Odin Automation

Office 365 Integration 18.4.1 Release Notes

Revision 1.18 (February 4, 2019)

Contents

Dependencies and Pre-Requisites

The Office 365 application package requires:

- Odin Automation 8.0.0 or a later 8.0.x version
- Odin Automation 7.4.0 or a later 7.4.x version
- Odin Automation 7.3.0 or a later 7.3.x version
- Odin Automation 7.2.0 or a later 7.2.x version

Fixed Issues

APSA-20624

Issue Summary: [Documentation] Remove the 'DNS Hosting' resource from the 'Office 365' service template.

Fix Description: Office 365 Integration Provider's Guide >> Cloud Solution Provider Scenario > Configuring Offers > Creating 'Office 365' Service Template is updated.

APSA-20786

Issue Summary: The reseller relationship between a partner tenant and a customer tenant must be removed if all Office 365 subscriptions related to the customer tenant are removed.

Fix Description: The relationship is now removed in this case.

APSA-20767

Issue Summary: The apsType field of an APSSubscriptionResource object can be null, and this should be handled correctly in request filters.

Fix Description: This situation is now handled correctly.

APSA-20764

Issue Summary: The application does not reactivate a subscription because its "Quantity" is greater than 1 in the endpoint database.

Fix Description: The reactivation procedure is fixed for subscriptions of this kind: "EndEffectiveDate" is expired; status is "Disabled"; "Quantity" is not 0.

APSA-20489

Issue Summary: A #EXT# user is set in "AdminLogin" during the initial provisioning of a subscription.

Fix Description: Now, #EXT# users are skipped and not used in "AdminLogin" during the initial provisioning of subscriptions.

APSA-20716

Issue Summary: The automatic synchronization procedure is not described properly.

Fix Description: Details on the procedure are added to Office 365 Provider's Guide >> Cloud Solution Provider Scenario > Useful Information > Synchronizing Changes from Office 365 Portal, and Office 365 Subscriber's Guide >> Synchronizing Office 365 Organization with Microsoft Online Services Portal.

APSA-20771

Issue Summary: A wrong path in Office 365 Provider's Guide, Synchronizing Changes from Office 365 Portal.

Fix Description: The path is fixed.

APSA-20670

Issue Summary: The Microsoft Cloud Agreement e-mail address validator allows unsupported symbols in e-mail addresses.

Fix Description: The validator now complies with Microsoft's e-mail validation policies.

APSA-20630

Issue Summary: On the 'Licenses' screen, all licenses have PROVISIONING status when only some of those licenses are being provisioned.

Fix Description: Resource rate filtering by the 'Included' and 'Additional' fields is added. As a result, the status of licenses uninvolved in a provisioning operation will not be not changed.

APSA-20169

Issue Summary: Multi-Factor Authentication (MFA) on the Microsoft side breaks Office 365 integration.

Fix Description: The Office 365 application has been updated to comply with the new Microsoft security model (https://docs.microsoft.com/en-us/partner-center/develop/enable-secure-app-model).

APSA-20628

Issue Summary: Blinking tabs in MyCP for disabled subscriptions.

Fix Description: MyCP is now improved for Office 365 users that belong to disabled subscriptions.

APSA-20592

Issue Summary: Domain verification failed: 'Verification of federated domains is not allowed.'.

Fix Description: The verification of federated domains is now performed correctly.

APSA-20746

Issue Summary: autoconf.py sets 'overusage fee' to 1 instead of 0.

Fix Description: Resource rates are now created with zero overuse fees.

APSA-20738

Issue Summary: Service plans with the 'Yearly on Statement Day' billing period type should be taken into account by the import tool.

Fix Description: Now, the cloud subscription import tool takes into account such service plans.

APSA-20633

Issue Summary: 'Unknown error' occurs when the Office 365 service is assigned to a user with a weak password.

Fix Description: Error handling is now improved in such situations.

