

User Management Pack™ 365 Service Provider Edition

Version 8.0.100



Table of Contents

1	Introduction	13
<hr/>		
	Installing User Management Pack 365.....	15
2	Requirements	17
2.1	Azure Deployments Requirements	17
2.2	Data Center Deployments Requirements	18
3	UMP 365 SP Edition Installation.....	19
3.1	Installing the Prerequisites.....	19
3.2	Operating System Roles and Features	20
3.3	Installing SQL Server.....	20
3.4	Installing SQL Server Management Studio	23
3.5	Installing ASP.NET SQL Authorization Manager	25
3.6	Installing ASP.NET Framework 4.8	29
3.7	Installing Skype for Business Online PowerShell	29
3.8	Installing SharePoint Online PowerShell.....	29
3.9	Installing ASP.NET Core	29
3.10	Installing ASP.NET Core Hosting Pack.....	29
3.11	Installing Azure Active Directory PowerShell Components	29
3.12	Installing UMP-SP	29
3.13	Updating UMP after Installation	33
3.13.1	Run Changes on the External SQL Server.....	34
3.14	Enable OVOC.....	35
3.15	Reinstall OVOC Alarm Agent.....	35
3.16	Accessing the UMP 365 for the First Time.....	36
3.16.1	Invitation Settings	37
3.16.2	Email Settings.....	38
3.16.3	Public Portal URL Setting	39
3.16.4	App Registration	40
3.16.5	WEB Application Setting (optional).....	43
3.16.6	Configure License.....	45
3.16.6.1	Installing the UMP 365 License.....	45
3.17	Setup the OVOC Connection on UMP (Optional)	46
3.17.1	Retrieve your UMP 365 Users License	47
3.18	Initial SBC Configuration	49
3.18.1	SBC Setup	49
3.18.2	SBC Configuration	50
3.19	M365 Configuration (Optional).....	52
3.20	UMP Networking Configuration.....	52
3.20.1	UMP Firewall Configuration.....	53
3.21	VPN Configuration (Optional)	53
3.22	SQL License Guidelines - Optional.....	55

User Management Pack 365 SP Edition.....	57
Onboarding a New Tenant (Microsoft 365 Customer).....	57
4 Overview	59
4.1 Provider Main Screen View	60
5 Adding a New M365 Tenant.....	61
5.1 Prerequisites	61
5.1.1 Registering a Subdomain Name for an M365 Tenant	61
5.1.2 Activating the Providers Domain	62
5.2 Adding the new Customer M365 Tenant.....	63
5.2.1 Securing Connection with Microsoft 365	63
5.2.2 Pending Requests	69
5.2.3 Adding Customer	71
User Management Pack 365 SP Edition.....	77
6 User Management Pack 365	79
6.1 General Access to UMP 365	79
6.2 UMP 365 Managing Users Replication (Tenant Portal).....	81
7 Provider Portal (Provider link)	83
7.1 Provider Portal Searching for Users	83
7.2 Edit Users.....	84
7.3 Assigning Phone Numbers	85
7.4 Lifecycle Management.....	87
7.5 Managing Unassigned Number Ranges	87
7.6 Managing Templates	88
7.7 Binding Templates to Security Groups.....	91
7.8 Configuring Online Voice Routing.....	93
7.8.1 PSTN Usage	93
7.8.2 Voice Routing Policy.....	94
7.8.2.1 Adding Voice Routing Policy	95
7.8.2.2 Editing Voice Routing Policy	95
7.8.2.3 Deleting/Canceling Voice Routing Policy	96
7.8.3 Voice Route	97
7.8.4 PSTN Gateways	98
7.8.5 Dial Plan & Normalization Rules.....	98
7.9 Reserving M365 Tenant Phone Numbers.....	102
7.10 Audit and Roll Back Historical Changes.....	103
7.11 Queued Changes	104
7.12 Office 365 Setting.....	105
8 Multitier Admin Access.....	107
9 Browser setting - IETF Same Site Cookie Attribute	109
10 Backup and Restore Customer Tenant	111
10.1 Backup the Customer Tenant Database	111
10.2 Restore the Customer Tenant Database	114

10.2.1	Restore to a Point-in-Time.....	117
A	UMP SP Installation on Azure	121
A.1	Installing the Prerequisites.....	121
A.1.1	Operating System Roles and Features	121
A.1.2	SQL Server Express	122
A.1.3	Install SQL Server Management Studio	125
A.1.4	Install ASP.NET SQL Authorization Manager	127
A.1.5	Install ASP.NET framework 4.8	131
A.1.6	Install SkypeOnline Powershell	131
A.1.7	Install Sharepoint Online Powershell.....	131
A.1.8	Install ASP.NET Core	131
A.1.9	Install ASP.NET Core Hosting Pack.....	131
A.1.10	Install Azure Active Directory PowerShell Components.....	132
A.2	(Optional) Install Support Tools for Debugging	132

List of Figures

Figure 2-1: UMP Azure Deployment	17
Figure 3-1: SQL Server Installation Server	20
Figure 3-2: SQL Server 2019 Setup Step 1	21
Figure 3-3: SQL Server 2019 Setup Step 2	21
Figure 3-4: SQL Server 2019 Setup Step 3	22
Figure 3-5: SQL Server 2019 Setup Step 4	22
Figure 3-6: SQL Server 2019 Setup Step 5	22
Figure 3-7: SQL Server 2019 Setup Step 6	23
Figure 3-8: Install SQL Server Management Studio Step 1	23
Figure 3-9: Install SQL Server Management Studio Step 2	24
Figure 3-10: Install .NET SQL Authorization Manager Step 1	25
Figure 3-11: Install .NET SQL Authorization Manager Step 2	25
Figure 3-12: Install .NET SQL Authorization Manager Step 3	26
Figure 3-13: Install .NET SQL Authorization Manager Step 4	26
Figure 3-14: Install .NET SQL Authorization Manager Step 5	27
Figure 3-15: Install .NET SQL Authorization Manager Step 6	27
Figure 3-16: Install .NET SQL Authorization Manager Step 7	28
Figure 3-17: Install .NET SQL Authorization Manager Step 8	28
Figure 3-18: File Properties	30
Figure 3-19: Local Security Policy Management Console	31
Figure 3-20: Computer Management	31
Figure 3-21: Computer Management (Local)	32
Figure 3-22: Installation Console	32
Figure 3-23: Wupdate Tool	33
Figure 3-24: SQL Browser Service	34
Figure 3-25: SQL Server Configuration Manager	34
Figure 3-26: Uninstall App	35
Figure 3-27: Multi-Tenant Access (Provider Only)	36
Figure 3-28: Invitation Setting	37
Figure 3-29: Email Example	37
Figure 3-30: Email Settings	38
Figure 3-31: Customer Authentication portal URL Setting	39
Figure 3-32: New App Registration	40
Figure 3-33: Redirect URI's	40
Figure 3-34: Add URI	41
Figure 3-35: Add Public Portal URL	41
Figure 3-36: Implicit Grant	41
Figure 3-37: Copy the Application (client) ID Value	42
Figure 3-38: Paste the Application (client) ID Value	42
Figure 3-39: Edit WEB Application	43
Figure 3-40: Edit WEB Application	43
Figure 3-41: New App Registration	44
Figure 3-42: System/License Key View	45
Figure 3-43: One Voice Operations Center Device Information	46
Figure 3-44: Set One Voice Operations Center Configuration	47
Figure 3-45: Select SQL Server Management Studio Tool	49
Figure 3-46: Select SQL Server Management Studio Tool	50
Figure 3-47: SBC Default Configuration	50
Figure 3-48: SBC Script Template	51
Figure 3-49: UmpAdmins user members	55
Figure 3-50: Tenant Admin User (Windows)	55
Figure 3-51: Account List	56
Figure 4-1: Provider Main Screen View	60
Figure 5-1: Adding Providers Domain	61
Figure 5-2: Active Users	62
Figure 5-3: M365 Tenants	63
Figure 5-4: Add New Customer	64

Figure 5-5: Add New Customer	64
Figure 5-6: Send link to customer IT administrator for Authentication	65
Figure 5-7: Message to IT Administrator	65
Figure 5-8: Enter Microsoft 365 Unified Communications Environment	66
Figure 5-9: Customer Authentication	67
Figure 5-10: Enter Code	67
Figure 5-11: Sign in	68
Figure 5-12: Enter Password (replace screen)	68
Figure 5-13: Authentication Complete	68
Figure 5-14: Pending Customers	69
Figure 5-15: List of Pending Customers	69
Figure 5-16: Send Customer Email	70
Figure 5-17: Revoke Request	70
Figure 5-18: Add Customer	71
Figure 5-19: Microsoft 365 Settings	71
Figure 5-20: Voice Route	72
Figure 5-21: Select Region	74
Figure 5-22: Select Carrier	74
Figure 5-23: Carrier Registration	75
Figure 5-24: Enable CAC	75
Figure 5-25: Add Prefix	76
Figure 5-26: Configuration Complete	76
Figure 6-1: Multi-Tenant Access (Provider Only)	79
Figure 6-2: UMP 365 Authentication	80
Figure 6-3: Customer Link UMP 365 Authentication	80
Figure 7-1: UMP 365 Home page - Provider Portal	83
Figure 7-2: Users List	83
Figure 7-3: Edit a User	84
Figure 7-4: Example User Policy	84
Figure 7-5: Grant Admin Rights	85
Figure 7-6: Assign Phone to Subscriber	85
Figure 7-7: Assign Phone Numbers	86
Figure 7-8: Unassigned Number Range	87
Figure 7-9: Number Range	87
Figure 7-10: Telephony Template	88
Figure 7-11: Add Policy	89
Figure 7-12: Set Policy Value	90
Figure 7-13: Set Telephony Setting	90
Figure 7-14: Life Cycle Management	91
Figure 7-15: Binding Template to AAD Security Group	91
Figure 7-16: PSTN Usage	93
Figure 7-17: PSTN Usage	94
Figure 7-18: Voice Routing Policy	94
Figure 7-19: Add New Voice Routing Policy	95
Figure 7-20: Edit Voice Routing Policy Step 1	95
Figure 7-21: Edit Voice Routing Policy Step 2	96
Figure 7-22: Delete Voice Routing Policy	96
Figure 7-23: Edit Voice Routing Policy - Step 2	96
Figure 7-24: Voice Routes	97
Figure 7-25: Add New Voice Route	97
Figure 7-26: Normalization Rules	98
Figure 7-27: Add New Normalization Rules	99
Figure 7-28: Dial Plan	99
Figure 7-29: Add New Dial Plan	100
Figure 7-30: Select Dial Plan	100
Figure 7-31: Edit Dial Plan	101
Figure 7-32: Reserved Numbers	102
Figure 7-33: Reserved Number	102

Figure 7-34: Rollback 103

Figure 7-35: Queued Changes 104

Figure 7-36: Queued Changes Entry Tooltip..... 104

Figure 7-37: Queued Actions..... 105

Figure 7-38: M365 Configuration..... 105

Figure 8-1: Access to the Portal 107

Figure 8-2: SSO with Azure Active Directory 107

Figure 8-3: SSO with Azure Active Directory 108

Figure 8-4: UMP 365 Customer Portal 108

Figure 9-1: Chrome Setting 109

Figure 9-2: Edge Setting..... 109

Figure 9-3: FireFOX Setting - about:config 110

Figure 9-4: FireFOX Setting 110

Figure 10-1: SQL Server 111

Figure 10-2: Run Back Up Task 112

Figure 10-3: Select the Database Destination..... 112

Figure 10-4: Database Backup Completed Successfully 113

Figure 10-5: Select the Database resource..... 114

Figure 10-6: Select the Device 114

Figure 10-7: Select the Backup File 115

Figure 10-8: Confirm the Backup File..... 116

Figure 10-9: Confirm the Backup File..... 116

Figure 10-10: Select the Backup File 117

Figure 10-11: Restore to point of time – Step 1 118

Figure 10-12: Restore to point of time – Step 2 118

Figure 10-13: Restore to point of time – Step 3 119

Figure A-1: SQL Server Installation Center..... 122

Figure A-2: SQL Install Rules 123

Figure A-3: Feature Selection 123

Figure A-4: Instance Configuration..... 124

Figure A-5: SQL Server Database Engine Configuration..... 124

Figure A-6: Authentication Mode..... 124

Figure A-7: Complete 125

Figure A-8: Microsoft SQL Server Management Studio 125

Figure A-9: Restart Management Studio..... 126

Figure A-10: NetSqlAzMan..... 127

Figure A-11: Welcome to Setup Wizard 128

Figure A-12: NET SQL Authorization Manager Information 128

Figure A-13: Microsoft Public License Agreement 129

Figure A-14: Select Installation Folder 129

Figure A-15: .NET Developer Documentation..... 130

Figure A-16: NetSQL Man Storage 130

Figure A-17: Confirm Installation..... 131

List of Tables

Table 3-1: UMP Ports Networking	53
Table 3-2: VPN Configuration	53
Table 3-3: VPN Tunnel Ports	54
Table 5-1: Microsoft 365 Settings.....	66
Table 5-2: Microsoft 365 Settings.....	72
Table 5-3: Direct Routing Configuration	73
Table 7-1: Office 365 Settings	106

This page is intentionally left blank.

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-24-2021

WEEE EU Directive

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

Customer Support

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

Stay in the Loop with AudioCodes



Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
26343	Initial release of this document.
26344	Update for software version 8.0.100
26348	Update to Section "Activating the Providers Domain"

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>.

This page is intentionally left blank.

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, SharePoint 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.

This document describes the following:

- **Part I:** [Installation of the UMP 365 SP Edition](#)
- **Part II:** [UMP 365 SP Edition: Onboarding of a new Tenant \(Microsoft 365 customer\)](#)
- **Part III:** [UMP 365 application version 8.0.100 2nd day operation](#)



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

This page is intentionally left blank.

Part I

Installing User Management Pack 365

2 Requirements

This version of AudioCodes' User Management Pack 365 SP can be deployed in the environment described below.

2.1 Azure Deployments Requirements

- **Small System up to 25 Tenants (M365 Customers)**
 - VM – B4ms (4 vCPUs, 16G RAM, 64G Local SSD)
 - ◆ SQL – SQL Express
 - ◆ OS – Windows server 2019 - **US English**
 - ◆ Managed Disk – Premium SSD 256G
- **Mid-Size System up to 250 Tenants (M365 Customers)**
 - VM WEB – B2ms (2 vCPUs, 8G RAM, 16G Local SSD)
 - ◆ SQL – SQL Express
 - ◆ OS – Windows server 2019 - **US English**
 - VM Admin - B8ms (8 vCPUs, 32G RAM, 64G Local SSD)
 - ◆ SQL – SQL 2017 Std edition or Higher
 - ◆ OS – Windows server 2019 - **US English**
 - Managed Disk – Premium SSD , Size = 80G System + 5G per Tenant
- **Above 250 Tenants, up to 1,250 Tenants**
 - In addition to the Mid-Size, the system will require additional VM Admin for every 250 Tenants
 - VM WEB – Upgrade to B8ms (8 vCPUs, 32G RAM, 64G Local SSD)
 - VM Admin - B8ms (8 vCPUs, 32G RAM, 64G Local SSD) per 250 Tenants.
 - ◆ SQL – SQL 2017 Std edition or Higher
 - ◆ OS – Windows server 2019 - **US English**
- **Backup (optional) – Additional disk**
 - Premium SSD – Minimum 128G, max 5G Per Tenant (average 2G per Tenant)

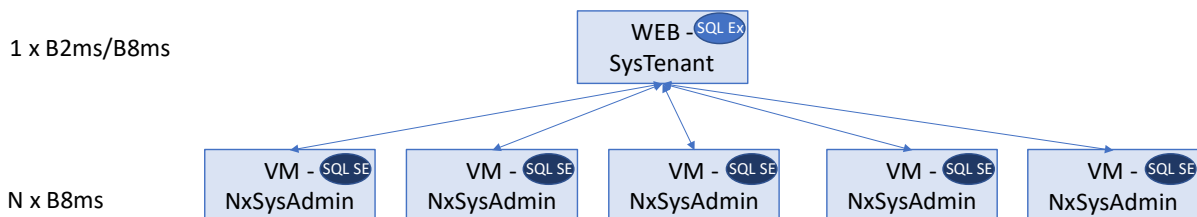


Note: The OS and SQL License are not included in the product pricing (UMP CPN). Customers will need to order it separately.



Note: For Azure Environment Installation guide lines, please refer to Appendix A.

Figure 2-1: UMP Azure Deployment



2.2 Data Center Deployments Requirements

The below describes the Data Center deployment Server requirements.

■ Base configuration – Up to 100 Tenants

- 4 core CPU
- 32 GB RAM
- 512 GB HDD
- SQL server 2017 Std edition or Higher
- OS – Windows Server 2019 – **US English**
- 1GB Ethernet

■ Guidelines for additional Tenant:

- RAM – 0.1 GB per Tenant
- Disk Size – System requirement of 80 GB + 1 GB per Tenant.

■ Backup (Option) – Additional Disk

- Minimum 128G, max 1 GB Per Tenant (large Tenants over 30,000 users can consume 2 GB per Tenant)



Note: The OS and SQL license are not included in the product pricing (UMP CPN). Customers must order them separately. For specific information on the SQL license, see Section 3.22.

3 UMP 365 SP Edition Installation

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.

3.1 Installing the Prerequisites

This section describes how to install the prerequisites.

➤ **Do the following:**

1. Download files to your PC and unblock as required at : https://downloads-audiocodes.s3.amazonaws.com/Download/AC_UMP_MT_ISO.html
2. Mount the UMP-MT ISO file.
3. Before UMP SP can be installed, the server needs to be prepared by installing the following prerequisites:
 - Install the operating system required roles and features (see Section 3.2)
 - Install the SQLSYSADMIN SQL server instance (see Section 3.3)
 - Install SQL management studio (see Section 3.4)
 - Install NetSQLAzMan (see Section 3.5)
 - Install dotnet 4.8 (see Section 3.6)
 - Install SkypeOnlinePowershell (see Section 3.7)
 - Install SharepointOnline Powershell (see Section 3.8)
 - Install ASP.NET core 3.1 runtime (see Section 3.9)
 - Install ASP.NET core 3.1 Windows Hosting Bundle installer (see Section 3.10)
 - Install azureAD Powershell with PowerShell commands (see Section 3.11)

All these prerequisites are currently on the installation ISO in the prerequisites folder and numbered 1-10 for the processing order. On all backend SQL servers, install the following prerequisite components:

- Install the SQLSYSADMIN SQL server instance
- Install SQL management studio (optional as it can be managed from the first server)



Note: The SQL server version that is provided on the ISO is SQL Express and should only be used during lab deployments. In production, SQL Server Standard Edition is required on all servers hosting customer databases.

3.2 Operating System Roles and Features

Issue the following PS cmdlet (in **1. OS Roles and Features**):

- Install-WindowsFeature Telnet-Client, Web-Server, Web-Mgmt-Tools, Web-Mgmt-Console, Web-WebServer, Web-Common-Http, Web-Default-Doc, Web-Static-Content, Web-Performance, Web-Stat-Compression, Web-Dyn-Compression, Web-Security, Web-Filtering, Web-Windows-Auth, Web-App-Dev, Web-Net-Ext45, Web-Asp-Net45, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Includes, Web-Net-Ext, Web-Asp-Net, rsat -Source "E:\Windows Server 2019"



Important: \\E: is the location of the mounted ISO. If after installation, a reboot is indicated, reboot the server before continuing.

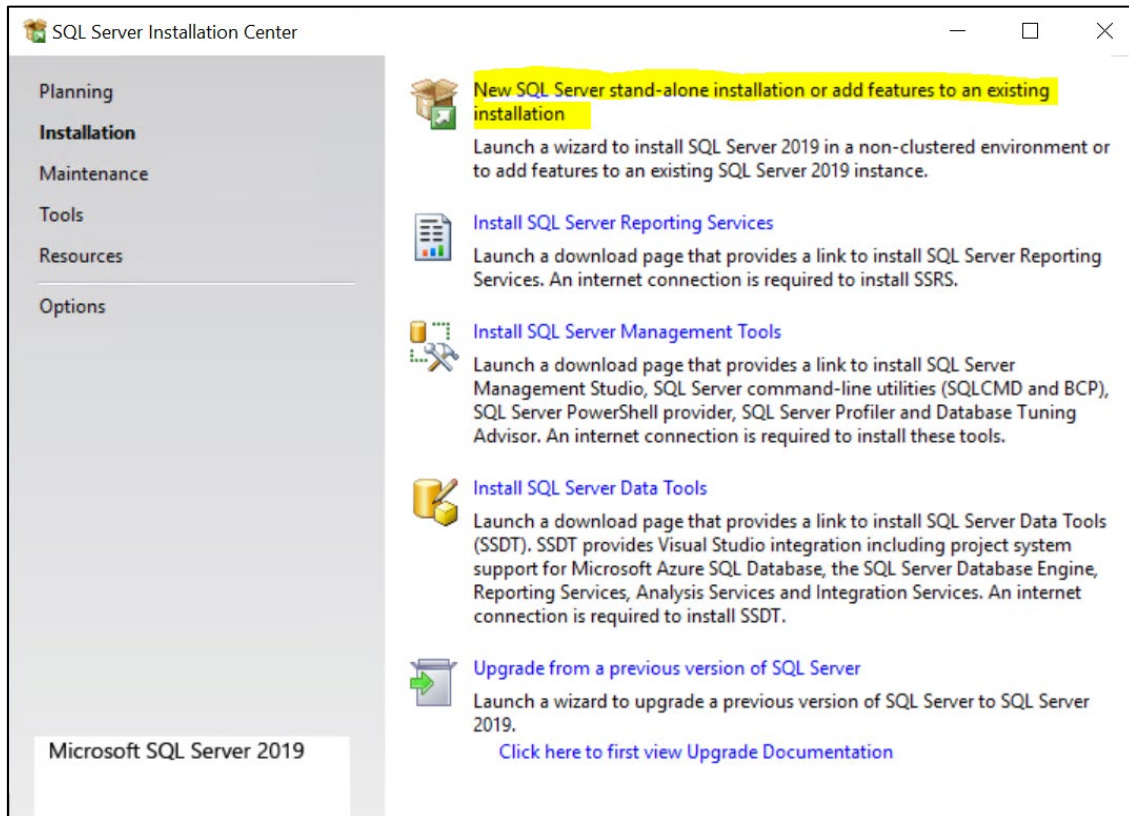
3.3 Installing SQL Server

Install SQL Server using the screenshots below as reference. For small and lab deployments, SQL Server Express can be used, which is included on the installation ISO in the 2 - SQLServer2019Media folder within the prerequisites folder.

➤ **To install SQL Server, do the following:**

1. Start the installation with "Setup.exe".

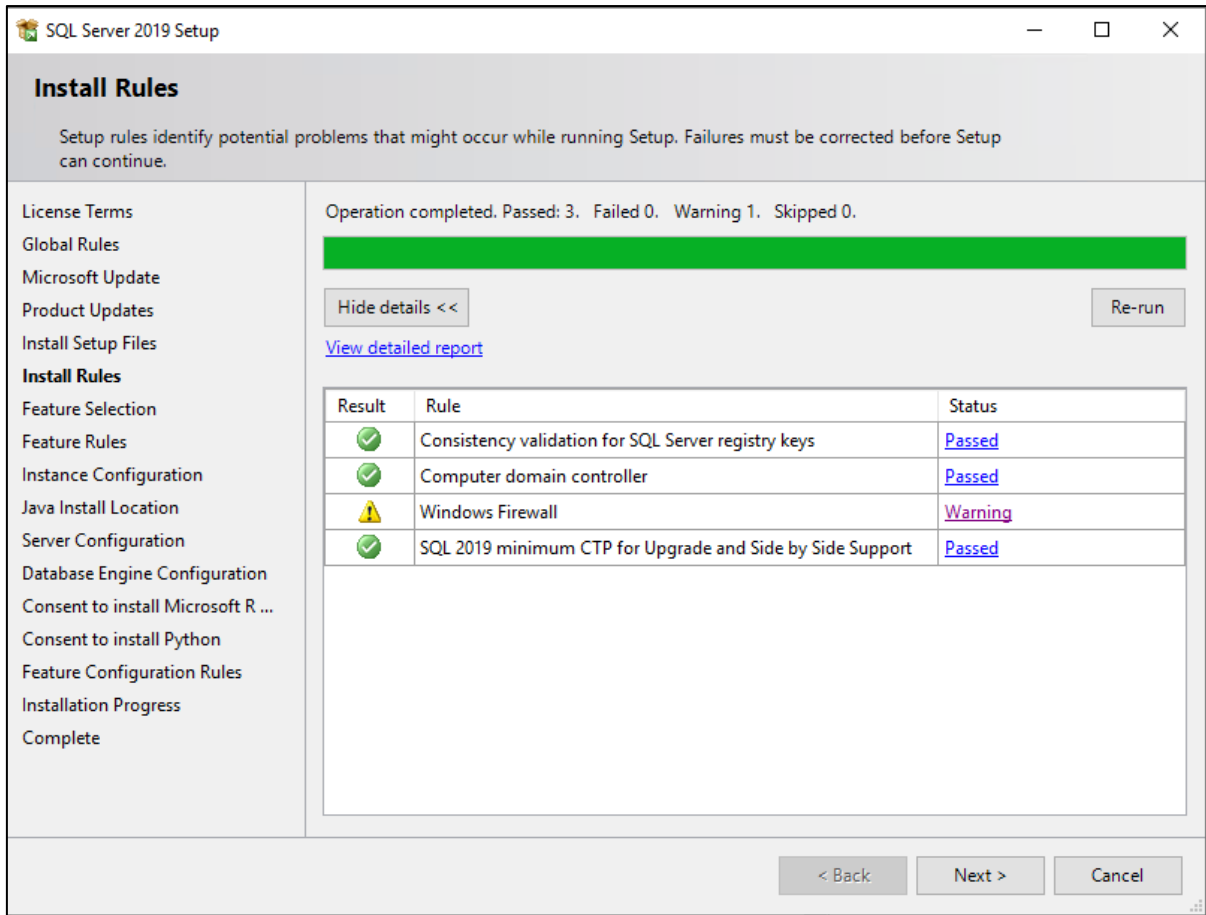
Figure 3-1: SQL Server Installation Server



2. Select the **New SQL Server stand-alone installation or add features to an existing installation** option.
3. Accept the license terms.

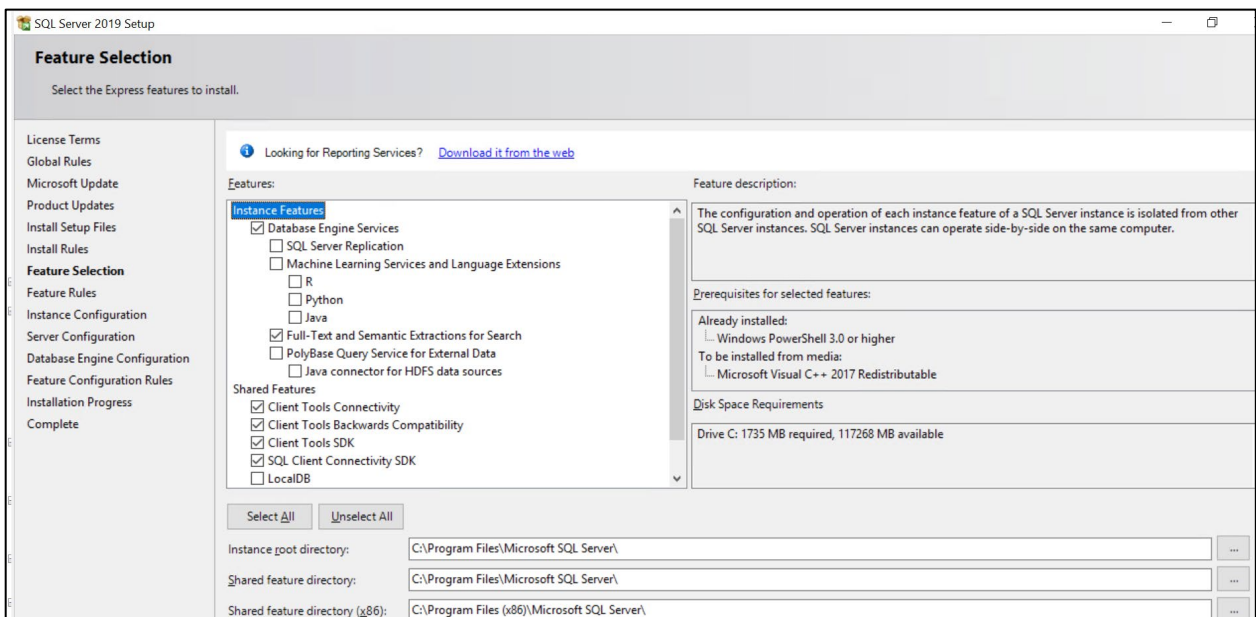
- Select the **Use Microsoft Update to check for updates** option.

Figure 3-2: SQL Server 2019 Setup Step 1



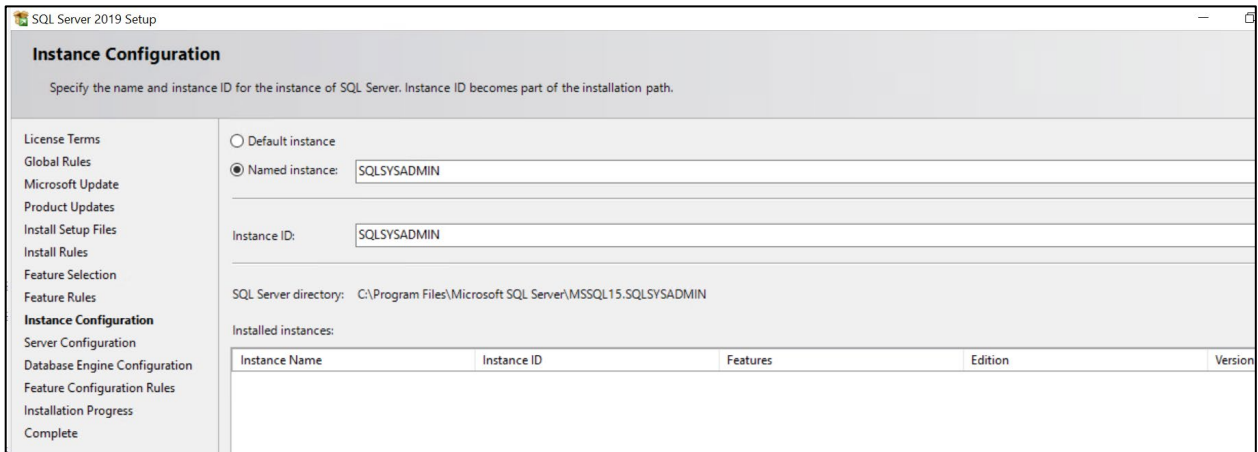
- Click **Next**.

Figure 3-3: SQL Server 2019 Setup Step 2



- Select the features. Use the figure above as a reference.

Figure 3-4: SQL Server 2019 Setup Step 3



7. Change the **Named instance** to SQLSYSADMIN.

Figure 3-5: SQL Server 2019 Setup Step 4

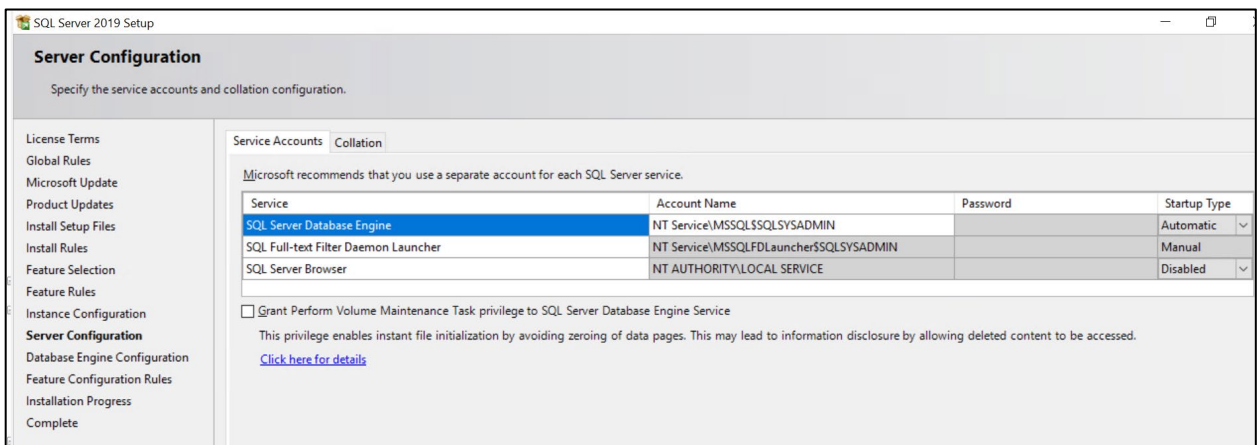
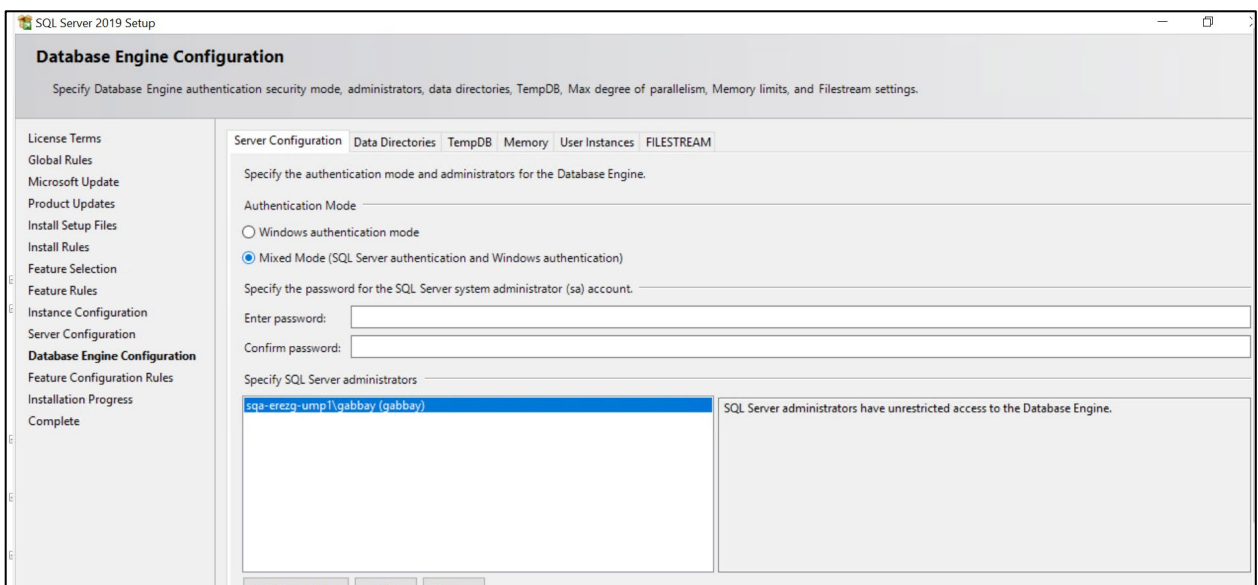
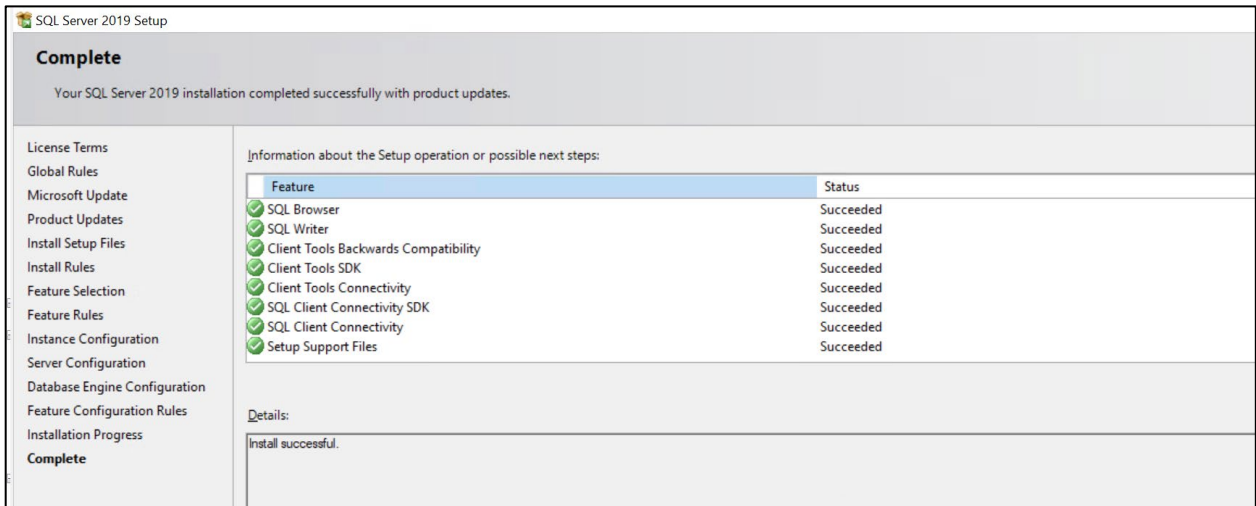


Figure 3-6: SQL Server 2019 Setup Step 5



8. Select **Mixed Mode** under the 'Authentication Mode' section.
9. Enter the system admin (sa) password and write it down for future use. AudioCodes' default for the sa password is "R3m0t3Supp0rt".

