Administration Guide (On Premise)

Arcserve® Unified Data Protection Archiving

Version 6.0

arcserve

Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Arcserve at any time. This Documentation is proprietary information of Arcserve and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Arcserve.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Contact Arcserve Support

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

Contact Support

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles which contain field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Global User Community to ask and answer questions, share tips and tricks, discuss best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.
- You can access other helpful resources appropriate for your Arcserve Support product.

Contents

Chapter 1: Documentation Overview

This section provides information about this guide and overall technical documentation available for *Arcserve® Unified Data Protection Archiving*. The documentation bookshelf available in multiple languages is designed to help in completing all tasks associated with UDP Archiving. From deployment to archiving of emails, the bookshelf helps user with information and links to all type of information related to UDP Archiving. For example, getting started, key features, videos, links to other information not related to technical documents listed under Related Documentation.

- **FAQs and Troubleshooting Sections** helps with solutions of general questions and issues in respective guides.
- **Best Practices Section** helps with guidelines to consider before starting a task.

For further questions on documentation, click link to email us.

This section contains the following topics:

About This Guide

Arcserve UDP Archiving Administration guide helps you:

- Use the UDP Archiving *Console*: Provides description of architecture, management hierarchy, and all other role-based screens.
- Understand function of every role: Provides separate sections for all four roles.
- Work with different additional features: For example, how to use UDP Archiving as plug-in.
- Troubleshoot problems: Provides troubleshooting section.

Related Documentation of UDP Archiving

- *UDP Archiving* *Deployment and Configuration guide*: Provides information about Deployment and configuration of UDP Archiving settings and journals.
- UDP Archiving *Release Notes*: Provides information about the current release.
- UDP Archiving Bookshelf: Contains all related documents and videos.
- UDP Archiving Licensing: Describes how to apply and manage UDP Archiving licenses.
- UDP Archiving Videos: Contains list of videos related to UDP Archiving.

Language Support

A translated product (sometimes referred to as a localized product) includes local language support for the product's user interface, online help and other documentation, as well as local language default settings for date, time, currency, and number formats.

This release is translated / localized into the following languages, in addition to the English release:

- German
- French
- Italian
- Japanese
- Portuguese
- Spanish
- Chinese (Simplified)
- Chinese (Traditional)

Chapter 2: Understanding UDP Archiving

Arcserve® UDP Archiving is a purpose-built email archiving solution designed to protect corporate email records and make them easily accessible for audits and legal discovery. The multi-tenant capable solution supports On-premise, private, and public cloud deployments.

You can start using UDP Archiving within an hour of deployment. You need to deploy using one of the multiple options available and configure mail exchange. You can deploy UDP Archiving:

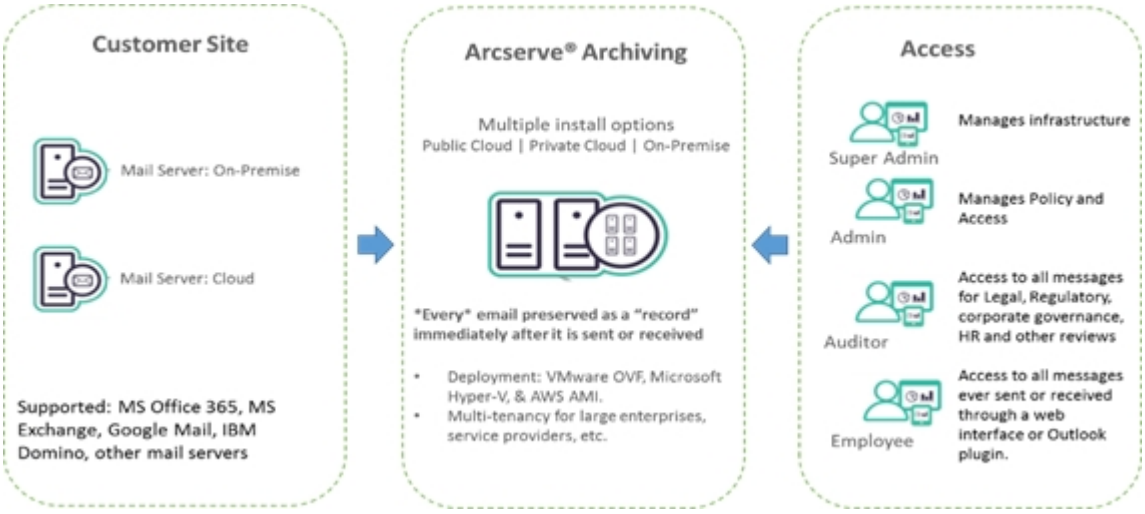
- as a virtual machine on VMware, Microsoft Hyper-V, or AWS AMI
- on private or public cloud

For details, refer to *UDP Archiving Deployment and Configuration Guide*.

This section contains the following topics:

UDP Archiving Overview

UDP Archiving supports all popular email platforms including Microsoft Exchange, Microsoft Office 365 (Exchange Online), IBM Lotus Domino, and Google Gmail.



UDP Archiving has multiple deployment options and gives customers maximum flexibility. Being also installed as a virtual machine, UDP Archiving supports VMware and Hyper-V virtual machines for private installation and AWS (Amazon Web Services) AMI for public cloud installations. Whether installed on premises or in the cloud, UDP Archiving connects to mail servers located on premises or in the cloud.

Key Features of UDP Archiving

UDP Archiving provides a full set of features that allow users to search mailbox using full text and Boolean search methods. Results are displayed and can be opened. Hit highlighting makes it easy to identify search text. Emails are tagged using tags defined by Employee, Auditor, and Compliance officer. Emails of a user are purged by Compliance Officer. Search results are saved and exported in standard Outlook format.

Key Features

- **Records Management:** Capture and retain emails as corporate record
- **Legal Hold management:** When needed, retain messages for specific individuals involved in legal cases
- **Life-cycle management:** Systematic removal of records at their end of life. All deletion activity is logged and reports can be run as proof of disposition for legal and compliance audits.
- **Compliance:** Meet all federal, state, local, and industry specific regulatory requirements to retain and produce emails when requested.
- **Purge Emails:** To meet privacy requirement, UDP Archiving lets you purge emails of desired users.
- **Legal Search:** Simple and advanced search capabilities allowing authorized users to search email and export results for legal discovery and compliance audits.
- **Fast search and retrieval:** The System Administrator (and authorized users) can perform quick, accurate on-demand retrieval of records for legal, regulatory, HR, and more.
- **Storage optimization:** Single Instance Storage (SIS) and compression to reduce the archive storage footprint. UDP Archiving saves money by reducing mail server storage, and increases mail server performance.

Best Practices for UDP Archiving

For setting up UDP Archiving and archiving emails, here are some best practices:

- **Modify Passwords of Super Admin and udp_admin:** Default passwords are publicly shared in documents over web and can be seen by all employees as well. To avoid misuse of access, we recommend to modify passwords of Super Admin and udp_admin immediately after the first login.
- **Set Retention rules and Archive Exception rules before configuring journaling:** Default retention settings may often result in major storage issue later as the archived emails are purged only after completing the number of days set in default Retention settings. You may not want all emails to be available for longer duration. We recommend to determine and configure the Retention Rules\Settings and Archive Exception Rules before configuring the E-mail Archiving on the Mail Server. Any new Exception and Retention Rules is applied to the messages only from the time when you create new rules and is not applicable to existing archived messages. For more information, see Manage Retention Rules.
- **Archive emails of only specific users:** Create a Distribution group to archive emails of specific users.
- **Increase storage when disk is 90% full:** When disk usage reaches 90%, disk usage percentage is displayed in Red to raise an alarm (Disk Usage in Super Admin, configuration). Increase disk space per your future requirements. Also, refer to projected storage requirement available in Health section of Super Admin to assess in how many days your disk will be full based on the current usage trend.
- **Best Practices for Import:**
  - Use POP3S, IMAP3S protocols for importing mails from Google professional mail boxes for hassle free operations.
  - Before adding a server for Import, always use Test Connection.
  - Before initiating Import, verify if the mailbox is having mails to be imported.
  - For using Import, verify if import credentials entered are valid and proper connection is established first.
- **Avoid peak hours for major work:** Plan your product updates installation / uninstallation when no active jobs are running or at non-peak hours of server

operations for smother completion. The same applies to Migration, import, downloading emails, and performing search.

- **Install outlook plug-in of respective outlook architecture (x86 / x64):** Install plug-in x86 on Outlook x86 , plug-in x64 on Outlook x64 to avoid compatibility problems.
- **Plan Monthly server maintenance:** Plan UDP Archiving server maintenance periodically once in a month to check the utilization of the Performance Key Indicators (PKI) status. If PKI appears over-utilized, increase CPU/Memory/Disk to reduce burden on the server.
- **Use Search criteria in Auditor:** Auditor by default displays 100000 emails. Use specific search criteria specifying different parameters (Date, From, To, subject, size, wildcard character "*") to view mails of specific user.
- **Make future search easier:** Save all your search queries into saved searches and in future use them to retrieve data quickly. Also, enable Advanced search parameters to narrow down your search results.
- **Use Smaller PSTs:** We recommend to have PST file within 10 GB, so that complete migration is not required in case of failure.
- **Thick vs Thin Provisioning:** Select thick provisioning over thin provisioning during OVF deployment. Both are supported. But, we strongly recommend to user thick provisioning, so that the space is allocated to the system in the beginning itself. This action would prevent issues like running out of space.
- **Host Name / IP Address of UDP Archiving Server:** Use static IP / host name for UDP Archiving server.
- **Best Practices for Migration:** Migration is a very time consuming operation, and time increases with more number of mails. At times, migration may consume more than an hour.
    - Start migration in non-peak hours.
    - Verify if the disk has enough space.

      For example, for a PST file of size 10 GB you need at least 25 GB free space for migration.
    - Particularly for VMware, if the thin provision option is selected during deployment of OVF, verify that the ESX Server has enough space.

