Upgrade Guide

AudioCodes One Voice™ for Microsoft 365

User Management Pack 365 SP Edition

Upgrade

Version 8.0.450

Notice

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

This document is subject to change without notice.

Date Published: July-20-2023

WEEE EU Directive

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

Customer Support

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

Documentation Feedback

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

Stay in the Loop with AudioCodes

Related Documentation

Document Name
User Management Pack 365 SP Edition Installation and Administration Guide
User Management Pack 365 SP Edition Release Notes

Document Revision Record

LTRT	Description
26722	Initial document version
26723	Update for version 8.0.450
26724	Correction to Installation ISO file package link in Section "Installing the Prerequisites"

Table of Contents

1 Introduction

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

- See Before Upgrading UMP-365 on page 2 for important prerequisites prior to upgrade.
- See Upgrading Main UMP-365 Tenant on page 14 for upgrade of the Main UMP-365 tenant.
- See Upgrading Customer Tenant on page 22 for upgrade of the Customer tenant.
- See Post Upgrade Actions on page 26for various actions required to perform following the completion of the upgrade.

2 Before Upgrading UMP-365

The following validations are performed automatically by wyUpdate:

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

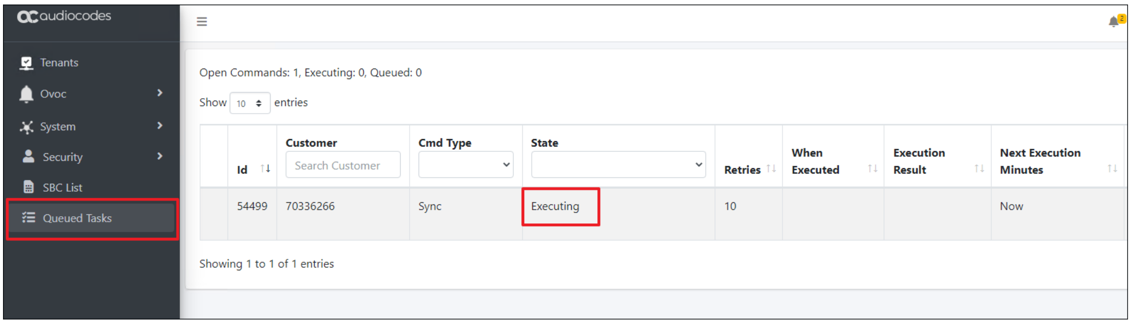
In addition, before upgrading, ensure the following:

- Create a snapshot backup of the UMP Virtual Machine (see Backing up UMP-365 – Disk Snapshot on page 4).
- Connection to the customers' M365 platform must be performed using token authentication instead of by username and password. This requirement is in accordance with stricter Microsoft's security policies. Before upgrading, make a list of all customers who are currently authenticated using username and password authentication. See Compiling List of Password Authenticated Customers on page 8.
- Install SSL certificates on the UMP Windows server for securing the HTTPS connection with Microsoft Azure. See Installing SSL Certificates on UMP Windows Server.
- Ensure ports HTTP/HTTPS ports are open in the Enterprise firewall (see Configure Firewall).
- Be aware of all processes running during the wyUpdate (see Stop wyUpdate Processes on page 9).
- When using a Backend SQL server, create the following directory on the SQL server:

  c:/acs/dbbackup/

> ⚠ The Backend SQL server username and password must be identical to the service account used for the installation of the UMP server. For more information, see SQL Server Configuration.

- Ensure all folders and all log files are closed in the C:\acs\ & C:\acs\tenants\ folders as the wyUpdate and SysAdminCustomerUpgrade access these folders and create backups. If the folders/files are open or in use, the upgrade process is interrupted.
- Ensure that there are currently no replication processes being executed (see Queued Tasks (Background Replication). Wait until all replication processes have been completed.



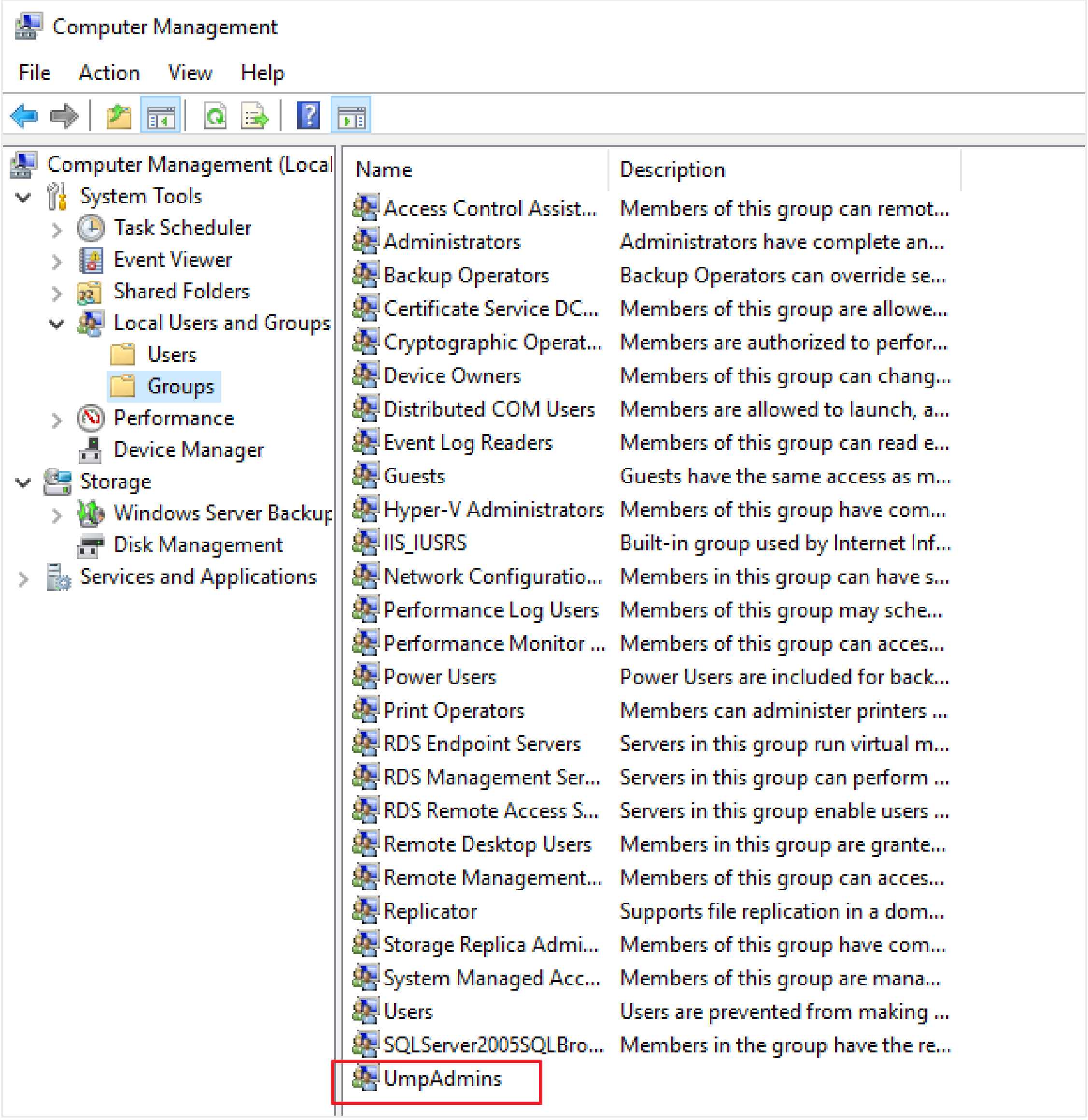
Open Commands: 1, Executing: 0, Queued: 0

Show 10 entries

Id	Customer	Cmd Type	State	Retries	When Executed	Execution Result	Next Execution Minutes
54499	70336266	Sync	Executing	10			Now

Showing 1 to 1 of 1 entries

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



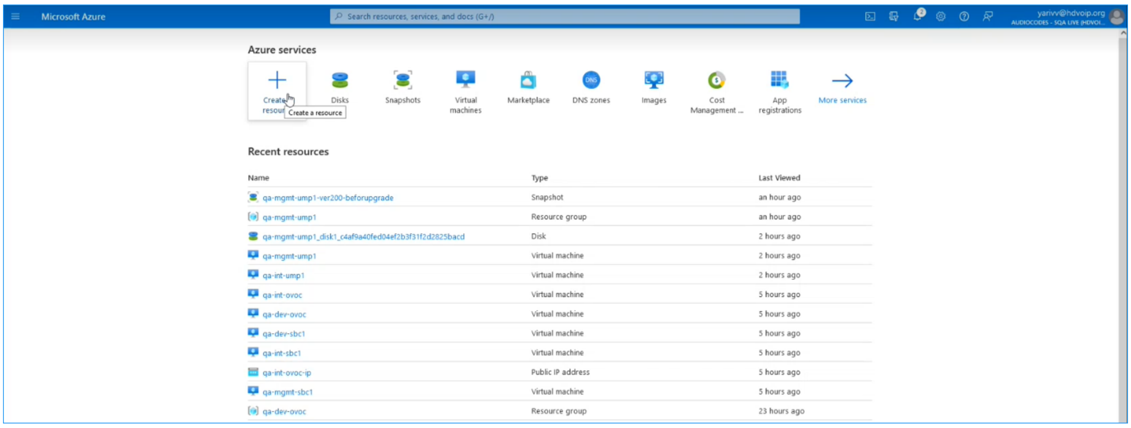
Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Certificate Service DC...	Members of this group are allowe...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Print Operators	Members can administer printers ...
RDS Endpoint Servers	Servers in this group run virtual m...
RDS Management Ser...	Servers in this group can perform ...
RDS Remote Access S...	Servers in this group enable users ...
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
Storage Replica Admi...	Members of this group have com...
System Managed Acc...	Members of this group are mana...
Users	Users are prevented from making ...
SQLServer2005SQLBro...	Members in the group have the re...
UmpAdmins	

Backing up UMP-365 – Disk Snapshot

This section describes how to create a snapshot of the UMP Virtual Machine. This procedure should be performed prior to running the upgrade and then rolled back once the upgrade is complete (see Restoring UMP Snapshot on page 26

➢ Do the following:

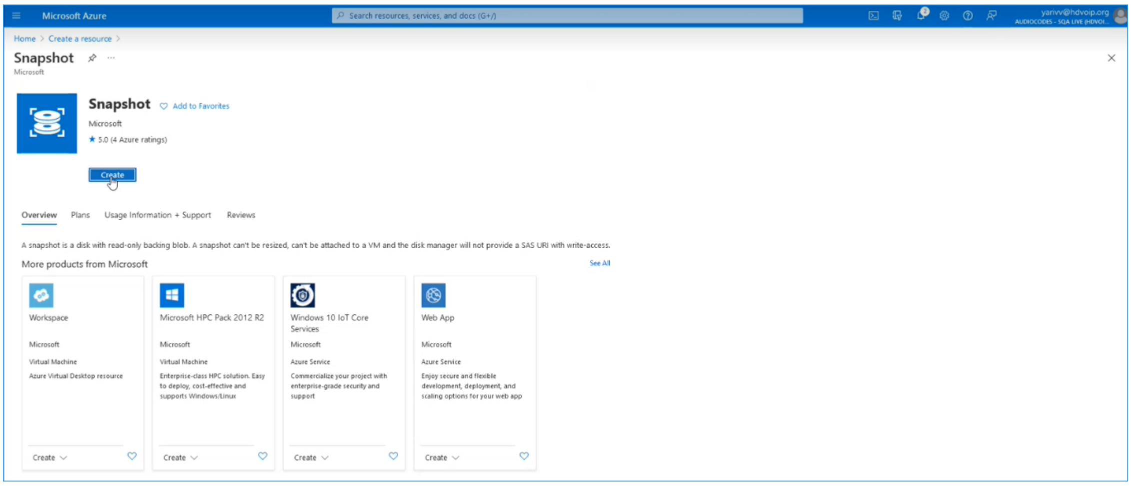
1. Open the Azure portal, type “Create a Resource” and then click **Create a Resource**.



Recent resources

Name	Type	Last Viewed
qa-mgmt-ump1-ver200-beforupgrade	Snapshot	an hour ago
qa-mgmt-ump1	Resource group	an hour ago
qa-mgmt-ump1_disk1_c4af9a40fed04ef2b3f31f2d2825bacd	Disk	2 hours ago
qa-mgmt-ump1	Virtual machine	2 hours ago
qa-int-ump1	Virtual machine	2 hours ago
qa-int-ovoc	Virtual machine	5 hours ago
qa-dev-ovoc	Virtual machine	5 hours ago
qa-dev-sbc1	Virtual machine	5 hours ago
qa-int-sbc1	Virtual machine	5 hours ago
qa-int-ovoc-ip	Public IP address	5 hours ago
qa-mgmt-sbc1	Virtual machine	5 hours ago
qa-dev-ovoc	Resource group	23 hours ago

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

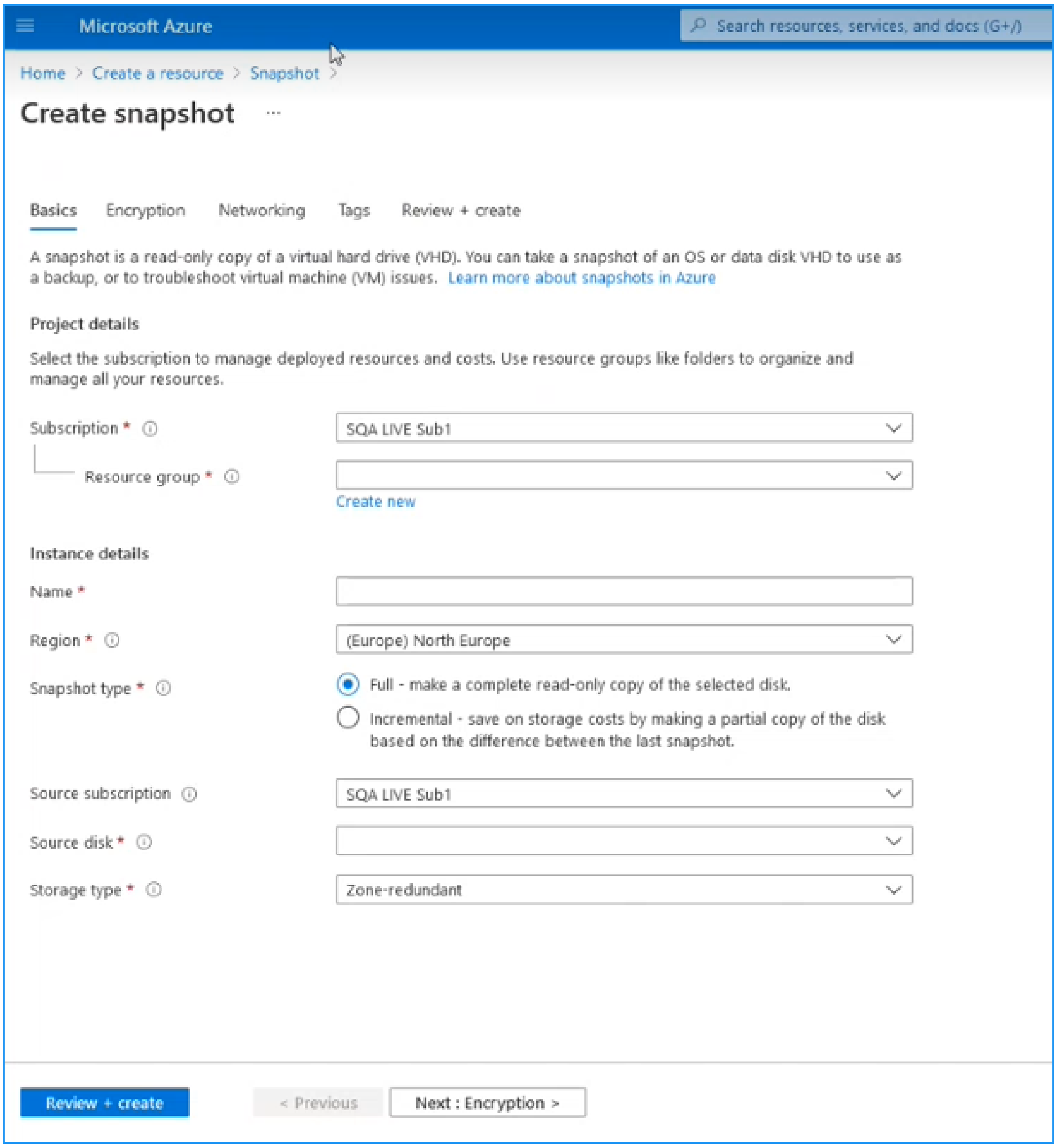


A snapshot is a disk with read-only backing blob. A snapshot can't be resized, can't be attached to a VM and the disk manager will not provide a SAS URI with write-access.

Enterprise-class HPC solution. Easy to deploy, cost-effective and supports Windows/Linux

Commercialize your project with enterprise-grade security and support

Enjoy secure and flexible development, deployment, and scaling options for your web app



Create snapshot ...

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

Project details

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

Subscription * : SQA LIVE Sub1

Resource group * :

Create new

Instance details

Name * :

Region * : (Europe) North Europe

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

Source subscription : SQA LIVE Sub1

Source disk * :

Storage type * : Zone-redundant

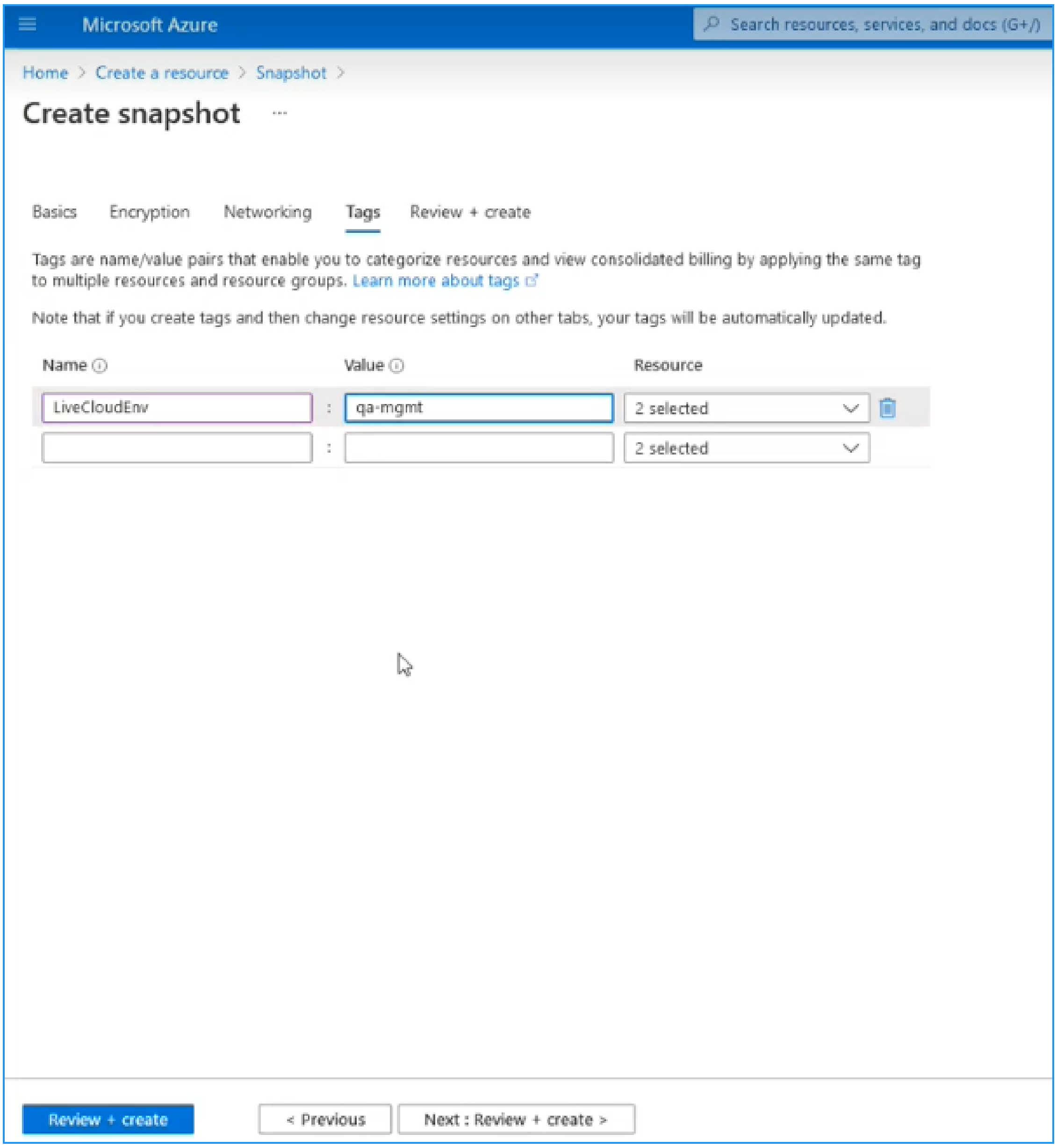
3. In the Resource group field, select your working Resource Group.

4. Enter the desired name of the snapshot.

5. In the Source disk field drop-down list choose the name of the disk that you wish to backup.

6. In the Storage type field drop-down list choose the type of disk that you wish to backup e.g. Standard HDD.

7. Select the Tags tab to optionally define tags for the snapshot and then click **Review + create**.



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Snapshot >

Create snapshot ...

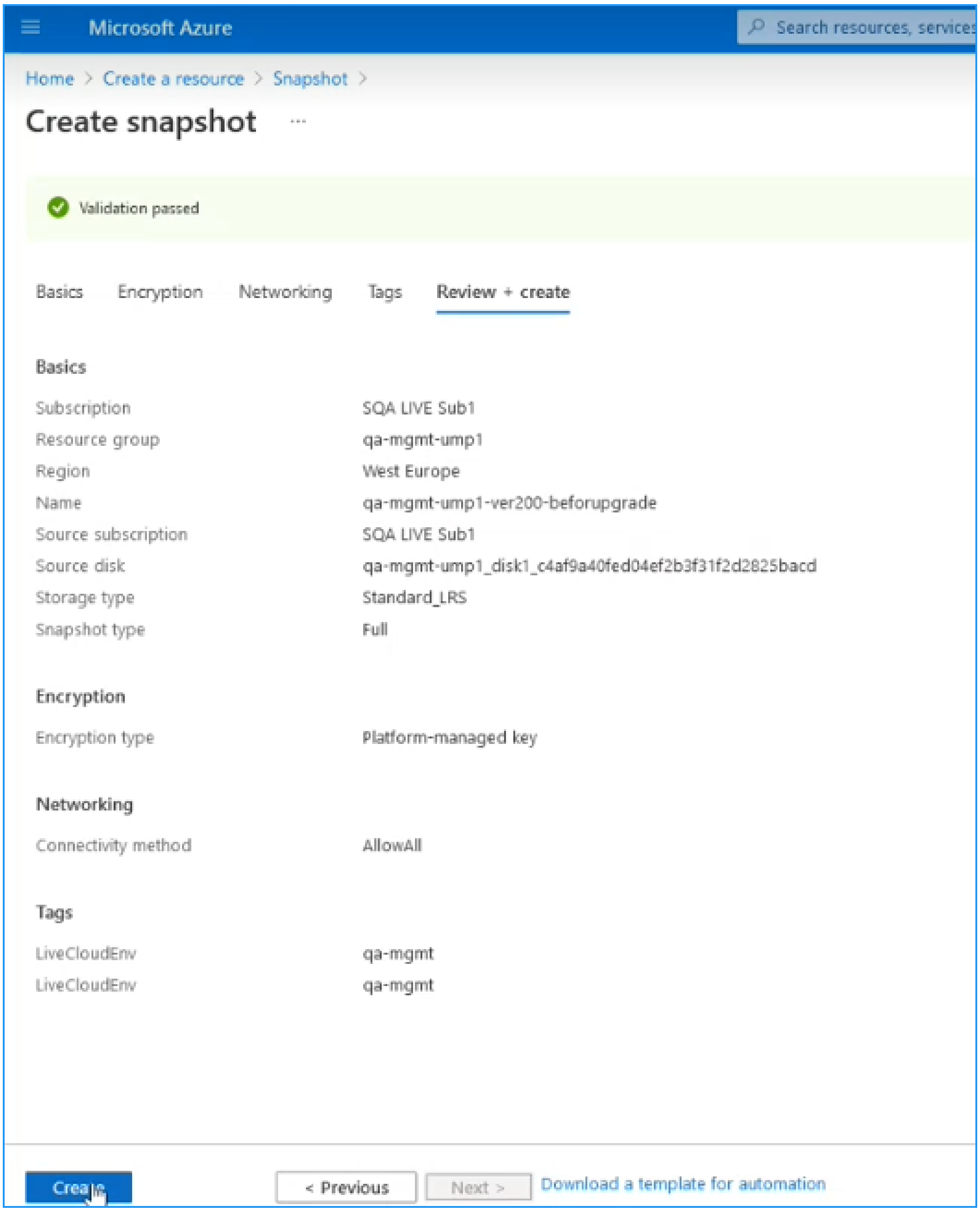
Basics
Encryption
Networking
Tags
Review + create

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

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

Name		Value	Resource
LiveCloudEnv	:	qa-mgmt	2 selected
	:		2 selected

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



Microsoft Azure
Search resources, services
Home > Create a resource > Snapshot >

Create snapshot

Validation passed

Basics
Encryption
Networking
Tags
Review + create

Basics

Subscription	SQA LIVE Sub1
Resource group	qa-mgmt-ump1
Region	West Europe
Name	qa-mgmt-ump1-ver200-beforupgrade
Source subscription	SQA LIVE Sub1
Source disk	qa-mgmt-ump1_disk1_c4af9a40fed04ef2b3f31f2d2825bacd
Storage type	Standard_LRS
Snapshot type	Full

Encryption

Encryption type	Platform-managed key

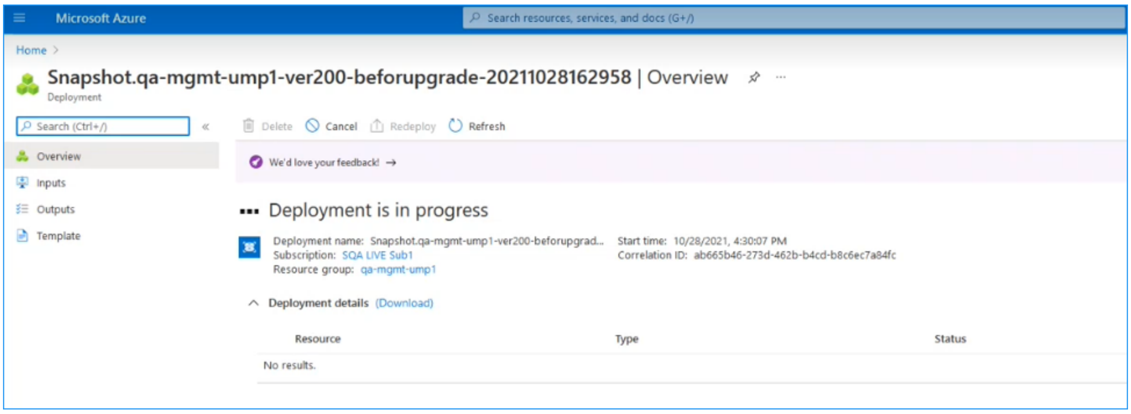
Networking

Connectivity method	AllowAll

Tags

LiveCloudEnv	qa-mgmt
LiveCloudEnv	qa-mgmt

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



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

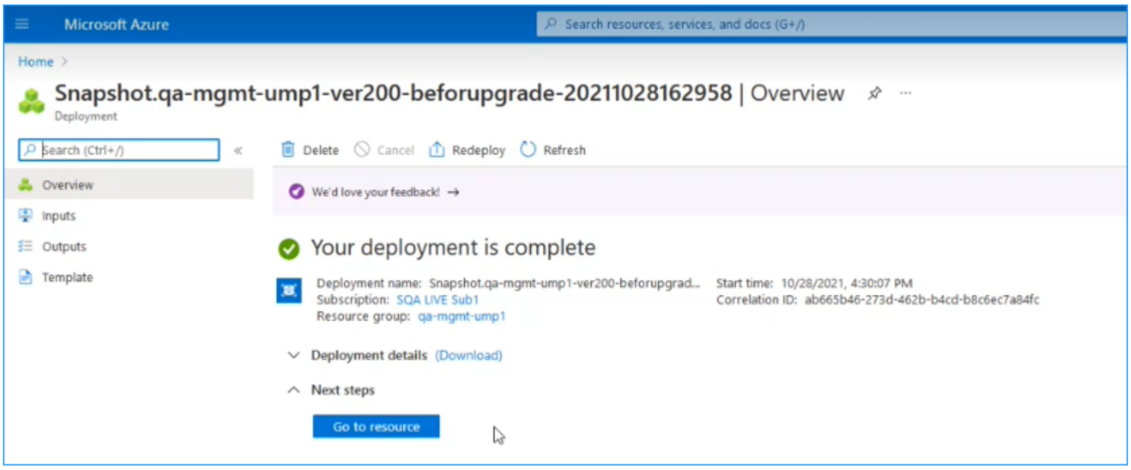
Deployment

Deployment is in progress

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

Deployment details (Download)

Resource	Type	Status
No results.		



