Asigra Cloud Backup™ v14.2

Release Notes v1.7

April 2023

asigra

Table of contents

Release notes history

Version	Date	Summary
1.0	August 31, 2020	• Released for General Availability.

1.1	October 2, 2020	• Management Console users can now scan their Microsoft 365 (Exchange Online) files for malware during the backup and restore process. Requires Windows DS-Client v14.2.0.1 and Management Console v14.2.0.1 or later.
		• The following operating systems are now supported:
		  • CentOS 7.8, 8.2
		  • Red Hat Enterprise Linux 7.8, 8.2
		  • SUSE Linux Enterprise Server 12 SP5, 15 SP2

1.2	January 20, 2021	• Management Console users can now scan their Microsoft 365 (Groups and Teams) files for malware during the backup and restore process. Requires Windows DS-Client v14.2.0.2) and Management Console v14.2.0.2 or later.
		• Management Console users can now remotely manage DS-Clients without opening a port in the firewall on the DS-Client machine. Requires DS-Client v14.2.0.2, DS-System v14.2.0.2, and Management Console v14.2.0.2 or later.
		• Management Console users can now configure a process to run before and/or after a File system backup to perform actions when a condition is met. Requires Windows DS-Client v14.2.0.2 and Management Console v14.2.0.2 or later.
		• The following operating systems and backup sources are now supported:
		  • Red Hat Enterprise Linux 7.9
		  • PostgreSQL 13
		  • VMware vCenter Server 7.0

1.3	July 9, 2021	• Users can now enable or disable the cleaning of DS-License Server logs and configure how often the logs are cleaned. Requires DS-License Server RLM v14.2.0.3 or later.
		• The following operating systems and backup sources are now supported:
		  • CentOS 7.9, 8.3
		  • Red Hat Enterprise Linux 8.3
		  • Mac OS X 11
		  • VMware Cloud Director Server 10.1, 10.2
		• The following operating systems and backup sources are no longer supported:
		  • CentOS 7.5, 7.6
		  • Red Hat Enterprise Linux 7.5, 7.6
		  • Mac OS X 10.13
		  • IBM DB2 10.5
		  • Microsoft Exchange Server 2016
		  • Microsoft Outlook 2016
		  • Oracle Database 12c
		  • Oracle MySQL 5.6, 5.7
		  • PostgreSQL 9.5
		  • VMware vCenter Server 6.0
		  • VMware vCloud Director 9.5, 9.7

Version	Date	Summary

1.4	February 1, 2022	• The version of the log4j component used by the Asigra software has been updated to the latest version to ensure our software is not flagged by any scanning tools. Requires Windows DS-Client v14.2.0.5, DS-NOC v14.2.0.4, and Management Console v14.2.0.5 or later.
		
		• When editing Microsoft 365 credentials in Management Console, updated credentials are now automatically applied to all Microsoft 365 backup sets that use the credentials. Requires Management Console v14.2.0.5 or later.
		
		• When configuring a Microsoft 365 backup set in DS-User, users can now perform folder-level backups of SharePoint and OneDrive Document libraries. Requires Windows DS-Client v14.2.0.5 and Windows DS-User v14.2.0.4 or later.
		
		• When configuring a DS-System or BLM Archiver license, users can now set a quota on a DS-System or BLM Archiver license. Requires DS-License Server RLM v14.2.0.4 or later.
		
		• BLM Archiver users can now configure a BLM cloud storage location using any S3-compatible storage solution that supports Signature Version 4 (SigV4). Requires BLM Archiver v14.2.0.3 or later.
		
		• When configuring a Salesforce backup set in DS-User, users can now sort the list of database tables. Requires Windows DS-User v14.2.0.4 or later.
		
		• When performing a backup of a virtual machine on a VMware vCenter Server, a warning message is now displayed in the Event Log if a backup snapshot cannot be removed at the end of the backup activity. Requires Windows DS-Client v14.2.0.5 or Linux DS-Client v14.2.0.4 or later.
		
		• The following operating systems and backup sources are now supported:
		  • Windows 11
		  • Windows Server 2022
		  • Red Hat Enterprise Linux 8.4
		  • SUSE Linux Enterprise Server 15 SP3
		  • Debian 10.x, 11.x
		  • Ubuntu 18.04, 20.04
		  • Mac OS X 12
		  • Oracle Database 21c
		  • PostgreSQL 14
		
		• The following operating systems and backup sources are no longer supported:
		  • CentOS 8.x
		  • Red Hat Enterprise Linux 7.7, 8.0, 8.1
		  • Mac OS X 10.14
		  • Microsoft Hyper-V Server 2016
		  • Microsoft SharePoint Server 2016
		  • Microsoft SQL Server 2016 SP2
		  • Oracle Database 18c
		  • PostgreSQL 9.6
		  • VMware Cloud Director 10.0
		
		• The following Asigra software tools are no longer supported:
		  • DS-Prerequisites Tool
		  • Storage and Bandwidth Calculation Tool
		  • System Information Collector