Hierarchy and Access Levels in UDP Archiving

This section contains the following topics:

Management Hierarchy

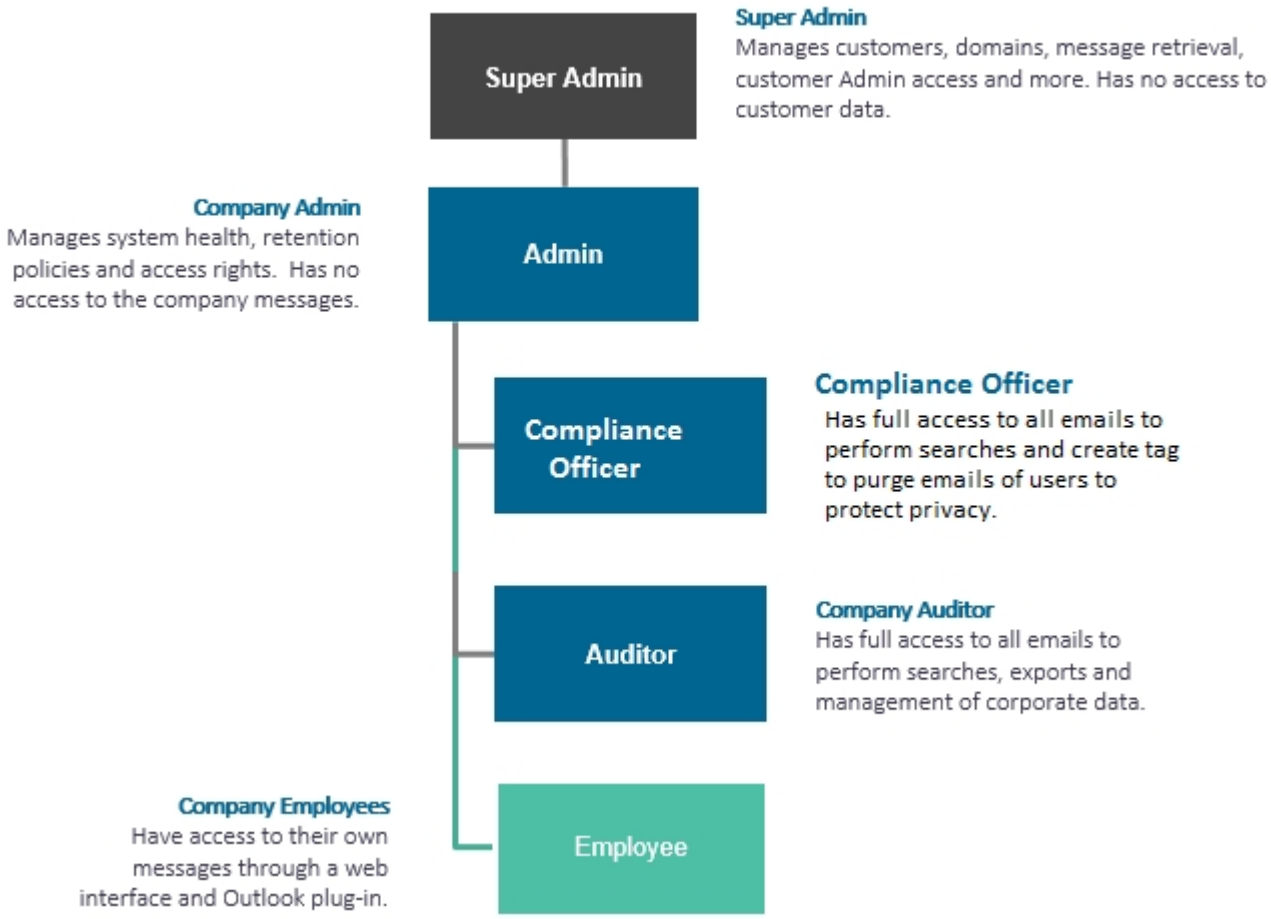
UDP Archiving is a single or multi-tenant solution used to manage multiple divisions or locations or by a service provider to support multiple clients. In both cases a Super Admin is created during the initial installation. This user controls the core administration functions of the system. If being used as a single tenant solution, the Super Admin will define one customer and the first Admin for that organization. In a multi-tenant environment, the Super Admin will define multiple customers and the first admin for each organization or organizational group if an Enterprise.

This section contains the following topics:

Single Company Deployment

Companies that have clearly defined roles & responsibilities, leveraging multiple applications to run their businesses need role-based access for mission-critical solutions like UDP Archiving. Arcserve UDP Archiving allows such organizations to comply with regulations while allowing them to take advantage of the predefined roles, created based on industry-standards.

For such organizations that want a separate division, UDP Archiving offers a single tenant solution where the Super Admin defines one customer and the first Admin for that organization.



Roles Assigned:

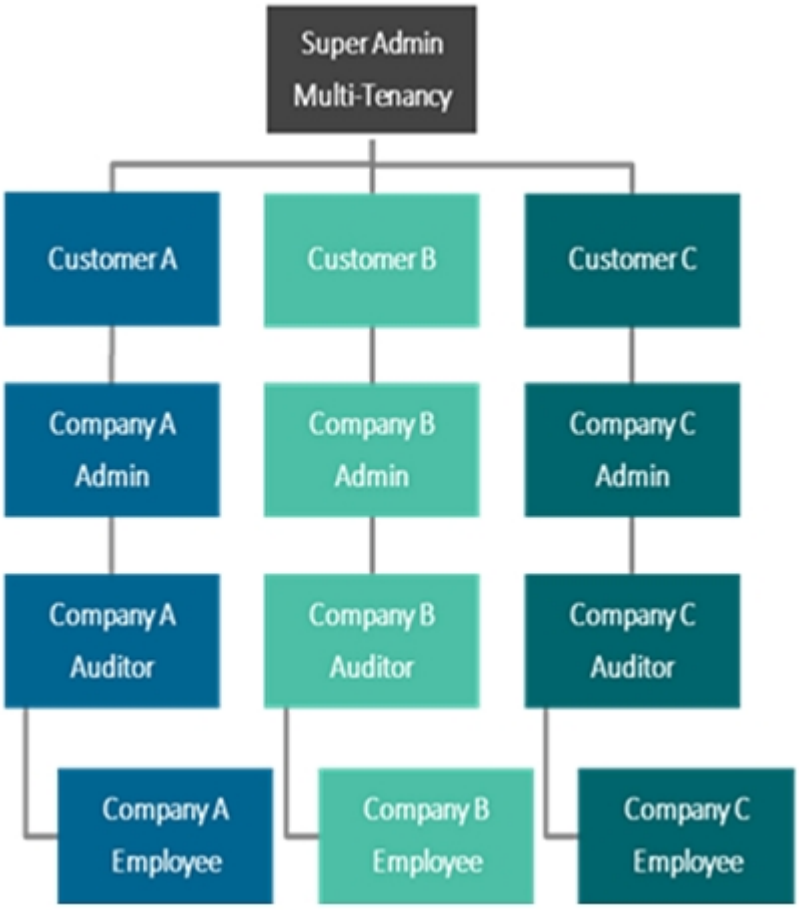
- **Super admin:** Refers to the role that assists to manage domains, create and manage administrators who would interact with the system, managing licenses of organization, and more. This role does not have access to the end

user data and is more useful in management.

- **Administrator:** Refers to the role that handles reporting and monitoring, setting up retention policies, providing access rights, managing licenses of users, and so on. Administrators cannot access company messages.
- **Compliance Officer:** Responsible for data protection of all users of an organization. Administrator creates the Compliance officer whose role is to purge the emails of user.
- **Auditor:** Auditor is the role created by the company administrator primarily for compliance audit. In UDP Archiving, this role has full access to emails of all users whose emails are being archived and can search messages or export them as corporate records for further use.
- **Employees:** Employees refer to all individuals of company who archive email messages. UDP Archiving provides effective ways such as Outlook plug-in to help employees with a direct restore ability. In a single company, this helps employees directly access their emails and allows the IT admin to focus on other important tasks without having to worry about serving such restore requests.

Multiple Company or Multiple Organizational Unit Deployment

Multi-tenant lets large enterprises manage divisions and locations as separate archives. Organizations with multiple divisions can group users by domain. UDP Archiving helps managing different user groups with different policies and tracking usage for internal billing or adjustments. Managed service providers (MSPs) benefit by being able to support multiple clients that require separation of policy management and storage.



Roles Assigned:

- **Super admin:** Refers to the role that assists to manage domains, create and manage administrators who would interact with the system, managing licenses of organization, and more. This role does not have access to the end user data and is more useful in management.

- **Administrator:** Refers to the role that handles reporting and monitoring, setting up retention policies, providing access rights, managing licenses of users, and so on. Administrators cannot access company messages.
- **Compliance Officer:** Responsible for data protection of all users of an organization. Administrator creates the Compliance officer whose role is to purge the emails of user.
- **Auditor:** Auditor is the role created by the company administrator primarily for compliance audit. In UDP Archiving, this role has full access to emails of all users whose emails are being archived and can search messages or export them as corporate records for further use.
- **Employees:** Employees refer to all individuals of company who archive email messages. UDP Archiving provides effective ways such as Outlook plug-in to help employees with a direct restore ability. In a single company, this helps employees directly access their emails and allows the IT admin to focus on other important tasks without having to worry about serving such restore requests.

User Roles and Access Levels

UDP Archiving is accessible to four types of users. The access level of system varies for every user. Following users can perform tasks related to UDP Archiving:

Role Name	Created By	Key Functions	Comments
UDP Admin	Credentials Shared With Deployment Package	Manages Key functions outside UDP Archiving Console. For example, migration of emails, Offline License activation, and manual installation of updates.	Cannot access UDP Archiving Console. Super Admin can change password of UDP Admin from UDP Archiving Console.
Super Admin	Credentials received after completion of Set up during deployment.	• First user of an organization at UDP Archiving Console. Responsible for configuring UDP Archiving Console and creating profiles of Master Admin. • Manages licensing, migration of .pst files, installing UDP Archiving updates. • Manages customers, domains, message retrieval by SMTP, default behaviors such as Retention policy, system control, and support logs.	Cannot access company emails.
Master Admin	Super Admin creates one or more administrators assigning the role of master admin.	• Manages access rights for Compliance Officer, Auditors, and Employees. • Assigns licenses to users. • Imports mails to UDP Archiving Console. • Manages system health, retention policies, exception rules for one or more domains. • Can create more Master admin. • Can assign an employee as Group Manager	• Cannot access company emails. • Cannot buy licenses. • Cannot install updates.
Compliance	Created by Master	Responsible to ensure privacy of	Cannot create user

Officer	Admin	users and data by purging required emails.	or manage licenses
Auditor	Created by Master Admin	• Responsible for auditing • Can access emails of all employees • Can perform email search and export data • Responsible for management of corporate data	Cannot create user or manage licenses
Group Manager	Assigned by Master Admin	One of the employees is assigned the role of Group Manager. Responsible for managing emails of a group of employees.	Cannot create users
Employees	Created by Domain Master Admin	• Access emails through a web interface and Outlook folder • Tag emails • Search emails	Cannot control other users Cannot create users

Chapter 3: Using Arcserve UDP Archiving as Super Admin

The Super Admin role is designed to manage the infrastructure of the system, configure new customers (if multi-tenant), domains and more. As Domains are added, an Administrator role is created by the Super Admin which allows them to manage specific details of their Company/Domain requirements.