Figure 3-7: SQL Server 2019 Setup Step 6



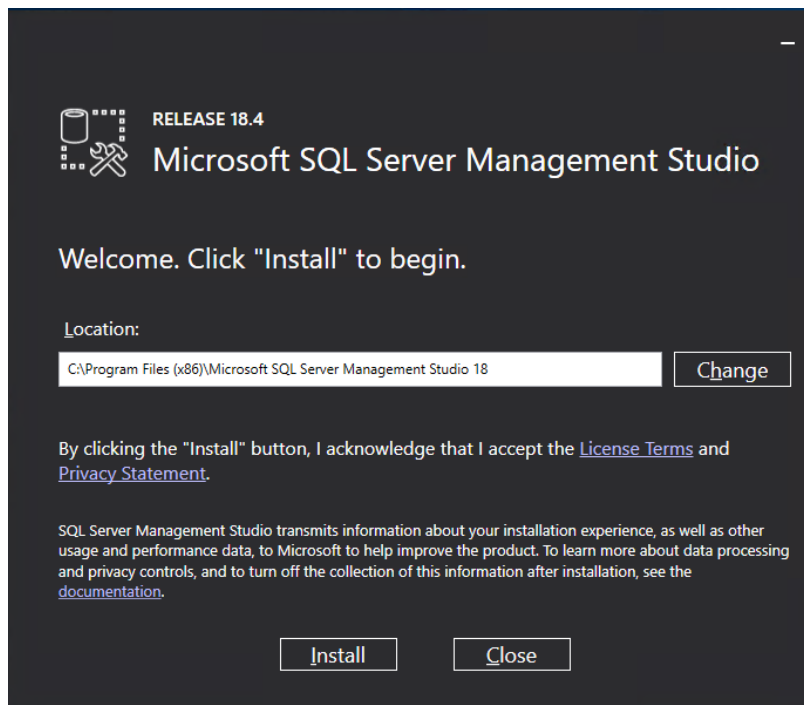
3.4 Installing SQL Server Management Studio

This section describes how to install SQL Server Management Studio (3 - SSMS-Setup-ENU.exe).

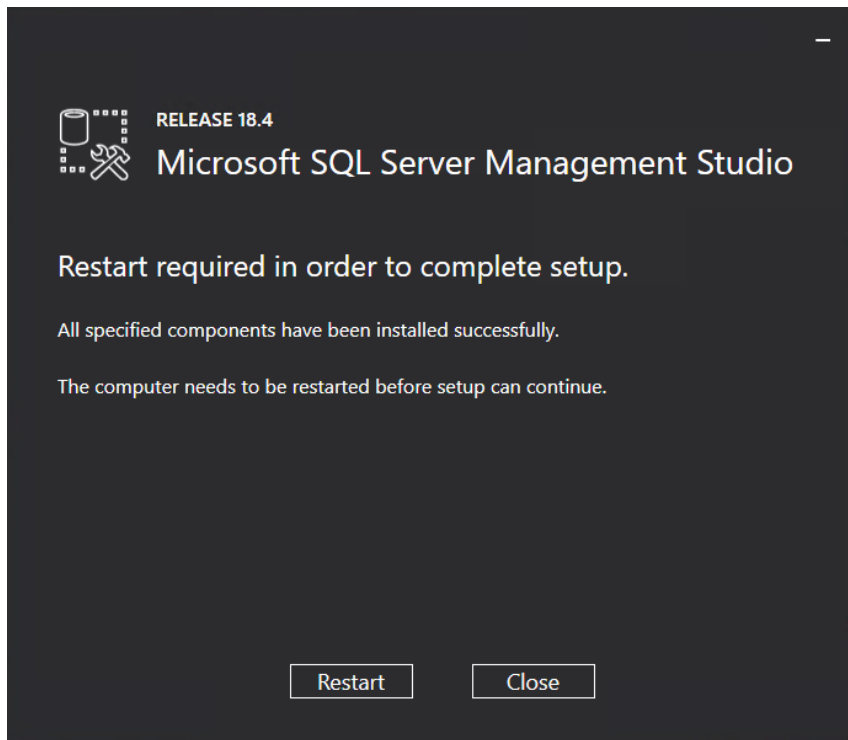
➤ **To install SQL Server Management Studio:**

1. Run SSMS-Setup-ENU.exe; the Welcome screen is displayed.

Figure 3-8: Install SQL Server Management Studio Step 1



2. Select **Install**.

Figure 3-9: Install SQL Server Management Studio Step 2

3. Select **Restart**.

3.5 Installing ASP.NET SQL Authorization Manager

Install .NET SQL Authorization Manager (4 - NetSqlAzManSetup_x64.msi) using the screenshots below as a reference.

Figure 3-10: Install .NET SQL Authorization Manager Step 1

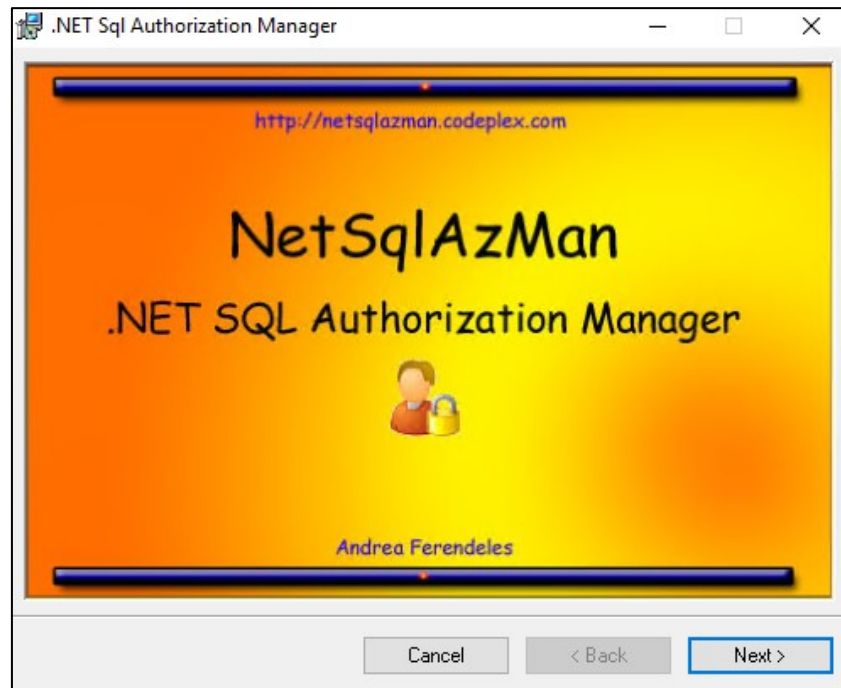


Figure 3-11: Install .NET SQL Authorization Manager Step 2

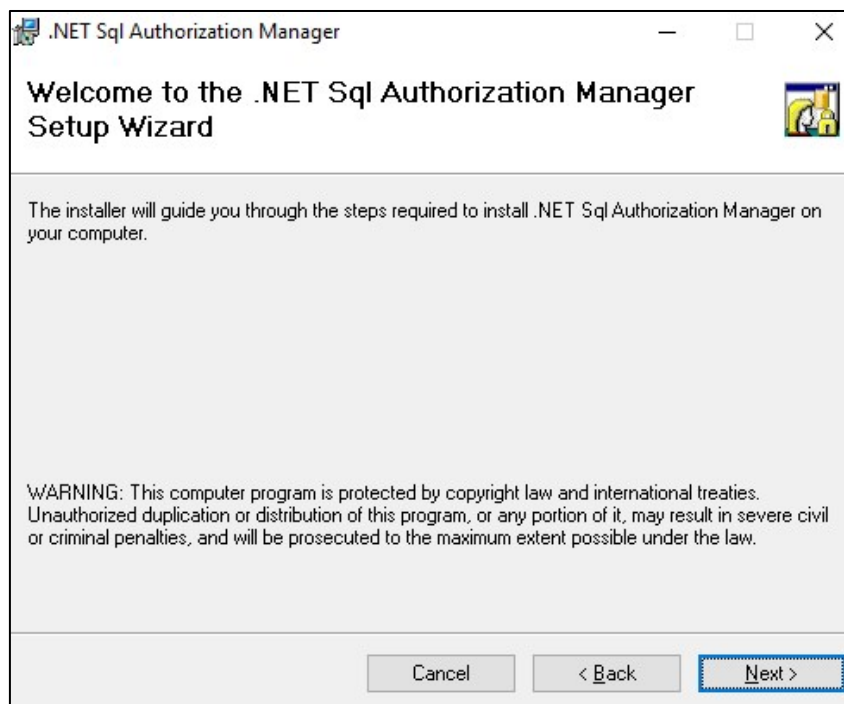


Figure 3-12: Install .NET SQL Authorization Manager Step 3

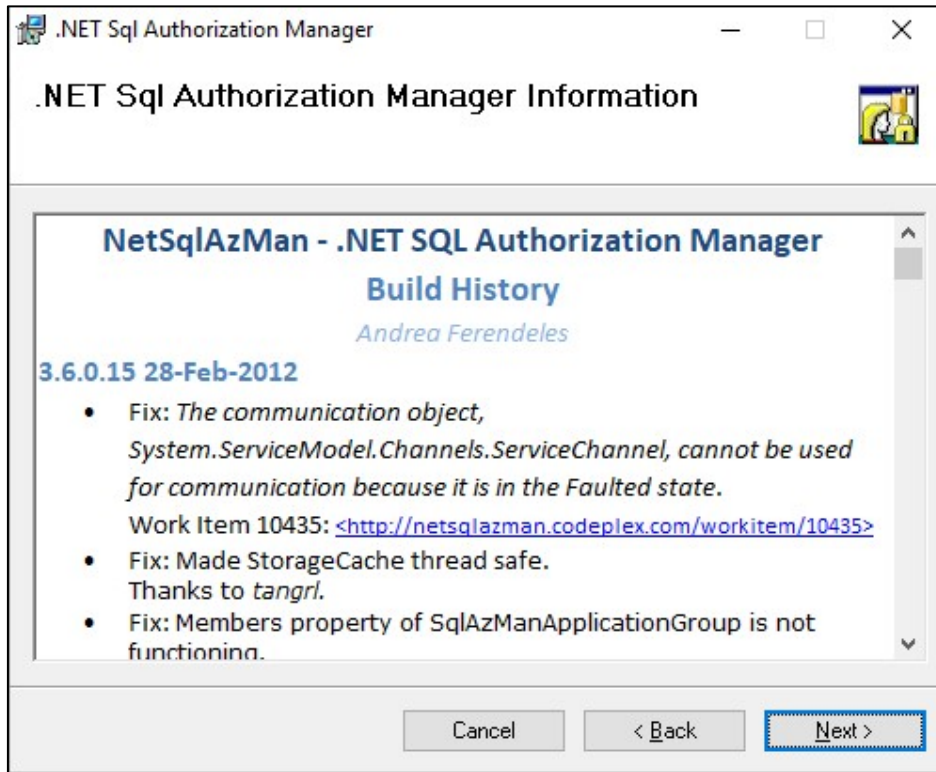


Figure 3-13: Install .NET SQL Authorization Manager Step 4

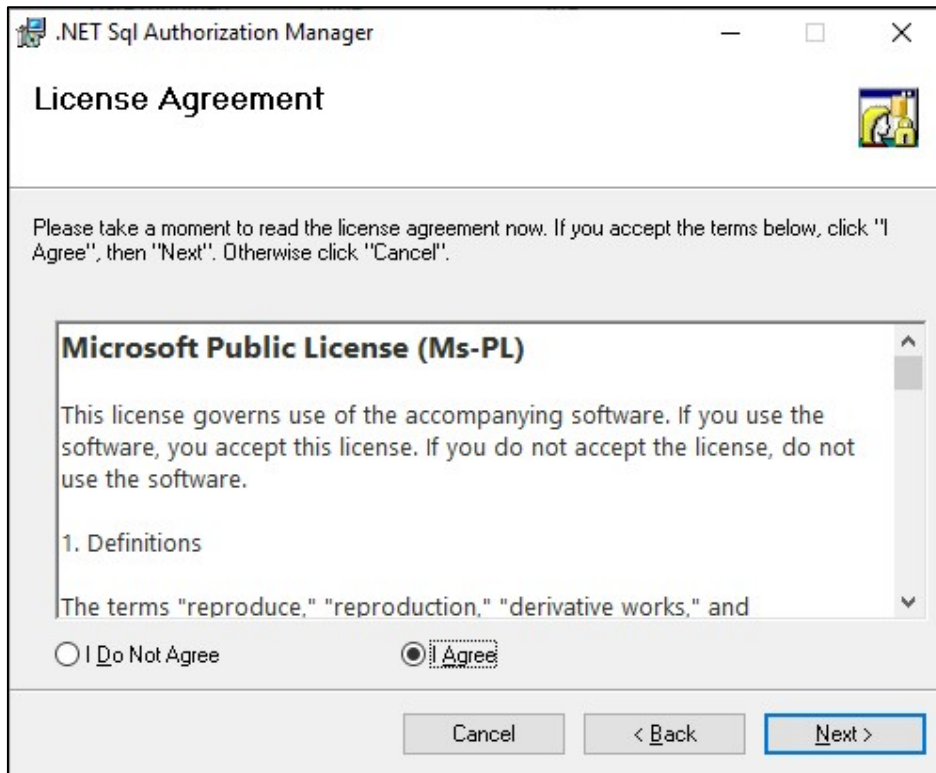


Figure 3-14: Install .NET SQL Authorization Manager Step 5

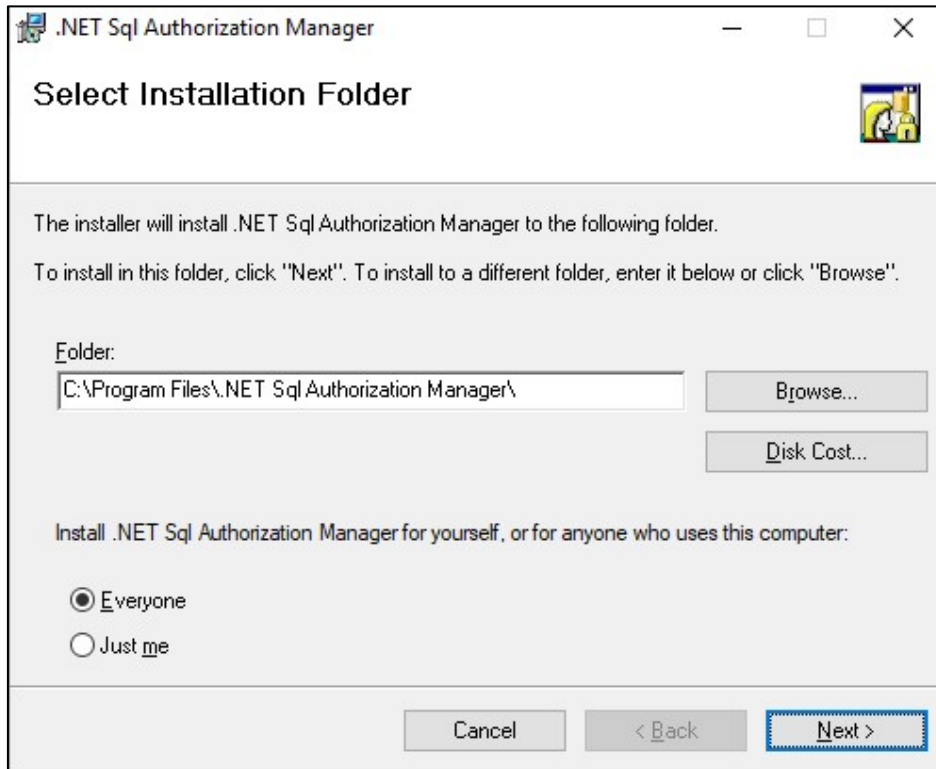


Figure 3-15: Install .NET SQL Authorization Manager Step 6

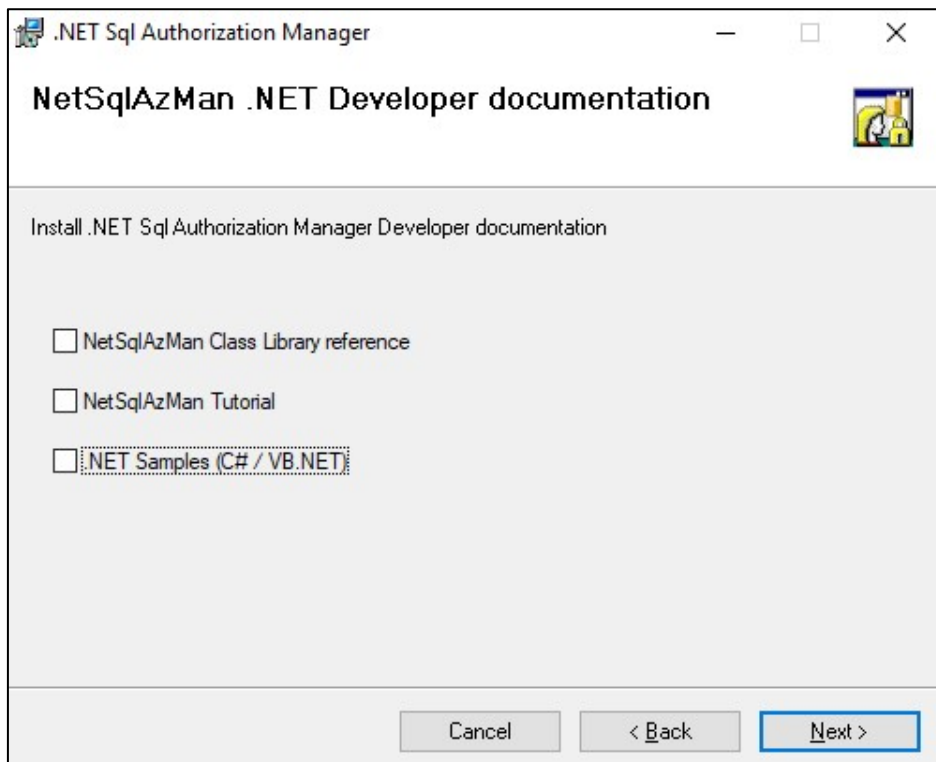


Figure 3-16: Install .NET SQL Authorization Manager Step 7

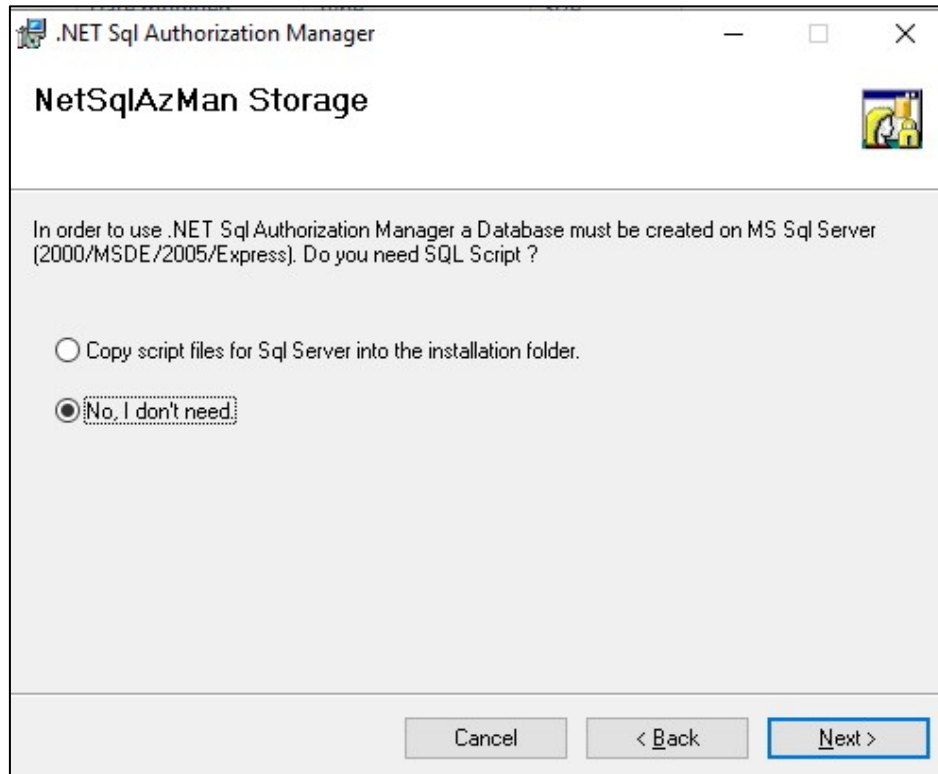
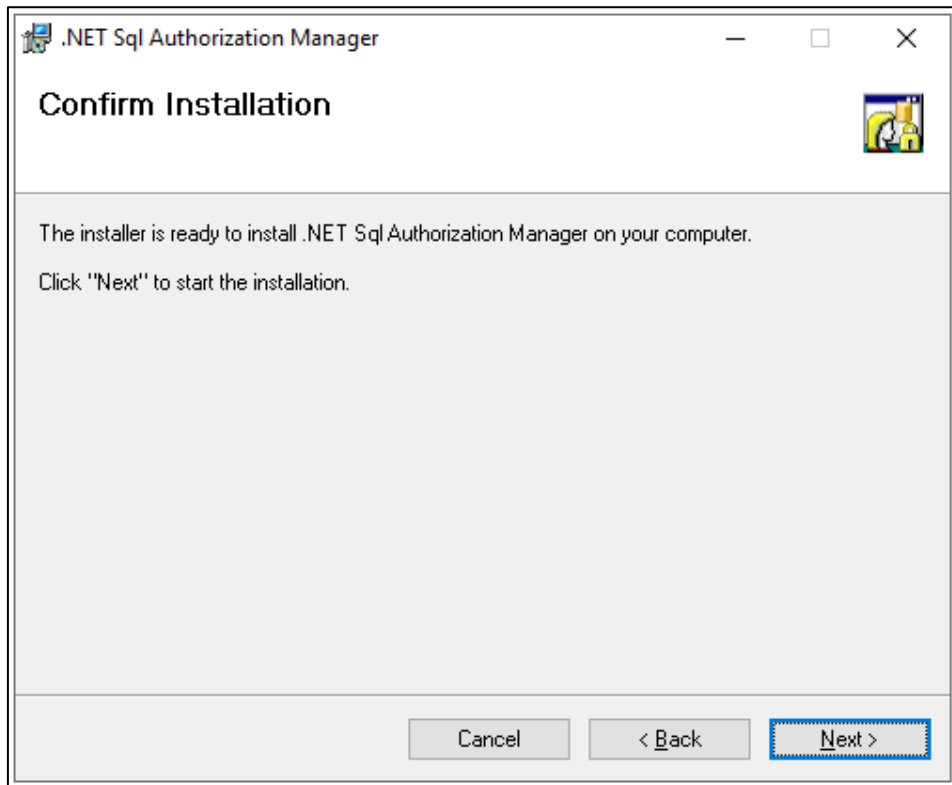


Figure 3-17: Install .NET SQL Authorization Manager Step 8



3.6 Installing ASP.NET Framework 4.8

Install .NET framework 4.8 by running “5 - ndp48-devpack-enu.exe”.
Restart if required by the installer.

3.7 Installing Skype for Business Online PowerShell

Install Skype online PowerShell by running “6 - SkypeOnlinePowerShell.Exe”.

3.8 Installing SharePoint Online PowerShell

Install SharePoint online PowerShell by running “7 - SharePointOnlineManagementShell_19724-12000_x64_en-us.msi”.

3.9 Installing ASP.NET Core

Install ASP.NET core by running “8 - aspnetcore-runtime-3.1.2-win-x64.exe”.

3.10 Installing ASP.NET Core Hosting Pack

Install ASP.NET core hosting pack by running “9 - dotnet-hosting-3.1.2-win.exe”.

3.11 Installing Azure Active Directory PowerShell Components

Issue the following PS cmdlet (written down in 10 - AzureAD.ps1):

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 - Force
Install-Module AzureAD -force
```

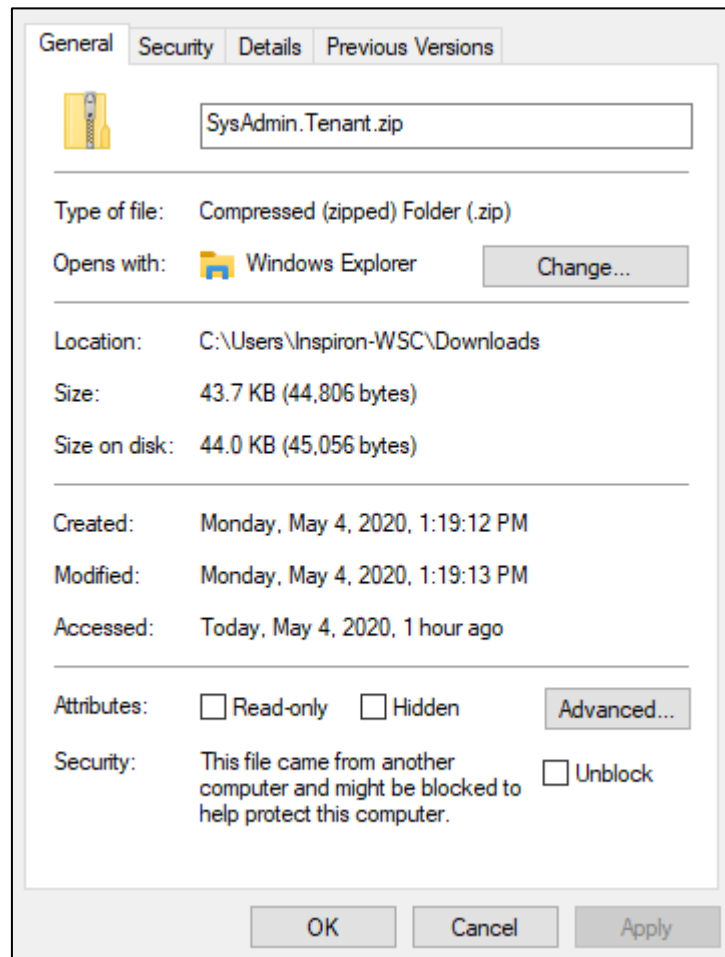
3.12 Installing UMP-SP

If you didn't reboot per the third-party component instructions, reboot now before starting the Automated installation script for UMP (install_multitenant.ps1), as the installation script uses SQL PowerShell, which is not operational directly after SQL installation; however requires a machine restart first.

➤ **To install UMP-SP:**

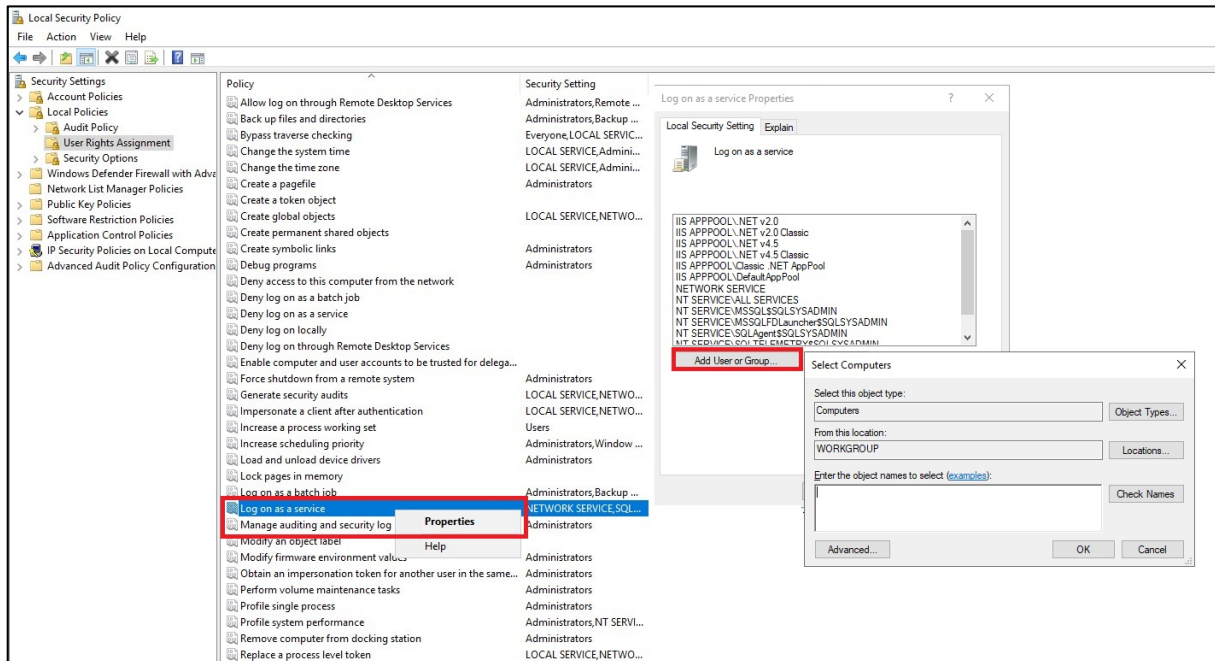
1. Create a directory under C:\multitenant and copy the following files to it:
 - SysAdmin.Tenant.zip
 - unzip.exe
 - Install-OVOCagents
 - install_multitenant.ps1
2. All files must be unblocked by right-clicking each file, selecting **Properties** and then selecting the **Unblock** option (if it is there) as shown in the screenshot below:

Figure 3-18: File Properties



3. A service account is used for background processing by UMP-SP. This account must be inserted during the installation and needs to be a “local admin” account on the computer where UMP-SP is installed and must have the right to log on as-a-service.
 - a. To grant this right, start the local security policy management console (secpol.msc)
 - b. Select **Local Policies > User Rights Assignment** and right-click “Log on as a service” to configure the properties and Add a User to the list as shown below:

Figure 3-19: Local Security Policy Management Console



- c. Click **OK** twice to close the properties after adding the user and close the policy editor application.
- d. Add this account to UmpAdmins Local group (open the Computer Management, and create a new Group “UmpAdmins”) and add the account created above to the UmpAdmins group as shown below:

Figure 3-20: Computer Management

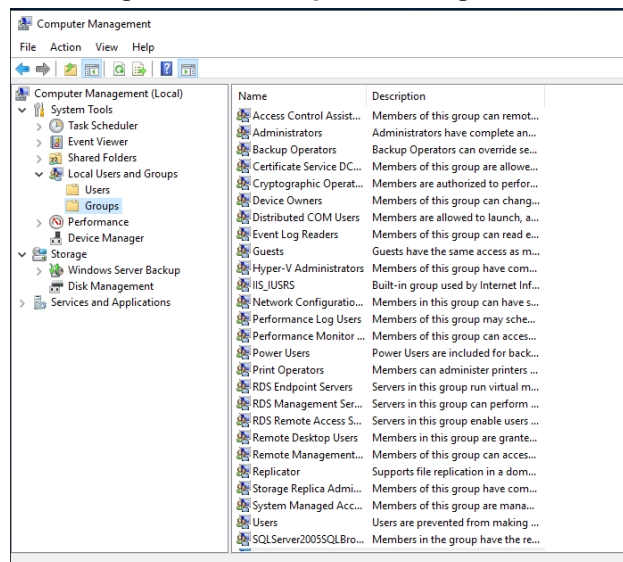
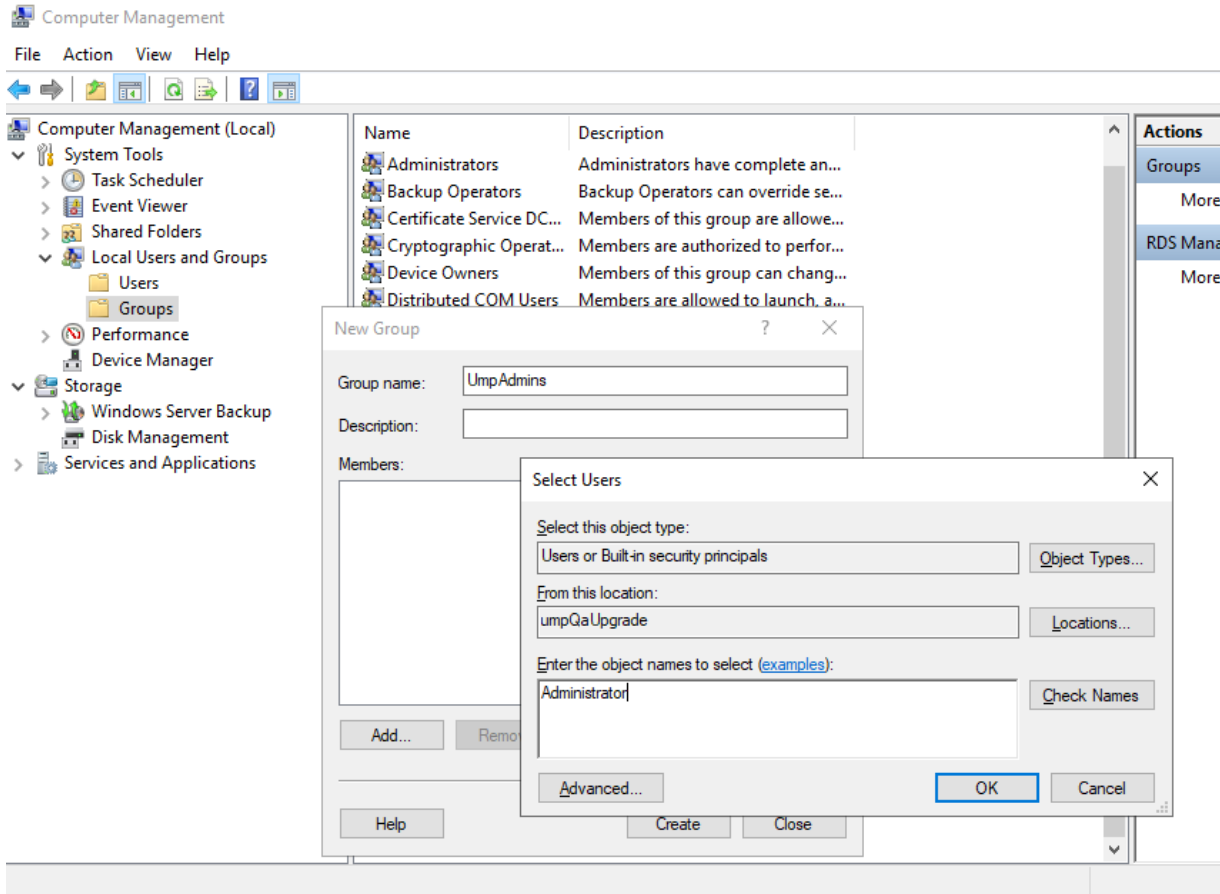


Figure 3-21: Computer Management (Local)



- e. Logout and login to RDP again.
- f. Click to continue. Open a PowerShell session, go to multitenant directory (cd c:\multitenant) and run the install_multitenant.ps1 script.
- g. You are prompted for the domain/user/password of the local server (for workgroup use "." For the domain). The account entered must be the service account created above.
- h. Open a PS session (Run as Administrator) and go to the multitenant directory (cd c:\multitenant) followed by running install_multitenant.ps1 script.
- i. You are prompted to enter the domain/user/password of the local server (for workgroup, put "." for the domain). The account provided here must be the service account created above.

Figure 3-22: Installation Console

```

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




Important: Select the **Manage Disk** that you would like to allocate to the UMP SP and verify that you have space for future growth. (See Section 2 for 'Disk requirements').

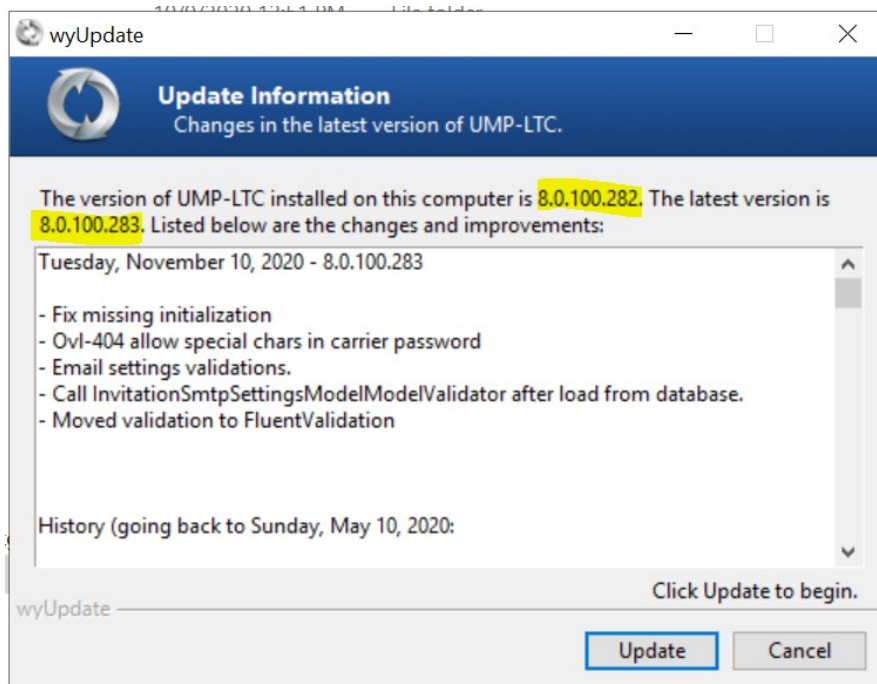
3.13 Updating UMP after Installation

To update the UMP-SP, run "c:\acs\wyupdate.exe" and check if updates are available. If updates are found, follow the steps in the wyupdate utility.



Important: Where ..\C: is the location of the ACS folder.

Figure 3-23: Wyupdate Tool



After running wyupdate for build versions prior than build 8.0.100.282, manually run the following SQL scripts from the c:\acs\SQLScript folder using SQL Server Management Studio:

- Add-columns
- RefreshSpf

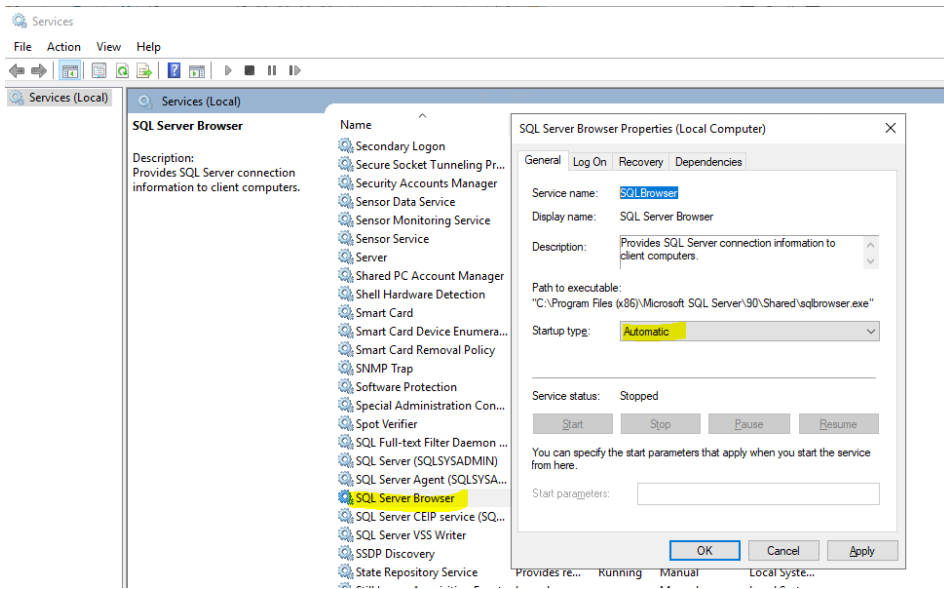
In addition, when UMP-SP is deployed with OVOC, set the 'OvocEnabled' parameter to true in the dbo.ApplicationSetting within the SysAdminTenant database.

