databases

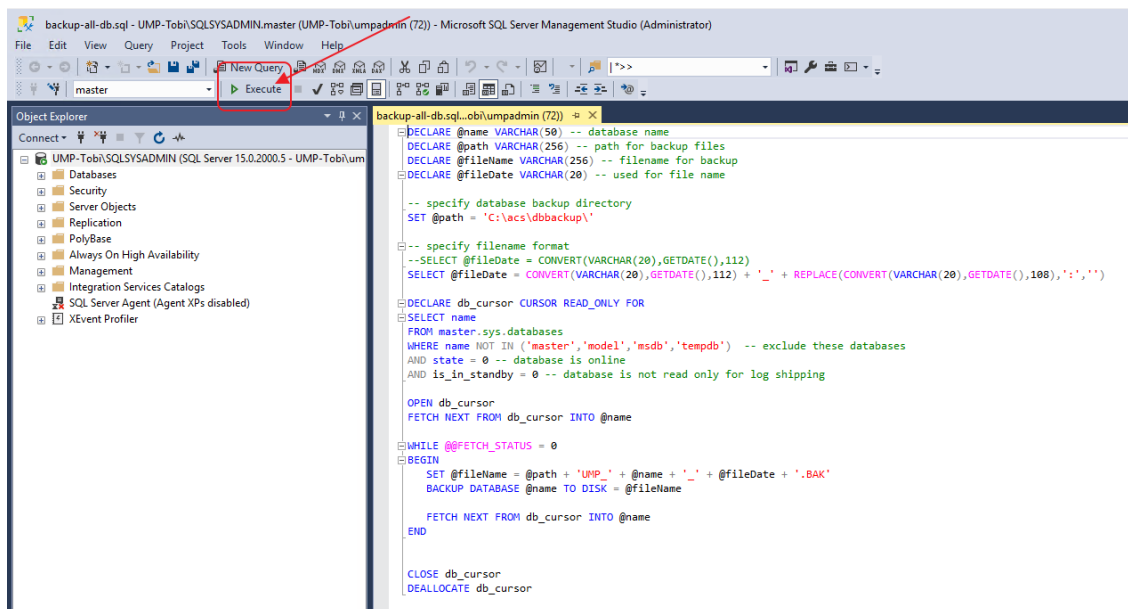
The folder `c:\acs\SqlScript` includes an sql script that creates a backup of all databases named: `backup-all-db.sql`.

➤ To backup all databases:

1. Open the SqlScript folder and open file **backup-all-db.sql**.



2. Click Execute.



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.

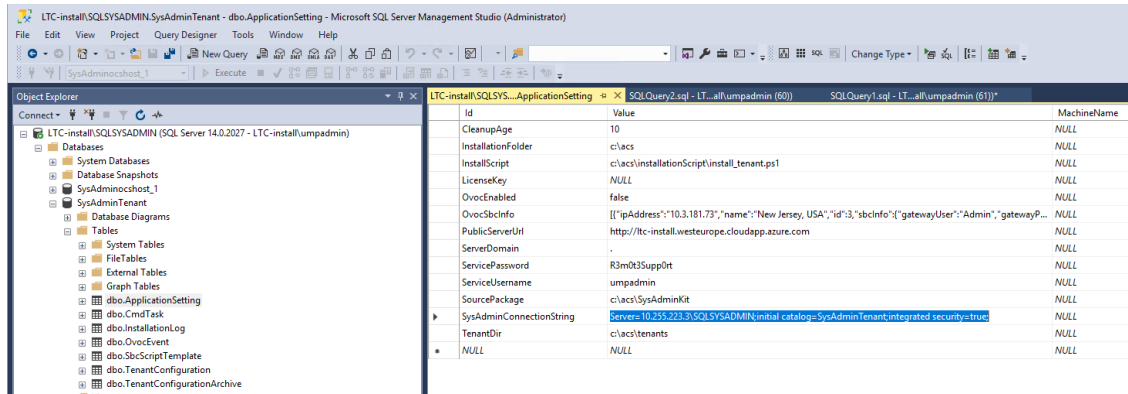
➤ To configure an external SQL server:

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.



Id	Value	MachineName
CleanupPage	10	NULL
InstallationFolder	c:\acs	NULL
InstallScript	c:\acs\installScript\install_tenant.ps1	NULL
LicenseKey	NULL	NULL
OvocEnabled	false	NULL
OvocSbcInfo	[{"ipAddress":"10.3.181.73","name":"New Jersey, USA","id":"3","sbcInfo":{"gatewayUser":"Admin","gatewayP...}	NULL
PublicServerUrl	http://ltc-install.westeurope.cloudapp.azure.com	NULL
ServerDomain	.	NULL
ServicePassword	R3m0t3Suppl0rt	NULL
ServiceUsername	umpadmin	NULL
SourcePackage	c:\acs\SysAdminKit	NULL
SysAdminConnectionString	Server=10.255.223.3\SQLSYSADMIN;initial catalog=SysAdminTenant;integrated security=true;	NULL
TenantDir	c:\acs\tenants	NULL
NULL	NULL	NULL



- 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.

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: <https://www.audiocodes.com/corporate/offices-worldwide>

Website: <https://www.audiocodes.com/>

Documentation Feedback: <https://online.audiocodes.com/documentation-feedback>

©2024 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, and AudioCodes Room Experience 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-26388