Super Admin can monitor and administer.

This section contains the following topics:

Personal Settings for Super Admin

Clicking your user name on the top-right corner of the UDP Archiving Console displays the **Settings** option.

The Settings page lets you update the following details:

Display Settings

Lets you define how content appears on your UDP Archiving Console.

Results Per page

Lets you define the number of results displayed on every page.

Language

Lets you set the preferred language for display.

Date Format

Lets you set the preferred display format of date.

Profile Picture

Lets you add a picture for your profile. Select a picture using the **Choose file** option and click **Upload**.

Change Password

Lets you reset your password. Enter the new password twice and click **Submit**.

Activate UDP Archiving License

This section describes how you can activate UDP Archiving licenses directly from the UDP Archiving Console. Activating license is possible even if the machine is not connected to Internet.

- Activating Licenses Online
- Activating Licenses Offline
- Extending Trial Period

Activating Arcserve UDP Archiving License Online

Using UDP Archiving, you can activate the product license directly from the UDP Archiving Console. Only Super Admin can activate the licenses for UDP Archiving.

For detailed steps, view Arcserve Licensing User Guide.

For viewing steps in video, click How to Activate Archiving License Online.

Activating Arcserve UDP Archiving License Offline

You can activate the UDP Archiving license even if you are not online. If your Arcserve product does not have access to internet, you are automatically redirected to offline activation.

The offline activation starts from the UDP Archiving Console, when you click **Activate** in the **Product Activation tab** of the **Activation and Licensing** dialog. UDP Archiving detects that an offline activation method is required and guides you in completing the offline activation.

Important: To complete the offline activation process on one machine, you must have internet access on another machine.

For detailed steps, view Arcserve Licensing User Guide.

Extending Trial

UDP Archiving lets you extend the trial version once. Extend trial appears when only 10 or less days are remaining for the trial period to expire. Using the Notification icon before Super Admin name on top of the screen, you can view the last date of trial version. For example, the notification displays the last date of trial.

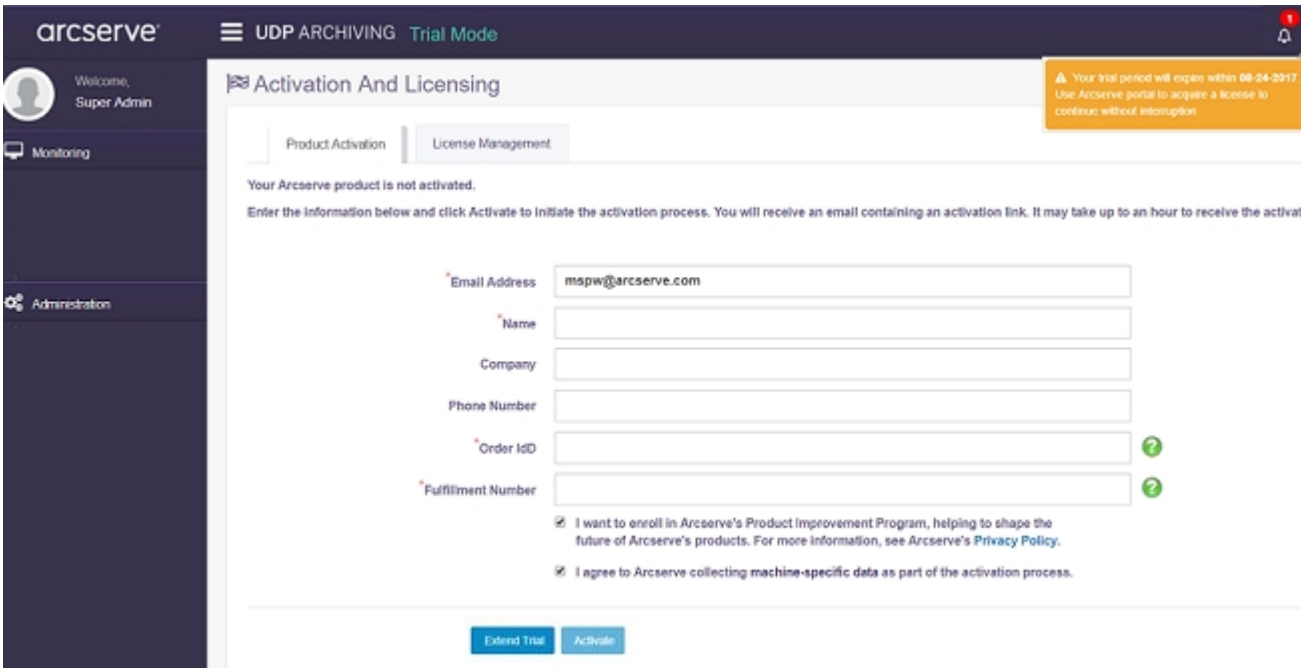
Follow these steps:

1. From the top-right corner of UDP Archiving Console, click the Super Admin icon.

   Multiple options are displayed.

2. From the list of options, click **Activation and Licensing**.

   The Activation and Licensing page is displayed. Details of the Product Activation tab is displayed.



3. From the **Activation and Licensing** dialog, enter the same **Email Address** that you have used before for UDP Archiving.
4. Click **Extend Trial**.

   Your trial duration for the Arcserve product gets extended.

Check Updates

Super Admin can update the system using the **Check for Updates** option. UDP Archiving lets you update online as well as offline. This topic describes procedures for both.

For viewing steps in video, click How to Install Updates of UDP Archiving.

Note: Before installation of an update, verify that the migration job is not running. To verify, use the command *sudo /etc/init.d/rc.migration status*. If a migration job is running, perform either of the following options:

- Wait till the migration job is complete to start installation of update.
- Manually stop the migration job to start installation of update installation. For more details, refer to Manage Migration.

Offline Update

If the UDP Archiving server does not have internet connection, you can manually download and install updates offline.

To download updates offline and to manually install, follow these steps:

1. Download the Update package (*.deb), readme.txt, lic98_Linux.tar from any machine that has internet access using the public link shared / communicated by Arcserve.

   Deb package: link

   MD5: cb26f1cea3809dfb0fcff2b8462d01c1

   Readme.txt: link

   MD5: 1d5261a973124e32b3a29c2795e9e9d9
2. Log into UDP Archiving machine as udp_admin.
3. Place / copy downloaded update package (*.deb), readme.txt, lic98_Linux.tar into */home/udp_admin*.
4. Navigate to the path */var/fas/www/utils/update* and run the following command to provide permissions to the file *manual_install.sh*:

   sudo chmod 777 manual_install.sh
5. Run the following command to manually install the package:

   sudo ./manual_install.sh

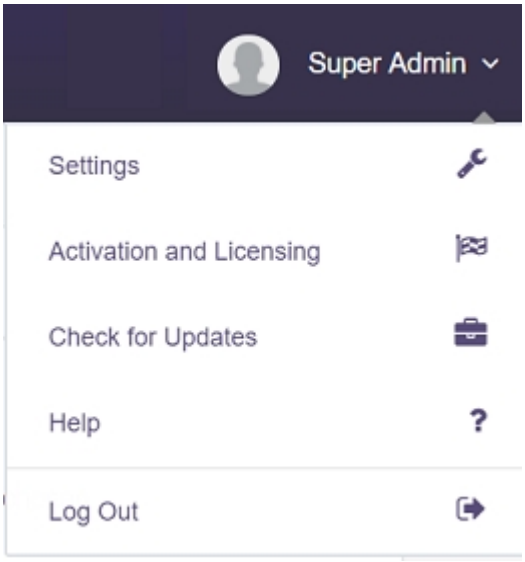
   Note: While installing the package if the public key is not available, the following message appears. This does not affect the installation.

The following signatures couldn't be verified because the public key is not available: NO_PUBKEY 85C25E95A16EB94D

Online Update

Follow these steps:

1. Click the Super Admin drop-down option.



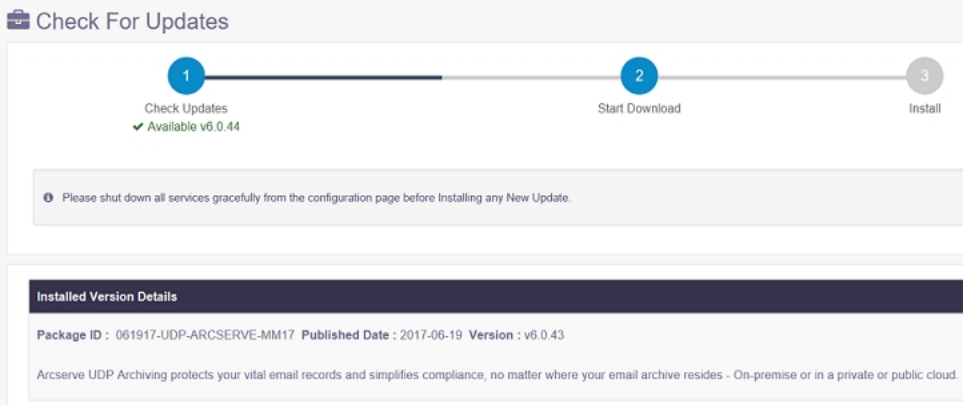
   The options for Super Admin appear.

2. Click **Check for Updates**.

   Check For Updates page appears displaying three steps: *Check Updates*, *Start Download*, and *Install*.

3. Click **Check Updates** to view the current and updated version.

   Checking for Updates dialog appears and displays versions available for download.



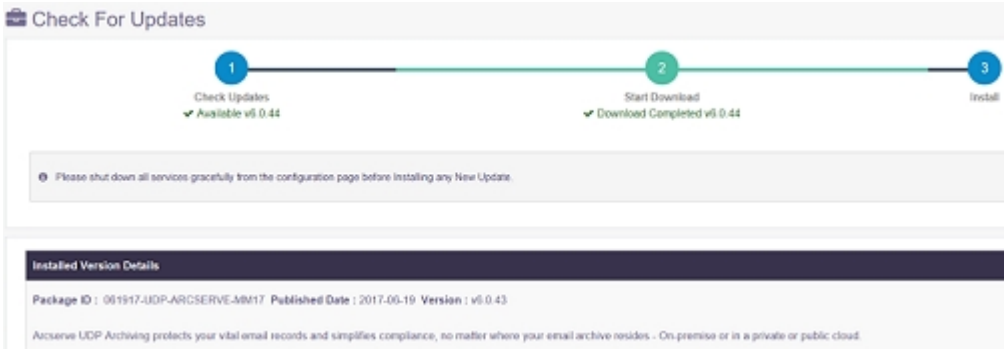
If UDP Archiving has further updates, **Available** message appears under **Check Updates**, and the *Start Download* option is enabled.