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

Deployment

Your deployment is complete

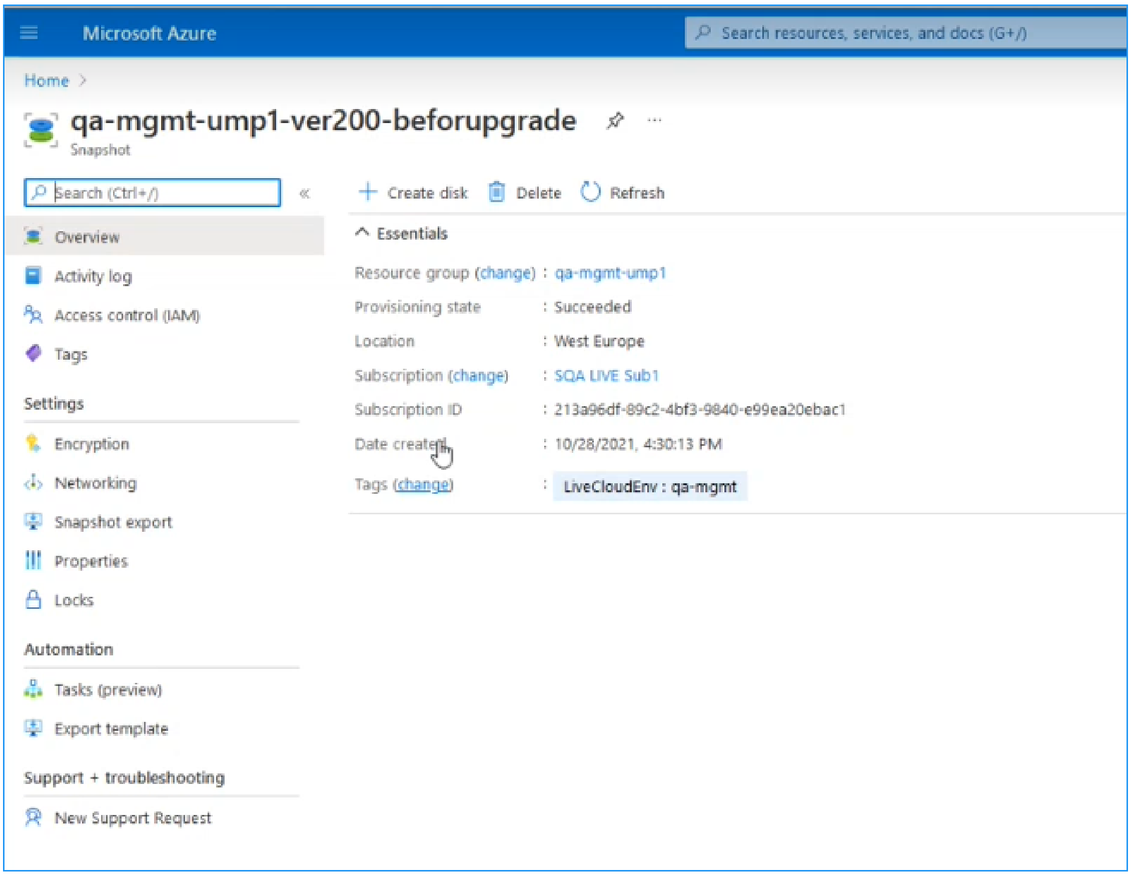
Deployment name: Snapshot.qa-mgmt-ump1-ver200-beforupgrad...
Subscription: SQA LIVE Sub1
Resource group: qa-mgmt-ump1

Start time: 10/28/2021, 4:30:07 PM
Correlation ID: ab665b46-273d-462b-b4cd-b8c6ec7a84fc

Deployment details (Download)

Next steps

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



qa-mgmt-ump1-ver200-beforupgrade

Snapshot

Essentials

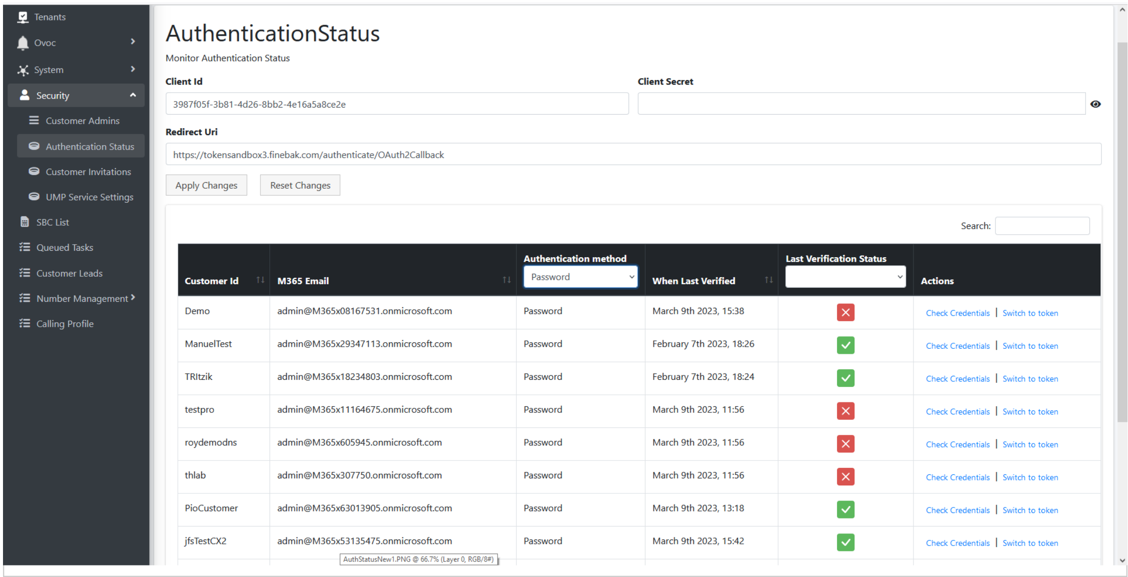
Resource group (change) : qa-mgmt-ump1
Provisioning state : Succeeded
Location : West Europe
Subscription (change) : SQA LIVE Sub1
Subscription ID : 213a96df-89c2-4bf3-9840-e99ea20ebac1
Date created : 10/28/2021, 4:30:13 PM
Tags (change) : LiveCloudEnv : qa-mgmt

Compiling List of Password Authenticated Customers

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

➢ To sort all customers authenticated with password:

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



AuthenticationStatus

Monitor Authentication Status

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

Client Secret:

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

Search:

Customer Id	M365 Email	Authentication method Password	When Last Verified	Last Verification Status	Actions
Demo	admin@M365x08167531.onmicrosoft.com	Password	March 9th 2023, 15:38	✗	Check Credentials | Switch to token
ManuelTest	admin@M365x29347113.onmicrosoft.com	Password	February 7th 2023, 18:26	✓	Check Credentials | Switch to token
TRItzik	admin@M365x18234803.onmicrosoft.com	Password	February 7th 2023, 18:24	✓	Check Credentials | Switch to token
testpro	admin@M365x11164675.onmicrosoft.com	Password	March 9th 2023, 11:56	✗	Check Credentials | Switch to token
roydemodns	admin@M365x605945.onmicrosoft.com	Password	March 9th 2023, 11:56	✗	Check Credentials | Switch to token
thlab	admin@M365x307750.onmicrosoft.com	Password	March 9th 2023, 11:56	✗	Check Credentials | Switch to token
PioCustomer	admin@M365x63013905.onmicrosoft.com	Password	March 9th 2023, 13:18	✓	Check Credentials | Switch to token
jfsTestCX2	admin@M365x53135475.onmicrosoft.com	Password	March 9th 2023, 15:42	✓	Check Credentials | Switch to token

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

3. Capture the filtered list.

Stop wyUpdate Processes

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

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

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

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

Process	Detail	Executable
InstallPowershellGetModule	update/install PowerShell get	PowershellGet/PackageManagement
InstallMicrosoftTeamsModule	update/install Microsoft Teams	MicrosoftTeams
InstallChocolatey	update/install Chocolatey	Chocolatey
InstallDotNet	update/install DotNet	choco dotnet-6.0-runtime/dotnet-6.0-windowshosting
InstallRabbitmq	update/install RabbitMQ	choco rabbitmq
InstallEmsMainAgent	update/install EMS Main Agent	EmsMainAgent.msi 7.8.19.51806
InstallEmsClientAgent	update/install EMS Client Agent	EmsClientAgent.msi 7.8.21.52131
InstallPublicOvocConnector	update/install Public OVOC Connector	PublicOvocConnector.msi 1.0.8.51546
Installtap-windows-9.23.3-I601-Win10	update/install Tap-Windows	tap-windows-9.23.3-I601-Win10.exe
RunCheckAzureTenantId_220	check tenants-ids/passwords	c:\acs\CheckAzureTenantId_220\CheckAzureTenantId_220.exe
RunCheckAzureTenantId_220_ Password	check tenantid/password	c:\acs\CheckAzureTenantId_220\CheckAzureTenantId_220.exe
AlertCustomerUpgrade	warning to run customer upgrade after wyUpdate finishes successfully	..\temp\170.AlertCustomerUpgrade.bat
runLogReport	show results wyUpdate process	c:\acs\tools\LogReport\LogReport.exe
Refresh_EMSClientAgent_ignoreList	Refresh data on the ignorelist with default values	..\temp\EMSClientAgentConfigIgnoreListData.ps1

Process	Detail	Executable
SysAdmin.QuickReplicationCycleWorker	Triggers the Cachesync mechanism for a specific customer.	
SysAdmin.UMP.Watchdog	Manages the database replication timer mechanism according the preconfigured setting in the dbo.ApplicationSetting {QuickReplicationCycleDelay}. Default-five minutes. Replication is processed only when no new changes are sent within the five minute interval. Grabs process threads for available queues.	
CacheSyncAzAd	Downloads users, groups and group membership using MSGraph.	
CacheSync/CacheSyncV2	■ Downloads all the CsOnlineUsers ■ Downloads all the Teams user policies	
SysAdmin.UMP.SyncAcquiredNumber	Used by Operator Connect (OC) for updating the Assignment Status column in the Number Management table in the	

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

3 Upgrading Main UMP-365 Tenant

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

➢ **Do the following:**

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

```
stop-service sysadmin*
```

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

```
stop-service w3svc
```

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

```
get-service sysadmin*
```

```
get-service w3svc
```

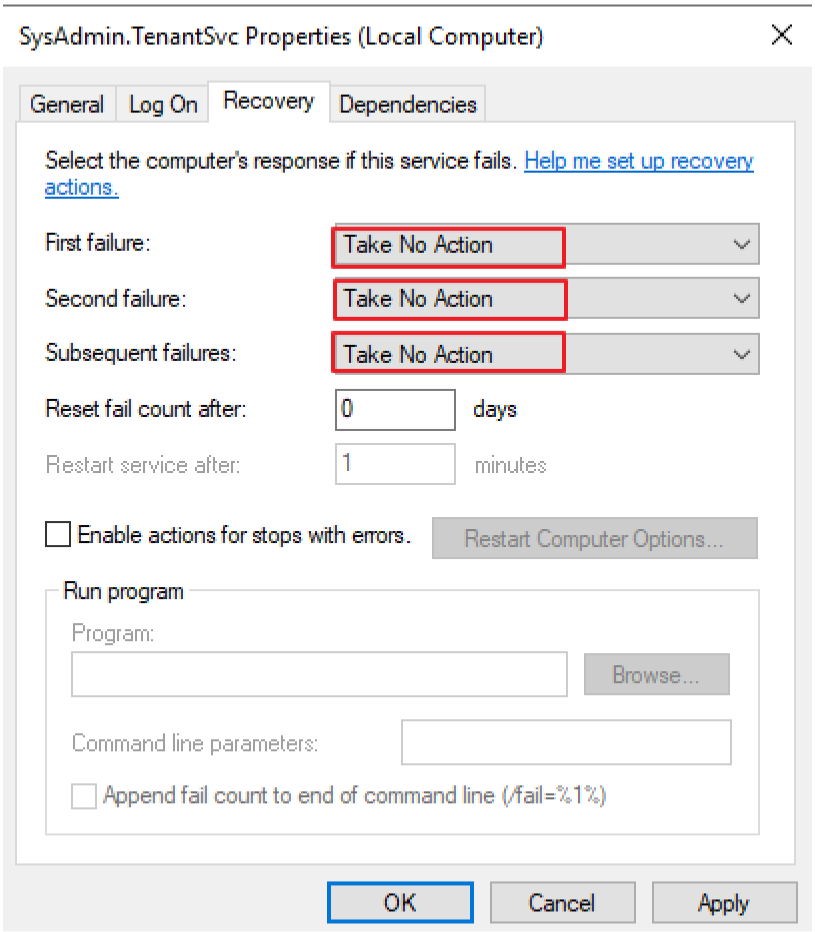
4. If one of the above services has not been stopped, open the Windows Services Manager Services (click ⊞ and type **Services**) right-click each of the above services, and then select **Stop**.

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

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

- SysAdmin.TenantSvc
- SysAdmin.PeeringSvc
- all SysAdmin.CacheSrv.[tenant_shortname]

5. If a service keeps restarting, set the properties of the service SysAdmin.TenantSvc to **Take No Action** (see example in figure below).



SysAdmin.TenantSvc Properties (Local Computer)

Select the computer's response if this service fails. Help me set up recovery actions.

First failure: Take No Action

Second failure: Take No Action

Subsequent failures: Take No Action

Reset fail count after: 0 days

Restart service after: 1 minutes

☐ Enable actions for stops with errors.

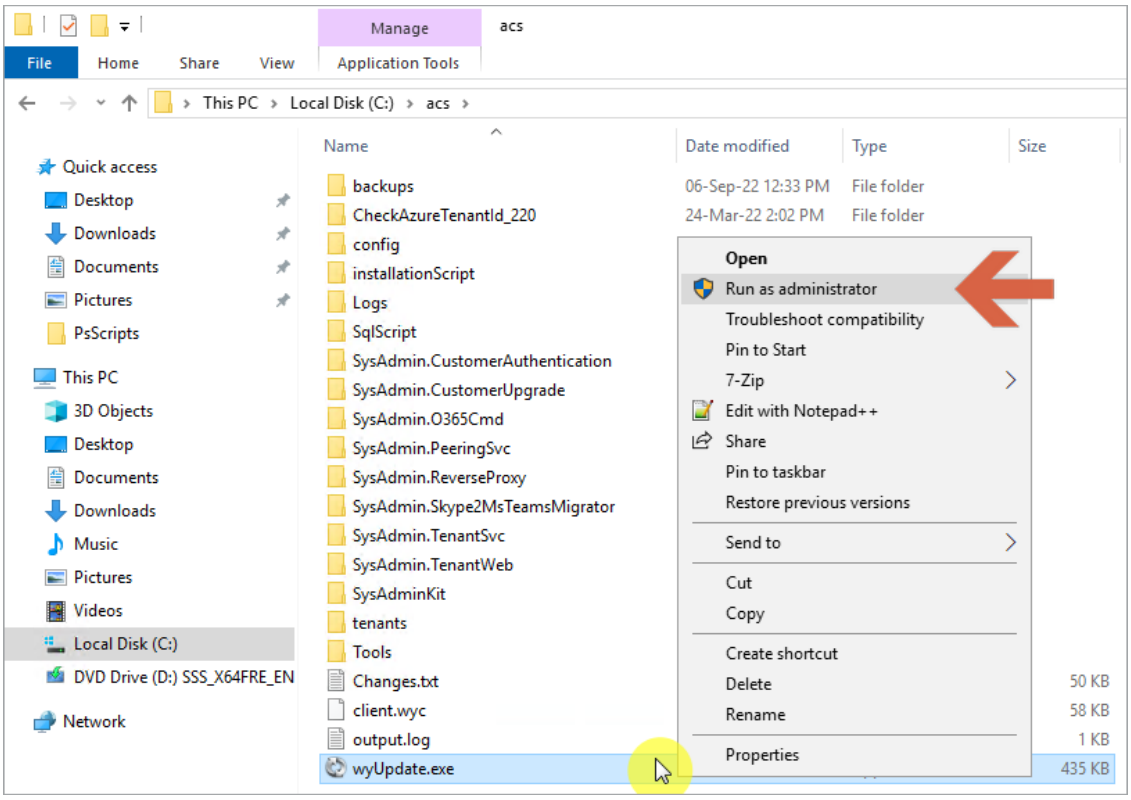
Run program

Program:

Command line parameters:

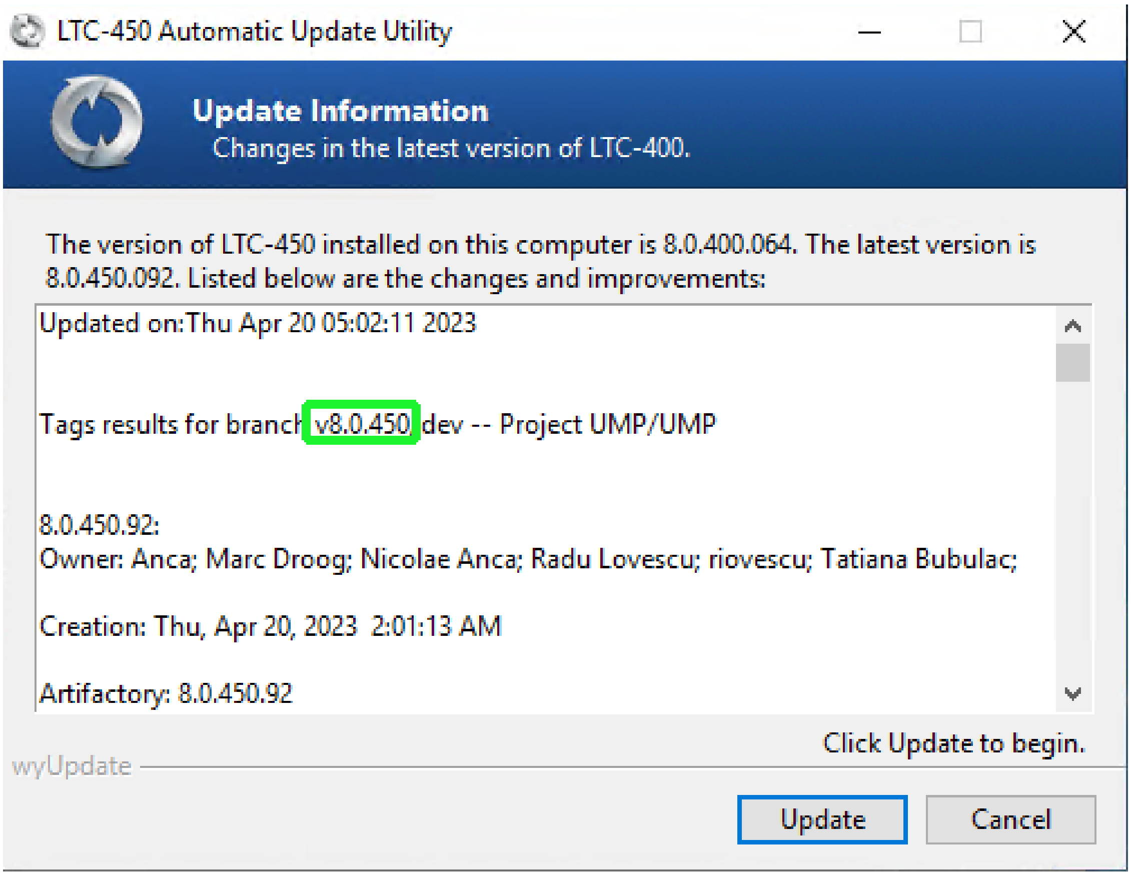
☐ Append fail count to end of command line (/fail=%1%)

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



Name	Date modified	Type	Size
backups	06-Sep-22 12:33 PM	File folder	
CheckAzureTenantId_220	24-Mar-22 2:02 PM	File folder	
config			
installationScript			
Logs			
SqlScript			
SysAdmin.CustomerAuthentication			
SysAdmin.CustomerUpgrade			
SysAdmin.O365Cmd			
SysAdmin.PeeringSvc			
SysAdmin.ReverseProxy			
SysAdmin.Skype2MsTeamsMigrator			
SysAdmin.TenantSvc			
SysAdmin.TenantWeb			
SysAdminKit			
tenants			
Tools			
Changes.txt			50 KB
client.wyc			58 KB
output.log			1 KB
wyUpdate.exe			435 KB

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

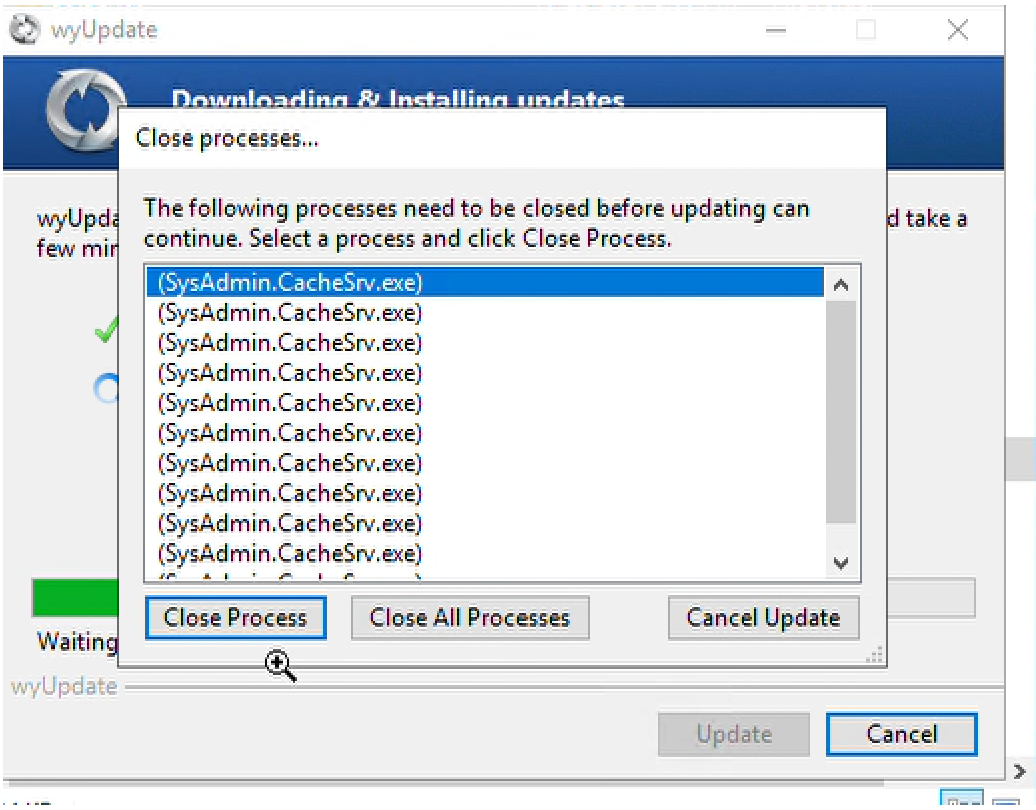

LTC-450 Automatic Update Utility
Update Information
Changes in the latest version of LTC-400.

The version of LTC-450 installed on this computer is 8.0.400.064. The latest version is 8.0.450.092. Listed below are the changes and improvements:

```
Updated on:Thu Apr 20 05:02:11 2023


Tags results for branch v8.0.450 dev -- Project UMP/UMP


8.0.450.92:
Owner: Anca; Marc Droog; Nicolae Anca; Radu Lovescu; riovescu; Tatiana Bubulac;

Creation: Thu, Apr 20, 2023  2:01:13 AM

Artifactory: 8.0.450.92
```

Click Update to begin.

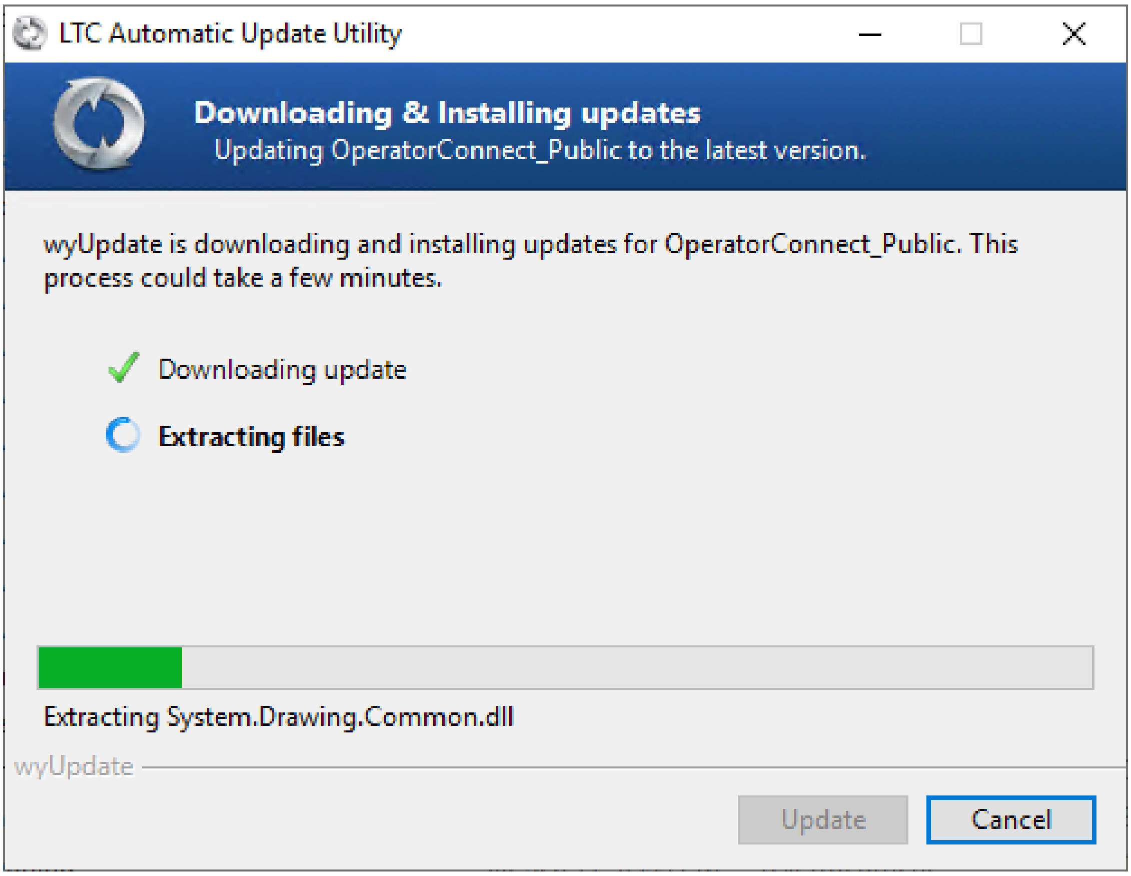
8. If you did not close all the services via PowerShell, then during the update you are prompted to “Close processes…”. Confirm this action. This kills the running processes and continues the upgrade.



The following processes need to be closed before updating can continue. Select a process and click Close Process.

(SysAdmin.CacheSrv.exe)
(SysAdmin.CacheSrv.exe)
(SysAdmin.CacheSrv.exe)
(SysAdmin.CacheSrv.exe)
(SysAdmin.CacheSrv.exe)
(SysAdmin.CacheSrv.exe)
(SysAdmin.CacheSrv.exe)
(SysAdmin.CacheSrv.exe)
(SysAdmin.CacheSrv.exe)
(SysAdmin.CacheSrv.exe)

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


LTC Automatic Update Utility
Downloading & Installing updates

Updating OperatorConnect_Public to the latest version.

wyUpdate is downloading and installing updates for OperatorConnect_Public. This process could take a few minutes.

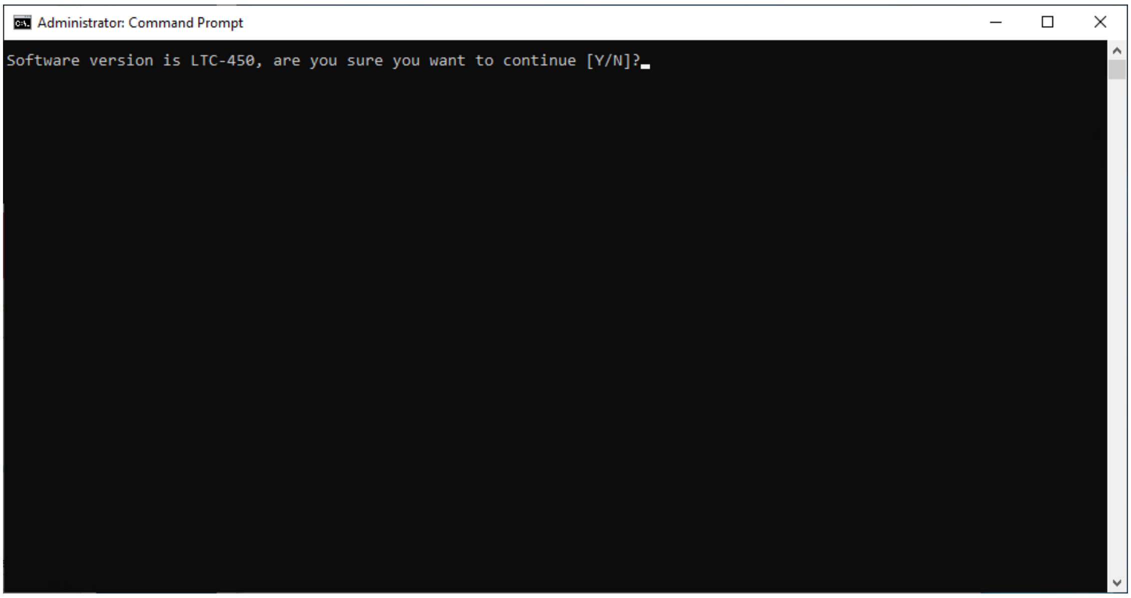
✓ Downloading update

Extracting files

Extracting System.Drawing.Common.dll

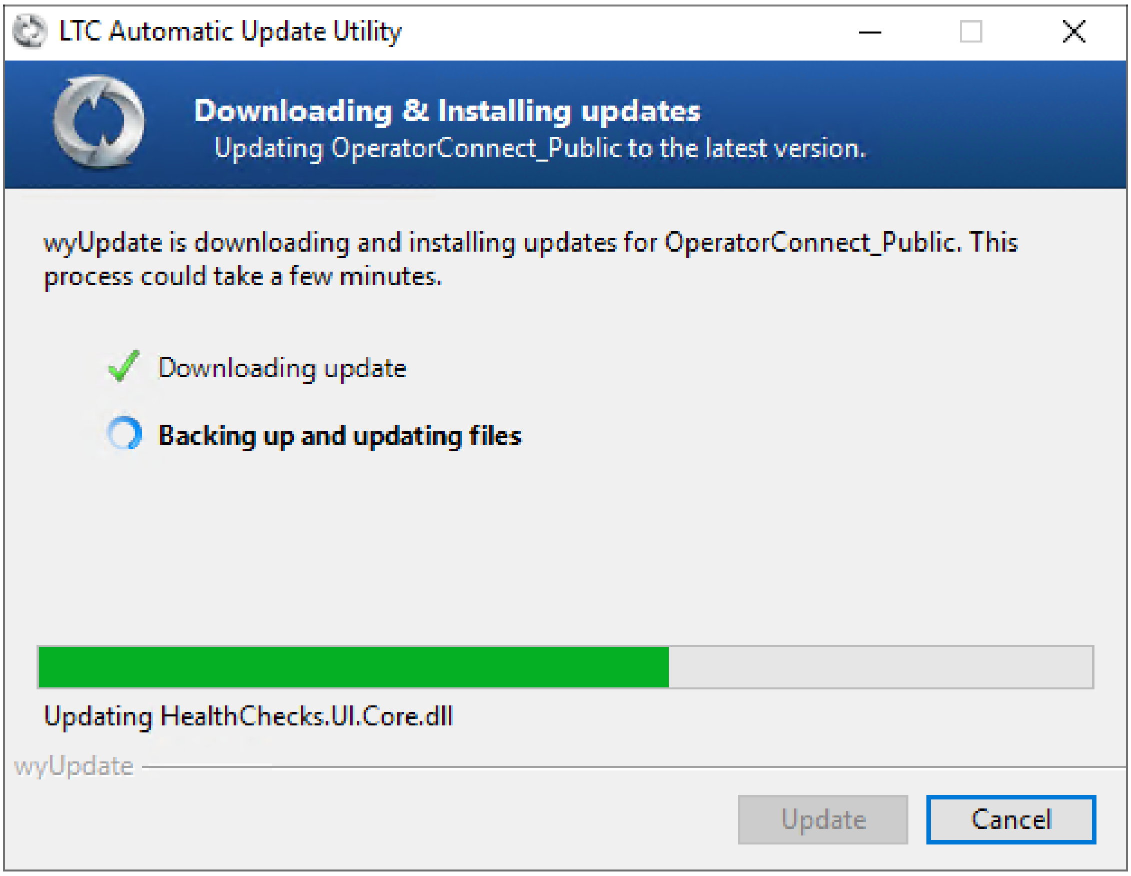
9. The upgrade process is interrupted via the CMD window pop-up. The following prompt is displayed:
   Warning … Are you sure you want to continue. [Y / N] ?

10. Type **Y** and press Enter.



```
Software version is LTC-450, are you sure you want to continue [Y/N]?_
```

- Folders are backed up and files are updated.


LTC Automatic Update Utility
Downloading & Installing updates
Updating OperatorConnect_Public to the latest version.

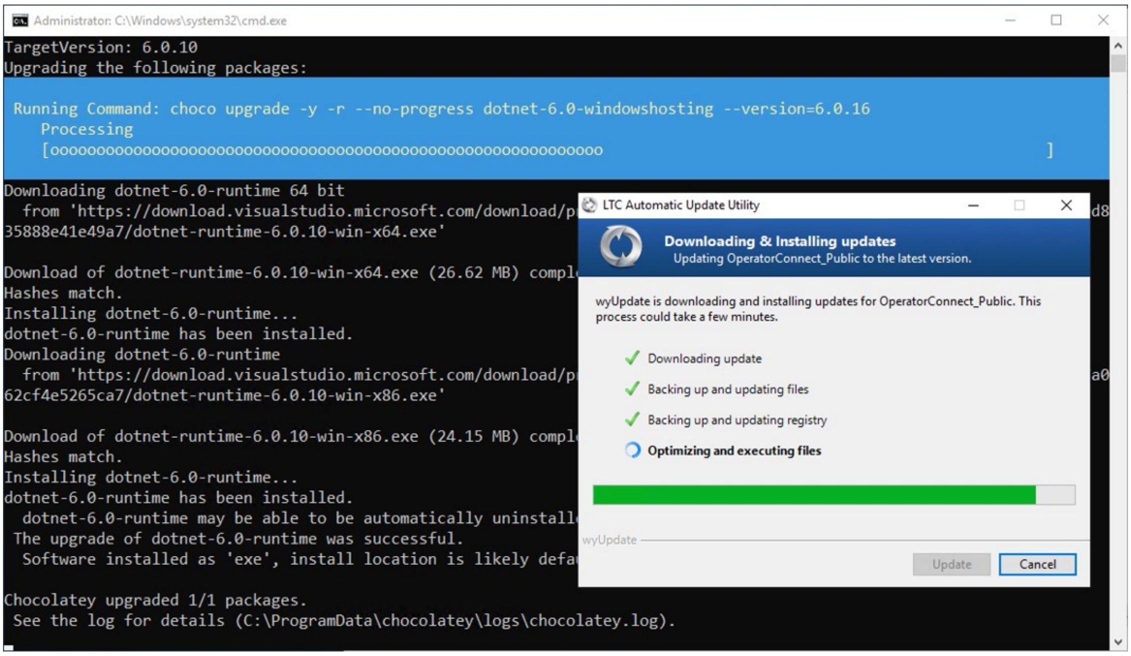
wyUpdate is downloading and installing updates for OperatorConnect_Public. This process could take a few minutes.

✓ Downloading update

Backing up and updating files

Updating HealthChecks.UI.Core.dll

- During the optimization and execution, various necessary software packages are installed as described in Stop wyUpdate Processes on page 9.



