

User Management Pack 365 SP Edition

Upgrade

Version 8.0.515



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: May-21-2024

WEEE EU Directive

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

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

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"
26725	Correction to "Before Upgrading UMP-365"
26726	Updated links to ISO files.
26727	Removed section for Script validation comparison and section 'Download Dial Plan from Managed SBC (Import Customer)'.

Table of Contents

1	UMP-365 Upgrade	1
2	Before Upgrading UMP-365	2
	Configure Firewall	4
	Backing up UMP-365 – Disk Snapshot	4
	Compiling List of Password Authenticated Customers	8
	Stop wyUpdate Processes	9
	Additional SysAdmin Verifications	13
3	Upgrading Main UMP-365 Tenant	14
4	Upgrading Customer Tenant	22
5	Post Upgrade Actions	26
	Restoring UMP Snapshot	26
	Verifying Tenant Admin Authentication	30
	Upgrading M365 Connection to Token Authentication	31
	Switching to Token Authentication	34
	Updating Scripts	41
	Verifying Component Statuses	41
	Updating SQL Server	44
	SBC Dialplan Verification	44
6	Appendix	45
	Device Status	45
	Deploy Status and Status Indicators	50
	Manually Provisioning Users	50
	Multitenant Portal Licensing	51
	Configuring Invitation Settings	51
	Authentication Status	53
	Managing SBC Devices	59
	Add SBC Devices	60
	Show SBC Site Locations	61
	Show Prefixes	63

1 UMP-365 Upgrade

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 26 for 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, verify the following:

- Ensure ports HTTP/HTTPS ports are open on the Enterprise firewall (see [Configure Firewall](#) on page 4).
- 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).
- Ensure the Authentication Status menu has been populated with the Azure Application Registration credentials (see [Authentication Status](#) on page 53):
 - For Standalone UMP-365 devices, the customer manages the application in their Azure environment.
- Connection to the customers' M365 platform must be performed using Token authentication instead of by username and password. This requirement is in accordance with stricter Microsoft security policies. Before upgrading, compile a list of all customers who are currently authenticated using username and password authentication. See [Compiling List of Password Authenticated Customers](#) on page 8.
- Stop processes prior to running the wyUpdate (see [Stop wyUpdate Processes](#) on page 9).
- Install SSL certificates on the UMP Windows server for securing the HTTPS connection with Microsoft Azure. See [Installing SSL Certificates on UMP Windows Server](#).
- 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 no replication processes currently being executed (see [Monitoring M365 Replication Actions Queue](#)). Wait until all replication processes have completed.

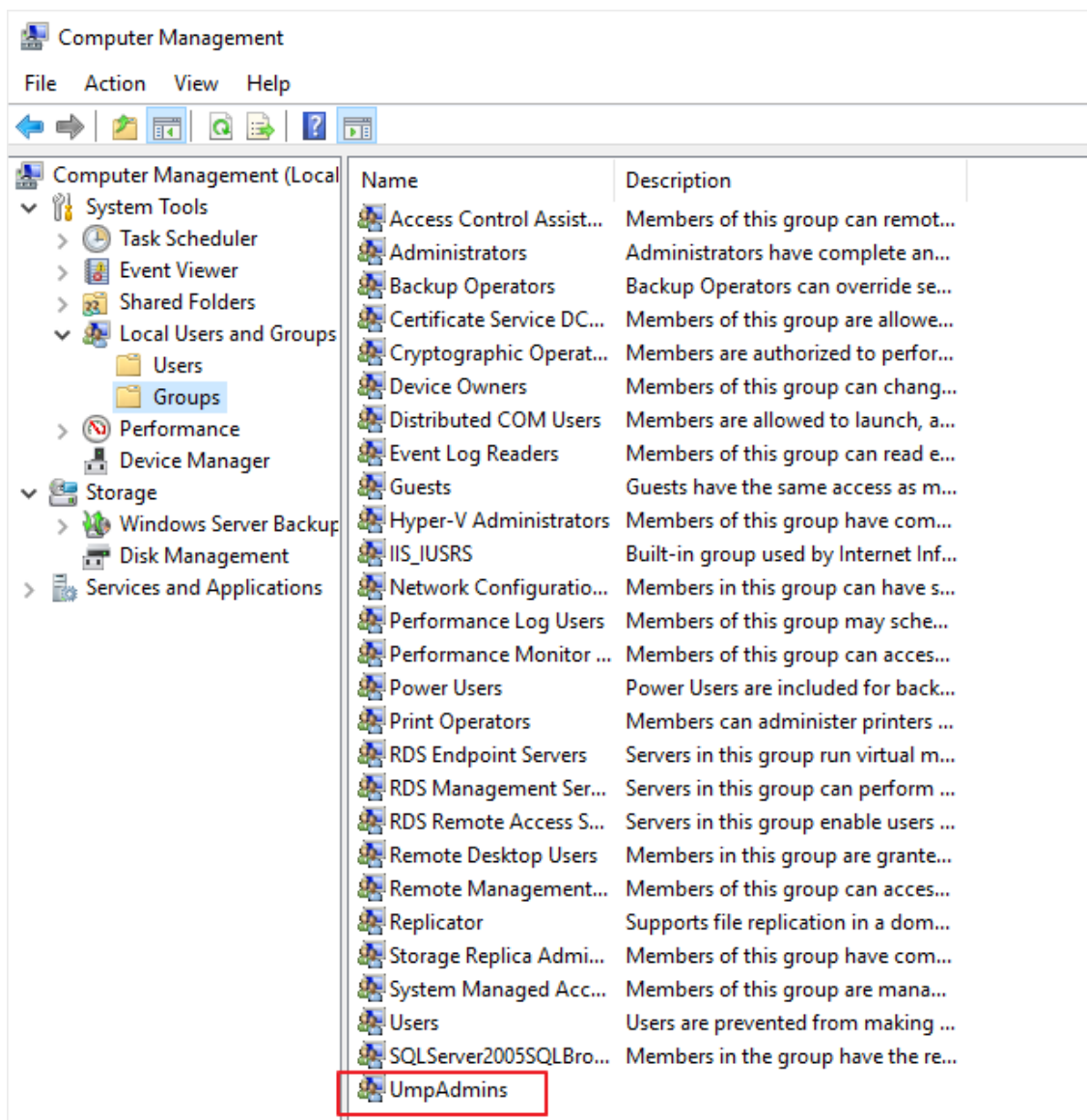
Open Commands: 1, Executing: 0, Queued: 0

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.



- See [Additional SysAdmin Verifications](#) on page 13 for additional verifications.

Configure Firewall

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

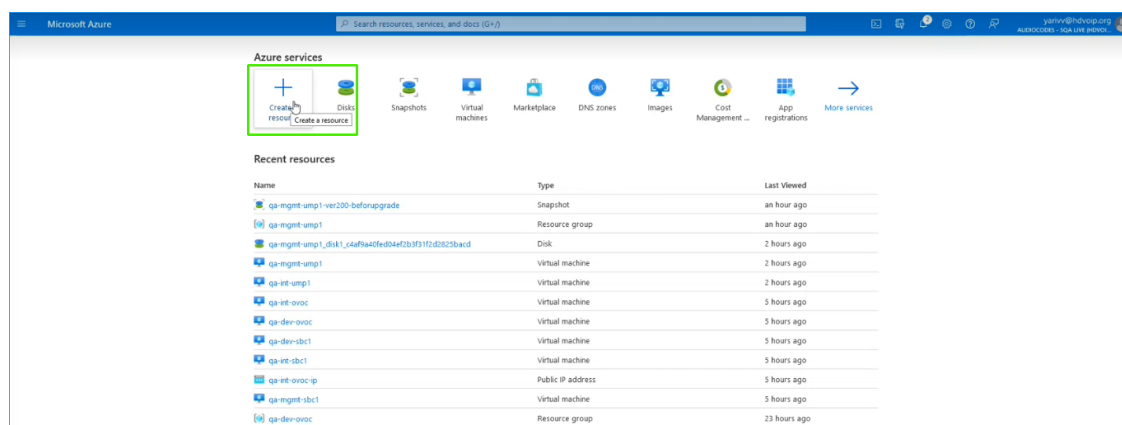
- PowershellGetModule
- MicrosoftTeamsModule
- Chocolatey
- DotNet
- Rabbitmq
- EmsMainAgent
- EmsClientAgent
- InstallPublicOvocConnector
- Installtap-windows-9.23.3-I601-Win10

Backing up UMP-365 – Disk Snapshot

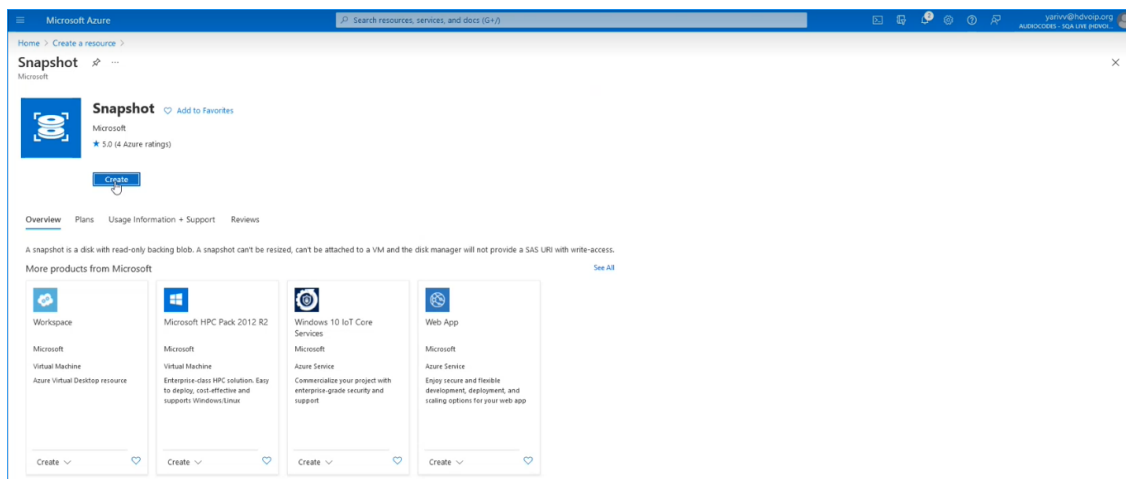
This section describes how to create a snapshot of the UMP Virtual Machine. This procedure should be performed prior to running the upgrade and then rolled back once the upgrade is complete (see [Restoring UMP Snapshot](#) on page 26).

➤ Do the following:

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



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

The screenshot shows the 'Create snapshot' form in the Microsoft Azure portal. The form is divided into several sections: 'Basics', 'Encryption', 'Networking', 'Tags', and 'Review + create'. The 'Basics' section is active and contains the following fields: 'Subscription' (set to 'SQA LIVE Sub1'), 'Resource group' (empty, with a 'Create new' link), 'Name' (empty), 'Region' (set to '(Europe) North Europe'), 'Snapshot type' (radio buttons for 'Full' and 'Incremental', with 'Full' selected), 'Source subscription' (set to 'SQA LIVE Sub1'), 'Source disk' (empty), and 'Storage type' (set to 'Zone-redundant'). At the bottom, there are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next : Encryption >'. A mouse cursor is visible over the 'Create new' link under the Resource group field.

3. In the Resource group field, select your working Resource Group.
4. Enter the desired name of the snapshot.

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

The screenshot shows the 'Create snapshot' wizard in the Microsoft Azure portal, specifically the 'Tags' tab. The breadcrumb navigation at the top reads 'Home > Create a resource > Snapshot >'. The main heading is 'Create snapshot'. Below this, there are tabs for 'Basics', 'Encryption', 'Networking', 'Tags' (which is selected), and 'Review + create'. A descriptive text states: '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](#)'. A note below says: 'Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.' The 'Tags' section contains a table with three columns: 'Name', 'Value', and 'Resource'. The first row has 'LiveCloudEnv' in the Name column, 'qa-mgmt' in the Value column, and '2 selected' in the Resource column. A second row is empty, with '2 selected' in the Resource column. At the bottom of the wizard, there are three buttons: 'Review + create' (in blue), '< Previous', and 'Next : Review + create >'.

Name	Value	Resource
LiveCloudEnv	qa-mgmt	2 selected
		2 selected

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

The screenshot shows the 'Create snapshot' wizard in the Microsoft Azure portal, specifically the 'Review + create' step. A green banner at the top indicates 'Validation passed'. The wizard has five tabs: Basics, Encryption, Networking, Tags, and Review + create. The 'Basics' tab is active, displaying the following configuration details:

Field	Value
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

Below the Basics section, the 'Encryption' section shows 'Encryption type' as 'Platform-managed key'. The 'Networking' section shows 'Connectivity method' as 'AllowAll'. The 'Tags' section shows two 'LiveCloudEnv' tags, both with the value 'qa-mgmt'. At the bottom, there is a 'Create' button, a '< Previous' button, a 'Next >' button, and a link to 'Download a template for automation'.

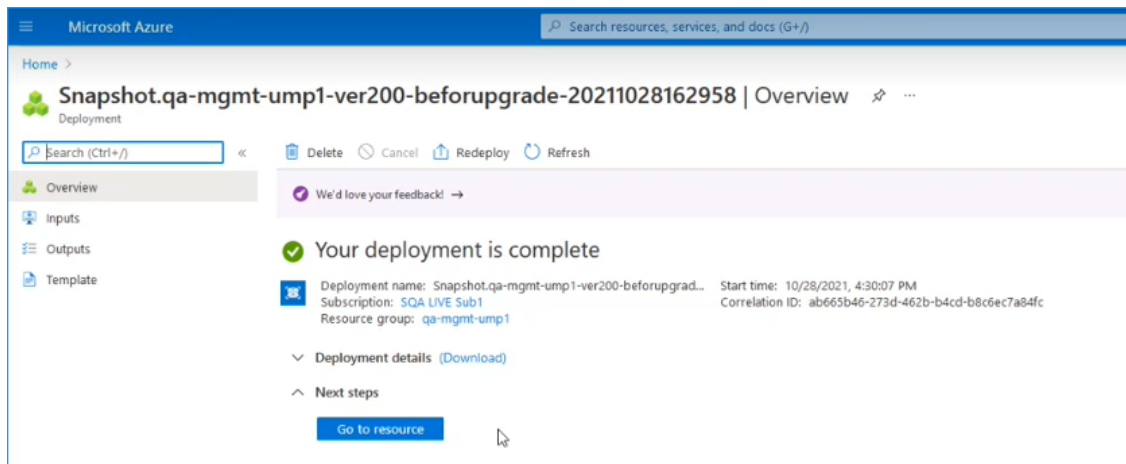
The snapshot is created. The following progress messages are displayed:

The screenshot shows the 'Overview' page for the deployment 'Snapshot.qa-mgmt-ump1-ver200-beforupgrade-20211028162958'. The page indicates that the deployment is in progress. The deployment details are as follows:

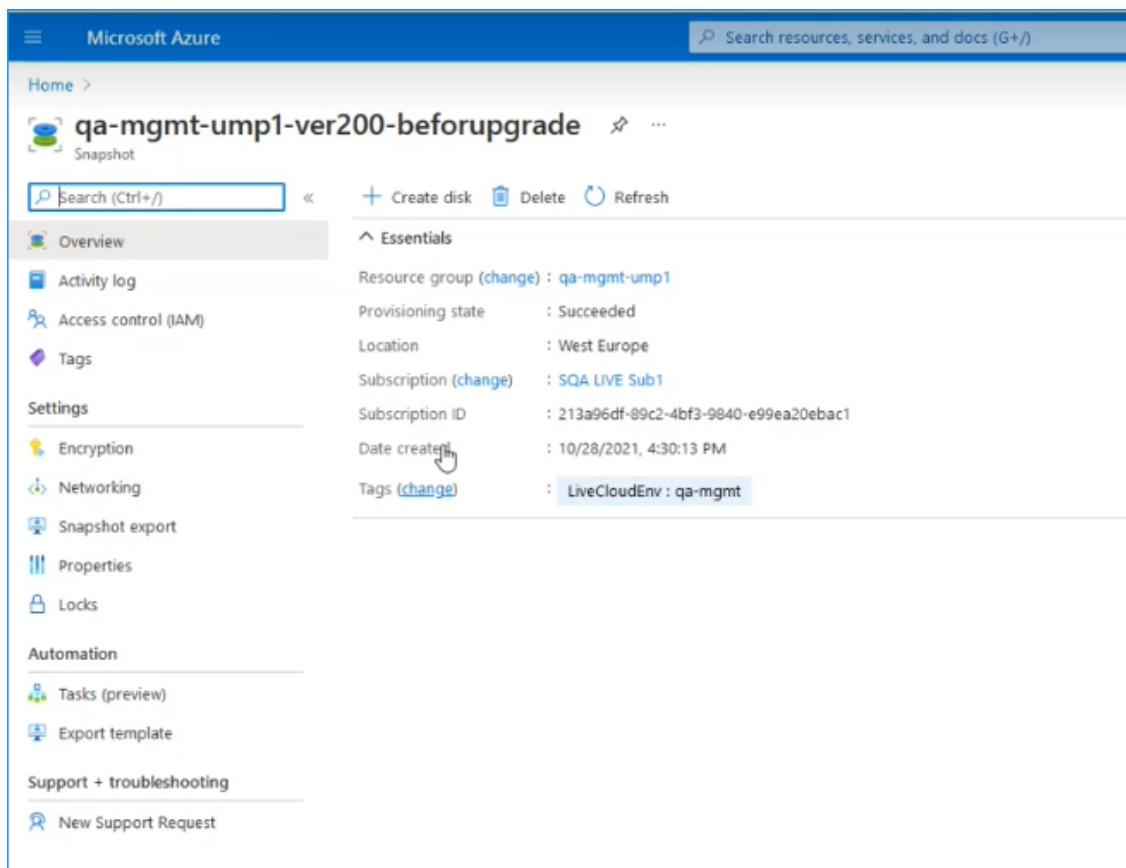
Resource	Type	Status
No results.		

Deployment details (Download)

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



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



Compiling List of Password Authenticated Customers

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

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

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

AuthenticationStatus
Monitor Authentication Status

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

Client Secret

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

Apply Changes Reset Changes

Search:

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

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

Stop wyUpdate Processes

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

Process	Detail
SysAdmin.TenantSvc	This service is the main service of UMP. It controls many operations. For example, it schedules and maintains the auto-replication cycles for all the customers, it sends information to the SysAdminTenant Database, etc.
all SysAdmin.CacheSrv. [tenant_shortname]	Each Hosted Essentials Plus and Hosted Pro 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

Process	Detail	Executable
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
InstallPowershellGetModule	update/install PowerShell get	PowershellGet/PackageManagement

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

Process	Detail	Executable
	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	<ul style="list-style-type: none"> ■ Downloads all the CsOnlineUsers ■ Downloads all the Teams user policies 	
SysAdmin.UMP.SyncAcquiredNumber	Used by Operator Connect (OC) for updating the Assignment Status column in the Number Management table in the self-service portal. It is run every 5	

Process	Detail	Executable
	minutes.	

Additional SysAdmin Verifications

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

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

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

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



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

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

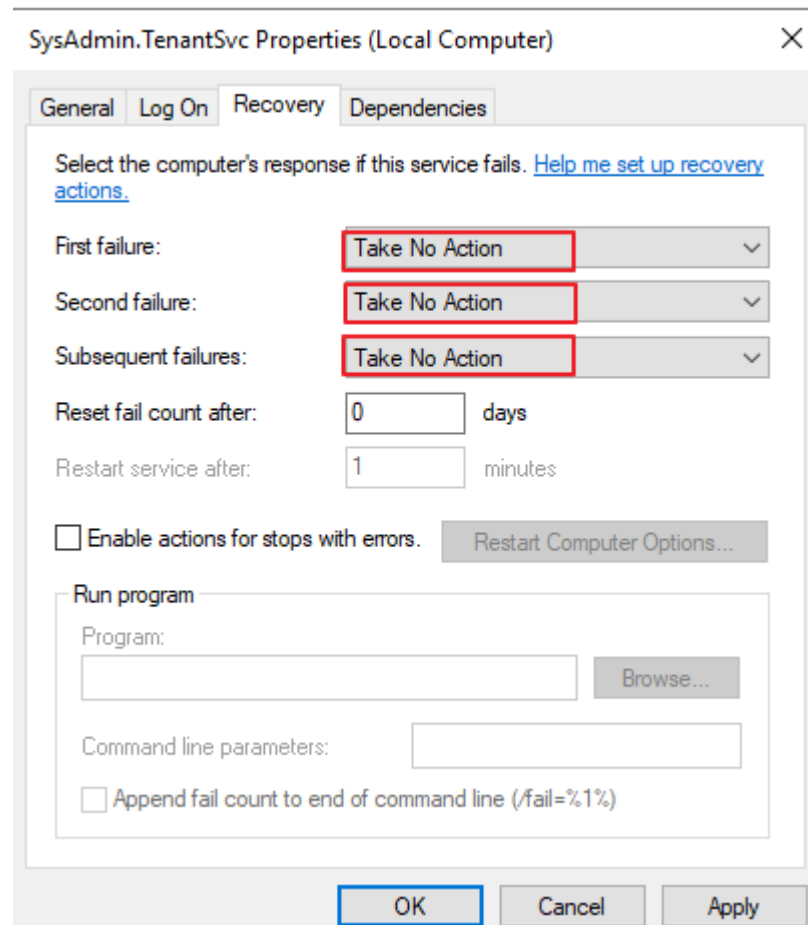
(click  and type **Services**) right-click each of the above services, and then select **Stop**.



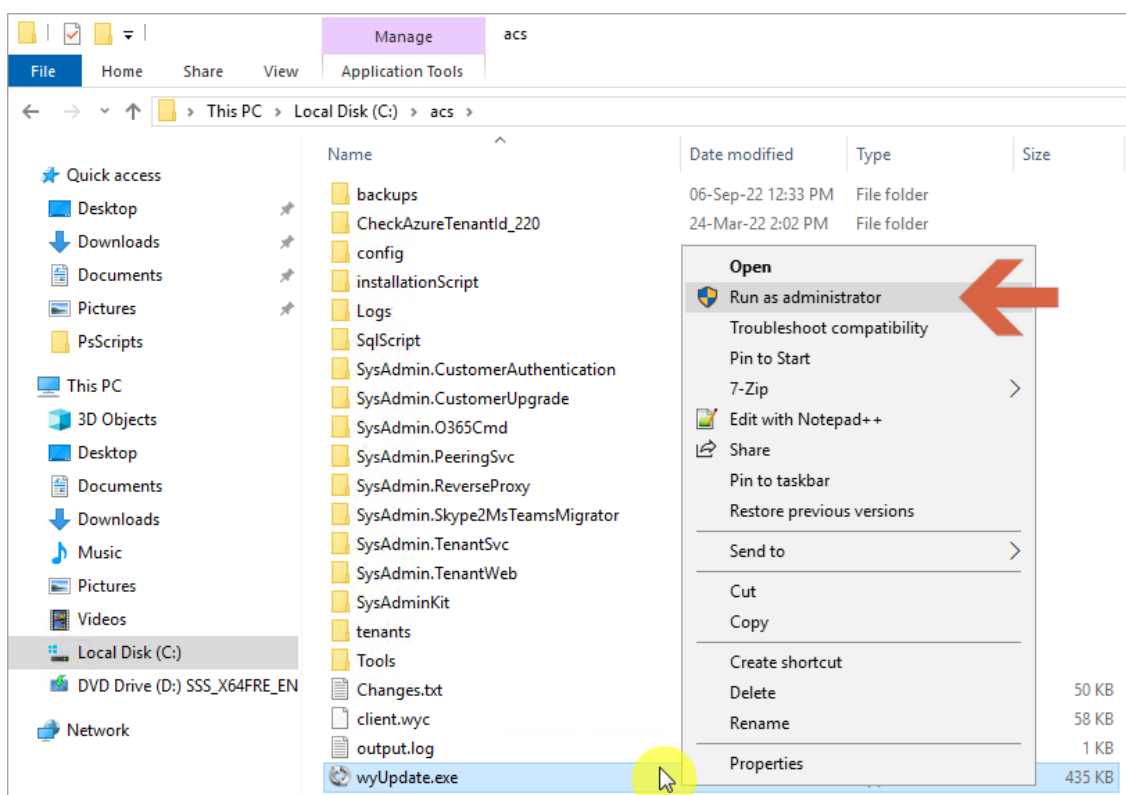
To save time, type only the following command:
`stop-service sysadmin*, w3svc`

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

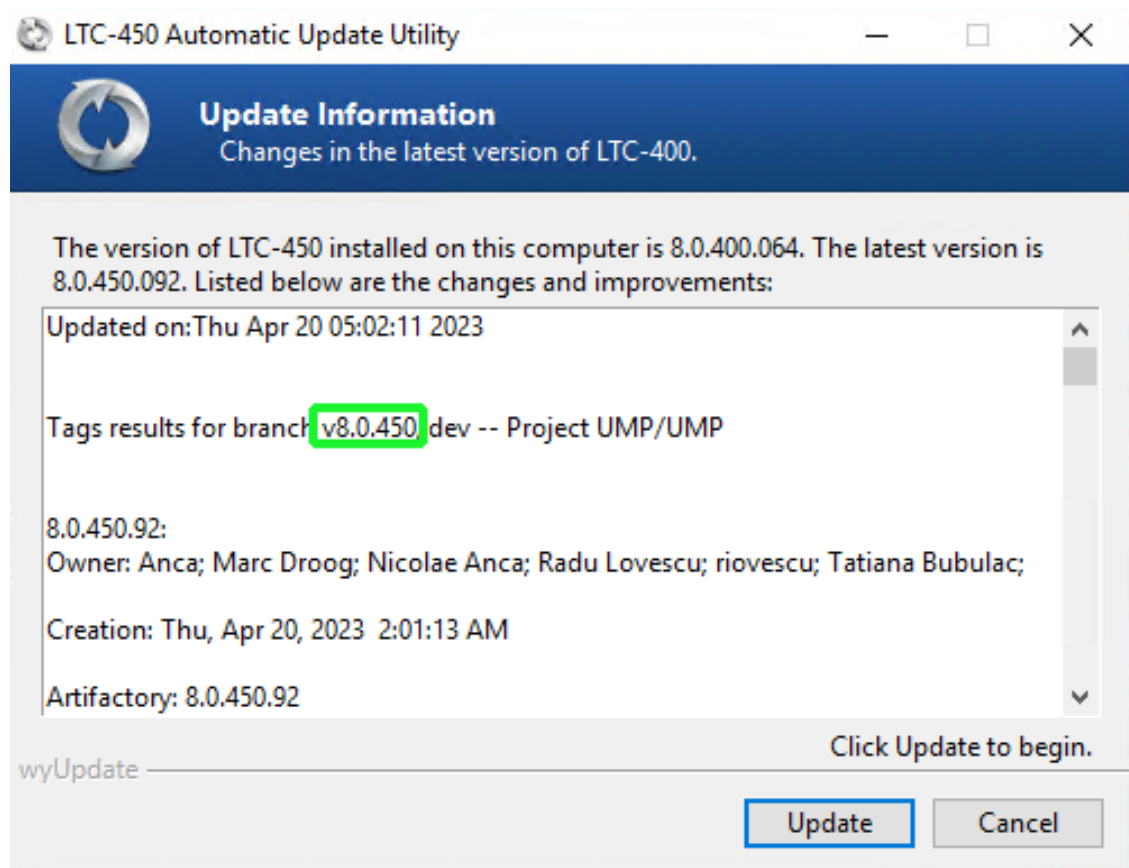
- SysAdmin.TenantSvc
 - SysAdmin.PeeringSvc
 - all SysAdmin.CacheSrv.[tenant_shortname]
5. If a service keeps restarting, set the properties of the service SysAdmin.TenantSvc to **Take No Action** (see example in figure below).



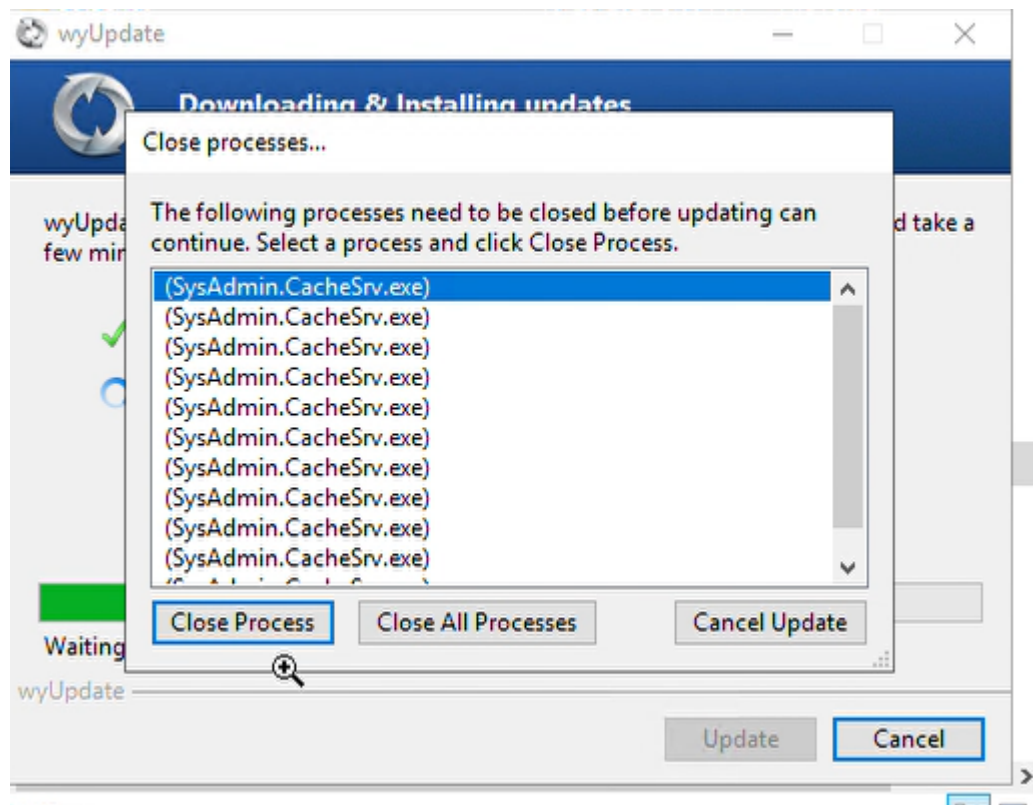
6. Run wyUpdate.exe. (right-click **Run as Administrator**).



