inSync Client v6.8.3 for GovCloud

A patch update v6.8.3 for macOS is released on April 15, 2021, and contains the fix for the following issue:

Fixed Issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS-21241</td>
<td>Fixed the issue wherein the number of files for each consecutive backup were seen increasing, and the backups were eventually failing due to connection issues.</td>
</tr>
</tbody>
</table>

Revision Information

<table>
<thead>
<tr>
<th>Product</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>inSync Client</td>
<td>macOS: r110041</td>
</tr>
</tbody>
</table>

Druva has not released a new version of inSync Client for Linux OS with inSync Client v6.8.3. You can continue using inSync Client v5.9 for Linux with inSync GovCloud.

Download the latest inSync Client [here](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

For upgrade instructions, see [Upgrade inSync Client](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

For more information, contact Support.

inSync GovCloud Update on Feb 27, 2021

With this cloud update, we bring you the following enhancements:
Enhancements

- CloudApps
- Platform
- Governance & Proactive Compliance
- inSync Client

CloudApps

Access Cloud Apps from the main menu

Faster and easier navigation to Cloud Apps data sources.

You can now access the configured Cloud App of your choice from the Data Sources tab on the inSync Management Console.

View details of the last backup and restore activity

inSync administrators can now get detailed insights into the latest backup and restore activity for the following Cloud Apps:

- Microsoft 365: Exchange Online and OneDrive
- Google: Gmail and Google Drive
This view provides administrators visibility into the latest completed backup and restore activity, enabling them to take action in the event of backup and restore failures.

**Office 365 rebranded as Microsoft 365 in Druva inSync**

Aligning with Microsoft’s recent rebranding, we have renamed all instances of Office 365 to Microsoft 365 in the Druva inSync Management Console.

**SharePoint Online (SPO) Enhancements**

**Protection of additional SPO settings**

Administrators no longer need to worry about losing the SPO customizations that are important to ensure business and operational continuity.

We have now added support to automatically backup and restore SPO settings of a SharePoint site, Subsite, Document Libraries, and Lists along with additional data such as Master Page Gallery, Site columns, Site content types, Composed looks, and much more.

For the complete list of data and settings protected by Druva inSync, see:

- Data backed up by inSync for SharePoint Online
- Restore SharePoint Online data

**Support for backup and restore of audit fields for SPO objects**

Druva inSync now supports backup and restore of the audit fields data for Files, SharePoint Online objects including Folder, List items, Site Pages, Document Library, List, Subsite, and Site. The audit field includes:

- Created By
- Created Time
- Modified By
- Modified Time

This ensures that the governance and compliance process is enforced for all SharePoint Online objects after data recovery from Druva inSync.

For the complete list of data and settings protected by Druva inSync, see Data backed up by inSync for SharePoint Online

**Additional protection of SharePoint Online site data**
inSync administrators no longer need to worry about losing the SPO customizations that are important to ensure business and operational continuity. inSync now automatically protects the following data and settings of a SharePoint site, Subsite, Document Libraries, and Lists:

- Document Library and List Settings
- Site Settings
- Master Pages
- Site Templates

With the complete protection of a Sharepoint environment, Druva helps minimize the Recovery Time Objective (RTO) in Disaster Recovery (DR) use-cases.

For more information, see:

https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud

Updated: Fri, 24 Sep 2021 20:44:28 GMT
Powered by
Exclude non-critical SharePoint site content for faster backups

Back up large SharePoint sites is a time-consuming activity. To enable faster backups, inSync administrators can now consider excluding non-critical contents in SharePoint sites from backup.

inSync administrators can use the **Relative URL Paths** feature available under **Backup and Retention Settings** while configuring the SharePoint site for protection.

This ensures that the SharePoint site backups are faster with only the required data being backed up.
For more information, see Relative URL Paths.

Introducing Filters for SharePoint sites
inSync administrators can quickly narrow down and review the backup status of specific SharePoint sites based on the built-in filters such as Site Type (Microsoft Teams Sites, Microsoft 365 Group Sites, and other Sites), Last Backup Status, and Site Status. This enables the administrators to quickly take the corrective action needed to effectively protect critical SharePoint, Team, and Group sites.

**Action Required:** To use Filters, discover sites again. For more information, see [Discover Sites](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**SharePoint Site title changes are now automatically managed in inSync**

When administrators change the site title in SharePoint Online, the new title is automatically captured by Druva inSync and reconciled with the old snapshots. The site is listed with the updated title on the inSync SharePoint site listing page, thus making it easy for administrators to search using its new name. Additionally, site title changes do not impact any ongoing backups.

**SharePoint Online: A new Activity Details page**

inSync administrators managing SharePoint Online can now get detailed insights into the latest backup and restore activities with the new **Activity Details** page.

The information is helpful for tracking identifying the exact number of items backed up or restored, with the option of download logs for further analysis and troubleshooting.

**Backup Activity Details**
Restore Activity Details

Activity Details

Summary
- Activity Type: Manual Backup
- Site Title: Demo_Site
- Status: Backed Up With Errors
- Total Size: 41.93 MB
- Start Time: Sep 21 2020, 15:24
- End Time: Sep 21 2020, 15:27

Backup Details

<table>
<thead>
<tr>
<th>Content</th>
<th>Total Items Scanned</th>
<th>Added</th>
<th>Updated</th>
<th>Deleted</th>
<th>Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subsites</td>
<td>74</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Document Library</td>
<td>65</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>List</td>
<td>45</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Files</td>
<td>3002</td>
<td>4</td>
<td>0</td>
<td>3002</td>
<td>0</td>
</tr>
<tr>
<td>Folders</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
For more information, see:

- [Backup Activity Details](#)
- [Restore Activity Details](#)

**Note:** The Activity Details page is displayed only for backup and restore activities initiated after the cloud update on October 3, 2020.

**Microsoft 365 Enhancements**

**Teams: Advanced restore capabilities**

As an inSync administrator, you can use the following restore enhancements to recover data, especially in case of accidental deletion of Team data or corruption of data during a ransomware attack.

- **Restore to the same destination** - Restore data of a team to the same team on the Microsoft 365 tenant with

https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud

Updated: Fri, 24 Sep 2021 20:44:28 GMT
Powered by
details such as Team name, Team Settings, and Channels from a point in time snapshot.

- **Share data between Teams** - Restore data of a team to any other existing team in their Microsoft 365 tenant from a point in time snapshot.

- **Restore to a new team** - Create a new team and restore entire data from any point in time snapshot.

To learn more, see [Restore Teams data](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Enhanced way to manage Teams and their sub-apps in inSync Microsoft Teams**

Now, when an inSync administrator updates a team's backup status or deletes the snapshots, the same actions get applied on that team's sub-apps that includes Teams Metadata, Conversation, and corresponding SharePoint Online site in Druva inSync.

**Microsoft Teams: Enhancements to Activity Stream and Reports**

The list view of backup activities now displays the backup activities of the last 30 days within Activity Stream and Reports.
Microsoft 365: Recover Conversations in HTML format

Druva inSync enables administrators to recover the protected Conversations or Posts in a Standard Channel in HTML format.

It is useful in scenarios such as accidental deletion or corruption of messages in a Channel’s Conversation or Posts, enabling administrators to quickly provide the Channel members the required information for business continuity.

For more information, see Recover Conversations in HTML format.

Exchange Online: Support for native restore of data within In-Place Archive Mailbox

Native restore is writing back (In-Place) to the same destination on the Microsoft 365 tenant.

You can now execute a complete recovery in the event of accidental deletion of mail or corruption of In-Place Archive Mailbox in Exchange Online during a ransomware attack on the Microsoft 365 tenant.

To learn more, see Restore Emails.

Preview and download Teams Conversations in HTML

You now have an option to preview the entire message thread in a Team’s Conversations (Posts) and download it as a Druva generated HTML from inSync Management Console. It helps you to retrieve any business relevant conversation to address internal governance or audit requirements.
For more information, see Download Teams data.

**Classification of Teams backup data on the Overview page**

Get a break-up of backup details for Teams Metadata and Conversation on the Microsoft 365 **Overview** page in the

https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud

Updated: Fri, 24 Sep 2021 20:44:28 GMT

Powered by
inSync Management Console. Here’s a quick preview.

**Protocols Exchange Online and OneDrive data of Microsoft 365 Multi-Geo tenants**

Many financial and legal services organizations use Microsoft 365 with Multi-Geo to provision and store data at rest in the Microsoft 365 supported geo locations to meet their data residency requirements.

To enable such organizations to protect Exchange Online and OneDrive data of Microsoft 365 Multi-Geo tenants, inSync now lets you assign Druva storage to users based on their geo location.

For more information, see [Microsoft 365 Multi-Geo for Exchange Online and OneDrive users in inSync](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**[Early Access] Manage multiple Public folders for backup**

The availability of this feature may be limited based on the license type, region, and other criteria. To access this feature, contact your Druva Account Manager or Support.

inSync administrators can now enable or disable multiple Public folders for backup at one go, for ease of use.

For more information, see [Manage Public folder](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).
G Suite Enhancements

New Overview page

You no longer need to toggle between your configured G Suite apps to view the overall status of each configured app. inSync now brings to you a new Overview page that provides you a single pane of glass to view the important details of all your G Suite apps such as backup status, number of User mailboxes, Users, Shared Drives, and Backup Failures. With this view, you can quickly identify the actionable to ensure business continuity.

Here’s a glimpse of the new Overview page:

To learn more, see Overview page.

Early Access: Protect Public folder using Druva inSync

inSync administrators can now protect Public folder data to ensure business and operational continuity.

With Druva inSync, you can backup and download the following Public folder data:

- Emails and Posts
- Journals
- Notes
- Calendars
- Contacts
Currently, only backup and download of Public folder data is supported.

The availability of this feature may be limited based on the license type, region, and other criteria. To access this feature, contact your Druva Account Manager or Support.

For more information, see Protect Public folder.

Platform

Improved User Backup Inactivity alerts

User Backup Inactivity alerts are sent to inSync administrators for devices that are not backed up recently. With this update, inSync will check the device status before triggering the alert. If a user device is disabled the alert is suppressed, allowing administrators to focus on true exceptions rather than false alarms. For more information, see About inSync Alerts.

Last Backup Details

Last Backup Details page provides you with the following information:

- Number of backed up items (Mails, Folders, Calendars, and so on)
- Newly added items and updated items from the previous backup, count of deleted items and also a count of items that were missed and were not backed up
- Reason for the failure of backup for missed items
- Capability to download logs in order to view the backup activity details.

Restore Details

Restore Details provides you with the following information:
• Count and data size of successfully restored items
• Count and data size of items that were missed and not restored
• Reason for the failure of restore for missed items
• Capability to download logs to view the restore activity details

For more information, see:

• Last Backup Details page
• Restore Overview page

Administrator dependency for profile deletion removed

Now, while deleting a profile from inSync, there is no longer a need to unmap the administrators associated with that
profile. Administrators are automatically unmapped when the profile is deleted. However, please note that users associated with a profile, still need to be moved to other profiles, prior to deleting a profile.

To help easily identify profile administrators, and audit administrator access permissions, we have introduced the Administrator Details and Profile Mapping report. For more information, see Administrator Details and Profile Mapping report

**New report to track deleted devices**

Want to keep track of devices that are deleted from Druva inSync? Go ahead and check the new Deleted Device report in the inSync Management Console under Reports.

Available only to Cloud administrators, the report lists all the devices that are manually deleted by inSync administrators or auto-deleted by Druva inSync using the available mechanisms. It includes information such as the device name, device user details, backed up data, deleted mechanism, and so on. For more information, see Deleted Device Report.

**Patch update for inSync Connector**

Along-with support for Windows Server 2019 (64-bit), the following security issues are fixed with this patch update -

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS-11335</td>
<td>DRA-2020-1015: Code consisting of hardcoded token used for push notification has been removed.</td>
</tr>
<tr>
<td>INS-10427</td>
<td>DRA-2020-1011: Code consisting of OAuth secrets used for testing in a non-production environment has been removed.</td>
</tr>
<tr>
<td>INS-10626</td>
<td>DRA-2020-1012: Code consisting of hardcoded tokens used for testing in a non-production environment has been removed from the inSync Connector installer.</td>
</tr>
</tbody>
</table>

To upgrade inSync Connector, see Install or Upgrade inSync Connector.

**Patch update for inSync CloudCache Server**

We have released a security patch with the following updates on August 25, 2020.