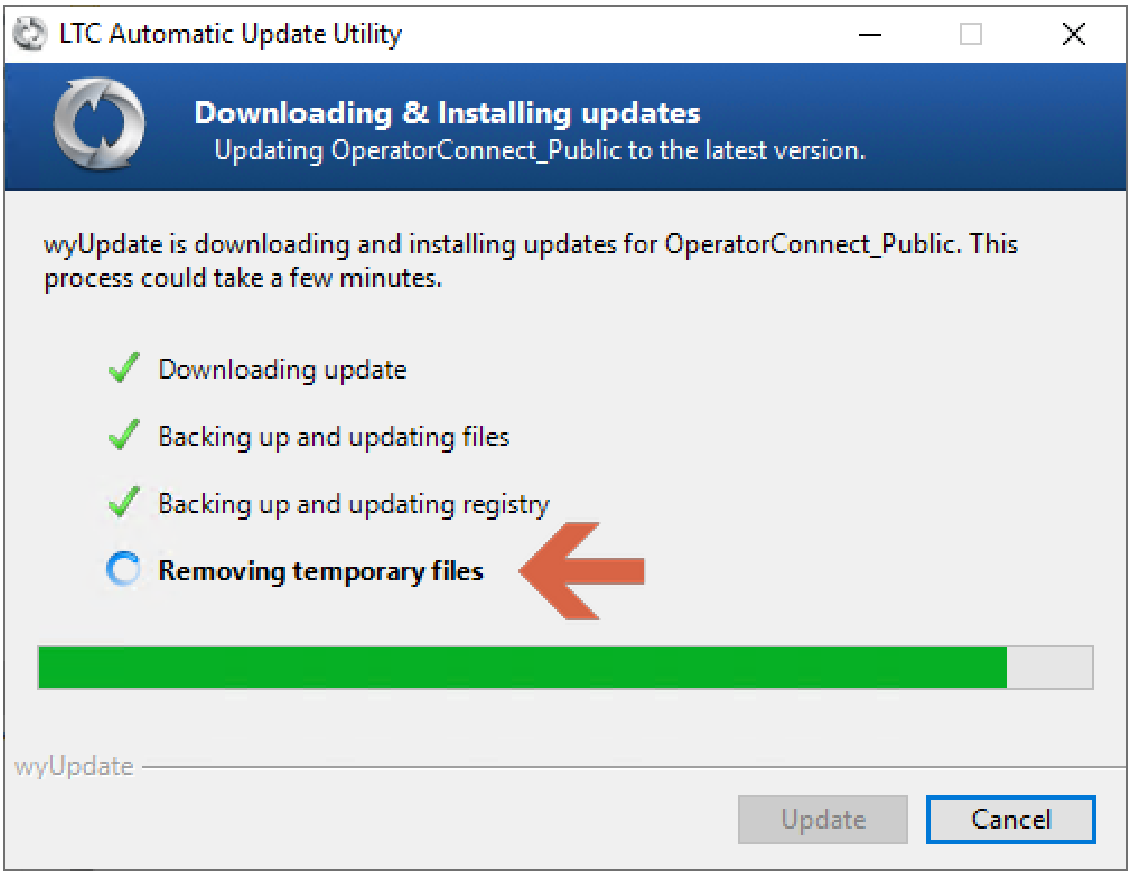
```
TargetVersion: 6.0.10
Upgrading the following packages:

 Running Command: choco upgrade -y -r --no-progress dotnet-6.0-windowshosting --version=6.0.16
    Processing
    [oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo                    ]

Downloading dotnet-6.0-runtime 64 bit
  from 'https://download.visualstudio.microsoft.com/download/p                                      d8
35888e41e49a7/dotnet-runtime-6.0.10-win-x64.exe'

Download of dotnet-runtime-6.0.10-win-x64.exe (26.62 MB) compl
Hashes match.
Installing dotnet-6.0-runtime...
dotnet-6.0-runtime has been installed.
Downloading dotnet-6.0-runtime
  from 'https://download.visualstudio.microsoft.com/download/p                                      a0
62cf4e5265ca7/dotnet-runtime-6.0.10-win-x86.exe'

Download of dotnet-runtime-6.0.10-win-x86.exe (24.15 MB) compl
Hashes match.
Installing dotnet-6.0-runtime...
dotnet-6.0-runtime has been installed.
  dotnet-6.0-runtime may be able to be automatically uninstall
 The upgrade of dotnet-6.0-runtime was successful.
  Software installed as 'exe', install location is likely defa

Chocolatey upgraded 1/1 packages.
 See the log for details (C:\ProgramData\chocolatey\logs\chocolatey.log).
```

Downloading & Installing updates
Updating OperatorConnect_Public to the latest version.

wyUpdate is downloading and installing updates for OperatorConnect_Public. This process could take a few minutes.

✓ Downloading update
✓ Backing up and updating files
✓ Backing up and updating registry
○ **Optimizing and executing files**

- Temporary files are removed.

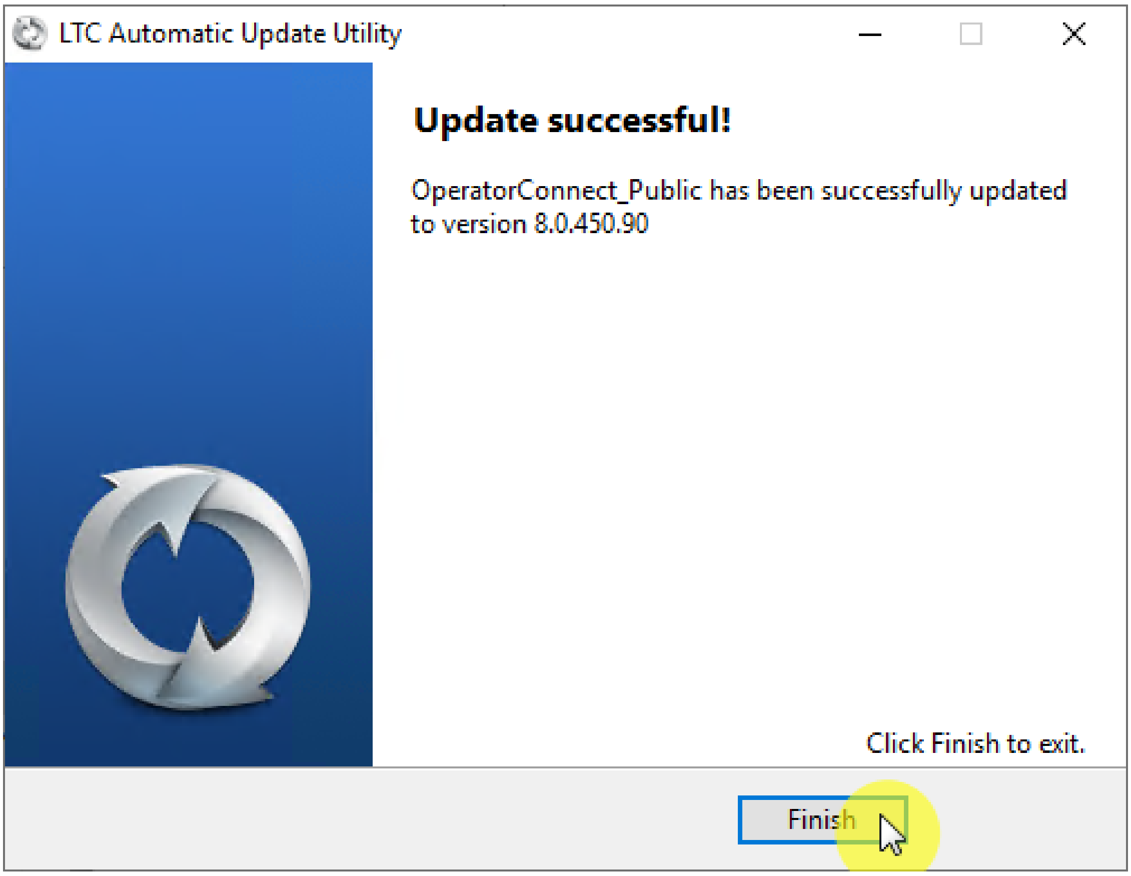


Downloading & Installing updates
Updating OperatorConnect_Public to the latest version.

wyUpdate is downloading and installing updates for OperatorConnect_Public. This process could take a few minutes.

✓ Downloading update
✓ Backing up and updating files
✓ Backing up and updating registry
○ **Removing temporary files**

11. Click **Finish**.

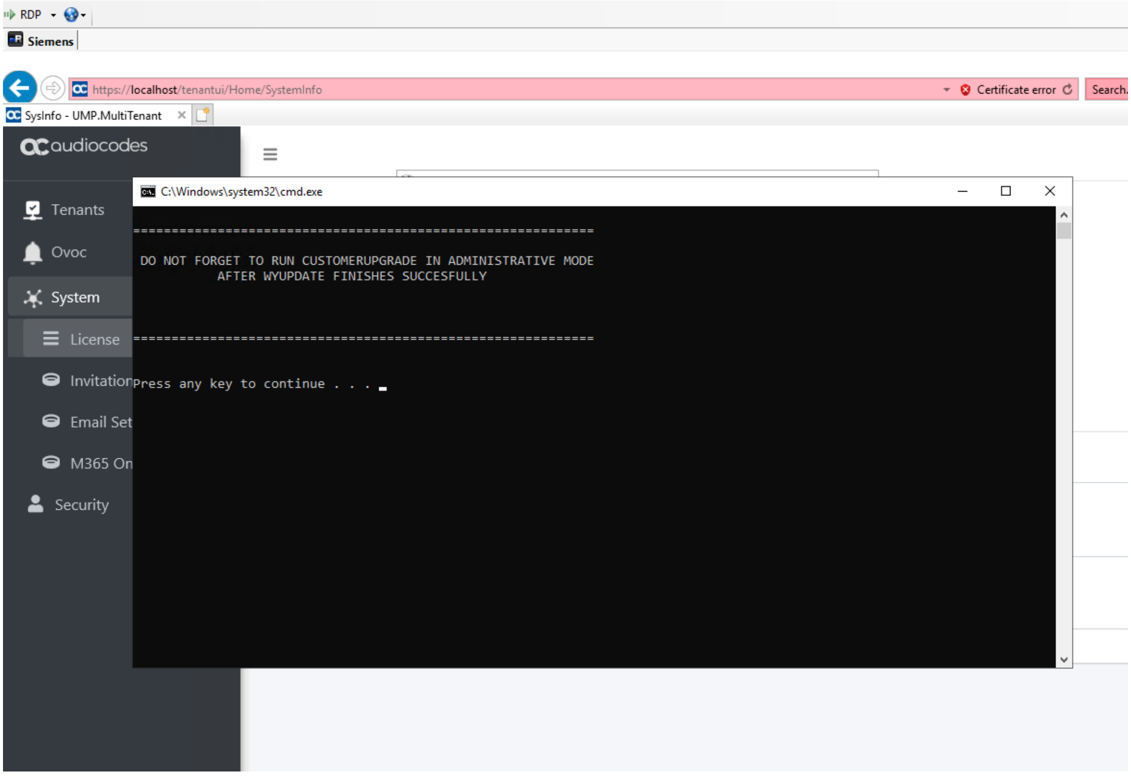


Update successful!

OperatorConnect_Public has been successfully updated to version 8.0.450.90

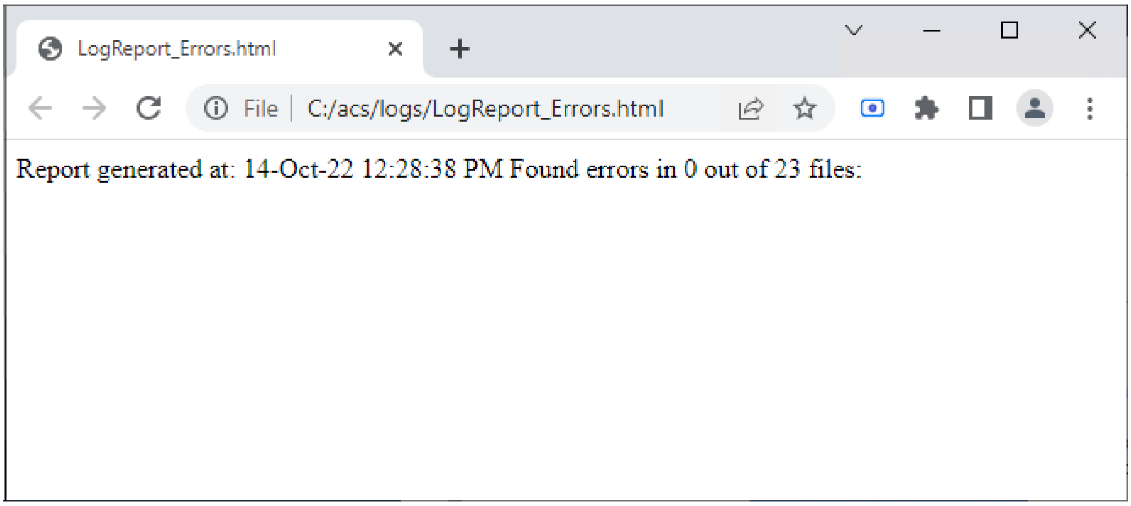
Click Finish to exit.

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



```
==========================================================

DO NOT FORGET TO RUN CUSTOMERUPGRADE IN ADMINISTRATIVE MODE
          AFTER WYUPDATE FINISHES SUCCESFULLY


==========================================================
Press any key to continue . . .
```

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



Report generated at: 14-Oct-22 12:28:38 PM Found errors in 0 out of 23 files:

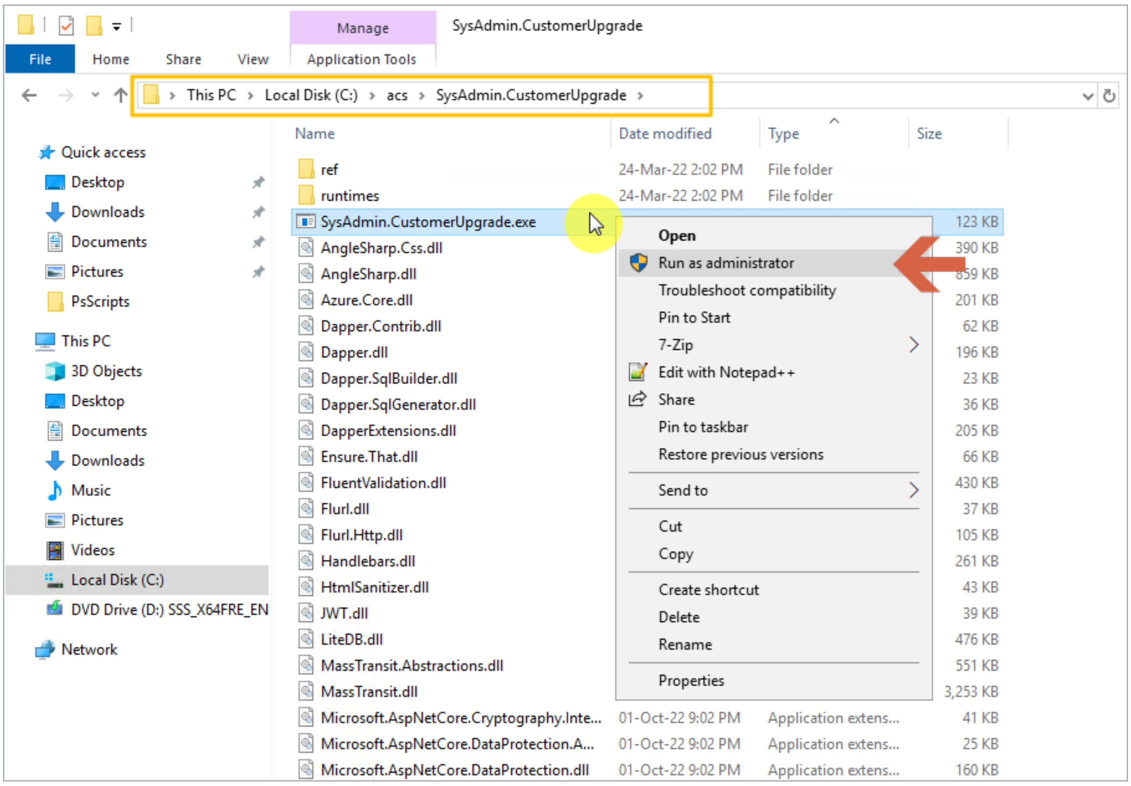
4 Upgrading Customer Tenant

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

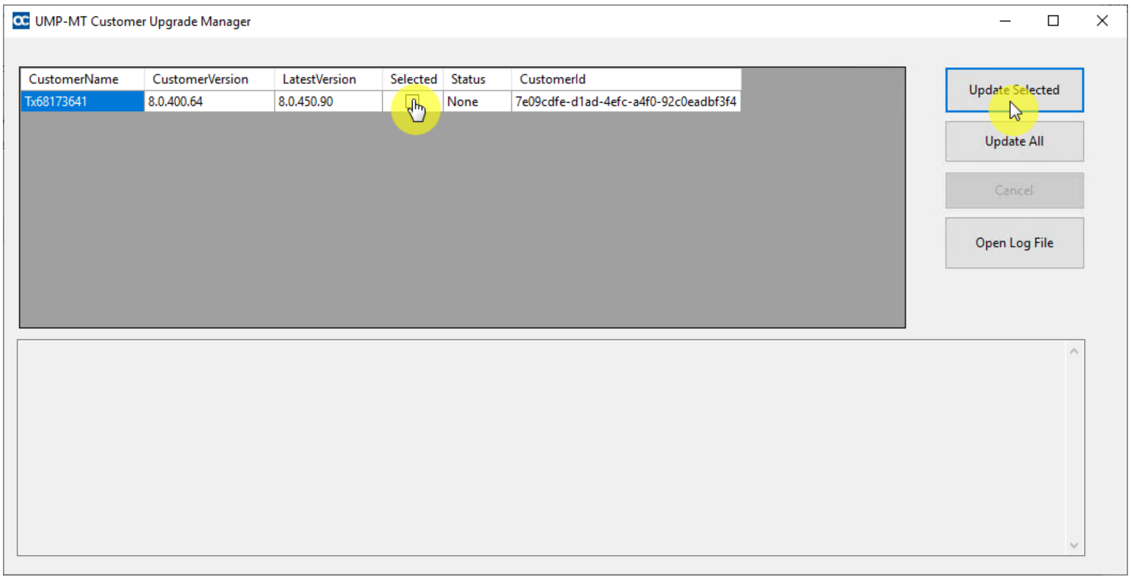
- Run the Sysadmin.CustomerUpgrade.exe as an Administrator using the UMP service admin account that was created in "Create UMP Service Account" in User Management Pack 365 Administrator and Installation Manual.
- If you have a back-end SQL server for all your tenants, ensure that the username and password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

➢ Do the following:

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

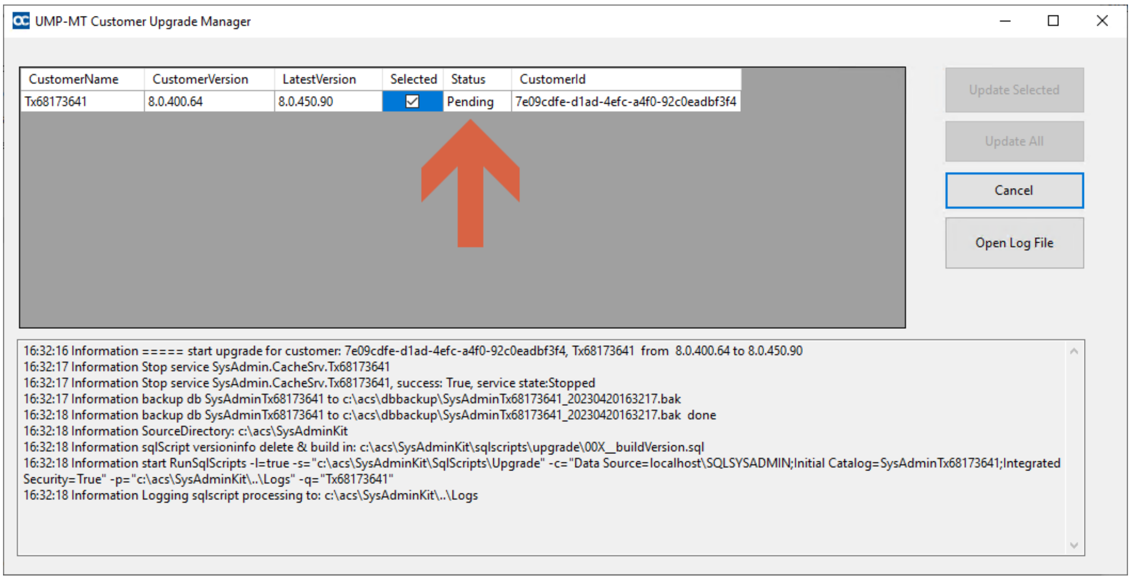


2. In the Customer Upgrade Manager, select the customers for which you wish to upgrade and then click **Update Selected**.



CustomerName	CustomerVersion	LatestVersion	Selected	Status	CustomerId
Tx68173641	8.0.400.64	8.0.450.90	☐	None	7e09cdfe-d1ad-4efc-a4f0-92c0eadbf3f4

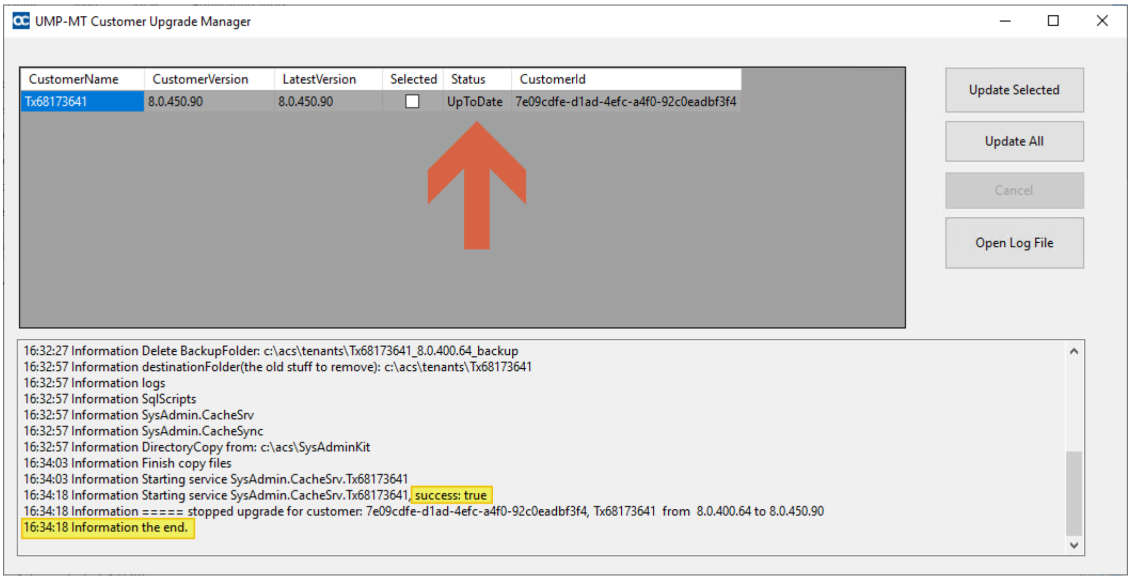
During the upgrade process, a pending message is displayed.



CustomerName	CustomerVersion	LatestVersion	Selected	Status	CustomerId
Tx68173641	8.0.400.64	8.0.450.90	☑	Pending	7e09cdfe-d1ad-4efc-a4f0-92c0eadbf3f4

```
16:32:16 Information ===== start upgrade for customer: 7e09cdfe-d1ad-4efc-a4f0-92c0eadbf3f4, Tx68173641  from  8.0.400.64 to 8.0.450.90
16:32:17 Information Stop service SysAdmin.CacheSrv.Tx68173641
16:32:17 Information Stop service SysAdmin.CacheSrv.Tx68173641, success: True, service state:Stopped
16:32:17 Information backup db SysAdminTx68173641 to c:\acs\dbbackup\SysAdminTx68173641_20230420163217.bak
16:32:18 Information backup db SysAdminTx68173641 to c:\acs\dbbackup\SysAdminTx68173641_20230420163217.bak  done
16:32:18 Information SourceDirectory: c:\acs\SysAdminKit
16:32:18 Information sqlScript versioninfo delete & build in: c:\acs\SysAdminKit\sqlscripts\upgrade\00X__buildVersion.sql
16:32:18 Information start RunSqlScripts -l=true -s="c:\acs\SysAdminKit\SqlScripts\Upgrade" -c="Data Source=localhost\SQLSYSADMIN;Initial Catalog=SysAdminTx68173641;Integrated
Security=True" -p="c:\acs\SysAdminKit\..\Logs" -q="Tx68173641"
16:32:18 Information Logging sqlscript processing to: c:\acs\SysAdminKit\..\Logs
```

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

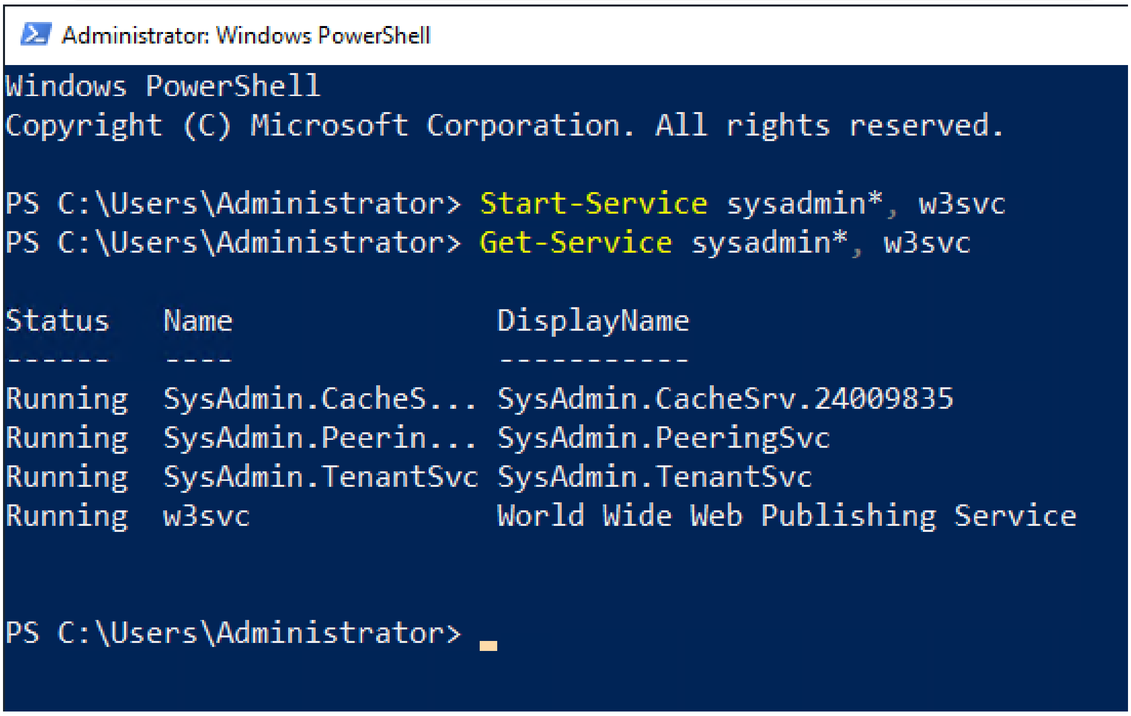


CustomerName	CustomerVersion	LatestVersion	Selected	Status	CustomerId
Tx68173641	8.0.450.90	8.0.450.90	□	UpToDate	7e09cdfe-d1ad-4efc-a4f0-92c0eadbf3f4

```
16:32:27 Information Delete BackupFolder: c:\acs\tenants\Tx68173641_8.0.400.64_backup
16:32:57 Information destinationFolder(the old stuff to remove): c:\acs\tenants\Tx68173641
16:32:57 Information logs
16:32:57 Information SqlScripts
16:32:57 Information SysAdmin.CacheSrv
16:32:57 Information SysAdmin.CacheSync
16:32:57 Information DirectoryCopy from: c:\acs\SysAdminKit
16:34:03 Information Finish copy files
16:34:03 Information Starting service SysAdmin.CacheSrv.Tx68173641
16:34:18 Information Starting service SysAdmin.CacheSrv.Tx68173641, success: true
16:34:18 Information ===== stopped upgrade for customer: 7e09cdfe-d1ad-4efc-a4f0-92c0eadbf3f4, Tx68173641  from  8.0.400.64 to 8.0.450.90
16:34:18 Information the end.
```

