# Management Console v14.2.0.8 Hotfix Readme

## 1.1 About this hotfix

The following packages have been distributed with this hotfix and must be installed on a system that is running Asigra Cloud Backup v14.2.

- app_amc_14.2_0_8_inst.win
- app_amc_14.2_0_8_inst.lnx
- app_amc_14.2_0_8_inst.mac

## 1.2 Applying this hotfix

**To apply this hotfix automatically:**

1. Download the required hotfix file.
2. Copy the hotfix file to the DS-System online storage Upgrade folder.

   **Note**: When Management Console connects to the DS-System or DS-Client, the upgrade packages will be downloaded to the Management Console installation folder and a notification will be sent.
3. On the Management Console toolbar, click **Notifications**.
4. In the **Notifications** window, click **Updates**.
5. In the **Management Console Updates** window, under **Package Name**, select the package(s) you want to install, and then click **Install**.

**To apply this hotfix manually:**

1. Download the required hotfix file.
2. Copy the hotfix package to the Upgrade_cache folder on the Management Console computer. For example:

   - **Windows**: `C:\Program Files\CloudBackup\Management Console\Upgrade_cache`
   - **Linux**: `/opt/CloudBackup/Management Console/Upgrade_cache`
   - **Mac**: `/Library/CloudBackup/Management Console/Upgrade_cache`
3. On the Management Console toolbar, click **Notifications**.
4. In the **Notifications** window, click **Updates**.
5. In the **Management Console Updates** window, under **Package Name**, select the package you want to install, and then click **Install**.

**Important**: You must restart your web browser for the update to take effect.

## 1.3 Issues resolved in this hotfix

This section lists issues that have been resolved in this hotfix.

**Note**: This hotfix might include additional fixes that are not documented in this Readme.

| ID | Issue |
|---|---|
| AF-54 | Management Console users can now automatically suspend backup sets associated with Microsoft 365 accounts that have been removed from the domain as part of the autodiscover process. |
| AF-105 | Management Console users can now search for a specific DS-Client based on the DS-Client number when viewing the list of backup sets on the Backup Sets tab of the Data Management page. |
| AF-106 | Management Console users can now view the IP address or host name of the backup source machine on the Backup Sets tab of the Data Management page. |
| AF-158 | Management Console users can now search the Activity Log based on the backup set name. |
| AF-183 | Management Console users can now view the platform (Windows, Linux, Mac) of each DS-Client on the Backup Sets tab of the Data Management page. |
| AF-200 | Management Console users can no longer delete Microsoft 365 credentials if there are existing backup sets using those credentials. Users must first assign new Microsoft 365 credentials to the affected backups sets. |
| AF-210<br>AF-562 | Management Console Global Administrators can now configure Multifactor Authentication (MFA) for users so they must authenticate using a six-digit Time-based one-time password (TOTP) application, such as Google or Microsoft Authenticator when signing in or attempting to perform a potentially destructive action that can result in the loss of data. |
| AF-242 | When creating a VMware Cloud Director backup set, if a user with administrator privileges configures the credentials for the Cloud Director server, a regular user can now create the backup set using the organization credentials. |
| AF-355 | Updated third-party components used by Management Console to address potential security vulnerabilities. |
| AF-403 | Management Console users can now scan their File System backup sets for malware during the backup and restore process when connected to a Linux or Mac DS-Client. |
| AF-509<br>AF-537 | When scanning File System backup sets for malware during the restore process, Management Console users can now either quarantine the infected files in a password-protected zip file or attempt to clean the infected files and restore them when the remediation is successful. |
| AF-571 | Replaced all references to “VMware vCloud Director” with “VMware Cloud Director”. |
| AF-586 | Management Console users can now search for specific items when restoring Microsoft 365 data from Exchange Online, Archive Mailboxes, and Public Folders, SharePoint Online, or OneDrive. Users can search for specific emails, contacts, calendars, tasks, and/or posts. |
| AF-651 | Management Console users can now select which Microsoft 365 services use the autodiscover feature to automatically create backup sets for items added to the Microsoft 365 domain. |
| AF-681 | Management Console users can now select which DS-Clients use the autodiscover feature to automatically create backup sets for items added to the Microsoft 365 domain. |
| AF-695 | Management Console Global Administrators can now configure Multiperson Approval (MPA) for accounts so users require multiple people to approve a potentially destructive action that can result in the loss of data. Administrators can set a threshold to specify how many approvals are required. |
| AF-700 | Management Console users can no longer use Secret Double Octopus (SDO) for Multifactor Authentication (MFA) because the integration is no longer supported. |
| TS-5753 | On occasion when a user attempted to search for and restore an email from a Microsoft 365 backup set, the email could not be found, and the Management Console became unresponsive. |
| TS-5756 | When a Microsoft 365 backup set was created using the autodiscover feature, the maximum number of generations was set to 30 by default instead of 9999. |