3.13.1 Run Changes on the External SQL Server

This section describes the changes to run on the external SQL server.

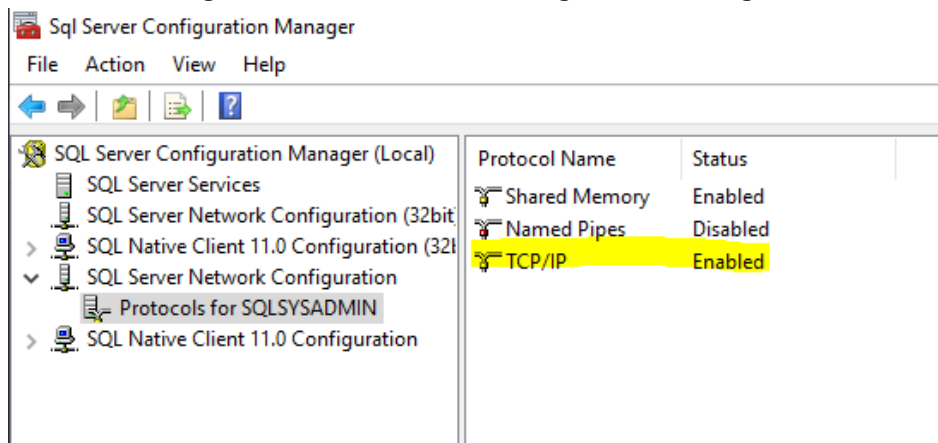
- **To run changes on external SQL server:**
 1. Enable Firewall rules to allow connection from remote to the DB (TCP 1433, 4022, 135, 1434, UDP 1434).
 2. Enable the SQLBrowser service:

Figure 3-24: SQL Browser Service



3. Enable SQL TCP/IP connection.
4. Open the Sql Server Configuration Manager (under Protocols for SQLSYSADMIN) and set TCP/IP to "Enabled".

Figure 3-25: SQL Server Configuration Manager



3.14 Enable OVOC

When UMP-SP is setup with OVOC as the Management system (Optional), set the 'OvocEnabled' parameter to true in the dbo.ApplicationSetting within the SysAdminTenant database.

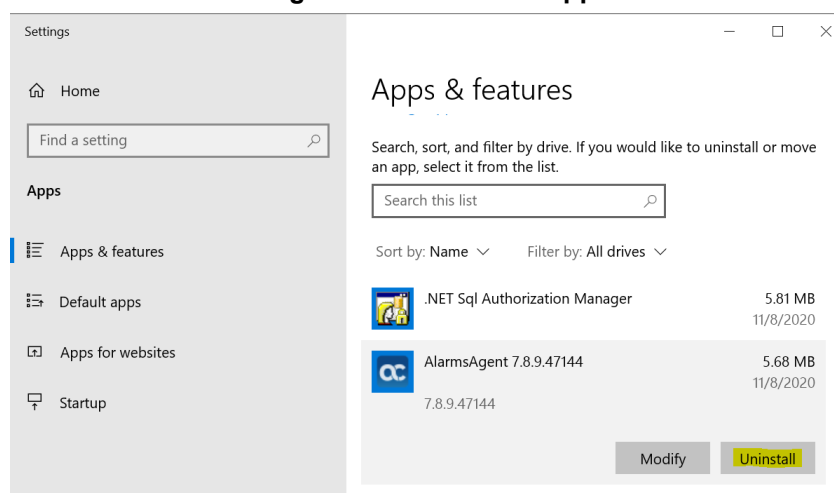
3.15 Reinstall OVOC Alarm Agent

In this release, there is a bug regarding configuration of which managed elements are monitored. Consequently, you need to reinstall the alarm agent and specify the correct command.

➤ **Do the following:**

1. Uninstall AlarmsAgent.

Figure 3-26: Uninstall App



2. Open PowerShell and re install OVOC Alarm agent:

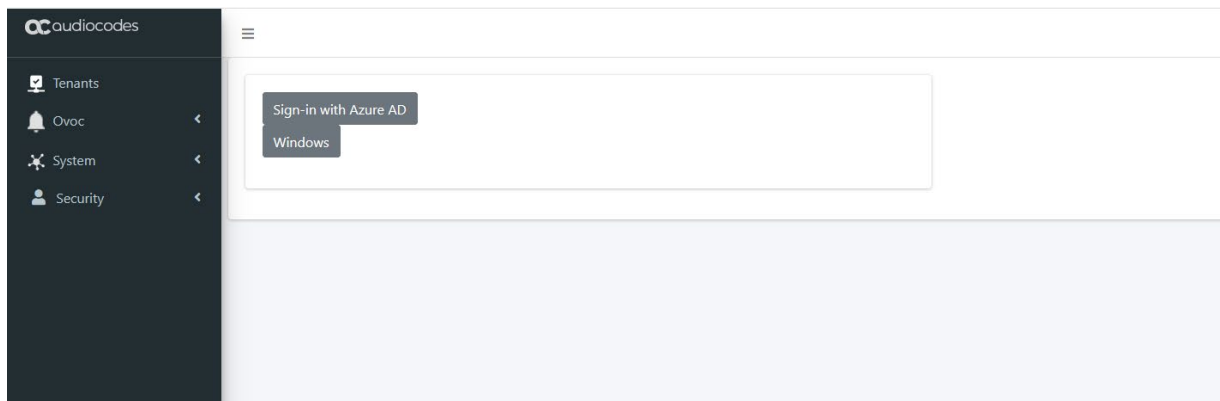
```
cd C:\multitenant\Install-OVOCagents\Packages\EMS\  
msiexec /i EmsClientAgent.msi MainAgent=<ump_computer_name>  
Type=OVL_UMP_MT /n
```

3.16 Accessing the UMP 365 for the First Time

Before the UMP 365 can be used in a production environment, an initial configuration needs to be performed including the configuration of the Office 365 Settings, App Registration, Email setting and loading of a license into the environment:

- Invitation Settings (see Section 0)
- Email Settings (see Section 3.16.2)
- Public Portal URL Setting (see Section 3.16.3)
- Application Registration (see Section 3.16.4)
- Web Application Setting (optional) (see Section 3.16.5)
- Configure License (see Section 3.16.6)

Figure 3-27: Multi-Tenant Access (Provider Only)



The provider can access with the following Admin User types:

- SuperAdmin: a predefined User Account (Windows, must be members of Group UmpAdmins)
 - Access to Multi - Tenant level and to all the Customers Tenant
- Admin User: SSO Sign-In with Azure AD user
 - Access to customers Tenant that received Grant access

For details, see Section 6.1.

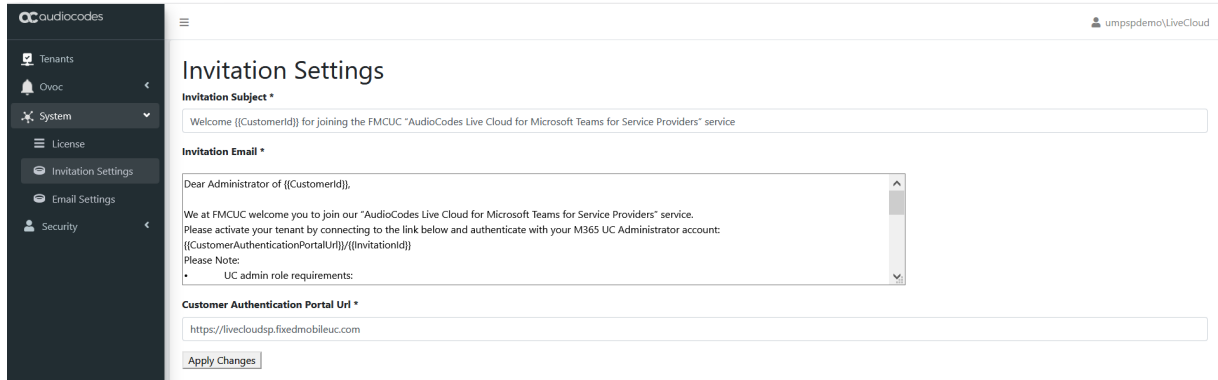
3.16.1 Invitation Settings

This section describes how to setup the email Invitation Settings.

➤ **To setup the invitation settings:**

1. In the UMP SP Main Tenant Main Page, select the **Invitation Settings** tab.

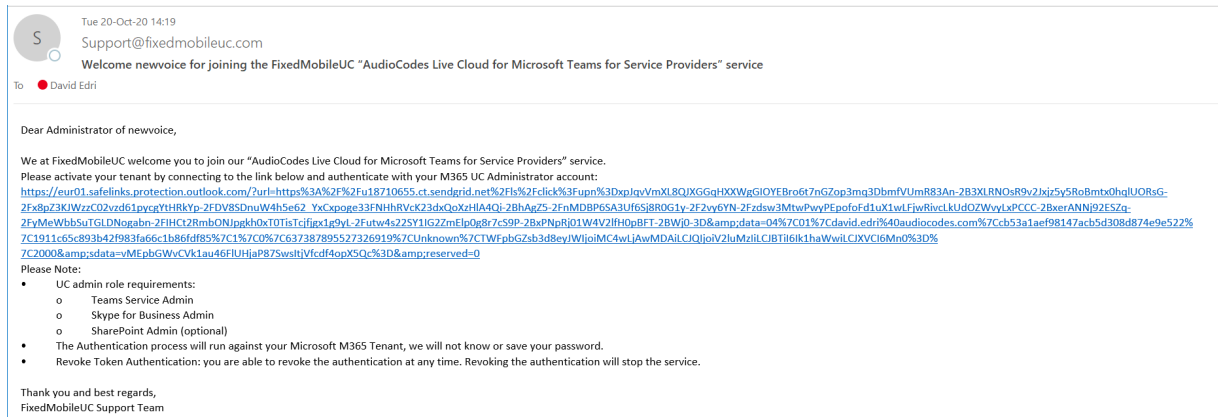
Figure 3-28: Invitation Setting



2. Enter the following details:

- Invitation Subject: Edit the email invitation.
- Invitation Email: Edit the email content
- Invitation Subject and Invitation Email include the follow place holders
 - {{CustomerId}} – The CustomerID, Unique per Customer Name (from onboarding new customer flow)
 - {{CustomerAuthenticationPortalUri}}/{{InvitationId}} – unique invitation (Customer Authentication Portal Uri / InvitationId)

Figure 3-29: Email Example



3.16.2 Email Settings

This section describes how to setup the Email Server settings.

➤ **To configure email settings:**

1. In the UMP SP Main Tenant Main Page, select the **Email Server Settings** tab.

Figure 3-30: Email Settings

The screenshot shows the 'Email Server Settings' configuration page. The left sidebar contains navigation options: Tenants, Ovoc, System, License, Invitation Settings, Email Settings (highlighted), and Security. The main content area has the following fields:

- From ***: Support@fixedmobileuc.com
- Username**: Support@fixedmobileuc.com
- Password already saved**: [Redacted]
- Confirm Password**: [Redacted]
- Host ***: smtp.sendgrid.net
- Port ***: 465
- EnableSsl**
- Network**: [Dropdown menu]
- Apply Changes** button

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

3.16.3 Public Portal URL Setting

This section describes how to setup the public portal URL. The Admin user (Provider/Channel/Customer Admin) accesses the Tenant via this portal and will Sign-in with the Azure AD.

➤ **To setup the public portal URL settings:**

1. In the UMP SP Main Tenant Main Page, select the **Invitation Settings** tab.

Figure 3-31: Customer Authentication portal URL Setting

The screenshot shows the 'Invitation Settings' configuration page. The left sidebar contains navigation options: Tenants, Ovoc, System, License, Invitation Settings (selected), Email Settings, and Security. The main content area is titled 'Invitation Settings' and includes the following fields:

- Invitation Subject ***: Welcome {{CustomerId}} for joining the FMCUC "AudioCodes Live Cloud for Microsoft Teams for Service Providers" service
- Invitation Email ***: Dear Administrator of {{CustomerId}},
We at FMCUC welcome you to join our "AudioCodes Live Cloud for Microsoft Teams for Service Providers" service.
Please activate your tenant by connecting to the link below and authenticate with your M365 UC Administrator account:
{{CustomerAuthenticationPortalUri}}/{{InvitationId}}
Please Note:
* UC admin role requirements:
- Customer Authentication Portal Uri ***: https://livecloudsp.fixedmobileuc.com

An 'Apply Changes' button is located at the bottom of the form.

- Customer Authentication Portal URL: Provider Public Portal
Example: Livecloudsp.fixedmobileuc.com
- Provider need to assign this Portal URL to the UMP VM IP address.
 - ◆ DNS A record for Domain Livecloudsp.fixedmobileuc.com to IP xxx.xxx.xxx.xxx (UMP – IP Address).
- App Registration: add the WEB URL to the Redirect URIs – see Section 3.16.4 App Registration.

3.16.4 App Registration

This section describes how to setup and config the App registration. The app Registration manages the Authentication token and the Admin Users (Account) redirect URI's sign-in. It requires you to add the App registration at the Provider Tenant.

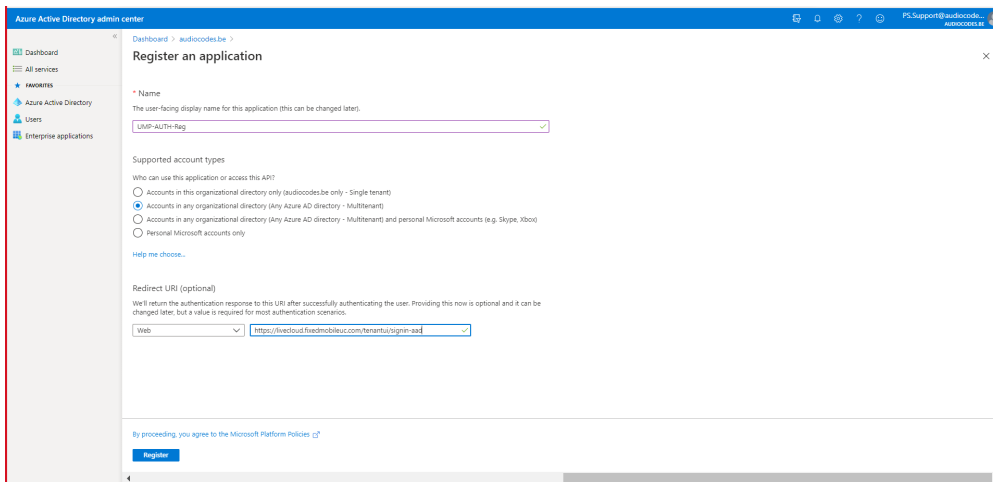


Note: This procedure must be performed by administrators with “Global Admin” privileges.

➤ **To configure the App Registration:**

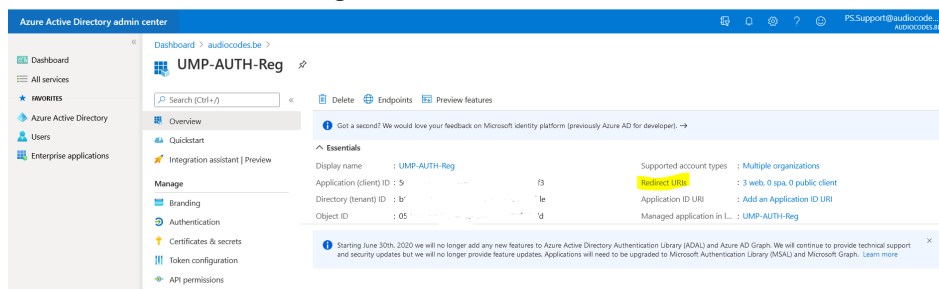
1. Access the Provider Azure active directory admin center/ app registration and select new registration.
2. Enter the following details:
 - Name: App registration name
 - Select account type: Recommendation - Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 - Register

Figure 3-32: New App Registration



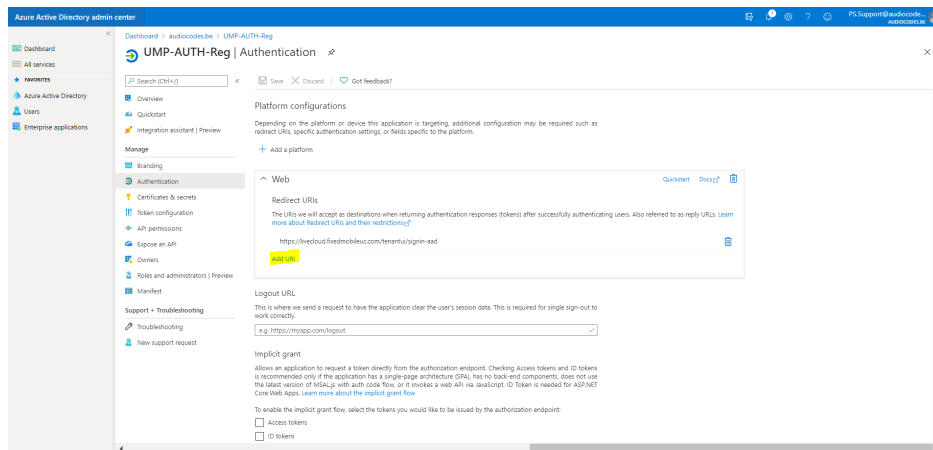
3. **Redirect URI's** – adds the WEB redirect URI (public portal URL).

Figure 3-33: Redirect URI's



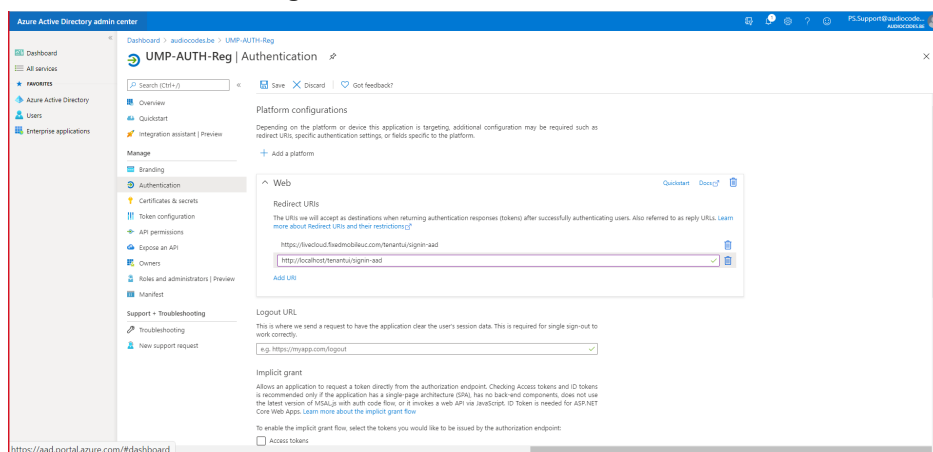
4. **Select Add URI.**

Figure 3-34: Add URI



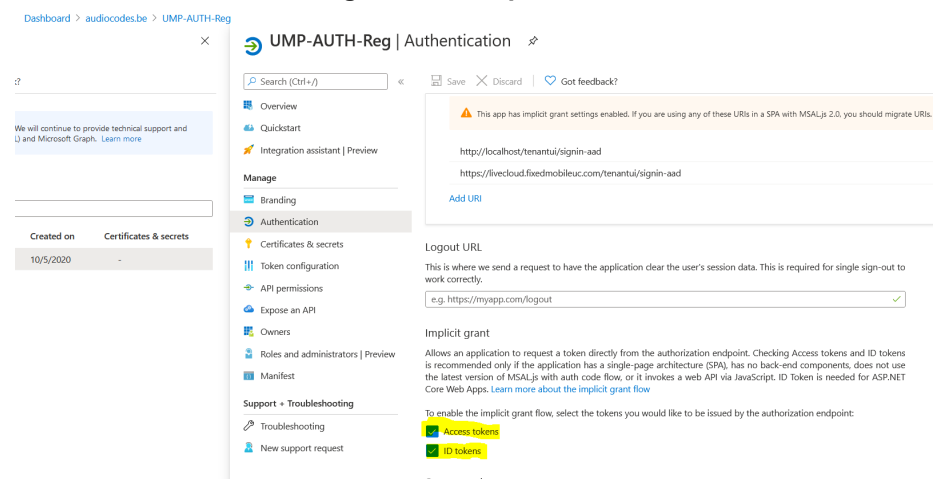
5. Edit the URI name as the Public portal URL /tenantui/signin-aad (e.g. <https://livecloudsp.fixedmobileuc.com/tenantui/signin-aad>)

Figure 3-35: Add Public Portal URL



6. To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:
 - Access tokens
 - ID tokens

Figure 3-36: Implicit Grant



- Copy the Application (client) ID value and paste it at the UMP/Security/Customer Admin / App Registration Client ID and save.

Figure 3-37: Copy the Application (client) ID Value

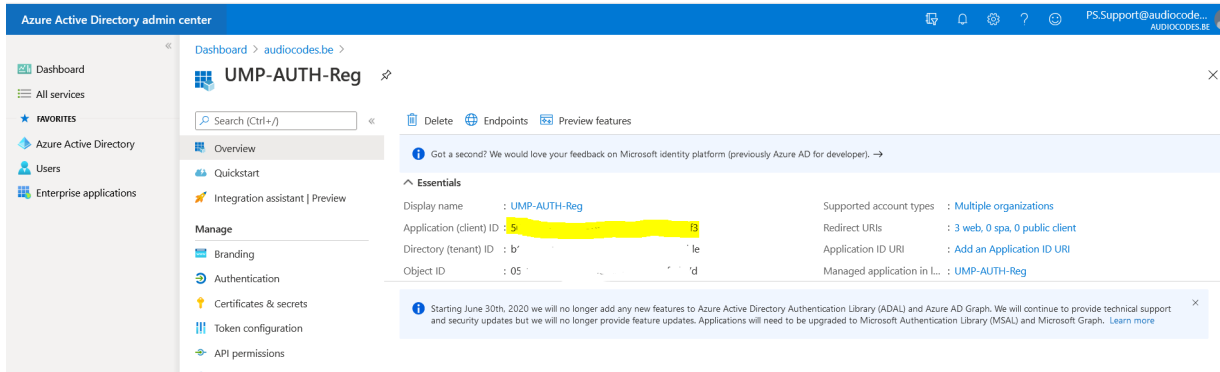
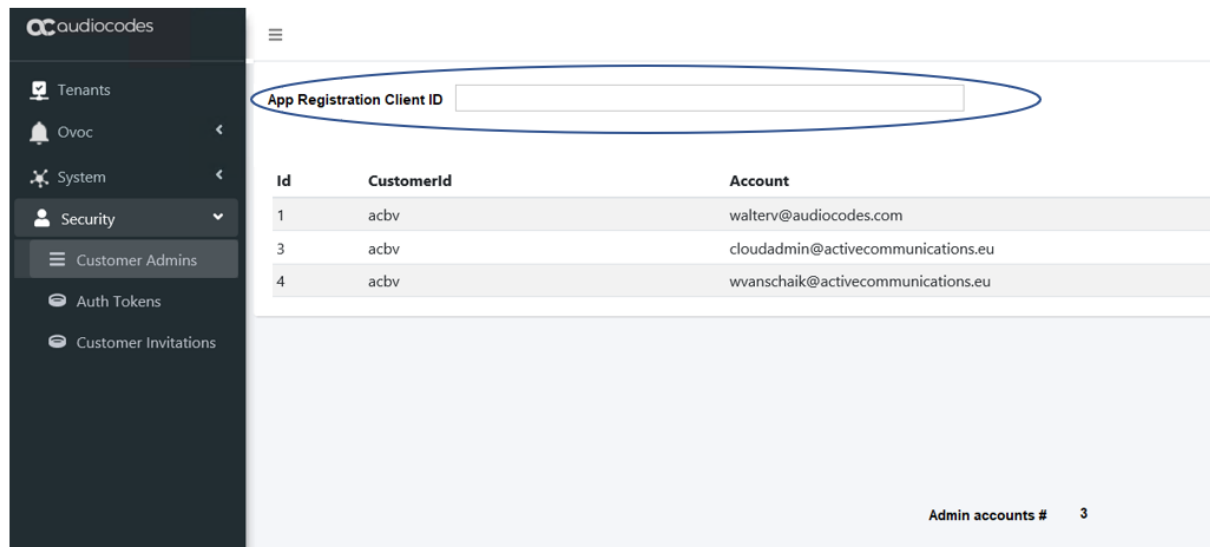


Figure 3-38: Paste the Application (client) ID Value



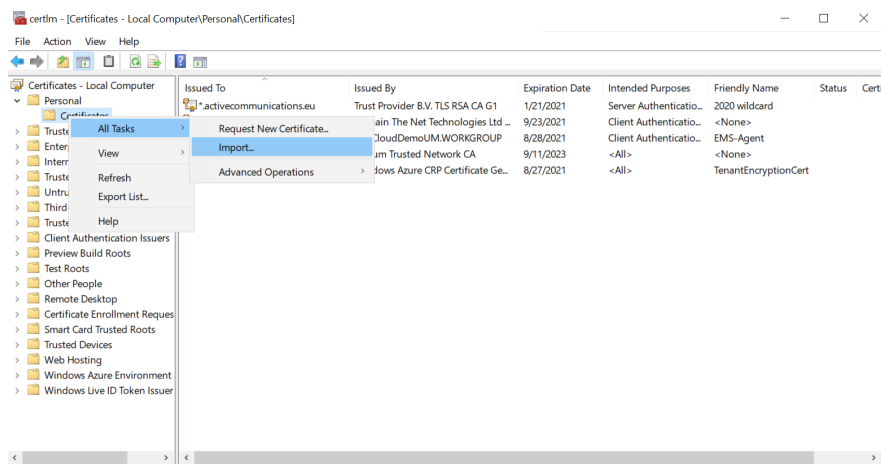
3.16.5 WEB Application Setting (optional)

As part of the installation process, the Wizard automatically create WEB Application, however the installation process only performs “bindings” for port 80 (HTTP), which addresses most of the Provider network topology. In case the Provider doesn’t have a Proxy server that manages the Public portal URL and Public URL IP address (DNS A record) direct the UMP VM; add “site bindings” for port 443 (Type HTTPS).

➤ **To configure the WEB Application:**

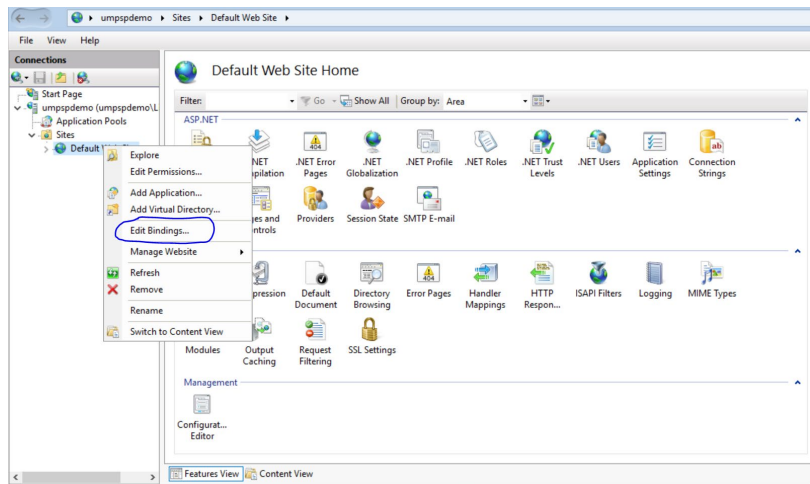
1. Add Certification – open command line and enter “certlm”
2. Import certificate – under Personal/ certificates folder.

Figure 3-39: Edit WEB Application



3. Open IIS manager – right-click the default WEB Site and select **Edit Bindings**.

Figure 3-40: Edit WEB Application



4. Type the following to add site bindings:

```
= https, Port = 443, SSL certificate = provider Cert for the URL
```

Where the provider certificate is a wild certificate for *.fixedmobileuc.com which also supports "Livecloud.fixedmobileUC.com".

Figure 3-41: New App Registration

3.16.6 Configure License

UMP365 supports the follow Licensing:

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

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

■ **User License:** Users license includes the following features support:

- User MACD (Teams, SharePoint and Voice policies)
- LifeCycle management
- Create and Edit Templates
- DID management
- Support Microsoft Teams
- Support SharePoint and OneDrive policies (Future)
- Manage emergency call Routing (Future)

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

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

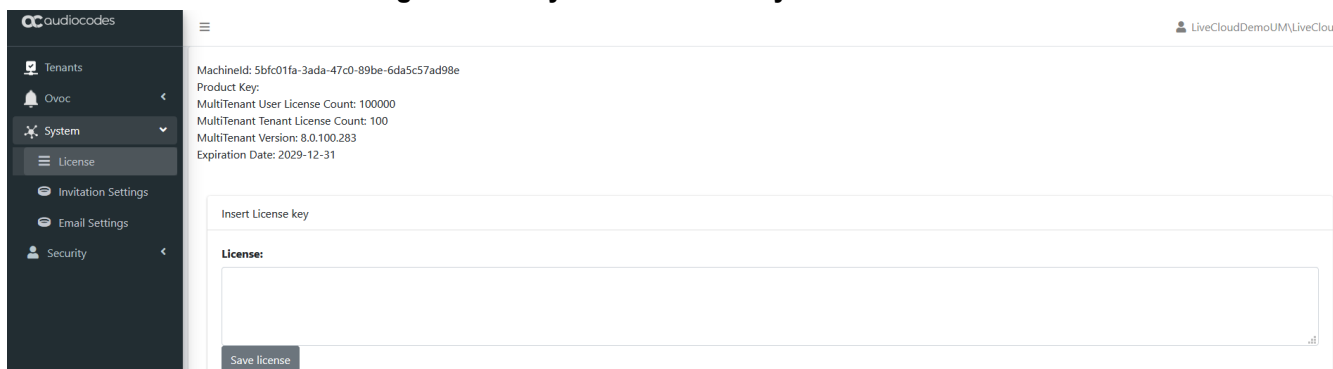
3.16.6.1 Installing the UMP 365 License

This section installs the UMP 365 license.

➤ **To configure the license:**

1. In the UMP Multi-Tenant GUI, open the Licensing page (**System Configuration > License**) and extract the Machine ID.
2. Activate your product through the AudioCodes License Activation tool at <http://www.audiocodes.com/swactivation>. You need your Product Key and Fingerprint (MachineID) for this activation process. An e-mail will subsequently be sent to you with your Product License.
3. Insert License Key and save.
4. Save License.

Figure 3-42: System/License Key View



This page includes the follow information:

- MachineID – required for the license generator tool
- MultiTenant User License Count: # of Users License, Pool License between the Customers Tenant

- MultiTenant Tenant License Count: # of Tenants Licenses
- MultiTenant Version: SW Version
- Expiration Date

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

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



Warning: When the maximum number of licensed users has been reached, it is no longer possible to automatically add users through Lifecycle management, nor is it possible to import users or onboard new Tenants (Tenant license).

3.17 Setup the OVOC Connection on UMP (Optional)

To obtain UMP 365 status information using AudioCodes One Voice Operations Center (OVOC) server, the UMP must connect to One Voice Operations Center via SNMP. Providers can obtain the following information from the AudioCodes One Voice Operations Center (OVOC) server:

- Device Information
- Active Alarms
- Journal Event
- Retrieve user licenses per UMP SP system (not per tenant/customer)

Figure 3-43: One Voice Operations Center Device Information

The screenshot shows the 'EREZ UMP Temp' device page in the AudioCodes One Voice Operations Center. The page is divided into several sections:

- Summary:** Shows the device name 'EREZ UMP Temp' and provides options for Actions, Edit, and Open Device Page.
- Device Information:** A table with the following data:

EREZ UMP Temp NAME	AutoDetection REGION	OK STATUS	UNLOCKED ADMIN STATE	No SAVE NEEDED?
10.21.28.187 IP ADDRESS/FQDN	7.8.100.327 FIRMWARE	User Management...	1610190663 S/N	No RESET NEEDED?
- Management: OK:**
 - Cleared (DEVICE ALARMS STATUS)
 - Unlocked (ADMINISTRATION STATUS)
 - Connected (CONNECTION STATUS)
- Voice Quality: Unmonitored:**
 - Unmonitored (CONTROL STATUS)
 - Unmonitored (MEDIA STATUS)
 - Not Defined (CONNECTION STATUS)
- License: OK:**
 - Managed (MANAGEMENT STATUS)
 - Not Requested (VOICE QUALITY STATUS)
 - Unmanaged (OVOC LICENSE STATUS)

At the bottom, there are sections for 'ACTIVE ALARMS' and 'JOURNAL EVENTS', with a table header for 'ACTIVE ALARMS' showing columns for SEVERITY, RECEIVED DATE AND TIME, NAME, and DESCRIPTION.

3.17.1 Retrieve your UMP 365 Users License

This section describes how to retrieve your UMP 365 users license.

➤ **To retrieve your UMP 365 Users license from One Voice Operations Center:**

1. On the Provider page (Tenant Web Portal) under **System**, select **OVOC settings**.

Figure 3-44: Set One Voice Operations Center Configuration

The screenshot shows the 'OVOC Settings' configuration page. On the left is a navigation menu with 'System' selected. The main content area is split into three columns. The first column contains 'OVOC Settings' with a checked 'Enable Ovoc' option and input fields for 'IP Address', 'Trap Port' (162), and 'Keep Alive Port *' (1161). The second column contains 'System Settings' with input fields for 'System Name *' and 'Location'. The third column contains 'Access Settings' with a 'Login Url' field. Below these is the 'SNMP' section with radio buttons for 'SNMPv2' (selected) and 'SNMPv3', and input fields for 'Community Read *' (public) and 'Community Write *' (public). At the bottom is the 'Managed Components' section with an 'SBC' field. 'Apply Changes' and 'Reset Changes' buttons are at the bottom left.

2. Select the **Enable OVOC** option.
3. Configure 'System Settings':
 - System Name – The name of the system. In an environment with multiple UMP servers, this value must be unique.
 - Location – Optional field to describe the system location.
4. Configure the following connection settings:
 - IP Address – the IP address of the One Voice Operations Center server
 - Trap Port – Destination port to which to send traps (default value is 162)
 - Keep Alive Port – Destination port to send Keep-alive requests over SNMP (default is 1161)
5. Configure the SNMP user settings:

All SNMP settings must be identical to the settings of the current UMP entity in the One Voice Operations Center (to support connecting the UMP entity to the One Voice Operations Center using auto detection, configure the default values in parenthesis).

 - SNMP V2:
 - ◆ Community Read – Access string for SNMP get requests ('public')
 - ◆ Community Write – Access string for SNMP set requests ('private')
 - SNMP V3:
 - ◆ Security Name – Identify the SNMP user ('OVOCUser')
 - ◆ Authentication Protocol - Protocol type that used to encrypt the 'Security Name' field ('SHA')
 - ◆ Authentication Key – Security Name encryption key. The field is valid only if 'Authentication Protocol' is selected ('123456789')
 - ◆ Private Protocol – Protocol type that is used to encrypt the SNMP message ('AES-128')
 - ◆ Private Key – SNMP message encryption key. The field is valid only if 'Private Protocol' is selected ('123456789')

6. **SBC** button – N/A for UMP SP Edition (applicable for CloudBond 365)
7. Click **Apply**.
The UMP 365 server connects to the One Voice Operations Center server.
8. Once the system has successfully detected on the OVOC server, follow the instructions in the *One Voice Operations Center User's* manual to allocate a license from the OVOC License Pool.
9. After you have completed license configuration in the OVOC, the UMP 365 server will retrieve the license from the OVOC and you may log in to the system.

3.18 Initial SBC Configuration

This section describes how to add an SBC to the UMP Database, configure the SBC parameter and select the common parameters.

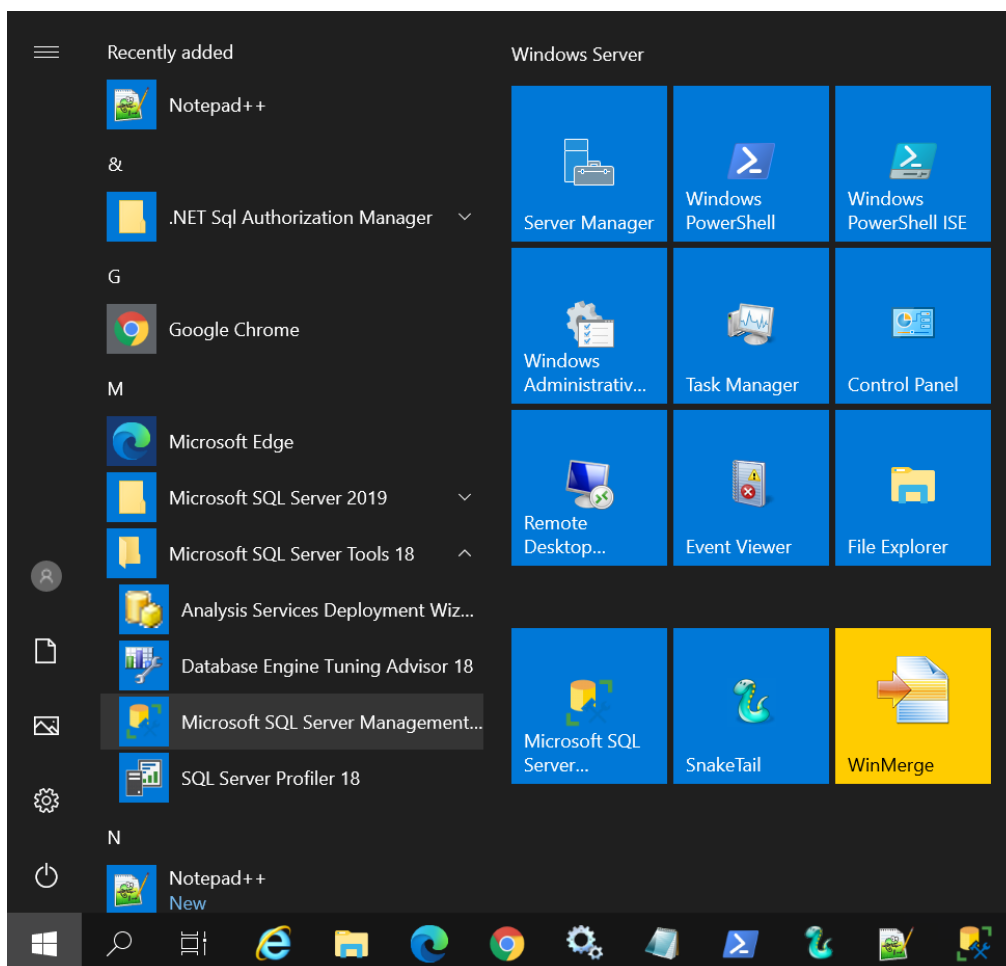
3.18.1 SBC Setup

This section describes how to setup the SBC.