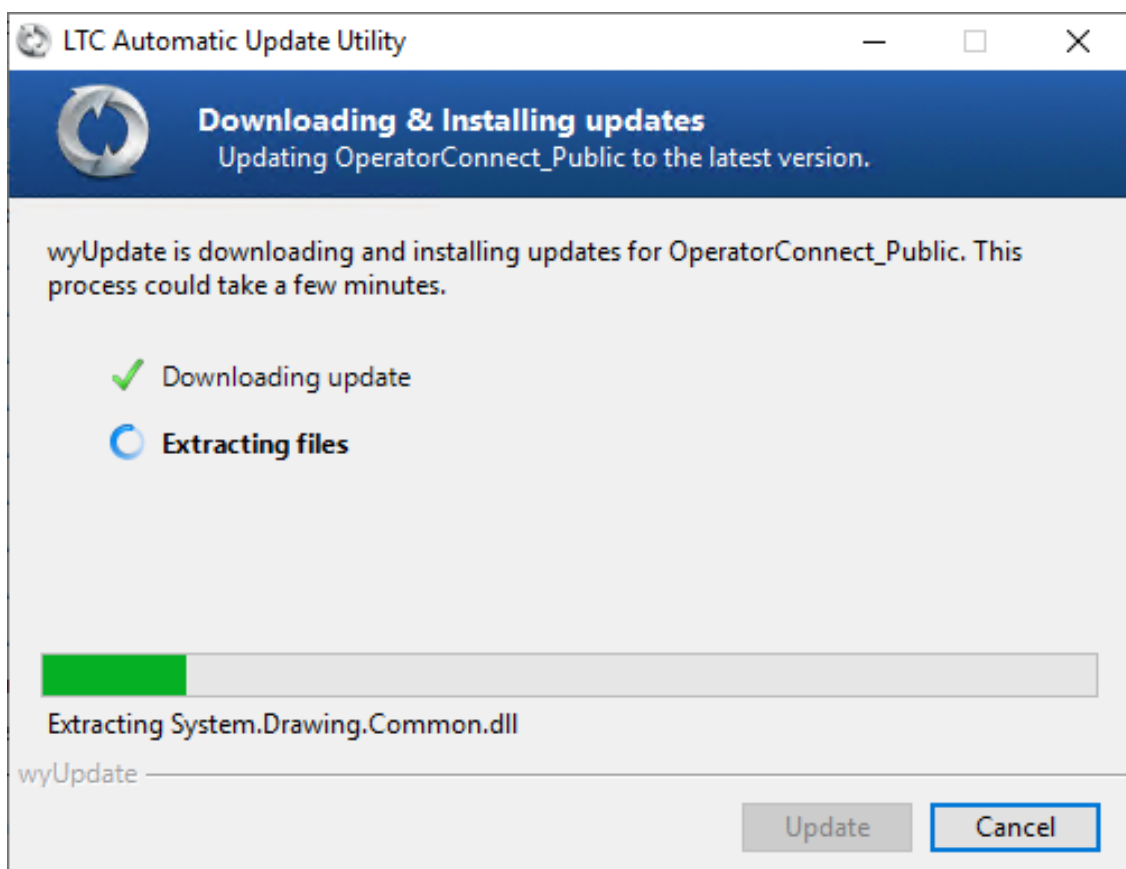
7. In the Updated dialog, click **Update**. The wyUpdate tool validates the installed version to determine whether updates are available, or an upgrade is required.



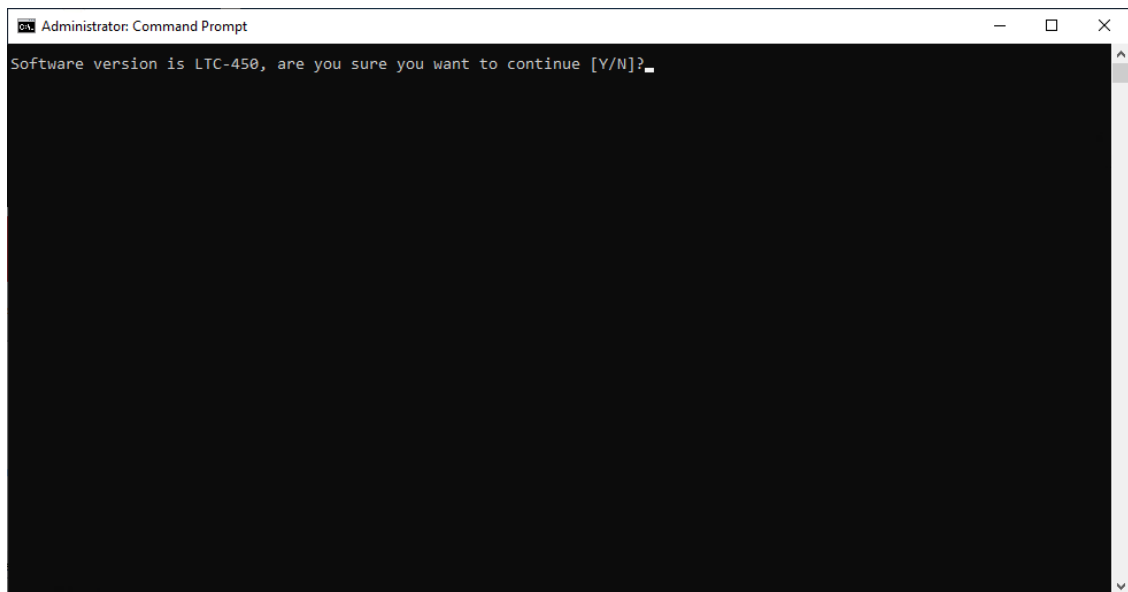
8. If you did not close all the services via PowerShell, then during the update you are prompted to "Close processes...". Confirm this action. This kills the running processes and continues the upgrade.



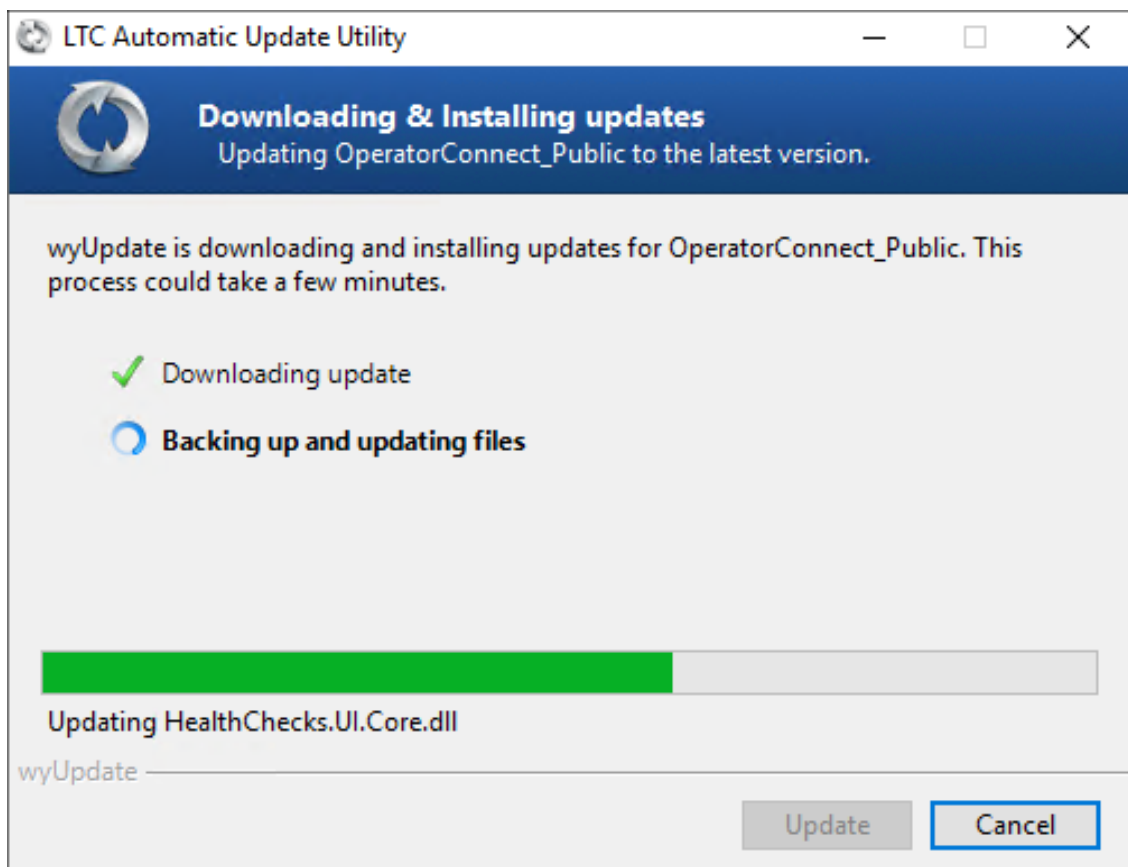
The available updates / version upgrade packages are downloaded to a temporary folder and the files are installed.



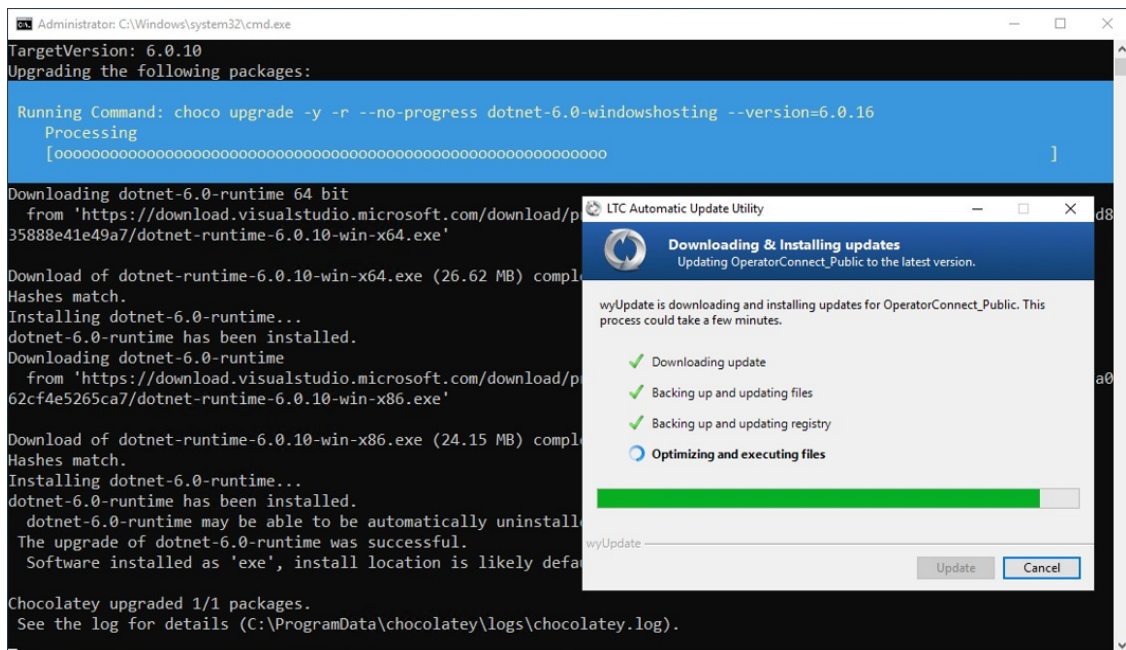
9. The upgrade process is interrupted via the CMD window pop-up. The following prompt is displayed:
Warning ... Are you sure you want to continue. [Y / N] ?
10. Type **Y** and press Enter.



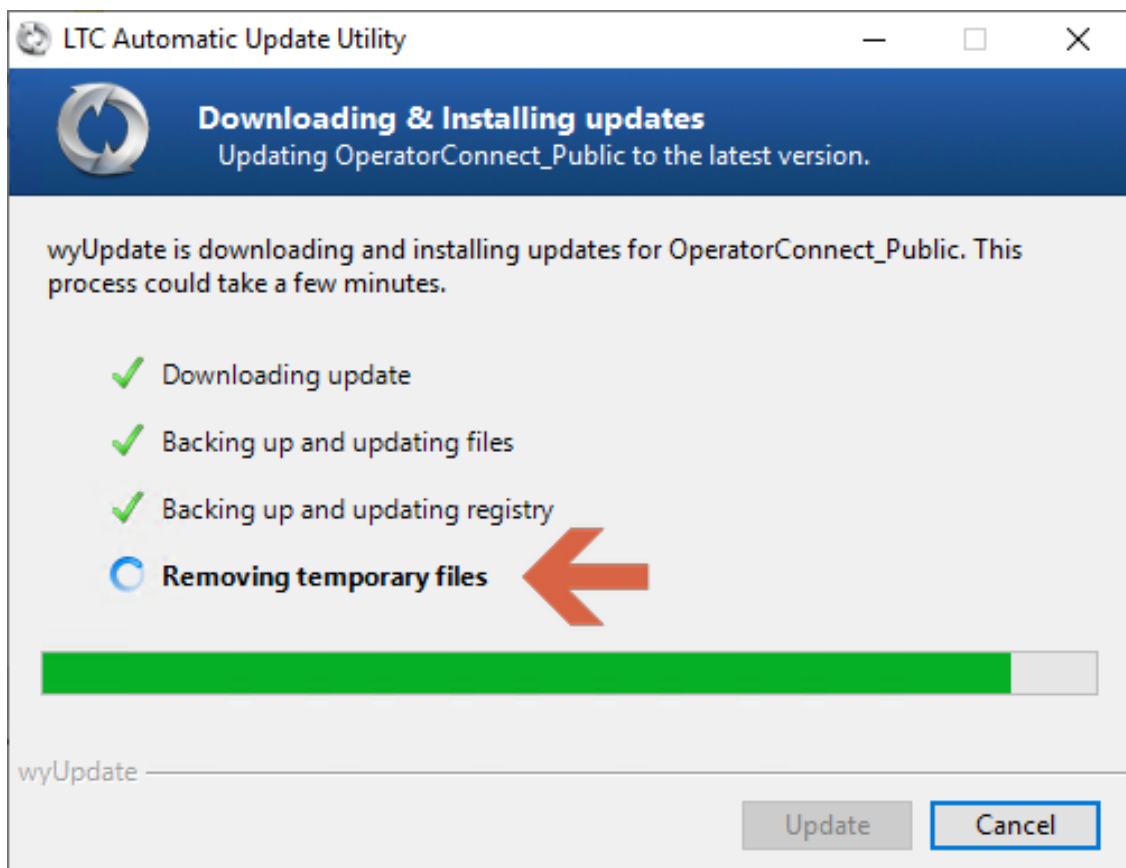
- Folders are backed up and files are updated.