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

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

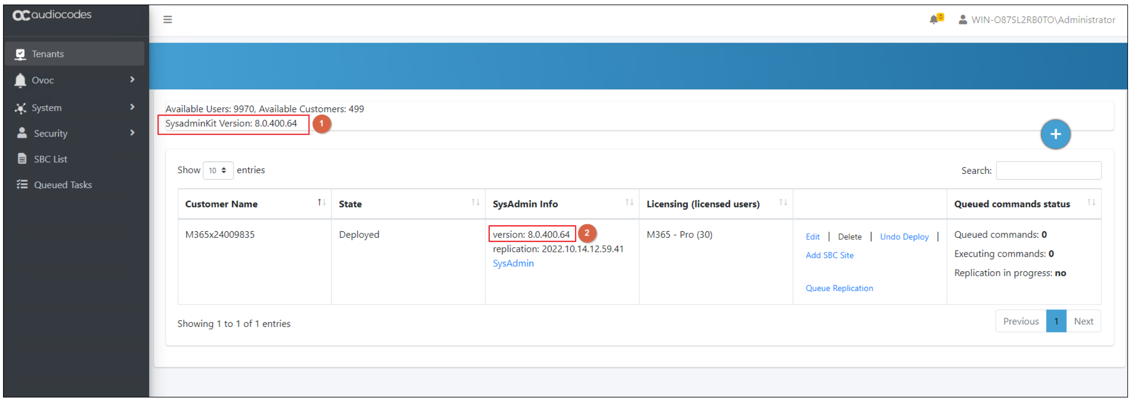


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

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


PS C:\Users\Administrator> _
```

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

5. In the Multitenant portal, open the Tenants page and verify that the following upgraded versions are displayed:

   - The wyUpdate version of the main UMP sysadminKit.
   - The SysAdminCustomerUpgrade version of the customers.



Available Users: 9970, Available Customers: 499
SysadminKit Version: 8.0.400.64

Show 10 entries

Search:

Customer Name	State	SysAdmin Info	Licensing (licensed users)		Queued commands status
M365x24009835	Deployed	version: 8.0.400.64 replication: 2022.10.14.12.59.41 SysAdmin	M365 - Pro (30)	Edit | Delete | Undo Deploy | Add SBC Site Queue Replication	Queued commands: **0** Executing commands: **0** Replication in progress: **no**

Showing 1 to 1 of 1 entries

Previous 1 Next

5 Post Upgrade Actions

This section describes the actions to perform following the upgrade:

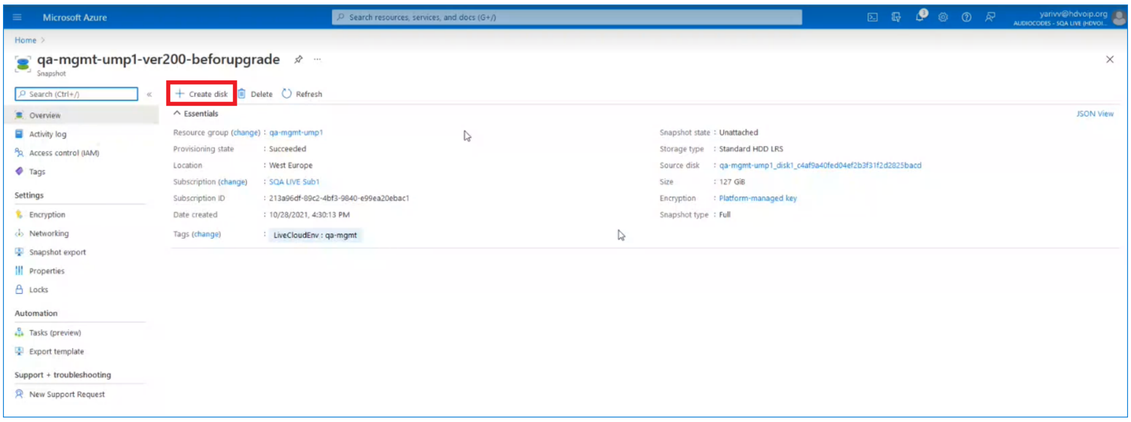
- Restoring UMP Snapshot below
- Upgrading M365 Connection to Token Authentication on page 30
- Updating Scripts on page 41
- SysAdmin Checklist on page 41
- Component Status Checklist on page 43

Restoring UMP Snapshot

This section describes how to create a new disk on the UMP VM and to restore the snapshot image created in Backing up UMP-365 – Disk Snapshot on page 4 to this disk (create a new VHD image for this disk).

➢ **Do the following:**

1. Open the new snapshot that you created in Backing up UMP-365 – Disk Snapshot on page 4 and click **Create Disk**.

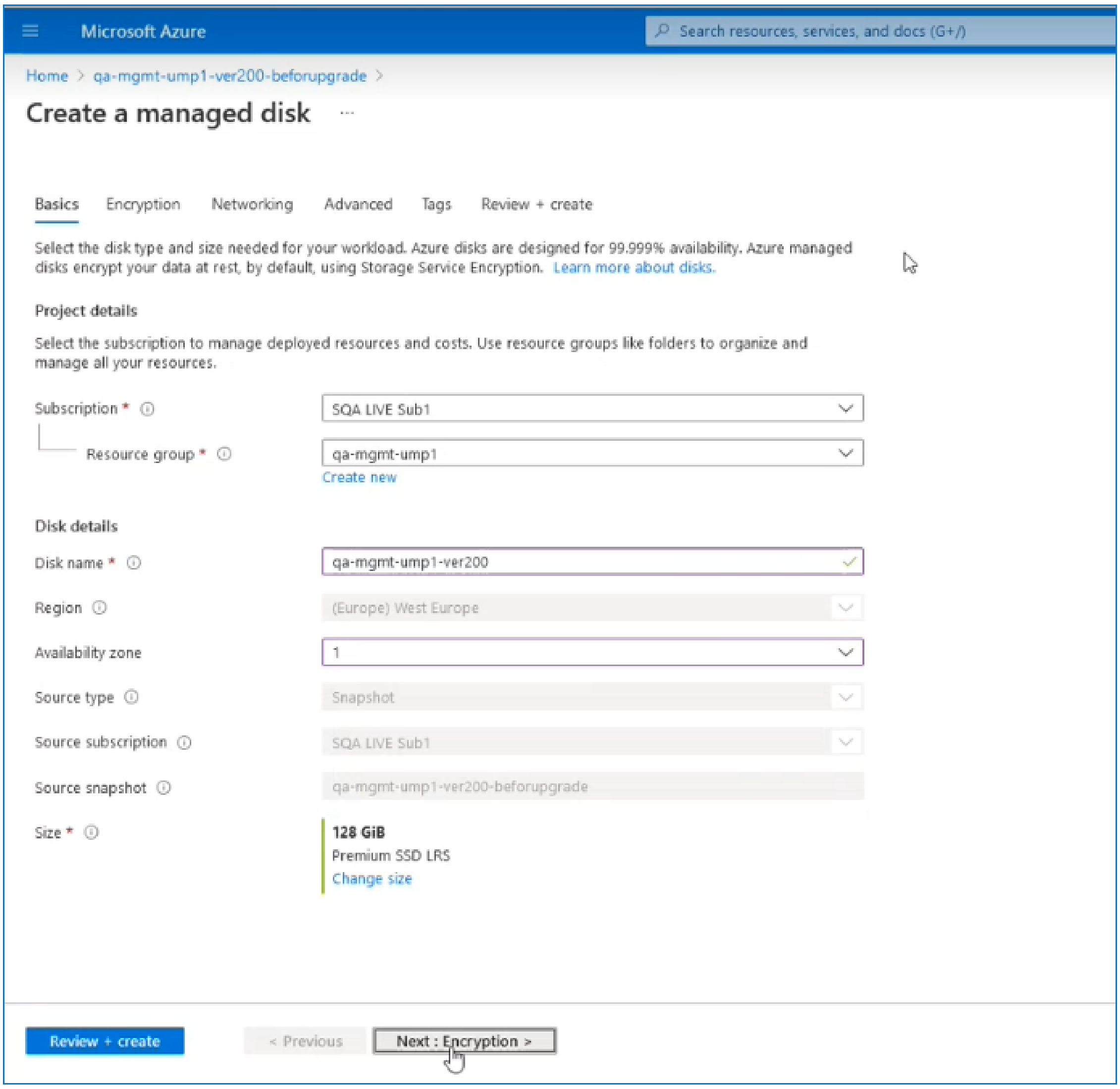


qa-mgmt-ump1-ver200-beforupgrade

Resource group (change) : qa-mgmt-ump1
Provisioning state : Succeeded
Location : West Europe
Subscription (change) : SQA LIVE Sub1
Subscription ID : 213a96df-89c2-4bf3-9840-e99ea20ebac1
Date created : 10/28/2021, 4:30:13 PM
Tags (change) : LiveCloudEnv : qa-mgmt

Snapshot state : Unattached
Storage type : Standard HDD LRS
Source disk : qa-mgmt-ump1_disk1_c4af9a40fed04ef2b3f31f2d2825bacd
Size : 127 GiB
Encryption : Platform-managed key
Snapshot type : Full

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


Microsoft Azure
Search resources, services, and docs (G+/)
Home > qa-mgmt-ump1-ver200-beforupgrade >

Create a managed disk

Basics
Encryption
Networking
Advanced
Tags
Review + create

Select the disk type and size needed for your workload. Azure disks are designed for 99.999% availability. Azure managed disks encrypt your data at rest, by default, using Storage Service Encryption. Learn more about disks.

Project details

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

Subscription *: SQA LIVE Sub1

Resource group *: qa-mgmt-ump1

Create new

Disk details

Disk name *: qa-mgmt-ump1-ver200

Region: (Europe) West Europe

Availability zone: 1

Source type: Snapshot

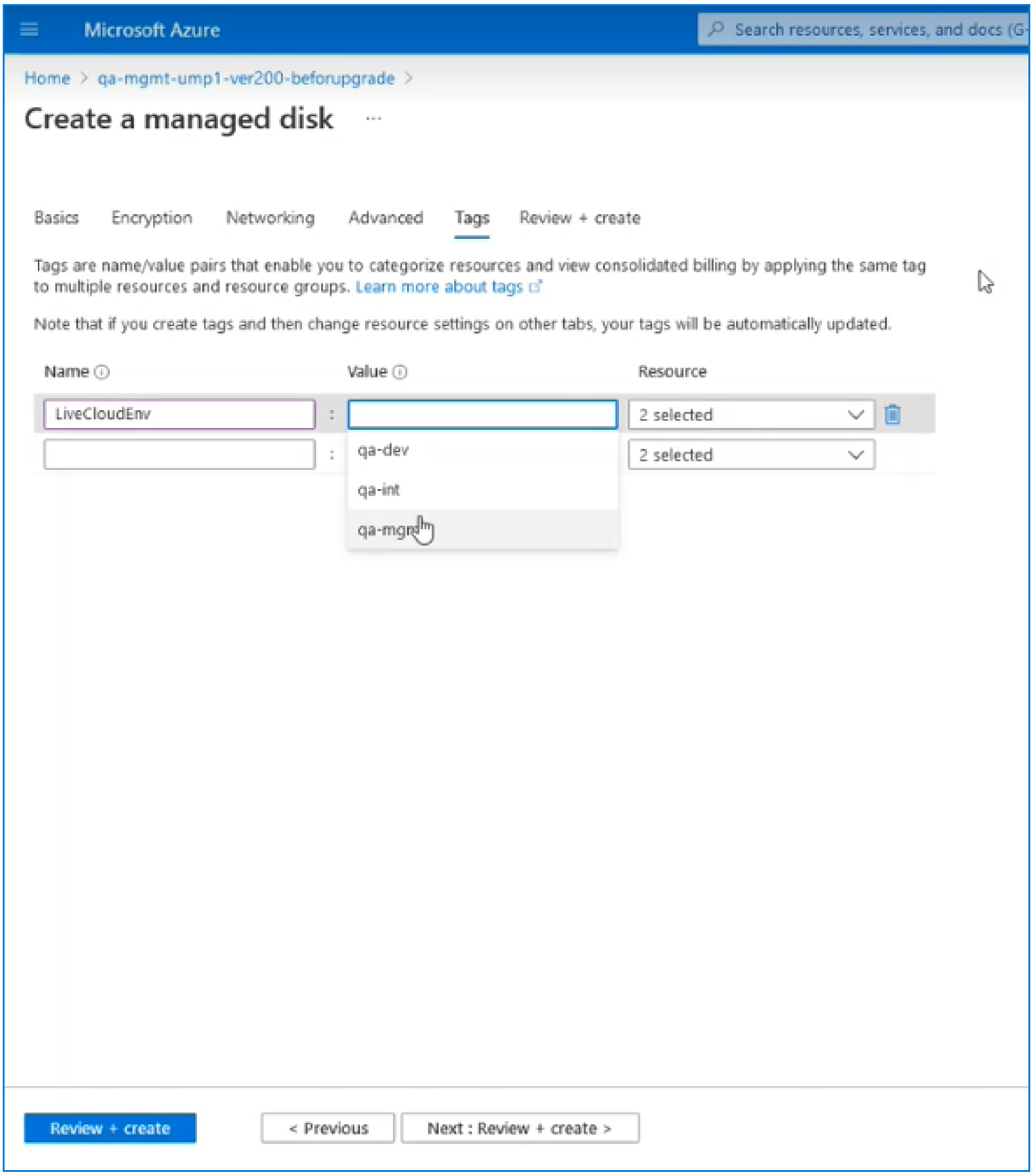
Source subscription: SQA LIVE Sub1

Source snapshot: qa-mgmt-ump1-ver200-beforupgrade

Size *: 128 GiB
Premium SSD LRS

Change size

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


Microsoft Azure
Search resources, services, and docs (G-
Home > qa-mgmt-ump1-ver200-beforupgrade >
Create a managed disk ...
Basics
Encryption
Networking
Advanced
Tags
Review + create

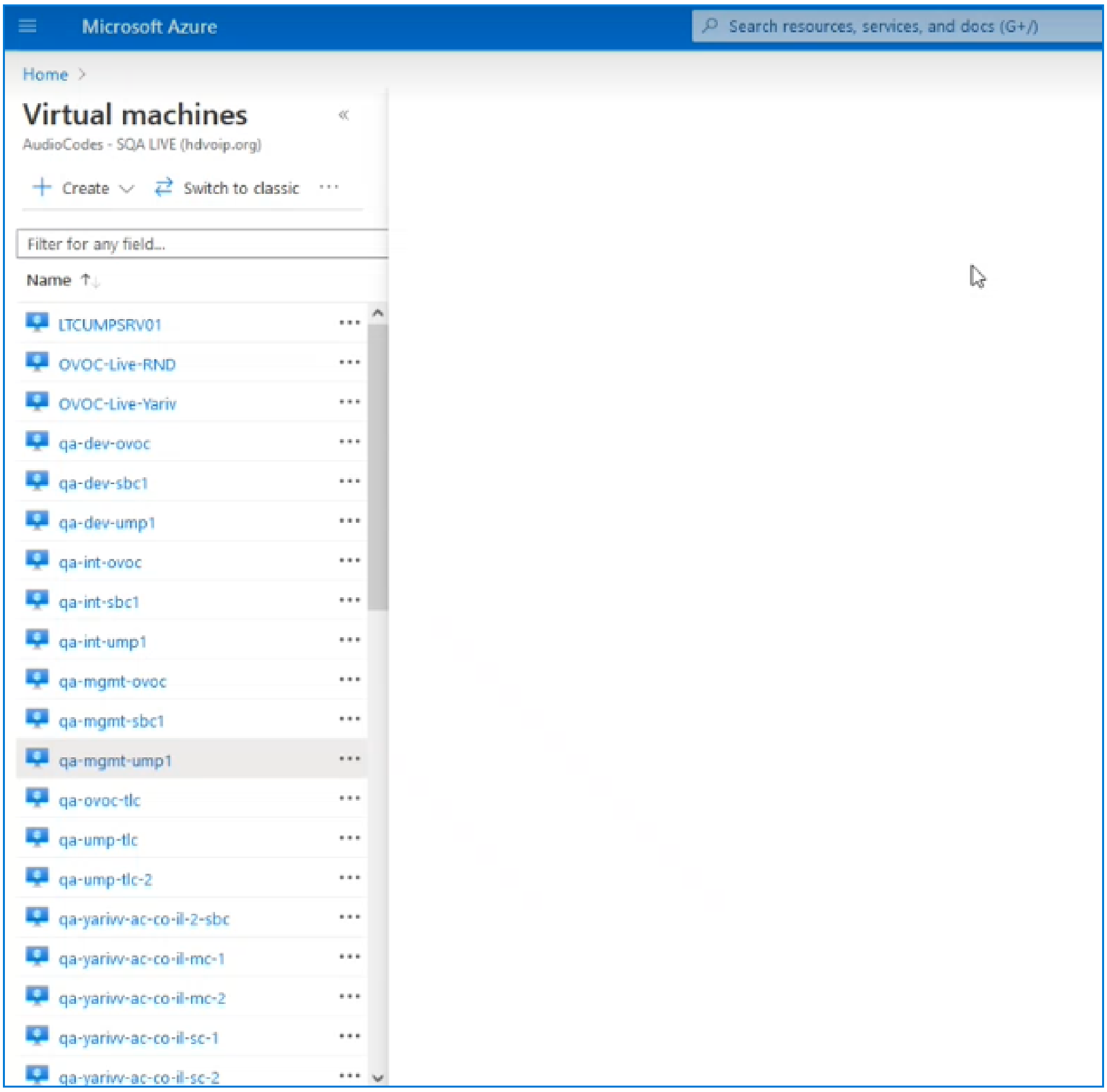
Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

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

Name	Value	Resource
LiveCloudEnv		2 selected
		2 selected

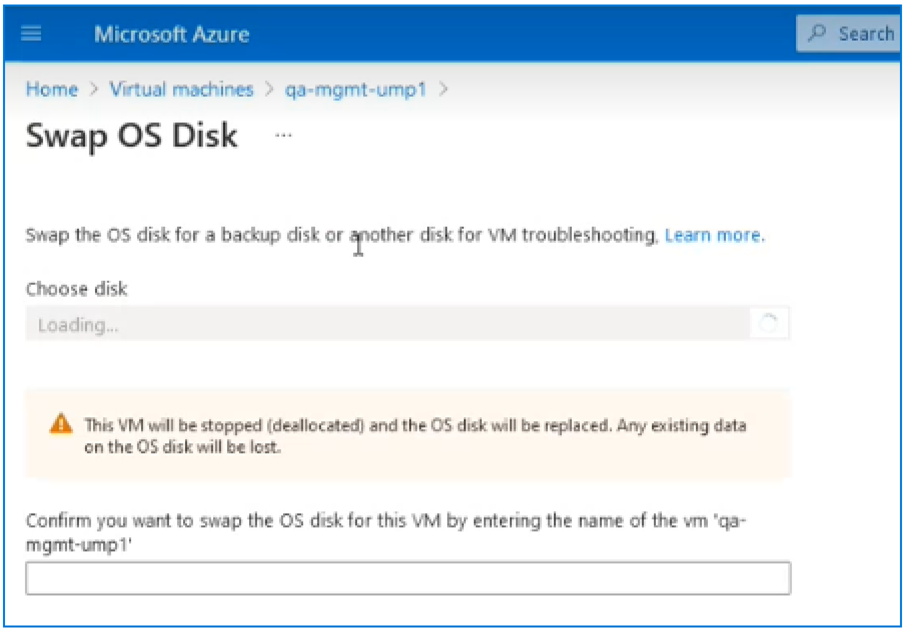
4. Click **Review + create**.

5. Navigate to the UMP Virtual Machine.



LTCUMPSRV01
OVOC-Live-RND
OVOC-Live-Yariv
qa-dev-ovoc
qa-dev-sbc1
qa-dev-ump1
qa-int-ovoc
qa-int-sbc1
qa-int-ump1
qa-mgmt-ovoc
qa-mgmt-sbc1
qa-mgmt-ump1
qa-ovoc-tlc
qa-ump-tlc
qa-ump-tlc-2
qa-yariw-ac-co-il-2-sbc
qa-yariw-ac-co-il-mc-1
qa-yariw-ac-co-il-mc-2
qa-yariw-ac-co-il-sc-1
qa-yariw-ac-co-il-sc-2

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



Swap the OS disk for a backup disk or another disk for VM troubleshooting. Learn more.

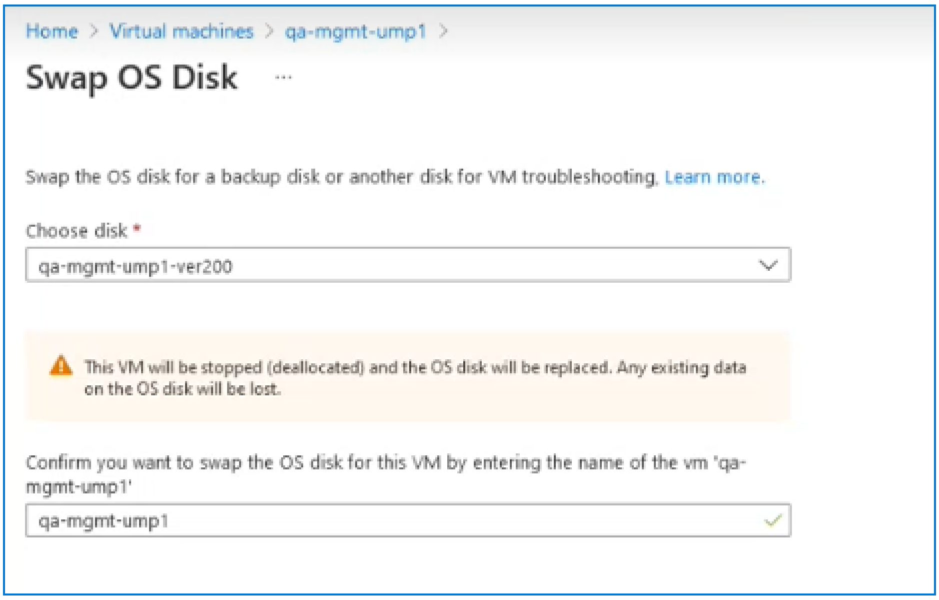
Choose disk

Loading...

This VM will be stopped (deallocated) and the OS disk will be replaced. Any existing data on the OS disk will be lost.

Confirm you want to swap the OS disk for this VM by entering the name of the vm 'qa-mgmt-ump1'

7. From the Choose Disk drop-down list, choose the snapshot that you created in Backing up UMP-365 – Disk Snapshot on page 4 (in this example "qa-mgmt-ump1-ver200").



Swap the OS disk for a backup disk or another disk for VM troubleshooting. Learn more.

Choose disk * qa-mgmt-ump1-ver200

This VM will be stopped (deallocated) and the OS disk will be replaced. Any existing data on the OS disk will be lost.

Confirm you want to swap the OS disk for this VM by entering the name of the vm 'qa-mgmt-ump1'

qa-mgmt-ump1

8. Enter the UMP VM name (in this example "qa-mgmt-ump1").

9. When the Swap Disk action completes, open the UMP interface and check that all customer data is displayed.

Upgrading M365 Connection to Token Authentication

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

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

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

- **Password-based authentication and Token authentication:** A Microsoft Graph access token is claimed based on the configured user name and password. For implementing this option, select the **Grant Consent** option in the Microsoft 365 Settings screen (see procedure below).
- **Token-only authentication:** A Microsoft Graph access token is claimed directly, triggered by an email link sent to the customer. For implementing this option, select the **Switch to auth token** option in the Microsoft 365 Settings screen (see Switching to Token Authentication on page 34). This is the **recommended** the method.

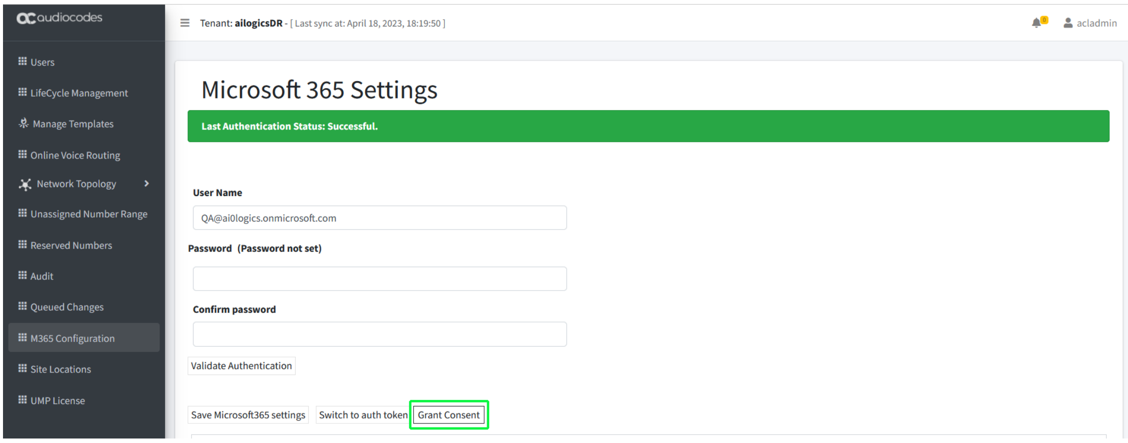
Once consent is provided, an Enterprise application is created on the customer Azure tenant including the following permissions:

- Access Microsoft Teams and Skype for Business as the signed in user

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

➢ To secure Token-based connection with Grant Consent:

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



Tenant: **ailogicsDR** - [Last sync at: April 18, 2023, 18:19:50]

Microsoft 365 Settings

Last Authentication Status: Successful.

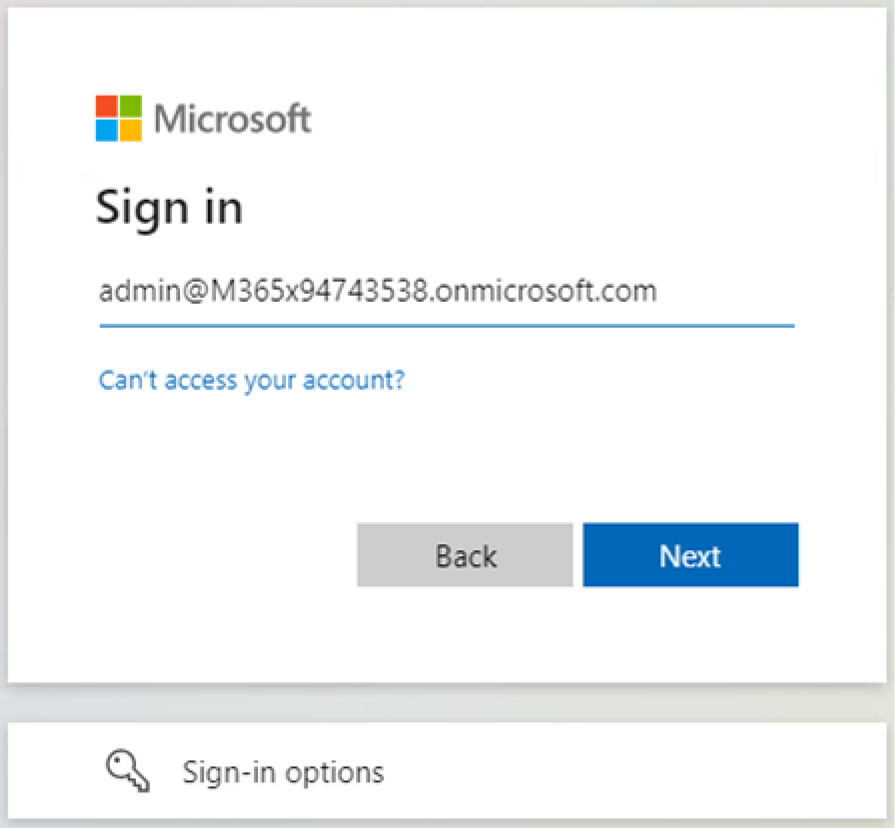
User Name

QA@ai0logics.onmicrosoft.com

Password (Password not set)

Confirm password

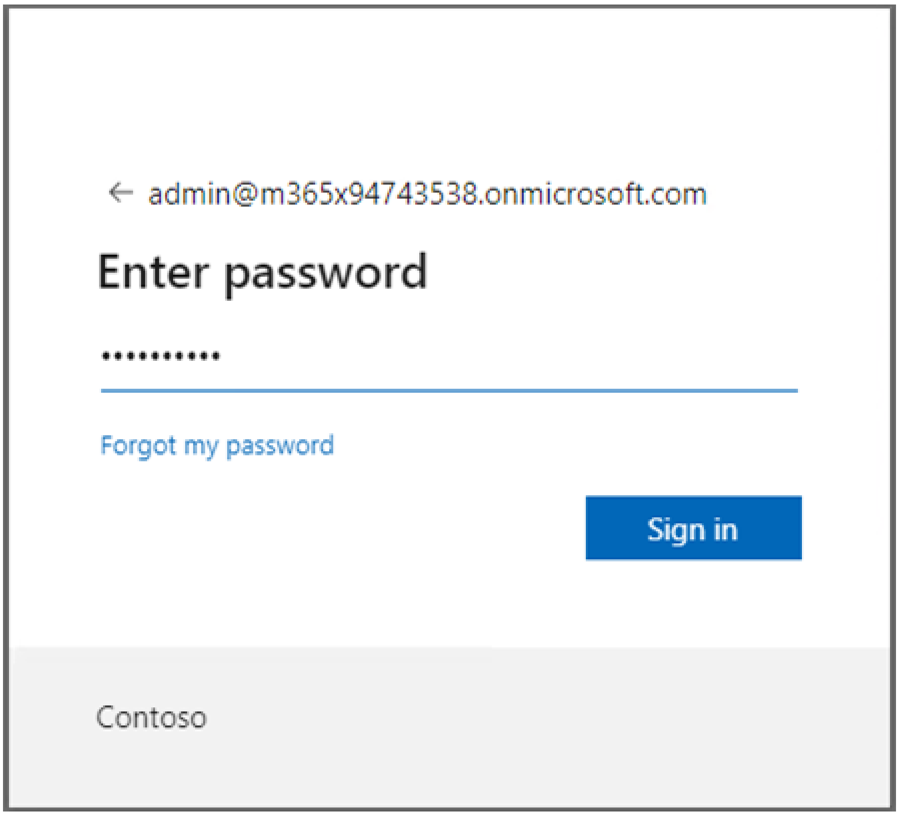
2. Click **Grant Consent**.



Sign in

admin@M365x94743538.onmicrosoft.com

Can't access your account?



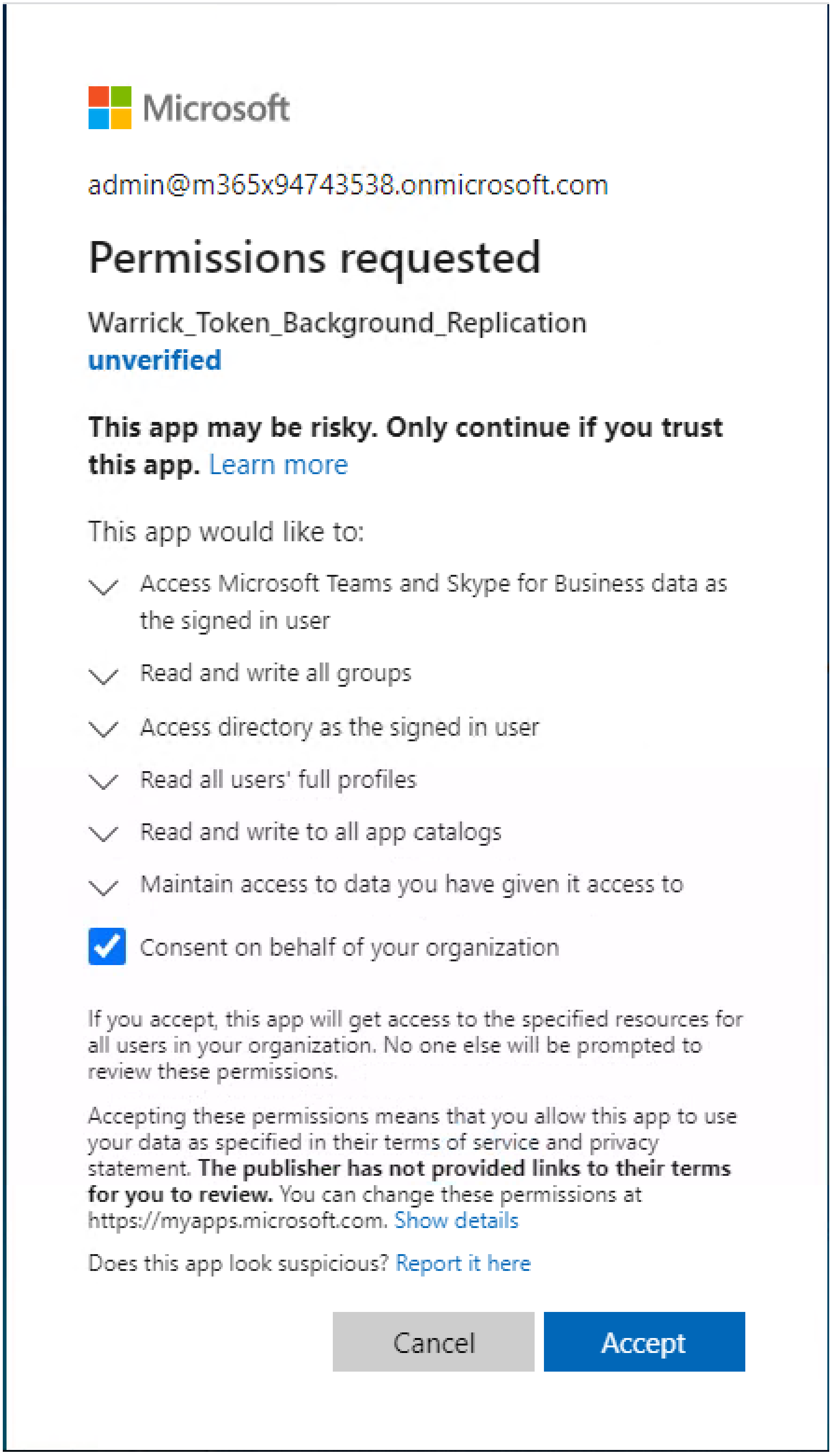
← admin@m365x94743538.onmicrosoft.com

Enter password

•••••••••••

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

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



admin@m365x94743538.onmicrosoft.com

Permissions requested

Warrick_Token_Background_Replication
unverified

This app may be risky. Only continue if you trust this app. Learn more

This app would like to:

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

☑ Consent on behalf of your organization

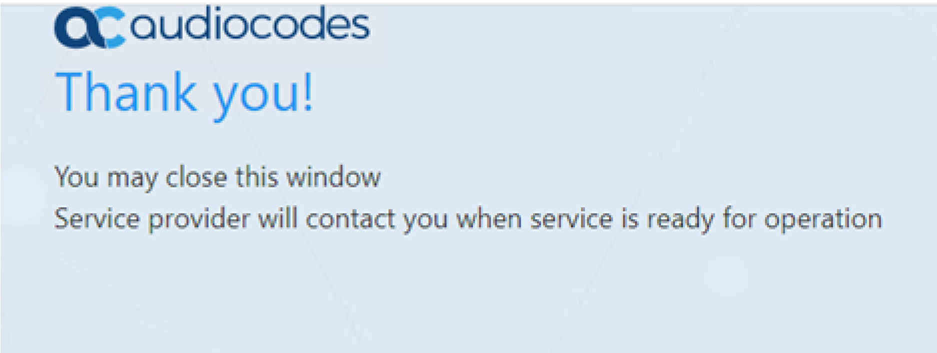
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

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

Does this app look suspicious? Report it here

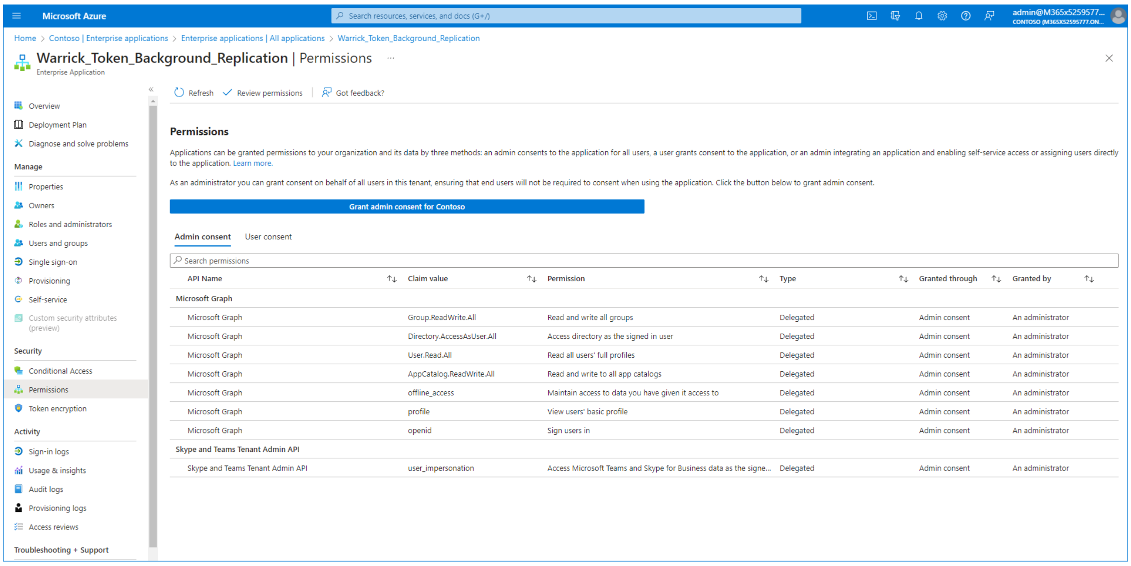
b. Click "Consent on behalf of your organization" and then click **Accept**.

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



Thank you!

You may close this window
Service provider will contact you when service is ready for operation



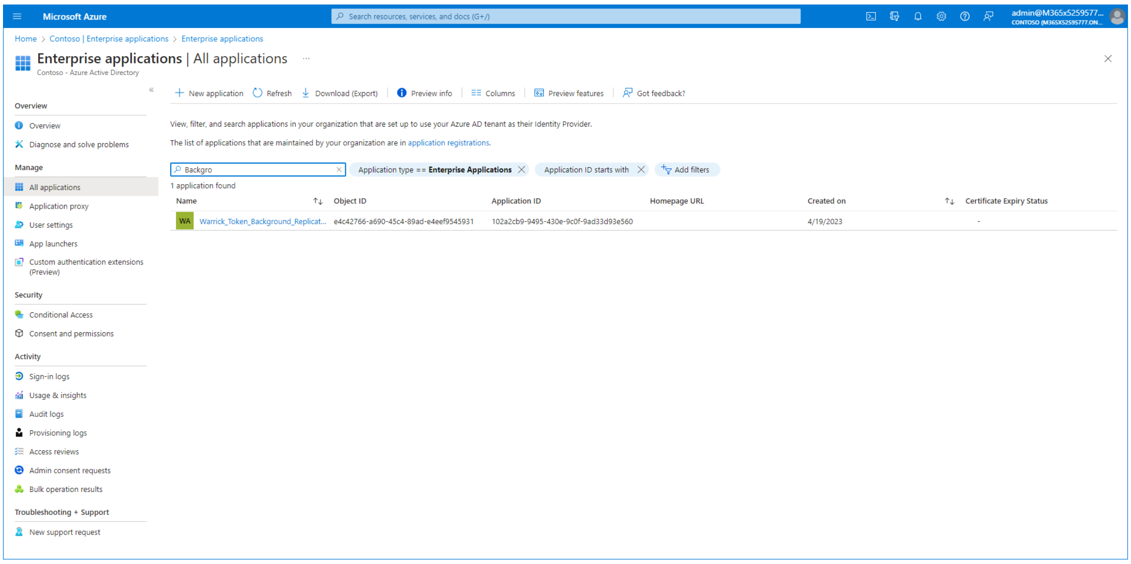
Warrick_Token_Background_Replication | Permissions
Enterprise Application

Permissions

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

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

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



Enterprise applications | All applications
Contoso - Azure Active Directory

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

The list of applications that are maintained by your organization are in application registrations.

Backgro
Application type == **Enterprise Applications**
Application ID starts with

1 application found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status
WA Warrick_Token_Background_Replicat...	e4c42766-a690-45c4-89ad-e4eef9545931	102a2cb9-9495-430e-9c0f-9ad33d93e560		4/19/2023	-

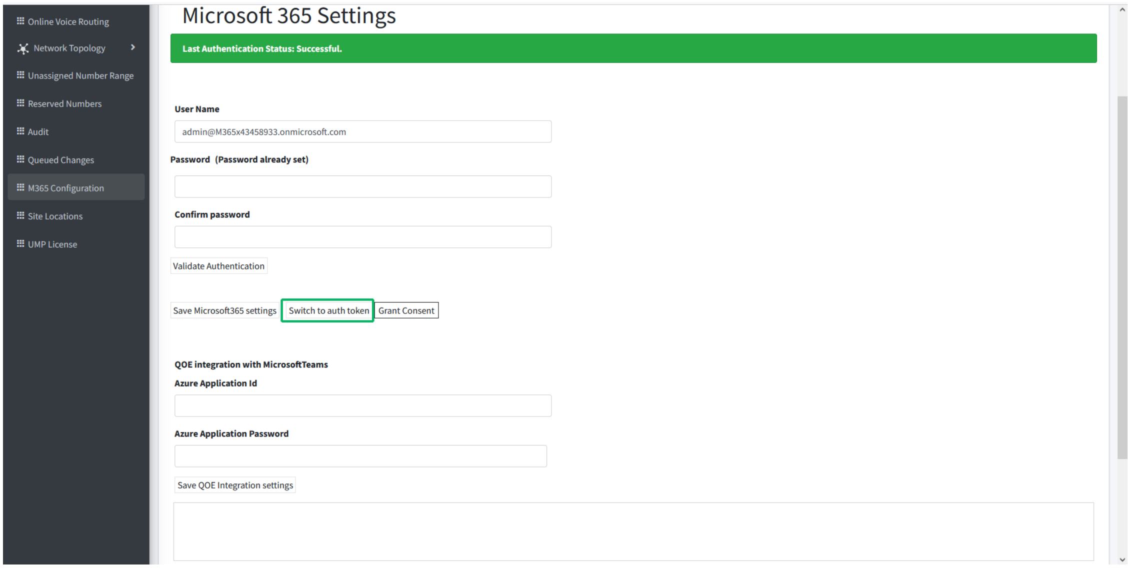
Switching to Token Authentication

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

⚠ This is recommended method for securing connection to Microsoft 365.

➢ To switch to token authentication:

1. In the **Microsoft 365 Settings** screen, click **Validate Authentication** to ensure current token is valid. Last Authentication Status: Successful is displayed.



Microsoft 365 Settings

Last Authentication Status: Successful.

User Name
admin@M365x43458933.onmicrosoft.com

Password (Password already set)

Confirm password

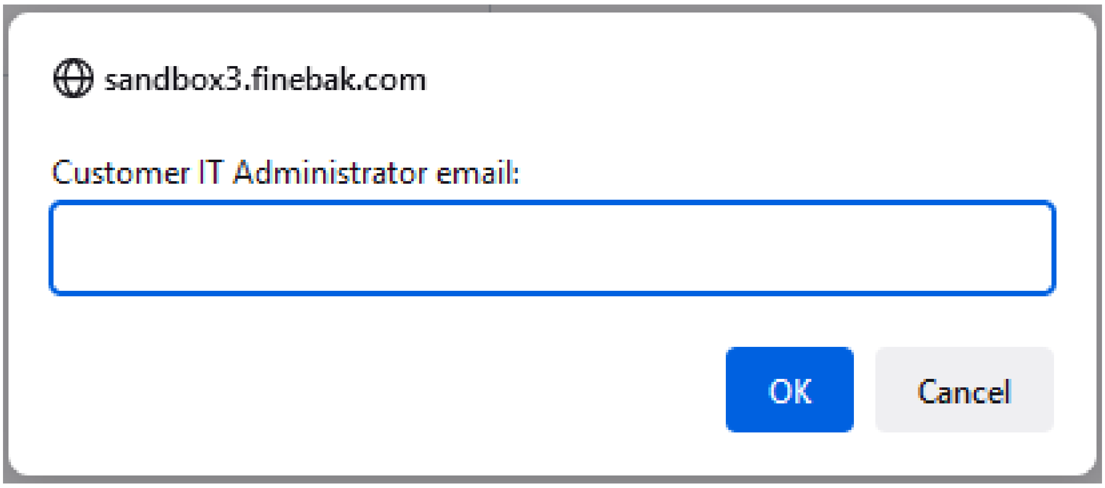
QOE integration with MicrosoftTeams

Azure Application Id

Azure Application Password

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

   The following dialog is displayed.

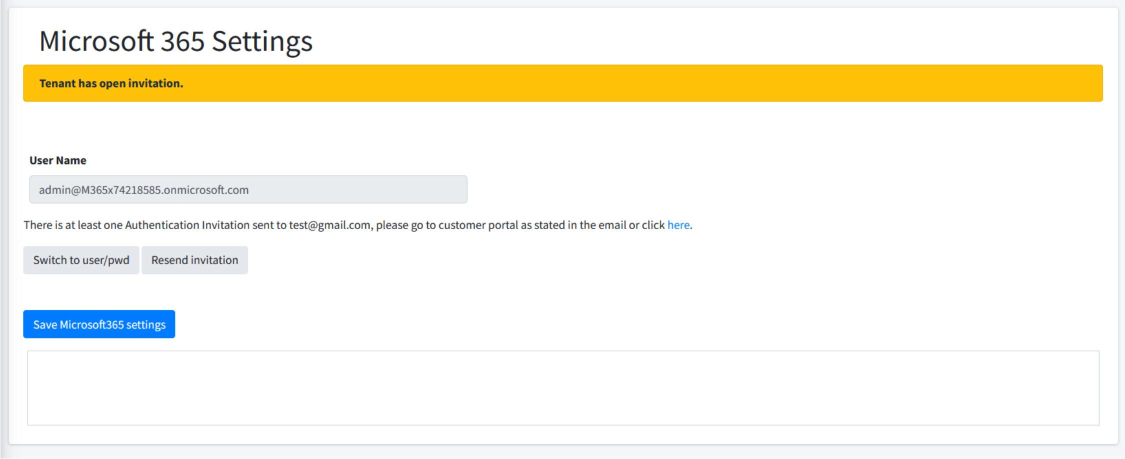


sandbox3.finebak.com

Customer IT Administrator email:

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

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



Microsoft 365 Settings

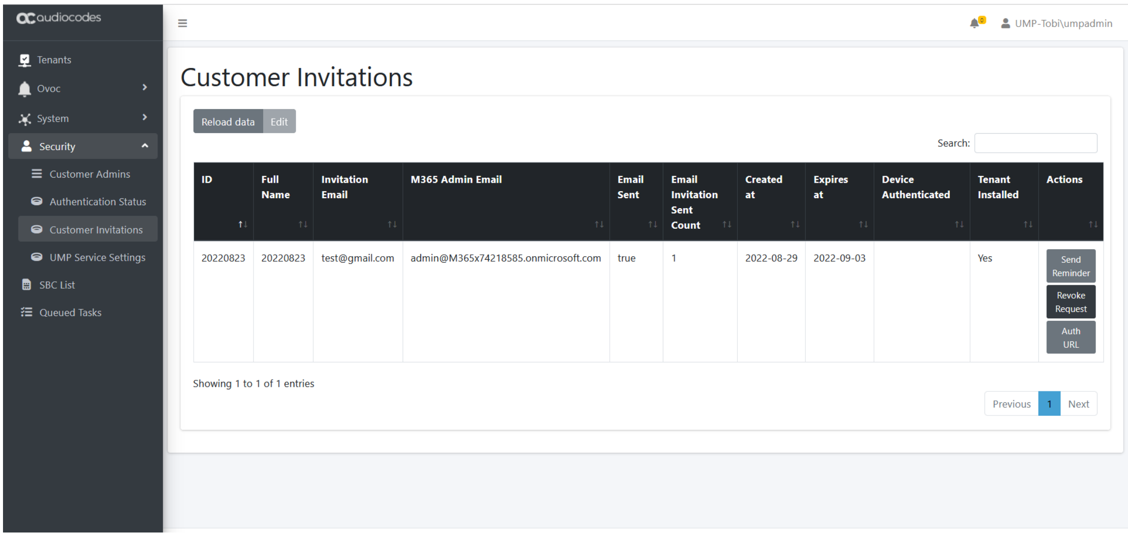
Tenant has open invitation.

User Name

admin@M365x74218585.onmicrosoft.com

There is at least one Authentication Invitation sent to test@gmail.com, please go to customer portal as stated in the email or click here.

4. In the Main Tenant interface, open the Customer Invitations screen (see Customer Invitations). View the Customer Invitation sent to the email address entered above.

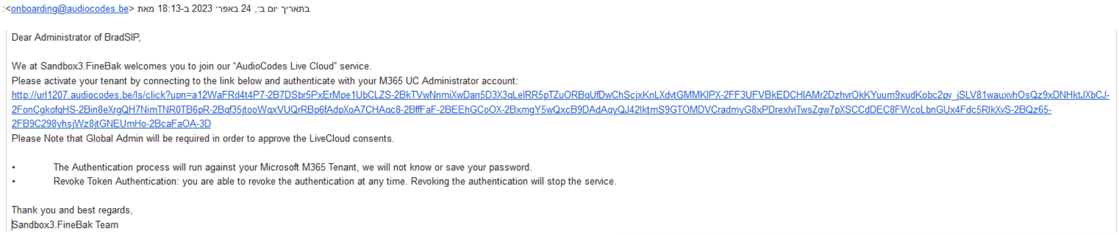


Customer Invitations

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

Showing 1 to 1 of 1 entries

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



בתאריך יום ב׳, 24 באפר׳ 2023 ב-18:13 מאת <onboarding@audiocodes.be>:

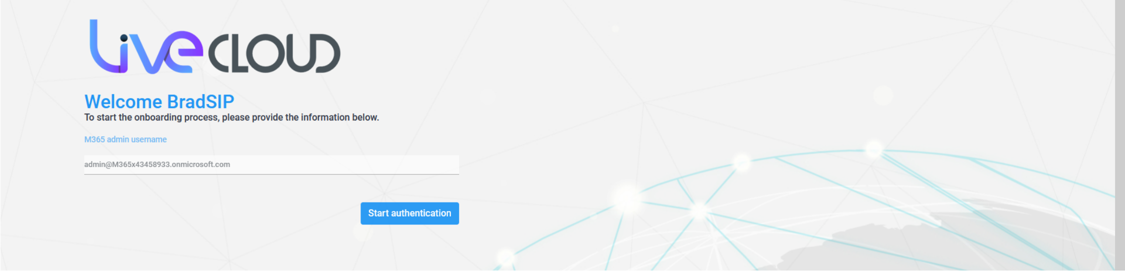
Dear Administrator of BradSIP,

We at Sandbox3.FineBak welcomes you to join our "AudioCodes Live Cloud" service.
Please activate your tenant by connecting to the link below and authenticate with your M365 UC Administrator account:
http://url1207.audiocodes.be/ls/click?upn=a12WaFRd4t4P7-2B7DSbr5PxErMpe1UbCLZS-2BkTVwNnmiXwDan5D3X3qLeIRR5pTZuORBqUfDwChScjxKnLXdvtGMMKIPX-2FF3UFVBkEDCHIAMr2DzhvrOkKYuum9xudKobc2pv_jSLV81wauxvhOsQz9xDNHktJXbCJ-2FonCgkofqHS-2Bin8eXrgQH7NimTNR0TB6pR-2Bqf35jtooWqxVUQrRBp6fAdpXoA7CHAqc8-2BffFaF-2BEEhGCoOX-2BxmgY5wQxcB9DAdAqyQJ42lktmS9GTOMDVCradmyG8xPDrexlviTwsZgw7pXSCCdDEC8FWcoLbnGUx4Fdc5RlkXvS-2BQz65-2FB9C298yhsjWz8jtGNEUmHo-2BcaFaOA-3D
Please Note that Global Admin will be required in order to approve the LiveCloud consents.

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

Thank you and best regards,
Sandbox3.FineBak Team

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



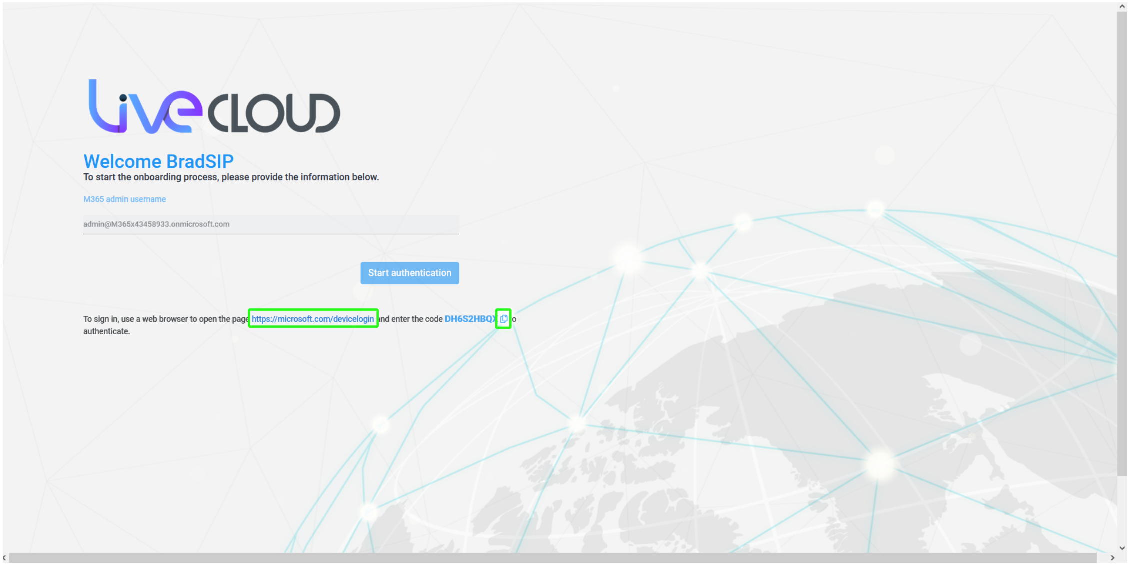
Welcome BradSIP

To start the onboarding process, please provide the information below.

M365 admin username

admin@M365x43458933.onmicrosoft.com

6. Click **Start authentication**.



Welcome BradSIP

To start the onboarding process, please provide the information below.

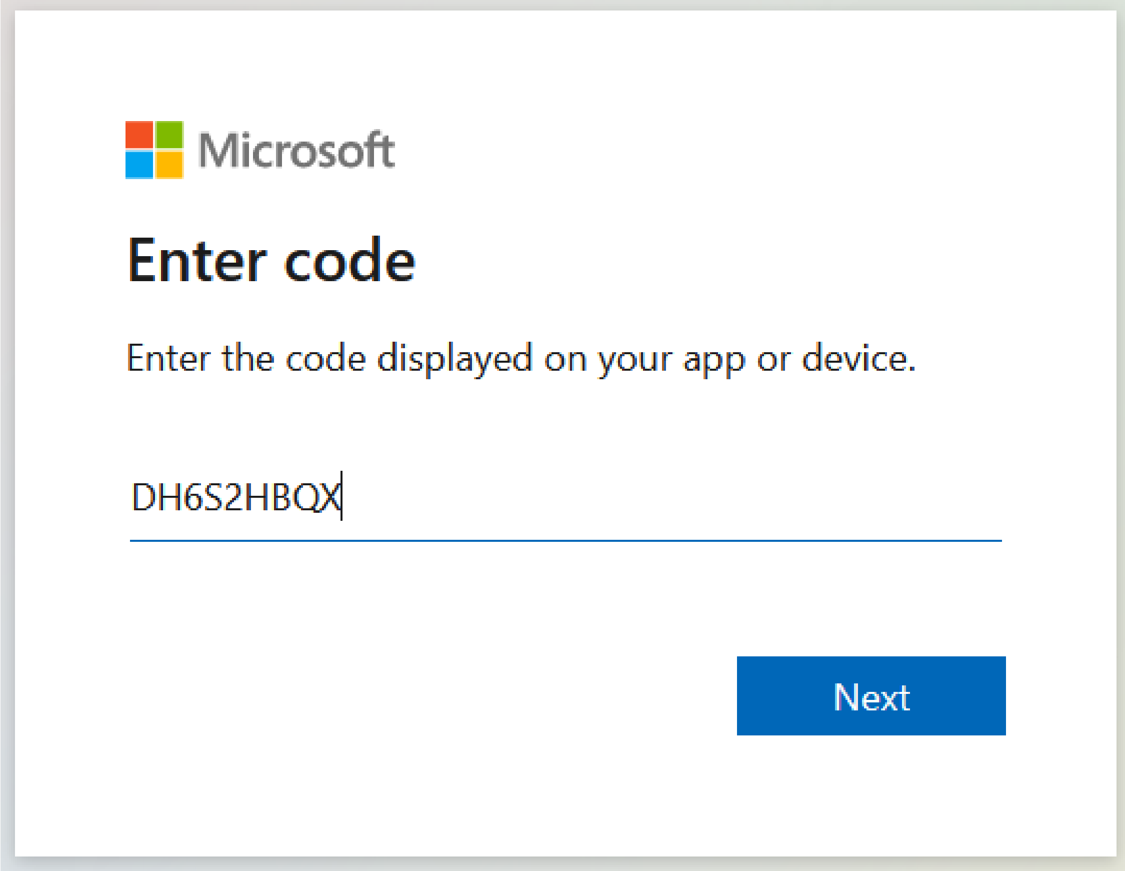
M365 admin username

admin@M365x43458933.onmicrosoft.com

To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code DH6S2HBQX to authenticate.

7. Copy the displayed code to clipboard.

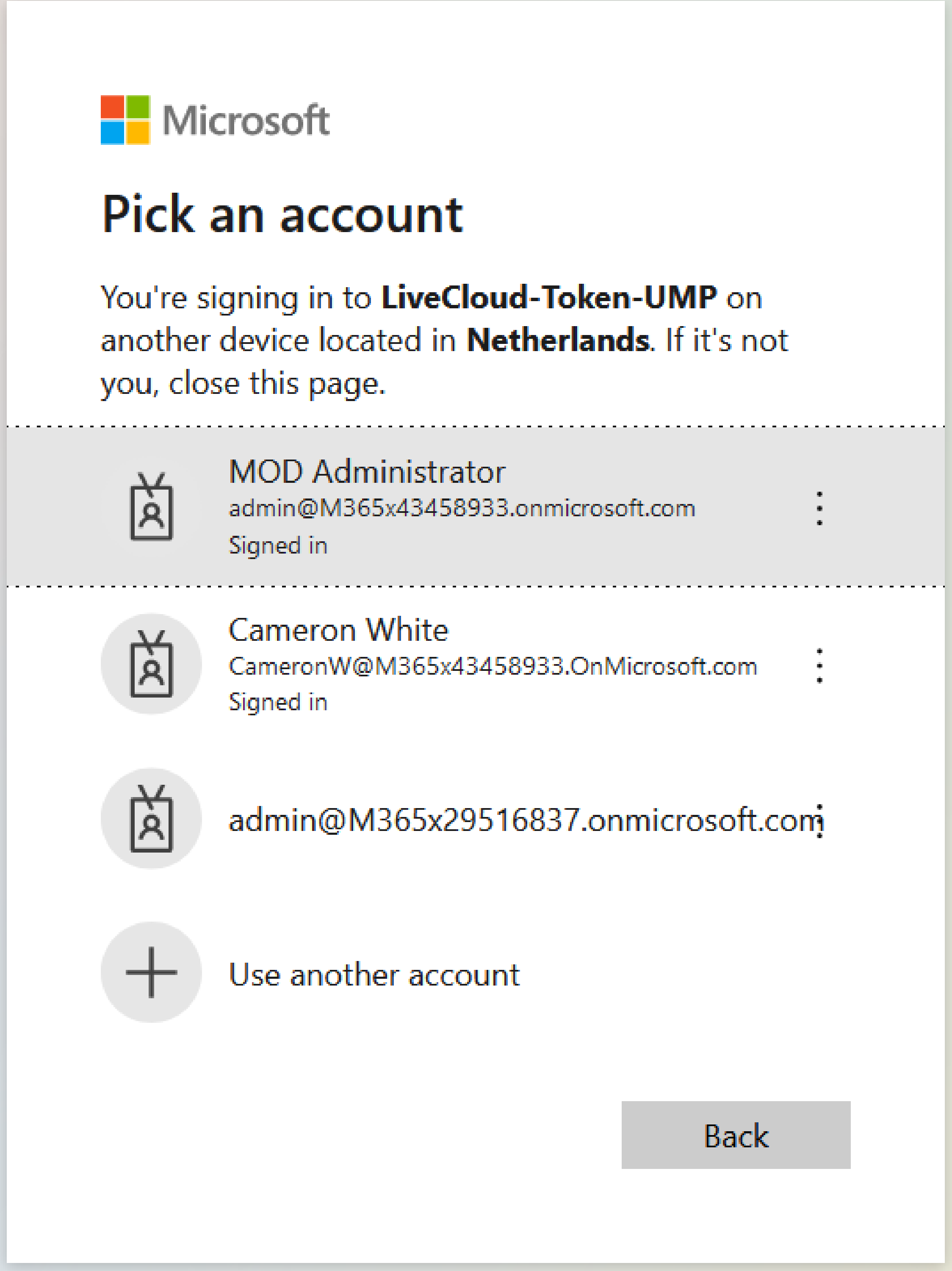
8. Open the web browser link shown below the **Start authentication** button.



Enter code

Enter the code displayed on your app or device.

DH6S2HBQX



Microsoft

Pick an account

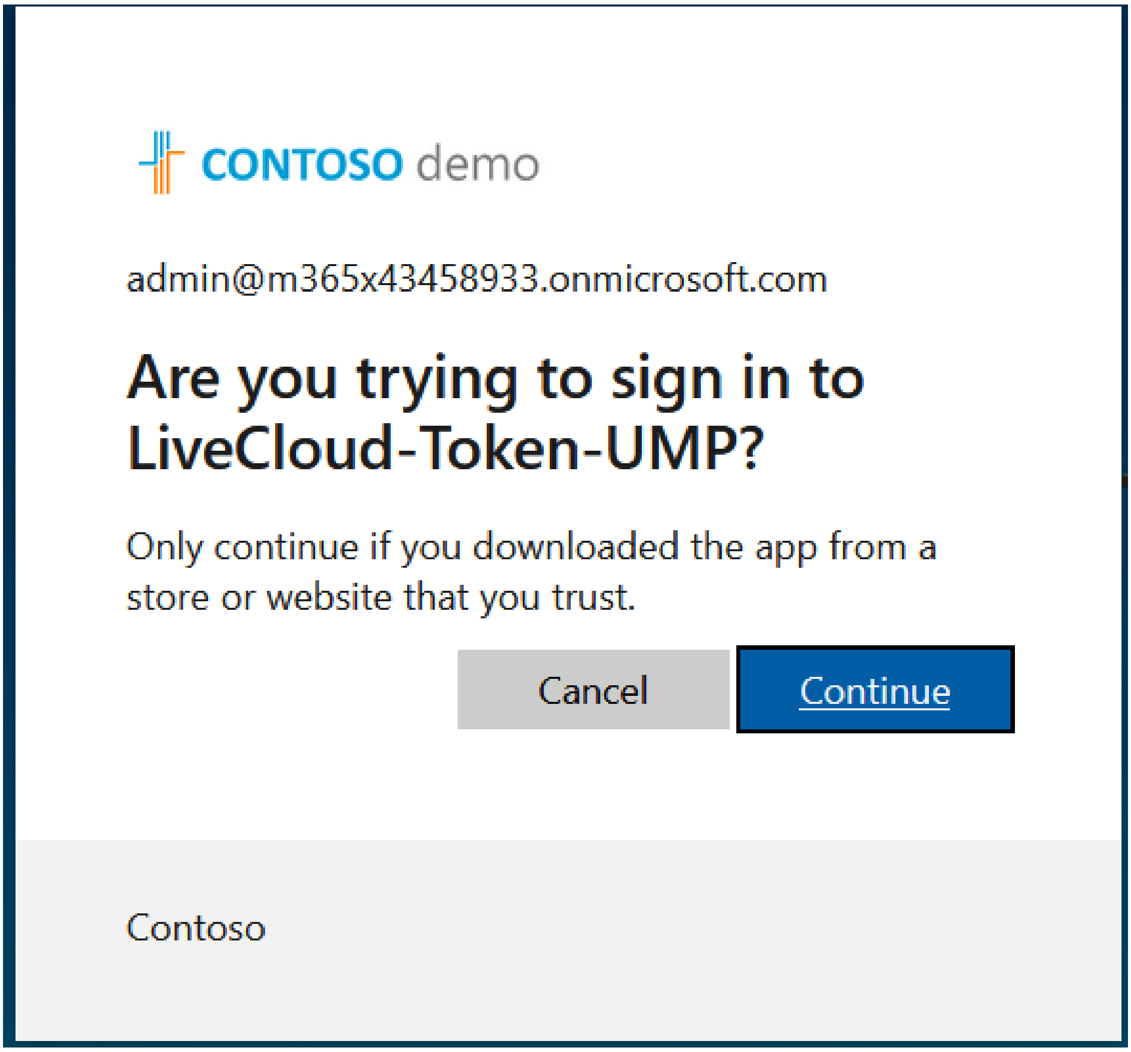
You're signing in to **LiveCloud-Token-UMP** on another device located in **Netherlands**. If it's not you, close this page.

MOD Administrator
admin@M365x43458933.onmicrosoft.com
Signed in

Cameron White