➤ **To set up the SBC:**

1. Run Microsoft SQL Server Management Studio.

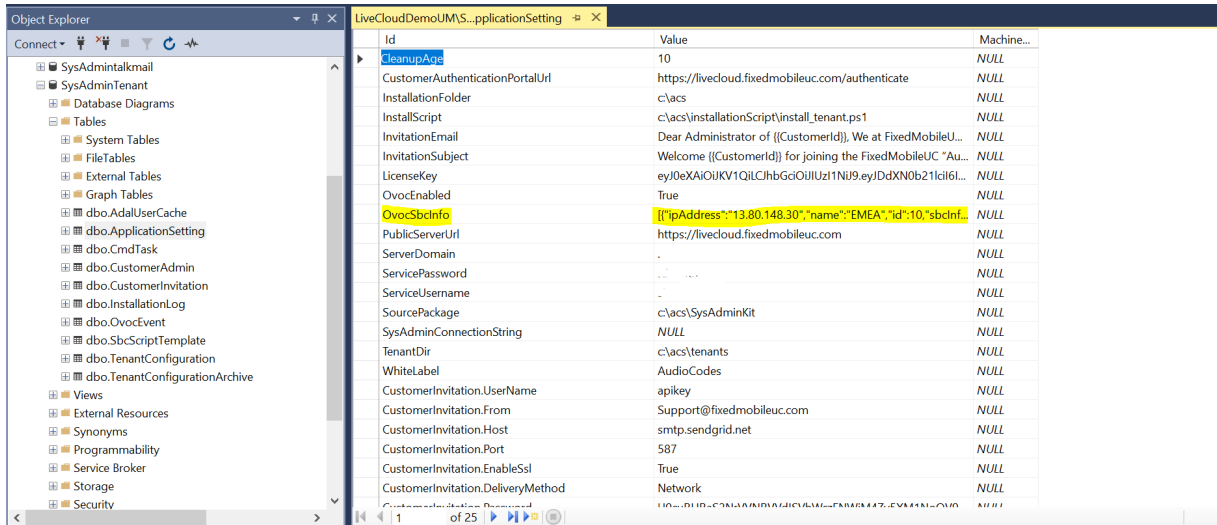
Figure 3-45: Select SQL Server Management Studio Tool



2. Run Microsoft SQL server Management Studio.
3. Select SysAdminTenant and dbo.ApplcationSetting, right-click, and then select Edit Top 200 Rows.
4. Add or edit the row with ID OvocSbcInfo to include the SBC parameters:
 - ipAddress: "xxx.xxx.xxx.xxx"
 - name: "The SBC Name", this will be the select region name you will select in step 3 - Voice Route Setting. Recommended name City/Region (e.g., "New Jersey, USA")
 - "id":# (SBC ID Number from, e.g., "1")
 - "sbcInfo"
 - ◆ gatewayUser: SBC User Name (default = "Admin")

- ◆ gatewayPassword: SBC User Password (Default = "Admin")
5. Typical String:
`{["ipAddress":"x.x.x.x","name":"NewJersey,USA","id":3,"sbcInfo":{"gatewayUser":"Admin","gatewayPassword":"Admin"}},{"ipAddress":"x.x.x.x","name":"London,UK","id":4,"sbcInfo":{"gatewayUser":"Admin","gatewayPassword":"Admin"}]}`

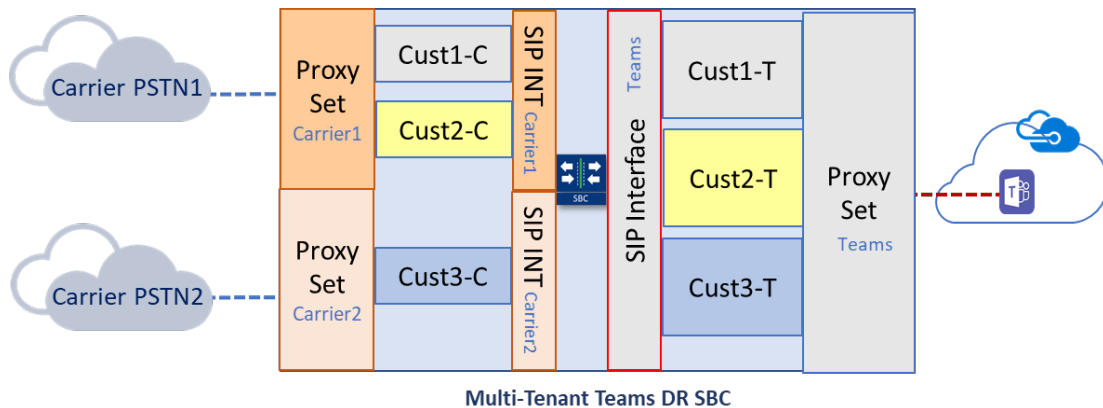
Figure 3-46: Select SQL Server Management Studio Tool



3.18.2 SBC Configuration

UMP SP allow the Provider (Service Provider or Hosted Provider) flexibility for the SBC configuration. In the current version, the SP needs to select the SBC configuration method and upload the script. This applies to all the new Tenant configurations. In the next version, this feature will be enhanced to add a GUI to select the configuration during the setup of the SBC and to select the configuration per SBC. The SBC default configuration is as follows:

Figure 3-47: SBC Default Configuration



- Common Parameters for all the Tenants per SBC:
 - 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:
 - IP Group name
 - ◆ Carrier Side = “customer Name”-C’
 - ◆ Teams Side = “customer Name”-T’
- 6. This above configuration can be changed per customer request. Verify that the SBC is configured accordingly. If you need to change this configuration, do the following:

Select SysAdminTenant and dbo.SbcScriptTemplate, right-click and **select Edit Top 200 Rows**

Figure 3-48: SBC Script Template

Id	Script	Descripti...	Friendly...
7	configure...	NULL	sbc-scen...
700	configure...	NULL	sbc-scen...
* NULL	NULL	NULL	NULL

7. Set the following parameters:
 - ID 7 – is default script to add new Tenant
 - ID 700 – is default script to remove Tenants
 - Copy the script and change **only** the common parameter Name



Warning: Editing the script, can damage the onboarding process and the SBC configuration. We recommend that only Audiocodes Professional services will perform this change.



Note: To upload different script configurations, refer to AudioCodes Professional Services.

3.19 M365 Configuration (Optional)

UMP SP allows the provider (Service Provider or Hosted Provider) flexibility on the M365 configuration. The default M365 script is hard-coded, and can be configured and customized according to your requirements per requests to AudioCodes Professional services.

3.20 UMP Networking Configuration

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

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

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

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

3.20.1 UMP Firewall Configuration

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

Table 3-1: UMP Ports Networking

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

3.21 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 3-2: 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	Attribute	Customer		AudioCodes
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	-



Note:

- 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 3-3: VPN Tunnel Ports

Transport/Port/Protocol	AudioCodes > Customer	Customer > AudioCodes
TCP 22 (SSH)	√	-
UDP 162 (SNMP)		√
UDP 161 (SNMP)	√	
TCP 443 (HTTPS)	√	-
TCP 3389 (RDP)	√	-
TCP; 636 (LDAPs)	-	-
The following ports are required if managed devices are monitored using central OVOC (AudioCodes Datacenter)		
UDP 1161 (SNMP)	Bi-directional	
TCP 5000 (QoE)		√



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

3.22 SQL License Guidelines - Optional

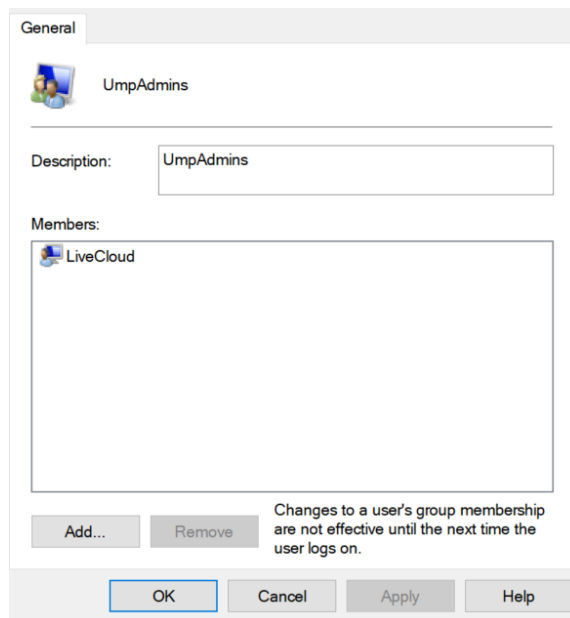
This chapter describes the SQL licensing guidelines. The UMP SP solution requires SQL 2019 Standard edition. Customers can do one of the following:

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

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

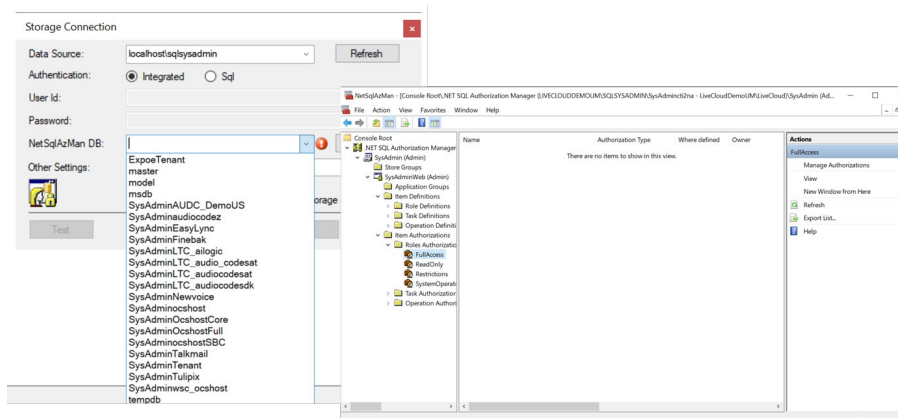
- **UMP SP Super Admin Users (Windows):**
 - All the users under Group “UmpAdmins”

Figure 3-49: UmpAdmins user members



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

Figure 3-50: Tenant Admin User (Windows)



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

Figure 3-51: Account List

The screenshot shows the Audiocodes Customer Admins interface. At the top, there is a search bar for 'App Registration Application (Client) ID' and a 'Save' button. Below this is a table with columns for 'Id', 'Customerid', and 'Account'. The table contains 17 entries. At the bottom of the table, it says 'Showing 1 to 10 of 10 entries' and has 'Previous', '1', and 'Next' navigation buttons.

Id	Customerid	Account
1	easylync	davide@audiocodes.com
2	finebak	davide@audiocodes.com
3	EnterpriseRTC	davide@audiocodes.com
5	easylync	Channel@ACLPS2.onmicrosoft.com
8	EnterpriseRTC	Channel@ACLPS2.onmicrosoft.com
9	talkmail	audcapac@audiocodes.be
10	MailVision	davide@audiocodes.com
11	EnterpriseRTC	admin@ACLPS2.onmicrosoft.com
16	Newvoice	Channel@ACLPS2.onmicrosoft.com
17	easylyncusa	rani@audio-codes.biz

The guidelines are the follow:

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



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

Part II

User Management Pack 365 SP Edition

Onboarding a New Tenant (Microsoft 365 Customer)

4 Overview

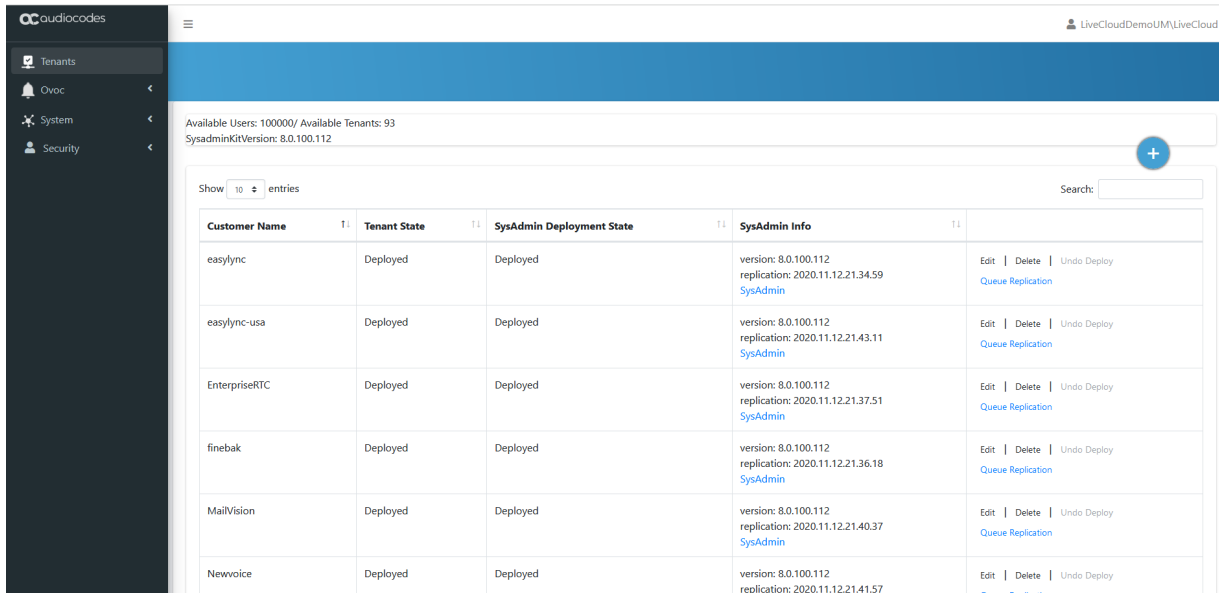
Microsoft 365 Tenant setups require deep PowerShell expertise and SBC configuration knowledge, where the acquisition of such skills involves high costs and is time consuming. The UMP 365 SP Edition application significantly simplifies the implementation of these skills through a sophisticated Microsoft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

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

4.1 Provider Main Screen View

The figure below displays an example screen including a list of M365 customers Tenant:

Figure 4-1: Provider Main Screen View



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

- Total # of available Tenants and Users (per system)
- Search
- 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
 - SysAdmin: Link to Customer WEB Application to manage their users.
- Action Bar: Edit, Details, Undo Deploy and Queue Replication

5 Adding a New M365 Tenant

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.

5.1 Prerequisites

This section shows how to set up the Office 365 platform prior to adding a new M365 Tenant:

- Add the providers domain to the tenant for the new M365 Tenant (see below)
- Activate the domain (see Section 5.1.2)



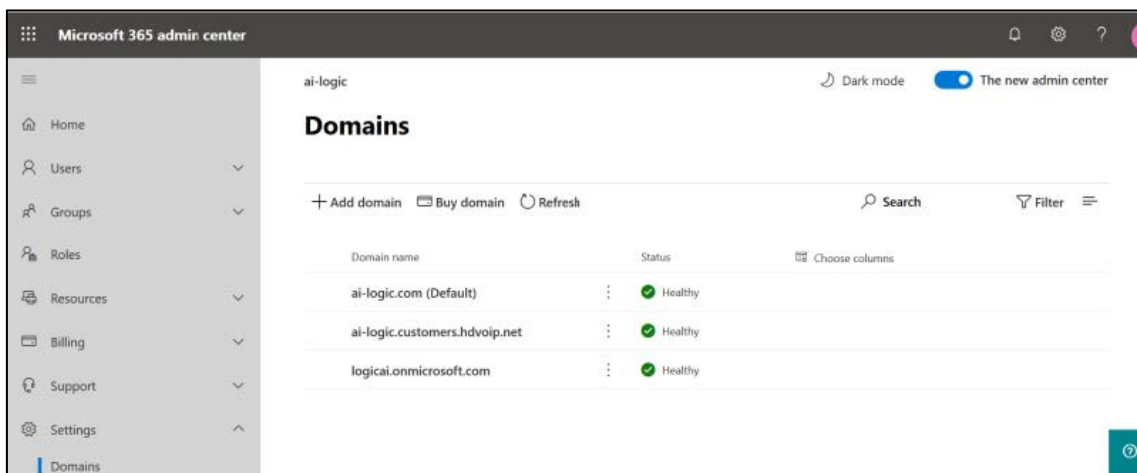
Notes:

- The provider needs to verify with the customer Tenant that Voice Routing Policy 'Unrestricted' isn't in use.
- For further information, see Microsoft's guidelines "Register a subdomain name in a M365 Tenant": <https://docs.microsoft.com/en-us/microsoftteams/direct-routing-sbc-multiple-tenants#register-a-subdomain-name-in-a-M365-Tenant-tenant>.

5.1.1 Registering a Subdomain Name for an M365 Tenant

You must register a subdomain name for the new M365 Tenant under the **Domains** tab.

Figure 5-1: Adding Providers Domain



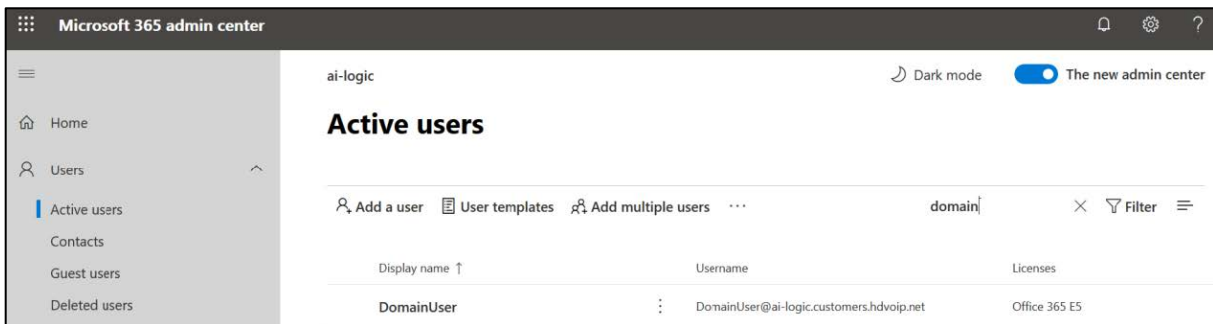
5.1.2 Activating the Providers Domain

Activate the new domain you created above by adding the E1or E3 licensed user and assigning a SIP address with the FQDN of the Providers subdomain under the **Active Users** tab. In addition, you need to add at least one user with a Phone System license and assign a SIP address with the FQDN portion of the SIP address that matches the created base domain. The License can be revoked after the domain activation (this may take up to 24 hours).



Note: The Carrier tenant must keep at least one Phone System license assigned to the tenant to avoid removal of the Skype for Business configuration.

Figure 5-2: Active Users



5.2 Adding the new Customer M365 Tenant

This section describes how to add the new M365 Tenant.

5.2.1 Securing Connection with Microsoft 365

Before you can add a new tenant, you need to connect to establish a secure connection to Microsoft 365. This can be performed by using one of the following methods:

- Use M365admin account with known password
 - Send link to customer IT administrator for authentication
- **To add a new M365 Tenant, do the following:**

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

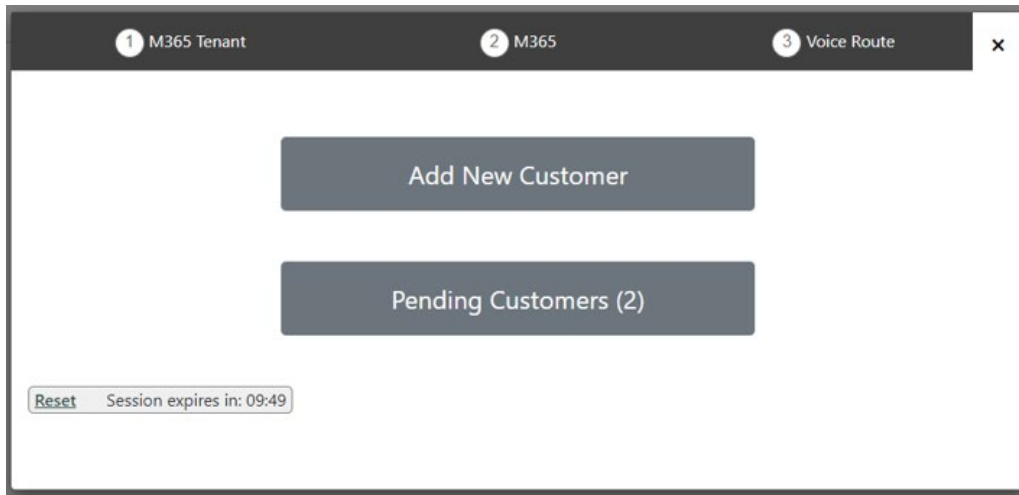


Figure 5-3: M365 Tenants

Customer Name	Tenant State	SysAdmin Deployment State	SysAdmin Info	
cti2na	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.08.54 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
enterpricentc	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.07.38 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
Finebak	Deployed	Deployed	version: 8.0.100.67 replication: 2020.09.22.17.11.31 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
MailVision EMEA	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.06.18 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
newvoice	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.10.09 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
TalkMail EMEA	Deployed	Deployed	version: 8.0.100.0 replication: 2020.09.22.18.05.08 SysAdmin	Edit Delete Details Undo Deploy Queue Replication
Tulipix	ReadyForRemove	ReadyForRemove		Edit Delete Details Cancel

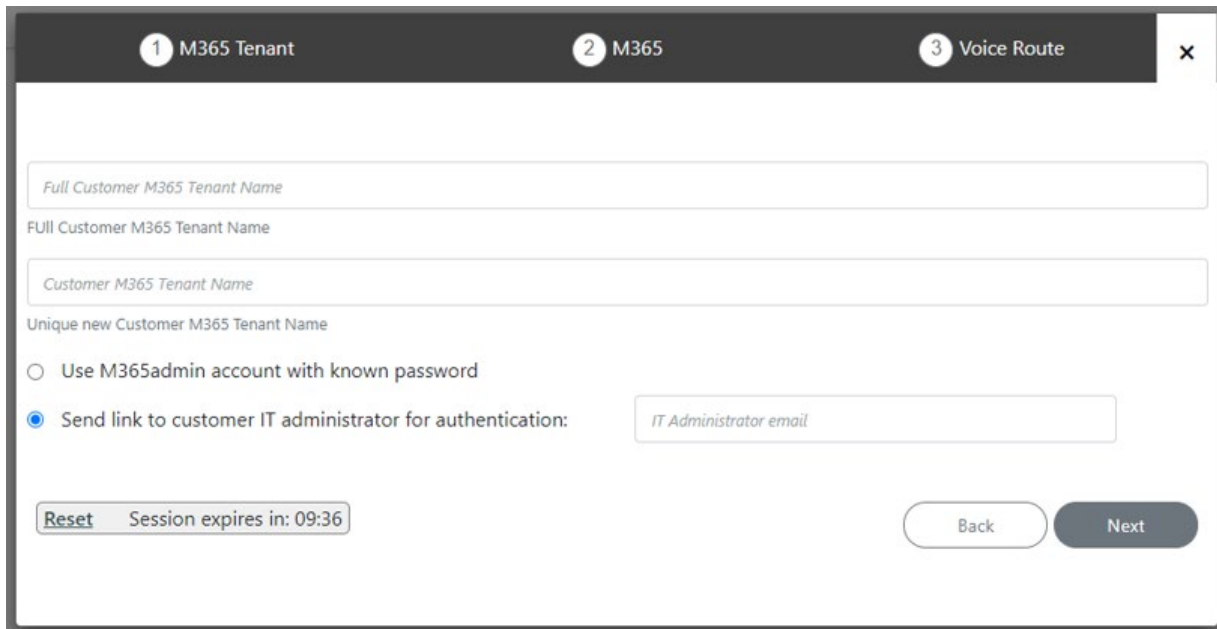
The Onboarding interface opens.

Figure 5-4: Add New Customer



2. Click **Add New Customer**

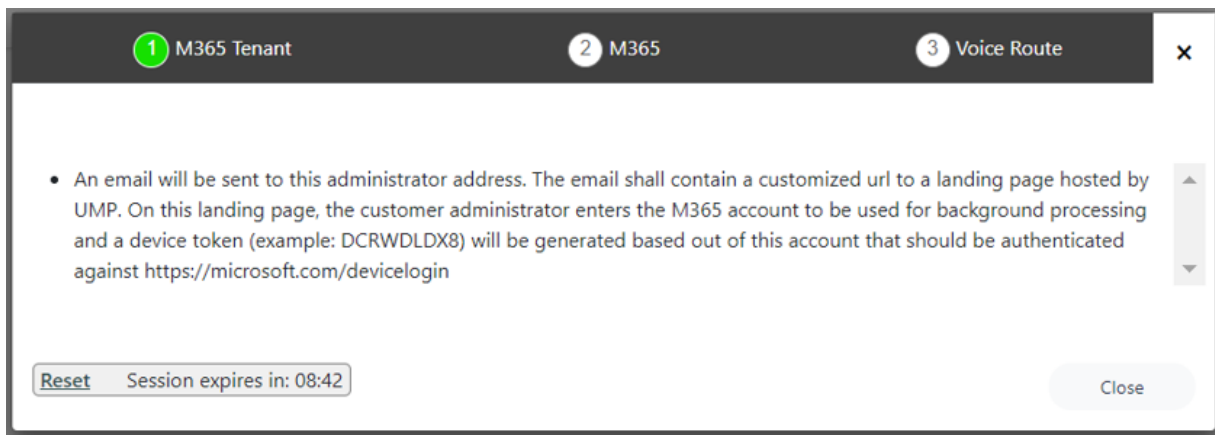
Figure 5-5: Add New Customer



3. Full Customer M365 Tenant Name – Free Text .
4. Unique new Customer M365 Tenant Name - Define a unique name for the new M365 Tenant.
 Note the following rules:
 - The string should be 3-15 characters long
 - 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 one of the following options and the click **Next**:
 - Use M365admin account with known password (proceed to Chapter 5.2.3)
 - Send link to customer IT administrator for authentication (see below)

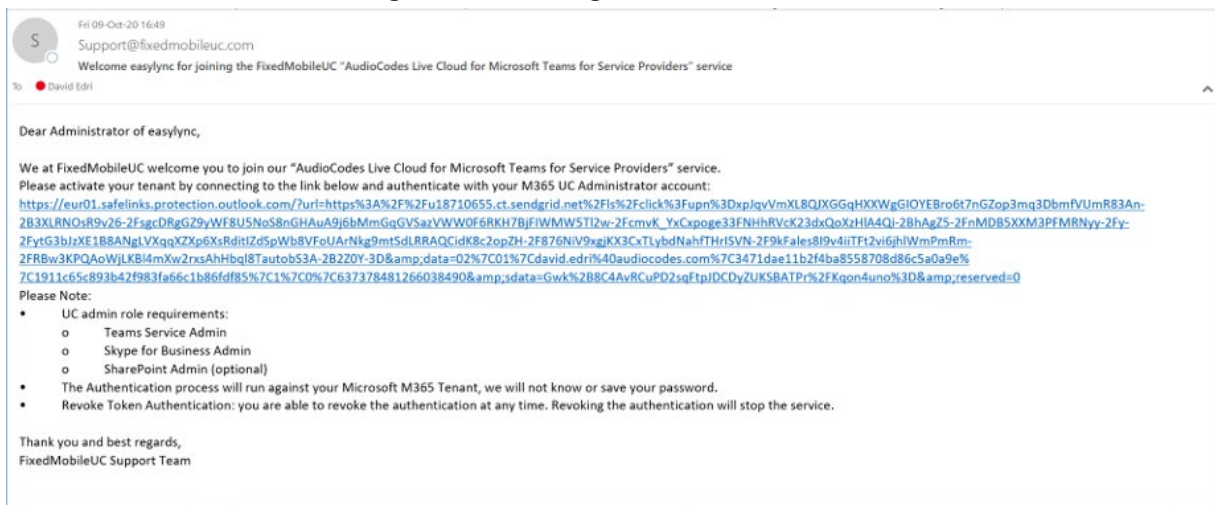
If you chose to send link to IT administrator, the following screen appears:

Figure 5-6: Send link to customer IT administrator for Authentication



An email message similar to the following is sent to the customer IT administrator:

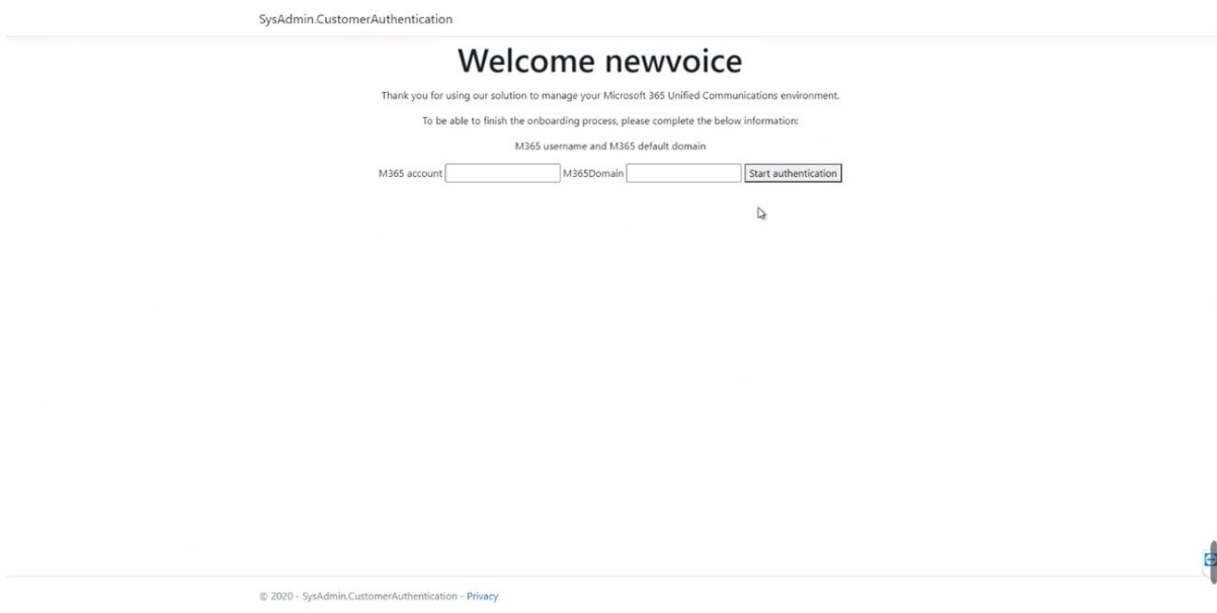
Figure 5-7: Message to IT Administrator



6. Monitor the requests sent to the customer IT administrator.

- When the IT administrator clicks the link shown in Figure 5-7, the following screen is displayed:

Figure 5-8: Enter Microsoft 365 Unified Communications Environment

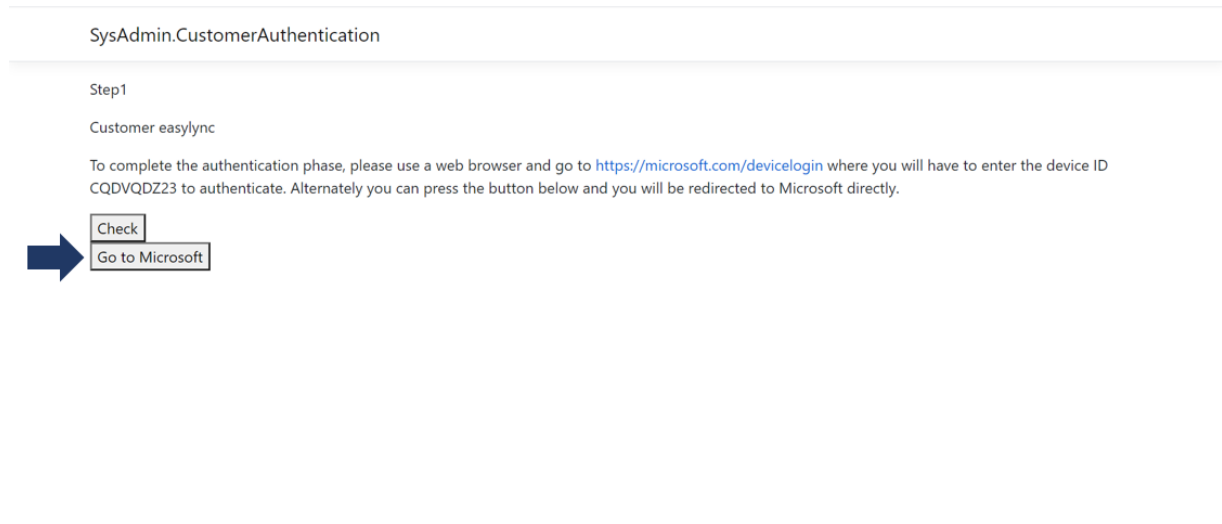


- Define Microsoft 365 credentials:

Table 5-1: Microsoft 365 Settings

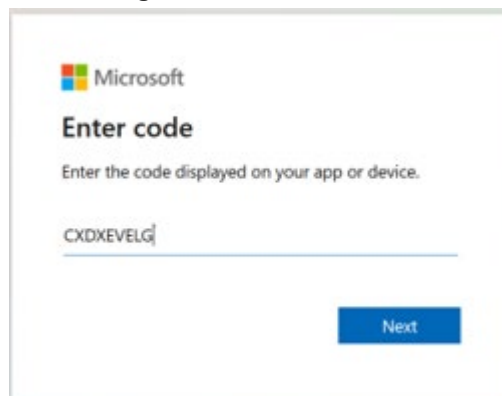
M365 Setting	Description
M365 UC Admin	Microsoft 365 UC Admin User (User with Teams Admin Credential). <ul style="list-style-type: none"> ▪ Admin roles <ul style="list-style-type: none"> ✓ Teams Admin & Skype for Business Admin ✓ Optional: User admin to manage usernames ✓ Optional SharePoint Admin to manage SharePoint, then this administrator must also have SharePoint Admin credential.
M365 Domain (Override Admin Domain)	Customer Tenant original Microsoft 365 domain prior to applying vanity domain names ("example.onmicrosoft.com")

9. Do one of the following:
 - a. Go to <https://microsoft.com/devicelogin> Microsoft link and enter the device ID (e.g. CQDVQDZ23).
 - b. Click Go to Microsoft to redirect to Microsoft directly.

Figure 5-9: Customer Authentication

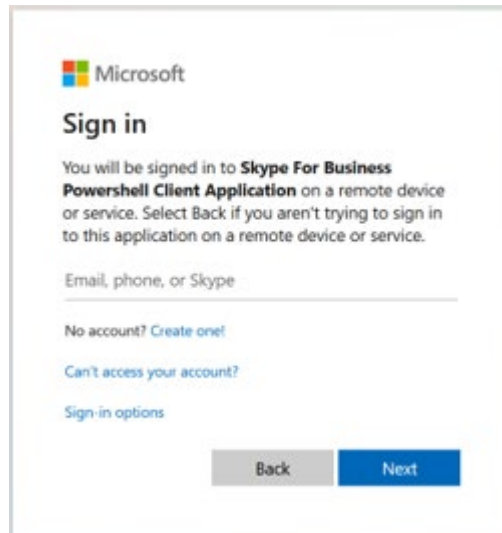
© 2020 - SysAdmin.CustomerAuthentication - [Privacy](#)

10. Enter the security code sent to your app or device and then click **Next**.

Figure 5-10: Enter Code

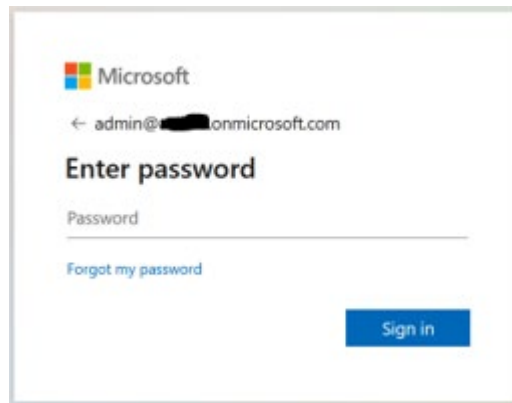
11. Enter your Microsoft 365 user credentials.

Figure 5-11: Sign in



12. Enter your Microsoft 365 password.

Figure 5-12: Enter Password (replace screen)



The following screen is displayed when the authentication has completed.

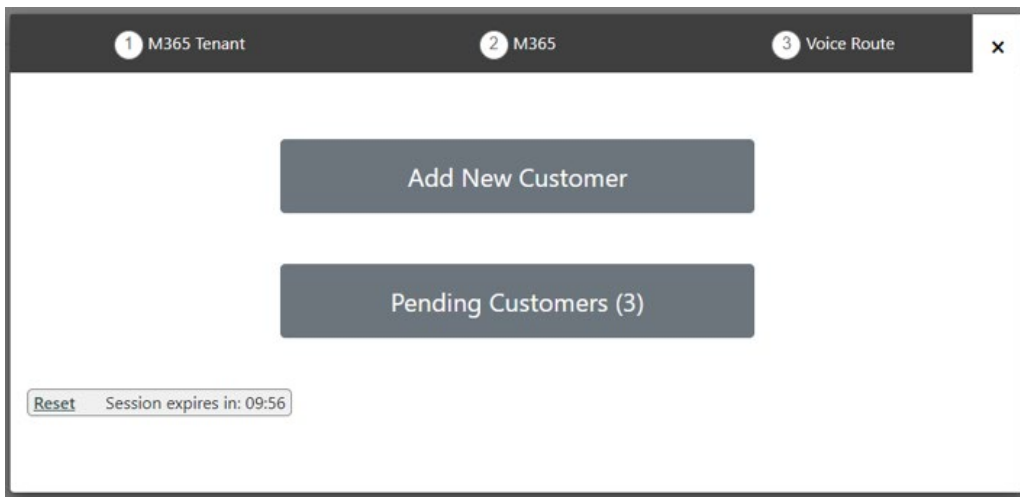
Figure 5-13: Authentication Complete



5.2.2 Pending Requests

You can monitor the status of Pending Requests by clicking **Pending Customers**.