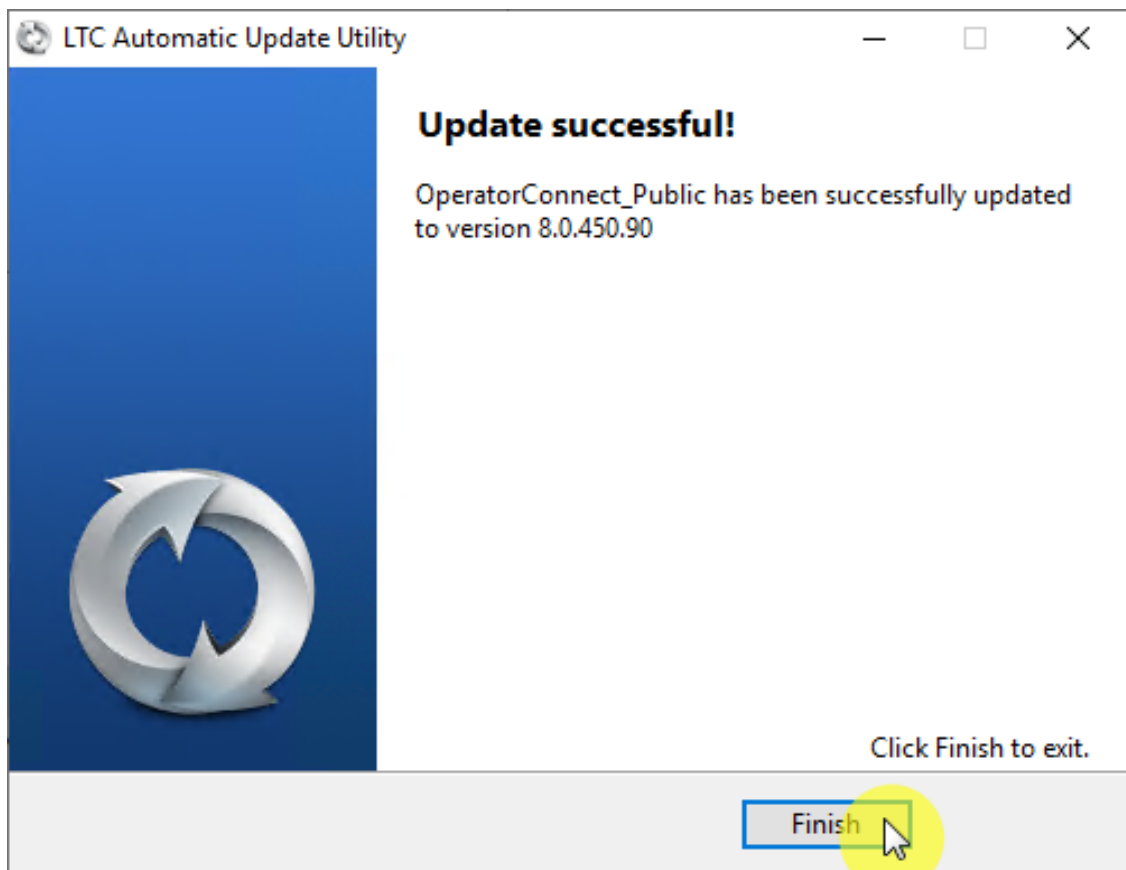
- During the optimization and execution, various necessary software packages are installed as described in [Stop wyUpdate Processes](#) on page 9.



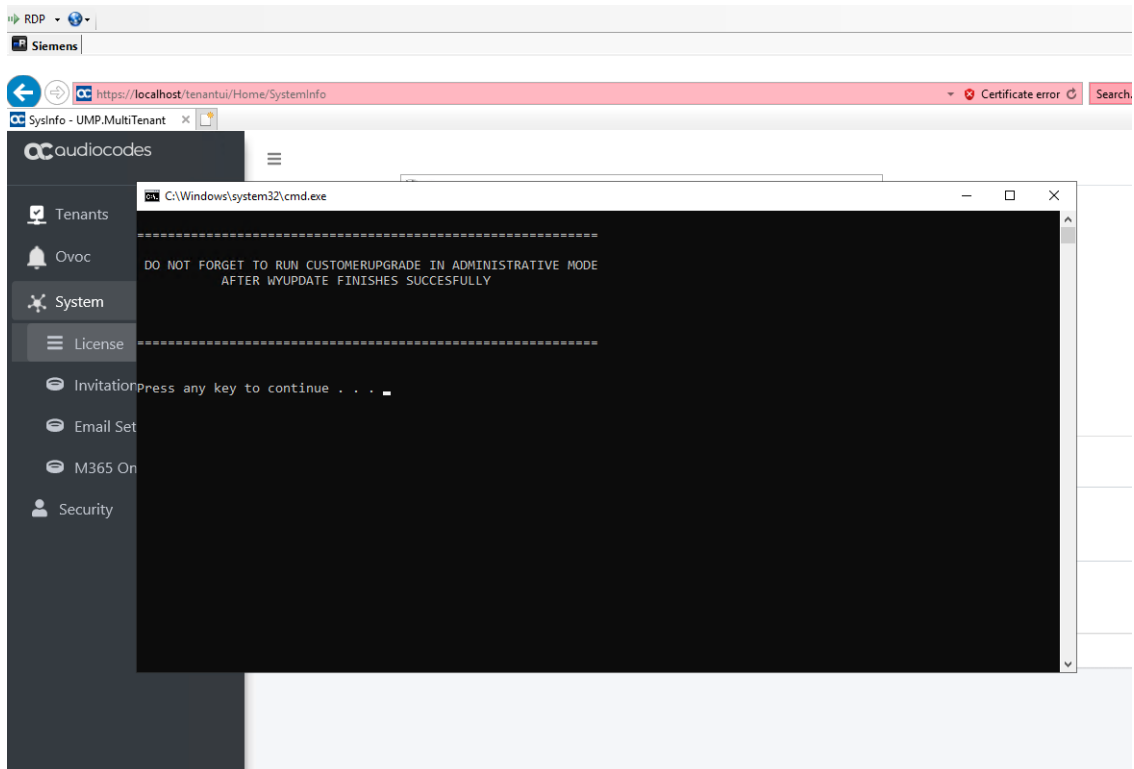
- Temporary files are removed.



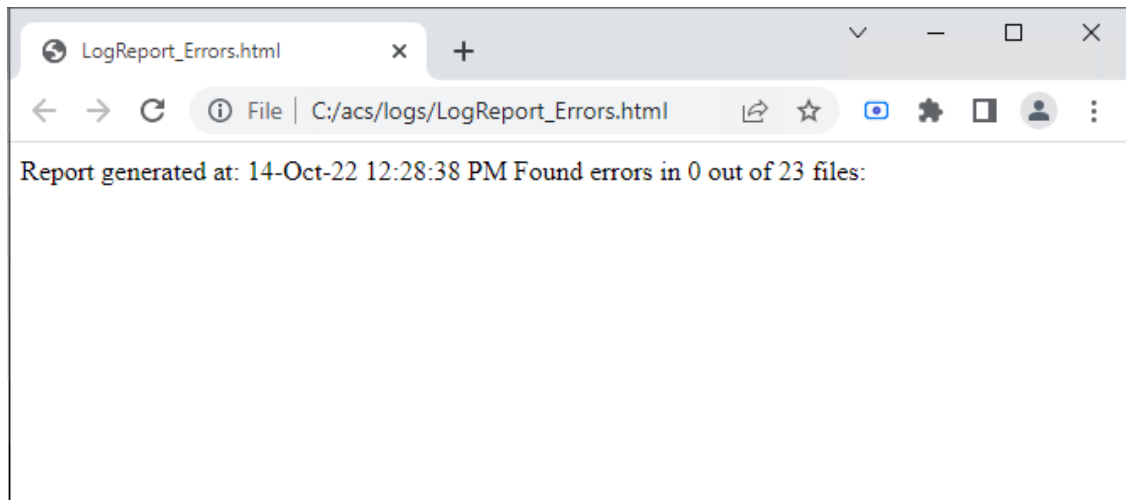
11. Click **Finish**.



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



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



4 Upgrading Customer Tenant

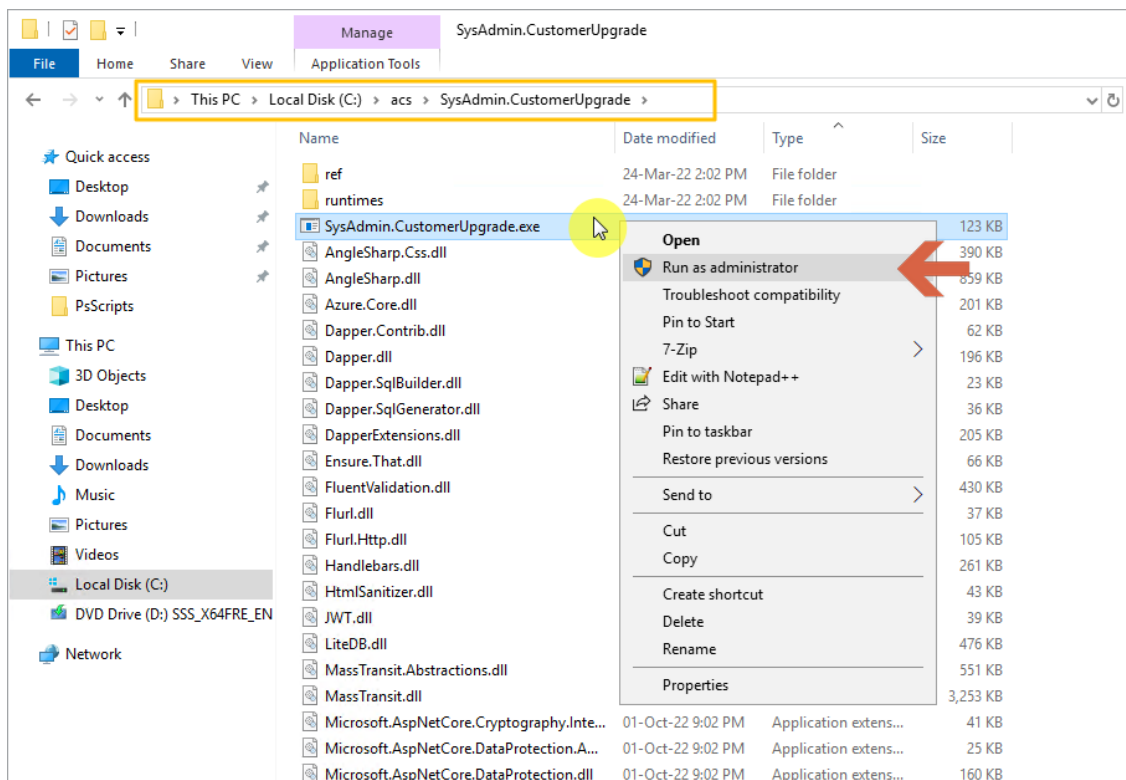
This step describes how to run the Customer Upgrade service for updating each customer tenant.



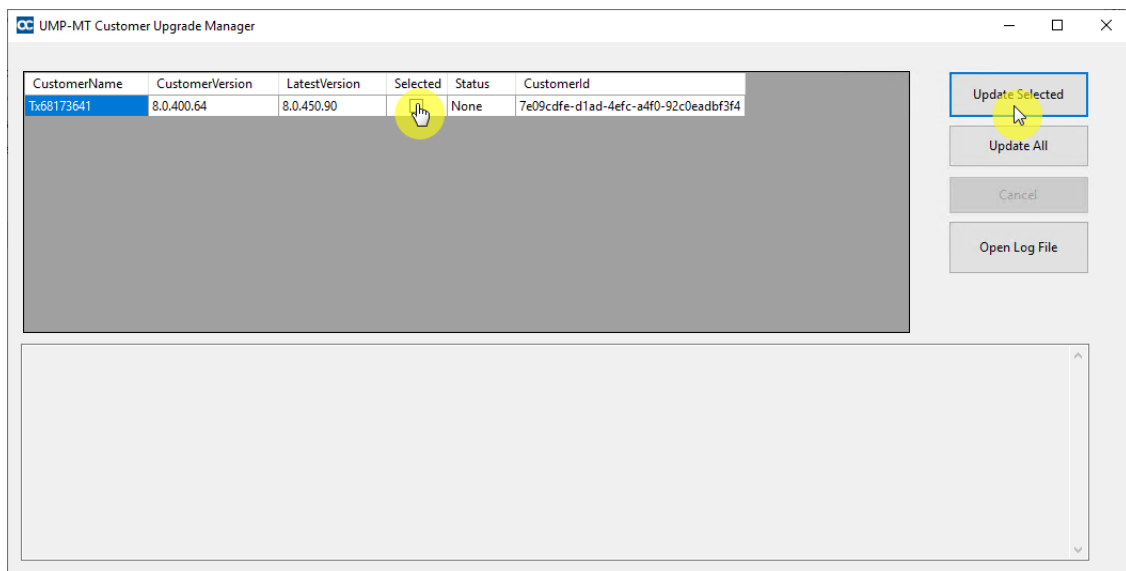
- Run the Sysadmin.CustomerUpgrade.exe as an Administrator using the UMP service admin account that was created in "Create UMP Service Account" in User Management Pack 365 Administrator and Installation Manual.
- If you have a back-end SQL server for all your tenants, ensure that the username and password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

➤ Do the following:

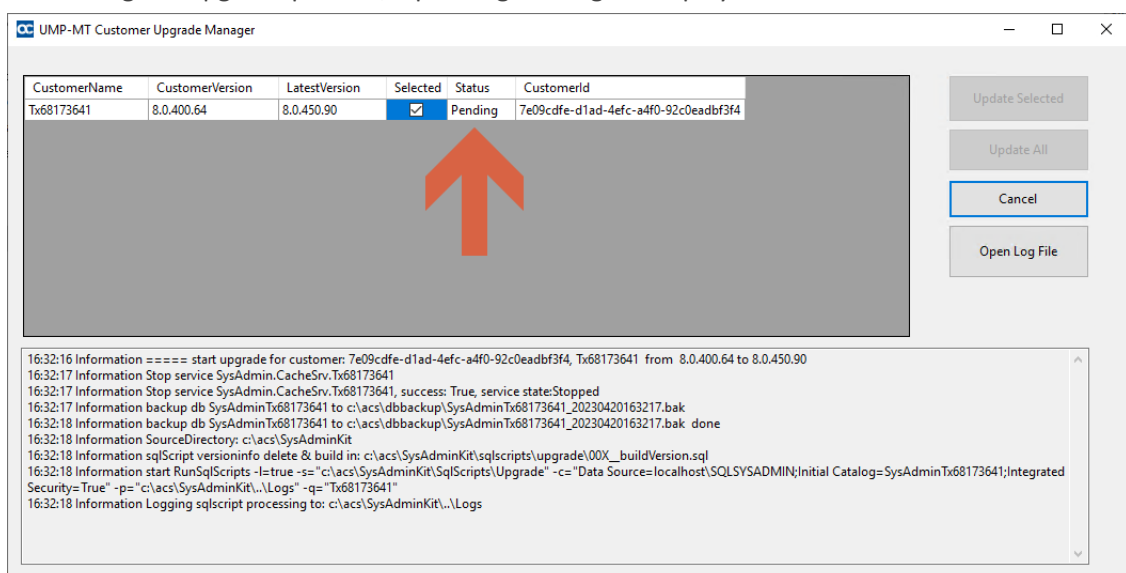
1. Run the file Sysadmin.CustomerUpgrade.exe from directory C:\acs\SysAdmin.CustomerUpgrade.