- Updated TLS certificate
- Restricted communication to allow securely only over TLS v1.2

Along-with support for Windows Server 2019 (64-bit), the following security issues are fixed with this patch update -

---

https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud

Updated: Fri, 24 Sep 2021 20:44:28 GMT

Powered by
<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS-9929</td>
<td>DRA-2020-1010: Code consisting of hardcoded AWS key, which was used for testing in a non-production environment and later revoked, has been removed.</td>
</tr>
<tr>
<td>INS-10626</td>
<td>DRA-2020-1012: Code consisting of hardcoded tokens used for testing in a non-production environment has been removed from the inSync CloudCache Server installer.</td>
</tr>
<tr>
<td>INS-11336</td>
<td>DRA-2020-1014: Code consisting of hardcoded tokens used for testing in a non-production environment has been removed.</td>
</tr>
<tr>
<td>INS-11337</td>
<td>DRA-2020-1013 Code consisting of hardcoded token used for push notification has been removed.</td>
</tr>
</tbody>
</table>


**New User Activity Report**

Keep track of user account related activities such as the number of user accounts added, deleted, or preserved in Druva inSync using the User Activity Report. The report provides weekly as well as monthly consolidated view of user account statistics and helps administrators understand user license consumption trends within the organization.

[User activity report_RN_Aug8.png](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)

To learn more, see [User Activity Report](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Update AD/LDAP GUID using inSync Management Console**

Updating AD/LDAP GUID for preserved users is now a self-service and offers more convenience to the inSync administrators to perform this action right from the inSync Management Console.

inSync administrators no longer have to reach out to the Druva Support Team to fix the AD/LDAP GUID for users who get preserved in inSync due to a mismatch in the GUID.

For more information, see [Update AD/LDAP GUID for preserved users](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).
Accelerated inSync Client mass deployment on non-AD bound devices

You can now bulk deploy inSync Client on non-AD bound devices without configuring the device mapping.

All you need to do is configure the domain names. inSync uses the combination of the logged-in username on the devices over the specified domain to automatically create users in inSync, and activate inSync Client on those devices.

For more information, see [Integrated mass deployment without device mapping](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

Governance and Proactive compliance enhancements

**inSync Compliance**

**Mark files as false positive in inSync Compliance**

As a Compliance administrator, it’s likely that you will find file violations in your environment that are false positives and not deemed sensitive by your organization. This is why now we introduce the option to mark such files as **False Positives**.

You can go ahead and whitelist the hash value of the file so that inSync does not report any more violations for the same file for any user across the organization. Also, all existing violations that have been reported for the whitelisted file are auto-resolved.
Whitelisting file hashes reduces the clutter of unwanted violations and helps you focus on violations that are business-critical for your organization. For more information, see File Hash Whitelist in inSync Compliance.

New reports to track deleted files and deleted emails

The new reports, Defensible Delete Report for Files and Defensible Delete Report for Emails, give detailed information about the files and emails that inSync Cloud administrators have deleted. You can view details such as the status of the delete action, the time, administrator name, and so on.

These reports can be viewed by all inSync administrators and are particularly useful if you do not have file and email deletion rights. Use these reports to understand and audit the actions taken by inSync Cloud administrators.

For more information, see Defensible Delete Report for Files and Defensible Delete Report for Emails.

Legal Hold

A new GUI-based utility to download custodian data

Gone are the days when administrators were required to manually create a CSV and run several commands to download custodian data.

By introducing eDiscovery Download Client, we have simplified the entire process of downloading and managing custodian data. Cloud and Legal administrators can now initiate a download and perform all other download-related actions directly from the inSync Management Console. For more information, see Download data using eDiscovery Download Client.

Benefits

Here are the benefits and a sneak-peek of the new Client:

► Easy installation and secure registration process

► Option to choose the type of data that you want to download

► Enhanced UI to manage and monitor the Download Jobs

► Up to 20x faster downloads

Customer action required
All you need do is ensure the hardware and software requirements are met to install the new eDiscovery Download Client. For more information, see [Prerequisites to install eDiscovery Download Client](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Governance**

**Additional details for Defensible Delete actions**

Whenever an inSync administrator initiates a file deletion, inSync creates the following Admin Audit Trail entry:

```
john.doe@druva.org deleted file, reports.txt from data source and snapshot
File was found on Win1498 owned by ernie.carter and was marked as delete from data source and snapshot.
```

Now, inSync will add additional details to the deletion audit trail entry, such as file path and file size.

```
john.doe@druva.org deleted file, reports.txt from data source and snapshot
File was found on Win1498 owned by ernie.carter and was marked as delete from data source and snapshot.
Filepath: D:\Data\NewFiles\reports.txt
Size: 97.00 KB
```

Similarly, for emails, inSync will now add attachment name, email attachment size, and so on. These details will also be a part of the inSync Events API that you have configured with SIEM tools.

During audits and investigations, the additional details will help your organization’s Legal, IT, and Information Security teams to get better visibility of administrator actions and act faster. For more information, see [Defensible Deletion of Files and Emails](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Quarantine files from Federated Search**

During compliance audits, if you learn about a non-compliant file, now you can use [Federated Search](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud) to find all possible matches of that file and quarantine them.

inSync moves the quarantined files to the Quarantine Bay so that inSync Client users cannot access the file or any of its previous versions present in the snapshots.

During the quarantining process, you can also choose to delete the non-compliant files from their data sources. This ensures that you meet regulatory requirements of retaining copies of the file in snapshots and eliminate the risk of the non-compliant data being shared across other users in the organization. For more information, see [Quarantine Files](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**inSync Client**

**inSync Client v6.8.2 for Mac: Support for Apple M1 devices**

Committed to providing enhanced endpoint data protection, we are excited to announce the availability of inSync Client

https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud

Updated: Fri, 24 Sep 2021 20:44:28 GMT

Powered by 21
v6.8.2 which provides seamless endpoint data protection on Mac devices with ARM-based Apple M1 processor.

**Customer action:** Upgrade to inSync Client version v6.8.2, as this version is a prerequisite for any future auto-upgrades of inSync Client on Apple M1 devices.

**Note:** Customer action is not required if you are already using inSync Client v6.8.0.

### inSync Client v6.8.1 for Windows

A patch update v6.8.1 is now available for Windows OS.

### Revision Information

<table>
<thead>
<tr>
<th>Product Version</th>
<th>OS</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>inSync Client v6.8.2</td>
<td>macOS</td>
<td>r110030</td>
</tr>
<tr>
<td>inSync Client v6.8.1</td>
<td>Windows</td>
<td>r110020</td>
</tr>
</tbody>
</table>

Druva has not released a new version of inSync Client for Linux OS with inSync Client v6.8.1. You can continue using inSync Client v5.9 for Linux with inSync Cloud.

Download the latest inSync Client [here](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

For upgrade instructions, see [Upgrade inSync Client](#).

For more information, contact [Druva Support](#).

### inSync Mobile App

#### Deprecation announcement

**Edit section inSync mobile app for Windows Phone 8.x**

The inSync mobile app is no longer supported on the Windows Phone 8.x. As a result, inSync users will not be able to activate the inSync mobile app on their Windows 8.x devices.

**Action required:** If you are an inSync mobile app user on Windows Phone 8.x, we recommend you to restore the data...
on your device within a period of 60 days from today.

The backed up data will be automatically erased from the inSync Cloud after a period of 60 days.

For more information, see [End of Life (EoL) Policies](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud) or contact [Druva Support](mailto:).

### Fixed issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS-11121</td>
<td>Fixed pagination issue with 'List EndPoint Backups' API where the next page of records was not returned after passing the 'pageToken' parameter in the API request.</td>
</tr>
<tr>
<td>INS-10602</td>
<td>User Rollout Report displayed incorrect status of System Settings backup.</td>
</tr>
<tr>
<td>INS-9663</td>
<td>Fixed the behavior wherein inSync customers with only Cloud Apps licenses were unable to create a new profile.</td>
</tr>
<tr>
<td>INS-9521</td>
<td>Fixed an issue where Idle Session Timeout duration was not honored, and administrators were logged out automatically too soon in case of inactivity on the inSync Management Console.</td>
</tr>
<tr>
<td>INS-10199</td>
<td>Fixed behavior for inSync Client auto-upgrade functionality where Daily Upgrade Limit, when set to unlimited (0), was not honored.</td>
</tr>
<tr>
<td>INS-10151</td>
<td>Fixed the behavior wherein inSync failed to auto-delete preserved users marked for deletion.</td>
</tr>
<tr>
<td>INS-12240</td>
<td>Fixed the behavior wherein there was a discrepancy in the Total Backup Data value displayed on the inSync Management Console and the value fetched using the Get Device API for a device.</td>
</tr>
<tr>
<td>INS-12049</td>
<td>Fixed the issue wherein the administrators did not receive <a href="https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud">User Backup Inactivity</a> alert despite being a part of the subscriber’s list.</td>
</tr>
</tbody>
</table>
INS-13265  Fixed the issue wherein Salesforce backup completed partially with an error stating connection aborted and object skipped from backup.

INS-13150  Restricted inSync from sending Cloud Apps backup alert emails when the AD connector is in a disconnected state.

INS-13127  Fixed an issue wherein the administrators were unable to unzip the downloaded SharePoint Online data using inSync.

INS-12485  Fixed Google Drive backup issue wherein backups failed with error: “Response too large”.

INS-13271  Fixed an issue wherein In-Place Archive mailbox backup fails for a single user.

INS-12632  Fixed the UI issues observed with the Global Exclusions > Exclude files page when multiple file extensions were added for exclusion.

INS-12172  Fixed the discrepancy observed in the data usage value displayed on the User Summary and Data Usage widget on the inSync dashboard page.

INS-13058  Fixed the administrator account creation issue wherein account creation for both inSync and DCP administrators failed with error: “Failed to create administrator. Attribute value in Active Directory is empty.”

INS-13737  Fixed the issue wherein SharePoint sites with the same URL were added multiple times in inSync after auto discovery.

INS-13926  Fixed the Exchange Online issue wherein In-Place Archive Mailbox was not getting backed up.

INS-14794  For customers with both endpoints and Cloud Apps, there was a mismatch in the count of inactive devices displayed on the inSync Management Console and the Inactive Devices report.
After enabling secured login, backups failed for Microsoft 365 users with **Authentication Failure** error.

During device mapping, if any mapping fails, the **Download Failed devices mapped** CSV contains only one entry even if there are multiple failed mappings.

Fixed the issue wherein **User Device Inactivity** alert is sent for disabled devices.

inSync Client v6.7.0 activation failed when trying to establish a connection with inSync Cloud using Kerberos-based proxy authentication.

CVE-2020-5798: Fixed a vulnerability in inSync Client for macOS, wherein an attacker could have gained privileges of a root user from a user of the admin group due to improper integrity checks and directory permissions.

Fixed the following issues for inSync Client running on macOS:

- inSync Client application failed to launch post successful installation
- SSO Authentication failed during inSync Client activation
- Bulk deployment of inSync Client failed using Integrated Mass Deployment (IMD)

If you have Federated Search enabled and you are trying to search and restore the user’s Microsoft OneDrive or Google Drive account using the **Restore as a copy** option, inSync creates the folder, however, fails to restore the files inside it and displays ‘Restore done with errors’ message.

### Known Issues

The following issues were identified by our Quality Assurance team

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>

https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud

Updated: Fri, 24 Sep 2021 20:44:28 GMT

Powered by 25
When you perform In-Place Restore of emails with Mails folder and Include In-Place Archive Mails option selected, the In-Place Archive Mails are restored under Primary Mailbox instead of In-Place Archive Mailbox folder.

For SharePoint List items with attachments, the audit details for the Modified time and Modified By fields do not get restored with the correct (original) modified time and user name or modifier.

File deletion fails when you try to search and delete a file using Federated Search.

**inSync Client v6.8.0 for GovCloud**

Committed to delivering an enhanced product experience, we are happy to announce the availability of inSync Client v6.8.0 for inSync GovCloud.

The following feature is available with this release, dated November 07, 2020:

**Enhancement**

**Enhanced capability to add new devices for remote users**

If you are issuing a replacement device to a non-AD bound remote user, be rest assured about the incremental data that is generated on the old device.

Enhancements to the device replacement workflow ensure that the remote users get the most recent data from their old devices onto their new devices.

For more information, see [Device replacement using Integrated Mass Deployment](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

*Note: This feature is available on request. Contact Druva Support to enable this feature for your account.*

**Fixed Issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS-64</td>
<td>inSync now seeks user's consent if inSync Client activation is being performed using a IDK file.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>INS-10418</td>
<td>Fixed a vulnerability where an attacker could have accessed other user's data through user impersonation during IMD activation (mass deployment) process.</td>
</tr>
</tbody>
</table>

Revision Information

**Product** | **Revision**
--- | ---
Windows: | r110000
inSync Client | Mac: r110000

Druva has not released a new version of inSync Client for Linux OS with inSync Client v6.8.0. You can continue using inSync Client v5.9 for Linux with inSync GovCloud.