Note: We recommend to shut down other services before starting download. To shut down services, view Manage System Controls.

4. Click **Start Download**.

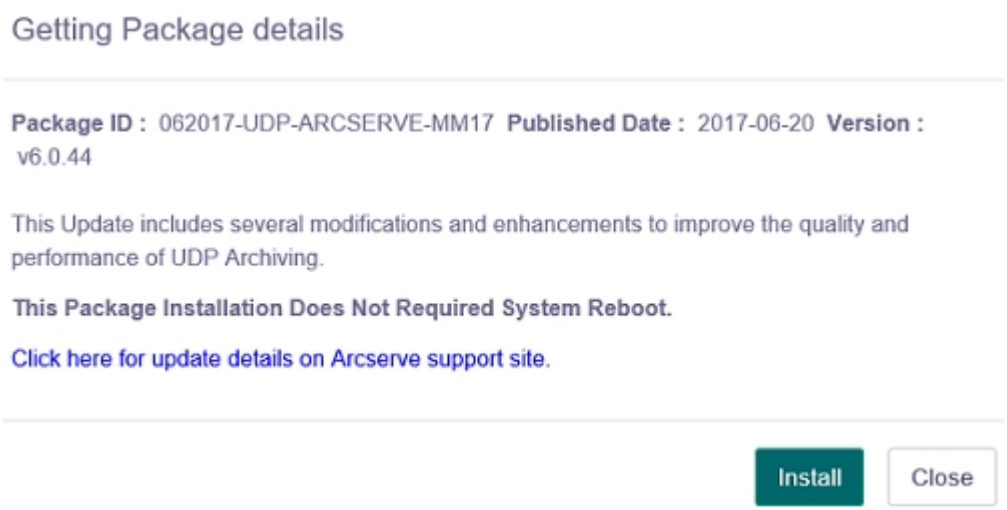
   Note: This option is enabled only if update is available.

   Downloading message is displayed. After completion, **Download Completed** message appears below **Start Download**.



5. Click **Install**.

   The **Getting Package Details** dialog displays the package information.



   Note: You can perform the update immediately or later based on the restart information provided in the dialog.

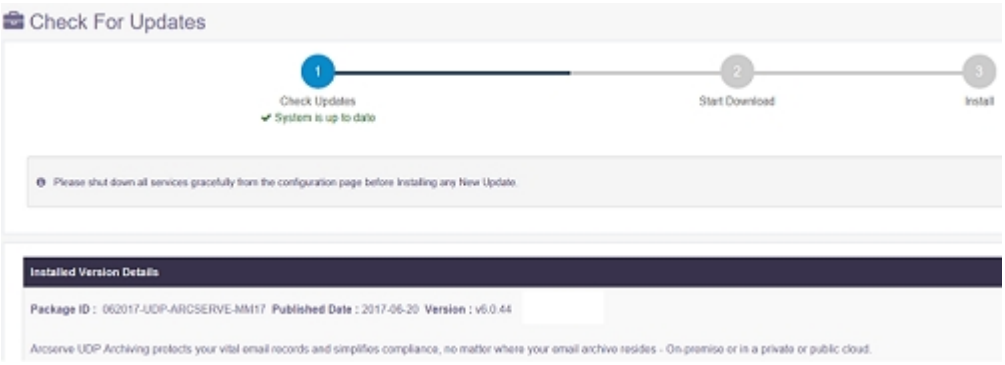
6. From Getting Package Details, click **Install** to update immediately.

   The **Successfully updated** message informs that the *update has been completed successfully*.

7. Click **Close** the Success message and verify if the update is successfully installed.

   Check for Updates page closes and you are automatically led to the **Health** dashboard where the version number of the latest update is visible on the top.

8. Return to the **Super Admin** drop-down option and click **Check for Updates**.



In the Check for Updates screen, below **Installed Version Details** you can match the last installed version. To verify if the system has latest updates, click **Check Updates** and the following message confirms that the last update was successful:

System is up to date

Monitor

Super Admin monitors Health, Statistics, and Message audit.

View Health

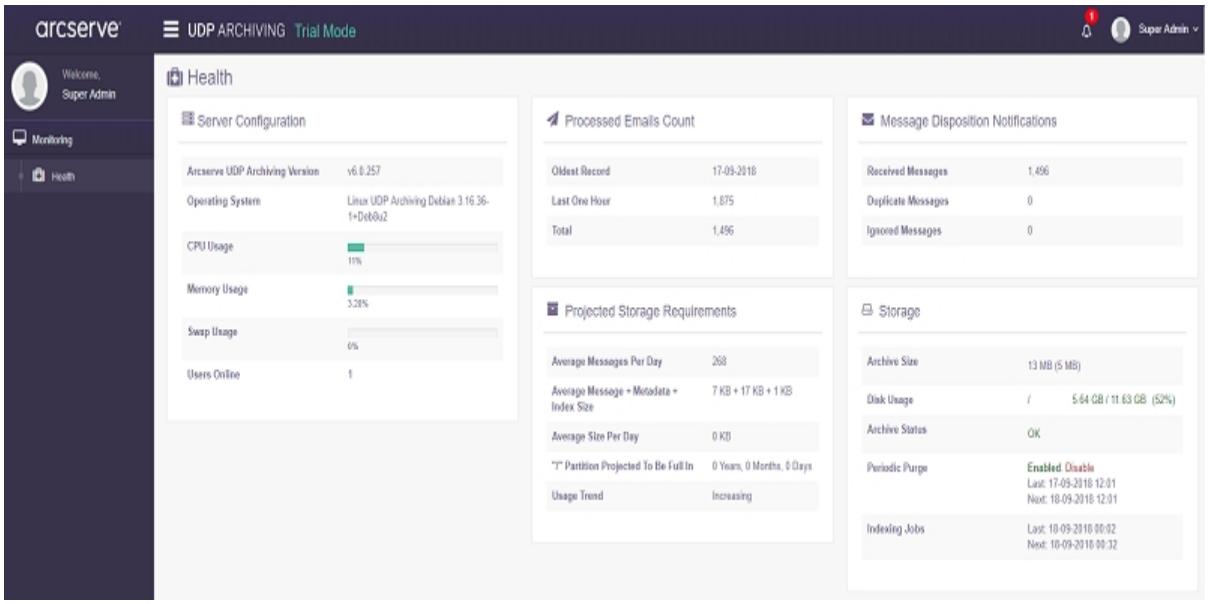
The Health monitor displays information about the health of the infrastructure as well as the flow of messages from all configured domains.

- **Server Configuration** provides details about UDP Archiving server. For example, version number, operating system, usage of CPU, memory, Swap, and Users Online.

  Note: Click the number displayed for **Users Online** in the *Server Configuration* section to view details. **Users Online** page opens and displays details about user activity.

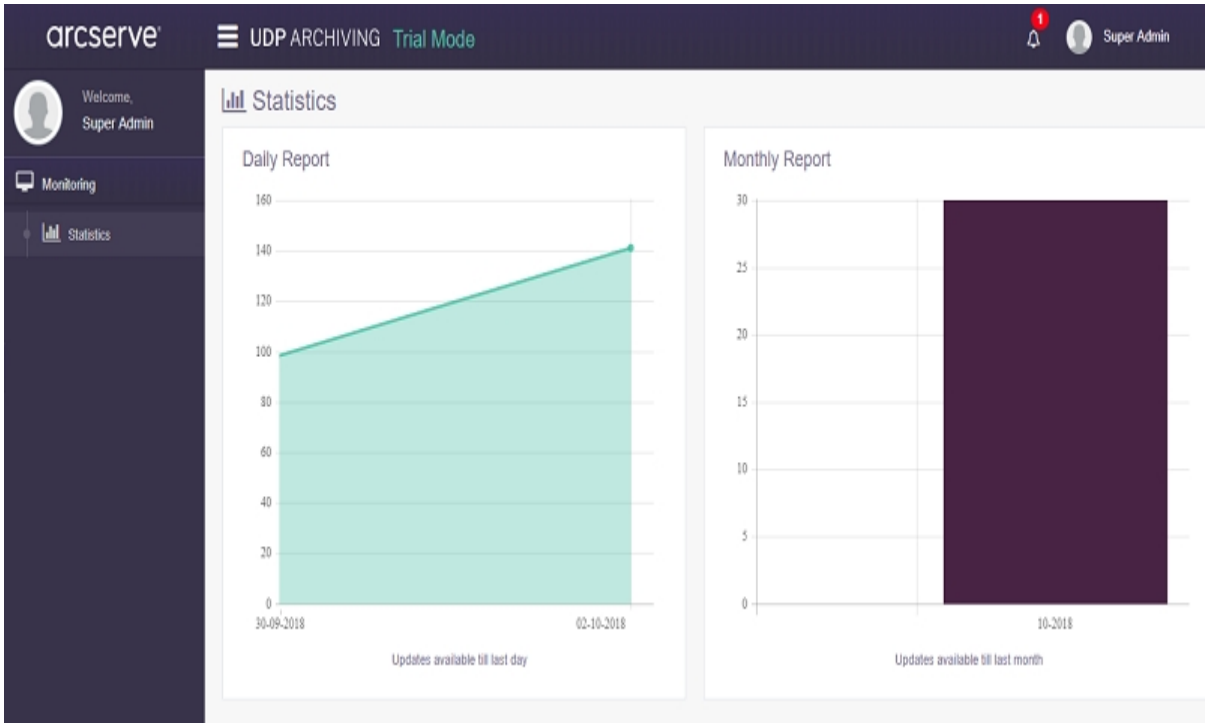
- **Processed Email Counts** displays oldest record and count of processed emails ranging from an hour to multiple days.
- **Message Disposition Notifications** displays data about received, duplicated, and ignored messages.
- **Projected Storage Requirement** displays inflow of messages, storage consumed and projection.
- **Storage** displays details about archive size, disk usage, archive status, periodic purge, and indexing jobs.

  Note: You can use the options to Enable or Disable periodic purge.