Version	Date	Summary
1.5	August 29, 2022	• Management Console users can now scan File System backup sets for potentially malicious or unauthorized content based on predefined policies. Active content is reported on during the backup process and filtered, blocked, or removed during the restore process. Requires Windows DS-License Server RLM v14.2.0.5, Windows DS-System v14.2.0.5, Windows DS-Client v14.2.0.6, and Management Console v14.2.0.6 or later. • Management Console users can now backup and restore Microsoft 365 SharePoint and OneDrive data using Modern authentication credentials. Requires Windows DS-Client v14.2.0.6 and Management Console v14.2.0.6 or later. • Management Console users can now backup and restore individual Microsoft 365 SharePoint and OneDrive files that are up to 250 GB in size. Requires Windows DS-Client v14.2.0.6 or later. • When configuring a Microsoft 365 backup set, users can now perform folder-level backups of SharePoint and OneDrive Document libraries. Requires Windows DS-Client v14.2.0.5, Windows DS-User v14.2.0.4 or Windows Management Console v14.2.0.6 or later. • SharePoint and OneDrive performance has been improved when backing up and restoring multiple large files. DS-Client memory usage has been reduced when backing up and restoring SharePoint and OneDrive data. Requires Windows DS-Client v14.2.0.6 or later. • Management Console administrators can now configure multifactor authentication (MFA) for a user so that the user requires approval to delete a backup set. Requires Management Console v14.2.0.6 or later. • Management Console administrators can now configure multifactor authentication (MFA) for a user so that the user requires approval to perform an on-demand backup. Requires Management Console v14.2.0.6 or later. • Management Console administrators can now configure multifactor authentication (MFA) for a user so that the user requires approval to perform an on-demand restore. Requires Management Console v14.2.0.6 or later. • Management Console administrators can now configure multifactor authentication (MFA) for a user so that the user requires approval to reassign, edit, or delete a retention rule for an existing backup set. Requires Management Console v14.2.0.6 or later. • Management Console administrators can now configure multifactor authentication (MFA) for a user so that the user requires approval to reassign, edit, or delete a schedule for an existing backup set. Requires Management Console v14.2.0.6 or later. • Management Console now integrates with the latest version (v5.0.8) of Secret Double Octopus (SDO) to support the multifactor authentication (MFA) feature. Requires Management Console v14.2.0.6 or later. • When performing backup, restore, or delete operations, Management Console users can now view the contents of folders that contain more than 10,000 items with improved performance. Requires Management Console v14.2.0.6 or later. • Management Console users can now enable or disable the Volume Shadow Copy Service (VSS) option for File system and Permissions backup sets. The option is enabled by default. Requires Management Console v14.2.0.6 or later.

Version	Date	Summary

		• When configuring Microsoft 365 credentials, Management Console users can now register a single or multitenant application when using Modern authentication (Manual) credentials. Requires Management Console v14.2.0.6 or later.
		• DS-Operator users can now configure the number of threads that can be used for the autonomic healing and system admin processes using the HealingThreads and SysAdminThreads advanced configuration parameters. Requires DS-System v14.2.0.5 and DS-Operator v14.2.0.5 or later.
		• Several third-party components used by DS-NOC have been updated to the latest version to improve performance and security. Requires DS-NOC v14.2.0.5 or later.
		• When configuring a VMware vCenter Server backup set, users can now configure the days of the week on which they want to validate the disk signature of a protected virtual machine. Requires DS-User v14.2.0.5 or Management Console v14.2.0.6 and Windows DS-Client v14.2.0.5 or Linux DS-Client v14.2.0.4 or later.
		• When configuring the SMTP server notification settings in DS-User, users can now enter a password for the SMTP Server that contains up to 128 characters. Requires DS-User v14.2.0.5, Windows DS-Client v14.2.0.6 or Linux DS-Client v14.2.0.5 or later.
		• Several software components (BLM Archiver, Windows DS-Client, DS-Recovery Tools, Remote DS-VDR) have been updated to address hardening changes implemented by Microsoft in DCOM (KB5004442) that were required for CVE-2021-26414. Requires BLM Archiver v14.2.0.4 DS-NOC 14.2.0.5, DS-Recovery Tools v14.2.0.1 or Remote DS-VDR 14.2.0.2 or later.
		• The embedded version of PostgreSQL installed with the DS-Client (Windows, Linux, Mac) software has been upgraded to the latest version of PostgreSQL 11 to address any security vulnerabilities. Requires Windows DS-Client v14.2.0.6, Linux DS-Client v14.2.0.5 or Mac DS-Client v14.2.0.5 or later.
		• The following operating systems are now supported:
		  • Red Hat Enterprise Linux 8.5
		  • Ubuntu 22.04
		• The following operating systems and backup sources are no longer supported:
		  • Red Hat Enterprise Linux 8.2
		  • IBM DB2 11.1

1.6	September 26, 2022	• Management Console users can now migrate their Microsoft 365 Basic authentication credentials to Modern authentication (Automatic or Manual) credentials and update the associated backup sets to use the migrated Modern authentication credentials. Requires Management Console v14.2.0.7 or later.