Download the latest inSync Client [here](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

For upgrade instructions, see [Upgrade inSync Client](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

For more information, contact [Druva Support](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**inSync Client released on Sept 19, 2020**

The following versions of inSync Client are available with this release for inSync GovCloud.

- **inSync Client for Windows** - v6.7.1
- **inSync Client for macOS** - v6.7.0

**Enhancements**

- [Enhanced restore UI for increased visibility and actionable insights](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
- [Capability to define MIME types](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
- [Protect only what is important for your organization](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
- [Enhanced settings for notifications shown on devices](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
- [Enhanced preferences to allow and restrict networks](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
- [Enhanced privacy settings to access user logs](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
- [Simplified inSync deployment for Microsoft Azure Active Directory](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
- [Customize system settings restore during device refresh](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
- [Improvements to backup OneDrive Files On-Demand](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
Enhanced Restore UI for increased visibility and actionable insights

The new inSync restore UI now provides additional details about the restore progress, time elapsed, and incomplete or failed restore responses. Such actionable insights prove to be of great help to the users to quickly understand and address simple issues with minimal involvement of inSync administrators.

In addition, the restore details page’s elements are now clickable to help you further explore the data.

Capability to define MIME types

We have introduced the option to backup data based on file MIME types to ensure that you do not miss out on backing up critical data.

This ensures that any inadvertent or malicious changes to the file extensions by end-users will not exclude business-critical files from being backed up to help with future data recovery or litigation.

Note: This feature is available on request. Contact Druva Support to enable this feature for your account.

To learn more about defining MIME types, see Define file inclusions.

Protect only what is important for your organization

Configuring specific folders that are located across different storage locations for backup now gets simpler!

The enhanced profile configuration enables you to precisely configure only a specific folder or a group of folders for backup. This significantly reduces the backup time and network bandwidth utilization and improves the overall end-user experience.

To learn more, see Add custom folders for backup.

Enhanced settings for notifications shown on devices

You can now select from a range of inSync notifications to notify users of all inSync activities or just the critical ones requiring immediate attention. You can also let the end-users configure the notifications to suit their preference from the inSync Client interface.

To learn more, see inSync Notifications.

Enhanced preferences to allow and restrict networks

Get precise control over allowing inSync backups only on preferred networks and restricting backups when users are connected through non-trusted networks. Also, to ensure clarity for inSync users, the enhanced inSync Client interface
displays the selected network settings.

To learn more, see Allow and restrict networks.

**Enhanced privacy settings to access user logs**

Backup Data Privacy Settings and Logs Privacy Settings are now separately configurable in inSync profiles, allowing administrators to retain visibility into a subset of user logs for troubleshooting. This allows the administrators to access the user logs from a user device, even when the administrators do not have visibility into the actual data being backed up.

To learn more, see Configure user data privacy policy.

---

**Important**

By default, inSync enables administrator access to user logs for all the existing profiles.

**Action required:** If you do not want administrators to access the user logs for an existing profile, you can modify these settings from the Profiles section on the inSync Management Console. To learn more, refer Update a profile.

**Simplified inSync deployment for Microsoft Azure Active Directory**

Introducing a new inSync mass deployment workflow that simplifies inSync deployment and automatic activation of inSync Client on Azure AD joined Windows 10 devices.

Users can be directly provisioned within inSync from Azure AD through SCIM integration and inSync Client activation process on Azure AD bound devices will not require users to enter their email address. All of it, without the need to configure the inSync Connector.

To learn more, see inSync mass deployment.

**Customize system settings during device refresh**

Do you come across device refresh instances where you might not want to restore the system/app settings for a particular program or application?

With the customizable system settings restore feature, you can now define the persona settings which you want to exclude from the restore. So that the users get the replacement device in a configured state just as you want.

To learn more, contact Druva Support.

**Improvements to backup OneDrive Files On-Demand**

Introducing the enhanced mechanism that backs up only the locally available OneDrive files and skips the Files On-Demand. This feature ensures that you get the correct status of the inSync backup activities.
## Fixed Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS-9223</td>
<td>The user device goes to an unstable state, and the user can no longer log in to the device using Azure AD credentials when data from Azure connected device is restored to another Azure connected device.</td>
</tr>
<tr>
<td>INS-7533</td>
<td>Microsoft Visual Studio distribution dependencies are updated to use visual studio version 2015.</td>
</tr>
</tbody>
</table>

## Known Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS-12167,</td>
<td>If you are using inSync Client on macOS Catalina (10.15), you cannot complete the following actions using the keyboard shortcuts, if VoiceOver is in turned on mode:</td>
</tr>
<tr>
<td>INS-12169,</td>
<td>• Add folders for backup in Backup &amp; Restore tab</td>
</tr>
<tr>
<td>INS-12225</td>
<td>• Select folders or sub-folders for restore on the inSync Restore window</td>
</tr>
<tr>
<td></td>
<td>• Select share folder location in the Sync &amp; Share tab</td>
</tr>
</tbody>
</table>

## Revision information

<table>
<thead>
<tr>
<th>Product</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>r108801</td>
</tr>
<tr>
<td>macOS</td>
<td>r107661</td>
</tr>
</tbody>
</table>

Druva has not released a new version of inSync Client for Linux OS with inSync Client v6.7.1. You can continue using inSync Client v5.9 for Linux with inSync Cloud.

Download the latest inSync Client [here](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

For upgrade instructions, see [Upgrade inSync Client](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

To learn more, contact [Druva Support](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).
Patch update for inSync CloudCache Server

We have released a security patch with the following updates on August 25, 2020.

- Updated TLS certificate
- Restricted communication to allow securely only over TLS v1.2

To upgrade inSync CloudCache Server, see inSync CloudCache Server.

inSync GovCloud Update on July 18, 2020

The following enhancements and issues are fixed with this GovCloud update.

Enhancements

- Platform enhancements
- Governance & Proactive Compliance enhancements
- CloudApps enhancements
- API enhancements

Platform enhancements

A refreshed inSync dashboard

You can now do more with the simplified and refreshed inSync dashboard:

► Separate widgets for your data sources
  Based on the services purchased, the new dashboard now displays the backup status and details of the devices and cloud application in their own dedicated widgets:

► Monitor the live activities of the ongoing backup and restore tasks
  Monitor and track the ongoing backup and restore tasks across various configured data sources through the Live Activities widget:

► View backup and restore trends at a glance
  Analyze the data backup and restore trends across all the workloads for a period of 30 days and detect anomalies, with this new widget:
Here’s the new look of the inSync dashboard:

**Accelerate device refresh through selective data restore**

inSync administrators now have an option to restore only the essential data when issuing a new device to the users during device refresh activity. This accelerates the device replacement process and helps users quickly get started.

This is a profile level setting and administrators can select the ‘Exclude from Automated Restore’ check-box if they do not want such folders to be restored automatically on the new device.

This feature does not restrict the inSync users from accessing their data that was not restored as a part of the device refresh through inSync Client on their new device. To learn more, see Create a profile.

---

**Note:** To enable the selective data restore feature, contact Druva Support who will be happy to assist you to set it up for your account.

---

**Now auto delete inactive devices starting 30 days**

Druva has relaxed the limit on the minimum number of days a device should be in the inactive state before it is automatically deleted from inSync from 90 days to 30 days. To configure auto deletion of inactive devices in inSync, see Configure auto-delete of inactive devices in a profile.

---

**Delegate device management capabilities to Profile and Helpdesk administrators**

---

https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud

Updated: Fri, 24 Sep 2021 20:44:28 GMT
Powered by
A Druva Cloud Admin or inSync Cloud Admin can now assign and delegate the Manage Device Mapping and Manage Client Upgrade rights to a Profile or Helpdesk Administrator. Profile and Helpdesk administrators can then manage devices and inSync Client installation for users under their control.

For more information, see Predefined roles and rights.

Enhanced privacy settings for user logs access

Backup Data Privacy Settings and Logs Privacy Settings are now separately configurable in inSync profiles, allowing administrators to retain visibility into user logs for troubleshooting purposes.

This allows the administrators to access the user logs from a user device, even when the administrators do not have visibility into the actual data being backed up. To learn more, refer Configure user data privacy policy.

**Important:** By default, inSync enables administrator access to user logs for all the existing profiles.

**Action required:** If you do not want administrators to access the user logs for an existing profile, you can modify these settings from the Profiles section on the inSync Management Console. To learn more, refer Update a Profile.

Option to upgrade inSync Client to any supported version

As an inSync administrator, you can now choose to upgrade the inSync Client on user devices to any of the supported versions within the list. To learn more, refer Upgrade inSync Client.

Governance & Proactive Compliance enhancements

New version of the inSync Direct Download utility

Go ahead and try the new version of the inSync Direct Download utility (v1.2) to experience the following enhancements:

- Support for the latest OS versions including macOS 10.15 Catalina.
- Improved Error Logs that contain only the list of files that failed to download even after retries. All the retry entries are now a part of the newly introduced Warning Logs.
- Notarized Direct Download utility app available in Zip format for macOS.

To learn more, see inSync Direct Download Utility.

inSync Compliance: New Sensitive Data types for CCPA, PII, and PHI use cases
To help you with CCPA (California Consumer Privacy Act), Personal Information Identifiers (PII) and Protected Health Information (PHI) data governance, we have introduced several new Sensitive Data types. We have also updated the CCPA (California Consumer Privacy Act) template to include the following sensitive data types:

- Credit/Debit numbers near PII
- Ethnicity terms
- Employer Identification Number
- Personal sensitive data

The new data types effectively widen the scope of data that can be scanned for Personal Information Identifiers (PII) and Protected Health Information (PHI). You can select the new data types while creating new custom templates or modifying existing custom templates. For more information, see Manage sensitive data.

**Delegate device management capabilities for Profile and Helpdesk administrators**

For a legal matter in question, Druva inSync collects data of custodians (users on Legal Hold) from all the supported data sources and makes it available for the legal administrators for further review and actions. As we expand our coverage of more data sources under protection, we want to ensure that all of custodians’ data sources are listed and available for immediate action in a single sortable view. Hence, we have introduced the Collection Stream feature.

The Collection Stream tab lists all the data sources of all the custodians who are on Legal Hold and also displays details related to backup activity on the device. You can also filter the Data Sources by the Custodian name. For more information, see View last backup details of users on legal hold.

**Group similar Legal Holds using custom Types**

You already have the ability to classify Legal Holds into 3 predefined Types. Now, we have added the ability to define a custom Type and associate it with a Legal Hold policy.

You can use Types to segregate the existing and new Legal Holds into easily identifiable groups. Later, you can filter Legal Holds by these Types to quickly find and view the desired Legal Hold. For more information, see Update the legal hold policy name and policy type.

**Support for email deletion using Federated Search and Proactive Compliance**

It is critical for organizations to ensure that a high risk, non-compliant, objectionable email is not present on the end user’s data sources and back up data set. Which is why, defensible deletion is a comprehensive approach that organizations implement to reduce legal and compliance risks associated with the retention of Electronically Stored Information (ESI).
To that effect, inSync now provides the capability to search and delete emails from the data source and/or snapshot through Federated Search and Proactive Compliance. This capability is available for the following hosted mail services configured in Druva inSync Elite and Elite Plus versions:

- Microsoft Exchange Online
- Gmail

For more information about how to delete emails by using Federated Search, see [How to search backed up files](#).

For more information about how to delete non-compliant emails by using Proactive Compliance, see [How do I resolve a compliance violation?](#)

**Federated Search for Google Shared Drives**

With this release, we have added Google Shared Drives to the list of Data Sources that you can query for file search.

For more information, see [Federated Search for backed up data](#)

**CloudApps enhancements**

**Protect Microsoft Teams Channels using Druva inSync**

With the rapid adoption of Microsoft O365 Teams as a key collaboration app, it has become essential for IT admins to protect the data shared within Teams in order to recover from any accidental deletion, data corruption, or malicious attack such as ransomware.

Druva inSync for O365 provides a comprehensive, scalable, and cost-effective backup and recovery solution for IT admins to:

- Protect all your Teams data with all channels (Standard and Private), posts (Conversations), files (including Wiki), apps, settings within the channels, and entire permissions and members of Teams.
- Rapidly recover Teams channels, files, posts (Conversations), and settings from any accidental deletion, data corruption, or ransomware attack. This, in turn, ensures business continuity for all users of Teams.
- Simplify the internal governance through access to audits, backup logs, and reports for Teams.

inSync administrators can also enable or disable multiple Teams for backup and restore at one go, for ease of use.

For more information, see [Protect Teams](#).

**Action required:** If you are already protecting Office 365 data with Druva, you have to [Reconfigure Office 365 app](#) to start protecting Teams.
inSync for Office 365 gets a new Overview page

You no longer need to toggle between your configured Office 365 apps to view the overall status of each configured app. inSync now brings to you a new Overview page that provides you a single pane of glass to view the important details of all your Office 365 apps such as backup status, number of User mailboxes, Users, SharePoint Sites, and Backup Failures. With this view, you can quickly identify the actionables to ensure business continuity.