APSA-20808

Issue Summary: Application pool recycling causes "provisioning Migration" tasks to fail. Restarting the migration procedure causes the "user is not present in gateway DB" error.

Fix Description: Now, the synchronization procedure automatically handles the "The Office 365 user with 'user_id' 'ID' is not presented in gateway DB." error.

New Features and Changes

Support of the New Application Security Model

As of February 4, 2019, Microsoft introduces a new application security model for authenticating cloud solution provider partners and control panel vendors (an overview of the new security model and technical details are available at https://docs.microsoft.com/en-us/partner-center/develop/enable-secure-app-model).

As of this version, the Office 365 application supports the new application security model and is compliant with its requirements:

- The application no longer stores the user credentials of CSP partner accounts. All user credentials will be erased during the upgrade of the application to version 18.4.1.
- The application no longer requires CSP partners to register any apps in the Azure ADs of their CSP partner accounts. Instead of this, a single app registered in Ingram Micro's control panel vendor account (ingrammicrocpv.onmicrosoft.com) is shared among all Office 365 application instances of all CSP partners. This makes the process of Office 365 application instance configuration simpler and less error-prone.
- Now, a CSP partner using the application must give explicit consent to the permissions that the application requires to make calls to the Partner Center and Graph APIs on behalf of the CSP partner; as a result of giving consent, the application acquires a refresh token. The application securely stores and uses this refresh token to make calls to the Microsoft APIs on behalf of the CSP partner.
  A CSP partner can give consent and acquire a refresh token from the UI of the application; during this procedure, signing in to the Microsoft Partner Center as an administrative user of the CSP partner account is required.
- A refresh token has a 90 day lifetime. A CSP partner must give consent and acquire a new refresh token before the current refresh token expires.

Warning: Service providers using the Office 365 application on their Odin Automation installations need to upgrade the application to version **18.4.1** before **February 4, 2019**. Otherwise, the application will not be able to manage existing Office 365 subscriptions or create new ones.

Please refer to **Odin Automation Office 365 Integration Provider's Guide** >> **Cloud Solution Provider Scenario** to learn more.

Microsoft Cloud Germany Is No Longer Supported

As of Office 365 18.4.1, the application no longer supports the national cloud Microsoft Cloud Germany.

Important: If you have application instances configured for Microsoft Cloud Germany, do not upgrade the application to 18.4.1.

Known Issues and Limitations

- Office 365 and Azure CSP resources cannot be sold in the same service template and service plan. You must use separate service templates and service plans for selling Office 365 and Azure CSP resources.
- Upgrading trial Office 365 subscriptions from trial service plans to paid service plans does not work in CCP v1. To work around this issue, you can switch customers with trial Office 365 subscriptions from CCP v1 to UX1 for Customers.
- In UX1 for Customers of Odin Automation 7.2, adding trial Office 365 services to users does not work on the **Users** screen. To work around this issue, customers can use the **Office 365** screen.

Technical Information

Obtaining the 'Office 365' Package

To obtain the Office 365 application package, contact your Ingram Micro technical account manager.

Installation Procedure

To install the Office 365 application, use the instructions provided in the **Odin Automation Office 365 Integration Provider's Guide**.

Upgrade Procedure (from Version 18.3)

The upgrade procedure consists of the following steps:

1. Prepare the necessary information for upgrading the Office 365 application endpoint (collect Office 365 gateway site parameters).
2. Stop provisioning Office 365 services.
3. Upgrade the Office 365 application endpoint.
4. Upgrade the Office 365 application.
5. Acquire refresh tokens for all application instances.
6. Remove the **o365_based_on_email** service parameter from all Office 365 service templates.
7. Update the OA Billing control panel and online store customizations.
8. Perform post-upgrade validation.
9. Start provisioning Office 365 services.

Important:

1. The upgrade procedure is not reversible.

2. Upgrade steps **1**-**9** are mandatory.

3. Make sure the current version of the Office 365 application is **18.3**. Upgrading from other versions is not supported.