View Statistics

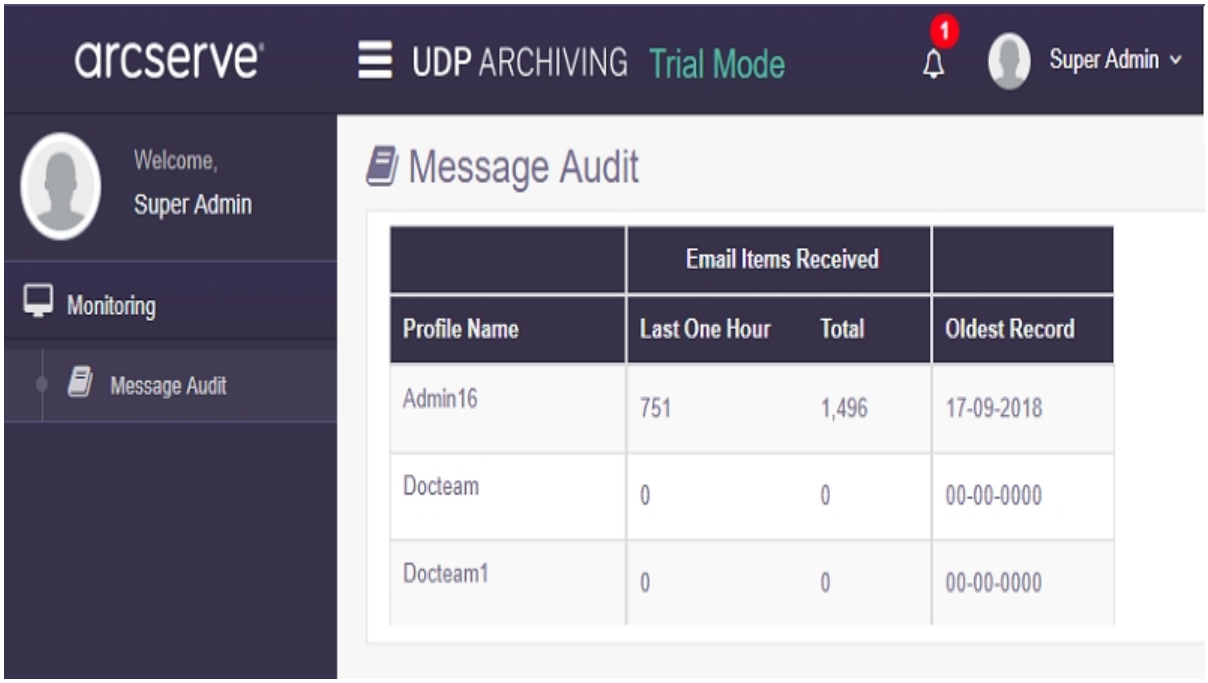
The statistics reports show the daily and monthly flow of all messages in UDP Archiving.



View Message Audit

Message Audit provides a quick view of messages received in the last 60 minutes and overall count of the messages received. The Oldest Record option displays the date on which the oldest record was received for the corresponding profile. This option provides only a quick view to analyze how the archive is growing for each configured domain.

Note: Super Admin cannot access the messages.



Administration

The Administration section lets you configure a company or multiple companies or organizational units with different email domains. In a single customer environment, only one customer is configured.

For viewing steps in video, click How to Configure UDP Archiving after Deployment.

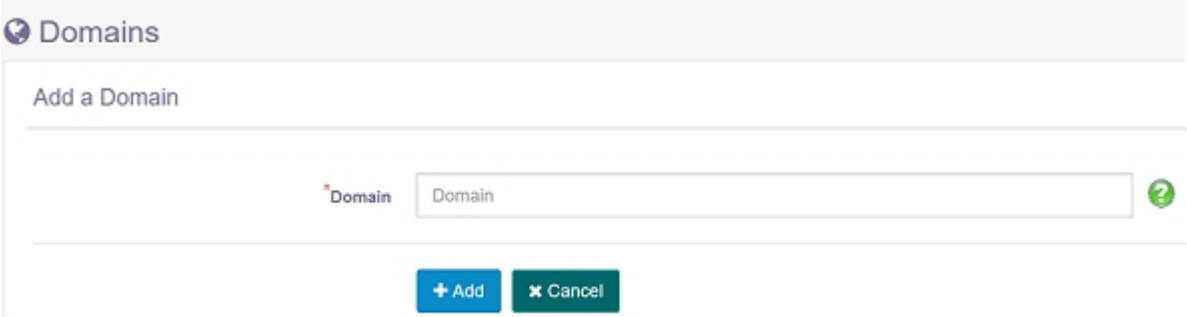
Using this section, Super Admin can manage the following requirements:

- Domains
- Profiles
- Administrators
- Configuration
- Migration

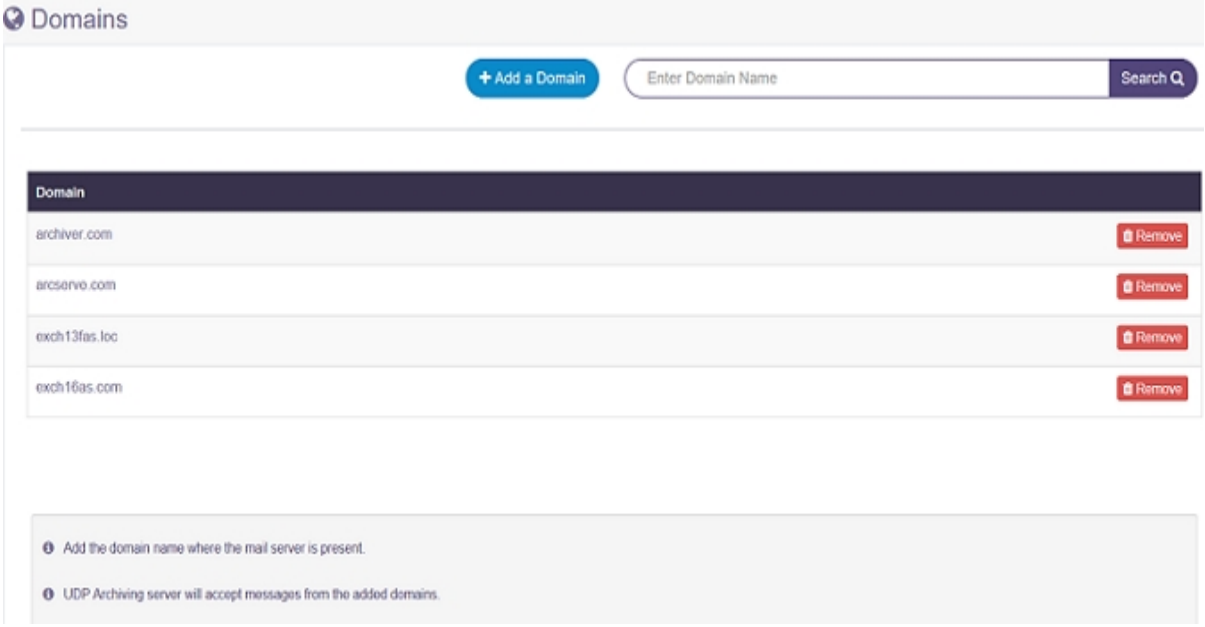
Managing Domain

Using Domains, Super Admin can add, delete, and search a domain. For example, you can add each domain for your company. For a service provider, add domains for each of your archiving customers. If you have a domain (Example: arc-serve.com) from where mail comes, Super Admin needs to set up this domain in the system. This process also lets UDP Archiving to accept messages from these domains that reach UDP Archiving over SMTP.

All customer domains are entered into the system and the process directs SMTP to accept messages from these domains.



Below is a summary of all domains in the UDP Archiving.



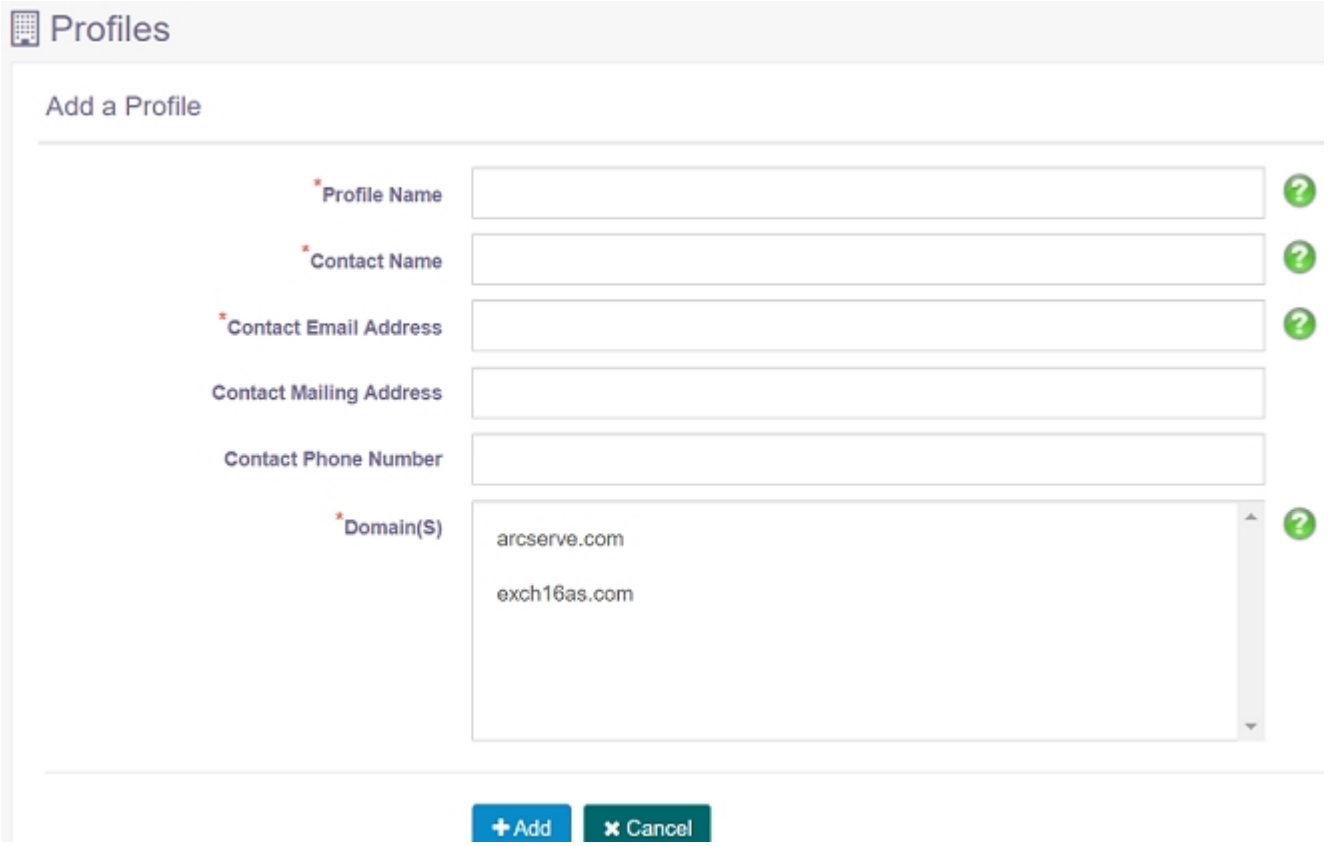
You can remove a domain if not required.