CameronW@M365x43458933.OnMicrosoft.com
Signed in

admin@M365x29516837.onmicrosoft.com

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

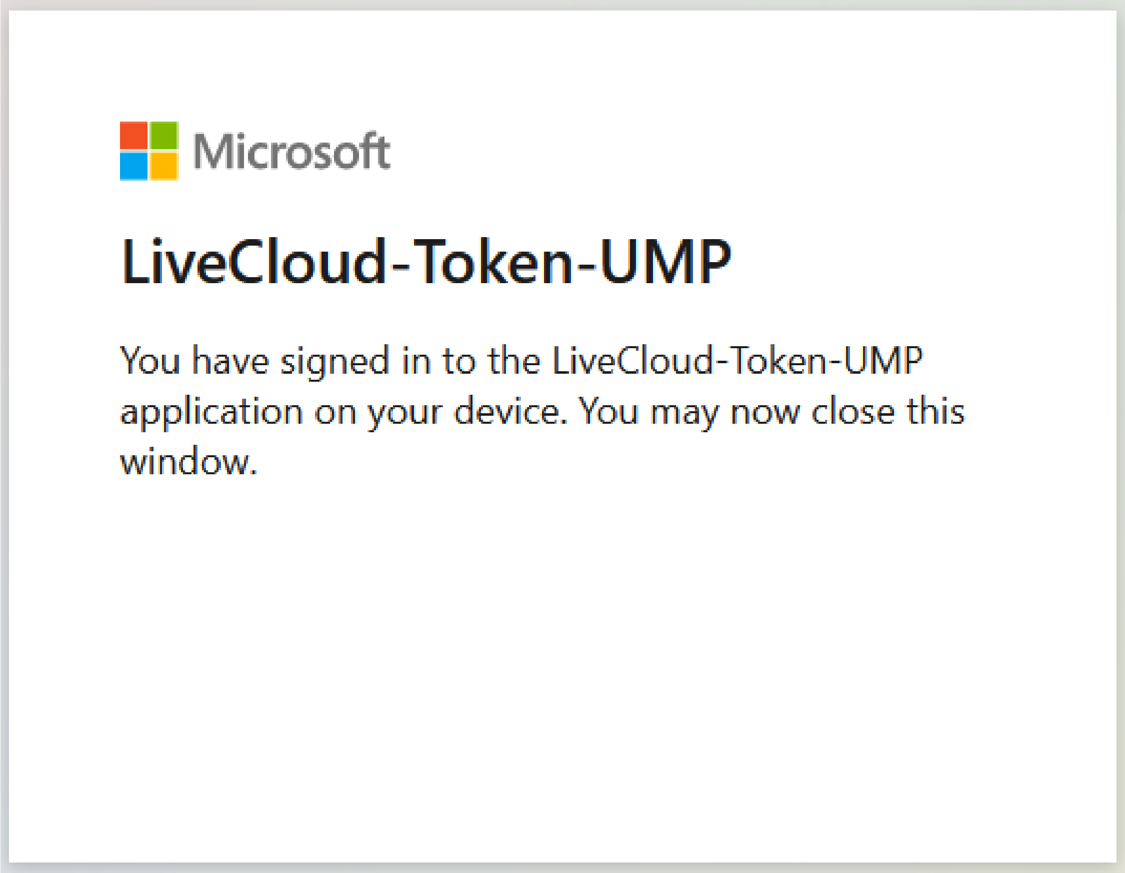


admin@m365x43458933.onmicrosoft.com

Are you trying to sign in to LiveCloud-Token-UMP?

Only continue if you downloaded the app from a store or website that you trust.

10. Click **Continue**.

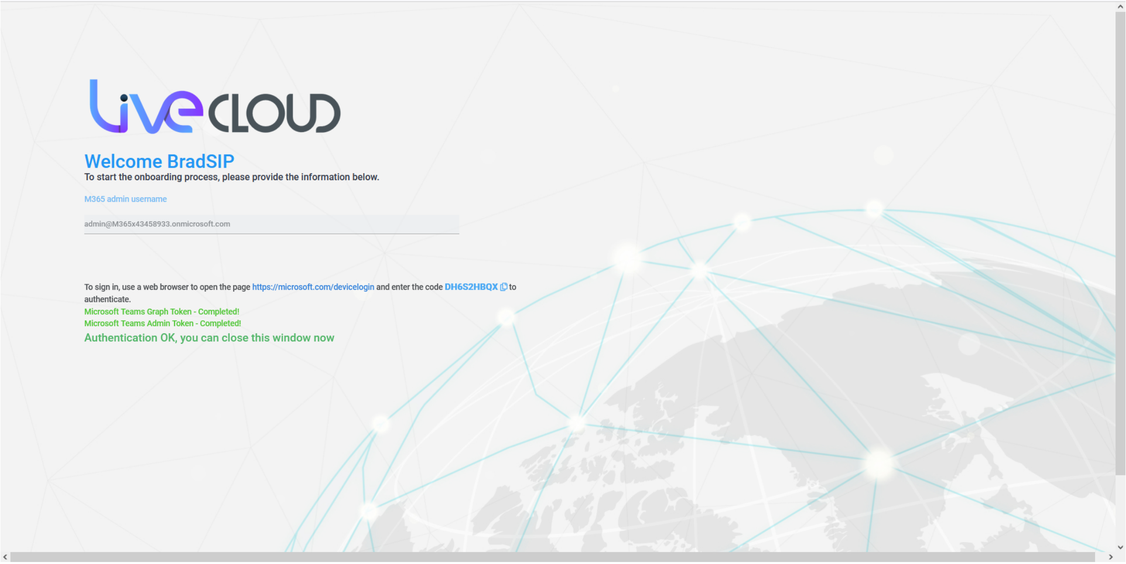


Microsoft

LiveCloud-Token-UMP

You have signed in to the LiveCloud-Token-UMP application on your device. You may now close this window.

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



Welcome BradSIP

To start the onboarding process, please provide the information below.

M365 admin username

admin@M365x43458933.onmicrosoft.com

To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code DH6S2HBQX to authenticate.

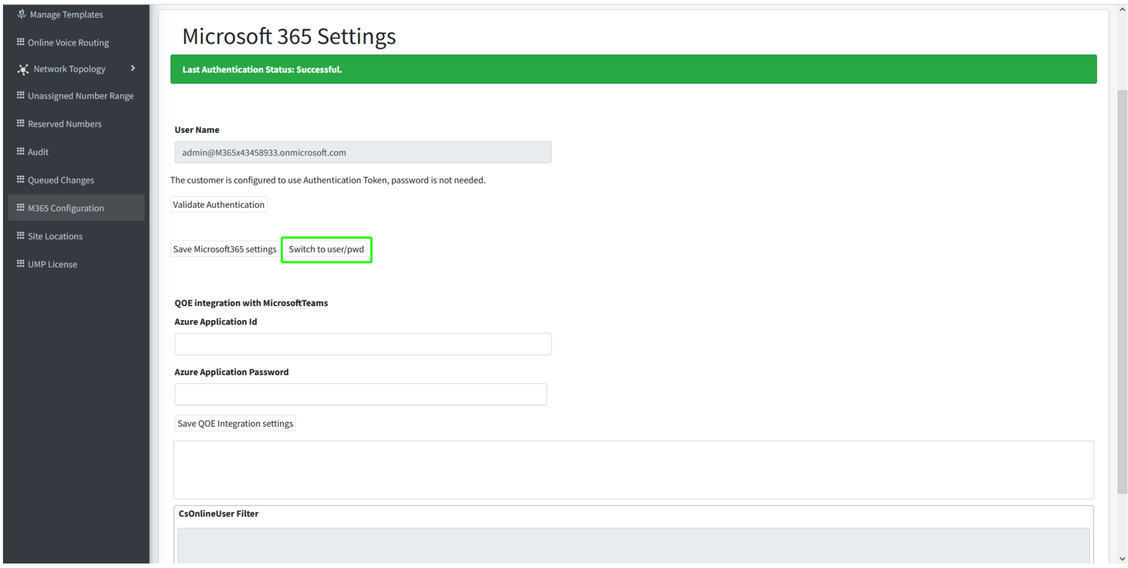
Microsoft Teams Graph Token - Completed!

Microsoft Teams Admin Token - Completed!

Authentication OK, you can close this window now

12. Close the above window.

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



Microsoft 365 Settings

Last Authentication Status: Successful.

User Name

admin@M365x43458933.onmicrosoft.com

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

Validate Authentication

Save Microsoft365 settings | Switch to user/pwd

QOE integration with MicrosoftTeams

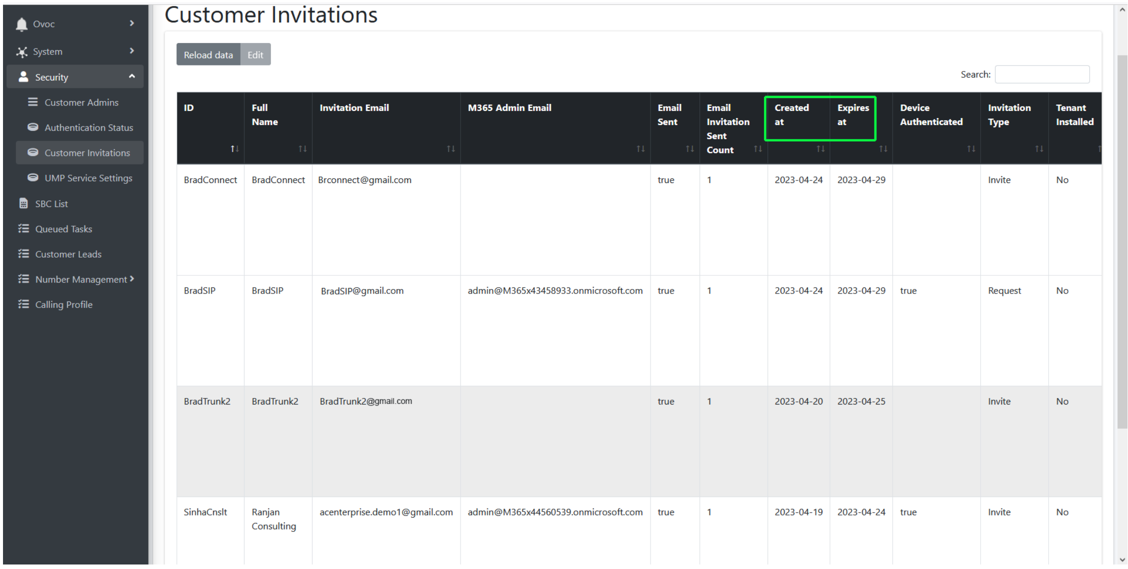
Azure Application Id

Azure Application Password

Save QOE Integration settings

CsOnlineUser Filter

14. In the Main Tenant interface, open the Customer Invitations screen (see Customer Invitations), view the "Created at" and "Expires at" of the claimed token.



Customer Invitations

ID	Full Name	Invitation Email	M365 Admin Email	Email Sent	Email Invitation Sent Count	Created at	Expires at	Device Authenticated	Invitation Type	Tenant Installed
BradConnect	BradConnect	Brconnect@gmail.com		true	1	2023-04-24	2023-04-29		Invite	No
BradSIP	BradSIP	BradSIP@gmail.com	admin@M365x43458933.onmicrosoft.com	true	1	2023-04-24	2023-04-29	true	Request	No
BradTrunk2	BradTrunk2	BradTrunk2@gmail.com		true	1	2023-04-20	2023-04-25		Invite	No
SinhaCnslt	Ranjan Consulting	acenterprise.demo1@gmail.com	admin@M365x44560539.onmicrosoft.com	true	1	2023-04-19	2023-04-24	true	Invite	No

Updating Scripts

Use the script compare feature to verify that the template scenario scripts have the correct syntax notation (see Scenario Scripts Templates Page on page 70).

⚠ Template scripts containing incorrect syntax will not be executed.

SysAdmin Checklist

Ensure the following prior to upgrade:

- Ensure the Authentication Status menu has been populated with the Azure Application Registration credentials (see Authentication Status on page 55):

  - For LiveCloud and LiveExpress setups, the credentials are provided by AudioCodes.
  - For standalone UMP-365 devices, the customer manages the application in their Azure environment.

- All Tenants using Username and Password must upgrade to Token-based authentication based on their existing user and password using the Grant Consent option (see Grant Consent).

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

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

- If a UMP server is hardened (via strict Security policies) and services are required to be whitelisted, add the following services (created when upgrading to version 8.0.450) to the whitelist :

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

  See Managing the Replication Cycle for details on the above services.

- Microsoft Graph PowerShell module is installed by the installation script (the AzureAD PowerShell module is approaching end-of-service). Consequently, ensure that the security Anti-virus does not restrict the installation of the Graph module.

- Ensure that the SQL Server Management Studio's server collation is correctly set to **SQL_ Latin1_General_CP1_CI_AS**. If not, then a re installation of SQL server is required to change the Server Collation.

  SQL Server collation determines how the server compares and sorts character data, such as text, in a database. Collation refers to the set of rules that dictate how characters are compared and sorted based on their language, culture, and other properties. If the collation of a database or table is not set correctly, it can cause unexpected behavior when performing string operations, such as sorting, grouping, and filtering data. For example, if the collation is not set properly, it may sort character data in a way that is not consistent with the expectations of the user or application. Furthermore, if there are different collations used across different databases or tables, it may cause issues when joining or comparing data between them. This can result in errors, data loss, or incorrect results. Therefore, it is important to choose the appropriate collation for a database or table, based on the needs of the application and the language and cultural context in which the data will be used.

Ensure all databases are backed up before removing the SQL server, so that they can be correctly restored (see Backing up UMP-365 – Disk Snapshot on page 4.).

Component Status Checklist

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

Interface	Menu Navigation Path	Check	Configuration Action
OVOC	Network > Device > Manage	☐	Verify the UMP-365 Device Status is Active in the Devices table (see Device Status on page 46).
		☐	Open the Managed Device page, select device , click Show and verify that “UMP Management” displays **Connected** (see Device Status on page 46).
OVOC	Open Device Page for UMP Tenant	☐	Verify Customers Deployment State is **Deployed**. See Deployment Status on page 51.
		☐	Verify for each customer that the SysAdminKit version is the latest version. See Upgrading Main UMP-365 Tenant on page 14.
UMP-365	System > License	☐	Verify "MultiTenant Version: latest version. See Configuring License on page 53.
		☐	Verify available license is not missing.
	System > Invitation Settings	☐	Verify Customer Authentication Portal Url is set to: https://<UMP_ FQDN>/authenticate. See Configuring Invitation Settings on page 53.
	Security > Authentication Status	☐	Verify that the Client ID and Secret ID are provided by the Synchronization app registration (check PMP site).
		☐	Verify that the Redirect Url is set to: https://<UMP_ FQDN>/authenticate/OAuth2Callback

Interface	Menu Navigation Path	Check	Configuration Action
			⚠ Verify that the same redirect Uri is configured for the Synchronization App registration. See Authentication Status.
	SBC List	☐	Verify that the SBC exists. See Managing SBC Devices on page 61.
OVOC	Network > Customers	☐	Verify the Customers Status and Deployment status is OK in the Devices table. See Managing SBC Devices on page 61.
		☐	Verify "Enabled" is checked.
		☐	Verify the "total number of DIDs and "users count.". See Customer Details Quick Glance.
		☐	Verify that the Azure Tenant Id exists.
		☐	Navigate to "Provider side" and verify the "Users Count" is displayed. See Customer Details Quick Glance.
	Customer Actions Menu > Edit Customer	☐	■ Edit User, update a parameter (e.g. Department) and then verify that the change has been implemented (see Editing Users on page 51. ■ To enforce the Teams update, in the Multitenant interface, navigate to Queue Changes > Process All (see Queued Tasks (Background Replication). ■ To verify users, see User Details. ■ To verify users in Microsoft Teams: Open **https://admin.Teams.microsoft.com**
UMP	Site Locations	☐	Verify that the SBC is in "Deployed"

Interface	Menu Navigation Path	Check	Configuration Action
Multitenant portal			status; click Add/Edit SBC Prefix (see Manage Site Locations).
		□	Verify that the DIDs are configured for the customer (see Upload Dial Plan Rules from Managed SBC Device on page 66 and Configure Dial Plans).
		□	Add DID and verify that it has been successfully added on the SBC.

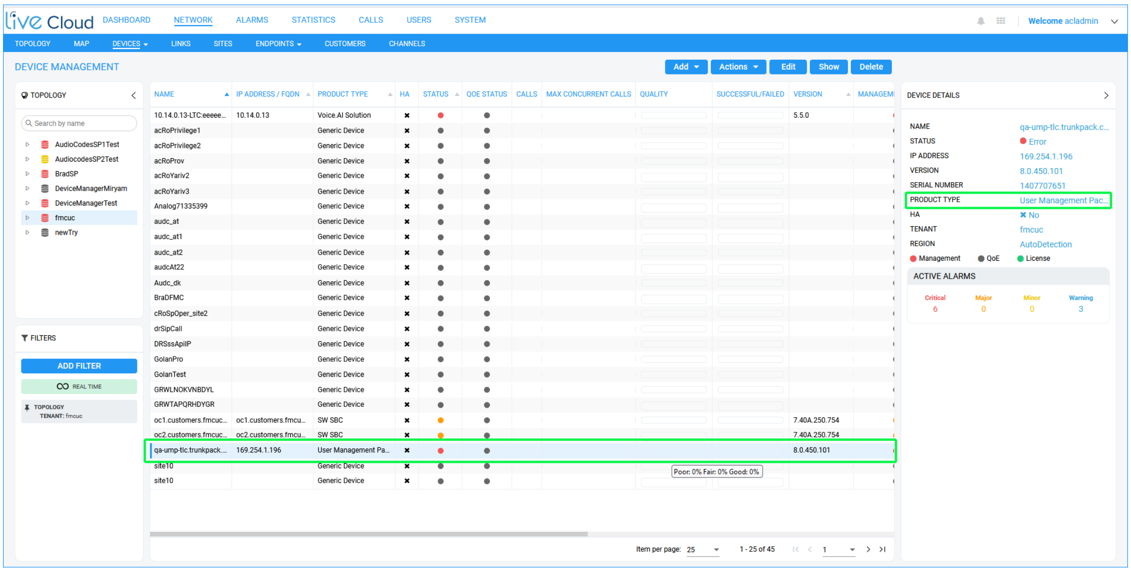
6 Appendix

This appendix includes the following references to the checklist in Component Status Checklist on page 43:

- Device Status below
- Deployment Status on page 51
- Editing Users on page 51
- Configuring License on page 53
- Configuring Invitation Settings on page 53
- Authentication Status
- Managing SBC Devices on page 61
- Managing Site Locations
- Scenario Scripts Templates Page on page 70

Device Status

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



DEVICE MANAGEMENT

TOPOLOGY
TENANT: fmcuc

NAME	IP ADDRESS / FQDN	PRODUCT TYPE	HA	STATUS	QOE STATUS	CALLS	MAX CONCURRENT CALLS	QUALITY	SUCCESSFUL/FAILED	VERSION	MANAGEMI
10.14.0.13-LTC:eeeee...	10.14.0.13	Voice.AI Solution	✖	●	●					5.5.0	●
acRoPrivilege1		Generic Device	✖	●	●						●
acRoPrivilege2		Generic Device	✖	●	●						●
acRoProv		Generic Device	✖	●	●						●
acRoYariv2		Generic Device	✖	●	●						●
acRoYariv3		Generic Device	✖	●	●						●
Analog71335399		Generic Device	✖	●	●						●
audc_at		Generic Device	✖	●	●						●
audc_at1		Generic Device	✖	●	●						●
audc_at2		Generic Device	✖	●	●						●
audcAt22		Generic Device	✖	●	●						●
Audc_dk		Generic Device	✖	●	●						●
BraDFMC		Generic Device	✖	●	●						●
cRoSpOper_site2		Generic Device	✖	●	●						●
drSipCall		Generic Device	✖	●	●						●
DRSssApiIP		Generic Device	✖	●	●						●
GolanPro		Generic Device	✖	●	●						●
GolanTest		Generic Device	✖	●	●						●
GRWLNOKVNBDYL		Generic Device	✖	●	●						●
GRWTAPQRHDYGR		Generic Device	✖	●	●						●
oc1.customers.fmcuc...	oc1.customers.fmcu...	SW SBC	✖	●	●					7.40A.250.754	●
oc2.customers.fmcuc...	oc2.customers.fmcu...	SW SBC	✖	●	●					7.40A.250.754	●
qa-ump-tlc.trunkpack....	169.254.1.196	User Management Pa...	✖	●	●					8.0.450.101	●
site10		Generic Device	✖	●	●						●
site10		Generic Device	✖	●	●						●

Poor: 0% Fair: 0% Good: 0%

Item per page: 25 1 - 25 of 45 1

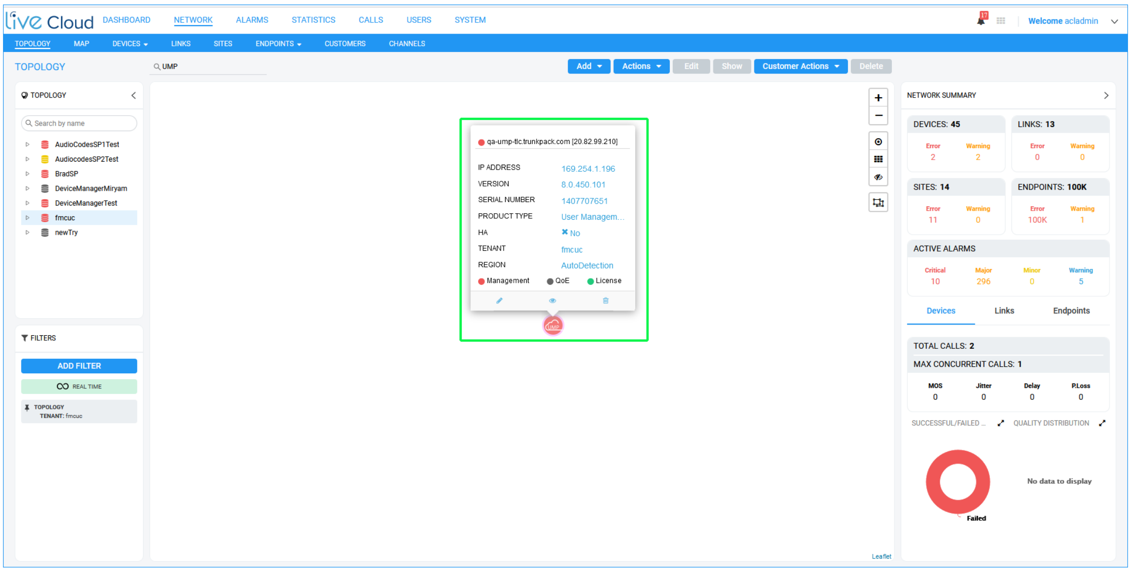
DEVICE DETAILS

NAME	qa-ump-tlc.trunkpack.c...
STATUS	● Error
IP ADDRESS	169.254.1.196
VERSION	8.0.450.101
SERIAL NUMBER	1407707651
PRODUCT TYPE	User Management Pac...
HA	✖ No
TENANT	fmcuc
REGION	AutoDetection

● Management ● QoE ● License

ACTIVE ALARMS

Critical	Major	Minor	Warning
6	0	0	3



TOPOLOGY

UMP

TOPOLOGY

- AudioCodesSP1Test
- AudiocodesSP2Test
- BradSP
- DeviceManagerMiryam
- DeviceManagerTest
- fmcuc
- newTry

FILTERS

TOPOLOGY
TENANT: fmcuc

● qa-ump-tlc.trunkpack.com [20.82.99.210]

IP ADDRESS	169.254.1.196
VERSION	8.0.450.101
SERIAL NUMBER	1407707651
PRODUCT TYPE	User Managem...
HA	✖ No
TENANT	fmcuc
REGION	AutoDetection

● Management ● QoE ● License

NETWORK SUMMARY

DEVICES: 45		LINKS: 13	
Error	Warning	Error	Warning
2	2	0	0

SITES: 14		ENDPOINTS: 100K	
Error	Warning	Error	Warning
11	0	100K	1

ACTIVE ALARMS

Critical	Major	Minor	Warning
10	296	0	5

Devices Links Endpoints

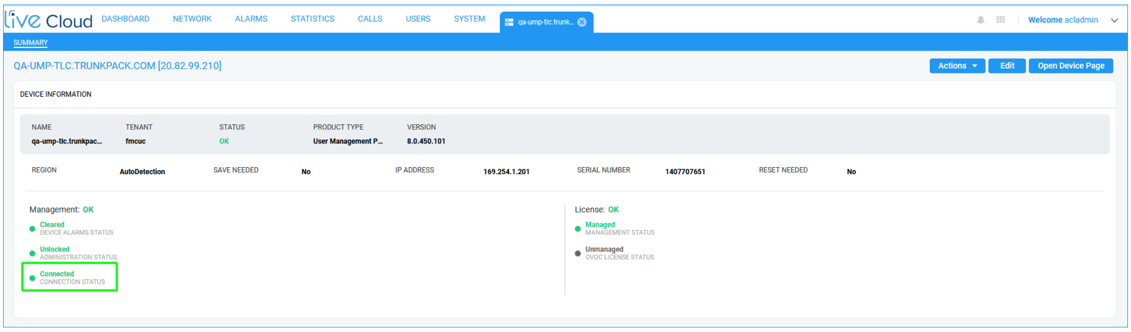
TOTAL CALLS: 2

MAX CONCURRENT CALLS: 1

MOS	Jitter	Delay	P.Loss
0	0	0	0

SUCCESSFUL/FAILED ... QUALITY DISTRIBUTION

No data to display



QA-UMP-TLC.TRUNKPACK.COM [20.82.99.210]

DEVICE INFORMATION

NAME	TENANT	STATUS	PRODUCT TYPE	VERSION
qa-ump-tlc.trunkpac...	fmcuc	OK	User Management P...	8.0.450.101

REGION	AutoDetection	SAVE NEEDED	No	IP ADDRESS	169.254.1.201	SERIAL NUMBER	1407707651	RESET NEEDED	No

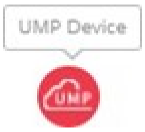
Management: OK

- ● Cleared
  DEVICE ALARMS STATUS
- ● Unlocked
  ADMINISTRATION STATUS
- ● Connected
  CONNECTION STATUS

License: OK

- ● Managed
  MANAGEMENT STATUS
- ● Unmanaged
  OVOC LICENSE STATUS

Table 6-1: UMP Device Status

Status	Topology Map	Device Management Page	Description
Error		●	Device status is Error when one or more of the following exist: ■ Management status is Error (if device alarms status or connection status is disconnected) ■ Voice quality status is Error (if control status or media status is Error, or if connection status is disconnected) ■ License status is Error only if license pool is failed or expired

Status	Topology Map	Device Management Page	Description
Warning	UMP Device UMP	🟠	Device status is Warning when one or more of the following exists: - Management status is Warning (if device alarms status or administration status is Warning) - Voice quality status is Warning (if control status or media status or connection status is Warning) - License status is Warning (if a reset/apply action is required in the license pool or if there is no management license in the device or if there is no voice quality license)