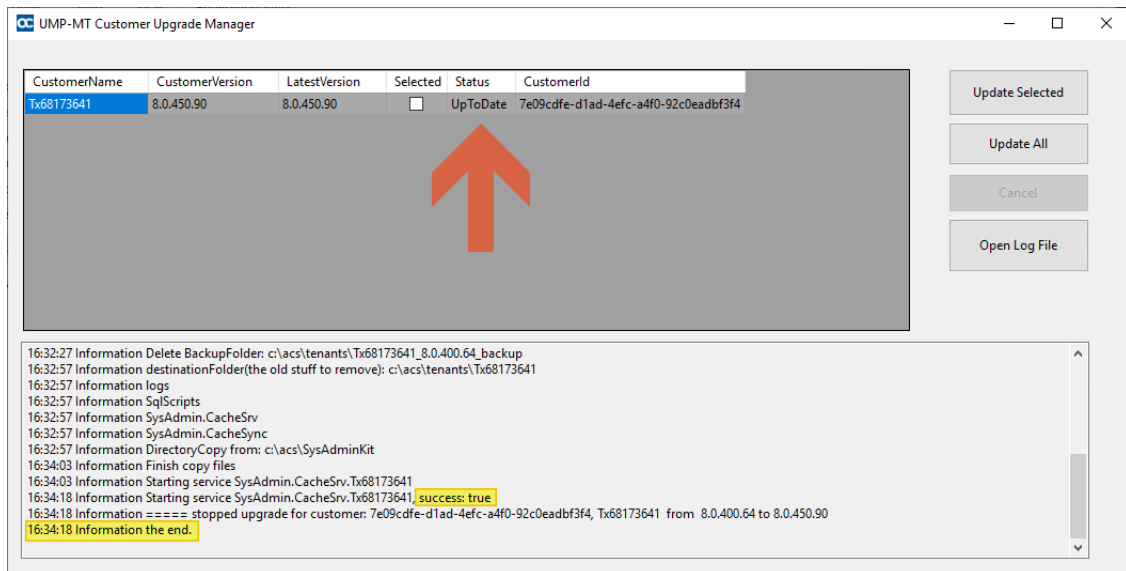
2. In the Customer Upgrade Manager, select the customers for which you wish to upgrade and then click **Update Selected**.





During the upgrade process, a pending message is displayed.



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



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

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

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

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

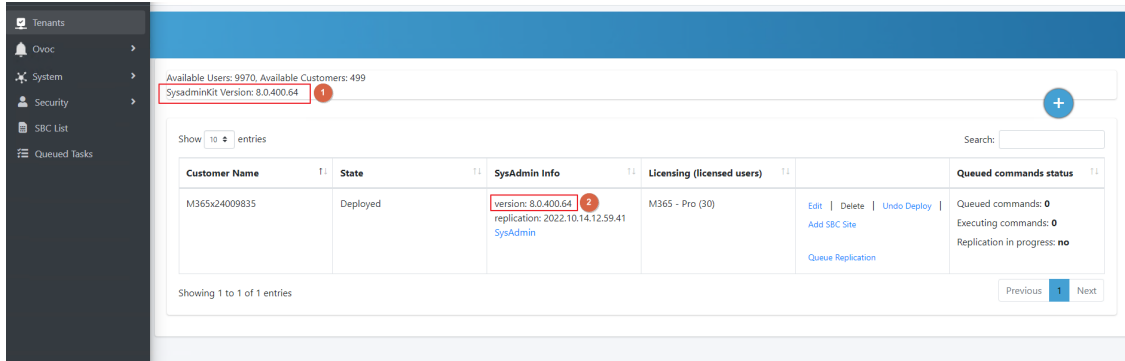
Status      Name                DisplayName
-----
Running     SysAdmin.CacheS... SysAdmin.CacheSrv.24009835
Running     SysAdmin.Peerin... SysAdmin.PeeringSvc
Running     SysAdmin.TenantSvc SysAdmin.TenantSvc
Running     w3svc               World Wide Web Publishing Service