Figure 5-14: Pending Customers



A list of pending authentication requests is displayed:

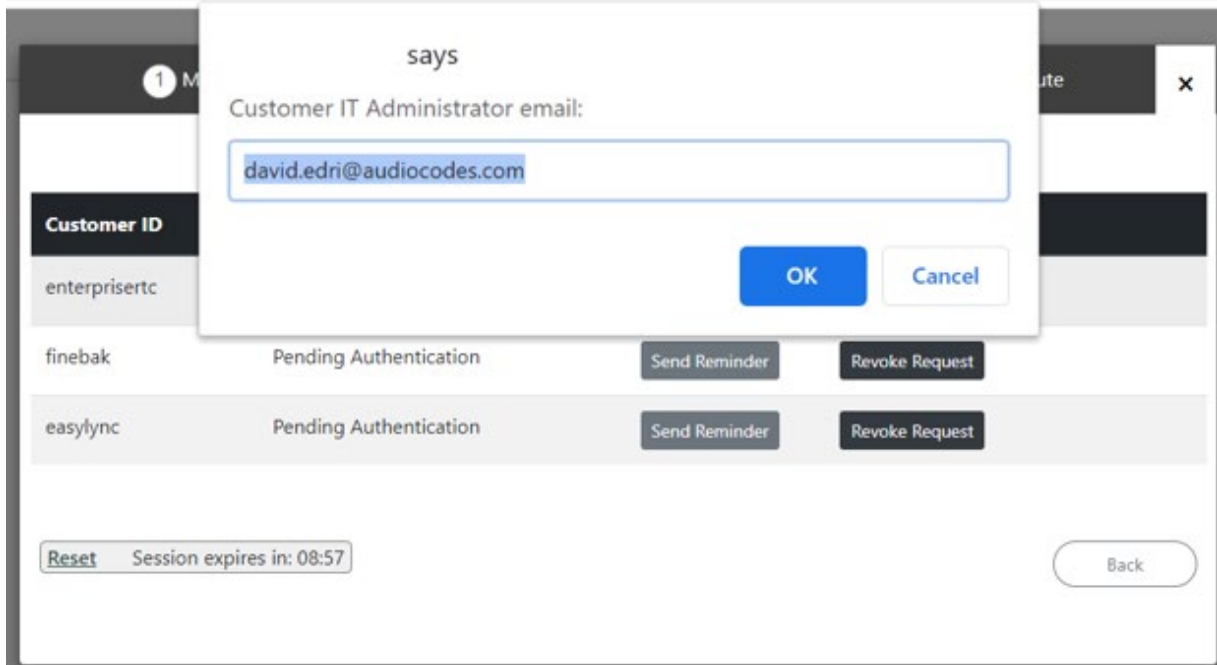
Figure 5-15: List of Pending Customers

Customer ID	Status	Actions
enterprisertc	Pending Authentication	Send Reminder Revoke Request
finebak	Pending Authentication	Send Reminder Revoke Request
easylync	Pending Authentication	Send Reminder Revoke Request

You can perform one of the following actions:

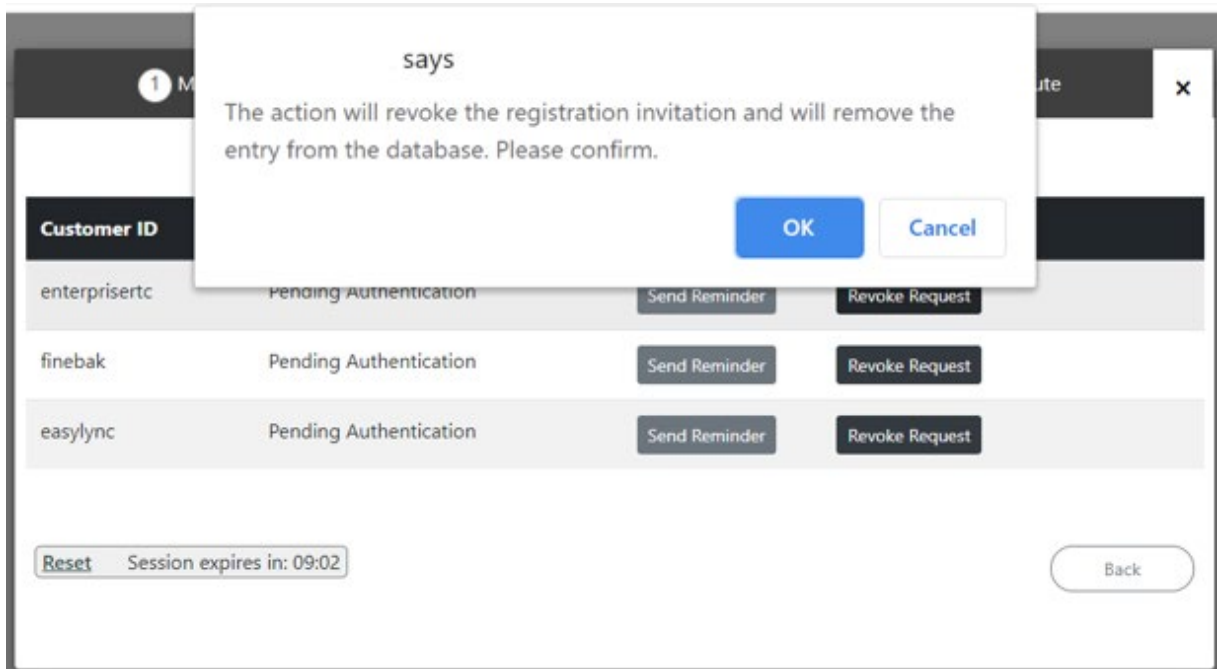
- **Send Reminder:** send a reminder to the customer IT administrator to approve the request. The windows will pop up with the email sent with the original request. The administrator can change the email address.

Figure 5-16: Send Customer Email



- **Revoke Request:** revoke the request sent to the customer IT administrator

Figure 5-17: Revoke Request



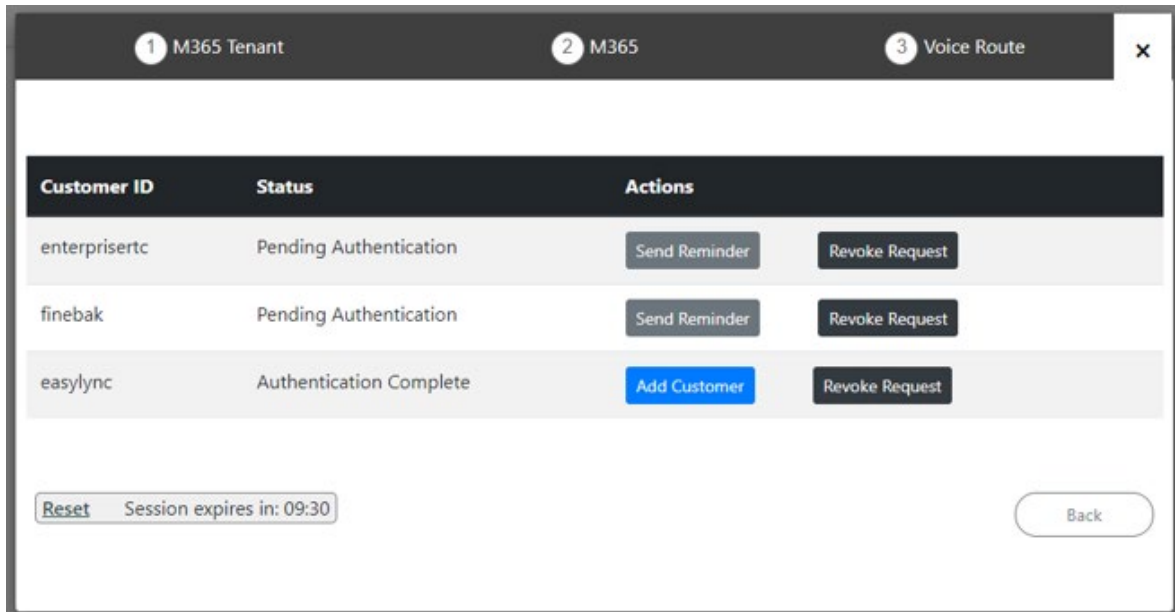
5.2.3 Adding Customer

Once you have established a secure connection to Microsoft 365, you can add a new customer M365 tenant.

➤ **To add a new customer:**

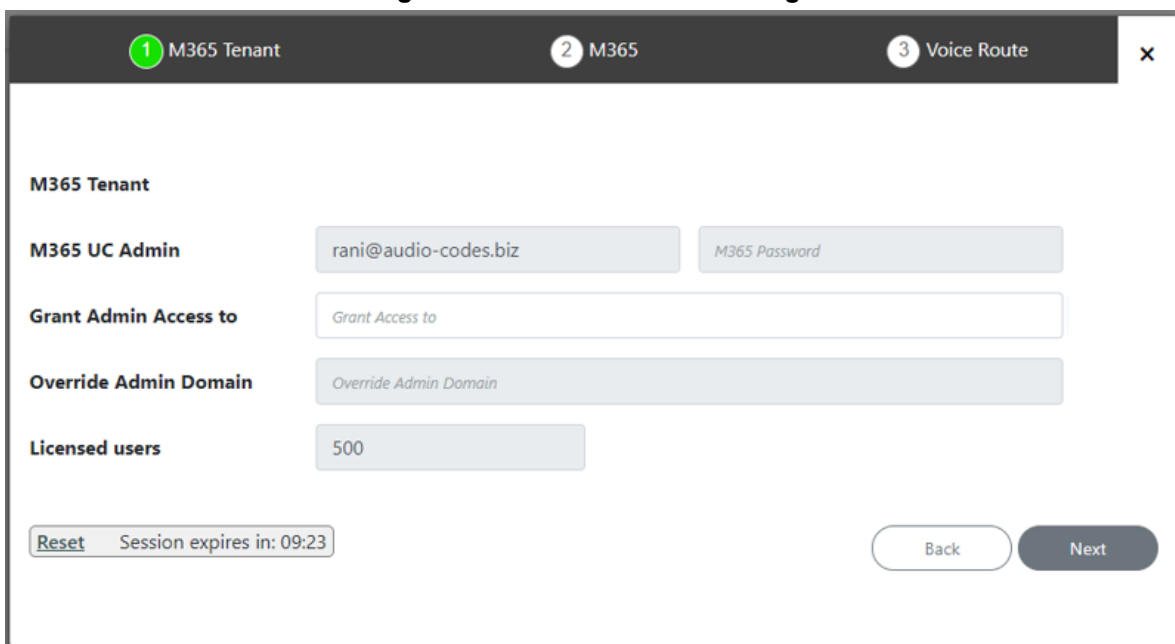
1. Click **Add Customer**.

Figure 5-18: Add Customer



2. Define M365 Setting. The Microsoft 365 Settings screen is displayed (this is the first step if you have logged in with M365admin account with known password option):

Figure 5-19: Microsoft 365 Settings



- Define Microsoft 365 settings.

Table 5-2:Microsoft 365 Settings

M365 Setting	Description
M365 UC Admin	Microsoft 365 UC Admin User (User with Teams Admin Credential). <ul style="list-style-type: none"> ▪ Admin roles <ul style="list-style-type: none"> ✓ Teams Admin & Skype for Business Admin ✓ Optional: User admin to manage usernames ✓ Optional SharePoint Admin to manage SharePoint, then this administrator must also have SharePoint Admin credential.
M365 Domain (Override Admin Domain)	Customer Tenant original Microsoft 365 domain prior to applying vanity domain names (“example.onmicrosoft.com”)

- Click **Next** to continue.

Figure 5-20: Voice Route

The screenshot shows a configuration window titled "Voice Route" with three steps: 1. M365 Tenant, 2. M365, and 3. Voice Route. The "Voice Route" step is active. The configuration options are:

- Online PSTN Gateway:** Select an Value from list
- Select Region:** Select an SBC from list
- Select Carrier:** Select a Carrier from list
- Carrier Registration**
- Enable CAC**
- Prefix / Number Range:** (Section header)
- Update from CSV:** Choose file | Browse
- Telephone Number Prefix:** New Number prefix

At the bottom, there is a "Reset" button, a "Session expires in: 08:36" timer, and "Back" and "Submit" buttons.

5. Configure Direct Routing parameters according to the table below.

Table 5-3:Direct Routing Configuration

O365 Setting	Description
Online PSTN Gateway	Unique subdomain name per M365 Tenant (CSOnlinePSTNGateway –FQDN) which represents the desired host name added for the carrier trunk. This name must be preconfigured on the M365 Tenant Domain (see Section 5.1.1).
Select Region	Select the required City/Area/Region device from the drop-down list. See below
Select Carrier	Select the desired carrier trunk to which the above host is using.
Carrier Registration	Select this option to perform SIP Registration for the Carrier trunk: <ul style="list-style-type: none"> • Username: Defines the digest MD5 Authentication username. The valid value is a string of up to 60 characters. By default, no value is defined. • Password: Defines the digest MD5 Authentication password. The valid value is a string of up to 50 characters. Note: The password cannot be configured with wide characters. • MainLine: 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	Enable Call Admission Control (CAC). From the drop-down list, select the desired CAC Profile including the desired number of call sessions.
Prefix Number Range	M365 Tenants to define a prefix number range using one the following methods:
Update from CSV	Browse to load a CSV file containing a range of telephone prefixes.
Telephone Number Prefix	Enter a specific telephone number prefix.

Figure 5-21: Select Region


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

Figure 5-22: Select Carrier

Figure 5-23: Carrier Registration

The screenshot shows the 'Carrier Registration' step in the M365 Tenant setup wizard. The breadcrumb trail at the top indicates the sequence: 1 M365 Tenant, 2 M365, and 3 Voice Route. The main configuration area includes:

- M365 Tenant** section with dropdowns for Online PSTN Gateway (EasyLync.customers.audiocodes.be), Select Region (EMEA), and Select Carrier (FixedMobileUC).
- Carrier Registration** checkbox, which is checked and highlighted by a blue arrow.
- Enable CAC** checkbox, which is unchecked.
- Prefix / Number Range** button.
- Update from CSV** section with 'Choose file' and 'Browse' buttons.
- Telephone Number Prefix** field with a placeholder 'New Number prefix' and a green plus icon.
- Footer with a 'Reset' button, a session timer 'Session expires in: 05:43', and 'Back' and 'Submit' buttons.

Figure 5-24: Enable CAC

The screenshot shows the 'Enable CAC' step in the M365 Tenant setup wizard. The breadcrumb trail at the top indicates the sequence: 1 M365 Tenant, 2 M365, and 3 Voice Route. The main configuration area includes:

- M365 Tenant** section with dropdowns for Online PSTN Gateway (EasyLync.customers.audiocodes.be), Select Region (EMEA), and Select Carrier (FixedMobileUC).
- Carrier Registration** checkbox, which is unchecked.
- Enable CAC** checkbox, which is checked and highlighted by a blue arrow.
- Prefix / Number Range** button.
- Update from CSV** section with 'Choose file' and 'Browse' buttons.
- Telephone Number Prefix** field with a placeholder 'New Number prefix' and a green plus icon.
- A dropdown menu for 'Select an CAC Profile' is open, showing options: 5 Sessions, 10 Sessions, 25 Sessions, 50 Sessions, and 1 sessions.
- Footer with a 'Reset' button, a session timer 'Session expires in: 04:47', and 'Back' and 'Submit' buttons.

Figure 5-25: Add Prefix

Figure 5-26: Configuration Complete

Part III

**User Management Pack 365
SP Edition**

2nd Day Operation

6 User Management Pack 365

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 and SharePoint Policies settings using the Teams Admin Center, SharePoint Admin Center and PowerShell commands.

User Management Pack 365 is a powerful software application that simplifies User Lifecycle & Identity management across Microsoft Teams and SharePoint 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 SharePoint 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.

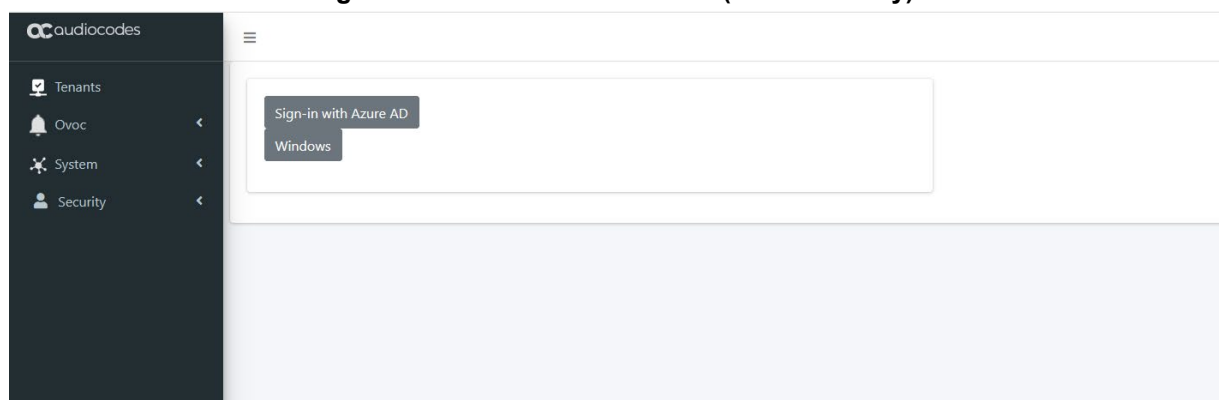
This section describes how to edit the M365 Tenant's configuration for second-day management. This interface allows you to do perform the following actions:

- Search for users
- Edit User MACD
- Assign Phone Number
- Users LifeCycle Management configuration
- Configure Online Routing
- Reserve M365 Tenant Phone Numbers
- Audit activities
- View queue for tasks status and results
- Update the Microsoft 365 Setting

6.1 General Access to UMP 365

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

Figure 6-1: Multi-Tenant Access (Provider Only)



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)

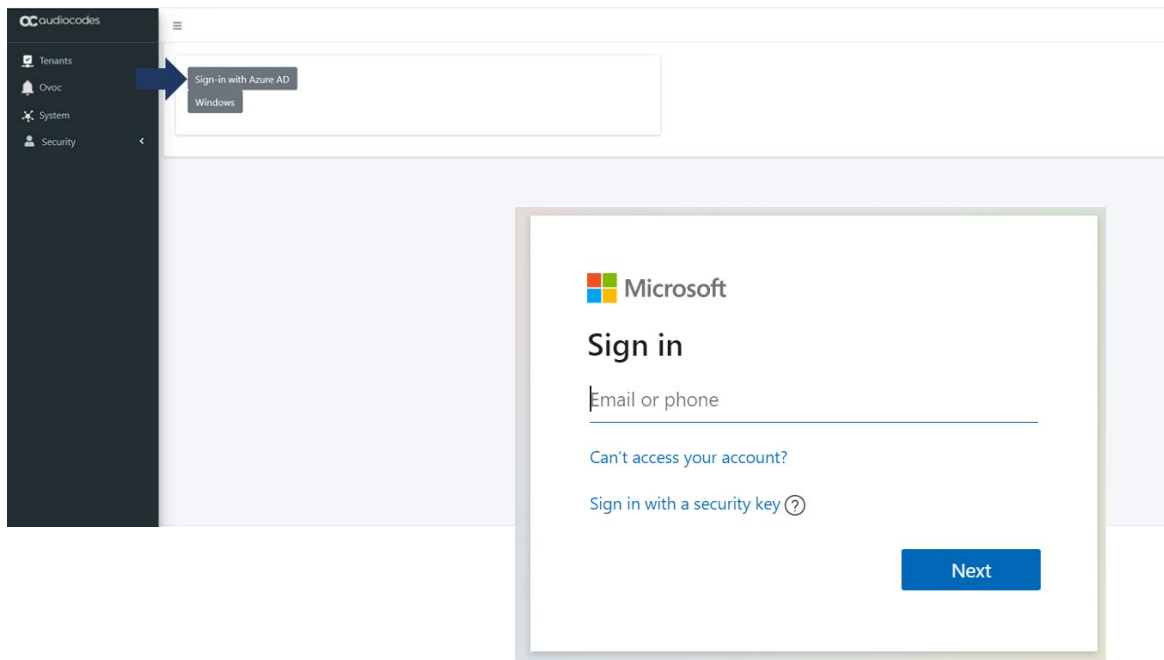
- Access to Multi-Tenant level and to all the Customers Tenant
- **Admin User:** SSO Sign-In with Azure AD user
 - ◆ Access to the customers Tenant that received Grant access

Figure 6-2: UMP 365 Authentication

Customer Name	Tenant State	SysAdmin Deployment State	SysAdmin Info	
easylync	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.34.59 SysAdmin	Edit Delete Undo Deploy Queue Replication
easylync-usa	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.43.11 SysAdmin	Edit Delete Undo Deploy Queue Replication
EnterpriseRTC	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.37.51 SysAdmin	Edit Delete Undo Deploy Queue Replication
finebak	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.36.18 SysAdmin	Edit Delete Undo Deploy Queue Replication
MailVision	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.40.37 SysAdmin	Edit Delete Undo Deploy Queue Replication
Newvoice	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.41.57	Edit Delete Undo Deploy

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

Figure 6-3: Customer Link UMP 365 Authentication



6.2 UMP 365 Managing Users Replication (Tenant Portal)

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

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



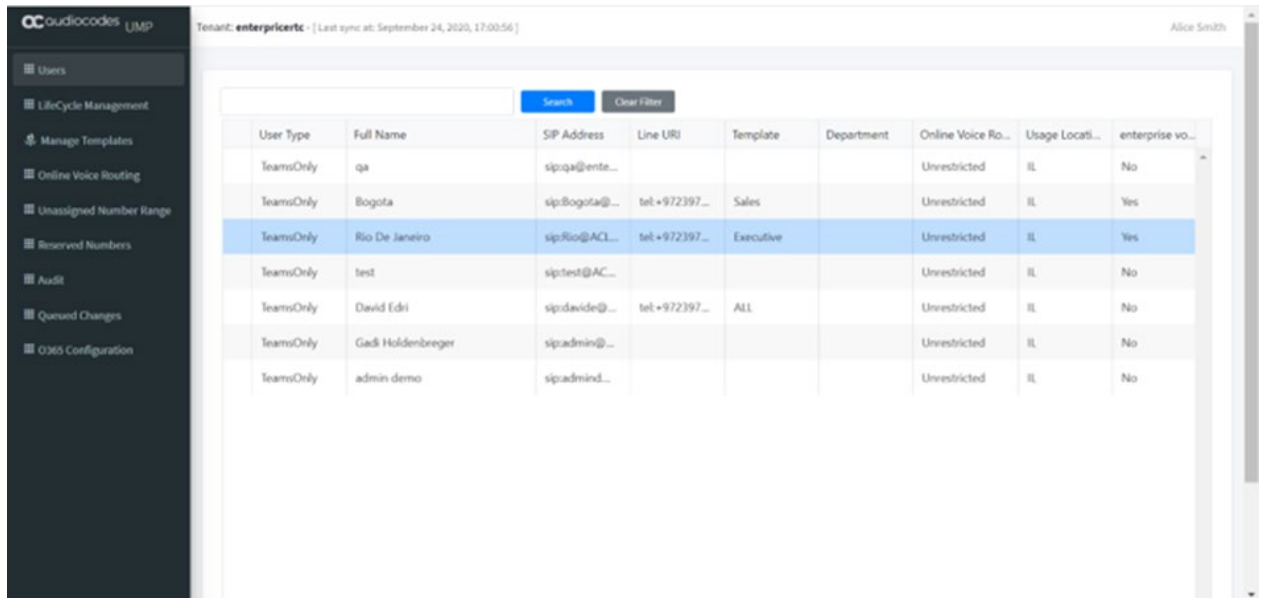
EnterpriseRTC	Deployed	Deployed	version: 8.0.100.112 replication: 2020.11.12.21.37.51 SysAdmin	Edit Delete Undo Deploy Queue Replication
---------------	----------	----------	--	--

This page is intentionally left blank.

7 Provider Portal (Provider link)

This section describes the Provider Portal view and configuration. The figure below displays the Provider Portal home page.

Figure 7-1: UMP 365 Home page - Provider Portal

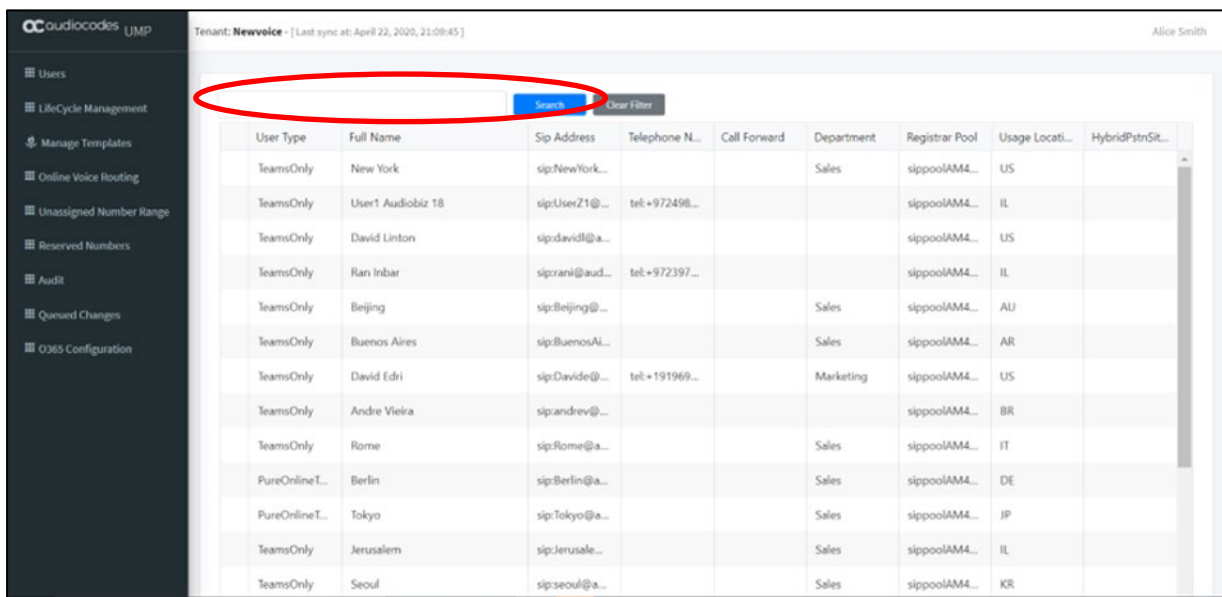


7.1 Provider Portal Searching for Users

You can search for specific users to display their details in the screen.

- **To search for a user, do the following:**
 - Click the user name or # of characters to search for a specific user.

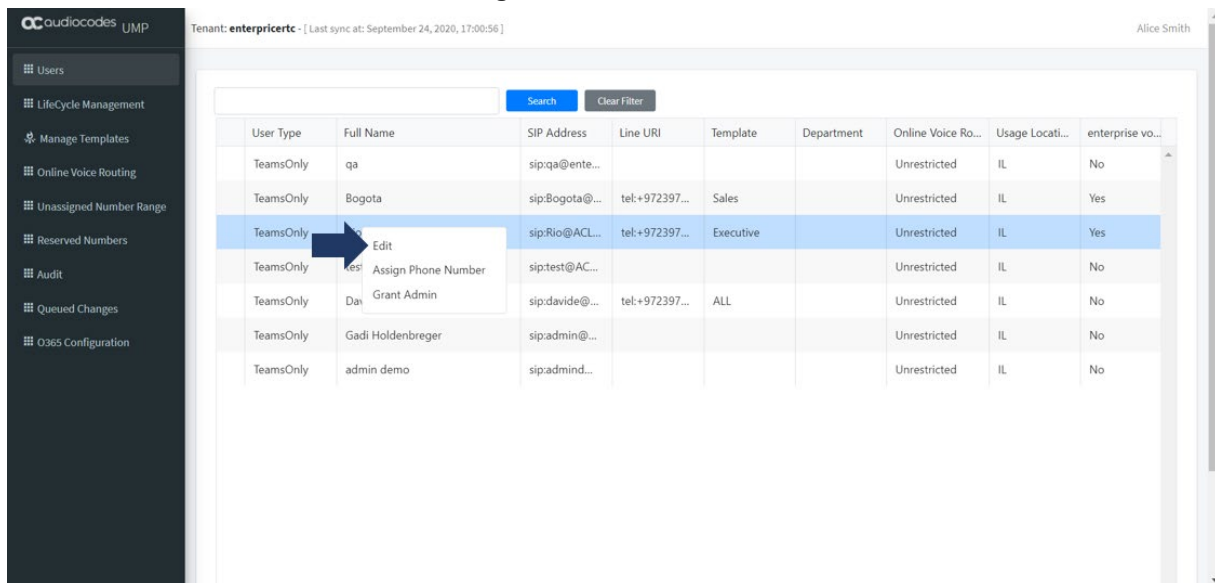
Figure 7-2: Users List



7.2 Edit Users

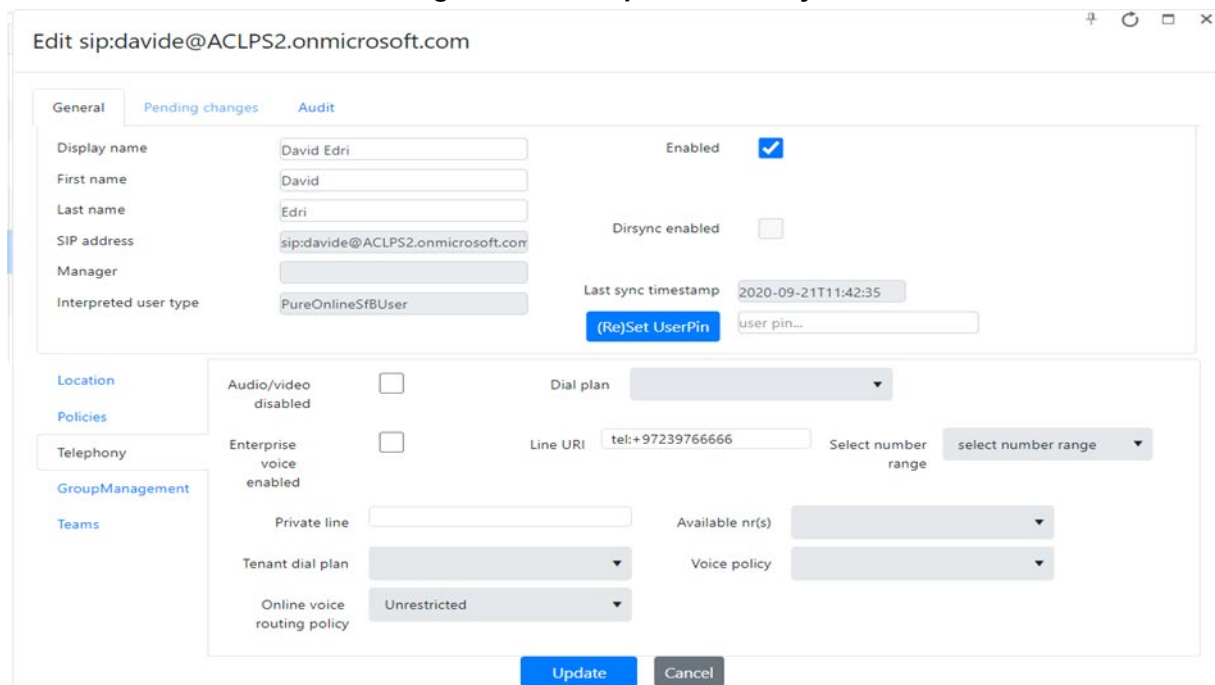
You can select a user and right-click **Edit** to edit User Policies.

Figure 7-3: Edit a User



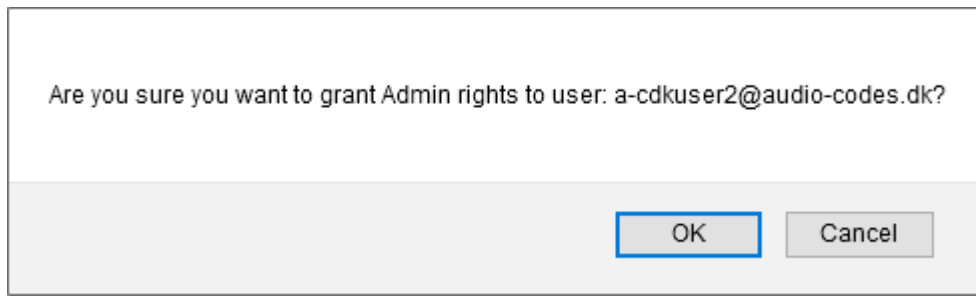
The figure below shows an example user policy.

Figure 7-4: Example User Policy



- Edit properties and click .
- Right-click and choose **Assign Phone Number** (see Section 'Assigning Phone Numbers' below).

- Right-click and choose **Grant/revoke Admin rights** to enable user as a third-party administrator (for multi-tier support).

Figure 7-5: Grant Admin Rights

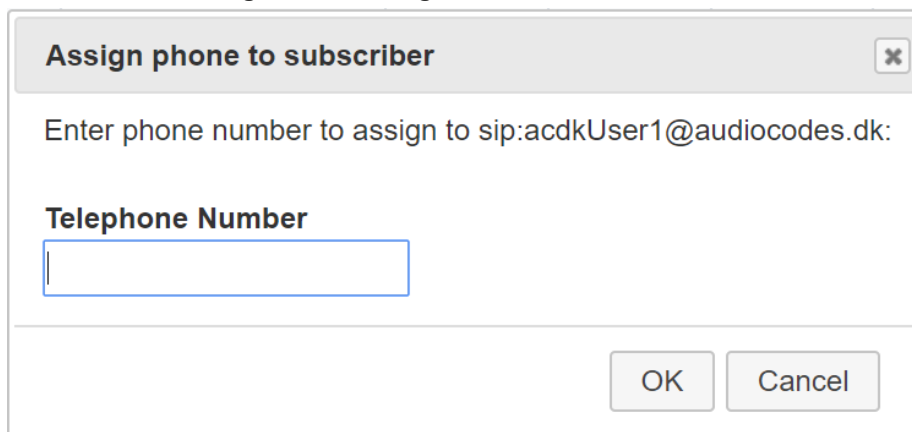
7.3 Assigning Phone Numbers

You can manually assign phone numbers that you do not wish to be automatically assigned.

➤ **To assign a phone number:**

- On the User view page, select a user and right click to assign a phone number

Assign Phone Number

Figure 7-6: Assign Phone to Subscriber

- Enter the phone number that you wish to assign to the user, and then click **OK**.
- Phone number format – tel:+xxxxxxxx
- Click Clear filter to return the list to its unfiltered view.

Figure 7-7: Assign Phone Numbers

Tenant: **Newvoice** • [Last sync at: April 22, 2020, 21:09:45] Alice Smith

User Type	Full Name	Sip Address	Telephone N...	Call Forward	Department	Registrar Pool	Usage Locati...	HybridPstrSit...
TeamsOnly	New York	sip:NewYork...			Sales	sippoolAM4...	US	
TeamsOnly	User1 Audiobiz 18	sip:User21@...	tel: +972498...			sippoolAM4...	IL	
TeamsOnly	David Linton	sip:davidl@a...				sippoolAM4...	US	
TeamsOnly	Ran Inbar	sip:rani@aud...	tel: +972397...			sippoolAM4...	IL	
TeamsOnly	Beijing	sip:Beijing@...			Sales	sippoolAM4...	AU	
TeamsOnly	Buenos Aires	sip:BuenosAI...			Sales	sippoolAM4...	AR	
TeamsOnly	David Edri	sip:David@...	tel: +191969...		Marketing	sippoolAM4...	US	
TeamsOnly	Andre Vieira	sip:andrev@...				sippoolAM4...	BR	
TeamsOnly	Rome	sip:Rome@a...			Sales	sippoolAM4...	IT	
PureOnlineT...	Berlin	sip:Berlin@a...			Sales	sippoolAM4...	DE	
PureOnlineT...	Tokyo	sip:Tokyo@a...			Sales	sippoolAM4...	JP	
TeamsOnly	Jerusalem	sip:Jerusale...			Sales	sippoolAM4...	IL	
TeamsOnly	Seoul	sip:seoul@a...			Sales	sippoolAM4...	KR	

7.4 Lifecycle Management

Lifecycle Management is a key element in the management of the M365 Tenants users. It allows automated user management based on Azure Active Directory Microsoft 365 security group membership. Users added to a security group will automatically be enabled for Microsoft Teams and will have policies and telephony settings like numbers applied based on the defined “persona” templates. Azure AD Security Group may represent a group of users on the M365 Tenants, as Site Members (HQ, Branch A unit or department where the template is tailored for the specific needs of the department or unit).

The lifecycle management feature is built upon three components, where it is critical to configure the components in the following order, because the completion of the configuration for each component is dependent on the previous one:

1. Configure unassigned number ranges, so numbers can be assigned to a template
2. Configure templates, holding policies and telephony settings
3. Configure lifecycle management and bind templates to security groups

7.5 Managing Unassigned Number Ranges

The Unassigned Number Range allows a provider administrator to define ranges with numbers that belong to their Customer M365 Tenant and should be configured under **Unassigned Number Ranges**. Unassigned Number Ranges can be used in Lifecycle Management to automatically assign telephone numbers upon user creation. You can configure a range of phone numbers to be automatically assigned to a new user.

➤ **To configure an unassigned number range, do the following:**

1. Click the **Unassigned Number Range** tab.

Figure 7-8: Unassigned Number Range

Identity	NumberRangeStart	NumberRangeEnd	NumbersAvailable
SMB	+97239766000	+97239766025	24

Showing 1 to 1 of 1 entries 1 row selected

tel:+97239766000	tel:+97239766001	tel:+97239766003	tel:+97239766004	tel:+97239766005	tel:+97239766006	tel:+97239766007	tel:+97239766008	tel:+97239766009
tel:+97239766010	tel:+97239766011	tel:+97239766012	tel:+97239766013	tel:+97239766014	tel:+97239766015	tel:+97239766016	tel:+97239766017	tel:+97239766018
tel:+97239766019	tel:+97239766020	tel:+97239766021	tel:+97239766022	tel:+97239766023	tel:+97239766024			

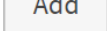
2. Click  to add a new number range.