Version	Date	Summary
1.7	April 10, 2023	• Management Console Global Administrators can now configure Multifactor Authentication (MFA) for users so they must authenticate using a six-digit Time-based one-time password (TOTP) application, such as Google or Microsoft Authenticator when signing in or attempting to perform a potentially destructive action that can result in the loss of data. Requires Management Console 14.2.0.8 or later. • Management Console Global Administrators can now configure Multiperson Approval (MPA) for accounts so users require multiple people to approve a potentially destructive action that can result in the loss of data. Administrators can set a threshold to specify how many approvals are required. Requires Management Console 14.2.0.8, Windows DS-Client 14.2.0.8 or Linux or Mac DS-Client 14.2.0.6, DS-System 14.2.0.6, and DS-Operator 14.2.0.6 or later. • Management Console users can now scan their File System backup sets for malware during the backup and restore process when connected to a Linux or Mac DS-Client. Requires Management Console 14.2.0.8 and Linux or Mac DS-Client 14.2.0.6 or later. • When scanning File System backup sets for malware during the restore process, Management Console users can now either quarantine the infected files in a password-protected zip file or attempt to clean the infected files and restore them when the remediation is successful. Requires Management Console 14.2.0.8 and Windows DS-Client 14.2.0.8 or Linux or Mac DS-Client 14.2.0.6 or later. • When scanning File System backup sets for malware during the backup process, files detected with malware are no longer quarantined. The files are backed up to the DS-System in an encrypted format so they cannot infect the data repository. Infected files can be quarantined or cleaned during the restore process. Requires Windows DS-Client 14.2.0.8 or later. • Management Console users can now select which Microsoft 365 services and DS-Clients use the autodiscover feature to automatically create backup sets for items added to the Microsoft 365 domain. Users can also automatically suspend backup sets associated with Microsoft 365 accounts that have been removed from the domain as part of the autodiscover process. Requires Management Console 14.2.0.8 or later. • Management Console users can now search for specific items when restoring Microsoft 365 data from Exchange Online, Archive Mailboxes, and Public Folders, SharePoint Online, or OneDrive. Users can search for specific emails, contacts, calendars, tasks, and/or posts. Requires Management Console 14.2.0.8 or later. • Improved performance when restoring Microsoft 365 (Exchange Online) data. Requires Windows DS-Client v14.2.0.8 or later. • Improved data processing and performance when backing up Microsoft 365 (SharePoint Online) data. Requires Windows DS-Client v14.2.0.8 or later • Management Console users can no longer delete Microsoft 365 credentials if there are existing backup sets using those credentials. Users must first assign new Microsoft 365 credentials to the affected backups sets. Requires Management Console v14.2.0.8 or later. • Management Console users can now view the platform (Windows, Linux, Mac) of each DS-Client, view the IP address or host name of each backup source machine, and search for a specific DS-Client based on the DS-Client number when viewing the list of backup sets on the Backup Sets tab of the Data Management page. Requires Management Console 14.2.0.8 or later. • Management Console users can now search the Activity Log based on the backup set name. Requires Management Console 14.2.0.8 or later.

Version	Date	Summary

		• Windows DS-Client now supports the Transport Layer Security (TLS) 1.3 encryption protocol. Requires Windows DS-Client 14.2.0.8 or later.
		
		• When performing a restore of a File system backup set, users now have the option to restore data deduplication links as links, skip data deduplication links, or restore the last non-link. Requires Windows DS-Client 14.2.0.8 and DS-User 14.2.0.6 or later.
		
		• When performing a Bare Metal Restore (BMR) of a computer with active retention rules, users can now select a backup session suitable for BMR. Requires Windows DS-Client 14.2.0.8 and DS-User 14.2.0.6 or later.
		
		• When attempting to perform a backup of a Microsoft Hyper-V Server backup set that is being replicated, a warning message is now displayed to indicate when a virtual machine is offline. Requires Windows DS-Client 14.2.0.8 or later.
		
		• When creating a VMware Cloud Director backup set, if a user with administrator privileges configures the credentials for the Cloud Director server, a regular user can now create the backup set using the organization credentials. Requires Management Console 14.2.0.8 or later.
		
		• Updated the Google Drive, Gmail, Calendar, and Contacts APIs to support the latest Google Workspace features and implemented dynamic thread pool management so the GAppsMaxJavaPluginThreads advanced configuration parameter is no longer required or available. Requires Windows DS-Client 14.2.0.8 or later.
		
		• Updated third-party components used by the Asigra software to address potential security vulnerabilities. Requires BLM Archiver v14.2.0.5, DS-Billing v14.2.0.3, Windows DS-Client 14.2.0.8, DS-License Server CLM 14.2.0.2, DS-License Server RLM 14.2.0.6, DS-NOC 14.2.0.6, DS-Operator 14.2.0.6, DS-System 14.2.0.6, DS-User 14.2.0.6, and Management Console 14.2.0.8 or later.
		
		• The following operating systems and backup sources are now supported:
		  • Red Hat Enterprise Linux 8.6, 8.7, 9.0, 9.1
		  • SUSE Linux Enterprise Server 15 SP4
		  • Mac OS X 13
		  • PostgreSQL 15
		
		• The following operating systems and backup sources are no longer supported:
		  • Debian 10.x
		  • Mac OS X 10.15
		  • PostgreSQL 10
		  • Microsoft SQL Server 2017
		  • NetApp
		  • VMware vCenter Server 6.5, 6.7
		
		• The following Asigra products are no longer supported:
		  • Converged Data Protection Appliance (CDPA)
		
		• The following Asigra software tools are no longer supported:
		  • Snapshot Manager
		
		• The following third-party software integrations are no longer supported:
		  • Secret Double Octopus (SDO)

About this document

This document describes the new features and enhancements that are available in this version of the product.

Important: Read this entire document before installing or upgrading the Asigra Cloud Backup software.

Important information

Discontinued version support

The following Asigra Cloud Backup software versions have reached the end of Mainstream Support.

- v13.3 (December 31, 2020)
- v14.0 (December 31, 2021)
- v14.1 (December 31, 2021)

For customers who require additional time to test or qualify their environments prior to updating to the current software release, Asigra offers Extended Support for a fee. For more information on how to obtain Extended Support, contact Asigra Client Services at client.services@asigra.com.

Note: For more information on the Asigra software support policy, see the Support Matrix.