PS C:\Users\Administrator> 
```



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

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



The screenshot shows the 'Tenants' page in the Multitenant portal. The left sidebar contains navigation links: Tenants, Ovoc, System, Security, SBC List, and Queued Tasks. The main content area displays a summary at the top: 'Available Users: 9970, Available Customers: 499' and 'SysadminKit Version: 8.0.400.64' (marked with a red box and a red circle with the number 1). Below this is a table with columns: Customer Name, State, SysAdmin Info, Licensing (licensed users), and Queued commands status. The table contains one entry for customer 'M365x24009835' with state 'Deployed'. The 'SysAdmin Info' column for this entry shows 'version: 8.0.400.64' (marked with a red box and a red circle with the number 2), 'replication: 2022.10.14.12:59:41', and a link to 'SysAdmin'. The 'Licensing' column shows 'M365 - Pro (30)' and links for 'Edit', 'Delete', 'Undo Deploy', 'Add SBC Site', and 'Queue Replication'. The 'Queued commands status' column shows 'Queued commands: 0', 'Executing commands: 0', and 'Replication in progress: no'. At the bottom of the table, it says 'Showing 1 to 1 of 1 entries' and has 'Previous', '1', and 'Next' navigation buttons.

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

5 Post Upgrade Actions

This section describes the actions to perform following the upgrade:

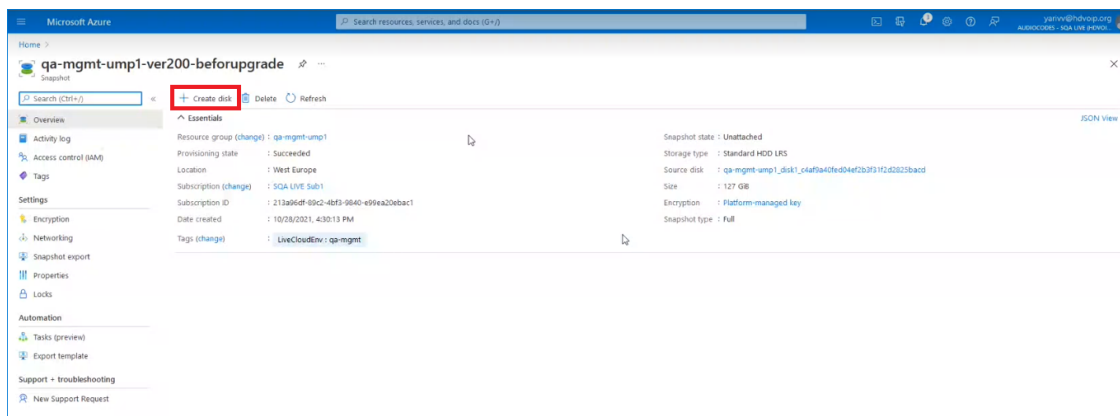
- [Restoring UMP Snapshot](#) below
- [Verifying Tenant Admin Authentication](#) on page 30
- [Upgrading M365 Connection to Token Authentication](#) on page 31
- [Updating Scripts](#) on page 41
- [Verifying Component Statuses](#) on page 41
- [Updating SQL Server](#) on page 44
- [SBC Dialplan Verification](#) on page 44

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**.



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

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

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

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

Disk details

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

At the bottom, there are three buttons: 'Review + create' (blue), '< Previous' (disabled), and 'Next : Encryption >' (disabled, with a mouse cursor hovering over it).

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

The screenshot shows the 'Create a managed disk' page in the Microsoft Azure portal. The breadcrumb path is 'Home > qa-mgmt-ump1-ver200-beforupgrade >'. The page title is 'Create a managed disk'. Below the title are tabs for 'Basics', 'Encryption', 'Networking', 'Advanced', 'Tags' (which is selected), and 'Review + create'. A note explains that tags are name/value pairs for categorizing resources and consolidated billing. Below the note is a table with three columns: 'Name', 'Value', and 'Resource'. The first row has 'LiveCloudEnv' in the 'Name' column, a dropdown menu in the 'Value' column (showing 'qa-dev', 'qa-int', and 'qa-mgmt' with 'qa-mgmt' selected), and '2 selected' in the 'Resource' column. The second row has an empty 'Name' field, 'qa-dev' in the 'Value' column, and '2 selected' in the 'Resource' column. At the bottom are three buttons: 'Review + create' (blue), '< Previous', and 'Next : Review + create >'.

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

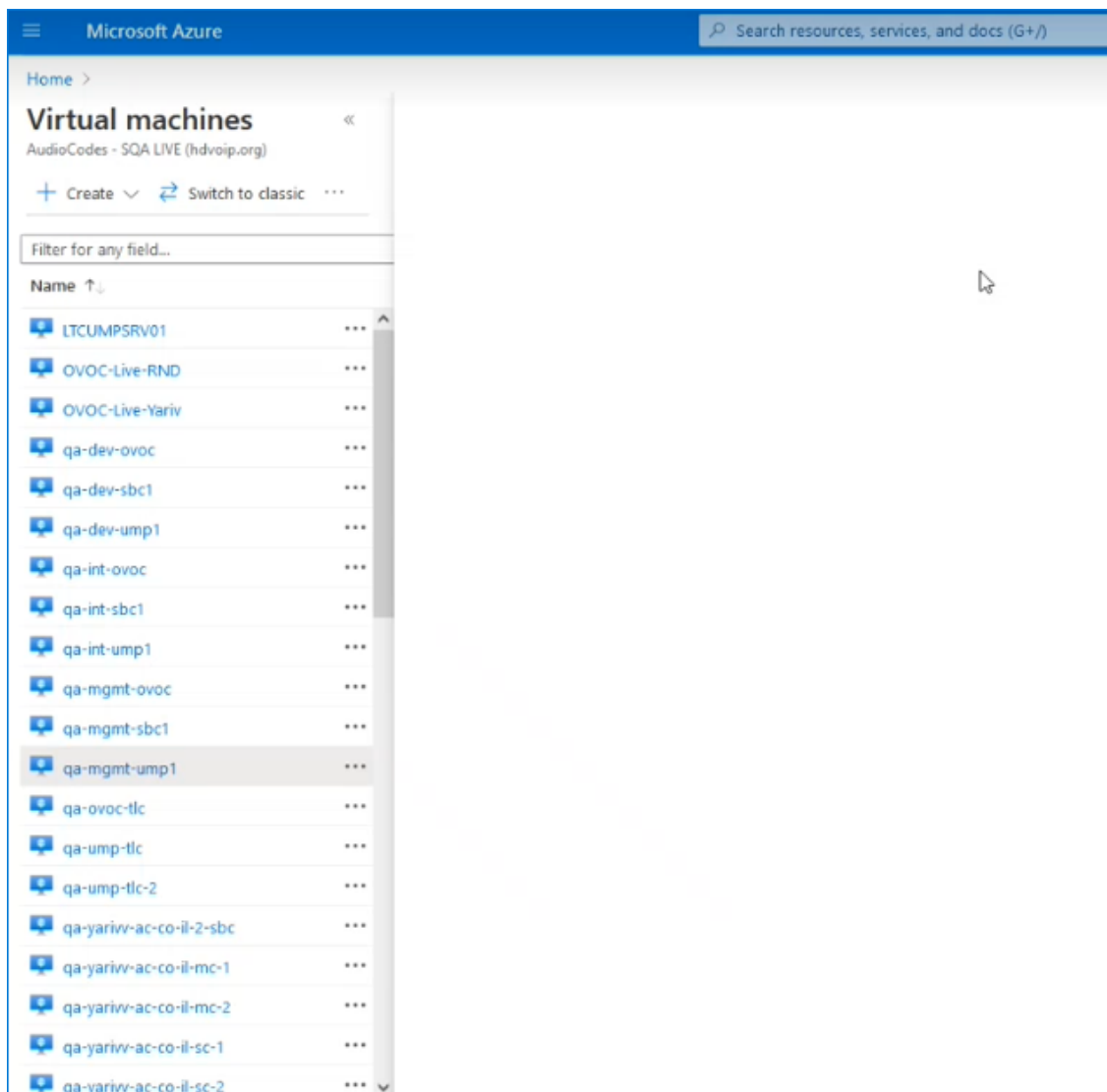
Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

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

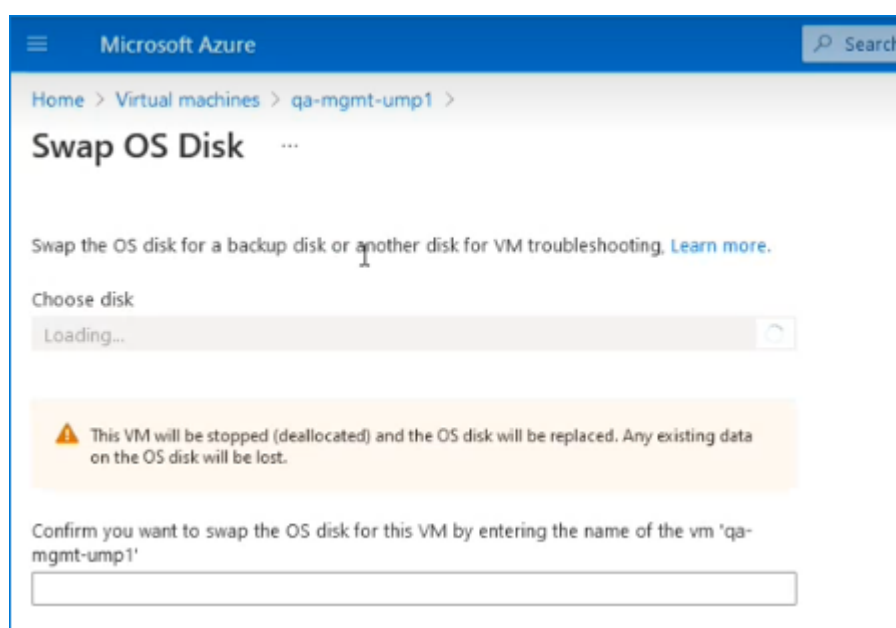
Name	Value	Resource
LiveCloudEnv	qa-mgmt	2 selected
	qa-dev	2 selected

Review + create < Previous Next : Review + create >

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



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



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

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

Verifying Tenant Admin Authentication

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

➤ Do the following:

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

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

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

4. Reload the table (3).
5. If any Tenant verification fails, verify credentials and retry.

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

Upgrading M365 Connection to Token Authentication

Customers upgrading 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).



Using this method, you must disable Multi-factor authentication.

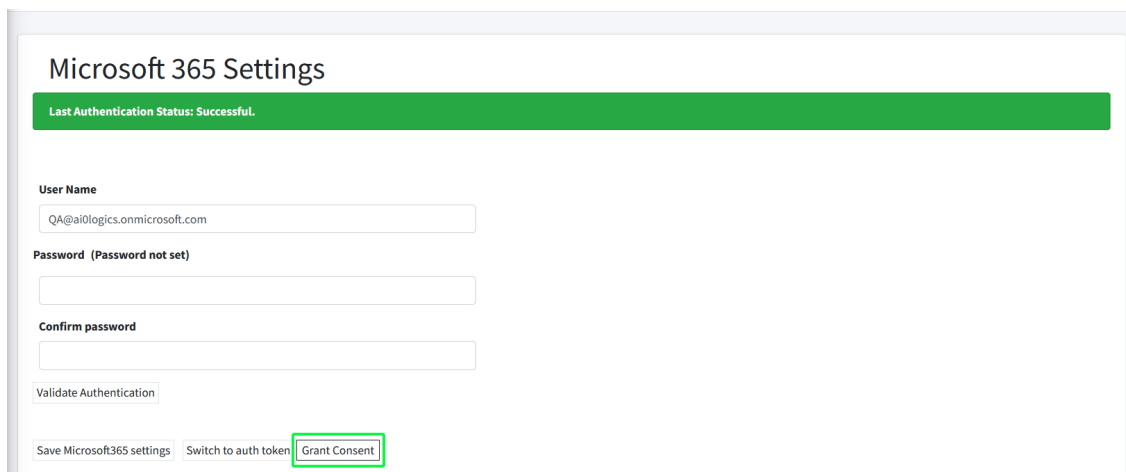
- **Token-only authentication:** A Microsoft Graph access token is claimed directly, triggered by an email link sent to the customer. For implementing this option, select the **Switch to auth token** option in the Microsoft 365 Settings screen (see [Switching to Token Authentication](#) on page 34). 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 Customer portal Navigation pane, select **Configuration > M365 Configuration**.



Microsoft 365 Settings

Last Authentication Status: Successful.

User Name
QA@ai0logics.onmicrosoft.com

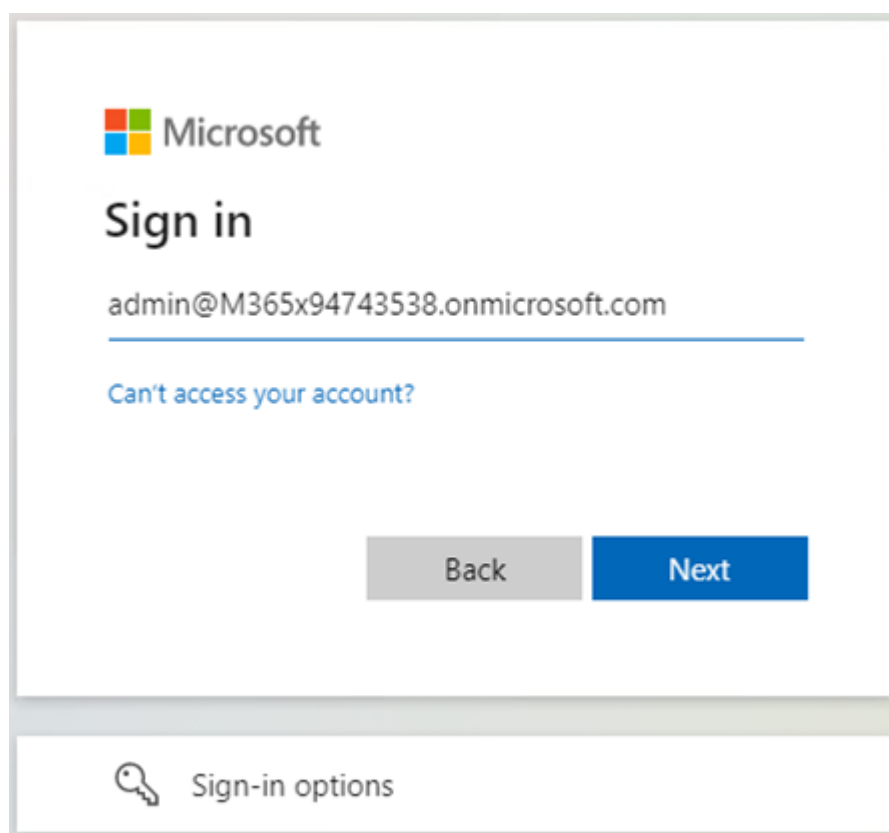
Password (Password not set)

Confirm password

Validate Authentication

Save Microsoft365 settings Switch to auth token **Grant Consent**

2. Click **Grant Consent**.



Microsoft

Sign in

admin@M365x94743538.onmicrosoft.com

[Can't access your account?](#)

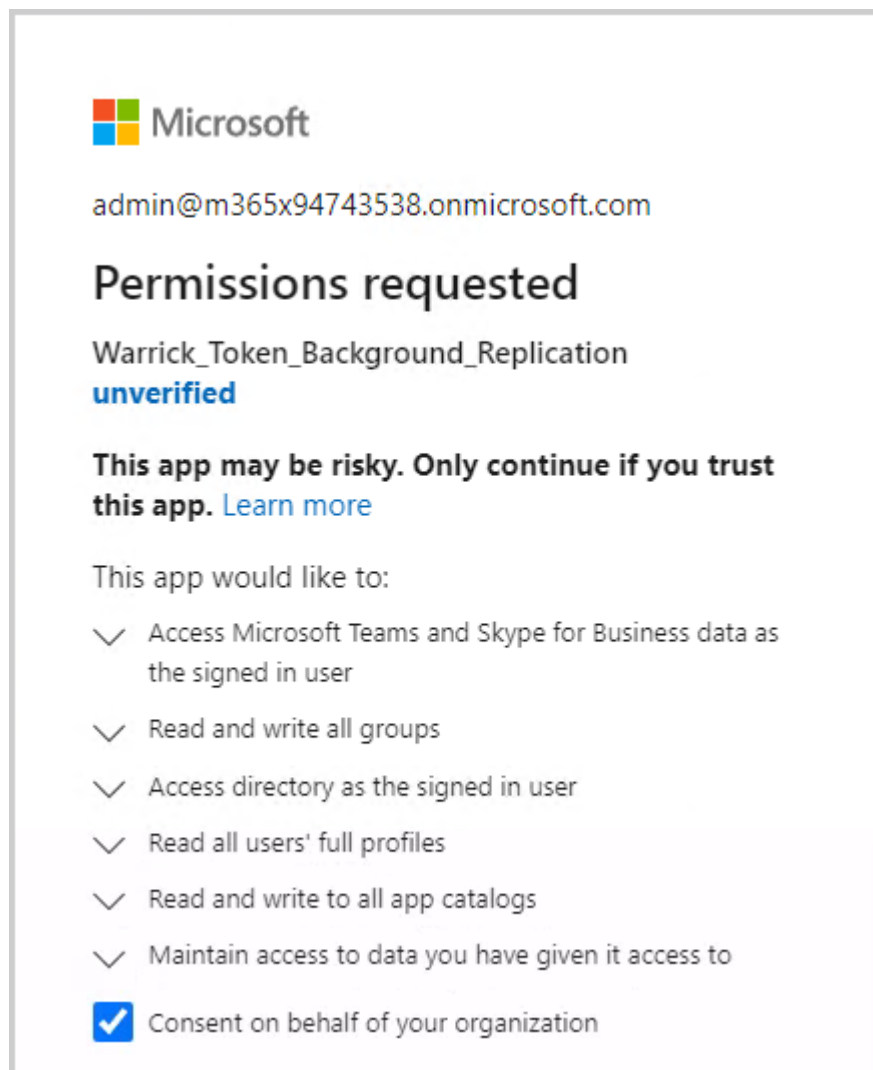
Back Next

Sign-in options

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

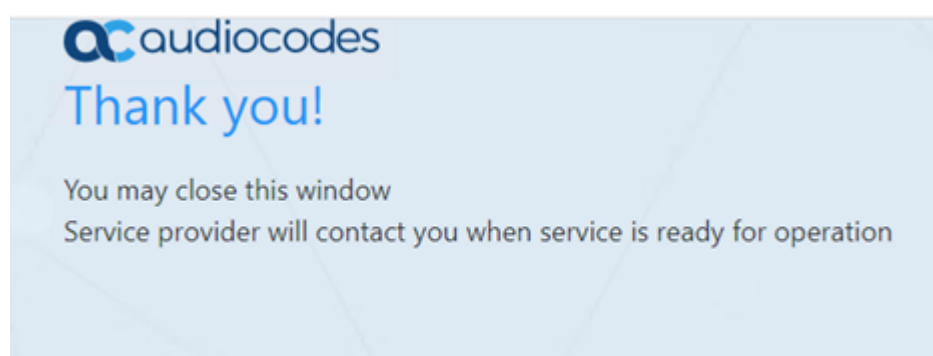
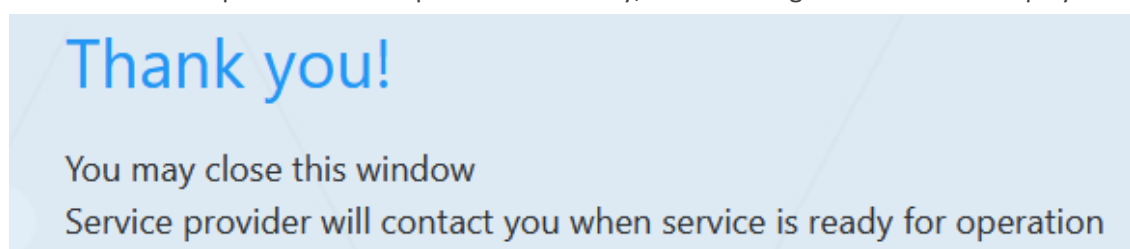


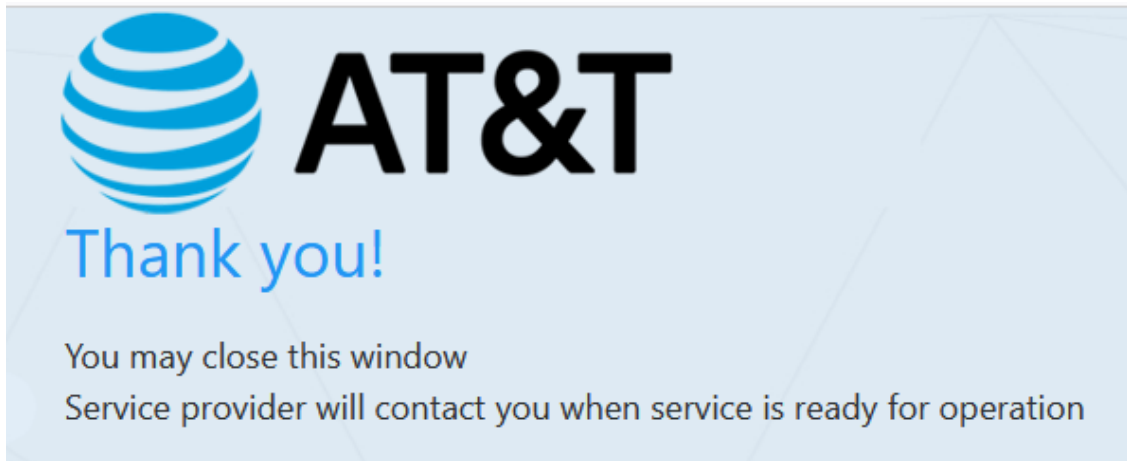
The M365 User Account must have "Global" Admin permissions, otherwise the "Consent on behalf of the organization" check box does not appear.



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

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





Microsoft Azure

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

Warrick_Token_Background_Replication | Permissions

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

Permissions

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

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

Grant admin consent for Contoso

Admin consent User consent

Search permissions

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

Microsoft Azure

Home > Contoso > Enterprise applications > Enterprise applications

Enterprise applications | All applications

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

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

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

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

1 application found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Status
Warrick_Token_Background_Replicat...	e4c42766-9690-4504-89ad-e4ef9545931	102a2c69-9495-430e-9c0f-9ad33d93e560		4/19/2023	-

Switching to Token Authentication

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



This is recommended method for securing connection to Microsoft 365.

➤ **To switch to token authentication:**

1. In the Customer portal Navigation pane, select **Configuration > M365 Configuration**.
2. Click **Validate Authentication** to ensure current token is valid. Last Authentication Status: Successful is displayed.

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

The following dialog is displayed.

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

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

Microsoft 365 Settings

Tenant has open invitation.

User Name

admin@M365x74218585.onmicrosoft.com

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

Switch to user/pwd Resend invitation

Save Microsoft365 settings

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

Customer Invitations

Reload data Edit

Search:

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

Showing 1 to 1 of 1 entries

Previous 1 Next

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

Dear Administrator of BBBTrunkService,

We at Sandbox3.FineBak welcomes you to join our "Live Platform" 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-2BkTVwNmIXwDan5D3X3qLeRR5pTZuHhM2MidO7oDmN0X9aTKlI9d-2F9aB3GzQwTashQwmnZ1GNQpY9nSv-2FPQcAE7HCH8GILSakaoPLTHOH9a7t6e62B9Ckux143YS62zSh4TadEeqek40lbnvqqcC0lberD-2FF19p2MaX8aJGieBlicCMYmF8-5BNb2H0WjMRq-3D-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

Delete Archive Report Reply Reply all Forward Read / Unread Categorize Flag / Unflag Print