## 1.4 Issues resolved in previous hotfixes

This hotfix is cumulative and contains the following updates from previous hotfixes:

### Hotfix 14.2.0.7

| ID | Issue |
|---|---|
| AF-25 | Management Console users can now migrate their Microsoft 365 Basic authentication credentials to Modern authentication (Automatic or Manual) credentials and update the associated backup sets to use the migrated Modern authentication credentials. |

### Hotfix 14.2.0.6

| ID | Issue |
|---|---|
| AF-46 | When performing backup, restore, or delete operations, Management Console users can now view the contents of folders that contain more than 10,000 items with improved performance. |
| AF-63 | When configuring a Microsoft 365 backup set, Management Console users can now perform folder-level backups of SharePoint and OneDrive Document libraries. |
| AF-163 | Management Console administrators can now configure multi-factor authentication (MFA) for a user so that the user requires approval to delete a backup set. |
| AF-266 | Management Console users can now enable or disable the Volume Shadow Copy Service (VSS) option for File system and Permissions backup sets. The option is enabled by default. |
| AF-296 | Management Console has been updated to integrate with the latest version (v5.0.8) of Secret Double Octopus (SDO) to support the multi-factor authentication (MFA) feature. |
| AF-299 | Management Console administrators can now configure multi-factor authentication (MFA) for a user so that the user requires approval to perform an on-demand restore. |
| AF-300 | Management Console administrators can now configure multi-factor authentication (MFA) for a user so that the user requires approval to perform an on-demand backup. |
| AF-301 | Management Console administrators can now configure multi-factor authentication (MFA) for a user so that the user requires approval to reassign, edit, or delete a retention rule for an existing backup set. |
| AF-317 | Management Console users can now backup and restore Microsoft 365 SharePoint sites and OneDrive accounts using Modern authentication credentials. |
| AF-337 | Management Console administrators can now configure multi-factor authentication (MFA) for a user so that the user requires approval to reassign, edit, or delete a schedule for an existing backup set. |
| AF-383 | When configuring Microsoft 365 credentials, Management Console users can now register a single tenant or multitenant application when using Modern authentication (Manual) credentials. |
| AF-408 | Management Console users can now scan File System backup sets for potentially malicious or unauthorized content during backup and restore based on predefined policies. Active content is identified and reported on during the backup process and filtered, blocked, or removed during the restore process. |
| AF-412 | The version of the log4j component used by the Asigra software has been updated to the latest version to ensure our software is not flagged by any scanning tools. |
| AF-421 | When configuring a VMware vCenter Server backup set, users can now configure the days of the week on which they want to validate the disk signature of a protected virtual machine. |

## Hotfix 14.2.0.5

| ID | Issue |
|---|---|
| AF-64 | When editing Microsoft 365 credentials in Management Console, the updated credentials are now automatically applied to all Microsoft 365 backup sets using the credentials. |
| AF-293 | The version of the log4j component used by the Asigra software has been updated to the latest version to ensure our software is not flagged by any scanning tools. |
| TS-3142 | On occasion when a user edited a Microsoft 365 backup set in the Management Console, the refresh token for the credentials was not updated correctly for Teams. |
| TS-3149 | When configuring a Microsoft 365 backup set in the Management Console, if the user performed a search to filter the list of Exchange mailboxes by subdomain, and then selected the check box beside the top-level domain name, all the mailboxes were selected rather than only the mailboxes found by the search. |
| TS-3168 | If the email notification settings in the Management Console were configured to use the SSL or TLS protocol, an error message was displayed when a user attempted to reset their password using the “Forgot user name or password” feature. |