4. Before upgrading the Office 365 application from one version to another, make sure that you are going to follow the allowed upgrade paths. See this KB article https://kb.cloudblue.com/en/130752 for details.

5. If a non-LocalDB edition of SQL Server is used by your Office 365 application endpoint, make sure all SQL Server logins of Office 365 gateway application databases have the **sysadmin** server role. See **Odin Automation Office 365 Integration Provider's Guide** >> **Cloud Solution Provider Scenario** >

Deployment Architecture > **Preparing SQL Server Databases** for details.

6. The names of the Office 365 gateway sites must not be changed after the installation of the Office 365 application endpoint. If you have changed them, reinstate the original names before upgrading the Office 365 application endpoint.

To upgrade an existing installation of the Office 365 application, perform the following steps:

1. Prepare the necessary information for upgrading the Office 365 application endpoint. You must prepare the name of the Office 365 gateway site, the name of the Office 365 gateway application, the hostname of the Office 365 gateway site, and the IP address of the Office 365 gateway site. This can be done in the following way:
    a. Log in to Provider Control Panel.
    b. Go to **Service** > **Applications** and click the **Office 365** application.
    c. Select the **Instances** tab and click the target application instance.
    d. Select the **General** tab.
    e. Obtain the value of the **Application API end-point URI** setting. This is a URL that is structured in the following way: https://<Hostname_of_Office_365_Gateway_Site>/<Name_of_Office_365_Gateway_Application>/aps/.
    f. Write down the name of the directory from the URL. This is the name of the Office 365 gateway application.
    g. Write down the hostname from the URL. This is the hostname of the Office 365 gateway site.
    h. Resolve and write down the hostname from the URL into the IP address. This is the IP address of the Office 365 gateway site.
    i. Log on to the Office 365 Application Endpoint Host as **Administrator** via RDP.
    j. Open **Internet Information Services (IIS) Manager**.
    k. Go to the list of sites.
    l. From the list, select the site with the IP address obtained above.
    m. Write down the name of the site. This is the name of the Office 365 gateway site.
2. Stop provisioning Office 365 services:
    a. Stop provisioning Office 365 services. For example, deactivate the **Office 365** service template in OA Operations.
    b. In OA Operations, go to **Operations** > **Tasks** and make sure all Office 365 tasks are processed.
3. Upgrade the Office 365 application endpoint:
    a. Upload the Office 365 application package to the Office 365 Application Endpoint Host.

b. Unpack the application package.
c. Unblock the contents of the O365-Web.zip file. To do this, right-click the file in **Windows Explorer**, click **Properties**, click **Unblock**, and click **OK**.
d. Unpack the O365-Web.zip file.
e. Start **Windows PowerShell Console** and go to the directory where the contents of the O365-Web.zip file are located.
f. Run the .\setup.cmd -GatewaySiteName <The name of the Office 365 gateway site> -GatewayAppName <The name of the Office 365 gateway application> -GatewayIPAddress <The IP address of the Office 365 gateway site> -GatewaySiteCertSubject <The hostname of the Office 365 gateway site> -Force command.
g. Run the iisreset command.

Note: If you have several Office 365 gateway sites on the Office 365 Application Endpoint Host, use the procedure provided above to upgrade each Office 365 gateway site.

4. Upgrade the Office 365 application:
   a. Import the **Office 365** application package to Odin Automation. See **APS Application Hosting Guide** >> **Application Hosting Configuration** > **Managing Applications** > **Importing Application** for details.
   b. Upgrade your **Office 365** application instances. See **APS Application Hosting Guide** >> **Application Hosting Configuration** > **Bulk Application Upgrades** for details.
5. For every application instance of the Office 365 application, acquire a refresh token by following these steps:
   a. Prepare the credentials of a user with the **Global admin** and **Admin agent** roles in the CSP partner account that the application instance belongs to. Also, make sure that Multi-Factor Authentication (MFA) is enabled for the user, as described at https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates.
   b. In the Provider Control Panel, perform the following:
      1. Go to **Services** > **Applications** and click on the **Office 365** application.
      2. Select the **Instances** tab and click on the application instance that belongs to the CSP partner account.
      3. Select the **Office 365** tab and select the **Settings** subtab.
      4. Click on the **Manage Refresh Token** button.
      5. In the **Automatic Update** area, click on the **Update Refresh Token** button. This will open the Microsoft Partner Center login page in a new browser window.
   c. In the new browser window, perform the following:

1. Sign in using the credentials of the user that you prepared.
2. Click on the **Accept** button to give consent to the permissions that the Office 365 application requires. You will be redirected from the Microsoft Partner Center to a special site.
3. Make sure that the *The consent has been granted successfully. The authorization code has been sent ...* message is shown on the **Partner Onboarding Web Application** page of the site. After that, close the new browser window.

d. In the Provider Control Panel, perform the following:
   1. Make sure that the *Your refresh token has been updated successfully* message or similar is shown.
   2. Click on the **Test Connection** button to check that the Office 365 application can make calls to the Partner Center and Graph APIs on behalf of the CSP partner account using the refresh token.

Warning: A refresh token has a limited lifetime of 90 days. This means that you must acquire a new refresh token before the current refresh token expires.

Note: You can also update a refresh token using another update procedure. To learn more, see **Odin Automation Office 365 Integration Provider's Guide** >> **Cloud Solution Provider Scenario** > **Deploying 'Office 365' Application** > **Giving Consent and Acquiring Refresh Token**.

6. Remove the **o365_based_on_email** service parameter from all Office 365 service templates in OA Billing. After removing the parameter, synchronize all online stores that are used for selling Office 365 services.
7. Update the installed OA Billing control panel and online store customizations. Use https://kb.cloudblue.com/en/130232 to find the necessary customizations and update instructions.

   Important: After upgrading Odin Automation, make sure the installed OA Billing control panel and online store customizations belong to the current version of Odin Automation. If necessary, update them. Use https://kb.cloudblue.com/en/130232 to find the necessary customizations and update instructions.

8. Perform the following post-upgrade validation steps:
   a. In Task Manager, make sure that there are no unprocessed Office 365 tasks scheduled during the upgrade.
   b. For each Office 365 application instance, make sure that all settings are correctly specified and all necessary Microsoft APIs are accessible. To do this, select the application instance you need to check and click **Test Connection**.
9. Start provisioning Office 365 services. For example, activate the **Office 365** service template in OA Operations.

Upgrade Procedure (from Version 18.4)

The upgrade procedure consists of the following steps:

1. Prepare the necessary information for upgrading the Office 365 application endpoint (collect Office 365 gateway site parameters).
2. Stop provisioning Office 365 services.
3. Upgrade the Office 365 application endpoint.
4. Upgrade the Office 365 application.
5. Update the OA Billing control panel and online store customizations.
6. Perform post-upgrade validation.
7. Start provisioning Office 365 services.

Important:

1. The upgrade procedure is not reversible.

2. Upgrade steps **1**-**7** are mandatory.

3. Make sure the current version of the Office 365 application is **18.4**. Upgrading from other versions is not supported.

4. Before upgrading the Office 365 application from one version to another, make sure that you are going to follow the allowed upgrade paths. See this KB article https://kb.cloudblue.com/en/130752 for details.

5. If a non-LocalDB edition of SQL Server is used by your Office 365 application endpoint, make sure all SQL Server logins of Office 365 gateway application databases have the **sysadmin** server role. See **Odin Automation Office 365 Integration Provider's Guide** >> **Cloud Solution Provider Scenario** > **Deployment Architecture** > **Preparing SQL Server Databases** for details.

6. The names of the Office 365 gateway sites must not be changed after the installation of the Office 365 application endpoint. If you have changed them, reinstate the original names before upgrading the Office 365 application endpoint.