OK	UMP Device UMP	🟢	Device status is OK when all of the following exists: - Management status is OK - Clear or Undetermined (if device alarms status or connection status is OK - Clear or Undetermined) - Voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear orUndetermined)

Status	Topology Map	Device Management Page	Description
			■ License status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) Strikethrough = locked No strikethrough = unlocked

Table 6-2: SBC Device Status

Status	Topology Map	Device Management Page	Description
Error	🔴	🔴	Indicates an SBC belonging to AudioCodes communicating with the OVOC. Device status is Error when one or more of the following exist: ■ Management status is Error (if device alarms status or connection status is disconnected) ■ Voice quality status is Error (if control status or media status is Error, or if connection status is disconnected) ■ License status is Error only if license pool is failed or expired
Warning	🟠	🟠	Device status is Warning when one or more of the following exists: ■ Management status is Warning (if device alarms status or administration status is Warning)

Status	Topology Map	Device Management Page	Description
			■ Voice quality status is Warning (if control status or media status or connection status is Warning) ■ License status is Warning (if a reset/apply action is required in the license pool or if there is no management license in the device or if there is no voice quality license)
OK	⇆	🟢	Device status is OK when all of the following exists: ■ Management status is OK - Clear or Undetermined (if device alarms status or connection status is OK - Clear or Undetermined) ■ Voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear orUndetermined) ■ License status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) Strikethrough = locked No strikethrough = unlocked

Deployment Status

The following table shows the statuses in the customer deployment process.

Table 6-3: Deployment Status

Deploy Status	Description	Description
🟩	Indicates that the M365 Tenant's Teams Phones System has been successfully deployed.	OK
🟧	Indicates that the request to deploy the M365 Tenant's Teams Phones System has been submitted.	Warning
	Indicates that the M365 Tenant's Teams Phones System is currently being deployed.	Warning
	Indicates that the M365 Tenant's Teams Phones System is ready for deployment.	Warning
🟧	Indicates that the M365 Tenant's Teams Phones System is ready for Disable Mode.	Unmonitored
	Indicates that the M365 Tenant's Teams Phones System is currently being Disable.	Unmonitored
⬜	Indicates that the M365 Tenant's Teams Phones System has been disabled.	Unmonitored
🟥	Indicates that an error has occurred in the deployment of the M365 Tenant's Teams Phones System.	Error
	Indicates that the M365 Tenant's Teams Phones System does not exist.	
	Indicates a M365 Tenant's Teams Phones System connection error.	

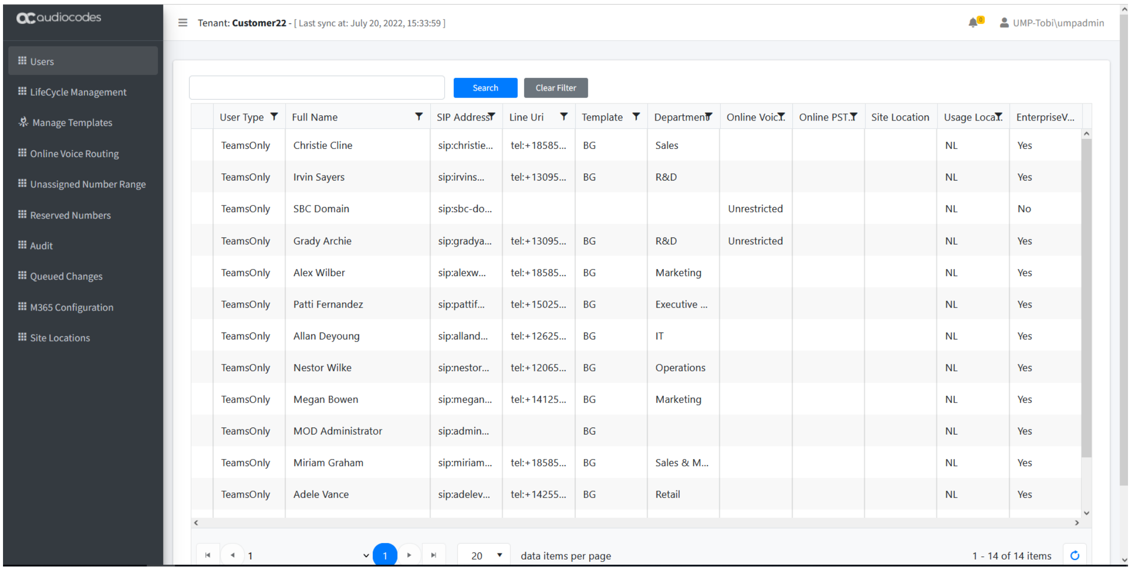
Editing Users

You can search for specific users to display their details in the screen and edit the assigned policies as part of Second day management. For example, change the assigned number range for the user or assign a different Online Voice routing Policy. When a new customer is onboarded, a default Online Voicerouting Policy "Unrestricted" is created, you can later assign custom routing policies to users according to their site location.

- See also Edit User Policies
- See also Assigning Phone Numbers

➢ To search for a user:

1. In the Customer portal **Users** page search field, select the username or # of characters to search for a specific user.



Tenant: **Customer22** - [Last sync at: July 20, 2022, 15:33:59]

User Type	Full Name	SIP Address	Line Uri	Template	Department	Online Voic…	Online PST…	Site Location	Usage Loca…	EnterpriseV…
TeamsOnly	Christie Cline	sip:christie...	tel:+18585...	BG	Sales				NL	Yes
TeamsOnly	Irvin Sayers	sip:irvins...	tel:+13095...	BG	R&D				NL	Yes
TeamsOnly	SBC Domain	sip:sbc-do...				Unrestricted			NL	No
TeamsOnly	Grady Archie	sip:gradya...	tel:+13095...	BG	R&D	Unrestricted			NL	Yes
TeamsOnly	Alex Wilber	sip:alexw...	tel:+18585...	BG	Marketing				NL	Yes
TeamsOnly	Patti Fernandez	sip:pattif...	tel:+15025...	BG	Executive ...				NL	Yes
TeamsOnly	Allan Deyoung	sip:alland...	tel:+12625...	BG	IT				NL	Yes
TeamsOnly	Nestor Wilke	sip:nestor...	tel:+12065...	BG	Operations				NL	Yes
TeamsOnly	Megan Bowen	sip:megan...	tel:+14125...	BG	Marketing				NL	Yes
TeamsOnly	MOD Administrator	sip:admin...		BG					NL	Yes
TeamsOnly	Miriam Graham	sip:miriam...	tel:+18585...	BG	Sales & M...				NL	Yes
TeamsOnly	Adele Vance	sip:adelev...	tel:+14255...	BG	Retail				NL	Yes

1 | 1 | 20 data items per page | 1 - 14 of 14 items

The table below describes the data shown for each user.

Parameter	Description
User Type	TeamsOnly
Full Name	M365 user name.
SIP Address	SIP Uri of the user.
Line Uri	Line Uri of the user.
Template	The name of the applied managed template.
Department	The organization department of the user.
Online Voice Routing Policy	The Online Voice Routing Policy applied to the user.
Online PSTN Gateway	The Online PSTN Gateway used to manage the user's calls.
Site Location	The Site Location of the user.
Usage Location	The Usage Location of the user.
Enterprise Voice	Indicates whether Enterprise Voice is enabled for the user.

Configuring License

UMP-365 supports the follow licensing schemes:

- **Tenants:** Tenants license includes the following features support:
  - Quick Connect
  - Tenant Online voice routing
  - User view only

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

- **Users:** User license includes the following features support:
  - User MACD (Teams, and Voice policies)
  - Lifecycle management
  - Create and Edit Templates
  - DID management
  - Support Microsoft Teams
  - Support OneDrive policies (Future implementation)
  - Manage emergency call Routing (Future)

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

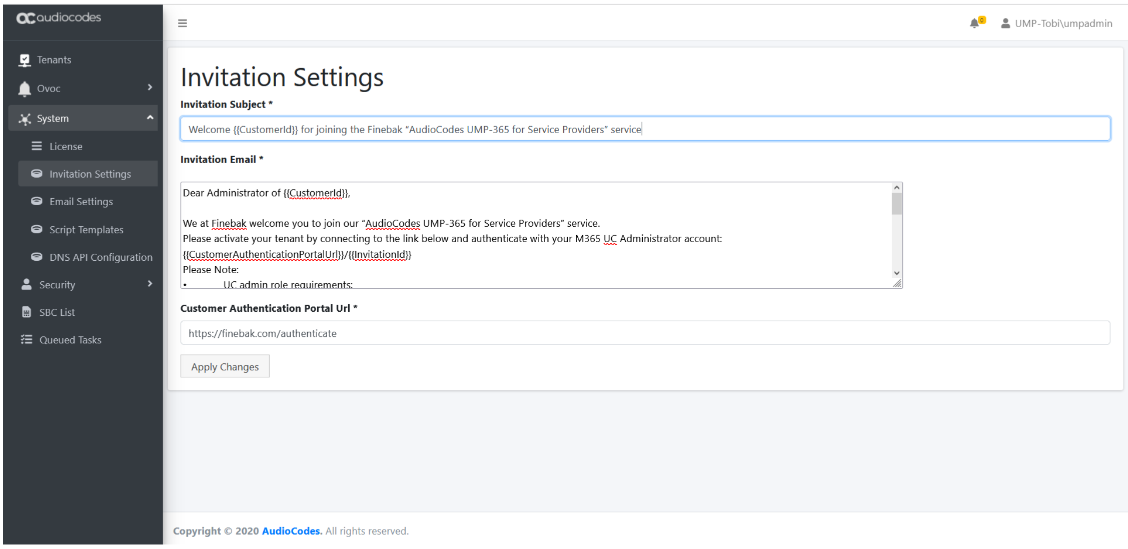
Configuring Invitation Settings

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

➢ **Do the following:**

1. Login to the Multitenant portal with Windows UMP Service account created in Creating UMP Service Account.

2. In the Multitenant portal Navigation pane, open the Invitation Settings page (**System** >**Invitation Settings**).



Invitation Settings

Invitation Subject *

Welcome {{CustomerId}} for joining the Finebak "AudioCodes UMP-365 for Service Providers" service

Invitation Email *

Dear Administrator of {{CustomerId}},

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

Customer Authentication Portal Url *

https://finebak.com/authenticate

Copyright © 2020 AudioCodes. All rights reserved.

3. Enter the following details:

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

4. In the Customer Authentication portal URL field define a **public Portal URL** for the provider.

For Example: https://finebak.com/authenticate

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

See example email below.

> Dear Administrator of {{CustomerId}},
>
> We at Finebak welcome you to join our "AudioCodes UMP-365 service".
> Please activate your tenant by connecting to the link below and authenticate with your M365 UC Administrator account:
> {{CustomerAuthenticationPortalUrl}}/{{InvitationId}}
> Please Note:
> - UC admin role requirements:
>   - Application Administrator

- o Skype for Business Admin
- o Teams Communications Administrator

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

Thank you and best regards,
Finebak Support Team
This email and any files transmitted with it are confidential material. They are intended solely for the use of the designated individual or entity to whom they are addressed. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, use, distribution or copying of this communication is strictly prohibited and may be unlawful.
If you have received this email in error please immediately notify the sender and delete or destroy any copy of this message

Authentication Status

The Authentication Status page configures the Client IDs and redirect URIs used by the Token Invitation mechanism for securing UMP-365 access to the customer tenant’s Microsoft Office 365 platform that is used for the Background Replication process (see Queued Tasks (Background Replication). In the Onboarding wizard (for Hosted Essentials + and Hosted Pro customers), connection to the customer's Microsoft 365 platform is secured using the following methods:

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

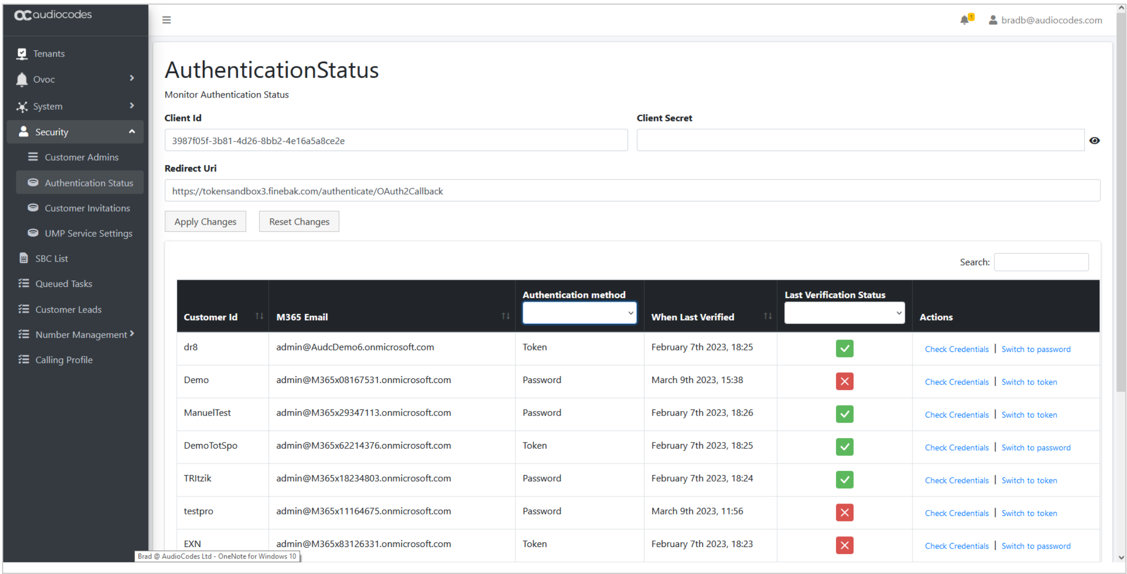
> ⚠ Customers onboarded prior to version 8.0.450 with user and password must be authenticated using token-based authentication as a result of enhanced Microsoft Security policies.

- **Switch to auth token:** This option secures the connection with M365 through a directly-claimed access token. See Switching to Token Authentication on page 34.

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

➢ To manage Authorization tokens:

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



AuthenticationStatus

Monitor Authentication Status

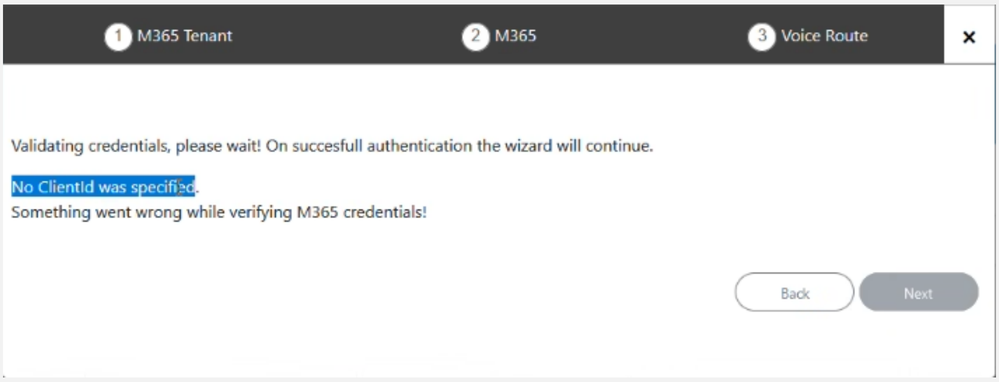
Client Id: 3987f05f-3b81-4d26-8bb2-4e16a5a8ce2e

Client Secret:

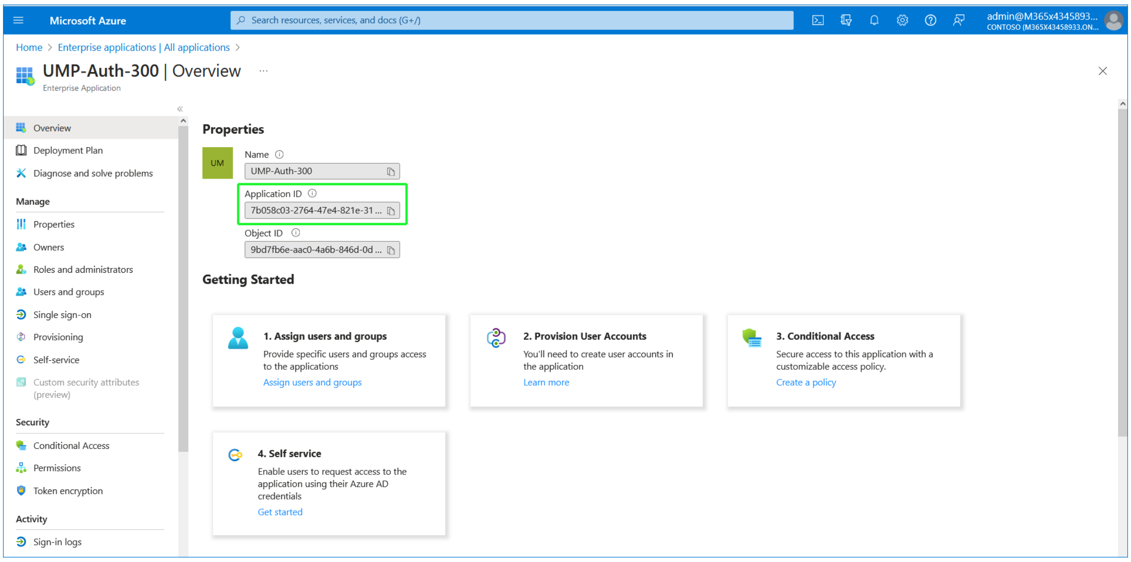
Redirect Uri: https://tokensandbox3.finebak.com/authenticate/OAuth2Callback

Customer Id	M365 Email	Authentication method	When Last Verified	Last Verification Status	Actions
dr8	admin@AudcDemo6.onmicrosoft.com	Token	February 7th 2023, 18:25	✓	Check Credentials | Switch to password
Demo	admin@M365x08167531.onmicrosoft.com	Password	March 9th 2023, 15:38	✗	Check Credentials | Switch to token
ManuelTest	admin@M365x29347113.onmicrosoft.com	Password	February 7th 2023, 18:26	✓	Check Credentials | Switch to token
DemoTotSpo	admin@M365x62214376.onmicrosoft.com	Token	February 7th 2023, 18:25	✓	Check Credentials | Switch to password
TRItzik	admin@M365x18234803.onmicrosoft.com	Password	February 7th 2023, 18:24	✓	Check Credentials | Switch to token
testpro	admin@M365x11164675.onmicrosoft.com	Password	March 9th 2023, 11:56	✗	Check Credentials | Switch to token
EXN	admin@M365x83126331.onmicrosoft.com	Token	February 7th 2023, 18:23	✗	Check Credentials | Switch to password

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

> If the Client Id is not configured and then the **Grant Consent** option in the Self-Service portal M365 Settings (see Microsoft 365 Settings) is clicked, the following error is displayed:
>
> 
>
>
>
> Validating credentials, please wait! On succesfull authentication the wizard will continue.
>
> No ClientId was specified.
>
> Something went wrong while verifying M365 credentials!

For example:



UMP-Auth-300 | Overview

Enterprise Application

Properties

Name: UMP-Auth-300

Application ID: 7b058c03-2764-47e4-821e-31 ...

Object ID: 9bd7fb6e-aac0-4a6b-846d-0d ...

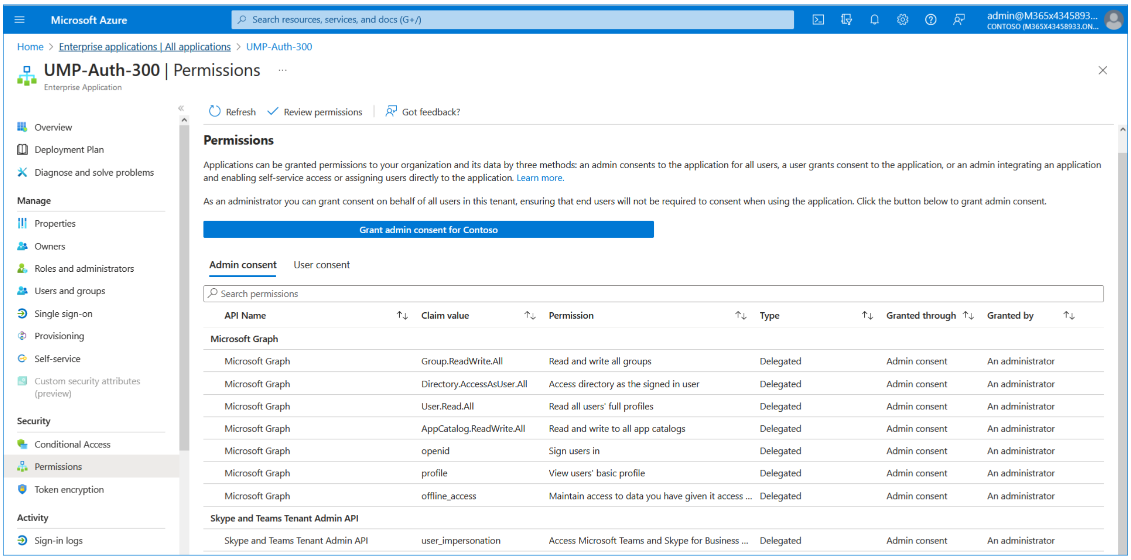
Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Provision User Accounts
You'll need to create user accounts in the application
Learn more

3. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

4. Self service
Enable users to request access to the application using their Azure AD credentials
Get started



UMP-Auth-300 | Permissions

Enterprise Application

Permissions

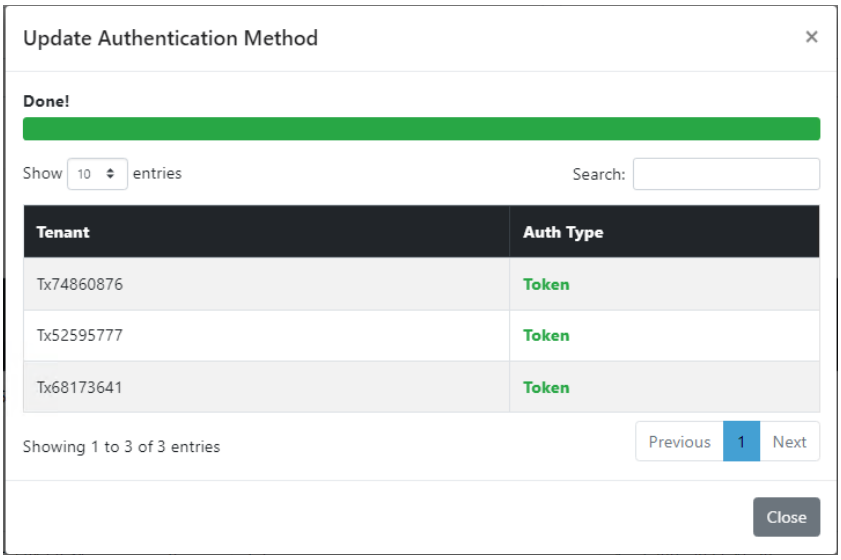
Applications can be granted permissions to your organization and its data by three methods: an admin consents to the application for all users, a user grants consent to the application, or an admin integrating an application and enabling self-service access or assigning users directly to the application.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

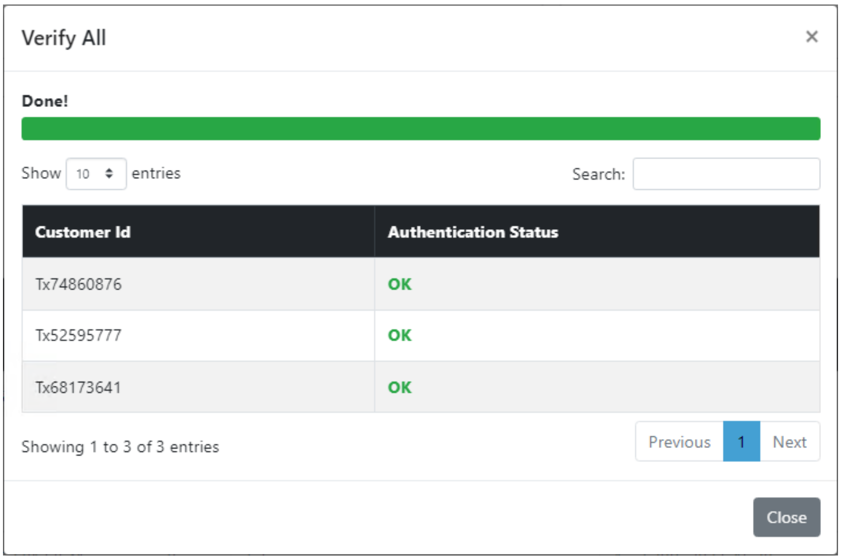
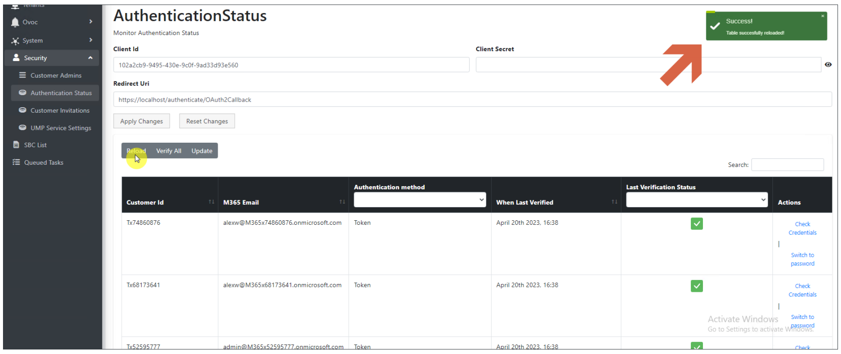
As an administrator you can grant consent on behalf of all users in this tenant, ensuring that end users will not be required to consent when using the application. Click the button below to grant admin consent.

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

Table 6-4: Authentication Status

Field	Description
Customer Id	The Customer name.
M365 Email	The email address of the Microsoft Office 365 administrator providing consent on behalf of the customer.