Discontinued installation support

Installing the Asigra software on machines running the following platforms or databases is no longer supported:

- CentOS 7.3, 7.4, 7.5, 7.6, 8.x
- Debian 10.x
- Red Hat Enterprise Linux 7.3, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2
- SUSE Linux Enterprise Server 11 SP4
- Mac OS X 10.12, 10.13, 10.14, 10.15
- Microsoft SQL Server 2014 SP2, 2016 SP2, 2017
- PostgreSQL 9.4, 9.5, 9.6, 10

Note: For more information on the third-party software installation support policy, see the Support Matrix.

Discontinued backup and restore support

Performing backup and restore activities on the following sources is no longer supported:

- IBM DB2 10.5, 11.1
- Microsoft Exchange Server 2016
- Microsoft Hyper-V Server 2016
- Microsoft Outlook 2016
- Microsoft SharePoint Server 2016
- Microsoft SQL Server 2014 SP2, 2016 SP2, 2017
- NetApp
- Oracle Database 12c, 18c
- Oracle MySQL 5.6, 5.7
- PostgreSQL 9.4, 9.5, 9.6, 10
- VMware vCenter Server 6.0, 6.5, 6.7
- VMware vCloud Director 9.5, 9.7, 10.0

Note: For more information on the third-party software backup & restore support policy, see the Support Matrix.

Discontinued product support

The following Asigra products are no longer supported:

- Converged Data Protect Appliance (CDPA)

Discontinued replication support

Performing replication on the following sources is no longer supported:

- Microsoft Hyper-V Server

Discontinued tools support

The following Asigra software tools are no longer supported:

- DS-Prerequisites Tool
- Snapshot Manager
- Storage and Bandwidth Calculation Tool
- System Information Collector

Discontinued third-party software support

The following third-party software integrations are no longer supported:

- **Secret Double Octopus (SDO)** – Management Console users can no longer use Secret Double Octopus (SDO) for Multifactor Authentication (MFA) because the integration is no longer supported.
- **VMware vCenter Converter Standalone** - Physical-to-Virtual (VMware vCenter) backup sets are no longer supported because the VMware vCenter Converter Standalone software has been retired by VMware.

Localization support

The user interfaces are available in English, German, and Simplified Chinese. The PDF files are available only in English. Users can translate online Help into over 100 languages from their web browser.

Product documentation

The latest product documentation is available at https://help.asigra.com/en/knowledge/documentation

Unused Asigra HASP USB keys

You must return unused DS-License Server HASP USB keys as the keys remain the property of Asigra Inc.

Backup set support in Management Console and DS-User

The following backup set types are supported in Management Console and DS-User:

File System Backup Sets	Management Console	DS-User
File system (Windows, Azure Storage)	✓	✓
File system (NAS, NFS, UNIX-SSH)	✓[1]	✓
Permissions	✓	✓
Cloud Backup Sets	**Management Console**	**DS-User**
Google Workspace		✓
Microsoft 365	✓	✓
Salesforce		✓
Database Backup Sets	**Management Console**	**DS-User**
IBM DB2		✓
Microsoft SQL Server (Classic)	✓[2]	✓
Microsoft SQL Server (VSS-aware)	✓[3]	✓
Oracle Database		✓
Oracle MySQL		✓
Oracle SBT		✓
PostgreSQL		✓
Email Message Backup Sets	**Management Console**	**DS-User**
Microsoft Exchange Server (EWS)		✓
Microsoft Outlook		✓
Server Backup Sets	**Management Console**	**DS-User**
Microsoft Exchange Server (VSS-aware)	✓[4]	✓
Microsoft SharePoint Server (Classic)		✓
Microsoft SharePoint Server (VSS-aware)	✓	✓
Virtual Machine Backup Sets	**Management Console**	**DS-User**
Microsoft Hyper-V Server (VSS-aware)	✓	✓
VMware vCenter Server	✓	✓
VMware Cloud Director Server	✓	
VM Replication Sets	**Management Console**	**DS-User**
VMware vCenter Server Replication	✓	✓

[1] NAS and NFS file system backups are not supported in Management Console.

[2] Cluster configuration not supported in Management Console for Microsoft SQL Server (Classic) backup sets.

[3] Cluster & AOAG configurations not supported in Management Console for Microsoft SQL Server (VSS-aware) backup sets.

[4] DAG configuration not supported in Management Console for Microsoft Exchange Server (VSS-aware) backup sets.

Installation and upgrade

The Asigra software is available to download for existing customers with valid annual maintenance and upgrade subscriptions. You can perform a new installation or upgrade from one of the following versions:

- v13.3 (DS-Clients only)
- v14.0
- v14.1

If you are running an unsupported version of the Asigra software, you must first upgrade to one of the versions listed above. If you are running an unsupported operating system, you must first upgrade the Asigra software and then upgrade the operating system.

Important: Prior to performing an upgrade, install the latest hotfix on the version from which you are upgrading. After performing the upgrade, install the latest hotfix on the new version.

When performing an upgrade, we recommend upgrading the following components at the same time, so they are all the same version: DS-NOC, DS-License Server, DS-System, DS-Billing, BLM Archiver. The recommended upgrade process is as follows:

1. Upgrade DS-NOC.
2. Upgrade DS-License Server.
3. Upgrade DS-System, DS-Billing, and BLM Archiver. If the component is a member of a replication group, upgrade all members of the group at the same time. Otherwise, upgrade the components in any order.
4. Upgrade DS-Clients.
5. Upgrade other software components in any order.