Figure 7-9: Number Range

Add new range ✖

Please enter the requested data

Identity

NumberRangeStart

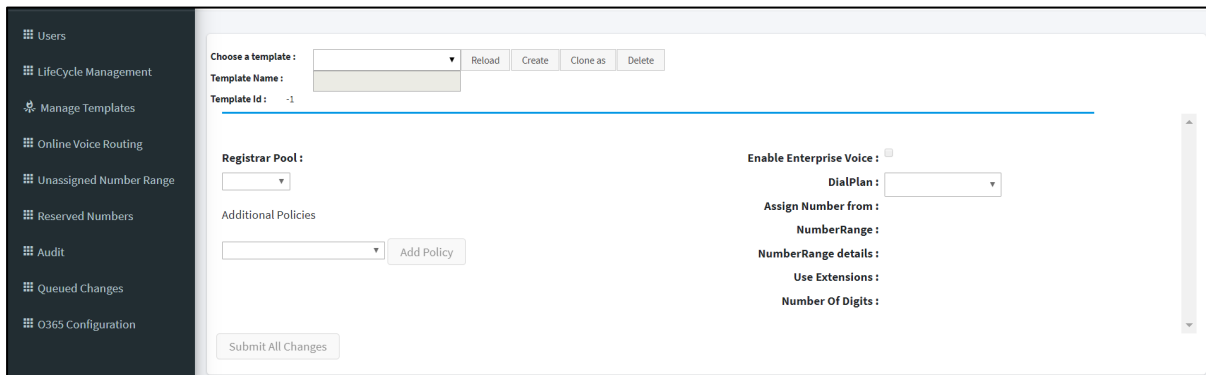
NumberRangeEnd

3. Select the Identity Name and the DID Range.
4. Click **OK**.

7.6 Managing Templates

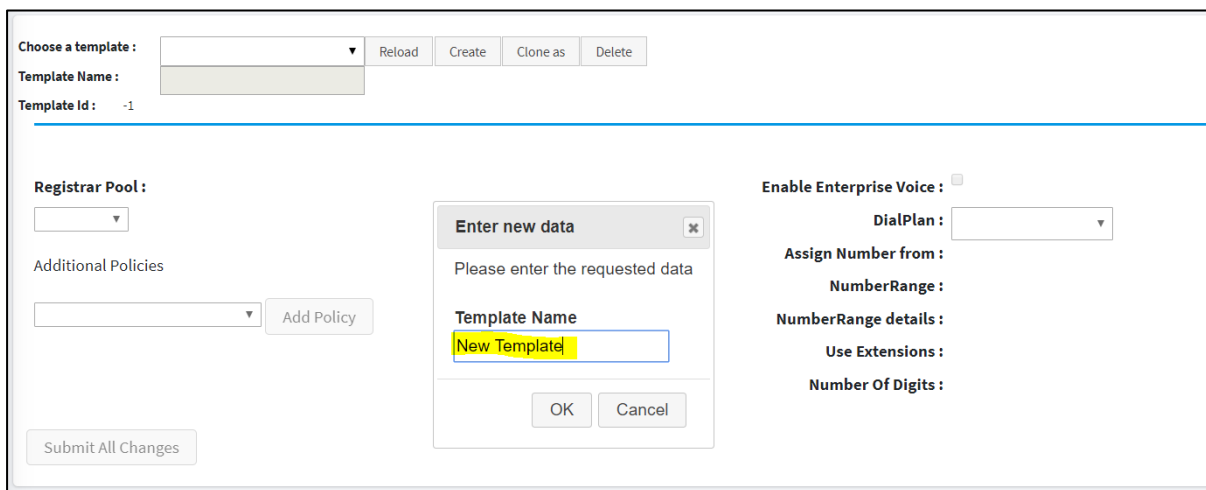
Templates are created under **Manage Templates** and are assigned to Azure AD security groups in Lifecycle management to automate policies and number assignment for users.

Figure 7-10: Telephony Template



➤ 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 (like New-Template).
2. In the Selected Template box, you can override the default text with the desired name.



3. Complete the Policy and Telephony settings section, and then select the policies you want to assign.


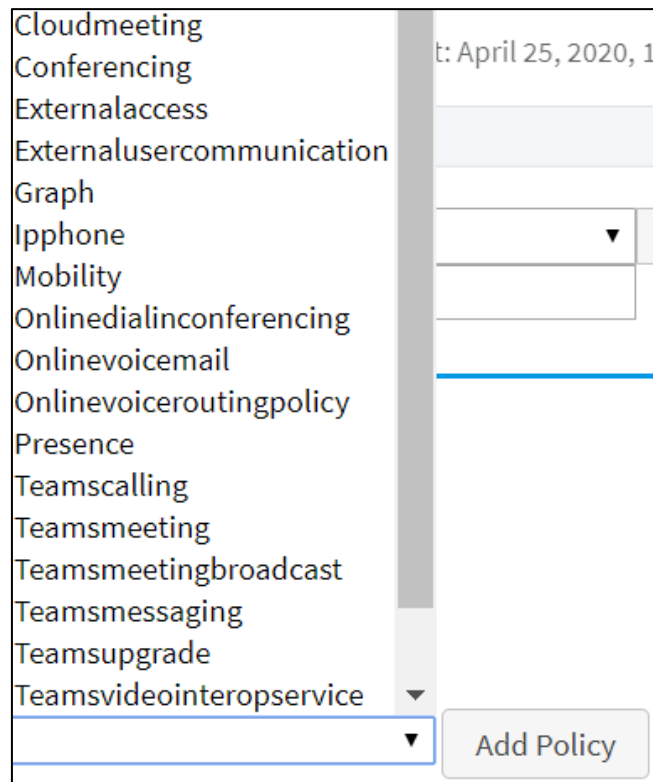
- From the Additional Policies drop-down list, select the desired Teams Policies, and then click  .

Figure 7-11: Add Policy



- Select the Policy Value for the selected policies.

Figure 7-12: Set Policy Value

Choose a template : All Users

Template Name : All Users

Template Id : 4

Registrar Pool :
Office365

Additional Policies

Teamsmeeting Policy:

Choose

- Global
- Alloff
- AllOn
- Default
- General
- Kiosk
- RestrictedAnonymousAccess
- RestrictedAnonymousNoRecording
- SalesMarketing
- Tech support
- Training

6. Select Telephony setting template. You must select the **Enable Enterprise Voice** option to enable Phone System in Microsoft 365 voice services. When configuring the Customer M365 Tenant voice in a template, a telephone number can automatically be assigned on user creation; a choice can be made from a selection of source numbers as follows:

Figure 7-13: Set Telephony Setting

Enable Enterprise Voice :

DialPlan : Local

Assign Number from :

NumberRange : -- Select Number Source --

NumberRange details : Phone

Use Extensions : Home

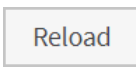
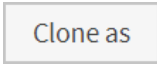
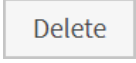
Number Of Digits : Mobile

7. When you have completed the configuration, click .



Note: 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.

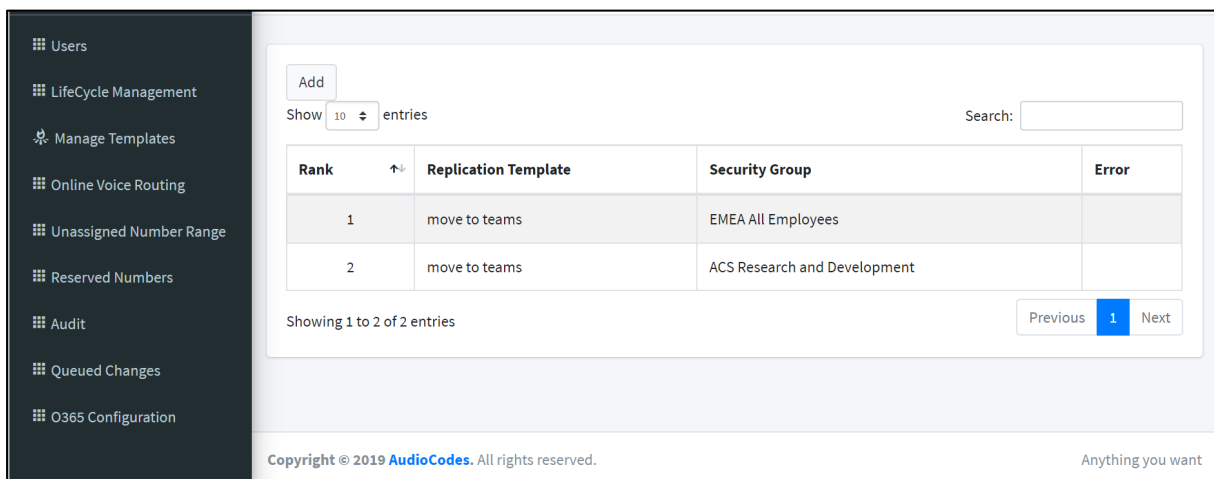
7.7 Binding Templates to Security Groups

This section describes how to assign templates to Security Groups.

➤ **To assign templates to security groups, do the following:**

1. Click the **Lifecycle Management** tab. A list of the assignments of templates to security groups is displayed.

Figure 7-14: Life Cycle Management



The screenshot shows the 'Life Cycle Management' section of the provider portal. On the left is a navigation menu with options like Users, LifeCycle Management, Manage Templates, etc. The main area displays a table with the following data:

Rank	Replication Template	Security Group	Error
1	move to teams	EMEA All Employees	
2	move to teams	ACS Research and Development	

Below the table, it says 'Showing 1 to 2 of 2 entries' and has 'Previous', '1', and 'Next' navigation buttons. At the bottom, there is a copyright notice for AudioCodes and the slogan 'Anything you want'.

2. Click  to assign a Template to a Security Group.

Figure 7-15: Binding Template to AAD Security Group

Add new
✕

Security Group (min 1 char):

Template:

-- Please select Template --

Close
Save

3. In the pop-up window, select a Security Group and select a Security Template.

4. Click .



Note: If a user is a member in multiple security groups, the template assigned to the group with the highest rank (listed last in the list) will prevail above the others. The processing order of the groups can easily be changed by dragging and dropping of the group position. Select a group and move it above or below the other group to change its rank.

7.8 Configuring Online Voice Routing

The Online Voice Routing screen allows a provider administrator to use a Web GUI interface to define their Customer M365 Tenant Voice Routing, including the following policies:

- PSTN Usage
- Voice Routing Policies
- Voice Route
- PSTN Gateways
- Normalization Rule Template
- Dial Plan



Note:

- A PSTN Gateway is not required on the customer tenant; instead, only the derived trunk FQDN must be added to the voice routing policies of the users.
- As part of the onboarding process of a customer M365 Tenant, the solution creates a new Online Voice Routing (Default name 'Unrestricted' however this can change per provider).

7.8.1 PSTN Usage

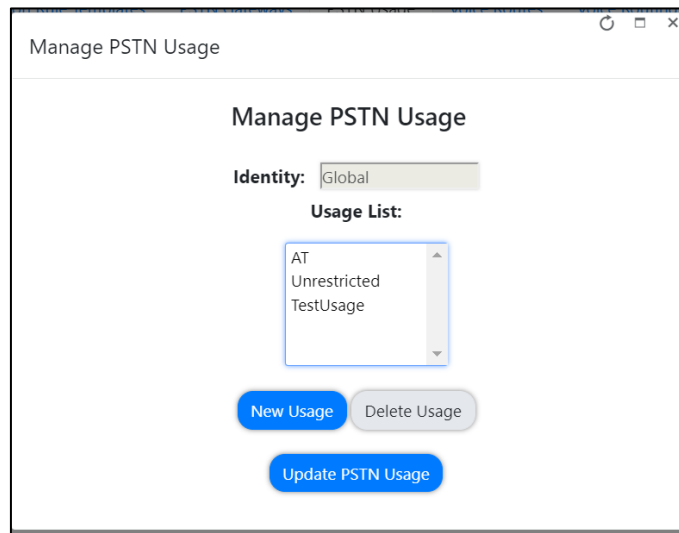
A container for voice routes and PSTN usages can be shared in different voice routing policies.

Figure 7-16: PSTN Usage

Dial Plans Normalization Rule Templates PSTN Gateways PSTN Usage Voice Routes Voice Routing Policies			
Manage Pstn Usage			
Identity	Routes	Policies	Last Replication
AT			
Unrestricted	Unrestricted		
TestUsage			

- Select the **Manage Pstn Usage** button to manage the PSTN Usage (Add/Edit/Delete).

Figure 7-17: PSTN Usage



7.8.2 Voice Routing Policy

A container for PSTN Usages can be assigned to a user or to multiple users.

Figure 7-18: Voice Routing Policy

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		

7.8.2.1 Adding Voice Routing Policy

- Select **Add New Voice Routing Policy** to add a New Voice Route.

Figure 7-19: Add New Voice Routing Policy

7.8.2.2 Editing Voice Routing Policy

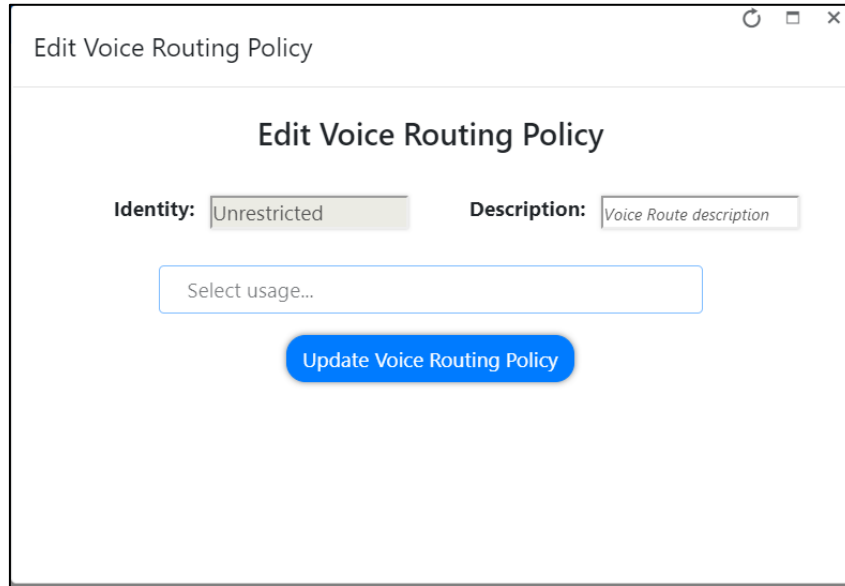
This section shows how to edit a Voice Routing Policy.

- **To edit Voice Routing Policy, do the following:**
 1. Select a Voice Routing policy.
 2. Right-click the selection
 3. Select the **Edit Voice Routing Policy** option.

Figure 7-20: Edit Voice Routing Policy Step 1

DataChang...	Identity	Description	PSTN Usage
	Global		
	Unrestricted		

Figure 7-21: Edit Voice Routing Policy Step 2



7.8.2.3 Deleting/Canceling Voice Routing Policy

This section shows how to delete or cancel a Voice Routing policy.

➤ **To delete (or cancel) a Voice Routing Policy, do the following:**

1. Select the Voice Routing policy.
2. Right-click on the selection.
3. Select the **Delete Voice Routing Policy** option, and then confirm in the pop-up prompt.

Figure 7-22: Delete Voice Routing Policy

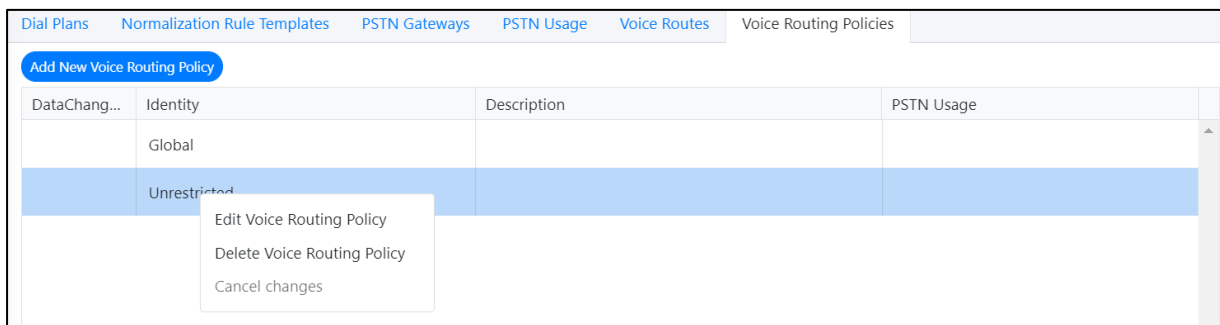
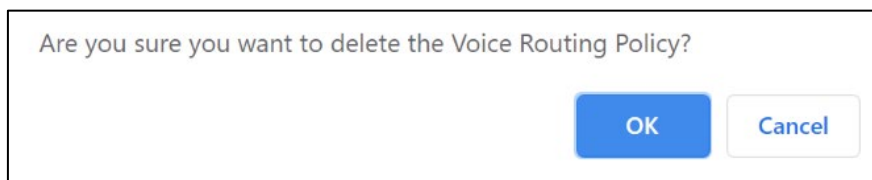


Figure 7-23: Edit Voice Routing Policy - Step 2



7.8.3 Voice Route

A voice route is a number pattern and set of online PSTN gateways to use for calls where the calling number matches the pattern.

Figure 7-24: Voice Routes

Dat...	Identity	P...	Pattern	Name	Description	Pattern	PSTN Gateway...	PSTN Usage	
	LocalRoute	0	^\{+1[0-9]{10}\}\$	LocalRoute		^\{+1[0-9]{10}\}\$			▼ ▲
	Unrestricted	1	.*	Unrestricted		.*	audiocodes-be.customers.audiocodes.be	Unrestricted	▼ ▲

To create a new Voice Route with a selection of assigned PSTN Usage records and assigned PSTN Gateway (Hosting solution - derived trunk FQDN), click [Add New Voice Route](#) to add a new Voice Route in the Voice.

Figure 7-25: Add New Voice Route

Add new Voice Route

Identity:

Name:

Description:

Number Pattern:

[Save](#)

The Voice Routing decisions are made top-down, so the table should be prioritized by using the green arrow buttons or drag and drop to make sure that a proper route is chosen if multiple routes to the same destination exist.

Voice Routing Policies will be assigned to subscribers, allowing them to reach certain destinations based on the PSTN Usage record that is assigned within the policy.

7.8.4 PSTN Gateways

A PSTN gateway is a pointer to an SBC that also stores the configuration that is applied when a call is placed through the SBC, such as forward P-Asserted-Identity (PAI) or Preferred Codecs. It can be added to voice routes.

For the hosting model (Microsoft Super Trunk), only the carriers need to set up and manage a single trunk (carrier trunk in the carrier domain).

For the customer tenant, the carrier needs to only add the derived trunk FQDN to the voice routing policies of the users. There is no need to create a new PSTN gateway for a customer trunk.

7.8.5 Dial Plan & Normalization Rules

A dial plan is a named set of normalization rules that translate phone numbers dialed by an individual user into an alternate format (typically E.164) for purposes of call authorization and call routing. Each dial plan consists of one or more normalization rules that define how phone numbers are expressed in various formats and are translated into an alternate format.

Normalization rules define how phone numbers expressed in various formats are to be translated. The same number string may be interpreted and translated differently, depending on the locale from which it is dialed. Normalization rules may be necessary if users need to be able to dial abbreviated internal or external numbers.



Note: If Dial Plans have been created in Microsoft 365 using PowerShell before UMP SP has been installed, the normalization rules that are assigned to it will not be shown in the Normalization Rule Templates in this version. Only templates that are created using UMP SP are displayed.

Figure 7-26: Normalization Rules

Dial Plans				
Normalization Rule Templates				
PSTN Gateways				
PSTN Usage				
Voice Routes				
Voice Routing Policies				
Add New Normalization Rule				
Name	Description	Pattern	Translation	IsInternalExtension

- **To create a new normalization rule, do the following:**

 1. Click **Add New Normalization Rule** to add a new Normalization rule.
 2. In the pop-up window, the following page appears. This page assists in the building of the required regular Pattern and Translation expressions.

Figure 7-27: Add New Normalization Rules

Add new Normalization Rule

Name:

Description:

Starting digits:

Length:

Digits to remove:

Digits to add:

Pattern:

Translation:

IsInternalExtension:

Save Normalization Rule

Normalization Rule Templates can be assigned to new or existing Dial Plans by double-clicking the normalization rule from the Normalization Rules section in the New or Edit Dial Plan screens. If multiple rules exist, they can be ordered by either using the green arrow buttons or by dragging-and-dropping, by placing one rule above or below another.

Figure 7-28: Dial Plan

Dial Plans | **Normalization Rule Templates** | PSTN Gateways | PSTN Usage | Voice Routes | Voice Routing Policies

Add New Plan

DataChang...	Identity	Simple Name	Description	External Prefix	Last Replicati...
	Global	DefaultTenantDialPlan			

1 - 1 of 1 items

Normalization Rules

Name	Description	Pattern	Translation	IsInternalExtension
------	-------------	---------	-------------	---------------------

- To add Normalization Rules to a New Dial Plan, do the following:
 - Click **Add New Plan** to add a new dial plan.

Figure 7-29: Add New Dial Plan

- To add Normalization Rules to an existing Dial Plan, do the following:
 1. Select a Dial Plan.
 2. Right-click the selection, and then select **Edit**.

Figure 7-30: Select Dial Plan

- In the pop-up window, add Normalization Rules to the Dial Plan.

Figure 7-31: Edit Dial Plan

The screenshot shows a window titled "Edit Dial Plan" with the following fields:

- Identity:** test
- Simple name:** testSN
- Description:** test dial plan
- External Access Prefix:** External Access Prefix

Below these fields is a section titled "Normalization Rules" with a dropdown menu set to "undefined". A table lists the rules:

Name	Pattern	Translation	IsIn...	
test1	^66\d{1}(\d{3})\$	+97239\$1		▼ ▲ 🗑️
test2	^111\d{1}(\d{-5\d+})\$	+888\$1		▼ ▲ 🗑️

A blue "Save" button is located at the bottom center of the window.

- If multiple rules exist, they can be ordered by either using the green arrow buttons or by dragging and dropping, by placing a rule above or below another.

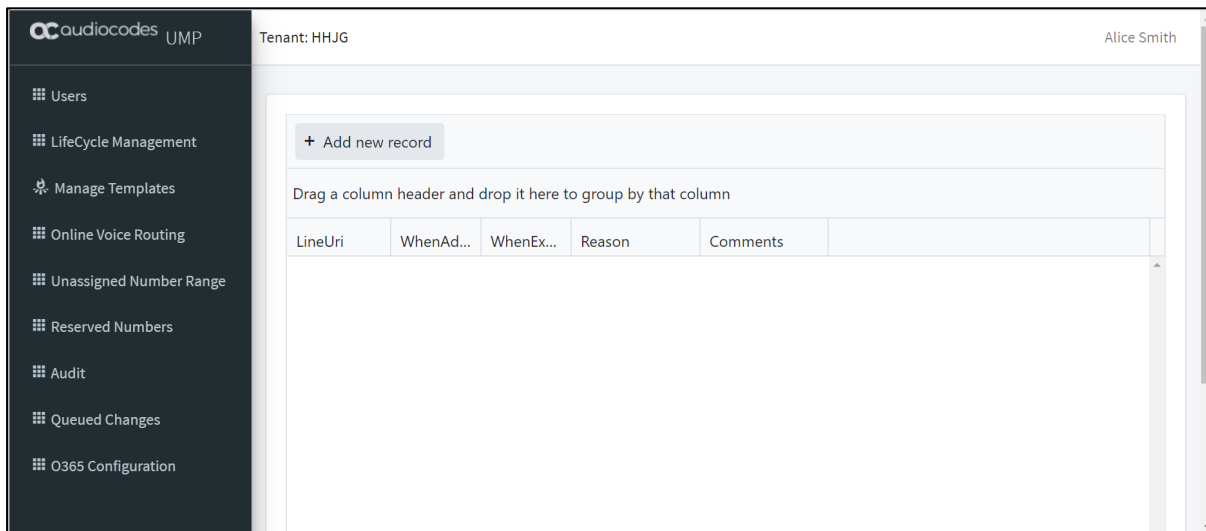
7.9 Reserving M365 Tenant Phone Numbers

You can reserve a phone number from the DID Range to assign to a specific user. When the phone number is reserved, it is not allocated in the automatic assignment.

➤ **To configure a reserved number range, do the following:**

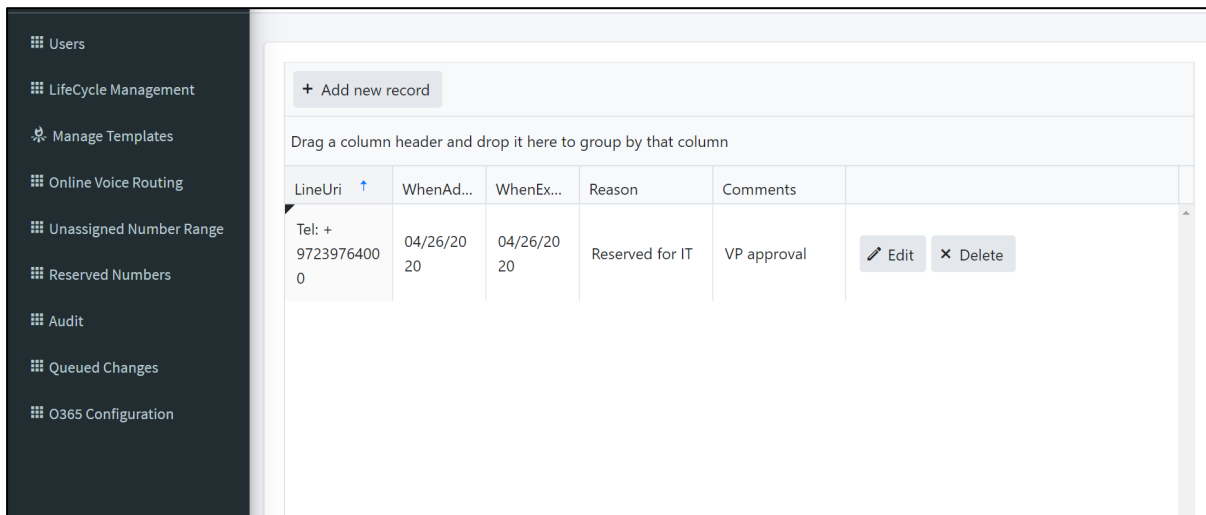
1. Click the **Reserved Numbers** tab.

Figure 7-32: Reserved Numbers



2. Click **+ Add new record** to add a new record.
3. Add the required fields and click **Update** to add the new record.

Figure 7-33: Reserved Number



7.10 Audit and Roll Back Historical Changes

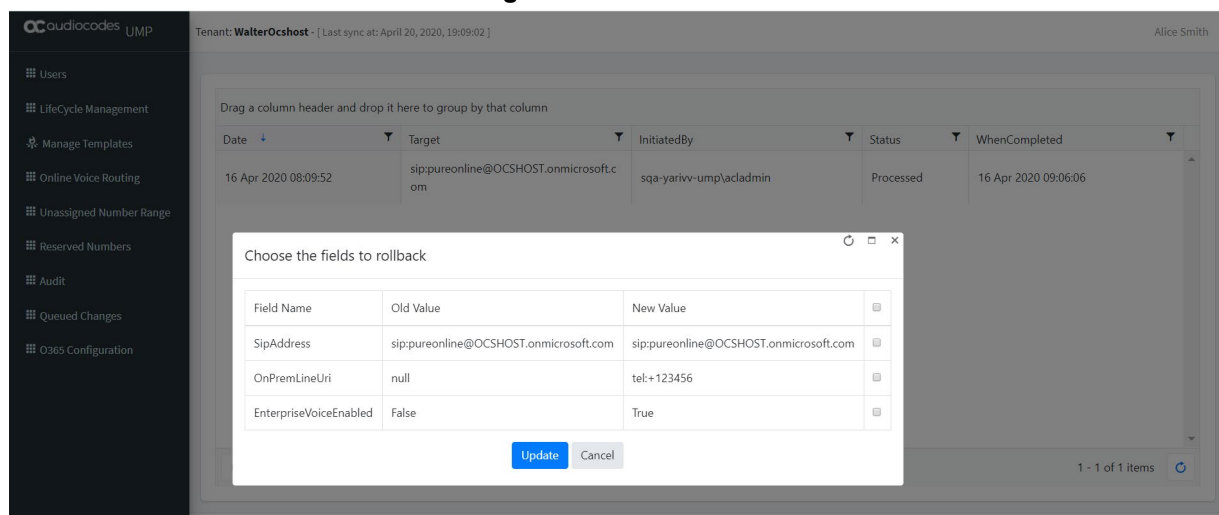
UMP SP includes tracking for changes made by administrators. Under **Audit**, all changes performed are shown and can be reverted by right-clicking a line. If multiple changes were performed in one action, a list is shown with the changes, where the appropriate change can be selected. Select the entry for the change that you wish to rollback and click **Update** to roll back to the previous value.


➤ **To view audit history and perform rollback, do the following:**

1. Click the **Audit** tab; the Audit History is displayed.

2. Right-click an entry, and then click  to undo the policy update for the selected user.

Figure 7-34: Rollback



3. Choose the specific fields that you want to rollback and then click .

7.11 Queued Changes

You can view the queue for all actions including those that have been executed and those in waiting.

➤ **To view queued changes, do the following:**

1. Select the **Queued Changes** tab; a list of updates is displayed.

Figure 7-35: Queued Changes

Id	SipAddress	Cmd ...	Queued Change	Execu...	Execution...	When Created	When Updated
1130	sipa-cbeUser2@audio-codes.be	Office 365	Set-CsUser -Identity 'sipa-cbeUser2@audio-codes.be' -EnterpriseVoiceEnabled \$true;	Ok	-	01 May 2020 19:35:36	01 May 2020 10:36:54
1129	sip:ErezG@audio-codes.be	Office 365	Set-CsUser -Identity 'sip:ErezG@audio-codes.be' -EnterpriseVoiceEnabled \$true;	Ok	-	01 May 2020 19:35:36	01 May 2020 10:36:54
1128	sip:SBC@audiocodes-be.customers.audiocodes.be	Office 365	Set-CsUser -Identity 'sip:SBC@audiocodes-be.customers.audiocodes.be' -EnterpriseVoiceEnabled \$true;	Ok	-	01 May 2020 19:35:36	01 May 2020 10:36:54
1127	sip:davide@audio-codes.be	Office 365	Set-CsUser -Identity 'sip:davide@audio-codes.be' -EnterpriseVoiceEnabled \$true;	Ok	-	01 May 2020 19:35:36	01 May 2020 10:36:54
1126	sip:MarinaR@audio-codes.be	Office 365	Set-CsUser -Identity 'sip:MarinaR@audio-codes.be' -EnterpriseVoiceEnabled \$true;	Ok	-	01 May 2020 19:35:36	01 May 2020 10:36:54

2. Hover over a specific column to view a callout of the text in the selection (this is useful when text is too detailed to be easily read in the initial view) as is shown in the example screen below. You can also drag-and-drop to group by a specific column.

Figure 7-36: Queued Changes Entry Tooltip

Id	SipAddress	Cmd ...	Queued Change	Execu...	Execution...	When Created	When Updated
1130	sipa-cbeUser2@audio-codes.be	Office 365	Set-CsUser -Identity 'sipa-cbeUser2@audio-codes.be' -EnterpriseVoiceEnabled \$true;			01 May 2020 19:35:36	01 May 2020 10:36:54
1129	sip:ErezG@audio-codes.be	Office 365	Set-CsUser -Identity 'sip:ErezG@audio-codes.be' -EnterpriseVoiceEnabled \$true;	Ok	-	01 May 2020 19:35:36	01 May 2020 10:36:54

- Use the table below as a guide to the actions available in this screen.

Figure 7-37: Queued Actions

Action	Description
Show all	Show all actions, including both executed and non-executed.
Show executed	Show all executed actions.
Show new	Show the latest actions.
Process all	Process all actions.
Delete selected	Delete selected actions.
Delete all	Delete all actions.

7.12 Office 365 Setting

You can update Microsoft 365 connection credentials.

- **To update Microsoft 365 connection credentials, do the following:**

- Click the **M365 Configuration** tab.

Figure 7-38: M365 Configuration

The screenshot shows the 'Office 365 Settings' configuration page. The left sidebar contains a navigation menu with items like Users, LifeCycle Management, Manage Templates, Online Voice Routing, Unassigned Number Range, Reserved Numbers, Audit, Queued Changes, and O365 Configuration. The main content area displays the following fields:

- User Name:** admin@ocshost.emea.microsoftonline.com
- Password:** (empty field)
- Confirm password:** (empty field)
- Lync Online Host:** sipfed.online.lync.com

- Configure the Office 365 credentials using the table below as reference.

Table 7-1: Office 365 Settings

Parameter	Description
User Name	Microsoft 365 UC Admin User (User with Teams Admin Credential). If you wish to manage SharePoint, then this administrator must also have SharePoint Admin credentials.
Password	Microsoft 365 UC Admin Password.
Lync Online Host	Auto-filled

8 Multitier Admin Access

Providers can create an additional layer of support and grant access to the provider portal to specific channels including multiple customers. When the Channel Admin users sign-in to the Public Portal URL (Azure AD), they receive the list of customers that the provider has granted them access to manage.

Figure 8-1: Access to the Portal

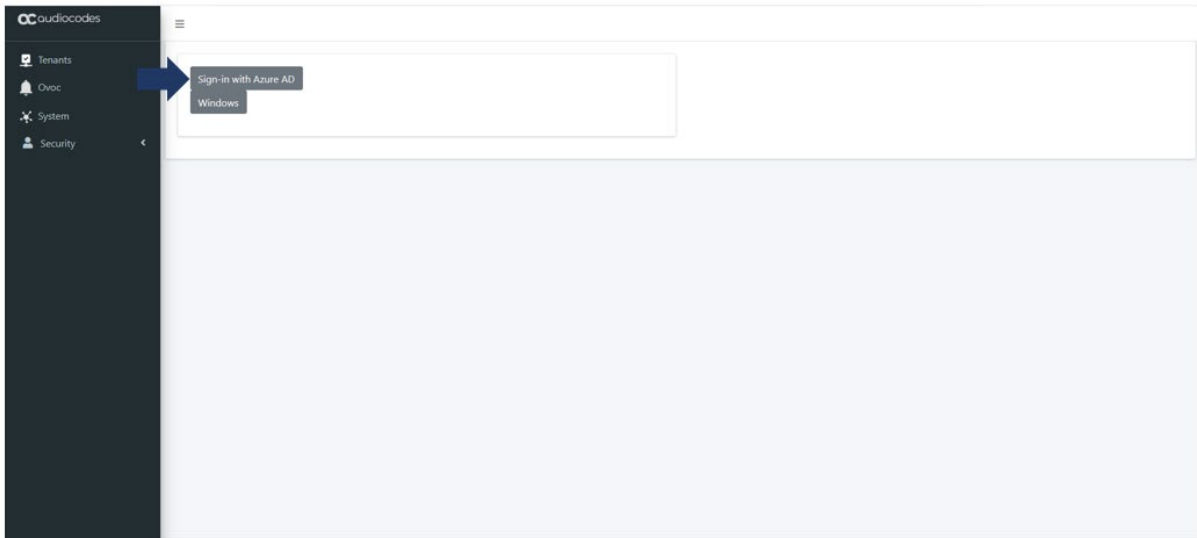


Figure 8-2: SSO with Azure Active Directory

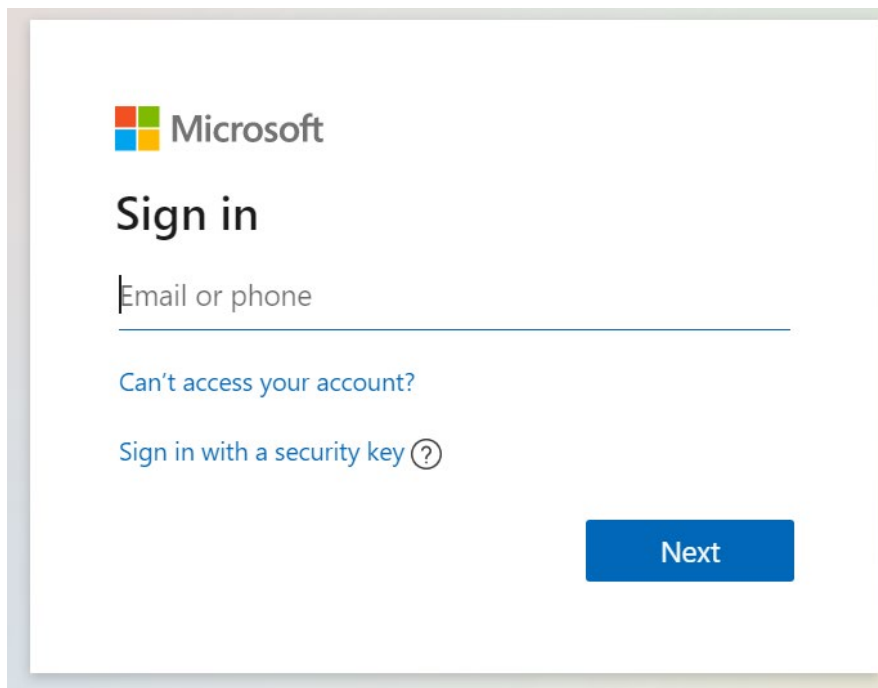


Figure 8-3: SSO with Azure Active Directory

List of customers for AudioCodes EMEA Channel

[enterpricertc](#)

[TalkMail](#)

[easylync](#)

[finebak](#)

[Logout](#)

Figure 8-4: UMP 365 Customer Portal

Tenant: **enterpricertc** - [Last sync at: September 24, 2020, 17:00:56] Alice Smith

User Type	Full Name	SIP Address	Line URI	Template	Department	Online Voice Ro...	Usage Locati...	enterprise vo...
TeamsOnly	qa	sipqa@ente...				Unrestricted	IL	No
TeamsOnly	Bogota	sipBogota@...	tel+972397...	Sales		Unrestricted	IL	Yes
TeamsOnly	Rio De Janeiro	sipRio@ACL...	tel+972397...	Executive		Unrestricted	IL	Yes
TeamsOnly	test	sipstest@AC...				Unrestricted	IL	No
TeamsOnly	David Edri	sipdavid@...	tel+972397...	ALL		Unrestricted	IL	No
TeamsOnly	Gaß Holdenbreger	sipadmin@...				Unrestricted	IL	No
TeamsOnly	admin demo	sipadmin@...				Unrestricted	IL	No

9 Browser setting - IETF Same Site Cookie Attribute

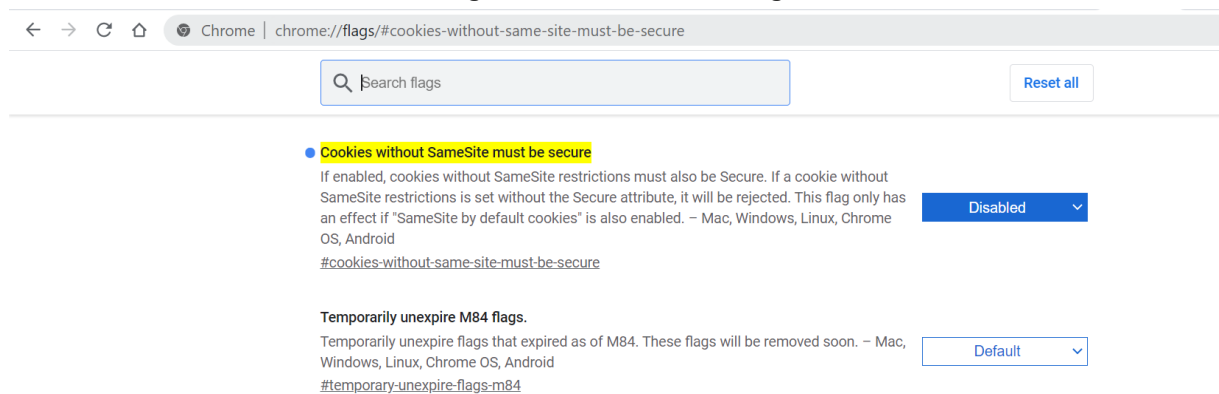
Due to the introduction of the IETF SameSite cookie attribute, default browsers addressing the UMP web pages using the http protocol requires the disabling of this new default behavior in the browser to prevent an access denied message. These problems do not occur when **https** is used and properly configured.