Key highlights of the new Overview page:

User account settings and validate Office 365 configuration

You can reconfigure Office 365, verify Office 365 configurations, and manage user account settings on the Overview page.

Summary of protected data for configured Office 365 apps

You can get an overview of storage consumption by each configured Office 365 app and data distribution details. You can also view the current status of the Office 365 app and the last configured date and timestamp details.

A comprehensive overview of the critical details of each configured Office 365 app

You can view the count and backup status of Users, User mailboxes, and SharePoint Sites.

For more information, refer to the documentation on the Overview page.

inSync for Office 365 gets a new user experience

The newly redesigned user interface for Druva inSync for Office 365 apps (Exchange Online, OneDrive, and SharePoint Online) provide inSync administrators with a modern and intuitive experience for easy access to backup settings and management of frequent admin tasks such as backup, restore, download.

Following are the key highlights of the new UI:

New navigation pane for quick access to all Office 365 apps

On the Manage Cloud Apps page, when you select Office 365, inSync will now display a new left navigation panel that lists all the supported Office 365 apps.

Exchange Online and OneDrive: Quick and easy access to frequent administration tasks

inSync now enables you to quickly perform the following key actions for Exchange Online and OneDrive:

- Manual or on-demand backup
• Enable backup
• Disable backup
• Delete user

**SharePoint: Simplified experience for managing SharePoint Sites**

inSync now provides an enhanced UI to quickly perform the following actions:

• Automatic and manual discovery of the SharePoint sites within your organization
• Adding Site Collection manually
• Auto-Configuration and custom configuration of SharePoint sites for backup
• Day-to-day housekeeping tasks such as disabling and deleting SharePoint sites that do not require backup

For more information, see [inSync Management Console](#).

**SharePoint: Intuitive approach for managing backups and snapshots**

With the new UI, we are introducing a new **Backups** tab to search SharePoint Sites and initiate a restore and download operation for the selected site collection. Folders and files within the folders are displayed in a tree structure for ease of navigation. For more information, see [inSync Management Console](#).

**inSync for G Suite gets a new user experience**

The newly redesigned user interface for G Suite apps (Gmail, Google Drive, and Shared Drives) provides inSync administrators with a modern, and intuitive experience for easy access and management of frequent admin tasks such as backup, restore, and download.

Following are the key highlights of the new UI:

**New navigation pane for quick access to all G Suite apps**

On the **Manage Cloud Apps** page, when you select **G Suite**, inSync now displays a new left navigation panel that lists all the supported G Suite apps.

**Gmail and Google Drive: Quick and easy access to frequent administration tasks**

inSync now enables you to quickly perform the following key actions for Gmail and Google Drive:

• Manual or on-demand backup
• Enable backup
• Disable backup
• Delete user

**Shared Drives: Simplified experience for managing Shared Drives**

inSync now provides an enhanced UI to quickly perform the following actions:

• Automatic and manual discovery of the Shared Drives within your organization
• Adding Shared Drives manually
• Auto-Configuration and custom configuration of Shared Drives for backup

For more information, see inSync Management Console.

**Shared Drives: Enhanced experience to restore and download Shared Drives data**

To quickly find the specific files to restore in GSuite Shared Drive, we are introducing an intuitive way to search Shared Drives and initiate a restore and download for the selected Shared Drive. Folders and files within the folders are displayed in a tree structure for ease of navigation. For more information, see inSync Management Console.

**Search and Restore Google Shared Drives files**

Restoring and downloading multiple files is simpler and faster now. You can also use the Search capabilities in the Restore Data window on the inSync Management Console to search, restore, and download Google Shared Drives files.

For more information, see Restore Shared Drives data.

**Cloud Apps: Added a new option to define the retention period for Emails**

inSync administrators now have the flexibility to choose the type of retention policy for emails protected as part of Exchange Online and Gmail backup.

Administrators can choose from any one of the following options:

• **Snapshot based**: Apply the same retention policy as applicable to Files.

• **Email event date and time based**: Define the number of months for which the emails should be retained.

For more information, see Define the backup retention policy for Cloud Apps.
**API Enhancements**

**Role-Based API Access**

As a Druva Cloud administrator, you can now restrict the information returned in an API response based on the role of the administrator accessing Druva APIs. You can assign access at the time of generating the API credentials.

Go ahead and check the feature to ensure Druva APIs are utilized more securely and effectively within your organization.

For more information, see [Apply Authorization Restrictions](#).

**Get device list using profileID**

The ‘List all devices’ API now enables administrators to get the list of all the user devices associated with multiple profiles using the ‘profileID’ parameter.

For more information, see [API reference on the Druva developer portal](#).

**Fixed Issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS-8612</td>
<td>Fixed an issue where data backed up for Exchange Online users was displayed in negative.</td>
</tr>
<tr>
<td>INS-3259</td>
<td>Fixed license upgrade issue which failed with Internal Error.</td>
</tr>
<tr>
<td>INS-6052</td>
<td>Fixed the behavior wherein the user provisioning automatically changed from AD/LDAP to SCIM without admin triggering any changes.</td>
</tr>
<tr>
<td>INS-7304</td>
<td>Fixed the behavior where Google Shared Drives backups failed.</td>
</tr>
<tr>
<td>INS-5769</td>
<td>Creation of SCIM mapping failed as SCIM attribute filter did not support value with special characters.</td>
</tr>
<tr>
<td>INS-5159</td>
<td>Fixed the behavior where the Integrated mass deployment process did not retry the deployment aborted due to a network failure.</td>
</tr>
<tr>
<td>INS-6160</td>
<td>Fixed caching behavior where inSync cached proxy details from the PAC file. When a user is moved to different locations, stale cache data caused inSync to use older proxy details leading to failed connection to inSync Cloud.</td>
</tr>
</tbody>
</table>

**Note**: Reconfigure G Suite from the inSync Management Console for this fix to work.
Known Issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6672</td>
<td>Due to OS limitations, if the data is downloaded using the Direct Download Utility tool across platforms, for example, Windows to Mac, the file properties on macOS may not display the true ‘Creation Timestamp’ for the selected file. <strong>Workaround:</strong> To view the true metadata value for the file ‘Creation Timestamp’ at the source device, refer to the Chain of custody report.</td>
</tr>
</tbody>
</table>

Deprecation Announcement

**Removed HTML support in inSync emails**

Druva has removed the support for HTML tags used in formatting custom email templates. inSync administrators can format the custom email templates in plain text.

For more information, contact [Druva Support](#).

inSync GovCloud Update on Jun 27, 2020

The following issues were fixed with this GovCloud update.

Fixed Issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS-10624</td>
<td>Fixed backup issues arising for Exchange Online archive mailbox due to the recent API changes made by Microsoft for Office 365 Exchange Online services. For the changes to take effect and continue seamless backups, Druva inSync requires additional permission to access your Office 365 data. <strong>Action required</strong> - Re-configure Druva inSync Office 365 app to grant the required permission to protect Exchange Online archive mailbox. For instructions, see <a href="#">Reconfigure Office 365</a>.</td>
</tr>
<tr>
<td>INS-11121</td>
<td>Fixed pagination issue with 'List EndPoint Backups' API where the next page of records was not returned after passing the 'pageToken' parameter in the API request.</td>
</tr>
</tbody>
</table>
inSync GovCloud Update on May 21, 2020

inSync Client patch update v6.6.4 for Windows OS is now available for inSync GovCloud, with the following fixed issue.

Fixed Issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5788</td>
<td>In continuation to the fix for CVE-2019-3999 that was provided with inSync Client v6.6.0, this release provides a complete fix for CVE-2019-3999 which includes the security vulnerability wherein an attacker could have exploited the improper neutralization of special elements and CVE-2020-5752 wherein an attacker could have exploited relative path traversal used in the OS commands to gain administrative access on the system.</td>
</tr>
</tbody>
</table>

Revision Information

<table>
<thead>
<tr>
<th>Product</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>inSync Client</td>
<td>Windows: r103713</td>
</tr>
</tbody>
</table>

Download the latest inSync Client, [here](#).

To upgrade inSync Client to the latest version, see [Upgrade inSync Client](#).

For more information, contact Support.

inSync GovCloud Update on Apr 11, 2020

The following issue is fixed with this GovCloud update.

Fixed Issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8116</td>
<td>The Devices column on the Manage Users page incorrectly displayed '0' as the device count against the actual device count associated with the users.</td>
</tr>
</tbody>
</table>

inSync Client released on Mar 23, 2020

The following versions of inSync Client are available for inSync GovCloud.

- inSync Client for Windows - v6.6.2
- inSync Client version for macOS - v6.5.1 and v6.6.2
Important: Upgrade to inSync Client v6.6.x on macOS is supported only from inSync Client v6.5.1.

Enhancements

The new version of inSync Client comes up with enhanced data protection features which include the following:

- **Support for Spanish language**
- **Simplified inSync Client activation on macOS**
- **Improved Remote Device refresh**
- **Enhanced Restore Activity Summary**
- **Branding changes with a fresh new look for inSync Client**

**Support for Spanish language**

This feature is exclusive to inSync Client v6.6.x.

You can start installing the new client in Spanish locale if that’s your preferred language.

With this addition, inSync Client is now available in English, Japanese, French, German, and Spanish languages to cater to the users with language diversity.

**Simplified inSync Client activation on macOS**

To help new inSync users get started quickly, we have simplified the inSync Client activation process for macOS.

Administrators now have an option to build a custom installer package for MAC devices, with pre-configured activation parameters such as Cloud URL, auto-launch, and Proxy settings. Users can then easily activate inSync Client by just providing their login credentials. Simple, isn’t it?

To learn more, see [customize inSync Client for Mac devices](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Improved Remote Device Refresh**

Next time you issue a new replacement device and ship it to the users with their data, you can rest assured that the data backed up on the old device during the transition period is available to users on their new replacement device.

Upon activation, inSync Client automatically restores the most recent data to the user’s new device.

To learn more, see [remote device refresh using IMD](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Enhanced Restore Activity Summary**

It is now even simpler to monitor and track the restore activities on the inSync Management Console.

Multiple files that are selected for restore are unified and displayed as a single restore activity on the Restore Overview.
page. You can now also download the missed file logs for the restores that are completed with errors.

In addition, for better visibility to users, a new ‘Failed’ status tab on the inSync Client restore window displays the restore activities that have failed.

**Branding changes with a fresh new look for inSync Client**

We have enhanced the inSync system tray icon for the ‘Backup in progress’ operation.

See the entire list of inSync icons and what they mean [here](#).

**Block backups on metered networks**

Connected to a VPN through a private network and worried about additional data consumption over this network? Rest assured, inSync will not perform backups if you are connected to VPN through a network which you have already added in the blocked list.

**Upgrade inSync Client**

To upgrade inSync Client to the latest version, see [Upgrade inSync Client](#).

**Fixed Issue**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5789</td>
<td>Security vulnerability during communication between inSync Client processes.</td>
</tr>
</tbody>
</table>

**inSync GovCloud Update on Mar 21, 2020**

**Enhancements**

The following enhancements are available with this GovCloud update:

- [inSync APIs](#)
- [Governance enhancements](#)
- [Proactive Compliance enhancements](#)
- [Platform enhancements](#)

**inSync APIs**

**Automate and manage routine inSync tasks using APIs**

---

https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud

Updated: Fri, 24 Sep 2021 20:44:28 GMT

Powered by
We are rolling out a bunch of new APIs which are designed to ease your efforts of managing inSync administrative tasks and features. Also, introducing a brand new developer portal to assist our customers’ interaction with APIs.

To enable and use APIs, see [Integration with Druva APIs](https://developer.druva.com).


Here’s a list of Druva inSync APIs available with this GovCloud update:

- APIs to manage user actions
  - List users
  - Create a new user
  - Get user information
  - Update user information
  - Delete a user
  - Reset password for a user
  - Preserve a user

- APIs to manage devices
  - List devices
  - Get device information
  - Disable a device
  - Delete a device and so on

- APIs to manage profiles configured in inSync
  - List all profiles
  - Get profile information

- APIs to view the consumption of storage and CloudCache servers
  - List all storage
  - Get storage information
  - List all CloudCache servers
- Get CloudCache server information

- Enhanced Legal Hold v3 to manage legal hold policies and get the list of users on legal hold.
  