Note: Management Console hotfix v14.1.0.5 is included with the DS-System and is automatically downloaded by the DS-Client when the DS-System is upgraded. The hotfix must be installed prior to upgrading the Management Console to v14.2. Do not upgrade the Management Console to v14.2 if you intend to connect to v14.1 DS-Clients. You must upgrade the Management Console at the same time as the DS-System or DS-Client to be compatible.

The DS-System and BLM Archiver are backwards compatible with the previous two versions of the DS-License Server. The DS-System is backwards compatible with the previous two versions of the DS-Client.

Backwards compatibility is not supported for the following:

- BLM Archivers in the same replication group
- DS-Systems in an N+1 configuration or the same replication group
- DS-Clients in the same grid configuration or VM replication group

To perform an automatic upgrade or apply a hotfix to a DS-Client, the upgrade or hotfix must be approved and configured in the DS-Operator. DS-Clients will not be automatically upgraded unless approved. By default, hotfixes are automatically applied the first time the DS-Client connects to an upgraded DS-System. For more information, see the *DS-System User Guide*.

The following hotfix packages are included with the DS-System and will be automatically downloaded when the DS-System is upgraded. The hotfixes must be installed on the DS-Client to allow for automatic upgrades to be approved in the DS-Operator.

- Windows DS-Client v13.3.0.23, v14.0.0.13, v14.1.0.11 or later
- Linux or Mac DS-Client v13.3.0.14, v14.0.0.6, v14.1.0.6 or later

The hotfix is applied automatically to a supported DS-Client the first time it connects to an upgraded DS-System. If you disable automatic upgrades, you must manually perform upgrades and apply hotfixes on the DS-Client.

Note: When performing an automatic upgrade of a DS-Client, an external PostgreSQL or Microsoft SQL Server databases will be automatically migrated to an embedded PostgreSQL database. To retain an external Microsoft SQL Server database, you must perform a manual upgrade of the DS-Client.

New installation support

Installing the Asigra Cloud Backup software on machines running the following platforms is now supported:

- Windows 11
- Windows Server 2019, 2022
- CentOS 7.7, 7.8, 7.9
- Debian 11.x
- Ubuntu 18.04, 20.04, 22.04
- Red Hat Enterprise Linux 7.8, 7.9, 8.3, 8.4, 8.5, 8.6, 8.7, 9.0, 9.1
- SUSE Linux Enterprise Server 12 SP5, 15 SP4
- Mac OS X 11, 12, 13

Note: Download the latest installation packages, hotfixes, and support files from https://help.asigra.com/en/knowledge/software-updates

New backup and restore support

Performing backup and restore activities on the following operating systems is now supported:

- Windows 11
- Windows Server 2019, 2022
- CentOS 7.7, 7.8, 7.9
- Debian 11.x
- Ubuntu 18.04, 20.04, 22.04
- Red Hat Enterprise Linux 7.8, 7.9, 8.3, 8.4, 8.5, 8.6, 8.7, 9.0, 9.1
- SUSE Linux Enterprise Server 12 SP5, 15 SP4
- Mac OS X 11, 12, 13

Performing backup and restore activities on the following sources is now supported:

- IBM DB2 11.5
- Microsoft 365 Teams
- Microsoft Exchange Server 2019
- Microsoft Hyper-V Server 2019
- Microsoft Outlook 2019
- Microsoft SharePoint Server 2019
- Microsoft SQL Server 2019
- Oracle Database 19c, 21c
- PostgreSQL 11, 12, 13, 14, 15
- VMware Cloud Director 10.1, 10.2
- VMware vSphere 7.0

New features and enhancements

This section describes the new features and enhancements in the v14.2 version of the product.

Activity Monitor

- Management Console users can now view the real-time progress of on-demand activities.

Amazon S3 SigV4 support

- BLM Archiver users can now configure a BLM cloud storage location using a bucket from an Amazon S3 account that supports Signature Version 4 (SigV4).

Antimalware: Files no longer quarantined on backup

- When scanning File System backup sets for malware during the backup process, files detected with malware are no longer quarantined. The files are backed up to the DS-System in an encrypted format so they cannot infect the data repository. Infected files can be quarantined or cleaned during the restore process. Requires Windows DS-Client 14.2.0.8 or later.

Antimalware: Linux and Mac DS-Client support

- Management Console users can now scan their File System backup sets for malware during the backup and restore process when connected to a Linux or Mac DS-Client. Requires Management Console 14.2.0.8 and Linux or Mac DS-Client 14.2.0.6 or later.

Antimalware: Remediation on restore

- When scanning File System backup sets for malware during the restore process, Management Console users can now either quarantine the infected files in a password-protected zip file or attempt to clean the infected files and restore them when the remediation is successful. Requires Management Console 14.2.0.8 and Windows DS-Client 14.2.0.8 or Linux or Mac DS-Client 14.2.0.6 or later.

Backup set creation wizard

- Management Console users are now guided through the backup set creation process and can create or edit schedules or retention rules from the wizard.

Backup Set Status Report

- Management Console users can now email a generated report that provides a consolidated view of the backup status on a daily and monthly basis so they can quickly see which backups completed successfully and which backups failed with errors.

Backup Set Storage Report

- Management Console users can now view detailed information about the backup data stored on the DS-System, including the protected size, stored size, and native size.

Bare Metal Restore (BMR) of historical data

- When performing a Bare Metal Restore (BMR) of a computer with active retention rules, users can now select a backup session suitable for BMR. Requires Windows DS-Client 14.2.0.8 and DS-User 14.2.0.6 or later.