Profiles

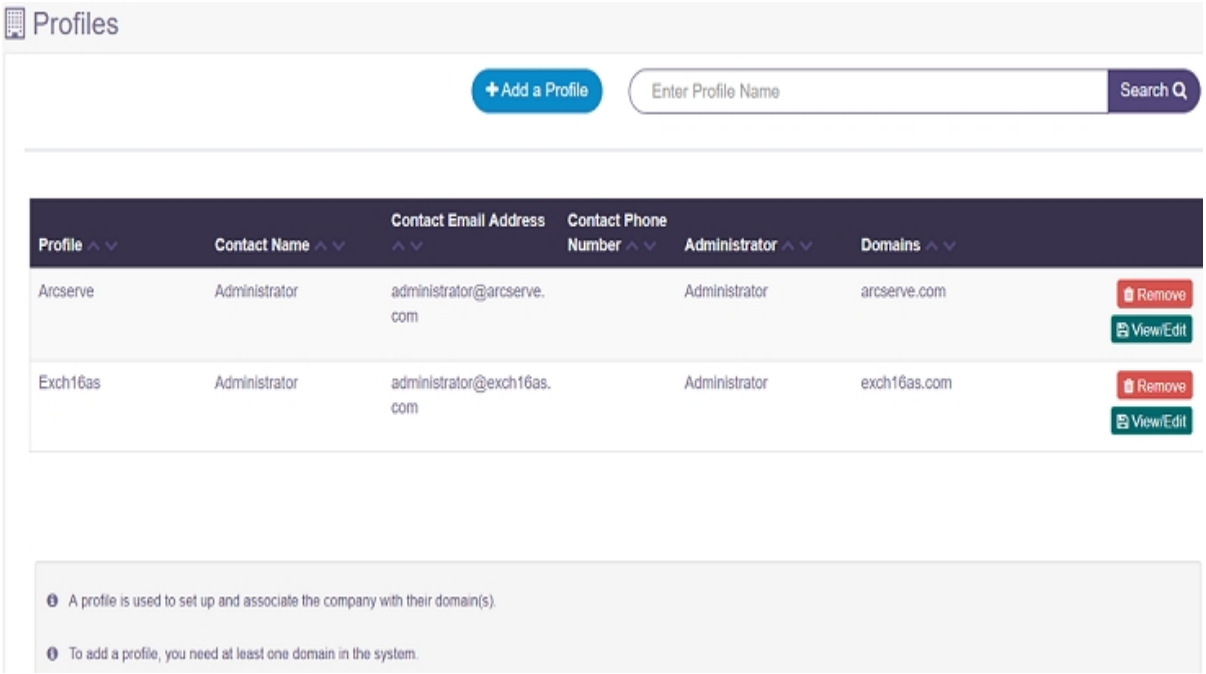
A profile is used to set up the company and associate the company with their domain(s). Using Profiles, Super Admin adds a profile for a company or in case of a service provider a separate profile for each customer.

To add a profile at least one domain is required. For multi-tenancy or while setting up different organizational units with different domains, Super Admin will add a new profile for each.

If a user has multiple aliases and domains, add multiple domains to the profile.

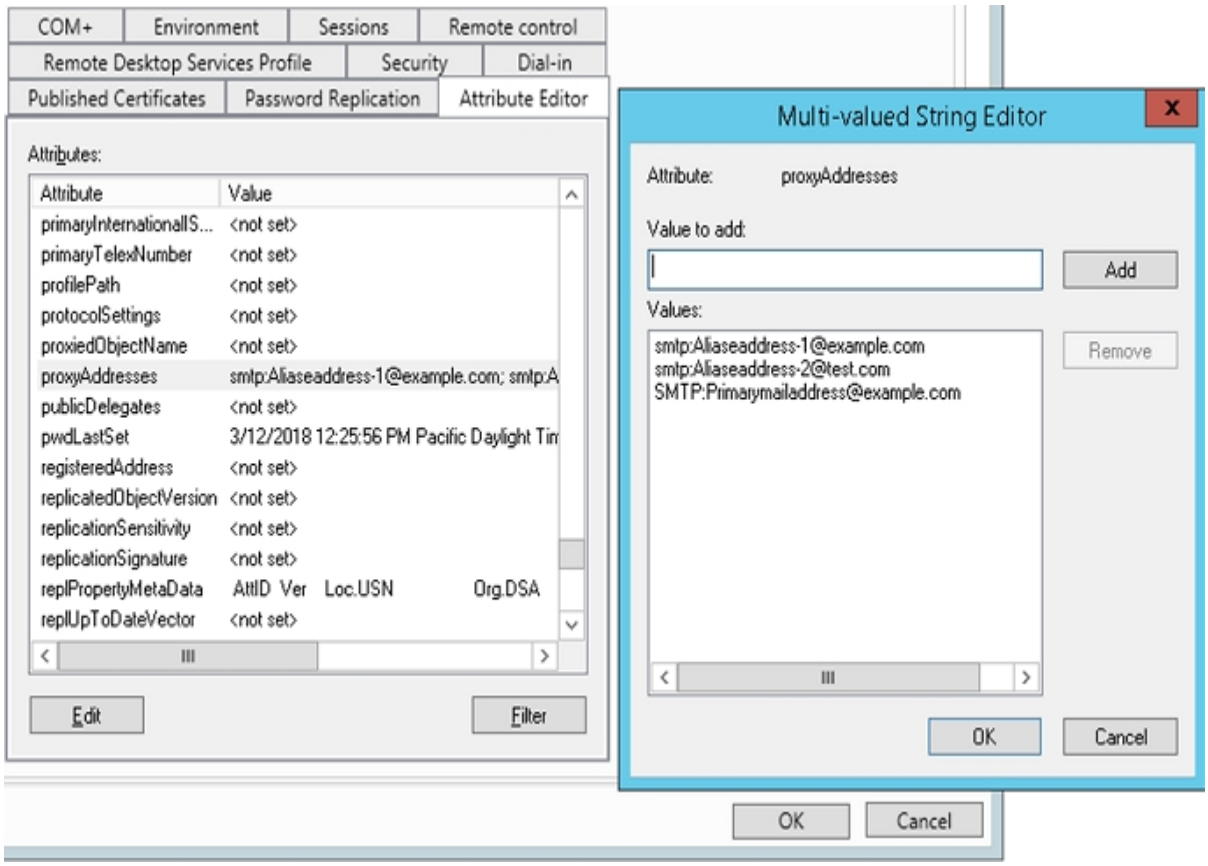


Below is a summary of all profiles.


Profiles
+ Add a Profile
Enter Profile Name
Search
Profile
Contact Name
Contact Email Address
Contact Phone Number
Administrator
Domains
Arcserve
Administrator
administrator@arcserve.com
Administrator
arcserve.com
Remove
View/Edit
Exch16as
Administrator
administrator@exch16as.com
Administrator
exch16as.com
Remove
View/Edit
A profile is used to set up and associate the company with their domain(s).
To add a profile, you need at least one domain in the system.

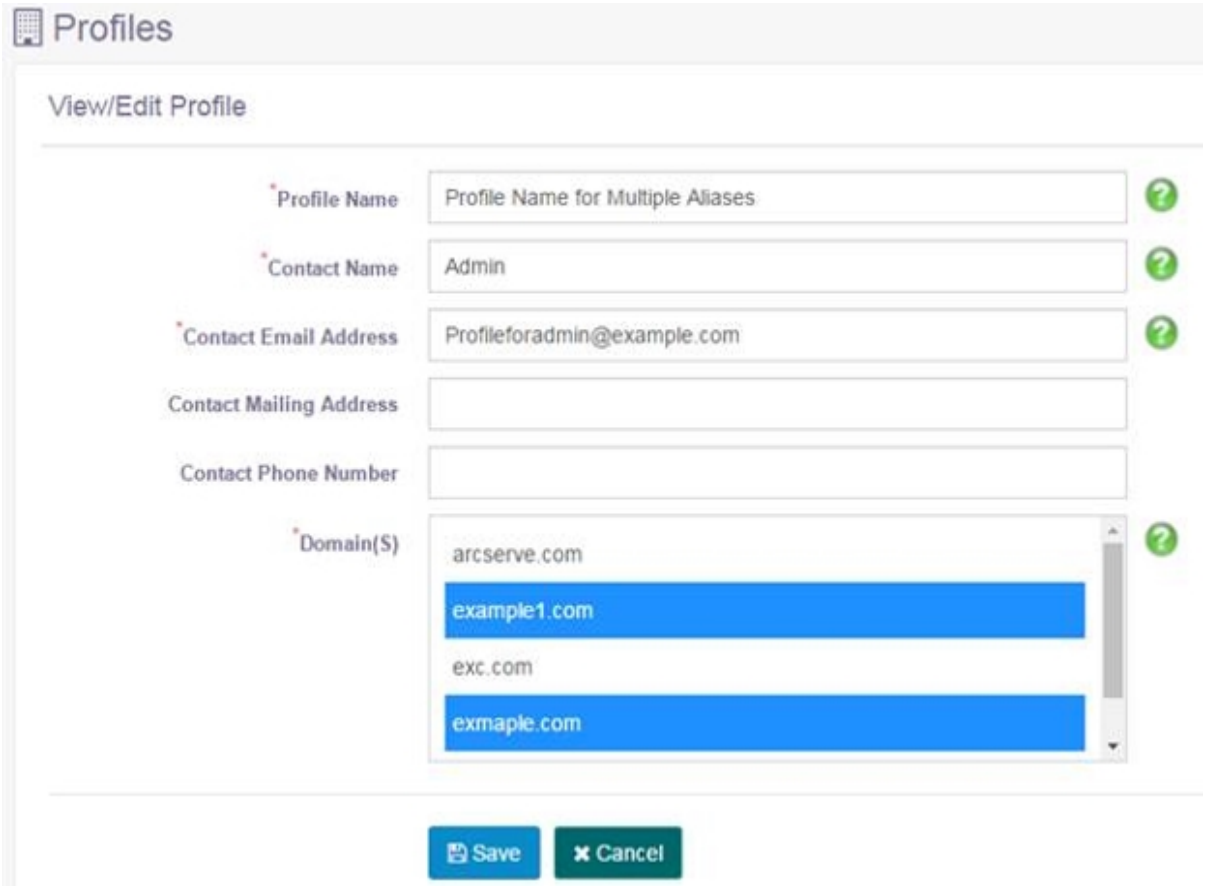
Adding Email Aliases to a Profile

A user can have a primary email with multiple aliases that are archived in UDP Archiving Solution. To display emails of the user from primary email and all aliases, you need to update the primary email at Active Directory (AD) with all the Aliases as ProxyAddresses followed by *smtp* in the lower case.