Authentication Method	One of the following authentication methods: ■ Password (relevant for customers until version 8.0.450). For version 8.0.450 and later, all customers must be authenticated using token authentication. ■ Token authentication.
When Last	The date and time of the last verification of connection to customers'

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Verified</td><td>M365 platform.</td></tr>
<tr><td>Last Verification Status</td><td>Indicates one of the following verification statuses:
- Never Performed
- Successful
- Failed
- Token not generated</td></tr>
<tr><td>Update</td><td>Updates for changes to Authentication method (Switch to User Password and Switch to Token). It also updates table for new customers.

Update Authentication Method
Done!
Show 10 entries Search:
<table><tr><th>Tenant</th><th>Auth Type</th></tr><tr><td>Tx74860876</td><td>Token</td></tr><tr><td>Tx52595777</td><td>Token</td></tr><tr><td>Tx68173641</td><td>Token</td></tr></table>Showing 1 to 3 of 3 entries
 </td></tr>
<tr><td>Verify All</td><td>Verifies that all claimed tokens are valid and user passwords are correct. Perform this action after 'Update' above.</td></tr>
</table>

Field	Description
	
Reload All	Refreshes table. Perform this action after 'Verify All'. 

Verify All ×

Done!

Show 10 entries Search:

Customer Id	Authentication Status
Tx74860876	OK
Tx52595777	OK
Tx68173641	OK

Showing 1 to 3 of 3 entries

Previous 1 Next

Close

AuthenticationStatus

Monitor Authentication Status

Client Id: 102a2cb9-9495-430e-9c0f-9ad33d93e560

Client Secret:

Redirect Uri: https://localhost/authenticate/OAuth2Callback

Apply Changes Reset Changes

Reload Verify All Update

Search:

Customer Id	M365 Email	Authentication method	When Last Verified	Last Verification Status	Actions
Tx74860876	alexw@M365x74860876.onmicrosoft.com	Token	April 20th 2023, 16:38	✓	Check Credentials | Switch to password
Tx68173641	alexw@M365x68173641.onmicrosoft.com	Token	April 20th 2023, 16:38	✓	Check Credentials | Switch to password
Tx52595777	admin@M365x52595777.onmicrosoft.com	Token	April 20th 2023, 16:38	✓	Check

Success! Table succesfully reloaded!

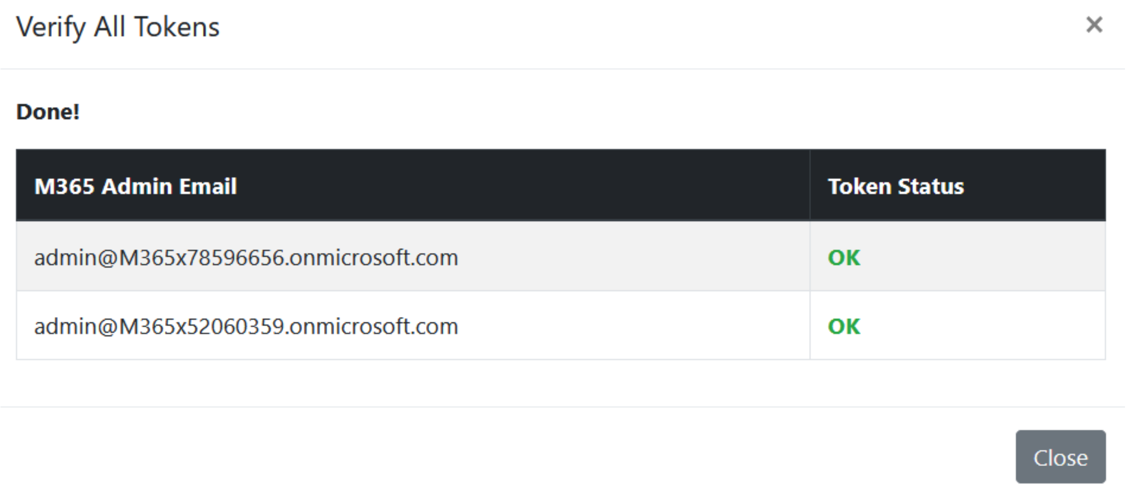
3. Enter the Client ID and Client secret generated in Deploy Synchronization Application.

4. Enter the Redirect URL which consists of the IP address of the Service Provider portal. For example:

   https://finebak.domain.com/authenticate/OAuth2Callback

Parameter	Description
Actions	One of the following actions can be performed: ■ **Check Credentials:** click to verify the token. Once verified, ✓ is displayed in the Last Verification Status column. ■ **Switch to password** ■ **Switch to token**

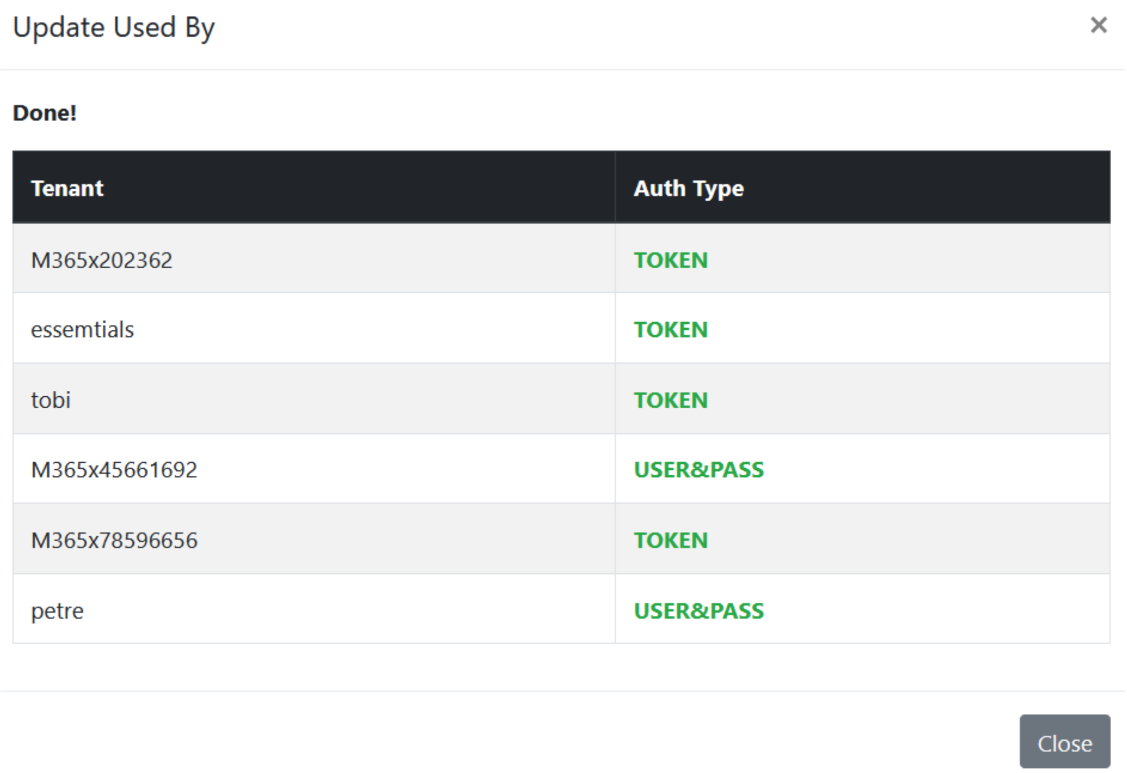
5. Click **Apply Changes** or click **Reset Changes** to reconfigure.



Verify All Tokens

Done!

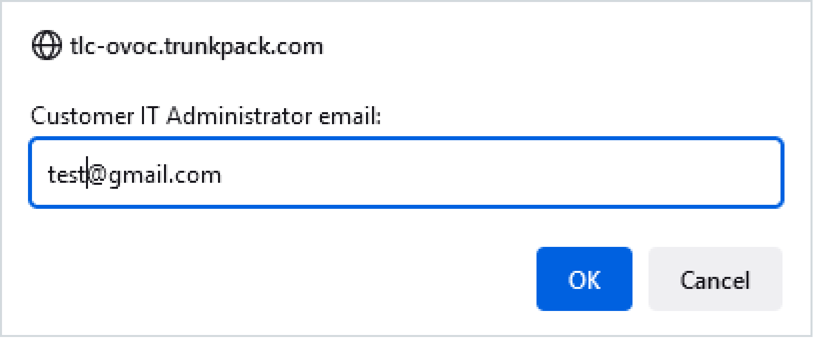
M365 Admin Email	Token Status
admin@M365x78596656.onmicrosoft.com	OK
admin@M365x52060359.onmicrosoft.com	OK



Update Used By

Done!

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



tlc-ovoc.trunkpack.com

Customer IT Administrator email:

test@gmail.com

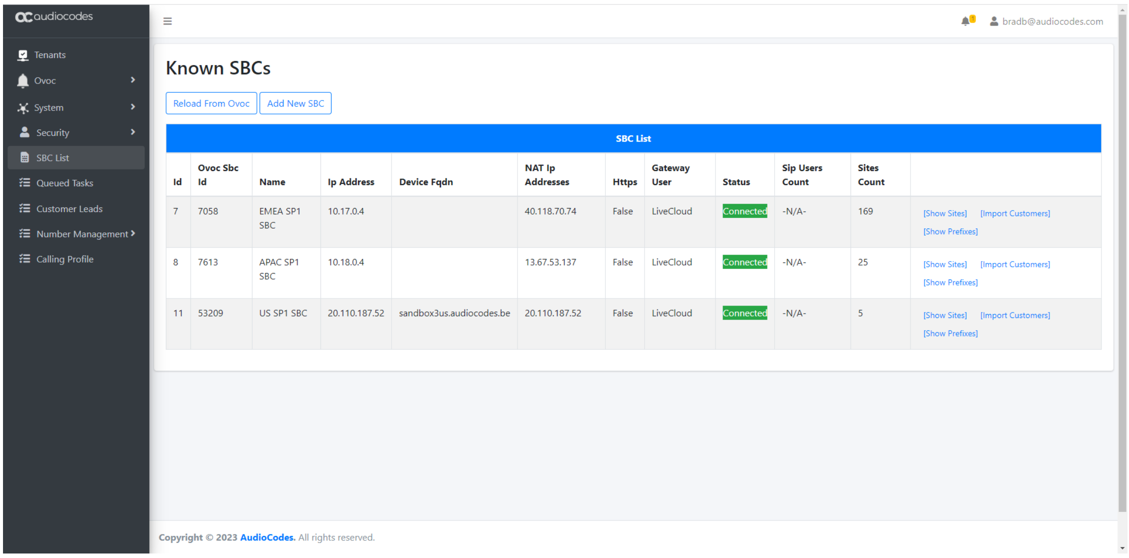
Managing SBC Devices

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

- Add SBC Devices on the next page: Add new SBC devices which can then later be configured for new customers and site locations when onboarding new customers in the Onboarding wizard.
- Show SBC Site Locations on page 63: Show a list of configured site locations that are connected to specific SBC devices.
- Show Prefixes on page 65: Show a list of configured number prefixes in the dialplans loaded to the managed SBC devices.
- Upload Dial Plan Rules from Managed SBC Device on page 66 : Import a list of customers from the SBC.

➢ To display list of managed SBC devices:

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



Known SBCs

SBC List

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

Copyright © 2023 AudioCodes. All rights reserved.

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

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

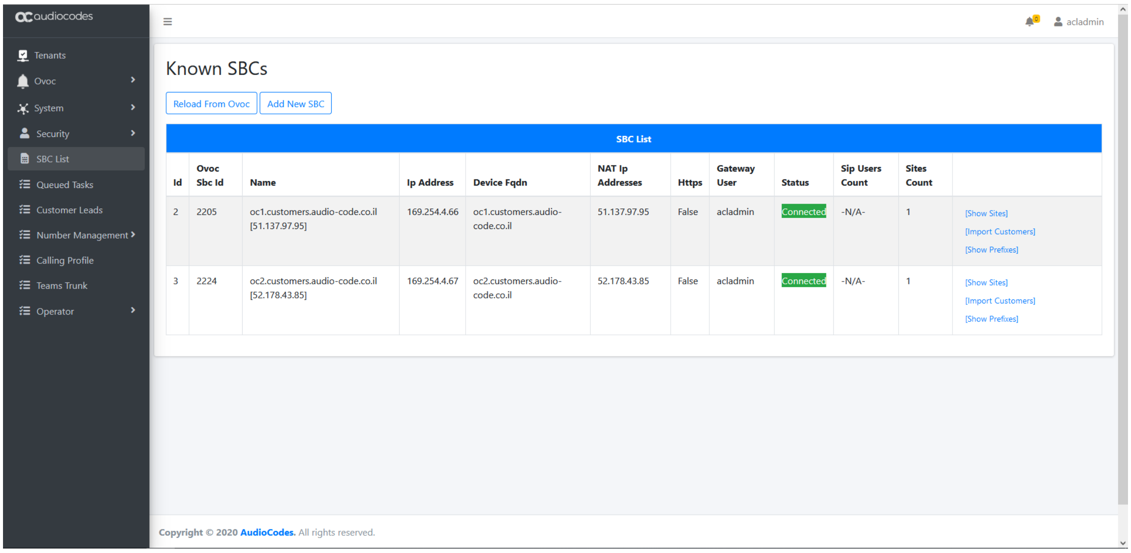
Parameter	Description
HTTPS	Indicates whether HTTPS is enabled for the device.
Gateway User	The name of the administrator user account of the SBC.
Status	The status of the connection between UMP-365 and the SBC.
SIP Users Count	The number of SIP users registered for the SBC.
Site Count	The number of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

Add SBC Devices

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

➢ To add a new SBC device:

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



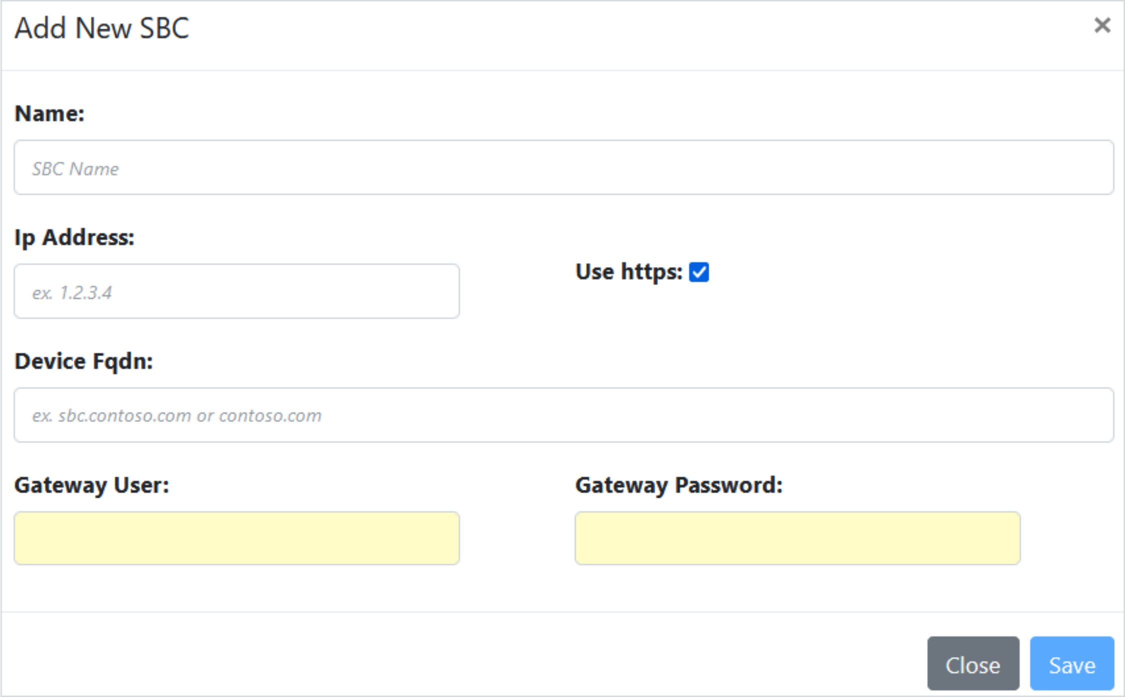
Known SBCs

SBC List

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

Copyright © 2020 AudioCodes. All rights reserved.

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



Add New SBC

Name: SBC Name

Ip Address: ex. 1.2.3.4

Use https: ☑

Device Fqdn: ex. sbc.contoso.com or contoso.com

Gateway User:

Gateway Password:

3. Enter the name of the SBC device.

4. Enter the IP address of the SBC device.

5. Enter the Device FQDN.

6. Enter the Gateway username and password.

7. Click Save to apply the changes.

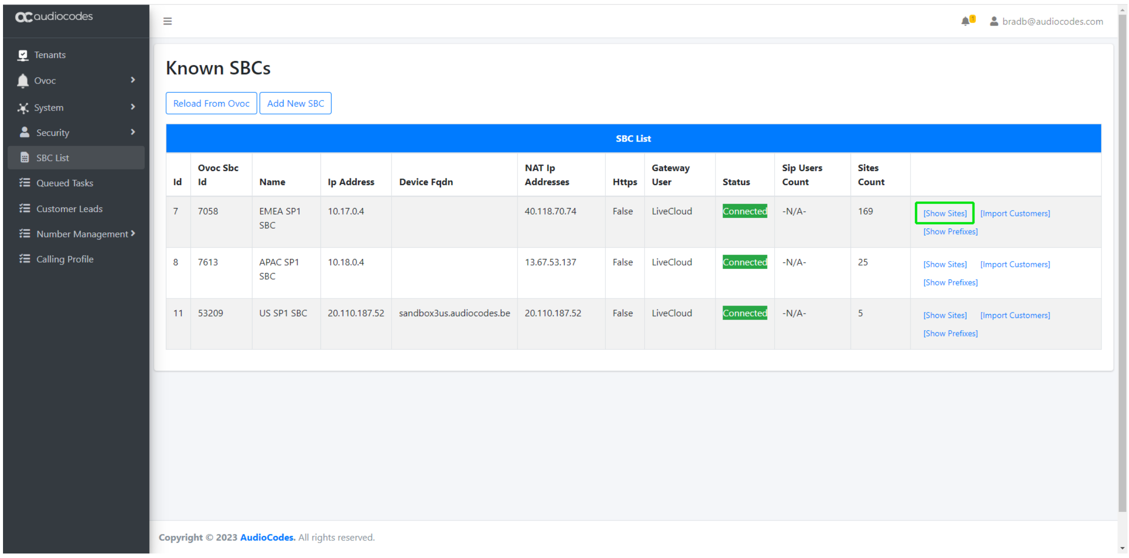
8. Click Reload From Ovoc to refresh the connection between the SBC devices list and the OVOC Server.

Show SBC Site Locations

You can display all configured site locations where each site is configured with an SBC devices that manages calls through that site.

➢ **To show site locations:**

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



Known SBCs

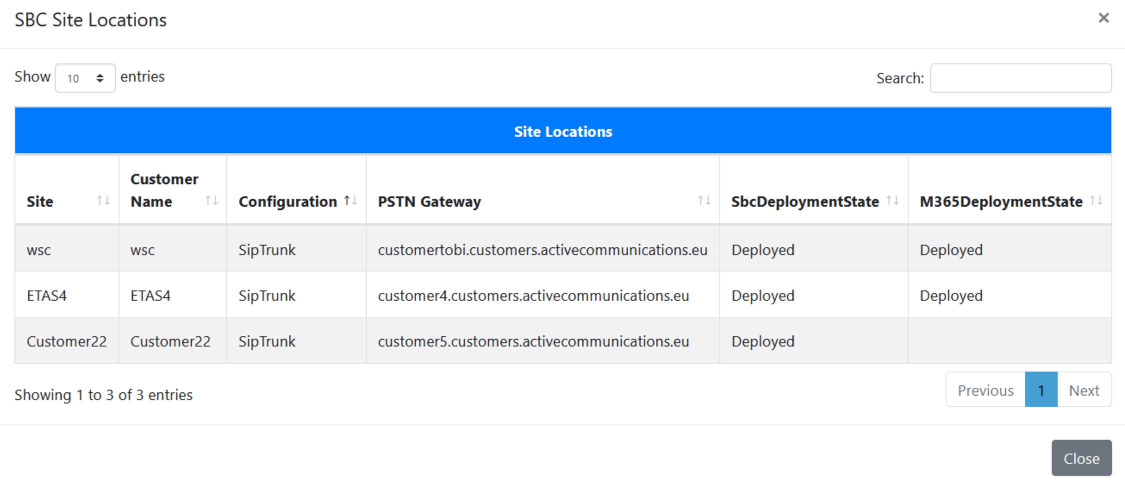
Reload From Ovoc | Add New SBC

SBC List

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

Copyright © 2023 AudioCodes. All rights reserved.

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



SBC Site Locations

Show 10 entries

Search:

Site Locations

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

Showing 1 to 3 of 3 entries

The table below describes the parameters in this table.

Parameter	Description
Site	Name of the site location.
Customer Name	Customer Name
Configuration	One of the following values: ■ SIP Trunk ■ IP-PBX ■ BYOC
PSTN Gateway	FQDN of the Online PSTN Gateway for the site location.
SBC Deployment State	Indicates that the SBC has been successfully connected to Live Cloud and UMP-365

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

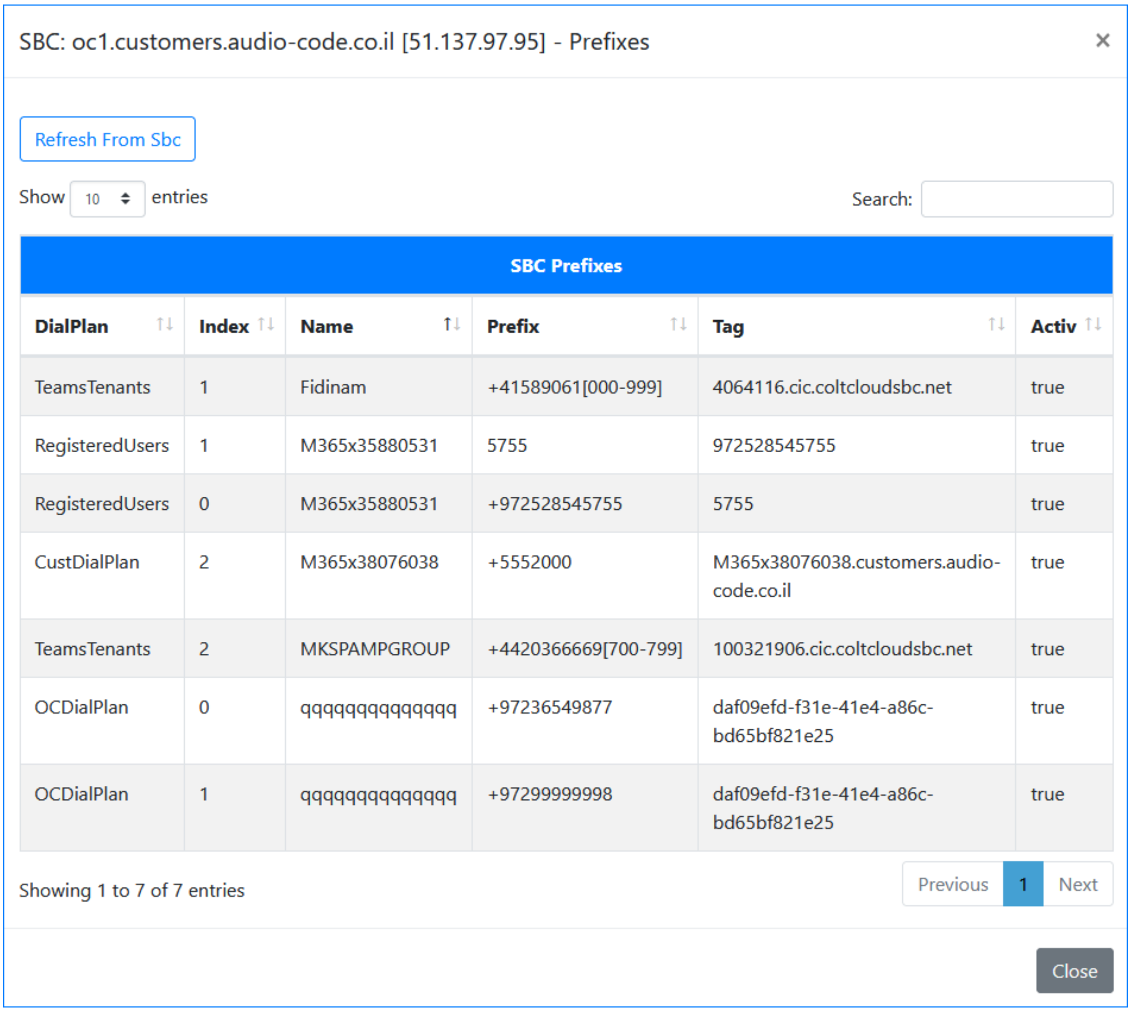
Show Prefixes

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

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

➢ To show prefixes:

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


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

SBC Prefixes

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

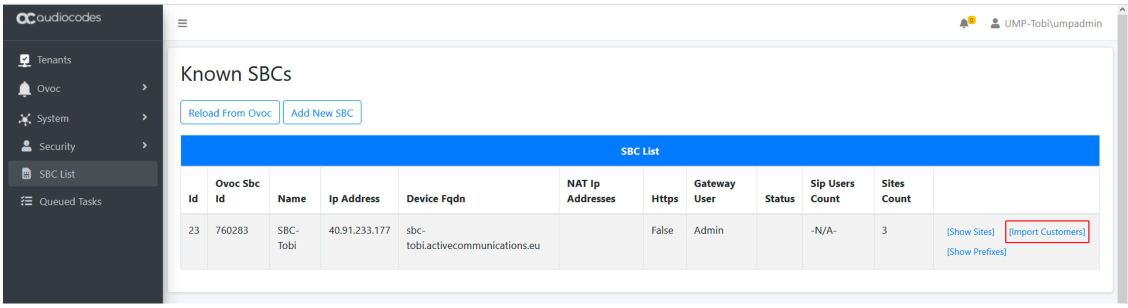
Showing 1 to 7 of 7 entries

Upload Dial Plan Rules from Managed SBC Device

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

➢ To upload dial plan from an SBC:

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



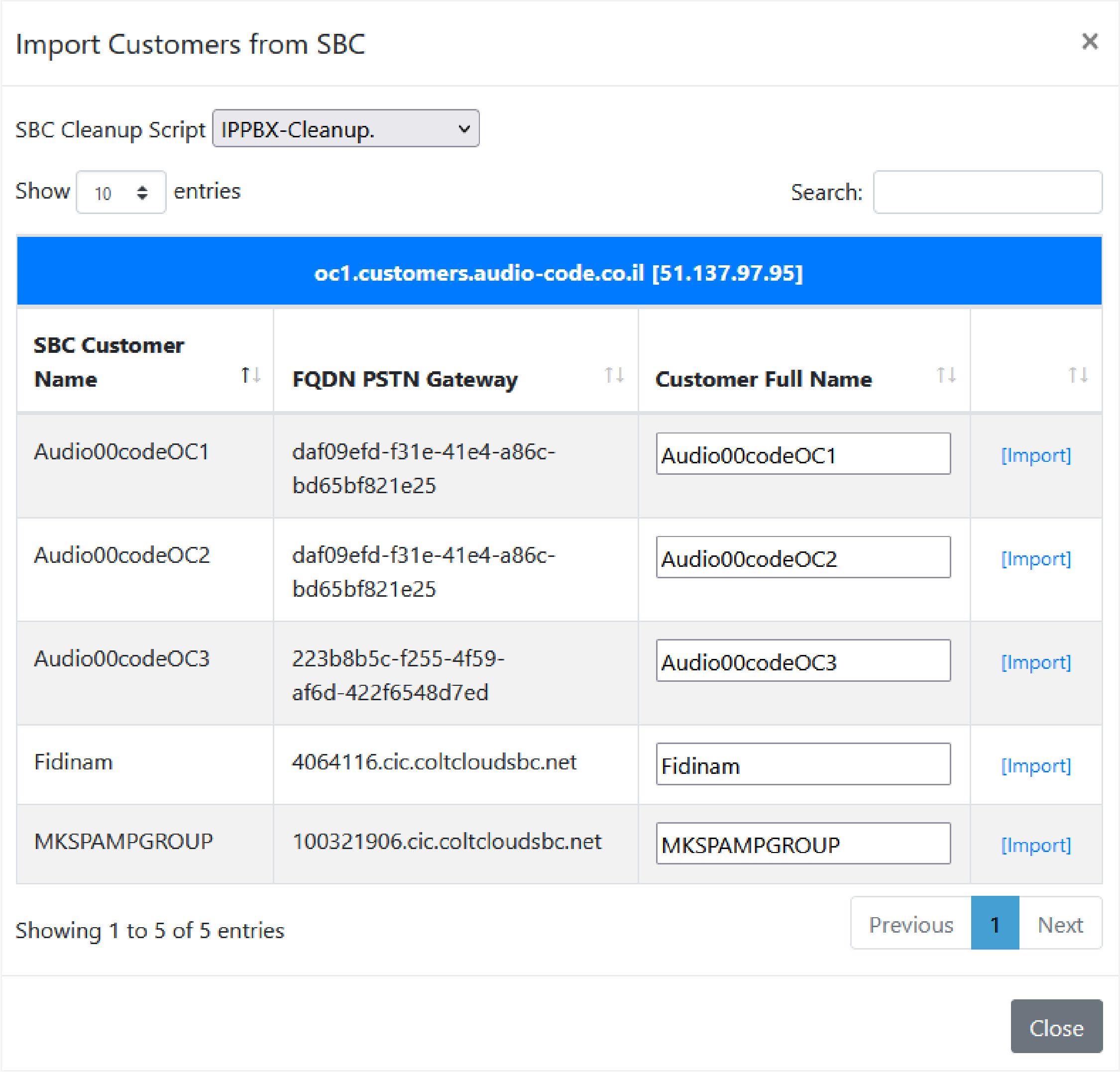
Known SBCs

SBC List

Id	Ovoc Sbc Id	Name	Ip Address	Device Fqdn	NAT Ip Addresses	Https	Gateway User	Status	Sip Users Count	Sites Count	
23	760283	SBC-Tobi	40.91.233.177	sbc-tobi.activecommunications.eu		False	Admin		-N/A-	3	[Show Sites] [Import Customers] [Show Prefixes]

A list of customers are displayed.

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



Import Customers from SBC

SBC Cleanup Script IPPBX-Cleanup.

Show 10 entries Search:

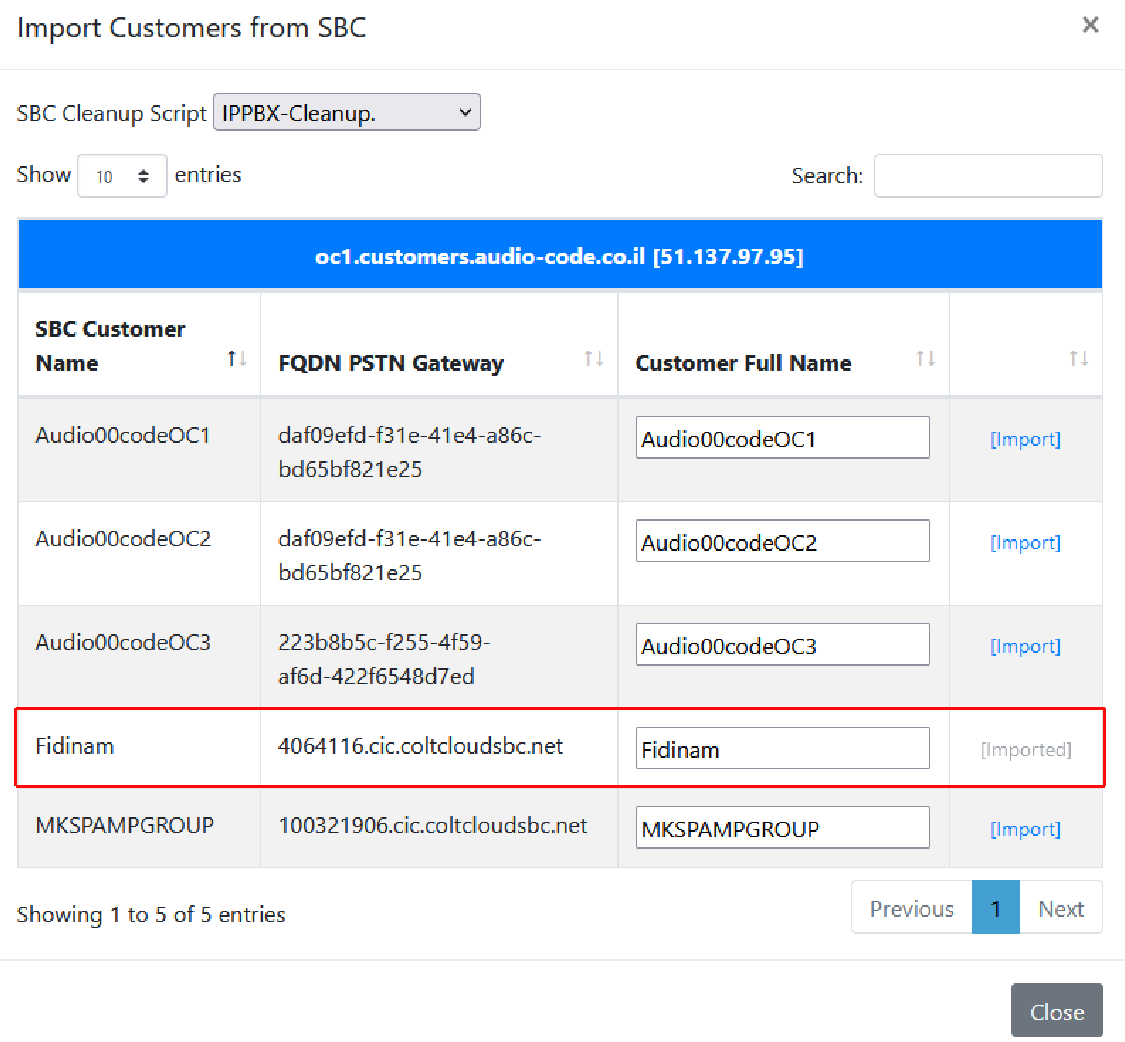
oc1.customers.audio-code.co.il [51.137.97.95]

SBC Customer Name	FQDN PSTN Gateway	Customer Full Name	
Audio00codeOC1	daf09efd-f31e-41e4-a86c-bd65bf821e25	Audio00codeOC1	[Import]
Audio00codeOC2	daf09efd-f31e-41e4-a86c-bd65bf821e25	Audio00codeOC2	[Import]
Audio00codeOC3	223b8b5c-f255-4f59-af6d-422f6548d7ed	Audio00codeOC3	[Import]
Fidinam	4064116.cic.coltcloudsbc.net	Fidinam	[Import]
MKSPAMPGROUP	100321906.cic.coltcloudsbc.net	MKSPAMPGROUP	[Import]

Showing 1 to 5 of 5 entries

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

   The customer is imported.



Import Customers from SBC

SBC Cleanup Script: IPPBX-Cleanup.

Show 10 entries

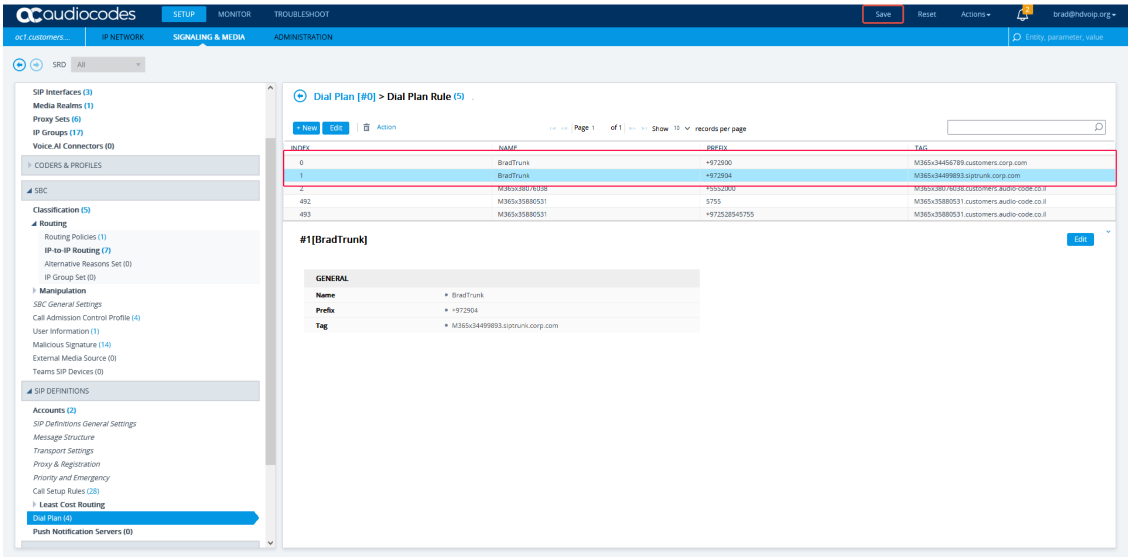
Search:

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

SBC Customer Name	FQDN PSTN Gateway	Customer Full Name	
Audio00codeOC1	daf09efd-f31e-41e4-a86c-bd65bf821e25	Audio00codeOC1	[Import]
Audio00codeOC2	daf09efd-f31e-41e4-a86c-bd65bf821e25	Audio00codeOC2	[Import]
Audio00codeOC3	223b8b5c-f255-4f59-af6d-422f6548d7ed	Audio00codeOC3	[Import]
Fidinam	4064116.cic.coltcloudsbc.net	Fidinam	[Imported]
MKSPAMPGROUP	100321906.cic.coltcloudsbc.net	MKSPAMPGROUP	[Import]

Showing 1 to 5 of 5 entries

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

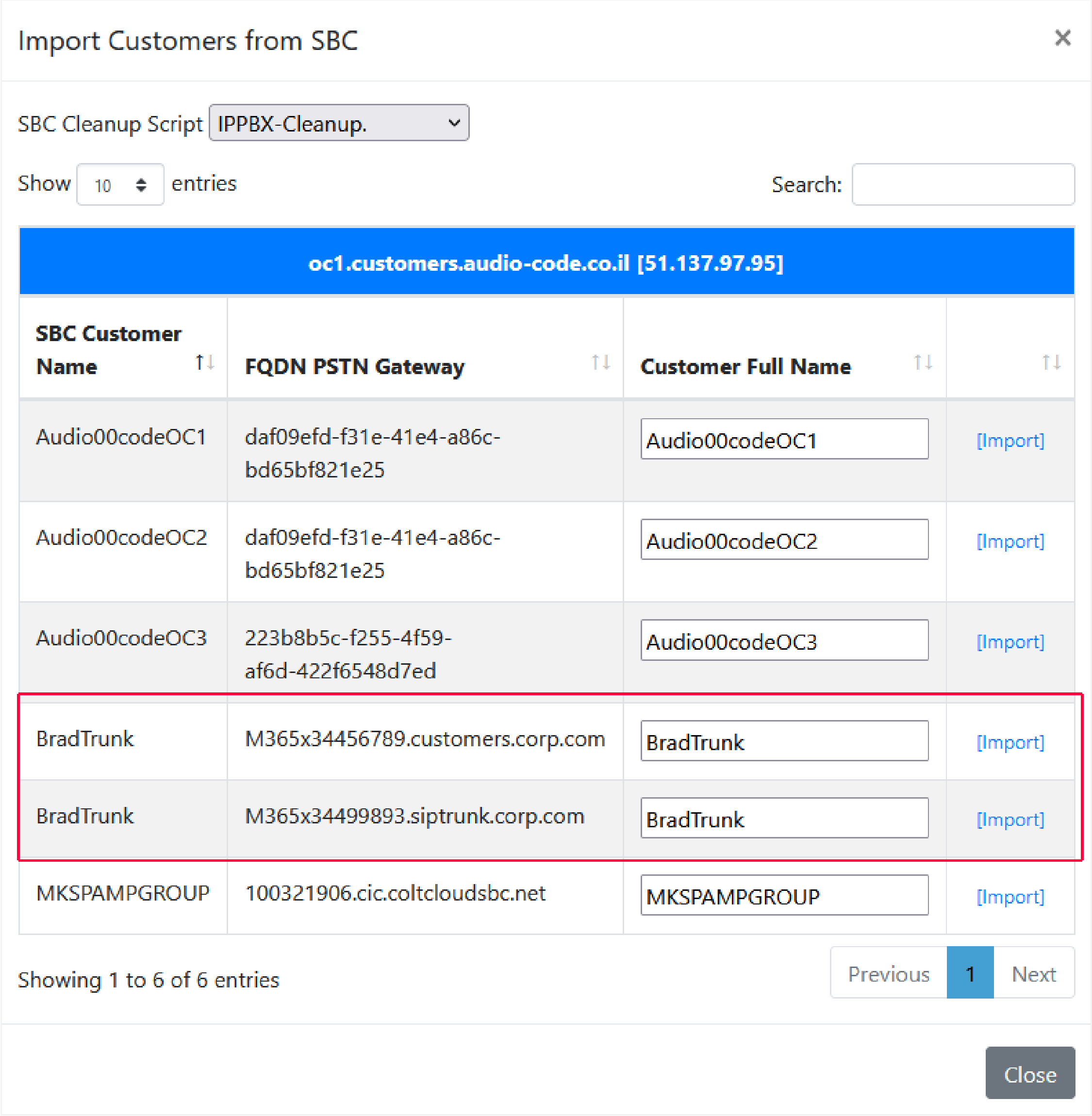


Dial Plan [#0] > Dial Plan Rule (5)

INDEX	NAME	PREFIX	TAG
0	BradTrunk	+972900	M365x34456789.customers.corp.com
1	BradTrunk	+972904	M365x34499893.siptrunk.corp.com
2	M365x38076038	+5552000	M365x38076038.customers.audio-code.co.il
492	M365x35880531	5755	M365x35880531.customers.audio-code.co.il
493	M365x35880531	+972528545755	M365x35880531.customers.audio-code.co.il

#1[BradTrunk]

GENERAL	
Name	BradTrunk
Prefix	+972904
Tag	M365x34499893.siptrunk.corp.com



Import Customers from SBC

SBC Cleanup Script: IPPBX-Cleanup.

Show 10 entries

Search:

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

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

Showing 1 to 6 of 6 entries

Scenario Scripts Templates Page

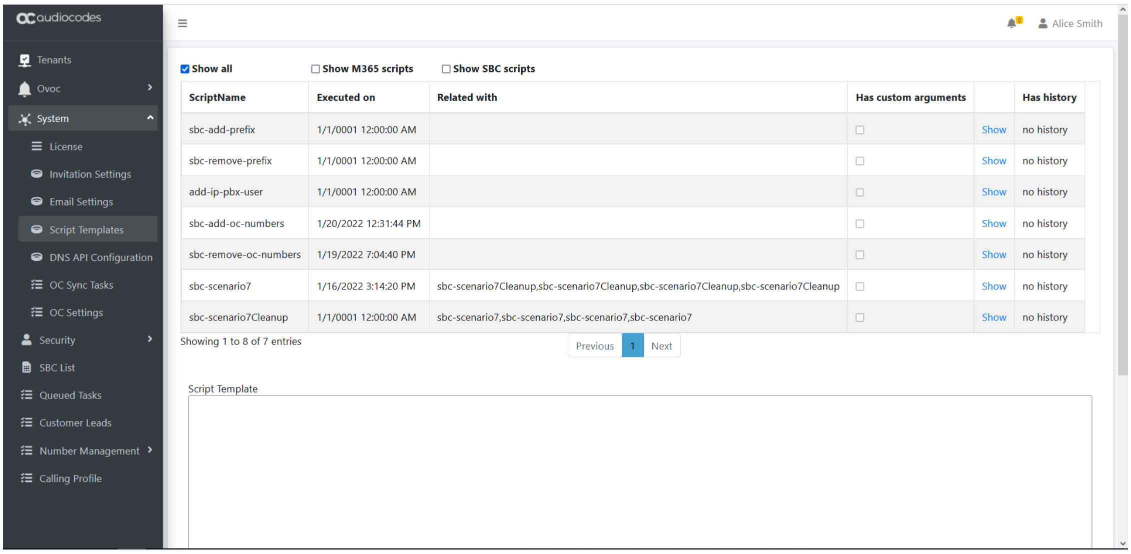
Scripts templates can be viewed and managed in the Scripts Templates page.

➢ To manage scripts:

1. In the Main Tenant Navigation pane, open the Scripts Templates page (**System** > **Script Templates**).

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

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



☑ Show all ☐ Show M365 scripts ☐ Show SBC scripts

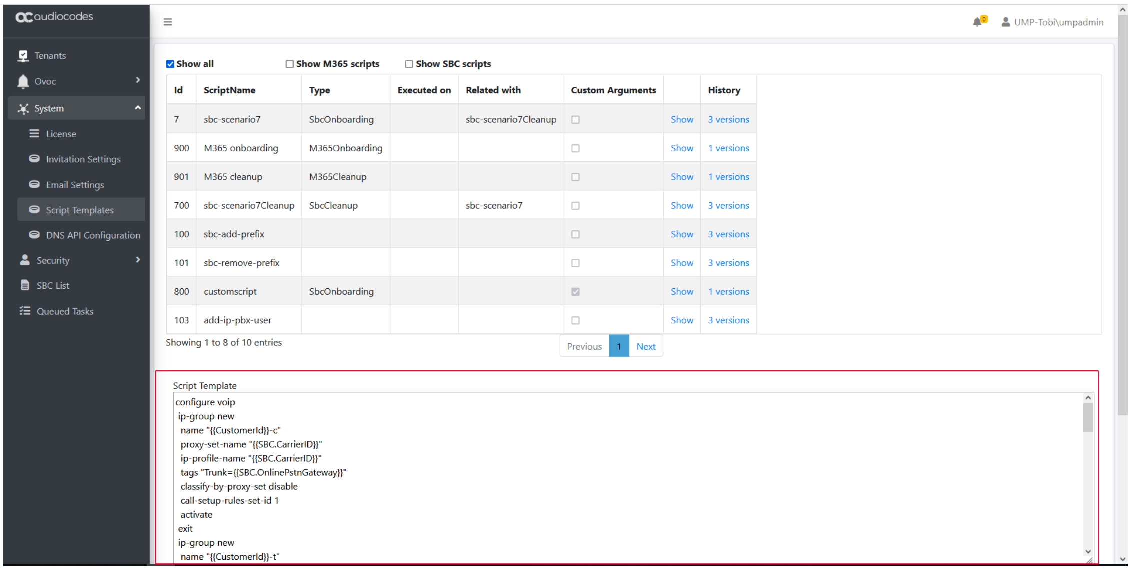
ScriptName	Executed on	Related with	Has custom arguments		Has history
sbc-add-prefix	1/1/0001 12:00:00 AM		☐	Show	no history
sbc-remove-prefix	1/1/0001 12:00:00 AM		☐	Show	no history
add-ip-pbx-user	1/1/0001 12:00:00 AM		☐	Show	no history
sbc-add-oc-numbers	1/20/2022 12:31:44 PM		☐	Show	no history
sbc-remove-oc-numbers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

Showing 1 to 8 of 7 entries

Previous 1 Next

Script Template

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



☑ Show all ☐ Show M365 scripts ☐ Show SBC scripts

Id	ScriptName	Type	Executed on	Related with	Custom Arguments		History
7	sbc-scenario7	SbcOnboarding		sbc-scenario7Cleanup	☐	Show	3 versions
900	M365 onboarding	M365Onboarding			☐	Show	1 versions
901	M365 cleanup	M365Cleanup			☐	Show	1 versions
700	sbc-scenario7Cleanup	SbcCleanup		sbc-scenario7	☐	Show	3 versions
100	sbc-add-prefix				☐	Show	3 versions
101	sbc-remove-prefix				☐	Show	3 versions
800	customscript	SbcOnboarding			☑	Show	1 versions
103	add-ip-pbx-user				☐	Show	3 versions

Showing 1 to 8 of 10 entries

Previous 1 Next

Script Template

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

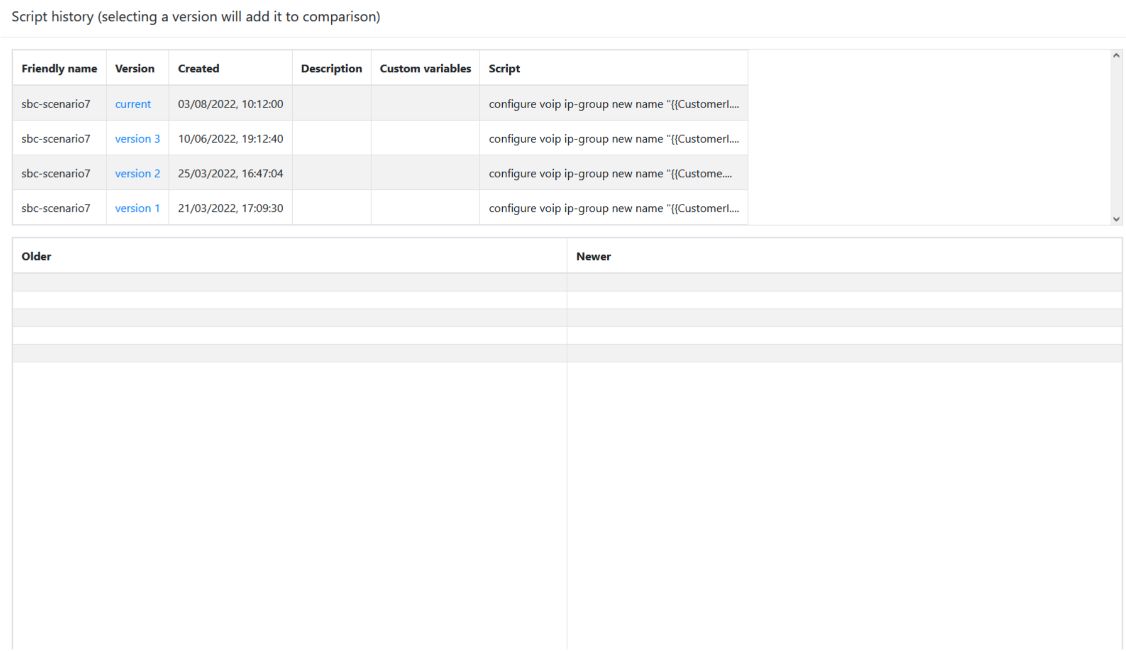
Script Scenario Comparison

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

➢ To compare scripts:

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

   The screen compare tool is displayed.



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

Friendly name	Version	Created	Description	Custom variables	Script
sbc-scenario7	current	03/08/2022, 10:12:00			configure voip ip-group new name "{{CustomerI....
sbc-scenario7	version 3	10/06/2022, 19:12:40			configure voip ip-group new name "{{CustomerI....
sbc-scenario7	version 2	25/03/2022, 16:47:04			configure voip ip-group new name "{{Custome....
sbc-scenario7	version 1	21/03/2022, 17:09:30			configure voip ip-group new name "{{CustomerI....

Older	Newer

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

Script Templates Updates

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

- Replace the attribute **SysAdmin.O365OnlinePSTNGateway** to **SBC.OnlinePstnGateway**
- Update scripts with the new syntax as shown in the sections below:
  - **Blue** indicates the syntax to add.
  - ~~Strikethrough~~ indicates the syntax to add.

sbc-scenario7