Cloud plug-ins (Google Workspace, Microsoft 365, Salesforce)

- The Cloud plug-ins for Google Workspace, Microsoft 365, and Salesforce are now installed automatically when the user installs the DS-Client software.

Content Disarm & Reconstruction (CDR)

- Management Console users can now scan File System backup sets for potentially malicious or unauthorized content based on predefined policies. Active content is reported on during the backup process and filtered, blocked, or removed during the restore process. Requires Windows DS-License Server RLM v14.2.0.5, Windows DS-System v14.2.0.5, Windows DS-Client v14.2.0.6, and Management Console v14.2.0.6 or later.

DS-Client database backup performance

- Several enhancements have been made to improve the performance of the DS-Client database backup during the Daily and Weekly Admin processes.

DS-Client embedded PostgreSQL version upgrade

- The embedded version of PostgreSQL that is installed with the DS-Client (Windows, Linux, Mac) software has been upgraded to the latest version of PostgreSQL 11 to address any security vulnerabilities. Requires Windows DS-Client v14.2.0.6, Linux DS-Client v14.2.0.5 or Mac DS-Client v14.2.0.5 or later.

DS-Client remote management support

- Management Console users (Windows or Linux) can now remotely manage DS-Clients without opening a port in the firewall on the DS-Client machine. Requires Windows or Linux DS-Client v14.2.0.2, DS-System v14.2.0.2, and Management Console v14.2.0.2 or later.

DS-Client TLS 1.3 support

- Windows DS-Client now supports the Transport Layer Security (TLS) 1.3 encryption protocol. Requires Windows DS-Client 14.2.0.8 or later.

DS-Client upgrades

- DS-System administrators can now manage the DS-Client automatic upgrade process by using the DS-Operator to approve and configure when hotfixes and upgrades are applied to the DS-Clients in their environment. DS-Clients will not be automatically upgraded unless approved.

DS-License Server clean logs

- Users can now enable or disable the cleaning of DS-License Server logs and configure how often the logs are cleaned. Requires DS-License Server RLM v14.2.0.3 or later.

DS-License Server online capacity

- Several enhancements have been to the DS-License Server, including supporting dynamic IP addresses. Users can now also view the total online capacity used by the DS-System.

DS-License Server quota management

- When configuring a DS-System or BLM Archiver license, users can now set a quota on a DS-System or BLM Archiver license. Requires DS-License Server RLM v14.2.0.4 or later.

DS-NOC reporting

- When creating a custom scheduled report in the DS-NOC, users can now select a dynamic date range (last 24 hours, last 7 days, or last 30 days) for the Connection Log start session time (log_start_session_time) field. Requires DS-NOC v14.2.0.3 or later.

DS-NOC security

- Several enhancements have been made to the DS-NOC to improve the security for the password reset process to prevent a malicious attacker from obtaining access to user accounts.

DS-System empty trash settings

- Users can no longer schedule an empty trash task in the DS-Operator. After upgrading to v14.2, existing scheduled empty trash tasks will be deleted. Users must now configure the DefaultTrashDays and EmptyTrashTime advanced configuration parameters in the DS-Operator.

DS-System autonomic healing and system admin process

- DS-Operator users can now configure the number of threads that can be used for the autonomic healing and system admin processes using the HealingThreads and SysAdminThreads advanced configuration parameters. Requires DS-System v14.2.0.5 and DS-Operator v14.2.0.5 or later.

DS-System replication

- Management Console users can now configure a DS-System to perform replication of DS-Client data.

DS-User and DS-Operator increased user name character limit

- Users can now enter a user name that contains up to 50 characters when logging on to the DS-User (Windows or Linux) or DS-Operator (Windows or Linux).

DS-User increased password character limit

- When logging on to the DS-User or entering the credentials for the backup source in DS-User, users can now enter a password that contains up to 128 characters.

DS-User increased SMTP server password character limit

- When configuring the SMTP server notification settings in DS-User, users can now enter a password for the SMTP Server that contains up to 128 characters. Requires DS-User v14.2.0.5, Windows DS-Client v14.2.0.6 or Linux DS-Client v14.2.0.5 or later.

File system restore enhancements

- When performing a restore of a File system backup set, users now have the option to restore Microsoft data deduplication links as links, skip data deduplication links, or restore the last non-link. Requires Windows DS-Client 14.2.0.8 and DS-User 14.2.0.6 or later.

Google Workspace enhancements

- Updated the Google Drive, Gmail, Calendar, and Contacts APIs to support the latest Google Workspace features and implemented dynamic thread pool management so the GAppsMaxJavaPluginThreads advanced configuration parameter is no longer required or available. Requires Windows DS-Client 14.2.0.8 or later.

Log4j vulnerability update

- The version of the log4j component used by the Asigra software has been updated to the latest version to ensure our software is not flagged by any scanning tools. Requires Windows DS-Client v14.2.0.5, DS-NOC v14.2.0.4, and Management Console v14.2.0.5 or later.

Mac DS-Client support

- Management Console now supports connections to Mac DS-Clients.

Management Console Activity Log

- Management Console users can now search the Activity Log based on the backup set name. Requires Management Console 14.2.0.8 or later.

Management Console credentials management

- Management Console users can now configure and manage their credentials from one location. Once the credentials are saved, the user can simply select the credentials when creating a backup set rather than having to manually enter them each time.