  - List legal hold policies
  
  - Create a legal hold policy
  
  - Get details of legal hold policy
  
  - Delete a legal hold policy
  
  - Add or delete users (custodians)
  
  - List the users on legal hold
  
  - List of legal hold policies associated with a user

**Governance enhancements**

**Legal Hold UX enhancements**

The newly redesigned Legal Hold user interface provides inSync administrators with a modern, and intuitive experience for managing custodians and legal holds. Following are the key highlights of the new UI:

- **New Overview page**

  A new Legal Hold Overview page provides a quick summary of the Legal Holds, data associated with Legal Holds, and the custodians across your organization. For more information, see [Legal Hold page](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

- **Simplified Legal Hold creation process**

  Legal Hold creation is now a 2-step process, instead of 3. While adding a custodian to a legal hold, inSync administrators can now search a custodian by name or email, thus eliminating the additional step of custodian validation. For more information, see [Create a Legal Hold](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

- **Option to filter Legal Holds**

  The new Legal Hold listing page has options to filter Legal Holds by name, type, and custodian name. These help you to get to the required information faster and quicker. For more information, see [Manage a Legal Hold policy](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Capability to search for Folders**

Now you can use the Search functionality available on the **Restore Data** window on inSync Management Console to search for folders present on devices, Google Drive, and One Drive.
This enables you to restore an entire directory of files at one go without having to restore them one-by-one.

For more information, see Search backed up data to download or restore.

### Proactive Compliance enhancements

#### Get ready for California Consumer Privacy Act (CCPA)

We have made it easy for your organization to comply with the newly introduced CCPA. Now, there is a new pre-defined template named California Consumer Privacy Act in inSync Compliance. By default, any compliance policy using this template scans data for the following personal information of a user:

- Passport Details (Global)
- Drivers License with qualifying terms (USA)
- Social Security Numbers (USA)
- Drivers License (USA)

inSync flags a violation if any one of the above-mentioned data types exceeds the critical threshold count.

For more information, see Manage policy template.

#### Capability to test violations on sample data for sensitive data and policy templates in inSync Compliance

Gone are the days when you had to wait for a backup cycle to check if inSync is flagging the expected violations. Now, you can test custom sensitive data and custom policy templates while creating them.

You can also validate predefined and existing custom sensitive data. For more information, see Test sensitive data.

For testing violations in policy templates, you can upload a file that contains sample violations and check the file to determine if the defined rules are working as desired. Instant evaluation saves you time and effort.

Similarly, you can also validate predefined and existing custom templates. For more information, see Test template rules.

#### Support to test violations on multiple files for policy templates in inSync Compliance

While defining a rule in policy templates, now you can test violations in multiple files that contain sample violations to determine if the defined rules are working as expected. Instant evaluation saves you time and effort. You can validate both predefined and existing custom templates.
For more information, see Test template rules.

## Platform enhancements

### Automated User Management using SCIM

Druva announces the availability of Automated User Management using Secure Cross Identity Management (SCIM) 2.0.

As organizations adopt SaaS applications (like O365, GSuite, and so on) to address core business needs, Druva inSync simplifies the ability to manage application users with SCIM APIs. Additionally, by leveraging open standards-based approach Druva provides customers with flexibility and choice in IdP solutions and also reduces the complexity, risk, and time to manage users.

**Benefits of using SCIM in Druva inSync**

- Fully automated compared to a manual CSV-based user management
- Consistent user creation and management of users not in AD or LDAP
- Customers can leverage UPN in their IdP to identify and manage SaaS users

**Core capabilities:**

1. Complete cloud-based user management
2. Using open standards - SCIM 2.0
3. Simple configuration
4. Pre-built apps: Okta and Azure Active Directory Service through the respective marketplace

**Druva inSync certified IdP Apps**

Currently, Druva inSync certifies the following SCIM 2.0 compliant IdPs:

- Okta
- Microsoft Azure AD

Druva will provide certified solutions for other SCIM 2.0 compliant IdPs through its partnership program.

For more information, see Manage Users using SCIM.

**Change user provisioning from AD/LDAP to SCIM and vice-versa**

You also have the flexibility to change the user provisioning method from AD/LDAP to SCIM and vice versa, irrespective of the method chosen during the initial inSync configuration. With this flexibility, you can switch the user provisioning
method based on your organizational requirements, without any data loss.

For more information, see [About using SCIM for user management in Druva inSync](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Add co-branding in alert emails and customize support contact information**

You can now extend the existing co-branding settings to the Alert email notifications sent out to users. As a result, your users feel assured that the alert email notifications sent to them are from an authorized source.

We have also added more options to let inSync users contact your organization's support for any assistance.

The email sent to inSync users in case of configured alert events can now contain one of the following ways to contact your Internal Support:

- A web link that redirects to your Support Portal.
- An email address of the contact or support-alias to whom the users can send an email.
- A phone client with the phone number of your Support Center.

For configuration steps, see [Co-branding inSync](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Fixed Issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3932</td>
<td>Fixed the discrepancy in the Last Backup Status displayed under Users &gt; Devices tab and Device’s Backup Summary tab on the inSync Management Console.</td>
</tr>
<tr>
<td>3271</td>
<td>The Manage Users’ list page and the Manage Users’ &gt; &lt;User Name&gt; details page now displays the correct Cloud Apps device count.</td>
</tr>
<tr>
<td>3262</td>
<td>Enhanced the error message to correctly display the exact reason for the device authentication failure.</td>
</tr>
<tr>
<td>5020</td>
<td>inSync now supports backup of a SharePoint folder containing more than 5000 files or folders.</td>
</tr>
</tbody>
</table>

**inSync GovCloud Update on Nov 23, 2019**

**Enhancements**

The following enhancements are available with this Cloud update:

- [Platform Updates](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
- [Cloud Apps](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
**Platform Updates**

The following platform enhancements are available:

- Report subscription of non-administrators
- New alerts
- Enhanced user auto-deletion behavior for AD and LDAP

**Report subscription of non-administrators**

You can now give non-administrator users in your organization access to inSync reports. You can subscribe these users in inSync so that they receive periodic reports.

For more information, see [Reports](#).

**New alerts**

Druva has added the following alerts to inform inSync administrators about the inSync Connector and inSync CloudCache Server connection status so that they can take immediate actions:

- **AD Connection Status** - Alerts administrator if the inSync Connector is not connected to inSync Cloud.
- **Cache Server Connection Status** - Alerts administrator if the inSync CloudCache Server is not connected to inSync Cloud.
- **AD/LDAP Authentication Failure** - Alerts administrator if the credentials used to connect to inSync Connector are either invalid or expired.

For more information on the alerts and subscription settings, see [Alerts](#).

**Enhanced user auto-deletion behavior for AD and LDAP**

AD or LDAP managed users, which are preserved in the inSync Management Console are now auto-deleted as part of the AD/LDAP synchronization job instead of the auto-deletion job. The auto-deletion of preserved users is performed based on the **Data Preservation** settings defined in the profile associated with the user account in Druva inSync.

Earlier, inSync did not auto-delete eligible preserved users, which satisfied the Data Preservation criteria, but continued...
to exist in the AD and LDAP.

The users are now automatically deleted if the users are not part of any of the AD or LDAP mappings defined in Druva inSync and are preserved for the duration specified in the Data Preservation settings.

For more information, see Synchronize inSync users with your AD/LDAP.

Cloud Apps

The following Cloud App enhancements are available:

- Gmail In-Place restore support
- Exchange Online In-Place restore support
- Option to disable Box notifications
- Support for file deletion from Microsoft OneDrive and G-Drive
- Added support for Exchange Online Notes and Tasks
- Support for Cloud Apps file deletion using Search

Gmail In-Place restore support

Many of our customers have expressed their preference to restore the data directly to the Gmail account. With this update, Druva inSync users and administrators can now do just that - directly restore Gmail data back into their Gmail account.

The key benefits of this support include:

- **Better user experience**: inSync administrators and users can directly restore the data to their mailbox in the same hierarchy.
- **Unlimited retention and business continuity**: inSync administrators can restore data from any point in time and even from users who no longer have a Gmail account.
- **Recover from malicious attack or accidental deletion**: Quickly restore users’ data directly from a backup copy in case of accidental deletion or malicious activities.

For more information about Gmail In-Place restore, see [How to restore G Suite data?](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)

Exchange Online In-Place restore support

To have flexibility in selecting the data restore location, many customers prefer to restore the data directly to the

---

Updated: Fri, 24 Sep 2021 20:44:28 GMT
Exchange Online account. With this support, Druva inSync users and administrators can now directly restore Exchange Online data back into the user’s Exchange Online account.

Key benefits to the users and administrators include the following:

- **Better user experience**: inSync administrators and users can directly restore the data to their mailbox in the same hierarchy.

- **Unlimited retention and business continuity**: inSync administrators can restore data from any point in time and even from users who no longer have the Exchange Online account.

- **Recover from malicious attack or accidental deletion**: Quickly restore users’ data directly from a backup copy in case of accidental deletion or malicious activities.

As a Druva inSync administrator, you can now protect and recover Notes and Tasks within a user’s mailbox.

For more information about the Exchange Online in-place restore for inSync administrator, see [Restore Exchange Online data](#).

**Action required for existing Office 365 customers**

Existing customers, to utilize the In-Place restore feature for Exchange Online, inSync administrators must reconfigure the Exchange Online Org in the inSync Management Console. For instructions, see [Re-configure Office 365](#).

**Option to disable Box notifications**

Customers who have subscribed to Box notifications for data download activity in their account, receive email notifications even when Druva inSync downloads the user’s data as part of the scheduled or manually triggered data backup activity.

With this enhancement, customers who do not intend to receive these email notifications can now opt to stop receiving email notifications from Box when Druva inSync performs a data backup activity.

**Action required for existing Box customers**

For existing customers, inSync administrators must contact Druva Support to enable this feature, and then reconfigure Box in the inSync Management Console.

For more information, see [Disable Box notifications](#).

**Support for file deletion from Microsoft OneDrive and G-Drive**

inSync administrators can now directly delete a non-compliant file residing on the end user’s Cloud Apps account. With this support, the Proactive Compliance capability provides complete 360-degree protection against non-compliant files.

For more information, see [How do I resolve a compliance violation?](#)
Customer action required: None

Added support for Exchange Online Notes and Tasks

We have introduced this support to help you:

- **Expand the reach of your protected data with comprehensive Exchange Online data protection**: inSync administrators are now ensured that all the apps, namely Mail, Calendar, Contacts, Notes, and Tasks are protected within the O365 Exchange Online Cloud Application.

- **Unlimited retention and business continuity**: inSync administrators can retain Exchange Online Notes and Tasks data for an unlimited period. Recover Exchange Online Notes and Tasks data from any point in time snapshot.

- **Enable faster decision making with uninterrupted and secure access to data**: Recover quickly from malicious attack or accidental deletion and restore users’ data directly from a backup copy in case of accidental deletion or malicious activities.

For more information, see [Configure inSync for Exchange Online](#).

**Action required by existing Office 365 customers:**

To start protecting Exchange Online Tasks, you must reconfigure the Office 365 app in the inSync Management Console. For more information, see [Reconfigure Office 365](#).

**Note**: Exchange Online Notes are protected as a part of Mails which is why you don’t need to take any action to be able to protect Notes.

Support for Cloud Apps file deletion using Search

inSync administrators can now search and delete non-compliant files from both, data source and snapshot from the following Cloud Apps configured in Druva inSync:

- Microsoft OneDrive
- G-Drive
- Box

For more information, see [How to search backed up files](#).

Compliance

The following Compliance enhancements are available:

---

*https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud*

Updated: Fri, 24 Sep 2021 20:44:28 GMT

Powered by 52
• Support for whitelisting keywords in violations

• UI update - New inSync compliance user interface

• Changes in scanning frequency for violations

• Preview violations for sensitive data

Support for whitelisting keywords in violations

To reduce the effort and time required to manage compliance violations, inSync Compliance administrators can now whitelist specific keywords that are not treated as compliance violations in their organization.

For more information, see Modify Compliance Settings.

UI Update - New inSync Compliance User Interface (UI)

To enhance the customer experience in the categorization of compliance data, Druva has made the following updates to the inSync Compliance UI:

• A new simplified view of the Compliance dashboard, file violations, and email violations.
  • Simplified navigation with tabs to view file and email violations categorized in Active, Resolved, and Quarantined states.
  • Enhanced filters to view violations based on the type of compliance policy.
  • Visual aid to quickly identify critical violations and users who are on Legal Hold.

For detailed UI changes, see Enhanced inSync Compliance experience.

Changes in scanning frequency for violations

Druva has updated the scanning frequency for violations in inSync Compliance to once a day instead of scanning it after every backup. inSync now scans the latest version of a file or email available in the day and reports the violations.

This change in the scanning behavior reduces overhead on the Compliance administrators by requiring them to take action only on the latest version of a file or email backed up per day. For more information, see About inSync Compliance.

Preview violations for sensitive data

inSync Compliance administrators can now see a preview of the violations reported for the sensitive data. The violated content is highlighted in bold to help you quickly view and locate the violation. By default, Druva inSync shows the preview of three occurrences of the violated text and gives you the option to view up to 15 such occurrences.
For more information, see Compliance page.