After updating AD profile with all the Alias addresses, UDP Archiving displays all the emails related to that particular user if administrator authenticates with the LDAP account.

If the domain of Aliases is different from the Primary Mail Domain, then you need to map the Profile with all the domains in UDP Archiving.

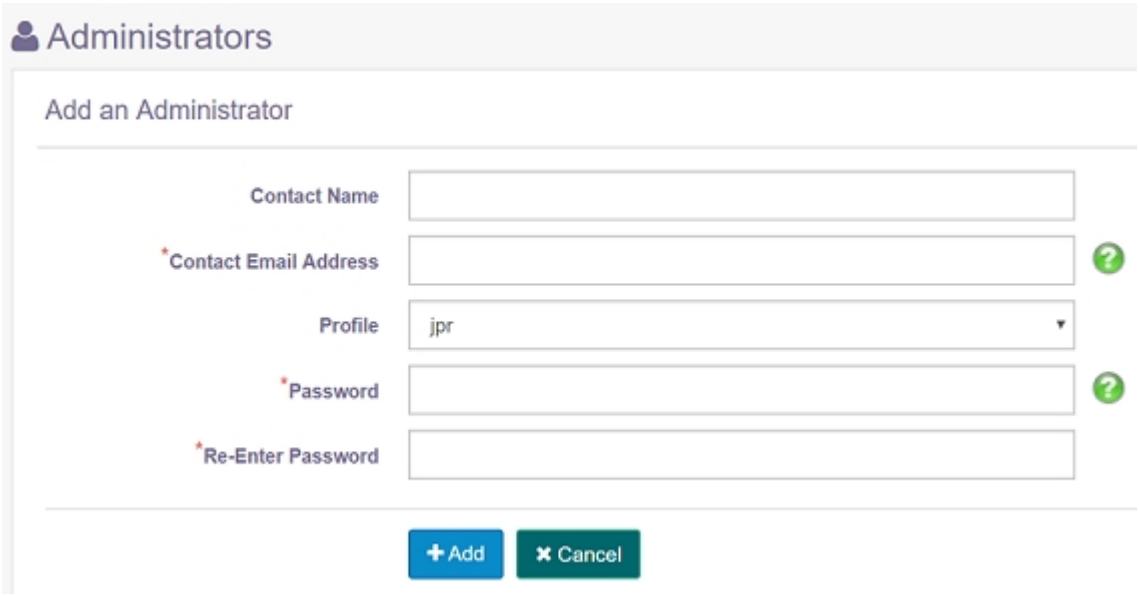


Now, emails of the user from all domains are archived.

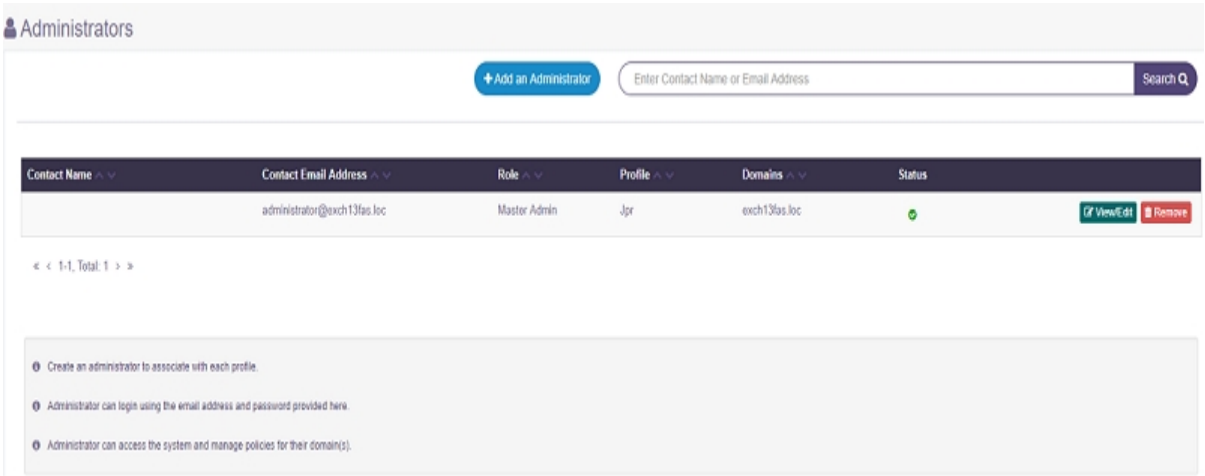
Manage Administrators

Super Admin creates administrators to associate with each profile and domains. The credentials are given to the administrator to access the system and manage policies for assigned domain(s).

For each profile, Super Admin creates the first Administrator with an email address and password. The credentials are used by the profile administrator who then adds policies, users and other functions specific to archiving requirements of respective profiles. The profile detail is also required to create an administrator.



Below is a view of all the Administrators created by the Super Admin for each Profile.



Manage Configuration

On the configuration screen, Super Admin can perform the following action:

- Specify Settings
- Email Retention
- Export Encryption Keys
- Increase Storage disk
- Specify Email Configuration For Alerts And Exported Encryption Keys
- Control Systems
- Access Controls
- Upload SSL Certificates

Specify Settings

On the configuration screen, Super Admin can perform multiple actions. This section describes how to specify settings for domain and emails.

The Settings section includes the following fields:

Fully Qualified Domain Name / IP Address

Refers to the domain of UDP Archiving that you set up during installation.

SMTP Forwarding Email Address

Refers to the email address that you use to forward messages via SMTP from your mail server to your UDP Archiving. According to your mail server, use your Instance Domain or archive@Instance domain (example: archive@arcserve1.com).

Security

Refers to spam security. For additional security to prevent computer generated attacks against the system, enable Captcha. As a result, while logging in all system users need to enter the displayed security code.

Specify Email Retention Period

On the configuration screen, Super Admin can perform multiple actions.

For viewing steps in video, click How to Manage Retention Rules.

From Configuration screen, using this option Super Admin can set the default number of days to retain messages of everyone in the organization.

Email Retention

Using Days to Retain Messages option, Super Admin can specify number of days for Email Retention. If administrators do not set Domain Level Retention Policy, then the Global Email Retention becomes the default. For more information, see Manage Retention Rules.

Export Encryption Keys

The **Export Encryption Keys** feature helps you prepare for disasters when the encryption keys gets corrupt and you are unable to access the archived data in the absence of backup.

Important! Complete Email configuration for the sender ID (not for receiving ID) to use Email Encryption Keys option. For more information, view Email configuration for alerts.

Need to back up Encryption Key

All the incoming archived messages are encrypted and encryption key is generated. While the encryption keys continues to encrypt archived message, at times the keys get unusable due to multiple reasons. You can identify such issue with keys when the displayed archived messages show abnormal behavior. For example, some of the messages appear blank. If the encryption key becomes unusable, you cannot access the archived messages.

How does Email Encryption Keys Help!

Using the Email Encryption Keys feature, you can take backup of your encryption keys. Just enter an email address of your choices and click **Send**. The receiver (owner of that email address) receives two files from UDP Archiving. Save those attachment (or the complete email) at a safe location.

Later if your encryption keys becomes unusable, you can simply call Arcserve Support team, provide details of encryption key and get the data restored.

To email encryption keys, follow these steps:

1. Log into UDP Archiving as Super Admin.

   The UDP Archiving Console appears.

2. From the left pane, click **Configuration**.

   Configuration screen appears with multiple options where one of the options is Export Encryption Keys.

3. In the **Export Encryption Keys** section, provide an email address.

   The receiver's email address is of your choice and does not need to be linked with UDP Archiving.

4. Click **Send**.

   The entered email address receives encryption keys from UDP Archiving.

Save the attachments available in the email. When the encryption keys get corrupt, share the attachments with Arcserve Support to restore.

Increase Storage Disk Space

On the configuration screen, Super Admin can perform multiple actions. This section describes how to increase storage disk.

From Configuration screen, using the following two options Super Admin can increase the storage of UDP Archiving:

- Add New Volume
- Extend Volume

Add New Volume to Increase Storage Disk Space

On the configuration screen, Super Admin can perform multiple actions. This section describes how to increase storage disk.

From Configuration screen, Using Add a New Volume option Super Admin moves existing email and application data to new volume and increase the storage of UDP Archiving.

Important! You can add a new volume only once. After using the function once, the **Add a New Volume** button is disabled.

Note: If multiple disks are available, then only the disk that was added first is considered for creating a new volume on clicking Add a volume.

Follow these steps:

1. (ESX or Hyper-V) Switch off the Virtual Machine and add a virtual hard disk in your virtual machine environment and link with your UDP Archiving. For example, create a virtual hard disk with 200 GB.

   Note: Reboot Archiving machine after adding disk. Without restart, UDP Archiving server may not recognize the new disk.

2. Log into UDP Archiving Console as Super Admin.
3. Navigate to the **Configuration** tab and click **Add a volume**.

   Within few minutes new volume is added and confirmed through a pop-up dialog.

   New volume is added.

   Notes:

   - If the root disk has more than 50 GB data, you cannot add new volume. To add a new volume, contact Arcserve Support.
   - If the volume with required storage is not available in the virtual machine, then volume is not added and unsuccessful message appears.

To check the usage details of the newly added volume, you can use one of the following options:

- Navigate to the Configuration page and from the Storage pane view the usage details of both root as well as archiving volumes.
- Navigate to the Health tab and from the storage pane view the usage details of both root as well as archiving volumes.

Extend Volume to Increase Storage Disk Space

On the configuration screen, Super Admin can perform multiple actions. This section describes how to increase storage disk.

From Configuration screen, using the Extend Volume option Super Admin can increase the storage of UDP Archiving.

Important! You can extend the size of root (/) disk to maximum 15 TB and /archiving disk to maximum of 64 TB.

Follow these steps:

1. Add a virtual hard disk in your virtual machine environment and link with your UDP Archiving. For example, create a virtual hard disk with 200 GB.

   Note: Reboot Archiving machine after adding disk (for VMware OVF deployment only)

2. Click **Check Disk**.

   Your UDP Archiving verifies availability of 200 GB disk that you created. If available, you are prompted to verify LVM.