Management Console data management

- Management Console users can now view the platform (Windows, Linux, Mac) of each DS-Client, view the IP address or host name of each backup source machine, and search for a specific DS-Client based on the DS-Client number when viewing the list of backup sets on the Backup Sets tab of the Data Management page. Requires Management Console 14.2.0.8 or later.

Management Console initial setup wizard

- New Management Console users are now guided through the initial setup process, including configuring security settings, DS-System and DS-Client connections, users and permissions, and email settings.

Management Console performance

- When performing backup, restore, or delete operations, Management Console users can now view the contents of folders that contain more than 10,000 items with improved performance. Requires Management Console v14.2.0.6 or later.

Management Console security

- Management Console global administrators can now configure a password policy, the number of failed sign-in attempts, the session timeout, and whether users must enter their password to perform any operation that can result in the loss of data.

Management Console Volume Shadow Copy Service (VSS) configuration

- Management Console users can now enable or disable the Volume Shadow Copy Service (VSS) option for File system and Permissions backup sets. Requires Management Console v14.2.0.6 or later.

Microsoft 365 antimalware support

- Management Console users can now scan Microsoft 365 (Exchange Online, SharePoint Online, OneDrive, Groups, or Teams) files for malware during backup and restore. Requires Windows DS-Client v14.2.0.1 and Management Console v14.2.0.1 or later to scan Exchange Online files, Requires Windows DS-Client v14.2.0.2 and Management Console v14.2.0.2 or later to scan Groups or Teams data.

Microsoft 365 archive mailboxes (Exchange Online)

- Management Console users can now backup and restore archive mailboxes when configuring a Microsoft 365 (Exchange Online) backup set.

Microsoft 365 autodiscover enhancements

- Management Console users can now select which Microsoft 365 services and DS-Clients use the autodiscover feature to automatically create backup sets for items added to the Microsoft 365 domain. Users can also automatically suspend backup sets associated with Microsoft 365 accounts that have been removed from the domain as part of the autodiscover process. Requires Management Console 14.2.0.8 or later.

Microsoft 365 credentials deletion

- Management Console users can no longer delete Microsoft 365 credentials if there are existing backup sets using those credentials. Users must first assign new Microsoft 365 credentials to the affected backups sets. Requires Management Console v14.2.0.8 or later.

Microsoft 365 credentials editing

- When editing Microsoft 365 credentials in Management Console, updated credentials are now automatically applied to Microsoft 365 backup sets using the credentials. Requires Management Console v14.2.0.5 or later.

Microsoft 365 credentials migration

- Management Console users can now migrate their Microsoft 365 Basic authentication credentials to Modern authentication (Automatic or Manual) credentials and update the associated backup sets to use the migrated Modern authentication credentials. Requires Management Console v14.2.0.7 or later.

Microsoft 365 file folder and 5000 file support (OneDrive)

- Users can now view OneDrive content in a file folder structure and back up more than 5000 OneDrive files.

Microsoft 365 file name character support (SharePoint Online and OneDrive)

- Users can now back up SharePoint Online and OneDrive files that contain the # and % characters in the file name.

Microsoft 365 folder-level backup support (SharePoint Online & OneDrive)

- When configuring a Microsoft 365 backup set, users can now perform folder-level backups of SharePoint and OneDrive Document libraries. Requires Windows DS-Client v14.2.0.5, Windows DS-User v14.2.0.4 or Windows Management Console v14.2.0.6 or later.

Microsoft 365 Groups and Teams support

- Management Console users can now backup and restore Microsoft 365 Groups and Teams.

Microsoft 365 large file support (SharePoint Online & OneDrive)

- Management Console users can now backup and restore individual Microsoft 365 SharePoint and OneDrive files that are up to 250 GB in size. Requires Windows DS-Client v14.2.0.6 or later.

Microsoft 365 modern authentication support (single or multitenant)

- When configuring Microsoft 365 credentials, Management Console users can now register a single tenant or multitenant application when using modern authentication (Manual) credentials. Requires Management Console v14.2.0.6 or later.

Microsoft 365 modern authentication support (SharePoint Online & OneDrive)

- Management Console users can now backup and restore Microsoft 365 SharePoint and OneDrive data using modern authentication credentials. Requires Windows DS-Client v14.2.0.6 and Management Console v14.2.0.6 or later.

Microsoft 365 modern team sites support (SharePoint Online)

- Management Console users can now backup and restore Microsoft SharePoint communication, hub, and team sites created using the new modern team site template. To back up and restore SharePoint modern team sites, you must create a new Microsoft 365 backup set.

Microsoft 365 OAuth support

- Management Console users can now use Microsoft Basic or Modern authentication to securely access their Microsoft 365 services. Our Modern authentication implementation has been designed for ease of use and requires only one click and no additional configuration from the user.

Microsoft 365 performance enhancements (Exchange Online)

- Improved performance when restoring Microsoft 365 (Exchange Online) data. Requires Windows DS-Client v14.2.0.8 or later.

Microsoft 365 data processing and performance enhancements (SharePoint Online)

- Improved data processing and performance when backing up Microsoft 365 (SharePoint Online) data. Requires Windows DS-Client v14.2.0.8 or later.

Microsoft 365 performance enhancements (SharePoint Online & OneDrive)

- Improved performance when backing up and restoring multiple large files for Microsoft 365 (SharePoint Online and OneDrive). DS-Client memory usage has been reduced when backing up and restoring SharePoint and OneDrive data. Requires Windows DS-Client v14.2.0.6 or later.