The following describes the steps required to prevent this occurrence of this issue for each respective browser:

■ Chrome:

1. Go to: "chrome://flags/#cookies-without-same-site-must-be-secure"
2. Disable option "Cookies without SameSite must be secure"
3. Restart Chrome.

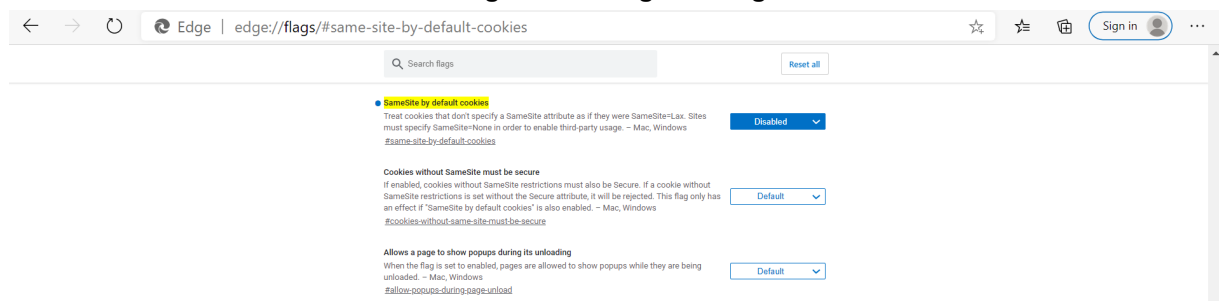
Figure 9-1: Chrome Setting



■ Edge:

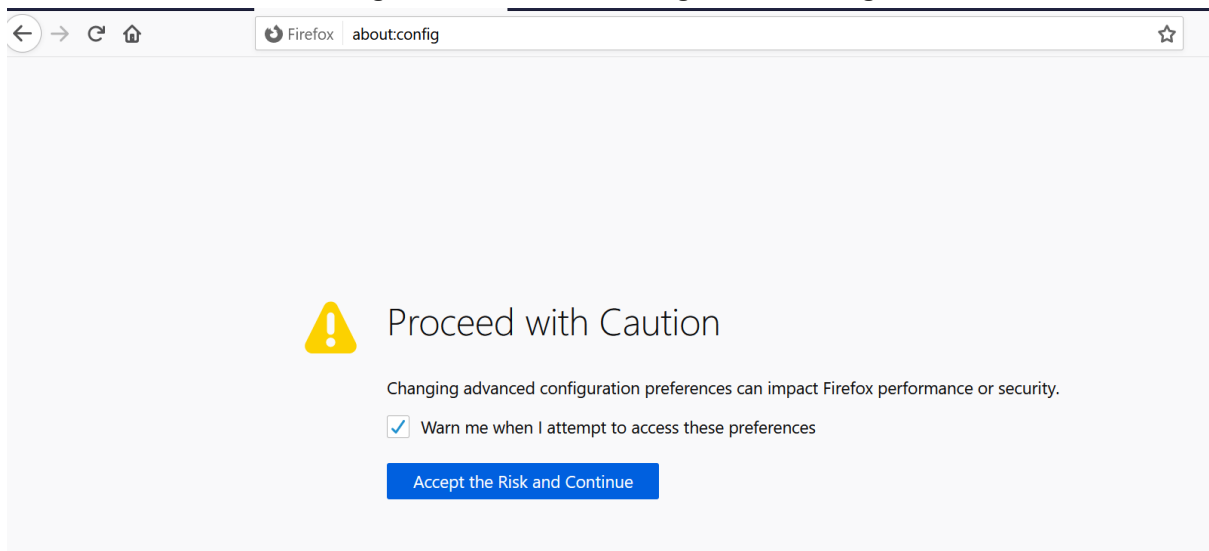
1. Go to: "edge://flags/#same-site-by-default-cookies"
2. Disable option "SameSite by default cookies"
3. Restart Edge.

Figure 9-2: Edge Setting



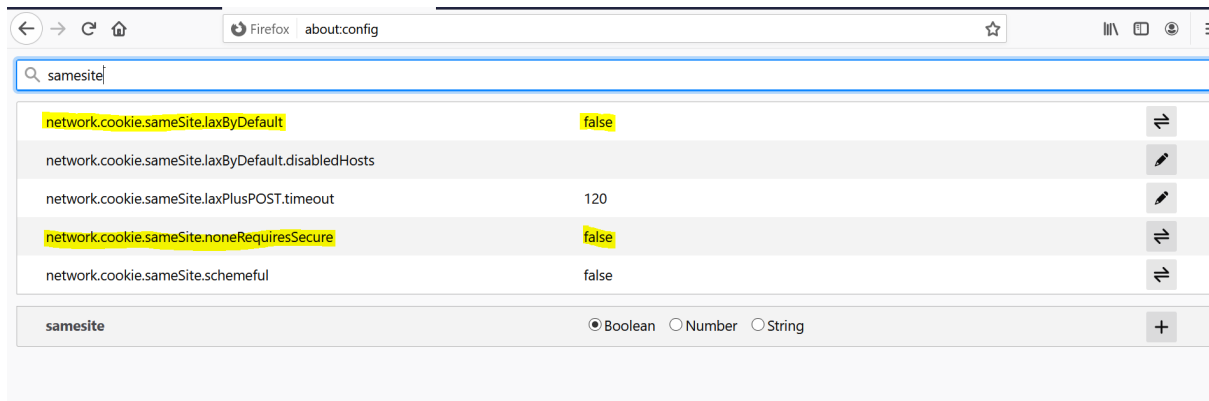
- **Firefox:** (works for version 75 and above):
 1. In the URL bar, navigate to about:config. (accept the warning prompt, if shown).

Figure 9-3: FireFOX Setting - about:config



2. Type SameSite into the “Search Preference Name” bar.
3. Set `network.cookie.sameSite.laxByDefault` to false using the toggle icon.
4. Set `network.cookie.sameSite.noneRequiresSecure` to false using the toggle icon.
5. Restart Firefox.

Figure 9-4: FireFOX Setting



Note: 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.

10 Backup and Restore Customer Tenant

This section describes how to Backup/Restore the customer tenant information.

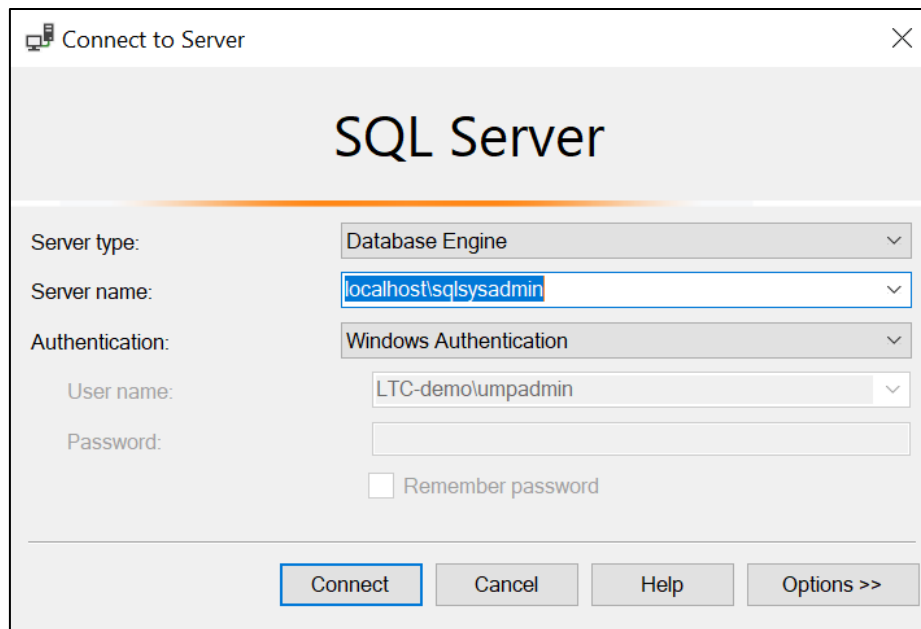
10.1 Backup the Customer Tenant Database

This section describes how to back up the customer tenant database.

➤ **To back up the customer tenant database, do the following:**

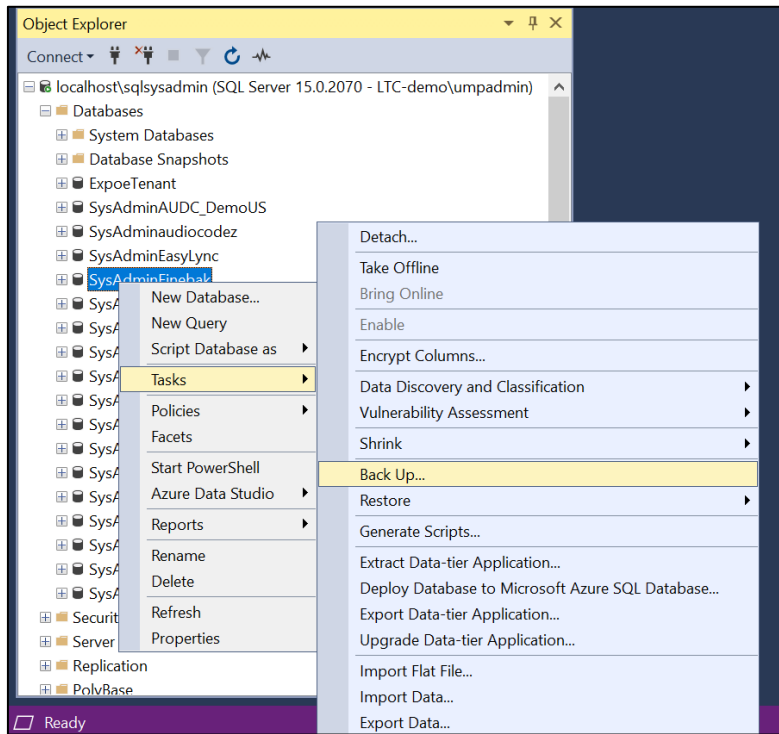
1. Start the Microsoft SQL Server Management Studio.

Figure 10-1: SQL Server



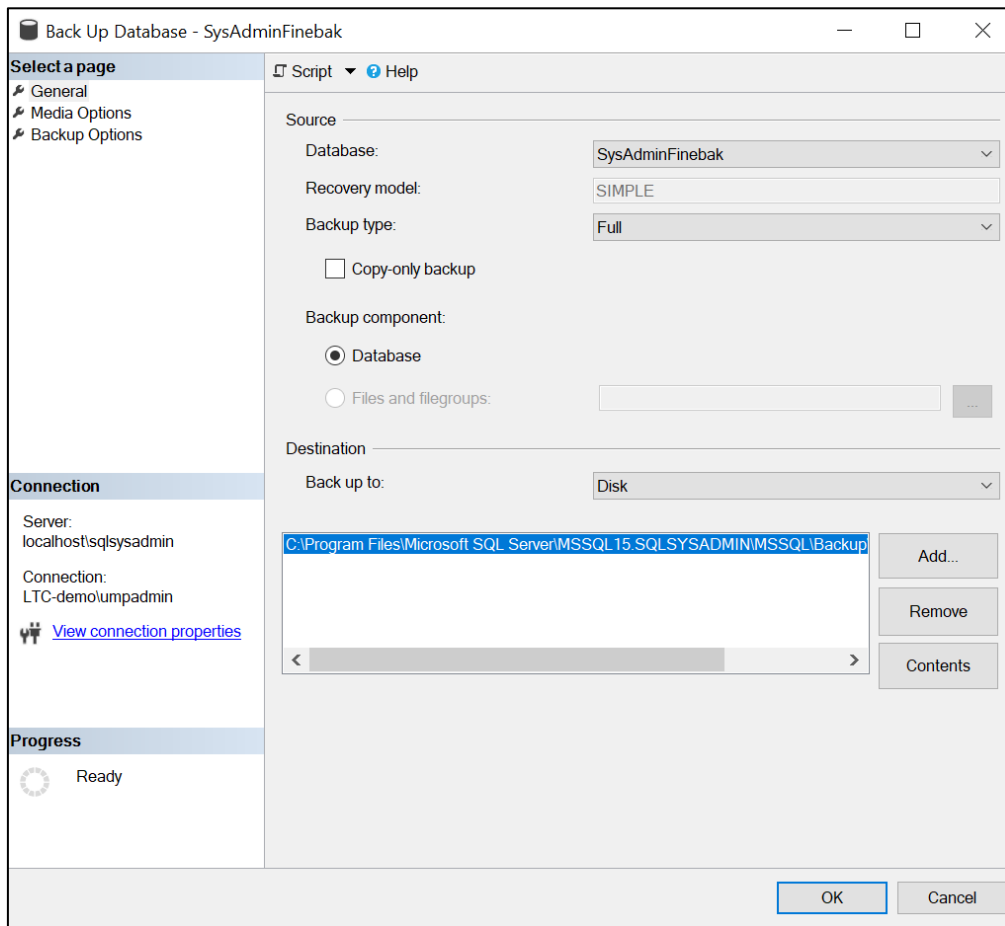
2. Apply **Connect** to the sysadmin database (localhost\sqlsysadmin).
3. Select the Customer Tenant that you would like to back up.
4. Right-click and select **Tasks/ Back Up**.

Figure 10-2: Run Back Up Task



5. Right-click and select the Destination.

Figure 10-3: Select the Database Destination

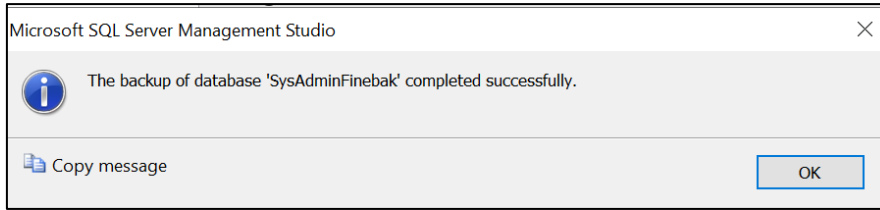




Note: Don't save the backup on the same disk as the SQL database.

6. Select the 'Destination', and then click **OK**.

Figure 10-4: Database Backup Completed Successfully



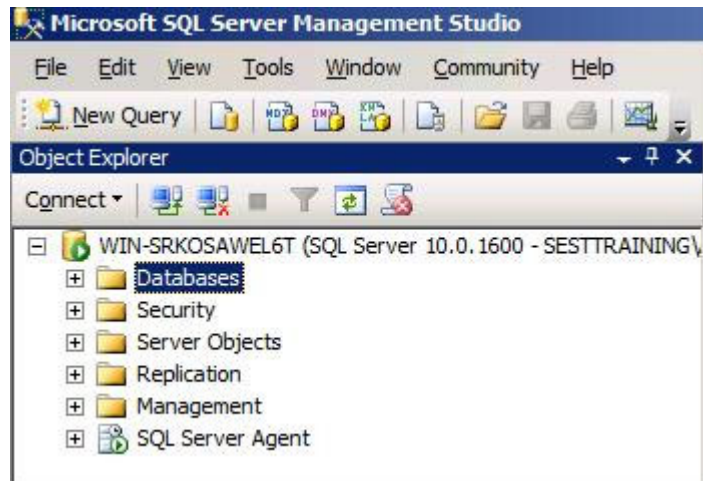
10.2 Restore the Customer Tenant Database

This section describes how to restore the customer tenant database.

➤ **To restore the database, do the following:**

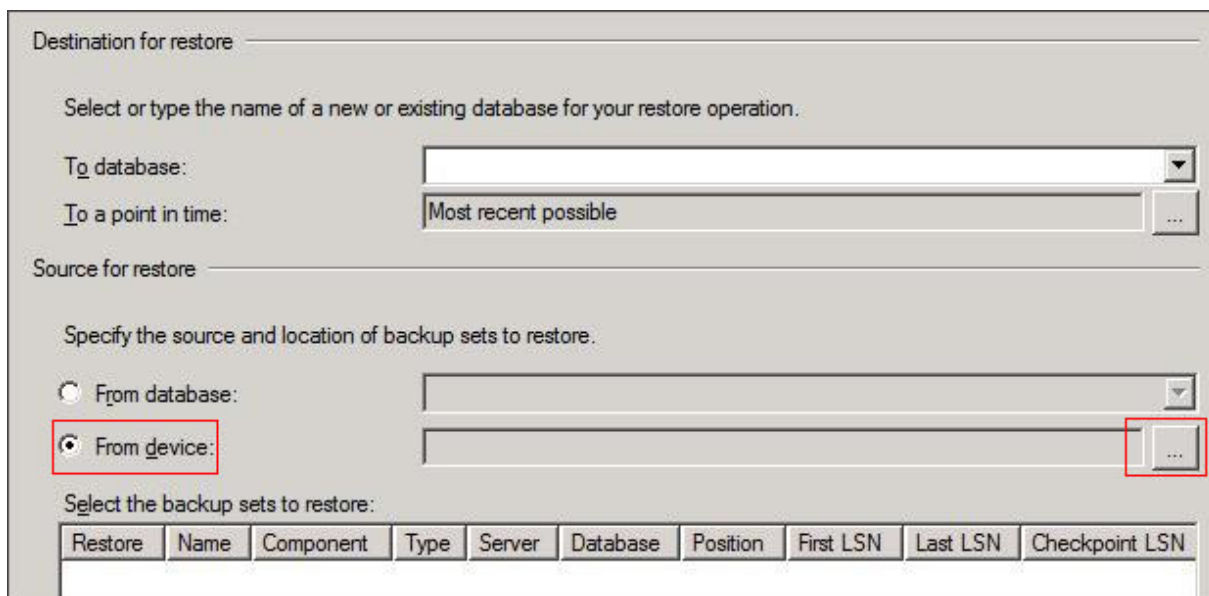
1. Open Microsoft SQL Server Management Studio and navigate to **Databases**:

Figure 10-5: Select the Database resource



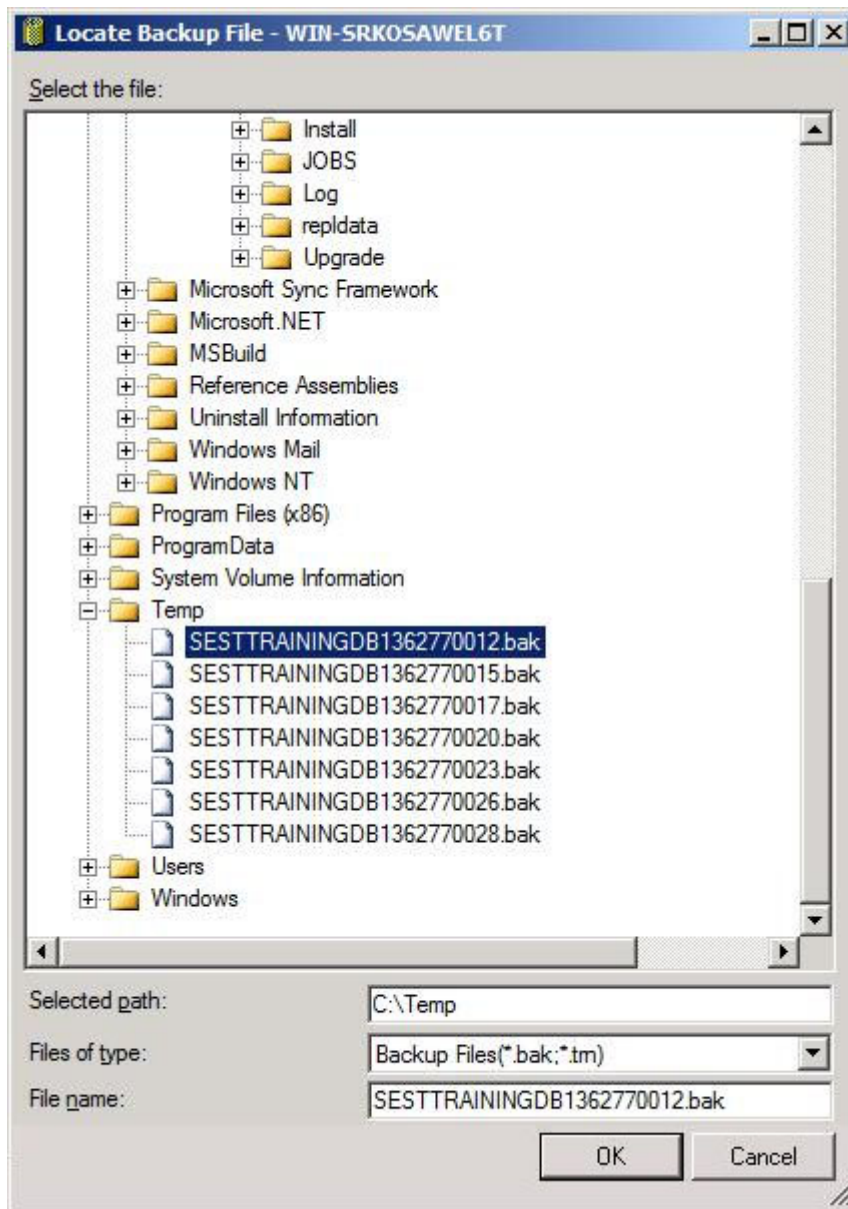
2. Right-click **Databases** and click **Restore Database**. In the screen section 'Source for restore', select **From Device** and then click the browse button:

Figure 10-6: Select the Device



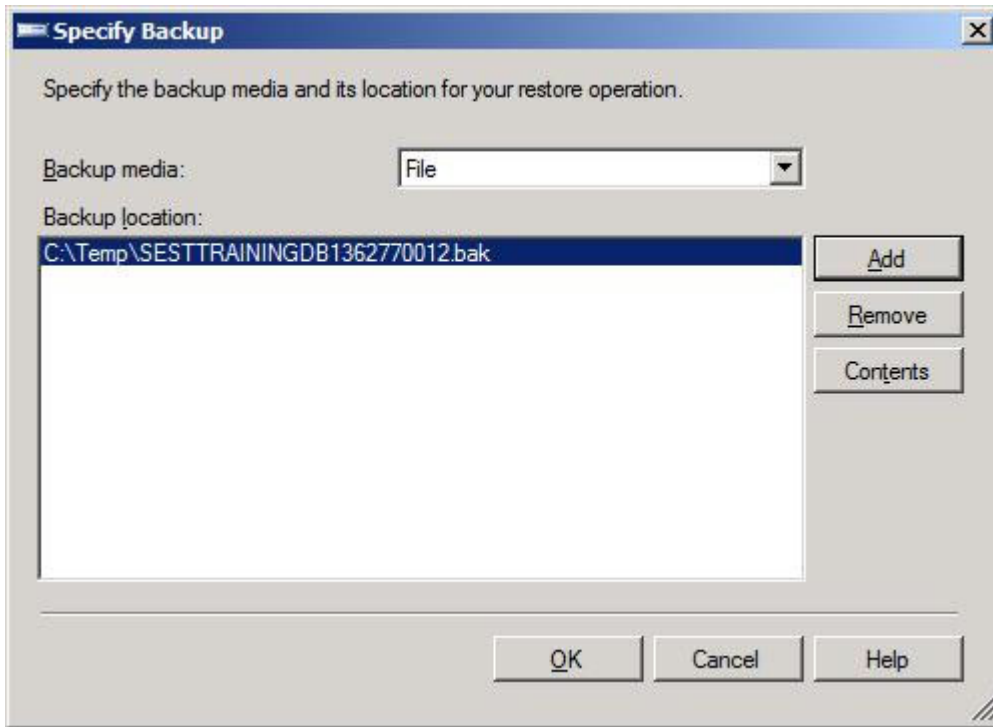
3. Click **Add** in the Specify Backup window. Browse to the location of your recently restored files. Choose the full backup file which should be the first backup file in the list:

Figure 10-7: Select the Backup File



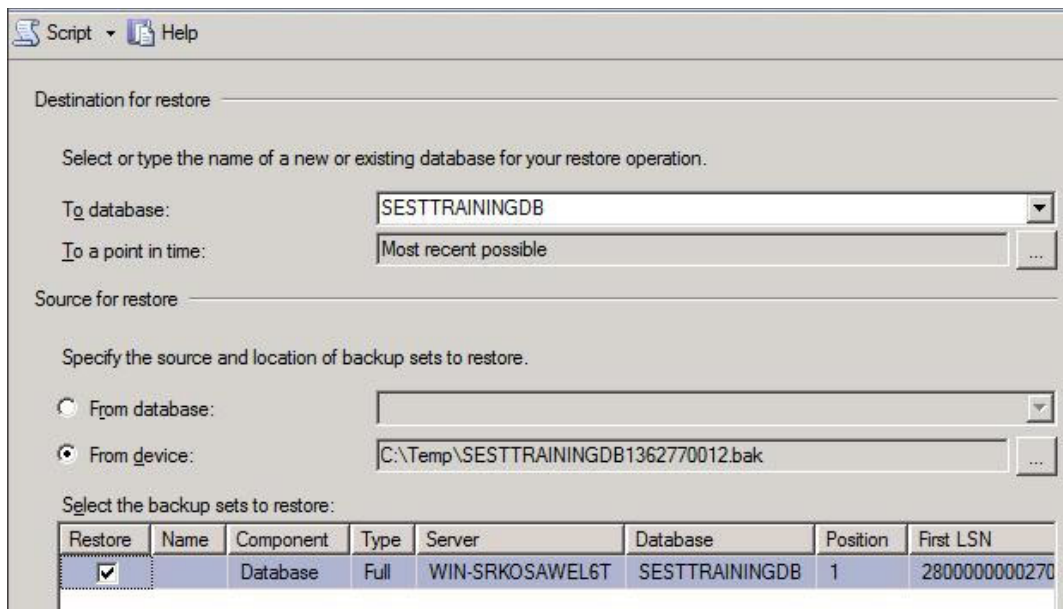
4. Click **OK**; the Specify Backup window is displayed.

Figure 10-8: Confirm the Backup File



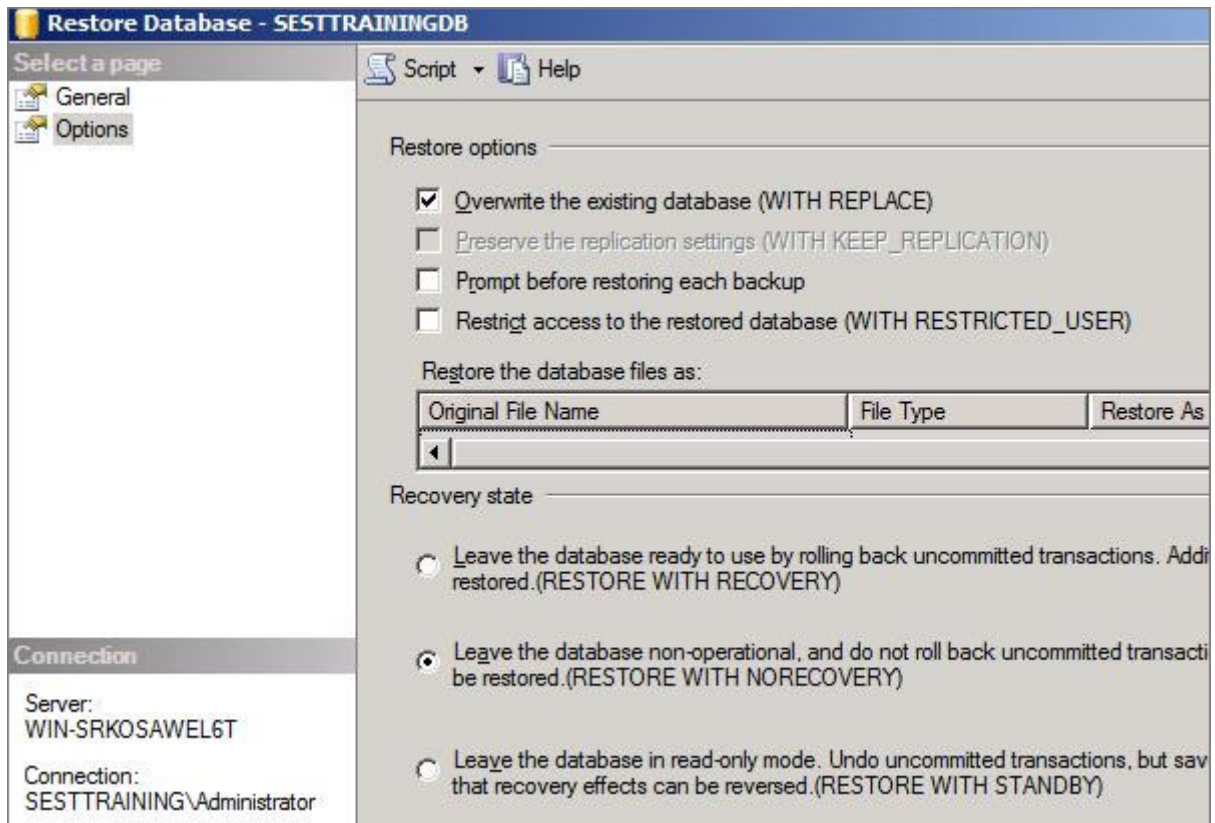
5. Click **OK**.
6. In the screen section 'Destination for restore', select the database to which you want to restore, and then in the 'Select the backup sets to restore' section of the screen, select the backup file you selected above.

Figure 10-9: Confirm the Backup File



7. In the left pane, click **Options**, and then select the following:
 - a. In the Restore options' section, select **Overwrite the existing database (WITH REPLACE)** and leave the other options unselected.
 - b. In the Recovery state' section, select Leave the database non-operational, and do not roll back uncommitted transactions. Additional transaction logs can be restored. (RESTORE WITH NORECOVERY):

Figure 10-10: Select the Backup File



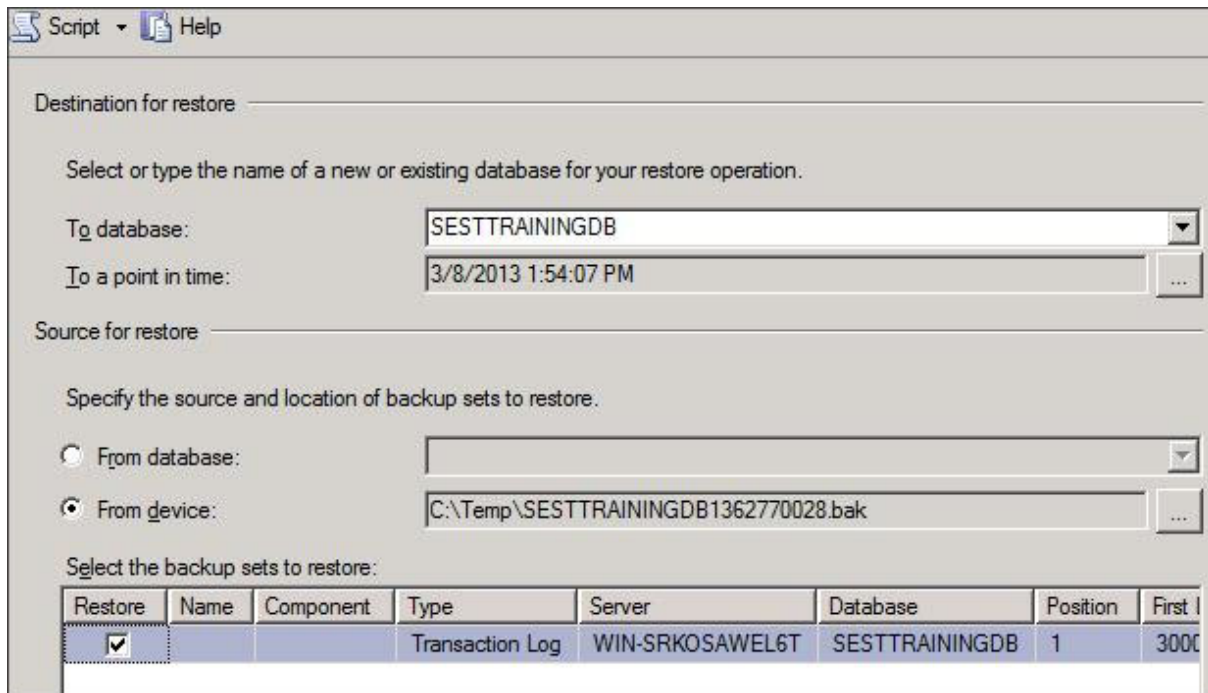
8. Click **OK** to perform the restore.
9. Complete these steps for each incremental backup file, including the .tm file, until you reach the incremental file containing the point-in-time file to which you want to restore.
10. A "Restoring" message is displayed; you can now proceed with the next section 'Restoring to a Point-in-Time'.

10.2.1 Restore to a Point-in-Time

Use the following steps to restore the last incremental file containing the point-in-time:

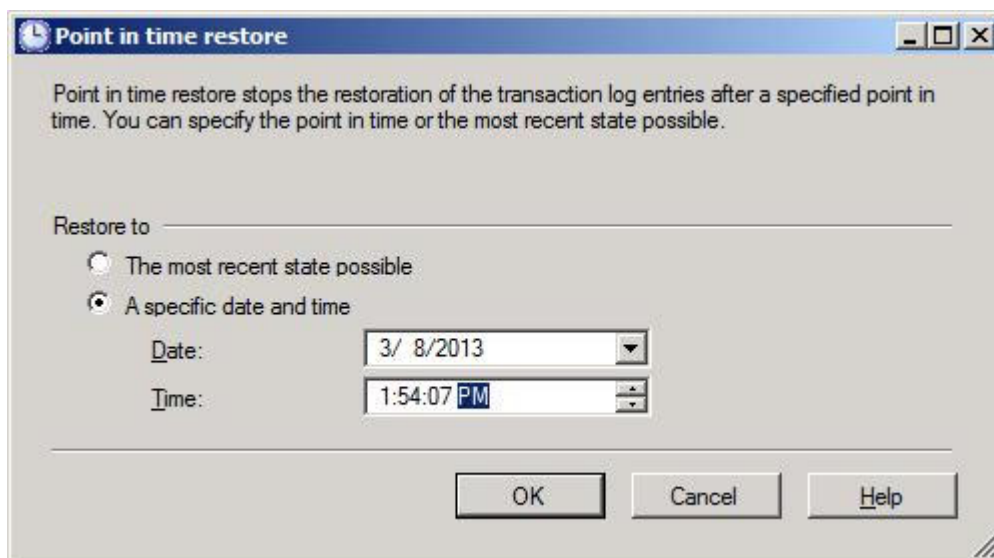
1. In Microsoft SQL Server Management Studio, right-click **Databases**, and click **Restore Database**.
2. In the Source for restore' section, select **From Device** and then click the browse button.
3. Click **Add** in the Specify Backup window. Browse to the location of your recently restored flat files, select the **incremental backup file containing the point-in-time to restore** to, and click **OK**.
4. Click **OK** in the Specify Backup window. In the Select the backup sets to restore' section, check the backup file you added in the previous step.
5. In the 'Destination for restore section', select the **database** to which to restore:

Figure 10-11: Restore to point of time – Step 1



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:

Figure 10-12: Restore to point of time – Step 2



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):

Figure 10-13: Restore to point of time – Step 3

Restore Database - SESTRAININGDB

Select a page

General
Options

Script Help

Restore options

Overwrite the existing database (WITH REPLACE)

Preserve the replication settings (WITH KEEP_REPLICATION)

Prompt before restoring each backup

Restrict access to the restored database (WITH RESTRICTED_USER)

Restore the database files as:

Original File Name	File Type	Restore As

Recovery state

Leave the database ready to use by rolling back uncommitted transactions. Additional transaction logs restored. (RESTORE WITH RECOVERY)

Leave the database non-operational, and do not roll back uncommitted transactions. Additional transactions to 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:
SESTRAINING\Administrator

10. Click **OK** to perform the restore. the restored database is displayed with only those changes up to the specified point-in-time.

This page is intentionally left blank.

A UMP SP Installation on Azure

This version of AudioCodes' User Management Pack 365 SP can be deployed in the environments described below:

- Azure Environment
- Data Center Environment

This appendix describe the Azure Deployment Installation Guide.

A.1 Installing the Prerequisites

To be able 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.

To be able to install UMP-SP, the Frontend server needs to be prepared by installing the following prerequisite components:

- Operating System required roles and features (see Section A.1.1)
- SQL Server Express (see Section 2A.1.2)
- SQL Server Management Studio (see Section A.1.3)
- NetSQLAzMan (see Section A.1.4)
- dotnet 4.8 (see Section A.1.5)
- SkypeOnlinePowershell (see Section A.1.6)
- SharepointOnline Powershell (see Section A.1.7)
- ASP.NET core 3.1 runtime (see Section A.1.8)
- ASP.NET core 3.1 Windows Hosting Bundle installer (see Section A.1.9)
- azureAD PowerShell with PowerShell commands (see Section A.1.10)

All the above prerequisites are available on the installation ISO in the Prerequisites folder and are numbered 1-10 for the processing order.

- On all backend SQL servers, install the following prerequisite components:
 - SQLSYSADMIN SQL server instance
 - SQL management studio (optional as it can be managed from the first server)



Note: The SQL server version that is provided on the ISO is SQL Express and should only be used during lab deployments. In production, SQL Server Standard Edition is required on all servers hosting customer databases.