## Hotfix 14.2.0.4

| ID | Issue |
|---|---|
| AF-282 | A vulnerability has been identified with the Apache log4j component that affects version 2.x to 2.15.0 when JNDI features are used. The log4j configuration used by Asigra software components does not utilize the JNDI feature affected by this vulnerability. However, we have updated the version of the log4j component used by the Asigra software to the latest version to ensure our software is not flagged by any scanning tools. |

## Hotfix 14.2.0.3

| ID | Issue |
|---|---|
| TS-1464 | On occasion when attempting to create a Microsoft 365 backup set, when the user selected the OneDrive account, an error message was displayed indicating there are too many items in the selected folder to display. |
| TS-2185 | If a user created a File system backup set in DS-User and excluded some folders, when the user edited the same backup set in the Management Console and enabled cybersecurity, the previously excluded folders were now included in the backup. |
| TS-2635 | On occasion after backing up Microsoft 365 data, there were no results displayed on the Exchange Mailboxes and Archive Mailboxes tabs in the Cloud Backup Status Report. |
| TS-2640 | On occasion when working with a large Microsoft 365 domain, the performance was slower than expected. |
| TS-2647 | On occasion when viewing the Cloud Backup Status Report for a specific domain, results were displayed from other domains as well. |
| TS-2657 | On occasion some Microsoft 365 backup sets were automatically suspended during the autodiscovery process if the Microsoft 365 license for a user was removed, or source data was deleted from the Microsoft 365 portal. Users must now suspend the backup sets manually. |
| TS-2703 | On occasion when using the autodiscovery feature, some Exchange mailboxes that were part of the Microsoft 365 domain were not detected. |
| TS-2704 | When a user manually created Microsoft 365 backup sets for a custom domain and enabled autodiscovery on the default domain, the same backup sets were created for the default domain resulting in duplication. |
| TS-2719 | When a user enabled the Autodiscover feature on a domain with a name that contained a hyphen (-), the system was unable to automatically detect and create Microsoft Office 365 backup sets for that domain |

## Hotfix 14.2.0.2

| ID | Issue |
|---|---|
| AF-190 | Management Console users can now protect their Microsoft 365 backup sets from malware by performing real-time scans of their files (Exchange Online, SharePoint Online, OneDrive, Groups, or Teams) during the backup and restore process. |
| AF-191 | Management Console users (Windows or Linux) can now remotely manage DS-Clients without opening a port in the firewall on the DS-Client machine. |
| AF-192 | Management Console users can now configure a process to run before and/or after a File system backup to perform specific actions when a condition has been met. |
| TS-1377 | On occasion when Microsoft 365 backup sets were created in DS-NOC or DS-User, the backup sets might get duplicated after upgrading to v14.2 if the DS-Clients were added in the Management Console using the same cloud domain with the auto-discovery option enabled due to new backup sets naming convention implemented in Management Console. Requires DS-Client (14.2.0.2), DS-NOC (14.2.0.1) and Management Console (14.2.0.2) or later. |
| TS-1378 | When backing up and restoring Microsoft 365 backup sets, Management Console users could not perform real-time scans of their Groups and Teams files for malware during the backup and restore process. Requires Windows DS-Client (14.2.0.2) and Management Console (14.2.0.2) or later. |
| TS-1379 | Management Console users (Windows or Linux) could not remotely manage DS-Clients without opening a port in the firewall on the DS-Client machine. Requires DS-Client (14.2.0.2), DS-System (14.2.0.2), and Management Console (14.2.0.2) or later. |
| TS-1380 | Management Console users could not configure a process to run before and/or after a File system backup to perform specific actions when a condition had been met. Requires Windows DS-Client (14.2.0.2) and Management Console (14.2.0.2) or later. |
| TS-1404 | On occasion when attempting to create a Microsoft 365 backup set using a credential that did not have .com in the domain name, an error message was displayed, and the process failed. |
| TS-1407 | On occasion when creating a Microsoft 365 backup set, the option to select individual subfolders in a mailbox was enabled before the mailbox was selected. |
| TS-1413 | If a user signed out after configuring the email notification settings with TLS, the email notification test failed after the user signed back in. |

## Hotfix 14.2.0.1

| ID | Issue |
|---|---|
| AF-189 | Management Console users can now protect their Exchange Online data from malware by performing real-time scans of their files during the backup and restore process. |