To upgrade an existing installation of the Office 365 application, perform the following steps:

1. Prepare the necessary information for upgrading the Office 365 application endpoint. You must prepare the name of the Office 365 gateway site, the name of the Office 365 gateway application, the hostname of the Office 365 gateway site, and the IP address of the Office 365 gateway site. This can be done in the following way:
    a. Log in to Provider Control Panel.
    b. Go to **Service** > **Applications** and click the **Office 365** application.

c. Select the **Instances** tab and click the target application instance.
d. Select the **General** tab.
e. Obtain the value of the **Application API end-point URI** setting. This is a URL that is structured in the following way: https://<Hostname_of_Office_365_Gateway_Site>/<Name_of_Office_365_Gateway_Application>/aps/.
f. Write down the name of the directory from the URL. This is the name of the Office 365 gateway application.
g. Write down the hostname from the URL. This is the hostname of the Office 365 gateway site.
h. Resolve and write down the hostname from the URL into the IP address. This is the IP address of the Office 365 gateway site.
i. Log on to the Office 365 Application Endpoint Host as **Administrator** via RDP.
j. Open **Internet Information Services (IIS) Manager**.
k. Go to the list of sites.
l. From the list, select the site with the IP address obtained above.
m. Write down the name of the site. This is the name of the Office 365 gateway site.

2. Stop provisioning Office 365 services:
   a. Stop provisioning Office 365 services. For example, deactivate the **Office 365** service template in OA Operations.
   b. In OA Operations, go to **Operations** > **Tasks** and make sure all Office 365 tasks are processed.
3. Upgrade the Office 365 application endpoint:
   a. Upload the Office 365 application package to the Office 365 Application Endpoint Host.
   b. Unpack the application package.
   c. Unblock the contents of the O365-Web.zip file. To do this, right-click the file in **Windows Explorer**, click **Properties**, click **Unblock**, and click **OK**.
   d. Unpack the O365-Web.zip file.
   e. Start **Windows PowerShell Console** and go to the directory where the contents of the O365-Web.zip file are located.
   f. Run the .\setup.cmd -GatewaySiteName <The name of the Office 365 gateway site> -GatewayAppName <The name of the Office 365 gateway application> -GatewayIPAddress <The IP address of the Office 365 gateway site> -GatewaySiteCertSubject <The hostname of the Office 365 gateway site> -Force command.
   g. Run the iisreset command.

Note: If you have several Office 365 gateway sites on the Office 365 Application Endpoint Host, use the procedure provided above to upgrade each Office 365 gateway site.

4. Upgrade the Office 365 application:
   a. Import the **Office 365** application package to Odin Automation. See **APS Application Hosting Guide** >> **Application Hosting Configuration** > **Managing Applications** > **Importing Application** for details.
   b. Upgrade your **Office 365** application instances. See **APS Application Hosting Guide** >> **Application Hosting Configuration** > **Bulk Application Upgrades** for details.
5. Update the installed OA Billing control panel and online store customizations. Use https://kb.cloudblue.com/en/130232 to find the necessary customizations and update instructions.

   Important: After upgrading Odin Automation, make sure the installed OA Billing control panel and online store customizations belong to the current version of Odin Automation. If necessary, update them. Use https://kb.cloudblue.com/en/130232 to find the necessary customizations and update instructions.
6. Perform the following post-upgrade validation steps:
   a. In Task Manager, make sure that there are no unprocessed Office 365 tasks scheduled during the upgrade.
   b. For each Office 365 application instance, make sure that all settings are correctly specified and all necessary Microsoft APIs are accessible. To do this, select the application instance you need to check and click **Test Connection**.
7. Start provisioning Office 365 services. For example, activate the **Office 365** service template in OA Operations.

Helpful Resources

The Odin Automation Office 365 integration guides are available here: https://docs.cloudblue.com/oa/services/office365/home.htm.