**Governance**

The following Governance enhancements are available:

- **Search 2.0**
- **Enterprise search is now called federated search**
- **Check the indexing progress**

**Important:**
- The **Federated Search** capabilities and the **Indexing Status indicator** enhancement are available to customers who on-boarded after July 13, 2019, with the inSync Elite Plus and Elite as licensed editions.
- For our existing customers, we will introduce **Federated Search** over the next few months. Druva will keep existing customers posted about the plan.

**Search 2.0**

Search 2.0 provides security, legal, and forensic administrators with enhanced forensic investigative capabilities. This helps extend inSync Search beyond the traditional keyword-based search.

Security, Legal, and Forensic teams using inSync can use Search 2.0 in the following use cases:

- HR and Legal teams can investigate files and emails sent out by custodians to their personal email ID.

- Security teams can search for files based on SHA1 value. This is ideal for identifying malware and ransomware files.

- Forensic investigation teams can search by identifying files edited or email sent by a custodian during an investigative window.

- Backup administrators can use search to find specific large file types (example, PST files) stored on an employee’s endpoint in case a user has reached its quota.

The following capabilities are also available with Search 2.0:

- Search using one or more emails or file metadata. Providing a file name or email subject is no longer necessary.

- Search files stored on Sharepoint Online sites

- Extended metadata support to search for files and emails
Search 2.0 will be enabled for customers who are on-boarded after June 08, 2019 with inSync Elite Plus and Elite as licensed editions.

Existing customers will be seamlessly migrated to Search 2.0 over the next few months.

To know the availability of Search 2.0 in other regions and for more information see Search 2.0. For any queries, contact Druva Support.

**Enterprise Search is now called Federated Search**

The Enterprise Search that we offer is much more than the traditional keyword-based search. You name it and we got it covered; Security, Legal, and Forensic teams with enhanced forensic investigative capabilities. This is why to communicate the effective use of the search functionality and deliver better value, we have renamed Enterprise Search to Federated Search.

For more information, see Introducing Federated Search.

Customer action required: None
Check the Indexing Progress

You can now view indexing progress on the **Governance > Federated Search** page. This is a one-time activity and is displayed only when inSync starts indexing the backed up data. You get to check all these details for complete visibility of the data indexing:

- The number of data sources that inSync has indexed out of the total number of available data sources.
- Time remaining to index the remaining data sources.
- The number of data sources indexed out of the total number of available data sources for each data source type.

For more information, see [Federated Search for backed up data](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Customer action required:** None

### inSync Client

- [Support for macOS Catalina](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)
- [Prevent unauthorized uninstallation of inSync Client](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)

### Support for macOS Catalina
The inSync Client v6.2.0 now supports macOS 10.15 Catalina. For details on prerequisites for installation, see hardware and software requirements.

Prevent unauthorized uninstallation of inSync Client

To better help inSync administrators secure the information on devices and reduce the risk of data loss, administrators can prevent end-users from uninstalling inSync Client from their Windows devices. Administrators can configure this setting during the inSync Client installation, whereby, inSync Client won’t be listed in the Windows Search and Add or Remove Programs list. For more information, see Prohibit users from uninstalling inSync Client on Windows devices.

Note: Support for this feature is available with inSync Client v6.2.0.

UX Enhancements

- Enhanced restore overview page
- Enhanced manage alerts page
- Enhanced live activities page

Enhanced Restore Overview Page

We have added the Restore Activity tab on the Restore Overview page to give you a view of all the restore jobs triggered in the past 60 days.
We have also introduced a restore details pop-up that displays the status of the restore job, size of the data, and the number of files missing from the restore.

The enhancement helps you get:

- A quick overview of all the restore jobs across the organization.
- Quick access to the user and device details right from the restore overview page.
- A quick glance of the restore jobs status.

For more information, see Manage Alerts.

For more information, see Restore overview page.

**Enhanced Manage Alerts page**

inSync administrators can now quickly access the alert source like users, Cloud Apps, CloudCache Server, and inSync Connector by clicking the source name listed under the **Sources** column on the Manage Alerts page.

The alerts reduce time to resolution for inSync administrators with visibility of the source and eliminate multiple steps in the inSync Management Console to identify and resolve the issue.

**Enhanced Live Activities page**

We have added filters on the Live Activities page to help you monitor specific activities that satisfy the filter criteria. The new filters are as follows:
• **Activity types**: View live activities based on the type of activity such as ongoing backup activities, ongoing restore activities, or view all the ongoing activities.

• **Data sources**: View live activities for only specific data sources like devices or Cloud Apps like Exchange Online, or OneDrive, and so on.

• **Profiles**: View on-going live activities only for specific profiles.

inSync administrators can use a combination of the filters to view the required live activities and take appropriate actions. For more information, see [Live Activities](#).

**Fixed Issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>43530</td>
<td>Improved the administrative activity logging experience to capture details about modifications made to Active Directory (AD) configuration.</td>
</tr>
<tr>
<td>49453</td>
<td>inSync Client auto-upgrade page now displays the latest version of the inSync Client available for auto-upgrade.</td>
</tr>
<tr>
<td>51833</td>
<td>Fixed the discrepancy between statistics displayed on the Data Activity Trend tab on the Manage Device page for a snapshot and the Unusual Data Activity snapshot logs downloaded from the inSync Management Console.</td>
</tr>
<tr>
<td>52812</td>
<td>inSync Cloud administrators were displayed 'Second cloud administrator not configured' prompt even when the second Cloud administrator was already created in the inSync Management Console.</td>
</tr>
<tr>
<td>54203</td>
<td>Fixed behavior where Exchange Online backups failed with Error: Internal Error. Backup failing for the same device with Malformed JSON error.</td>
</tr>
</tbody>
</table>

**inSync GovCloud Update on July 20, 2019**

https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud

Updated: Fri, 24 Sep 2021 20:44:28 GMT

Powered by
inSync Client for GovCloud v6.2.0

Druva is happy to announce the availability of inSync Client for Cloud v6.2.0, which offers the following features:

- Automatic proxy detection support through DHCP
- Request user permission for full disk access on macOS Mojave

For more information, see Release Notes for inSync Client v6.2.0.

To auto-upgrade inSync Client to the latest version, see Auto-upgrade inSync Client.

inSync GovCloud Enhancements

The following enhancements and fixed issues are available with this GovCloud update:

**Google Drive native restore support**

Druva inSync users and administrators can now directly restore Google Drive data back into Google Drive account.

Key benefits to users and administrators include the following:

- **Reduce network costs**: As the data is directly restored, the data does not have to traverse your organization's network.

- **Better user experience**: inSync administrators and users no longer have to download the data on to their device before uploading it back to Google Drive.

- **Reduce risk**: While in most cases inSync administrators or users might choose to replace the data directly, they also have the choice to restore the data as a copy. This helps avoid the chances of overwriting an existing version.

- **Unlimited retention and business continuity**: inSync administrators can restore data from any point in time and even from users who no longer have a G Suite account.

- **Recover from malicious attack or accidental deletion**: Quickly restore users’ data directly from a backup copy in case of accidental deletion or malicious activities.

For more information about the Google Drive native restore for inSync administrator, see How to restore G Suite data?

**Action required for existing G Suite customers**

For existing inSync G Suite customers, to utilize the native restore feature for Google Drive, inSync administrators must reconfigure the G Suite Org in the inSync Management Console. For instructions, see Re-configure G Suite.

**Announcing a new version of inSync Connector - v6.1.1**

The new version of inSync Connector v6.1.1 supports proxy configuration through the Web Proxy Autodiscovery
Changes to inSync Compliance policy templates and sensitive data

Druva has upgraded all the inSync Compliance policies that used the predefined templates and sensitive data types that were deprecated in October 2018 with the newly introduced predefined templates and sensitive data types. The new predefined compliance templates and sensitive data benefits the inSync Elite Plus customers as they are stronger and more accurate at identifying Credit Card and HIPAA sensitive data violations.

For more information about this update, see Changes in inSync Compliance policy templates and sensitive data.

Enterprise Search is now Federated Search

The Enterprise Search that we offer is much more than the traditional keyword-based search. You name it and we got it covered; Security, Legal, and Forensic teams with enhanced forensic investigative capabilities. Which is why to communicate the effective use of the search functionality and deliver better value, we have renamed Enterprise Search to Federated Search.

Customer action required: None.

Known Issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1375</td>
<td>The Cloud Status section on the Druva Cloud Platform Dashboard does not display the inSync GovCloud status. The inSync GovCloud storage location and its functional state can be checked <a href="https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud">here</a></td>
</tr>
</tbody>
</table>

Fixed Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>51737</td>
<td>File deletion failed with 'Internal Error' when trying to resolve a compliance violation by deleting the file.</td>
</tr>
<tr>
<td>51502</td>
<td>During deployment, incorrect device count was displayed for users on the Users page.</td>
</tr>
<tr>
<td>51494</td>
<td>OneDrive restores failed with &quot;Failed to establish a new connection: [Errno -2] Name or service not known&quot; error if inSync administrators did not have OneDrive license enabled for their account.</td>
</tr>
<tr>
<td>47845</td>
<td>Import and activation of inSync users failed with 'Could not find matching AD Mappings for user' error when</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>using Integrated Mass Deployment (IMD).</td>
</tr>
<tr>
<td>51009</td>
<td>Users were auto-preserved after upgrading inSync Connector.</td>
</tr>
<tr>
<td>51090</td>
<td>Fixed pagination issue with the SharePoint Online site collection page.</td>
</tr>
</tbody>
</table>

**inSync GovCloud Update on Feb 02, 2019**

The following enhancements and fixed issues are available with this GovCloud update:

**Enhancements**

**Cloud Apps: Increase in retention period for emails**

Druva has increased the limit to retain emails backed up from a Cloud App account from 100 months to 250 months. By default, inSync retains the emails for 84 months. As an inSync administrator, you can increase the limit to 250 months if your organization requires longer data retention. This enhancement benefits customers in highly regulated industries such as the construction industry, where they need to retain data of the preserved users for longer periods of time.

To update the retention settings for emails, see [Configure the backup retention policy](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Enhanced inSync Management Console menu bar**

Druva has enhanced the inSync Management Console menu bar to provide a seamless experience to the Druva administrators who manage different Druva products. Few options on the menu bar are reorganized and realigned for consistency. Here is a quick look at the update:
Fixed Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>
| 50513 and 50512 | Exchange Online and other Cloud Apps backup intermittently failed with the error - Internal Error!!.
Please check logs for details. |
| 49120     | Subscribed alert notifications were not sent to the customers and AD/LDAP sync did not happen as per the defined schedule. |

inSync GovCloud Update on Jan 19, 2019

The following enhancements and fixed issues are available with this GovCloud update:

Enhancements

**Cloud Key Management for Cloud Apps**

Druva is pleased to introduce the integration with the highly secure and FIPS 140-2 validated AWS Key Management Service (KMS) for the data protection of the cloud applications namely Office 365, Box, and G-Suite. This feature offers the key management web service and thus eliminates the need to deploy the inSync Connector within the premise for cloud applications. For more information, see Configure Cloud Key Management for Cloud Apps.

**Support for Recoverable Items folder in Exchange Online**

inSync administrators can now configure the Recoverable Items folder in Exchange Online for backup and protect the data that is accidentally deleted or removed due to malicious programs or unauthorized activities. To configure the Recoverable Items folder for backup, see How to back up Office 365 data?

**Enterprise Search enhancements**

Druva has made the following enhancements to Enterprise Search:

- **Enhanced user interface**
  Druva is pleased to offer a new and intuitive user interface (UI) for Enterprise Search. The key enhancements are as follows:
  - Filters and search actions (such as Download and Load more) are now more prominent.
  - Filter option to narrow down search results by using the username or email address of users.
  - Real-time updates on search progress and search results.
    To learn more about the enhancements, see Enhanced inSync Enterprise Search experience.

- **Enterprise Search for Legal administrators**
  Legal administrators now have access to Enterprise Search to search, view, and download files and emails.
associated with legal holds and custodians (users). Enterprise Search reduces the time and effort it takes for Legal administrators to access the relevant data without having to depend on Cloud administrators. For more information, see Enterprise Search for Legal administrators.

**Proactive Compliance enhancements**

**Define complex sensitive data rule types and violation life cycles**

**Use regular expressions to identify sensitive data**
inSync administrators can now use regular expressions to define keywords that violate sensitive data policies of the organization. For more information, see Manage sensitive data.

**Define search behavior to find violated files and emails using keywords**
inSync administrators can choose if inSync should flag a violation if any of the keyword or sensitive data type is found in a document, or only if all the keywords or sensitive data types are found in a document. For more information, see Manage policy template.