A.1.1 Operating System Roles and Features

This section describes how to configure system roles and features that are included in the installation ISO in 1 - OS Roles and Features.ps1.

➤ **To configure operating system roles and features, do the following:**

1. Enter the following PowerShell cmdlet:

```
Install-WindowsFeature Telnet-Client, Web-Server, Web-Mgmt-Tools,  
Web-Mgmt-Console, Web-WebServer, Web-Common-Http, Web-Default-Doc,  
Web-Static-Content, Web-Performance, Web-Stat-Compression, Web-  
Dyn-Compression, Web-Security, Web-Filtering, Web-Windows-Auth,
```

```
Web-App-Dev, Web-Net-Ext45, Web-Asp-Net45, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Includes, Web-Net-Ext, Web-Asp-Net, rsat -Source "E:\Windows Server 2019"
```

Where E: is the location of the mounted ISO.

2. If after installation, you are prompted to reboot; reboot the server before continuing.

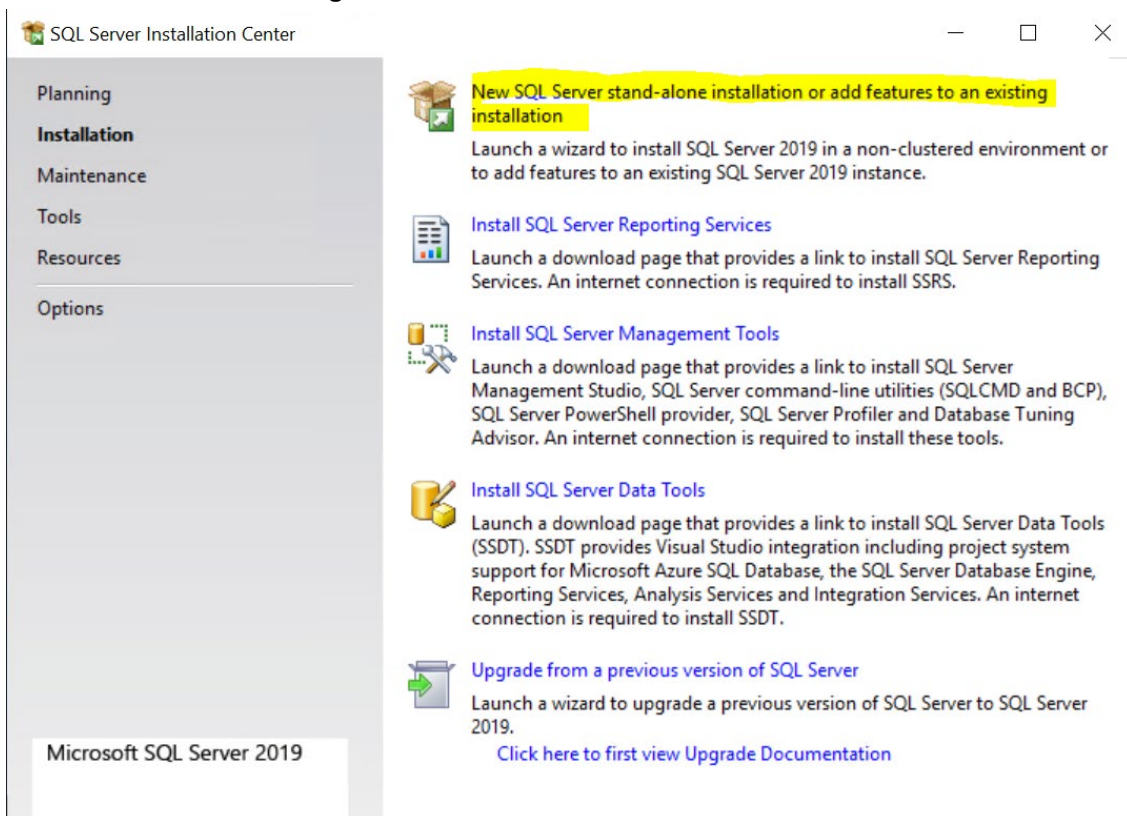
A.1.2 SQL Server Express

This procedure describes how to install SQL Server Express. SQL Server Express (2 - SQLServer2019Media).

➤ **To install SQL Server Express, do the following**

1. Start the installation with "Setup.exe".

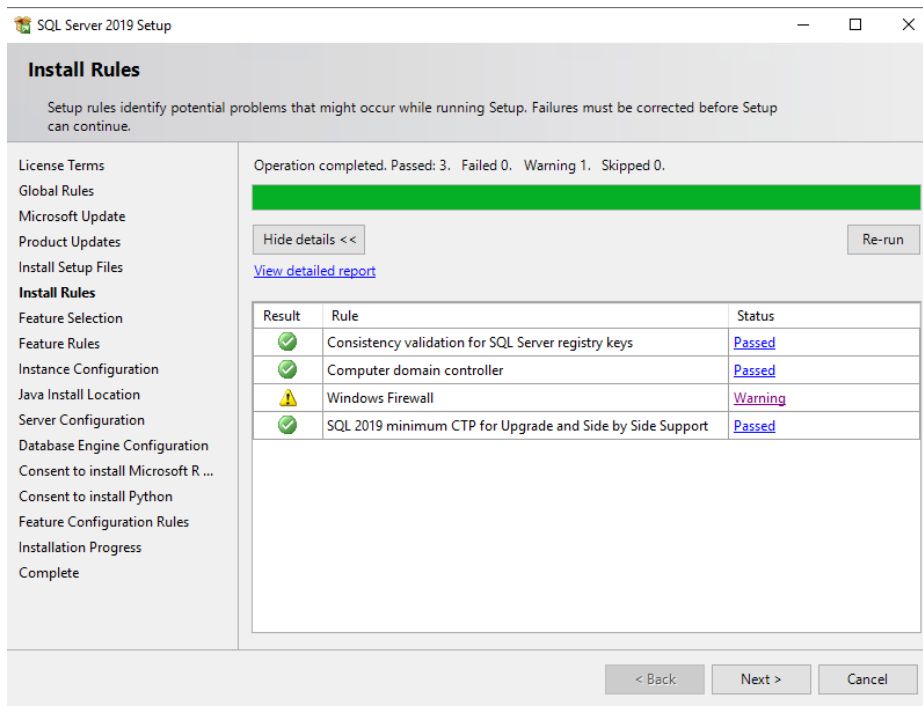
Figure A-1: SQL Server Installation Center



2. Select **New SQL Server stand-alone installation or add features to an existing installation.**
3. Accept the license terms.

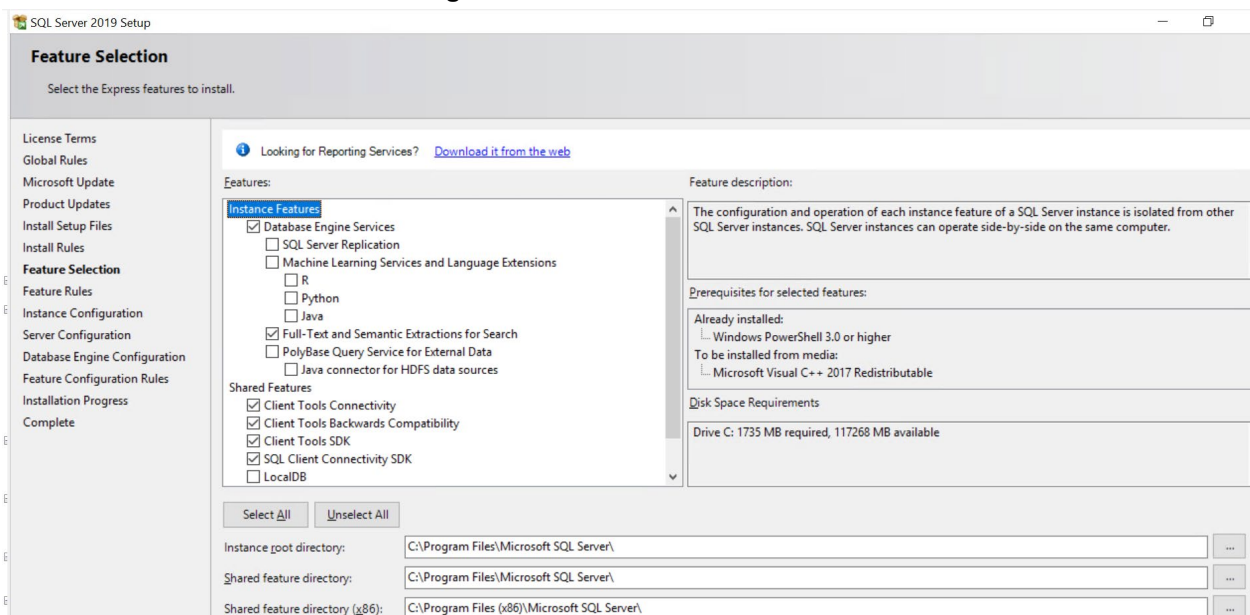
4. Select **Use Microsoft Update to check for updates**. The SQL Install Rules screen is displayed.

Figure A-2: SQL Install Rules



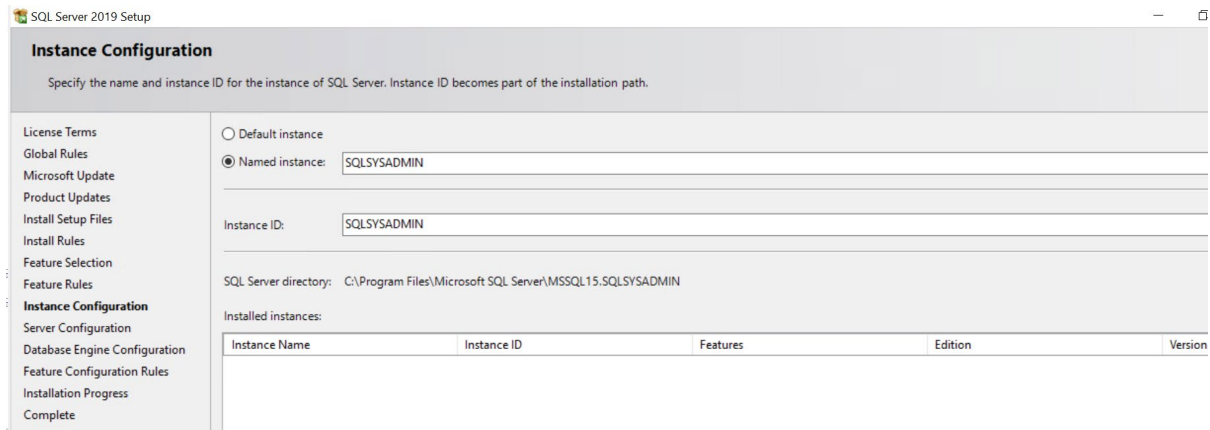
5. Click **Next** to continue. The Feature Selection screen is displayed.

Figure A-3: Feature Selection



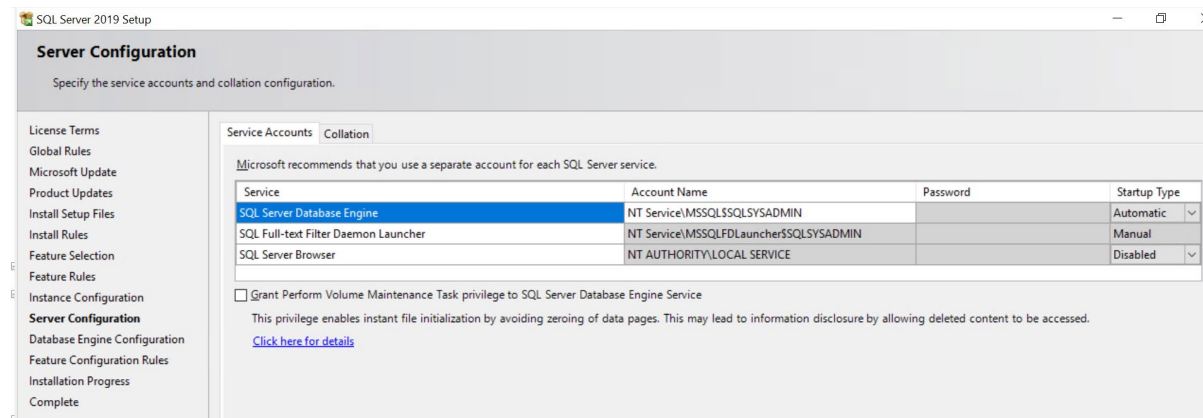
6. Select the features according to the selections in the screen above, and then click **Next**. The Instance Configuration screen is displayed.

Figure A-4: Instance Configuration



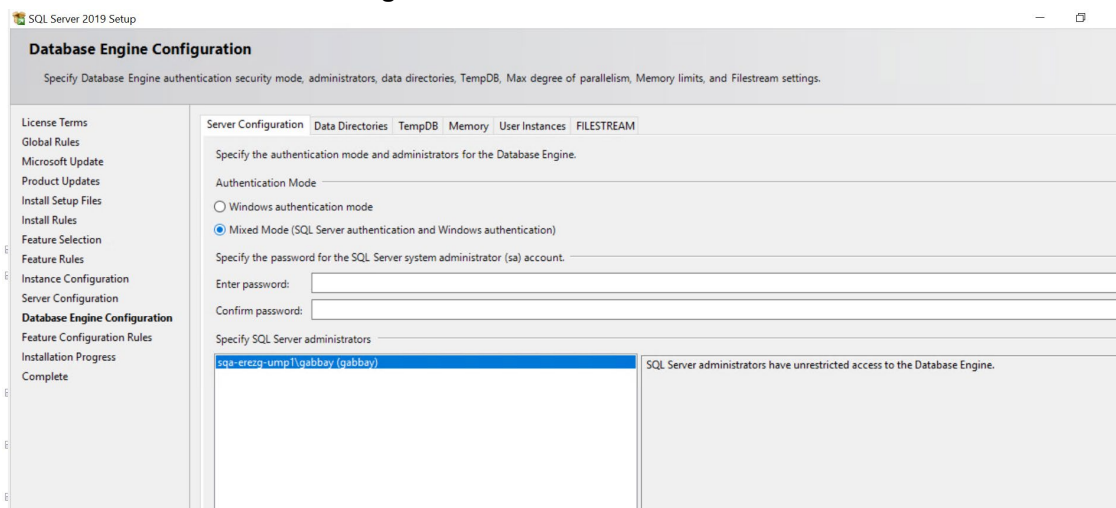
7. Change the “Named instance” to SQLSYSADMIN, and then click **Next**.

Figure A-5: SQL Server Database Engine Configuration



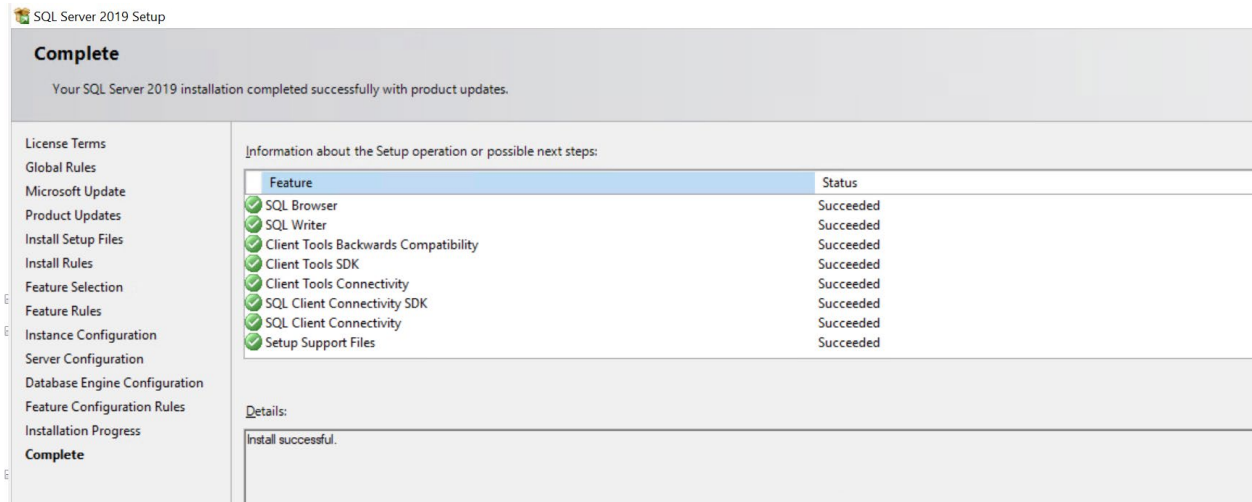
8. In the “Authentication Mode” pane, select **Mixed Mode**. Enter the system admin (sa) password and write it down for future use. AudioCodes default sa password is “R3m0t3Supp0rt”.

Figure A-6: Authentication Mode



At the end of the installation, the following confirmation screen is displayed:

Figure A-7: Complete



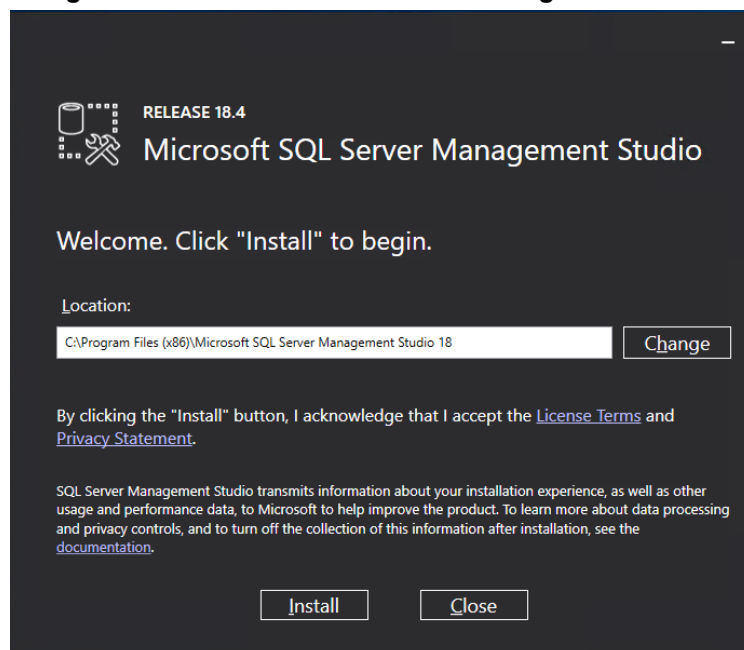
A.1.3 Install SQL Server Management Studio

This section describes how to install SQL Server Management Studio (3 - SSMS-Setup-ENU.exe).

➤ **To install SQL Server Management Studio, do the following:**

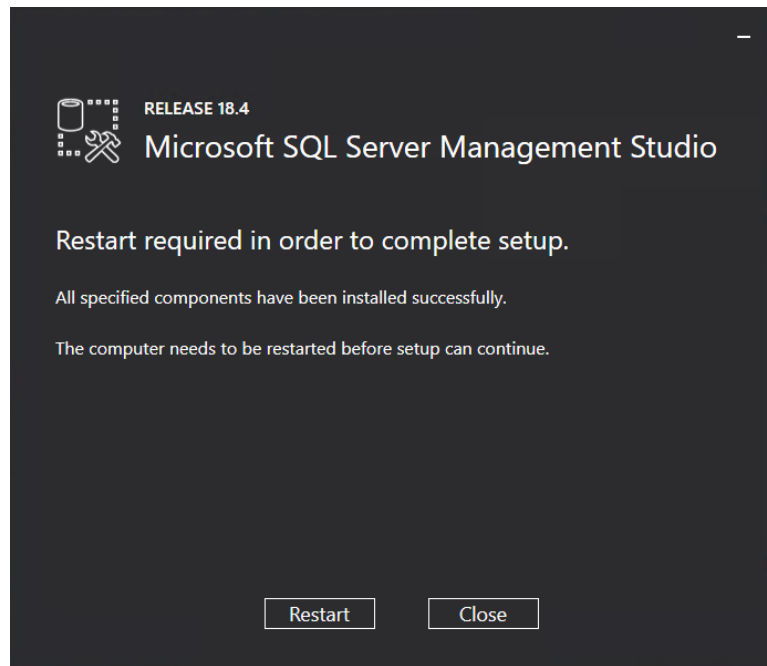
1. Run SSMS-Setup-ENU.exe; the Welcome screen is displayed.

Figure A-8: Microsoft SQL Server Management Studio



2. Click **Install**.

Figure A-9: Restart Management Studio



3. Click **Restart**.

A.1.4 Install ASP.NET SQL Authorization Manager

This procedure describes how to install .NET SQL Authorization manager (4 - NetSqlAzManSetup_x64.msi).

➤ To install ASP.NET SQL Authorization Manager, do the following:

1. Run 4 - NetSqlAzManSetup_x64.msi.

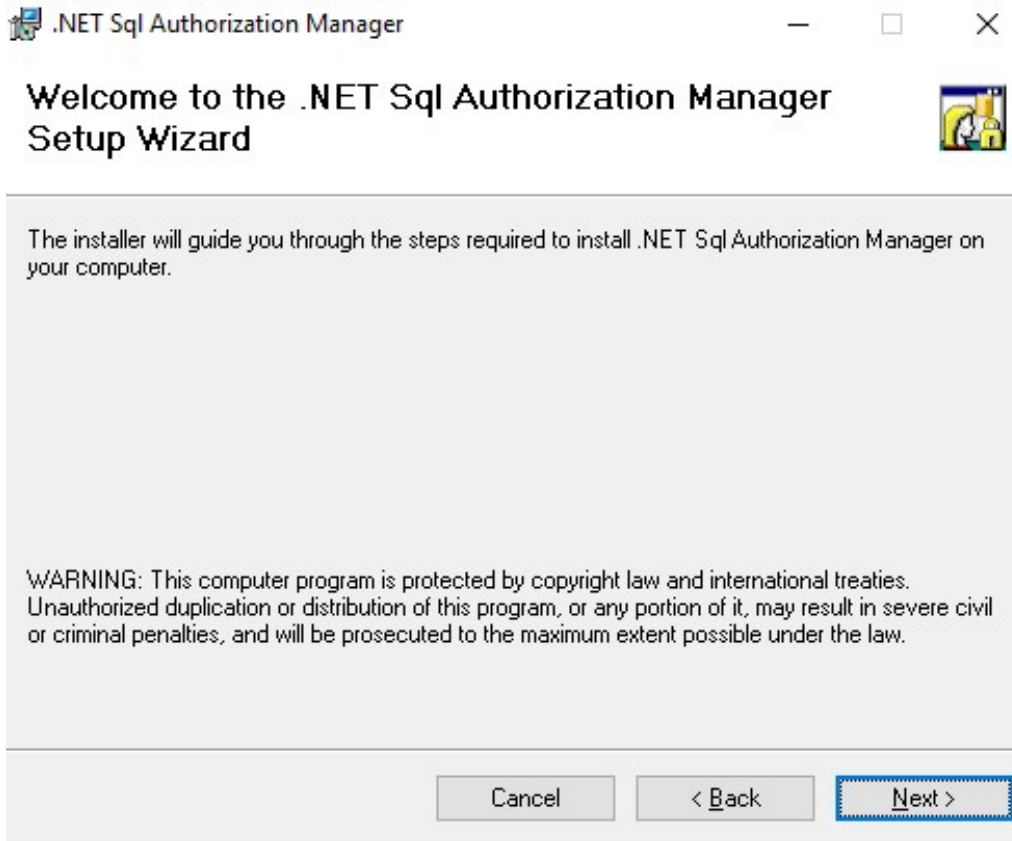
Figure A-10: NetSqlAzMan



The Welcome screen is displayed.

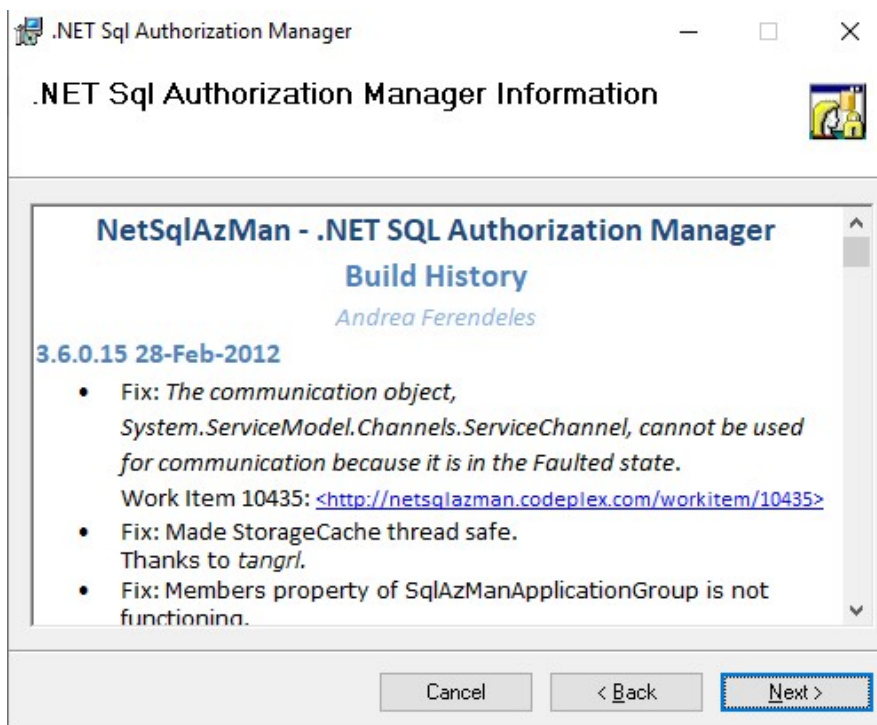
2. Click **Next** to continue.

Figure A-11: Welcome to Setup Wizard

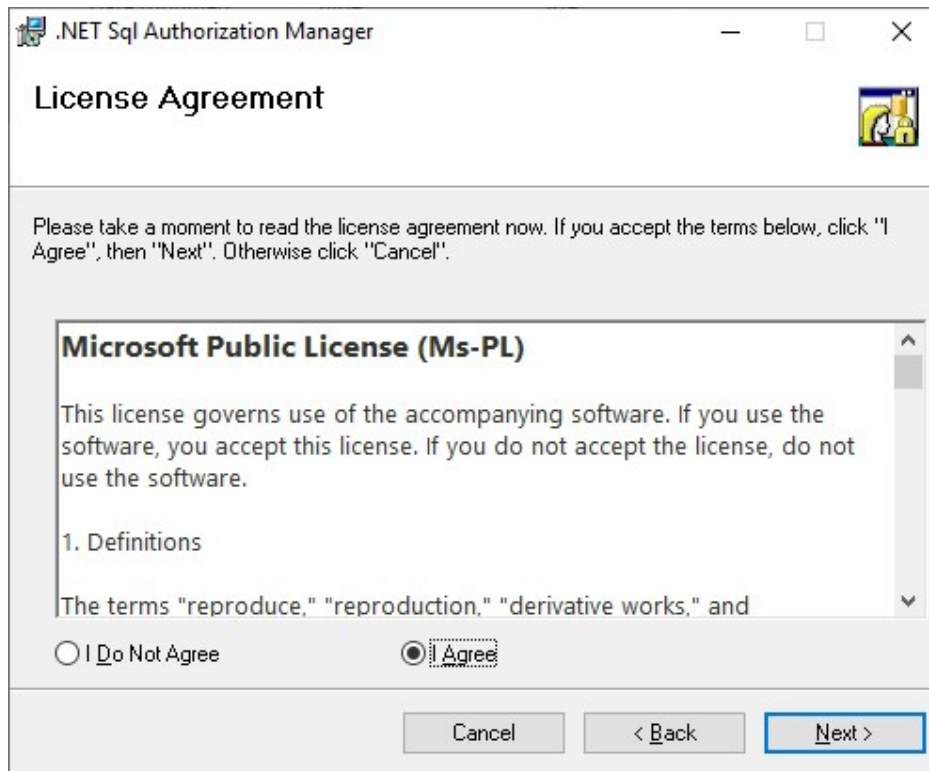


3. Click **Next** to continue. The NET SQL Authorization Manager Information screen is displayed.

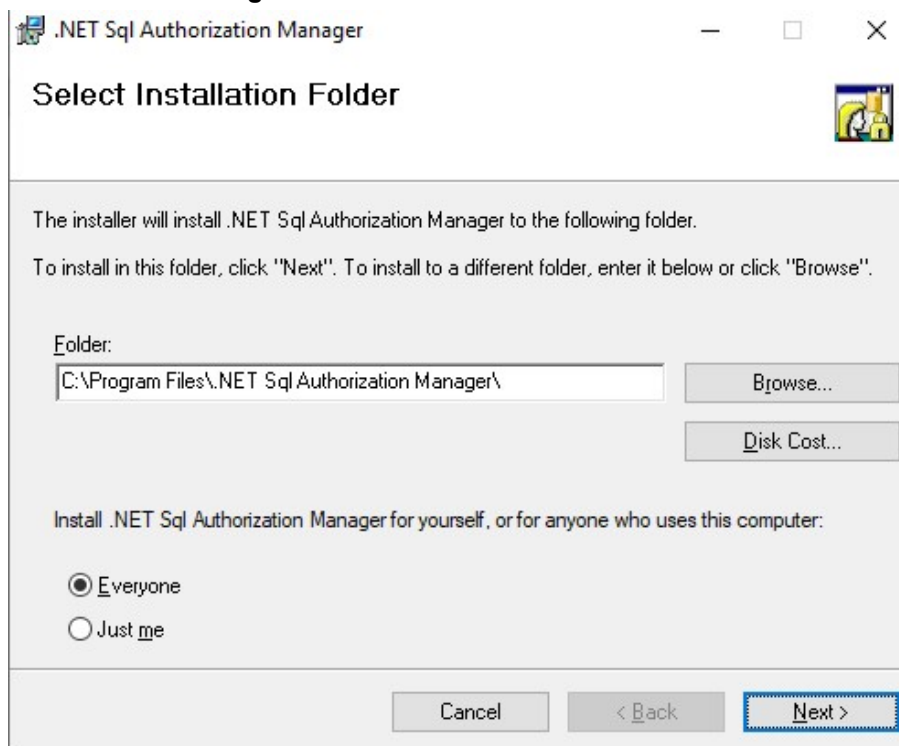
Figure A-12: NET SQL Authorization Manager Information



- Click **Next** to continue. The Microsoft Public License Agreement screen is displayed.

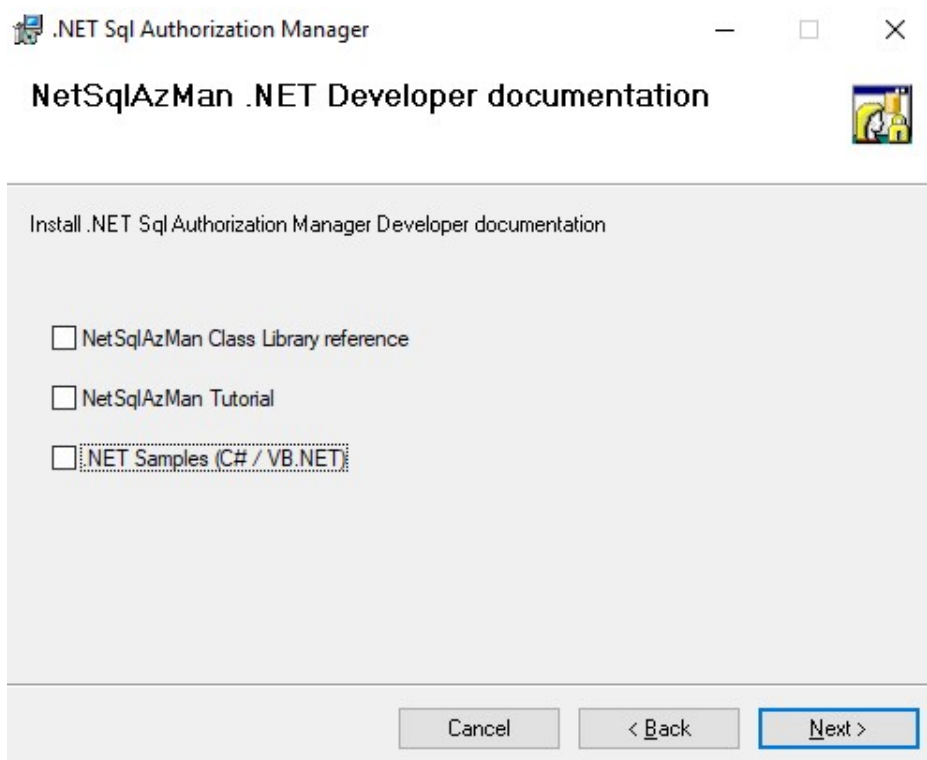
Figure A-13: Microsoft Public License Agreement

- Accept the License terms, and then click **Next** to continue. The Select Installation Folder screen is displayed.

Figure A-14: Select Installation Folder

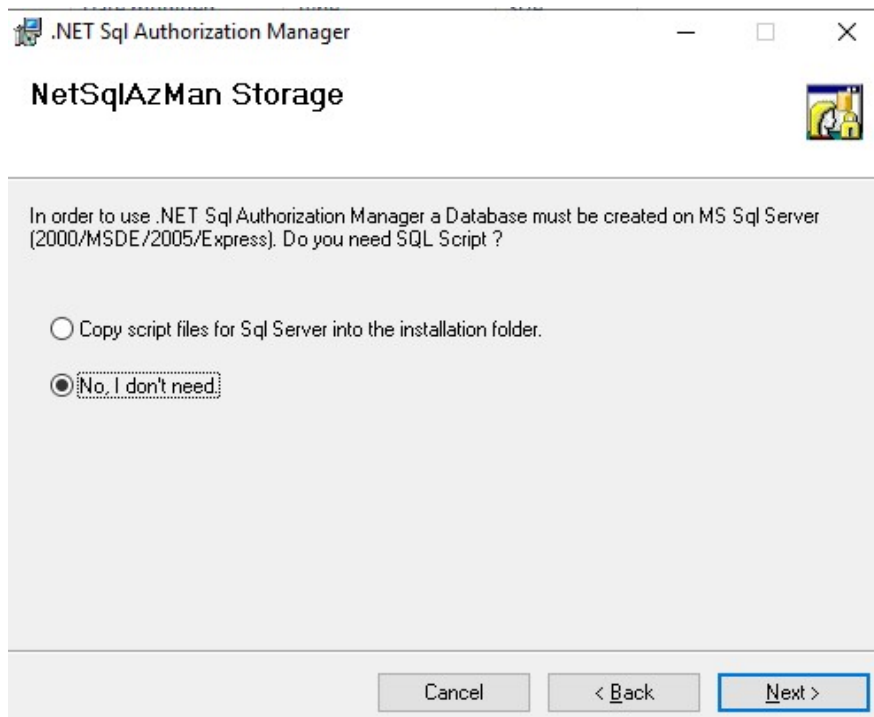
- Click **Next** to continue. The .NET Developer Documentation screen is displayed.

Figure A-15: .NET Developer Documentation



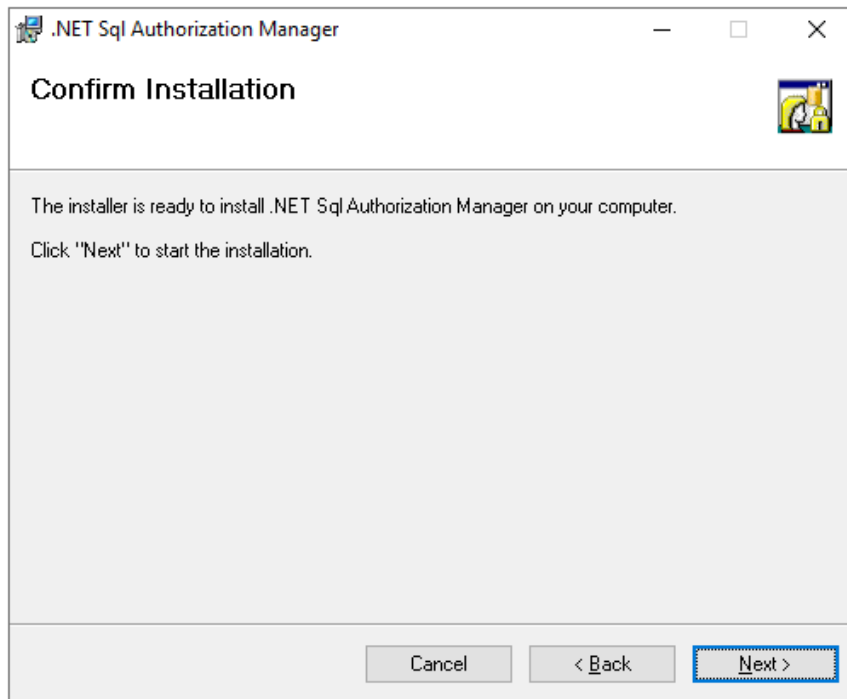
- Select the .NET Developer documentation options, and then click **Next**. The NetSqlAzMan Storage screen is displayed.

Figure A-16: NetSQL Man Storage



8. Select the appropriate option for copying script files if required, and then click **Next**. The Confirm Installation screen is displayed.

Figure A-17: Confirm Installation



9. Click **Next** to start the installation, and then close the wizard when finished.

A.1.5 Install ASP.NET framework 4.8

Install .NET framework 4.8 by running "5 - ndp48-devpack-enu.exe". Restart if required by the installer.

A.1.6 Install SkypeOnline Powershell

Install Skype online PowerShell by running "6 - SkypeOnlinePowerShell.Exe".

A.1.7 Install Sharepoint Online Powershell

Install Sharepoint online PowerShell by running "7 - SharePointOnlineManagementShell_19724-12000_x64_en-us.msi".

A.1.8 Install ASP.NET Core

Install ASP.NET core by running "8 - aspnetcore-runtime-3.1.2-win-x64.exe".

A.1.9 Install ASP.NET Core Hosting Pack

Install ASP.NET core hosting pack by running "9 - dotnet-hosting-3.1.2-win.exe".

A.1.10 Install Azure Active Directory PowerShell Components

This procedure describes how to install Azure Active Directory PowerShell Components (10 - AzureAD.ps1).

- Enter the following PowerShell cmdlet:

```
Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -  
Force  
Install-Module AzureAD -force
```

A.2 (Optional) Install Support Tools for Debugging

You can optionally install support tools for debugging:

```
Postman (https://dl.pstmn.io/download/latest/win64)  
Sqlite Browser
```

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.
200 Cottontail Lane
Suite A101E
Somerset NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: <https://www.audiocodes.com/corporate/offices-worldwide>

website: <https://www.audiocodes.com/>

©2021 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, AudioCodes Room Experience and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-26348