Welcome BradTokenMail for joining the FixedMobileUC "AudioCodes UMP-365 for Microsoft Teams for Service Providers" service

onboarding@audiocodes.be
To: Christie Cline
Tue 10/10/2023 7:06 AM

Dear Administrator of BradTokenMail,

We at Sandbox3.FineBak welcomes 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:

http://url1207.audiocodes.be/ls/click?upn=a12WafRd4t4P7-2B7DSbr5PxErMpe1UbCLZS-2BkTVwNmIXwDan5D3X3qLeRR5pTZuHhM2MidO7oDmN0X9aTKlI9d-2B792BcHOZfmXMslQ9k0MBuV-2FZSJh04lpolVN89d-2BvsvdV8_Zf9noBSXp6zmd8GcAmse0OWHK9cYyBOWUHtR10jabvaXDFepb1E5fL9imoJaYqeHfCE4A7a6Zu25GCAdRYVKrTPJMR48G4xBSL4zSW1vrBOxm6rDxgjyHg-2F7RUtIEEK2K6pem-2Fnavt3vINGb2Rx-2B3ykMieYXDN8ZCDYhc9UOhWkdIwFHmUlf0i-2Bp8fTdsWYiKlpUAetlBHEyeS7LuzurpzAzy7nxUSFDnM5ADmrobSpvBkZWGff6c9YqCXIrjZT

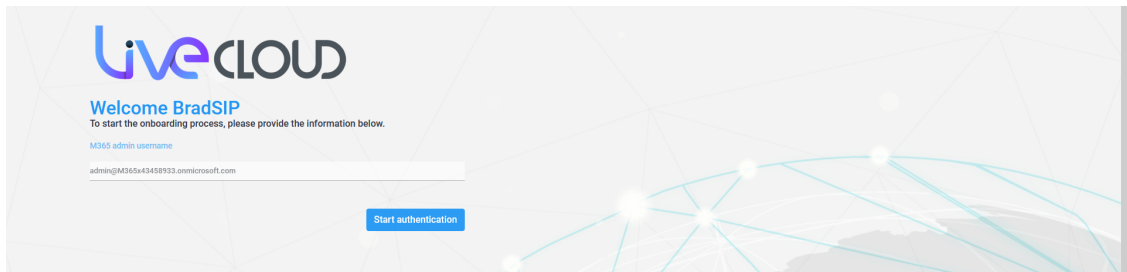
Please Note that Global Admin will be required in order to approve the UMP-365 consents.

- 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.

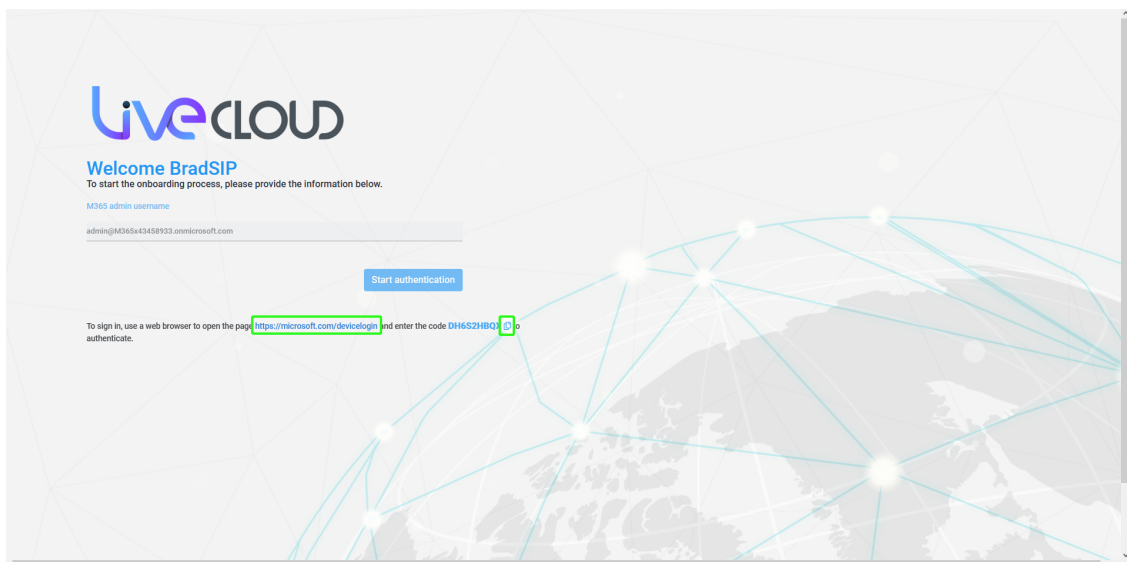
Thank you and best regards,
Sandbox3.FineBak Team

Reply Forward


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



- Click **Start authentication**.



- Copy the displayed code to clipboard and then click the link highlighted above.
- Open the web browser link shown below the **Start authentication** button.


 Microsoft

Enter code

Enter the code displayed on your app or device.


DH6S2HBQX|

Next

 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

⋮

10. Choose the account of the customer tenant administrator with "Global" permissions or Service Account (see Secure Token Connection).
11. You will be prompted to authenticate your account using Microsoft Authenticator. A screen similar to the following is displayed.



admin@m365x43868129.onmicrosoft.com

Approve sign in request



Open your Authenticator app, and enter the number shown to sign in.

17

No numbers in your app? Make sure to upgrade to the latest version.



admin@m365x43458933.onmicrosoft.com

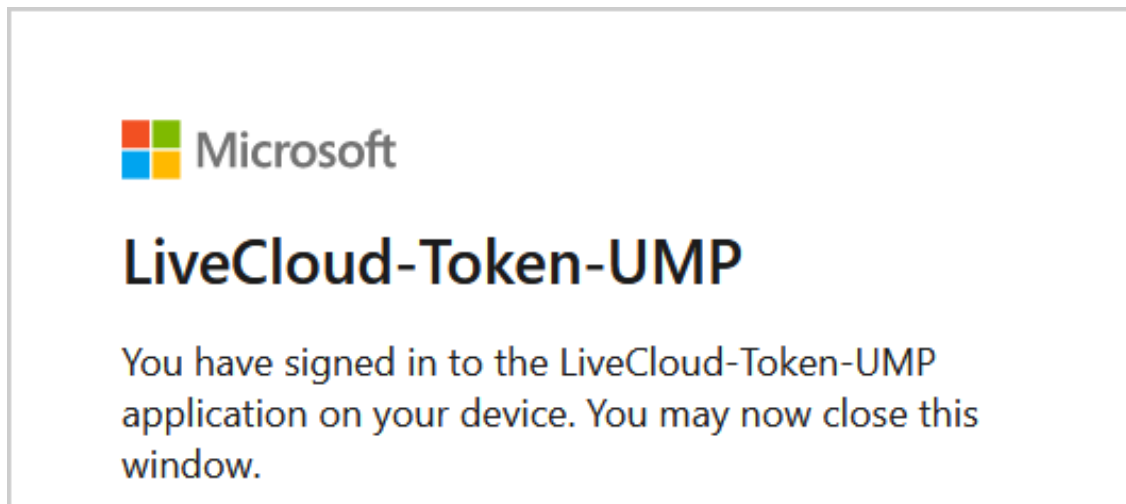
Are you trying to sign in to LiveCloud-Token-UMP?

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

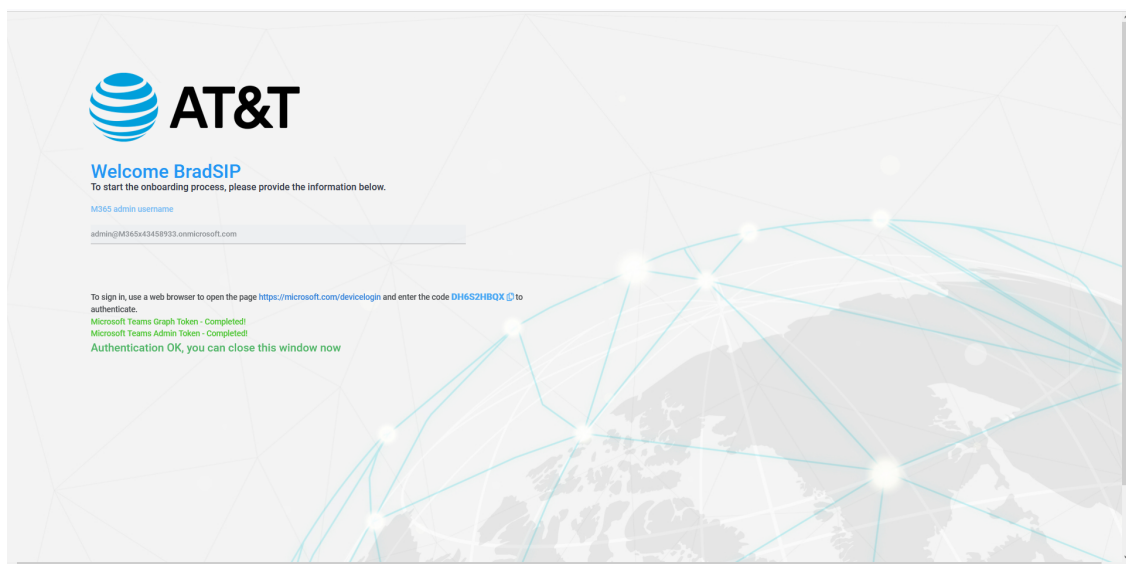
Cancel

[Continue](#)

12. Click Continue.



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



14. Close the above window.

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

Microsoft 365 Settings

Last Authentication Status: Successful.

User Name
admin@M365x43458933.onmicrosoft.com

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

Validate Authentication

Save Microsoft365 settings **Switch to user/pwd**

QOE Integration with Microsoft Teams

Azure Application Id

Azure Application Password

Save QOE Integration settings

CsOnlineUser Filter

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

Customer Invitations

Reload data Edit

Search:

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



Template scripts containing incorrect syntax will not be executed.

Verifying Component Statuses

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

Interface	Menu Navigation Path	Check	Configuration Action
Live Cloud/OVOC	Network > Device > Manage	<input type="checkbox"/>	Verify the UMP-365 Device Status is Active in the Devices table (see Device Status on page 45).
		<input type="checkbox"/>	Open the Managed Device page, select device , click Show and verify that “UMP Management” displays Connected (see Device Status on page 45).
Live Cloud Only	Open Device Page for UMP Tenant	<input type="checkbox"/>	Verify Customers Deployment State is Deployed . See Deploy Status and Status Indicators on page 50.
		<input type="checkbox"/>	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	<input type="checkbox"/>	Verify "MultiTenant Version: latest version. See Multitenant Portal Licensing on page 51.
		<input type="checkbox"/>	Verify available license is not missing.
	System > Invitation Settings	<input type="checkbox"/>	Verify Customer Authentication Portal Url is set to: https://<UMP_FQDN>/authenticate. See Configuring Invitation Settings on page 51.
	Security > Authentication Status	<input type="checkbox"/>	Verify that the Client ID and Secret ID are provided by the Synchronization app registration (check PMP site).
		<input type="checkbox"/>	Verify that the Redirect Url is set to: https://<UMP_FQDN>/authenticate/OAuth2Callback <div>  Verify that the same redirect Uri is configured for the Synchronization App registration. See Authentication Status on page 53. </div>

Interface	Menu Navigation Path	Check	Configuration Action
	SBC List	<input type="checkbox"/>	Verify that the SBC exists. See Managing SBC Devices on page 59.
Live Cloud Only	Network > Customers	<input type="checkbox"/>	Verify the Customers Status and Deployment status is OK in the Devices table. See Managing SBC Devices on page 59.
		<input type="checkbox"/>	Verify "Enabled" is checked.
		<input type="checkbox"/>	Verify the "total number of DIDs and "users count". See Customer Details Quick Glance.
		<input type="checkbox"/>	Verify that the Azure Tenant Id exists.
		<input type="checkbox"/>	Navigate to "Provider side" and verify the "Users Count" is displayed. See Customer Details Quick Glance.
	Customer Actions Menu > Edit Customer	<input type="checkbox"/>	<ul style="list-style-type: none"> ■ Edit User, update a parameter (e.g. Department) and then verify that the change has been implemented (see Manually Provisioning Users on page 50). ■ To enforce the Teams update, in the Multitenant interface, navigate to Queue Changes > Process All (see Monitoring M365 Replication Actions Queue). ■ To verify users, see User Details. ■ To verify users in Microsoft Teams: Open https://admin.Teams.microsoft.com
Multitenant portal	Site Locations	<input type="checkbox"/>	Verify that the SBC indicates "Deployed" status; click Add/Edit SBC Prefix (see Add SBC Site Locations).
		<input type="checkbox"/>	Verify that the DIDs are configured for the customer (see Upload Dial Plan Rules from Managed SBC Device and Configure

Interface	Menu Navigation Path	Check	Configuration Action
			Dial Plans).
		<input type="checkbox"/>	Add DID and verify that it is successfully added on the SBC.

Updating SQL Server

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



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

SBC Dialplan Verification

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

6 Appendix

This appendix includes the following references to the checklist in [Verifying Component Statuses](#) on page 41:

- [Device Status](#) below
- [Deploy Status and Status Indicators](#) on page 50
- [Manually Provisioning Users](#) on page 50
- [Multitenant Portal Licensing](#) on page 51
- [Configuring Invitation Settings](#) on page 51
- Authentication Status
- [Managing SBC Devices](#) on page 59
- Managing Site Locations
- Scenario Scripts Templates Page

Device Status

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

The screenshot displays the 'Device Management' page in the UMP-365 interface. The main table lists various devices with columns for Name, IP Address / FQDN, Product Type, HA, Status, QoS Status, Calls, Max Concurrent Calls, Quality, Successful/Failed, Version, and Manage. A device named 'qa-ump-365-trunkpack...' is highlighted in green. The right sidebar shows 'Device Details' for this device, including Name, Status (Error), IP Address, Version, Serial Number, Product Type (User Management Pa...), HA (No), Tenant (fmcuc), Region (AutoDetection), and Active Alarms (Critical: 6, Major: 0, Minor: 0, Warning: 3).

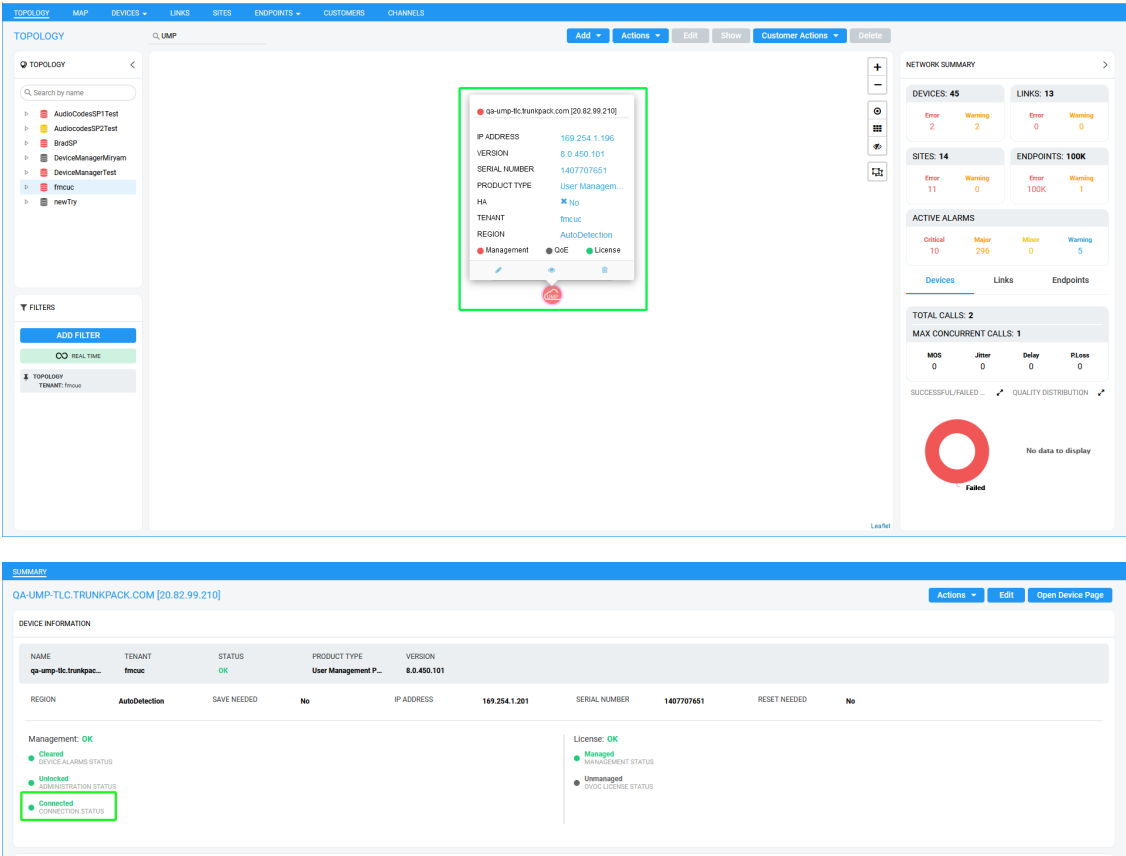










Table 6-1: UMP Device Status



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

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

Status	Topology Map	Device Management Page	Description
			<ul style="list-style-type: none"> License status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined) <p>Strikethrough = locked No strikethrough = unlocked</p>
















Table 6-2: SBC Device Status

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

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

Deploy Status and Status Indicators

The following table shows the various 'Deploy' statuses and their corresponding 'Status' indicators.

Description	Deploy Status	Status
Indicates that the customer tenant has been successfully deployed.	 Deployed	 OK
Indicates that the customer tenant is ready for deployment.	 Ready	 Warning