**Define schedules to manage violation lifecycles automatically**
inSync administrators can now define a schedule to automatically resolve violations and archive resolved violations. For more information, see Modify Compliance Settings.

**New administrator role, rights, and new reports**

**New Compliance administrator role and rights**
inSync Cloud administrator can now create a new Compliance administrator who, by default, has access to all inSync Compliance features. Cloud administrators can assign Proactive Compliance rights to other inSync administrators allowing them to perform the following actions:

- View violations and compliance settings
- Manage violations
- Manage compliance settings
- Download backup and share data

For more information, see Create a Compliance administrator.

**New reports to view the archived, non-compliance data**

The following new reports help administrators to view the violations based on the keywords for a specific period.

- **Archived Non-Compliance File Report** - This report provides information on archived violations reported for non-compliant files. For more information, see Archived Non-Compliance File Report.
- **Archived Non-Compliance Email Report** - This report provides information on archived violations reported for non-compliant emails. For more information, see Archived Non-Compliance Email Report.

**Enhanced behavior for auto-deletion of inactive devices**
Druva has enhanced the algorithm that is used to auto-delete inactive devices. inSync now deletes a maximum of 500 devices per day.

The following rules now apply during the inactive device deletion process:

1. If the total number of devices marked for deletion is greater than 500, inSync will delete 500 devices in one day, and the remaining devices will be queued up for auto-deletion on the next day.
2. If the total number of devices marked for deletion for the day is less than or equal to 500, then all the marked devices are deleted.

For more information, see Configure auto-delete of inactive devices in a profile.

Enhanced inSync Client Restore User Interface

Druva is pleased to offer a new and intuitive User Interface (UI) for the data restore activity performed using the inSync Client. The new UI is available to users of inSync Client version 6.0.1 and later.

The key enhancements are as follows:

- **Snapshot listing**
  Enhanced Snapshots selection window that groups and displays all the available snapshots based on date and time.

- **Files and folder listing**
  Enhanced tree view that lists the folders, sub-folders, and files, to quickly browse and select for restore.

- **Search results window**
  Enables the selection of multiple files and folders for restore.

- **Select custom location**
  Quickly browse and select a custom location on the device to restore the data.

To learn more about the enhancements, see inSync Client Restore User Interface Enhancements.

Fixed Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>48684</td>
<td>The User Details page (accessed using Users &gt; {User name}) in the inSync Management Console is now improved to load faster to display user information.</td>
</tr>
<tr>
<td>49925</td>
<td>Subscribed inSync reports were not sent as per the defined schedule.</td>
</tr>
<tr>
<td>40491</td>
<td>inSync administrators were not able to download or restore files and folders using Internet Explorer in case the URL length of the selected path for restore was more than 2048 characters.</td>
</tr>
<tr>
<td>45533</td>
<td>Password expiry log was added to inSync logs even though the Password policy was not enabled in inSync.</td>
</tr>
<tr>
<td>49185</td>
<td>Snapshots were not listed in the SharePoint site restore view in the inSync Management Console.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>50342</td>
<td>Office 365: Exchange Online backup failed for users.</td>
</tr>
<tr>
<td></td>
<td>While restoring folders and files with the same name from a parent folder to the desktop or a custom location, inSync overwrote the folders and files with the same name and displayed only the last restored folder and file.</td>
</tr>
</tbody>
</table>

### Known Issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>49566</td>
<td>inSync displays incorrect file path in the Restore window for files backed up using the inSync Android app.</td>
</tr>
</tbody>
</table>

### Alert! - End of Support for inSync Client v5.9.5

inSync Client v5.9.5 for Windows and macOS will reach its End of Support on January 01, 2019. Druva recommends its customers to upgrade the inSync Client on user devices to the latest version. For more information, see [inSync Cloud support and EOL policies](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

### inSync GovCloud Update on Dec 15, 2018

The following enhancements and fixed issues are available with this GovCloud update:

#### Enhancements

**Enhanced Live Activity page for Cloud Apps Activities**

inSync administrators can now see the real-time progress and status of the on-going scheduled and manually triggered backup activities for a configured Cloud App. inSync administrators can click on the Status column of an on-going Cloud App activity to view information like the actual number of files backed up, progress of the backup activity, and other details such as the actual path being backed up and status of the activity. For more information, see [Live Activities page](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Changes to Backup Interval for Cloud Apps**

To alleviate the backup issues, observed primarily due to Microsoft throttling API calls across regions, Druva is implementing changes in the backup intervals for Cloud Applications that will allow inSync to avoid and recover from throttling scenarios. For more information, see [Define the backup interval for Cloud Apps](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

### Custom Domain Support for Office 365 and G Suite

[id download]
inSync now provides the capability to manage custom domains associated with different applications such as O365 and G Suite. inSync administrators who manage different domains for separate cloud applications such as O365 and G Suite can now define a custom domain for a cloud application and protect a user's data within each of the domain across applications. For more information, see Configure the User Custom Domain for Office 365 and G Suite.

**Office 365 - Support for Contact Notes in Exchange Online**

Druva inSync now automatically backs up the 'Notes' created for a Contact in Exchange Online.

**Office 365 - Improved Performance for SharePoint Online Restore Activities**

inSync administrators can now experience faster restore of the SharePoint Online data. Druva has optimized its restore mechanism for SharePoint Online, which automatically prioritizes the restore activities triggered by inSync administrators.

**Changes to inSync Compliance policy templates and sensitive data**

Druva has changed some of the predefined inSync Compliance policy templates and sensitive data types with this cloud update. inSync Elite Plus customers will benefit from the updated predefined compliance templates and sensitive data as they are stronger and more accurate at identifying Credit Card and HIPAA sensitive data violations. With these changes, inSync ensures that administrators continue to have full visibility of risks associated with the end-user data in an accurate and transparent manner. For detailed information about the changes, see Changes in inSync Compliance policy templates and sensitive data.

**inSync Compliance for Archive File Types**

inSync administrators can now utilize inSync Compliance to monitor usage of any regulated or sensitive data within the .zip and .tar file types. This enables inSync administrators to gain full visibility of risks associated with end-user data in the archive file types. For more information, see Enable scanning of Archive Files for violations.

**Enhanced inSync Direct Download utility for Mac OS**

inSync Direct Download utility for Mac OS is now enhanced to set the birth time of a file. When downloading a file using the inSync Direct Download utility, inSync sets the birth time of the file to the file creation time in the user time zone.

**Enhanced Reports**

Druva has updated the following inSync reports to include information on inSync Client upgrade status and Operating System (OS) details.

- **User Rollout report** is enhanced to include the following information for a device:
  - inSync Client version
• Upgraded on
• Upgrade state
• OS Platform
• Device OS

For more information, see User Rollout report.

• Last Backup Status report is enhanced to include the following information for a device:
  ◦ OS Platform
  ◦ Device OS

For more information, see Last Backup Status report.

Download of data in the applicable Archive Format

When an administrator or a user downloads data, inSync now automatically detects the operating system and downloads the data in the appropriate archive format. On Mac OS, now the data is automatically downloaded in the .tar.gz or .tar archive format, and on the Windows OS, the data is downloaded in the .zip archive format.

Fixed Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>49199</td>
<td>inSync failed to back up multiple occurrences of a Calendar event as part of Exchange Online backup.</td>
</tr>
<tr>
<td>46576</td>
<td>inSync failed to honor the User Data Privacy settings and administrators had access to the user data even though the users had blocked access to their data.</td>
</tr>
<tr>
<td>48970</td>
<td>Exchange Online Backup failed with 'Backed Up with Errors'.</td>
</tr>
<tr>
<td>48919</td>
<td>inSync Restore Status alert email displayed an incorrect restore initiated date and time.</td>
</tr>
<tr>
<td>48352</td>
<td>Enhanced error message on the Restore UI when internet connectivity is lost while trying to restore the data.</td>
</tr>
<tr>
<td>47678</td>
<td>UI fixes to prevent insertion of bad characters.</td>
</tr>
</tbody>
</table>

Optimized the job that was causing the following issues:

48254
  • AD/LDAP sync process was not running as per the schedule.
  • Subscribed inSync reports were not sent as per the schedule.
  • Alert notifications for restore activities were delayed to inSync administrators.

48658 | inSync administrators experienced failure of Gmail backups and observed the errors 404 and 429. |
<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>47866</td>
<td>UI fixes for inSync Client automatic upgrade process in the inSync Management Console.</td>
</tr>
<tr>
<td>47976</td>
<td>Improvements to SharePoint Online logs and Activity Stream table.</td>
</tr>
<tr>
<td>48036</td>
<td>UI fixes for Restore window in the inSync Management Console and inSync Web Console to seamlessly list a large number of snapshots for a user.</td>
</tr>
<tr>
<td>48663</td>
<td>inSync restored two versions of the same file when inSync administrators tried restoring the SharePoint Online site data using the 'In-Place Restore' option.</td>
</tr>
<tr>
<td>48796</td>
<td>inSync's compaction process failed to remove the expired snapshots as per the defined retention period.</td>
</tr>
<tr>
<td>48567</td>
<td>inSync Client backup activity failed with error: Internal error. (#100000001).</td>
</tr>
<tr>
<td>48123</td>
<td>inSync failed to honor the pre-defined daily download limit set for inSync Client auto-upgrade.</td>
</tr>
<tr>
<td>48944</td>
<td>inSync failed to backup OneNote files in OneDrive.</td>
</tr>
</tbody>
</table>

**Alert! - End of Life for inSync Client v5.9**

inSync Client v5.9 for Windows and macOS will reach its End of Life on December 01, 2018. Druva recommends its customers to upgrade the inSync Client on user devices to the latest version. For more information, see [inSync Cloud support and EOL policies](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud).

**Important**

Druva will continue to support the inSync Client v5.9 for Linux OS.

**inSync GovCloud Update on Nov 17, 2018**

The following enhancements are available with this GovCloud update:

**Enhancements**

**inSync Elite Plus edition is now available for GovCloud customers**

inSync Elite Plus edition offers the following add-on features, that offer you complete data protection with information governance:

- **Automated Compliance Monitoring** - Proactive Compliance enables enterprises to automate the tracking, monitoring and risk-alerting of regulated or policy managed data, and allows IT administrators to assess and act.
upon data risks across data sources. For more information, see About inSync Compliance.

- **Defensible Deletion** - Defensible deletion enables the deletion of files from data sources and snapshots, for removal of sensitive and malware-infected files. For more information, see Delete files.

- **Unusual Data Activity** - Unusual Data Activity monitors for abnormal file creations, updates, and deletions for the early detection and recovery against ransomware. inSync provides you Unusual Data Activity report that flags and lists the devices or Cloud App accounts for anomalous behavior. For more information, see Unusual data activity.

To upgrade, contact your Druva Sales representative or Druva Support.

### inSync GovCloud Update on Sept 29, 2018

**inSync Client v6.1.1 for GovCloud**

Druva is excited to announce the release of inSync Client v6.1.1 for GovCloud. inSync Client v6.1.1 is a patch release over the previous version - v6.1.0.

inSync Client v6.1.1 includes the following enhancements:

- For MacOS
  - inSync Client v6.1.1 supports macOS Mojave (version 10.14).
  - Support for the new user data protection feature introduced in macOS Mojave. It allows inSync Client users to provide access to protected locations for backup and restore. To learn more about the actions that inSync administrators and inSync Client users need to take, see inSync Client changes for macOS Mojave (version 10.14).
  - Adherence to the Quality of Service (QoS) guidelines for Mac. This makes macOS Mojave remain more responsive and efficient.
  - Improvements to CPU performance during the backup estimation phase for the first backup as well as incremental backups.

  **Important** Druva recommends that you upgrade the inSync Client to v6.1.1 before upgrading user devices to macOS Mojave.

- For Windows OS
  - inSync Client v6.1.1 contains minor improvements and bug fixes.

inSync administrators can opt to upgrade the inSync Clients to version 6.1.1 using either manual upgrade, bulk upgrade, or auto upgrade. To upgrade inSync Client on end-user devices, see inSync Client Upgrade.

For inSync Client updates, see Release Notes for inSync Client 6.1.1.
Updated inSync Client Support and EOL policy

Druva has updated the Support and EOL policy for inSync Client for Cloud as follows:

- **End-of-Support (EOS):** Druva ends all support for the inSync Client for Cloud versions that are more than 18 months old, and no patches are made available to customers. Auto upgrades will continue to work.
- **End-of-Life (EOL):** EOL for an inSync Client for Cloud version means an end to all technical assistance, auto-upgrades, and bug fixes for that version. The inSync Client for Cloud versions that are more than 24 months old may stop connecting to the inSync Cloud, and all backups and restores may be blocked.

For more information and to see the updated EOS and EOL dates for the version of inSync Client your organization is using, see inSync Cloud support and EOL policies.