Microsoft 365 search enhancements

- Management Console users can now search for specific items when restoring Microsoft 365 data from Exchange Online, Archive Mailboxes, and Public Folders, SharePoint Online, or OneDrive. Users can search for specific emails, contacts, calendars, tasks, and/or posts. Requires Management Console 14.2.0.8 or later.

Microsoft Azure storage backup

- Management Console users can now backup and restore network file shares located in Microsoft Azure Storage using the Azure Files data service.

Microsoft DCOM security hardening

- Several software components (BLM Archiver, Windows DS-Client, DS-Recovery Tools, Remote DS-VDR) have been updated to address hardening changes implemented by Microsoft in DCOM (KB5004442) that were required for CVE-2021-26414 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26414). Requires BLM Archiver v14.2.0.4, DS-NOC 14.2.0.5, DS-Recovery Tools v14.2.0.1 or Remote DS-VDR 14.2.0.2 or later.

Microsoft Hyper-V Server backups

- When attempting to perform a backup of a Microsoft Hyper-V Server backup set that is being replicated, a warning message is now displayed to indicate when a virtual machine is offline. Requires Windows DS-Client 14.2.0.8 or later.

Microsoft SQL Server transaction logs

- Management Console users can now configure Microsoft SQL Server (Classic) backup sets to include the “Full plus incremental” or “Transaction logs only” database backup policies for the database dump.

Multifactor Authentication (MFA) support

- Management Console Global Administrators can now configure Multifactor Authentication (MFA) for users so they must authenticate using a six-digit Time-based one-time password (TOTP) application, such as Google or Microsoft Authenticator when signing in or attempting to perform a potentially destructive action that can result in the loss of data. Requires Management Console 14.2.0.8 or later.

Multiperson Approval (MPA) support

- Management Console Global Administrators can now configure Multiperson Approval (MPA) for accounts so users require multiple people to approve a potentially destructive action that can result in the loss of data. Administrators can set a threshold to specify how many approvals are required. Requires Management Console 14.2.0.8, Windows DS-Client 14.2.0.8 or Linux or Mac DS-Client 14.2.0.6, DS-System 14.2.0.6, and DS-Operator 14.2.0.6 or later.

  Note: For security reasons, users should not use DS-User to manage accounts for which MPA has been enabled in the Management Console.

Pre/Post for File System backup sets

- Management Console users can now configure a process to run before and/or after a File system backup to perform specific actions when a condition has been met. Requires Windows DS-Client v14.2.0.2 and Management Console v14.2.0.2 or later.

Product documentation

- The documentation (PDF files) is no longer installed with the product or available on the ISO image. The latest documentation is available for download from the Asigra Support Portal.

Replication set creation wizard

- Management Console users are now guided through the replication set creation process and create or edit schedules or retention rules from the wizard.

Retention rules

- Management Console users can now configure a retention rule to automatically delete obsolete files that have been removed from the source.

S3-compatible storage SigV4 support

- BLM Archiver users can now configure a BLM cloud storage location using any S3-compatible storage solution that supports Signature Version 4 (SigV4). Requires BLM Archiver v14.2.0.3 or later.

Salesforce backup sets

- When configuring a Salesforce backup set in DS-User, users can now sort the list of database tables. Requires Windows DS-User v14.2.0.4 or later.

Scheduled restore

- Management Console users can now schedule a restore of backup data to the original or an alternate location for data validation purposes.

Security enhancements

- Updated third-party components used by the Asigra software to address potential security vulnerabilities. Requires BLM Archiver v14.2.0.5, DS-Billing v14.2.0.3, Windows DS-Client 14.2.0.8, DS-License Server CLM 14.2.0.2, DS-License Server RLM 14.2.0.6, DS-NOC 14.2.0.6, DS-Operator 14.2.0.6, DS-System 14.2.0.6, DS-User 14.2.0.6, and Management Console 14.2.0.8 or later.

Suspend backup sets

- Management Console users can now suspend and activate backup sets.

Usage metrics

- Management Console users can now view detailed usage history so they can charge their customers based on capacity usage or by the number of machines being protected. Users can also drill down and see the usage breakdown for each cloud service.

VMware vCenter Server backup sets

- When performing a backup of a virtual machine on a VMware vCenter Server, a warning message is now displayed in the Event Log if a backup snapshot cannot be removed at the end of the backup activity. Requires Windows DS-Client v14.2.0.5 or Linux DS-Client v14.2.0.4 or later.

VMware vCenter Server disk signature validation

- When configuring a VMware vCenter Server backup set, users can now configure the days of the week on which they want to validate the disk signature of a protected virtual machine. Requires DS-User v14.2.0.5 or Management Console v14.2.0.6 and Windows DS-Client v14.2.0.6 or Linux DS-Client v14.2.0.5 or later.

VMware Cloud Director

- Management Console users can now backup and restore a virtual machine or an entire VMware vApp in a VMware Cloud Director environment.

VMware Cloud Director enhancements

- When creating a VMware Cloud Director backup set, if a user with administrator privileges configures the credentials for the Cloud Director server, a regular user can now create the backup set using the organization credentials. Requires Management Console 14.2.0.8 or later.

VMware vSphere replication

- Management Console users can now configure VMware vSphere replication sets so they can replicate virtual machines from one server to another and perform a failover and failback.

VSS validation

- Users can now enable or disable an option in DS-User to perform VSS validation on File system and VSS-aware backup sets prior to performing the backup.

Known issues and limitations

For a list of known issues and limitations, visit https://help.asigra.com/en/knowledge/known-issues