Indicates that the customer tenant is deployed with a warning.	 Deployed	 Warning
Indicates that the customer tenant is deployed with an error.	 Deployed	 Error
Indicates that the customer tenant is deployed and has been disabled.  This status is only relevant for the 'Device Manager' Service Type.	 Deployed	 Unmonitored
Indicates customer tenant deployment failure: <ul style="list-style-type: none">■ An error has occurred in the deployment of the customer tenant.■ The customer tenant does not exist.■ Customer tenant connection error.	 Failed	 Error
Indicates that the request to deploy the customer tenant has been submitted.	 Unknown	 Warning

Manually Provisioning Users

You can manually provision users with phone numbers and a subset of Calling policies. For provisioning the full set of available Teams Calling Policies, users must be provisioned through template automation.

- Manually Assigning Phone Numbers to Users
- Manually Applying M365 User Policies

Multitenant Portal Licensing

Multitenant portal 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.

See the following:

- Installing the Multitenant License
- Configuring Global License Settings

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 Subdomains](#) Registering 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**).
3. In the Multitenant portal Navigation pane, open the Invitation page (**Configuration > UMP > Email > Invitation**).

The screenshot shows the 'Invitation Settings' page. It has three main input fields:

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

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 ***: A text box containing 'https://finebak.com/authenticate'.

At the bottom, there is an 'Apply Changes' button.

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

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

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

See example email below.

Dear Administrator of {{CustomerId}},

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

Please Note:

- UC admin role requirements:
 - o Application Administrator

- o Skype for Business Admin
- o Teams Communications Administrator

The Authentication process will run against your Microsoft M365 Tenant, we will not know or save your password.

Revoke Token Authentication: you are able to revoke the authentication at any time. Revoking the authentication will stop the service.

Thank you and best regards,
Finebak Support Team

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

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

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.

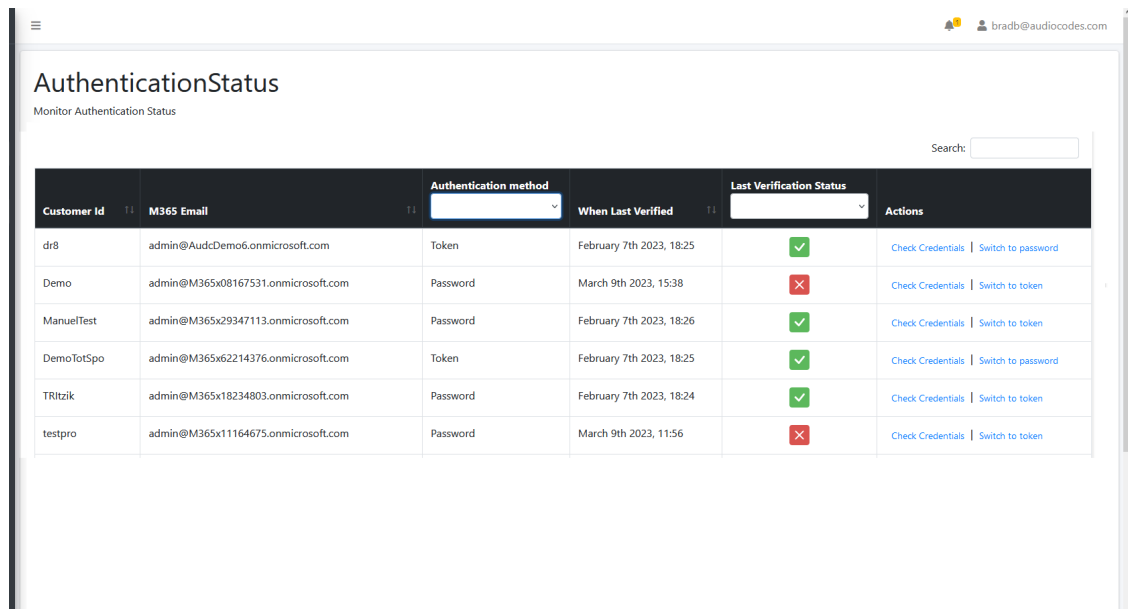
- **Switch to auth token:** This option secures the connection with M365 through a directly-claimed access token. See [Switching to Token Authentication](#) on page 34.

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, open the Authentication Status page (**Monitoring > Customer > Authentication Status**).

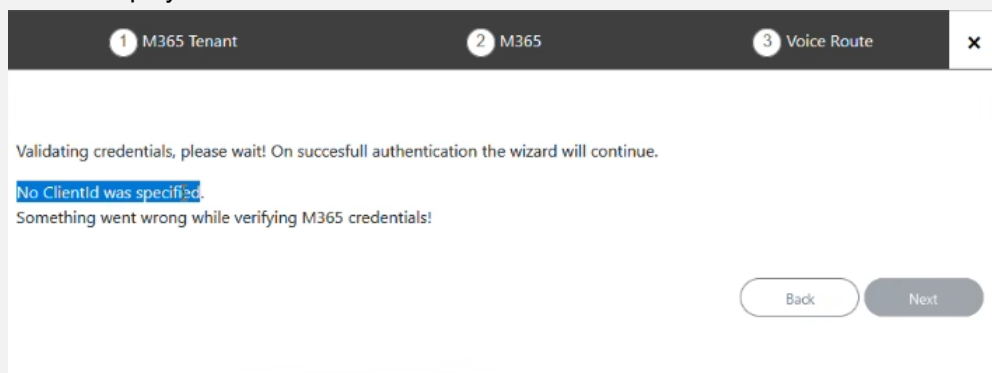


Customer Id	M365 Email	Authentication method	When Last Verified	Last Verification Status	Actions
dr8	admin@AudcDemo6.onmicrosoft.com	Token	February 7th 2023, 18:25	✓	Check Credentials Switch to password
Demo	admin@M365x08167531.onmicrosoft.com	Password	March 9th 2023, 15:38	✗	Check Credentials Switch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

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



If the Client Id is not configured and then the **Grant Consent** option in the Self-Service portal M365 Settings (see Microsoft 365 Settings) is clicked, the following error is displayed:



1 M365 Tenant 2 M365 3 Voice Route X

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

No ClientId was specified.

Something went wrong while verifying M365 credentials!

Back Next

For example:

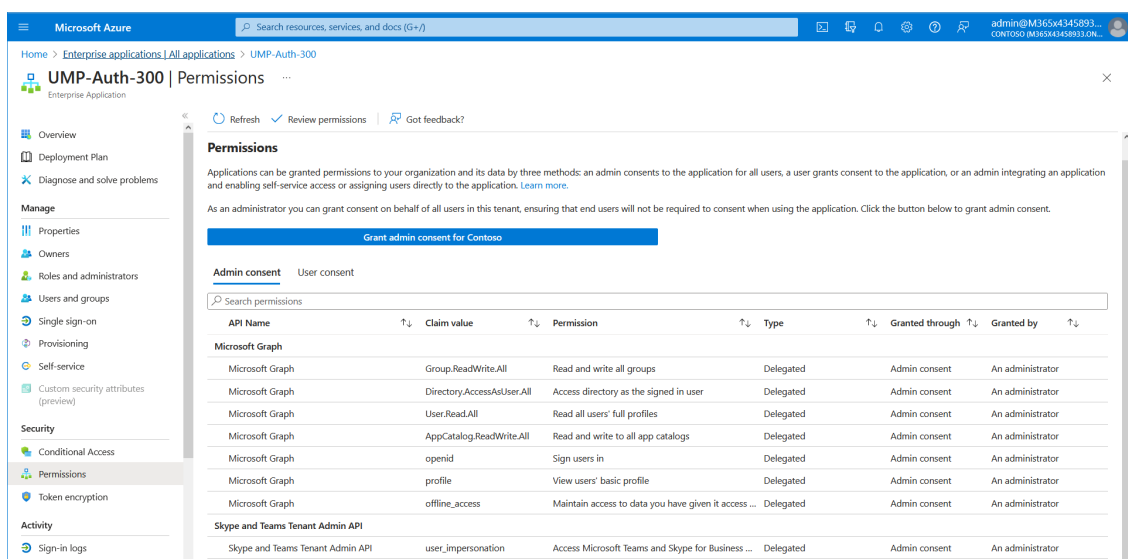
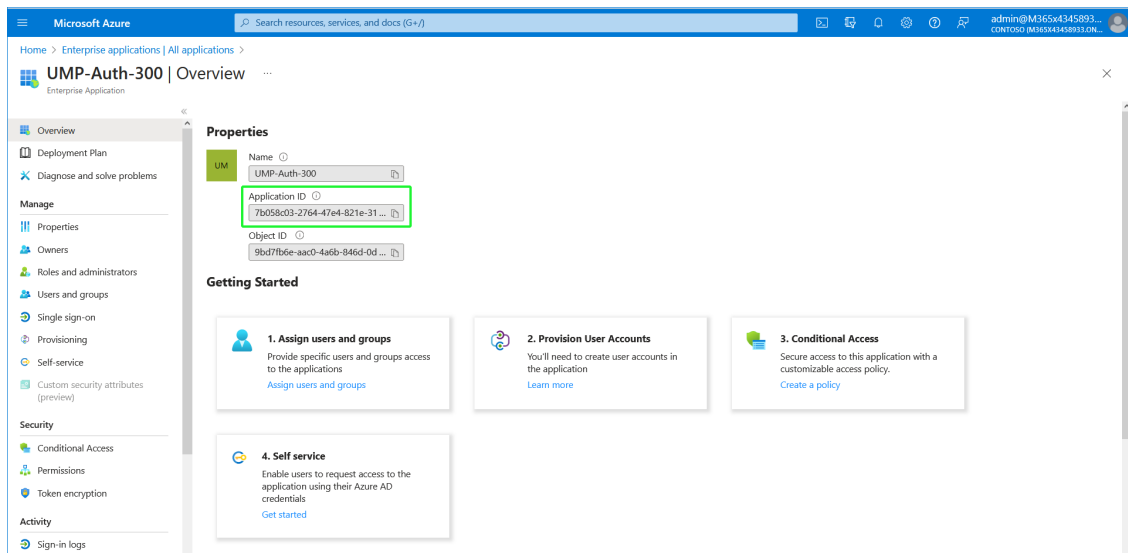
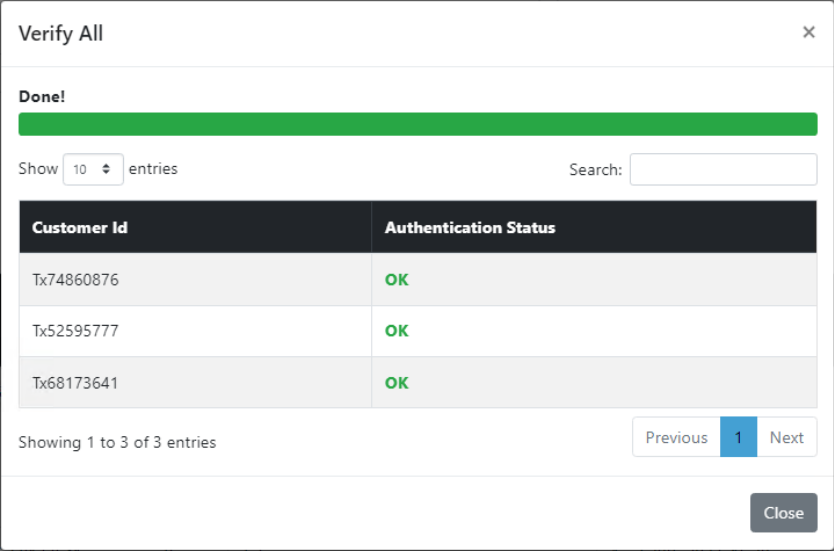
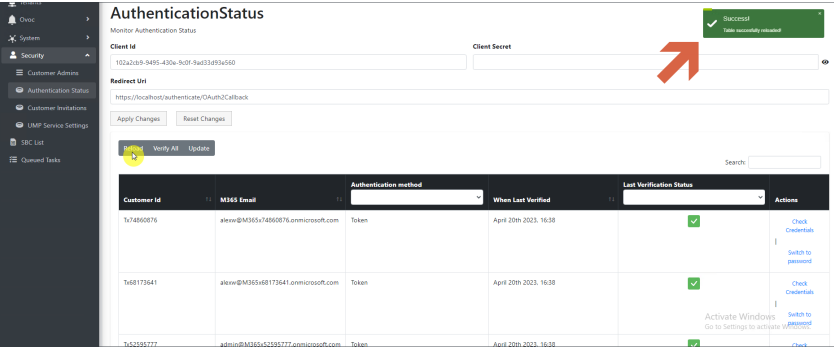


Table 6-3: Authentication Status


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

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

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

- Enter the Client ID and Client secret generated in [Deploy Synchronization Application](#).
- Enter the Redirect URL which consists of the IP address of the Service Provider portal. For example:

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

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

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

Verify All Tokens



Done!

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

Close

Update Used By



Done!

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

Close

tlc-ovoc.trunkpack.com

Customer IT Administrator email:

test@gmail.com

OK

Cancel

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 61: Show a list of configured site locations that are connected to specific SBC devices.
- **Show Prefixes** on page 63: Show a list of configured number prefixes in the dialplans loaded to the managed SBC devices.
- Upload Dial Plan Rules from Managed SBC Device : Import a list of customers from the SBC.

➤ To display list of managed SBC devices:

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

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

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.

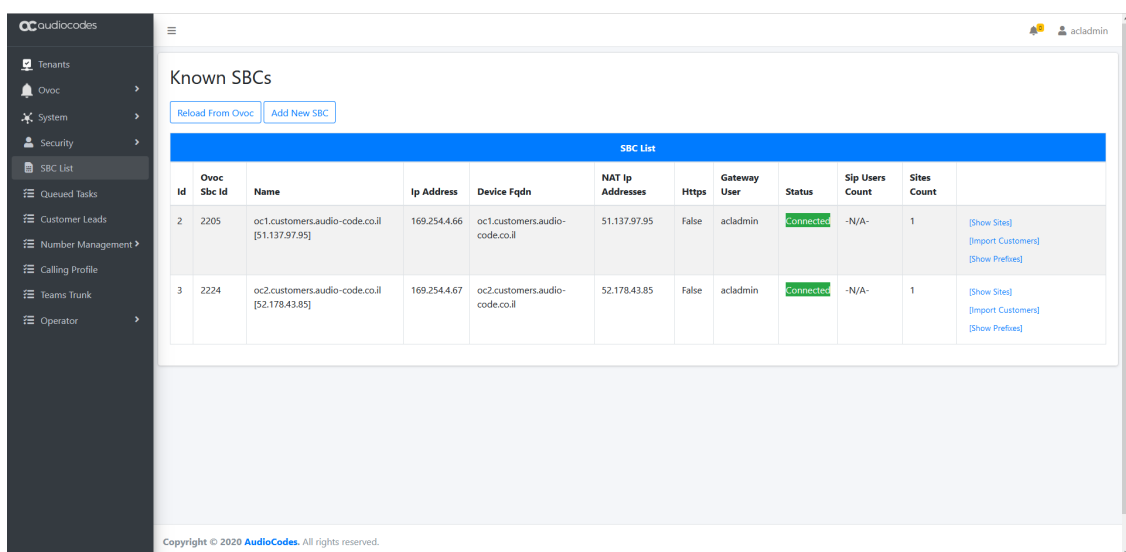
Parameter	Description
HTTPS	Indicates whether HTTPS is enabled for the device.
Gateway User	The name of the administrator user account of the SBC.
Status	The status of the connection between UMP-365 and the SBC.
SIP Users Count	The number of SIP users registered for the SBC.
Site Count	The number of 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 Multitenant portal Navigation pane, click **SBC List**. A list of managed SBC devices is displayed.



Known SBCs

[Reload From Ovoc](#) [Add New SBC](#)

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

[\[Show Sites\]](#) [\[Import Customers\]](#) [\[Show Prefixes\]](#)

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

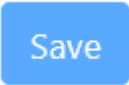
Gateway User:


Gateway Password:

Close

Save

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

7. Click  to apply the changes.

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

9.

Show SBC Site Locations

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

➤ To show site locations:

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

Known SBCs

Reload From Ovoc Add New SBC

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

Copyright © 2023 AudioCodes. All rights reserved.

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

SBC Site Locations

Show 10 entries Search:

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

Showing 1 to 3 of 3 entries

Previous 1 Next

Close

The table below describes the parameters in this table.

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

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

Show Prefixes

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



In User Management Pack 365 SP Edition the Dialplan name and the Dialplan rule are the same. On the SBC device, the dial plan rules defined under each dialplan are configured with unique names.

➤ To show prefixes:

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

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

Refresh From Sbc

Show 10 entries
Search:

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

Showing 1 to 7 of 7 entries

Previous
1
Next

Close

The table below describes the parameters in this screen.

Parameter	Description
Dial Plan	Name of the Dial plan
Index	SBC index
Name	Name of the Live Cloud server instance.
Prefix	Configured phone prefix
Tag	One of the following: <ul style="list-style-type: none">■ Tenant ID■ IP Group Name
Active	

This page is intentionally left blank.

International Headquarters

Naimi Park

6 Ofra Haza Street

Or Yehuda, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

80 Kingsbridge Rd

Piscataway, NJ 08854, USA

Tel: +1-732-469-0880

Fax: +1-732-469-2298

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

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

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

©2024 AudioCodes Ltd.. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice, AudioCodes Meeting Insights, and AudioCodes Room Experience are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-26726