Fixed Issues

The following issues are fixed on inSync GovCloud with this update:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>48567</td>
<td>inSync Client backup activity failed with error: Internal error. (#100000001).</td>
</tr>
<tr>
<td>47679</td>
<td>Backups failed with inSync Client running on Windows OS with the Creators Update 1803, wherein if the user has configured OneDrive or Sharepoint mapped folders for backup.</td>
</tr>
<tr>
<td>47589</td>
<td>On the Manage Alerts page, the Backup Stalled alert graph listed in the Top Alert Types section was misaligned.</td>
</tr>
<tr>
<td>47750</td>
<td>While backing up SharePoint Online, inSync skipped the sites, subsites, lists, and document libraries if a '/' (forward slash) character was present in the title.</td>
</tr>
</tbody>
</table>

inSync GovCloud Update on July 21, 2018

The following enhancements are available with this inSync GovCloud update:

- **Enhancements for inSync GovCloud administrators**
- **New inSync Client v6.1.0 and enhancements for inSync Client users**

Enhancements for inSync GovCloud administrators

**Important** The following enhancements work only with inSync Client v6.1.0 for inSync GovCloud.

**Integrated Mass Deployment v4 to replace devices at scale**

inSync now provides administrators an easy way to manage the device replace activity at scale using the Integrated
Mass Deployment version 4 (IMD v4) process.

For more information, see Bulk replace devices using Integrated Mass Deployment version 4.

**Regular Expressions support for endpoint devices**
inSync administrators can now exercise more control over what endpoint data is being backed up by leveraging regular expressions (regex-based) exclusions for endpoint devices.

For more information, see Excluding files and folders using regular expressions.

**Quick Configuration of My Pictures, My Music, and My Videos through Profile**
inSync administrators can now quickly configure My Pictures, My Music, and My Videos folders for backup on Windows devices from **inSync Management Console > Profiles**.

For more information, see Configure folders for backup.

**Enhanced configuration to restrict inSync activities on VPNs**
inSync administrators can now block inSync backup and restore activities on VPNs by specifying the actual adapter name or device name.

For more information, see Restrict data networks for device backups.

**Enhancements for inSync Client users**

**New and enhanced inSync Client v6.1.0 for GovCloud**

Druva is excited to announce the release of the inSync Client v6.1.0. Druva is committed to making inSync accessible to all individuals. This includes making the inSync Client navigable using the keyboard and adding support for assistive technology like screen readers. Beginning with inSync Client v6.1.0, Druva follows the internationally recognized standards in Section 508 of the Rehabilitation Act and the Web Content Accessibility Guidelines (WCAG) 2.0 to the extent possible.

With the new inSync Client, Druva also introduces a simplified, intuitive Client interface, redesigned workflows to activate a device, add or replace a device, and other improvements as described below, which make the end user's experience seamless and easy. Labels, messages, and instructions across the interface have been simplified for a better and consistent experience. The updated interface aligns with the standards used across inSync Management Console to provide a simplified and consistent experience to the end users and administrators alike.

inSync Client v6.1.0 is available for devices running on Windows and Mac OS.

You can opt to upgrade the inSync Clients to v6.1.0 using either manual upgrade, bulk upgrade, or auto upgrade. To
upgrade inSync Client on end-user devices, see inSync Client Upgrade.

Improved inSync Client User Interface experience

The new inSync Client user interface has been improved to provide end users with an intuitive data protection and restore experience with simplified workflows and consistent labels and messages across the interface.

Simplified Activation workflow

The simplified and enhanced inSync Client Activation workflow helps the end user to quickly get through the activation process and configure the device easily as shown in the following illustration.

inSync Client Activation Screen

![inSync Client Activation Screen](https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud)

Improved Add and Replace device workflow

The improved Add or Replace devices workflow displays a more streamlined interface, where complex steps and technical labels have been replaced with easy to understand labels and instructions. The new inSync Client interface provides a re-designed and simplified workflow to enable the user to add or replace a device easily as shown in the following illustration.
Add or Replace Device Workflows

Configure "ERNIE'S MACBOOK PRO" for Backup

Add as New Device

Replace an Existing Device

You have 1 device already configured for Backup
**Intuitive Backup summary**

The inSync Client user interface displays **Backup** and **Restore** on the same screen, making it a user-friendly experience for end users to easily find the actions they need to perform to back up their data or restore content. Folder names displayed under **Backup Content** have been made more intuitive and labels and messages across the interface have been simplified.

The following illustration displays these changes as seen on inSync Client.

**Backup Summary**
Updated Restore workflow

The *Restore* window now displays the recent snapshot instead of the entire snapshot listing. If required, the user can select the previous snapshots from the drop-down list. Also, the search capability has been moved to the center of the *Restore* window to allow users to search through devices and snapshots quickly.

The following illustration displays the latest snapshot details on the *Restore* screen.

**Restore screen**

<table>
<thead>
<tr>
<th>Name</th>
<th>Flies</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Desktop</td>
<td>108</td>
<td>41.76 MB</td>
</tr>
<tr>
<td>Documents</td>
<td>2267</td>
<td>383.46 MB</td>
</tr>
<tr>
<td>Desktop1</td>
<td>1</td>
<td>16.82 KB</td>
</tr>
<tr>
<td>Images</td>
<td>18</td>
<td>752.86 KB</td>
</tr>
</tbody>
</table>

```
3394  425.98 MB
```
Enhanced Settings screen

In the inSync Client, the pop-up windows on the Settings screen have been updated and designed to give a seamless experience. The following illustration displays the Proxy Settings pop up window.

Proxy settings screen
Improved display of folder names

On the inSync Client, users can now see the actual folder names on the Backup Content and Restore Snapshot screens, instead of the system path variables that are defined by the administrators in the inSync Management Console.
Fixed issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>43814</td>
<td>inSync Client displayed misconfigured folder alerts for Microsoft Office applications that were not installed on the user device.</td>
</tr>
<tr>
<td>46608</td>
<td>On a Windows device, the restore window opened behind the inSync Client window.</td>
</tr>
<tr>
<td>45746</td>
<td>The smart menu option on Mac OS High Sierra devices did not display icons for initializing backup, backup in progress, and finishing backup.</td>
</tr>
<tr>
<td>46292</td>
<td>In selective sync, inSync did not sync the contents of the parent folder if all of its sub-folders were deselected or removed from sync and share.</td>
</tr>
<tr>
<td>46760</td>
<td>If a user had not completed the first backup on all the user's devices that were configured for backup, snapshots of the backed up devices were not available for restore on the devices that were not backed up.</td>
</tr>
</tbody>
</table>
| 47489 | inSync Client for Windows OS fails to launch and displays a Java Exception error when it is installed by a

https://docs.druva.com/Endpoints/010_Release_Details/Archived_inSync_Release_Notes_-_GovCloud
Updated: Fri, 24 Sep 2021 20:44:28 GMT
Powered by
standard user, whose username contains a Unicode character.

Backups failed with inSync Client running on Windows OS with the Creators Update 1803, wherein if the user has configured OneDrive or Sharepoint mapped folders for backup.

Known issues and workarounds

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>45517</td>
<td>After the system administrator uninstalls the inSync Client from the Mac OS and manually deletes all inSync folders, the operating system continues to display the inSync folders for the Mac user.</td>
</tr>
</tbody>
</table>

All Backup Status messages do not get translated when the language is changed.

46425

**Workaround:** The Backup Status messages are successfully displayed in the selected language after the backup cycle.

Revision Information

<table>
<thead>
<tr>
<th>Product</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>inSync Client</td>
<td></td>
</tr>
<tr>
<td>Windows:</td>
<td>r69845</td>
</tr>
<tr>
<td>Mac:</td>
<td>r69845</td>
</tr>
</tbody>
</table>

**Important:** Druva has not released a new version of inSync Client for Linux OS with this inSync GovCloud update.

For more information, contact Druva Support.

inSync GovCloud Update on July 07, 2018

The following enhancements are available with the inSync GovCloud update on July 07, 2018:
Enhancements

**Improved inSync Client upgrade process**

inSync now enables its administrators to automatically run the inSync Client upgrade process for all devices that need an upgrade. Devices that are scheduled for an upgrade will be automatically upgraded to the latest version in the upgrade cycle that starts at 10:00 am UTC every day.

For more information, see [Upgrade the inSync Client on the user's device](#).

**Capability to identify and manage devices with the same hostname**

inSync now uses the device UUID and Serial Number as the unique identifier to identify and manage devices. This method of device identification ensures that the user devices with the same hostname are not deactivated or replaced while using IMD for deploying inSync Clients.

For more information, see [Allow users to activate inSync when device host name is same](#).

**Capability to exclude Network Drive from backup**

In addition to Windows devices, inSync administrators can now configure inSync to exclude network drives from backup on Mac devices, too. This capability is useful in cases where you do not want to backup network share folders.

For more information, see [Exclude Network Drive from backup](#).

**Restrict inSync administrators from downloading User Authkeys**

inSync now restricts administrators from downloading authentication keys for a user who has Data Privacy settings enabled. Administrators can no longer download User Authkeys and use it to activate inSync Client or access the data of users who have Data Privacy settings enabled.

**Modify LDAP mapping**

inSync administrators can now update the Filter Users criteria, which is used to filter and import users from the registered LDAP.

Based on the updated criteria:

- New inSync user accounts are created for the imported users.
- Existing inSync user accounts which do not belong to any LDAP mapping are preserved.

For more information, see [Modify an LDAP Mapping](#).

**Auto delete inactive devices option**

The option to auto delete inactive devices is now GA and available to all the customers.
inSync provides administrators the option to manage inactive devices through the inSync Management Console to:

- Define the period after which inSync will mark a device as inactive.
- Select the option to automatically delete inactive devices in a profile. For more information, see Configure auto-delete of inactive devices in a profile.
- Specify the number of days after which inSync will delete the inactive devices.
- View a consolidated report of inactive devices and their respective deletion date. For more information, see Inactive Devices Report.

**Updates to SharePoint Online**

- **Auto-discovery of Site Collections**
  inSync now provides the option to automatically discover new site collections added to the SharePoint Online setup of an organization. Office 365 administrators will no longer have to discover SharePoint site collections manually. The discovery process runs once every 24 hours. This setting is enabled by default.

- **Support for Team Sites**
  inSync now supports backup and restore for Team Sites that are used by Office 365 Groups and Teams Web App within an Office 365 tenant. These sites are generally hidden from an IT administrator and as a result are missed out from the backup. The auto-discovery process ensures that these hidden sites are added to the SharePoint sites list in inSync. This support extends inSync's capability in protecting confidential and valuable business data present in Team Sites in SharePoint Online.

- **Global backup and data retention policies for Site Collections**
  Routine data backup for Sharepoint Online Site Collections is imperative for the business as crucial data is being saved during the collaboration between the employees of an organization. To protect this data, inSync now enables administrators to define global data backup and retention policies that apply to all Site Collections within Sharepoint Online. inSync administrators also have the option to define custom policies for a site collection.

- **Set unlimited retention period for SharePoint Online backups**
  Administrators can set the retention period to unlimited for the SharePoint Online backups.

For more information, see Configure SharePoint for backup and restore and How to manage SharePoint Online for Office 365?

**OneDrive native restore**

inSync administrators and inSync Client users can now restore the backed up OneDrive data directly into the OneDrive account.

The details are as follows:

- An inSync administrator can restore a OneDrive user's data by overwriting the data in the existing location or as a copy in a different location in the user's OneDrive account. An inSync administrator can also restore the data of a OneDrive user into the account of another OneDrive user as a copy, and choose to retain or discard the sharing settings for the restored data.
For more information, see How to restore Office 365 data?

• An inSync Client user can search and restore their OneDrive data in the same location by overwriting the existing data or restore the data as a copy in a different location of their OneDrive account.

For more information, see Restore data using the inSync Web.

UTF-8 support on inSync GovCloud

inSync GovCloud now supports emojis, special characters, and other symbols that are based on UTF-8 Unicode-based character encoding.

Reports update

Druva has modified the date and time format in the HTML and CSV reports that you download from inSync Management Console. The format is changed from alphanumeric to numeric so that you can easily sort the report data by date and time.

inSync GovCloud Update on Mar 03, 2018

The following enhancements is available with the inSync 5.9.5 CU10, govcloud update:

Enhancement

Password workflow change

Adhering to the IA-5 guidelines for storing and transmitting user passwords, inSync GovCloud now mandates users and administrators to set their password during account activation. As a result of this change, inSync GovCloud users and administrators will no longer receive passwords in plain text format in their account invitation email. The account invitation email will now provide a link to set the password during account activation or password reset.

For more information, see:

• About the inSync Cloud invitation email
• About the inSync account activation email
• Reset the password for an administrator
• Reset the password for a user