```
configure voip
 ip-group new
  name "{{CustomerId}}-c"
  proxy-set-name "{{SBC.CarrierID}}"
  ip-profile-name "{{SBC.CarrierID}}"
  tags "Trunk={{~~SysAdmin.O365OnlinePSTNGateway~~ SBC.OnlinePstnGateway}}"
  classify-by-proxy-set disable
  call-setup-rules-set-id 1
  activate
 exit
 ip-group new
  name "{{CustomerId}}-t"
  proxy-set-name "Teams"
  ip-profile-name "Teams"
  local-host-name "{{ ~~SysAdmin.O365OnlinePSTNGateway~~ SBC.OnlinePstnGateway}"
  always-use-source-addr enable
  tags "Tenant={{SBC.OnlinePstnGateway ~~SysAdmin.O365OnlinePSTNGateway~~}}"
  classify-by-proxy-set disable
  call-setup-rules-set-id 0
  {{#if  SBC.EnableCAC}}
   cac-profile "{{SBC.CacProfile}}"
  {{/if }}
  activate
 exit


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


 {{#each SBC.DialPlanPrefixes}}
  sbc dial-plan where name "{{this.~~Cust~~DialPlanName}}"
  {{#each this.Rul~~SBC Phones~~}}
```

```
   dial-plan-rule new
     name "{{this.Name~~../CustomerId~~}}"
     prefix "{{this.Prefix}}"
     tag "{{ ~~SysAdmin.O365OnlinePSTNGateway~~this.Tag}}"
   exit
  {{/each}}
  activate
  exit
 {{/each}}
do write
```

sbc-scenario7Cleanup

```
configure voip
 no ip-group where name "{{CustomerId}}-c"
 no ip-group where name "{{CustomerId}}-t"
 no sip-definition account where account-name "{{CustomerId}}"
 {{#each SBC.DialPlanPrefixes}}
   sbc dial-plan where name "{{this.~~Cust~~DialPlanName}}"
   no  dial-plan-rule where name "{{../CustomerId}}"
   activate
   exit
 {{/each}}
```

```
do write
```

sbc-add-prefix

```
configure voip
    sbc dial-plan where name "{{~~Cust~~DialPlanName}}"
    {{#each CmdData.DialPlanRules.ToAdd}}
    dial-plan-rule new
    name "{{../SBC.SbcSiteName}}"
    prefix "{{this.Prefix}}"
    tag "{{~~SysAdmin.O365OnlinePSTNGateway~~this.Tag}}"
    exit
    {{/each}}
    activate
exit
do write
```

sbc-remove-prefix

```
configure voip
    sbc dial-plan where name "{{~~Cust~~DialPlanName}}"
    {{#each ToRemove}}
    no dial-plan-rule "{{this.Index}}"
    {{/each}}
```

```
  activate
exit
do write
```

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

Website: https://www.audiocodes.com/

Documentation Feedback: https://online.audiocodes.com/documentation-feedback

Document #: LTRT-26724