3. Click **Check LVM**.

   Note: When the LVM check passes and if a volume is already created then a drop-down list appears where you need to select a partition to expand.

4. Click **Increase disk**.

   The storage space is increased.

Specify Email Configuration For Alerts and Exported Encryption Keys

From the Configuration screen, using **Email Configuration For Alerts And Exported Encryption Keys** feature Super Admin can define details required to receive storage alerts.

Storage alert is sent as email messages when the storage disk approaches full capacity. You receive alert emails daily when the storage used level reaches 80% of the capacity. If the storage used level reaches 90% of full capacity, messages are not archived. To continue archiving of messages, you need to increase storage space.

Important! Microsoft Exchange retries to send new messages for archiving by default for 2 days. If the disk is full for those two days, then the messages are returned without archiving. Even after starting the increase disk process, to avoid such situation login to MS Exchange and modify the default number of days.

You can configure storage alert fields to define the email of senders and recipients.

Follow these steps:

1. Select an Email Service from the **Service** drop-down options.

   UDP Archiving lets you select from multiple options. For example, Google Mail, Yahoo Mail, and Others.

2. Enter **port** number.

   Note: For Office 365, use port number 587 or 25.

3. Enter **Email Server**.

   For example, smtp.gmail.com if the Email service is Google Mail. For Office 365, use email server name as Outlook.office365.com or smtp.office365.com.

4. For Office 365, Google Mail, Live Mail, and Yahoo mails , select the check box of **Requires authentication** and verify if the option for **send STARTTLS** is selected.

   Note: For On-premise Exchange server, verify that neither **Use SSL** nor **Send STARTTLS** option is selected.

5. Enter **Account Name**.

   Note: Required only when you select the check box of **Requires authentication**.

6. Enter **Password** of the application for the account name provided as sender's email.

   Note: Required only when you select the check box of **Requires authentication**.

7. Enter description for **Subject**.

8. In **From**, enter email ID of sender.

   Email ID in From field can differ from email ID in Account name.

   Important! Do not use the following characters: ':', ';', ',', '[', '\', ']', '<', '>', ' (', ')', "

9. In **Recipients**, enter email ID of receiver.

   Important! Do not use the following characters: ':', ';', ',', '[', '\', ']', '<', '>', ' (', ')', "

10. Click **Send a test Email** to verify if the email is sent from sender's email.

11. Click **Save**.

    UDP Archiving is configured to send the storage alerts to the recipients email.

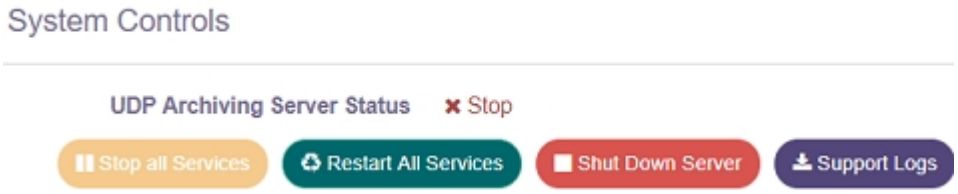
Manage System Controls

On the configuration screen, Super Admin can perform multiple actions.

Using System Controls feature, Super Admin can perform the following options:

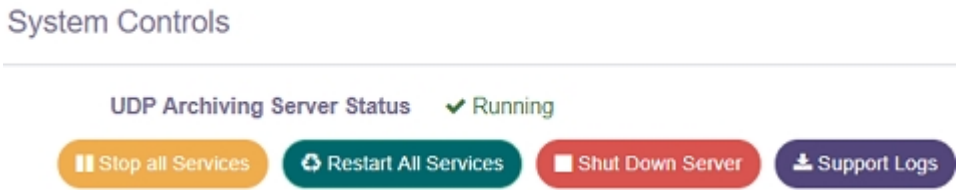
- **Stop all Services**

  Using this option, when required you can stop all services. For example, while installing UDP Archiving updates. When stopped, UDP Archiving Server Status appears as **Stop**.



- **Restart All services**

  Using this option, you can restart all services. For example, while installing UDP Archiving you stop all services and then you need to restart all services after installing updates. When restarted, the UDP Archiving Server Status appears as **Running**.



- **Shut Down Server**

  Using this option, when required you can shut down UDP Archiving server. After shutting down the server, you cannot use UDP Archiving Console.

  Important! To restart server, contact your system administrator.

- **Support logs**

  Using this option, you can download and view all the available logs. Click **Support Logs**, download the *support-logs.zip* and extract the files.

  You can view logs for the following options:

  - **UDPArchiving:** Contains UDP Archiving application logs that provide information about the LDAP test connection errors, license notifications, and statistics of processed Emails and reports.

- **fas:** Contains UDP Archiving application logs that provide information about the SMTP server including pool of children processes to handle SMTP requests.
- **fasconf:** Contains UDP Archiving application logs that provides information about querying UDP Archivingconfiguration logs from a configuration file.
- **fasexport:** Contains UDP Archiving application logs that provides information about exporting Emails from UDP Archiving.
- **fasget:** Contains UDP Archiving application logs that provides information about Email and related attachment retrieval
- **fasgetd:** Contains UDP Archiving application logs that provides information about managing SMTP requests.
- **fasimport:** Contains UDP Archiving application logs that provides information about importing Emails to UDP Archiving system.
- **faspurge:** Contains UDP Archiving application logs that provides information about purging Emails from UDP Archiving.
- **message:** Contains general system activity logs, such as logs of valuable non-debug and non-critical messages.
- **mysql:** Contains Debian system logs that provides information about MySQL database logs.
- **ngnix:** Contains Debian system logs that provides information about NGINX web service.
- **reindex:** Contains UDP Archiving application logs that provides information about re-indexing the messages stored in UDP Archiving.
- **searchd:** Contains Debian system logs that provides information about Searchd daemon (Sphinx search).
- **storage_usage:** Contains UDP Archiving application logs generated while tracking the System Storage usage.
- **syslog:** Contains logs of all activity of the system except authentication-related messages.
- **ewsImport:** Contains logs of all details of all the mailboxes and the folders that are imported from the mail server to UDP Archiving server.
- **ewsSchedule:** Contains logs related to the scheduled ewsImport job.

Reset Password

On the configuration screen, Super Admin can perform multiple actions.

From Access Controls, using this option Super Admin can modify the default password of UDP Admin.

Important! Super Admin must modify the passwords of superadmin and udp_admin immediately after the first login as other users may have access to the default password.

Follow these steps:

1. From the Access Controls section, click **Reset Password**.

   A box appears where you can enter password.

2. Enter desired password and click **Reset**.

Upload SSL Certificates

UDP Archiving lets you secure the connection using SSL Certificates. Upload the private key with the intermediate and root SSL Certificate. Before uploading, you must complete the following prerequisites:

- Generate a certificate signing request (CSR) from the server
- Purchase certificate using the CSR file

After completing the prerequisites, you can upload the SSL certificate files.

Follow these steps:

1. Login as super admin in UDP Archiving and navigate to the **Configuration** page.
2. Navigate to the **SSL Certificate** pane.

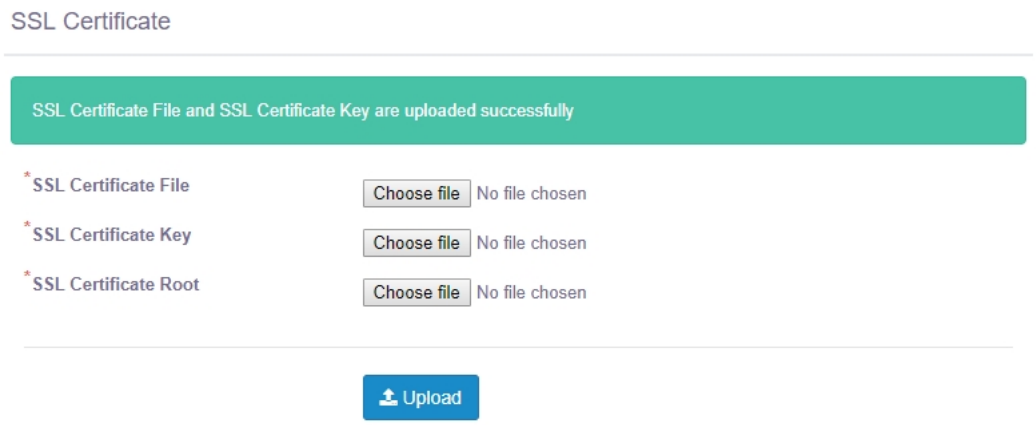
   The pane displays three fields to select files and upload.
3. Click **Choose file** and select the appropriate files for the following three fields:
   - SSL Certificate File

     Note: If the certificate authority provided root and intermediate certificates separately, then combine the root certificate followed by intermediate certificate as a single .crt file in the order which the certification authority suggests and select in the SSL certificate File option to upload.
   - SSL Certificate Key

     Note: The key file refers to the udpprivatekey.key generated with CSR.
   - SSL Certificate Root

     Note: Select the root certificate provided by the certificate authority.
4. Click **Upload**.

A message confirms successful upload.



All the files are uploaded and the http connection is now secured.

Generate a Certificate Signing Request (CSR) from the Server

You need to generate a CSR from the server to get a root and intermediate certificate required for SSL Certificate upload.

Follow these steps:

1. Open the UDP Archiving instance using putty and login as udp_admin.
2. Create and enter a directory to generate the private key and the CSR.

   For example,

   sudo mkdir /CSR

   cd /CSR
3. Run the following command to generate key for the server:

   sudo openssl genrsa -out udpprivatekey.key 2048
4. Run the following command to generate CSR using this key:

   sudo openssl req -new -key udpprivatekey.key -out udparchiving.csr

   Note: The command prompts for your organization and common name (FQDN or domain), locality, and country. Enter your FQDN as Common Name. Avoid filling details for password, optional company name, and email fields.
5. Use this CSR file to order SSL from CA (Certificate Authority).

You will receive certificates from the CA (Certificate Authority). Use the key and certificates to upload on UDP Archiving.

Manage Migration

Using Migration, you can migrate the historical data to UDP Archiving. If you have a PST file from an existing archive or exported from your mail server, use the UDP Archiving Migration utility to bulk migrate large amounts of emails. UDP Admin performs migration. Super Admin verifies if the migration is successful.

As a prerequisite, the mailbox data is first exported into the .PST file at a shared location. UDP Admin (not Super Admin) starts the migration job. These files are copied to the migration directory of the archiving machine (Using FTP tools, such as FileZilla, WinSCP, and so on). During the migration job, the data from the .PST files is read and archived.

Notes:

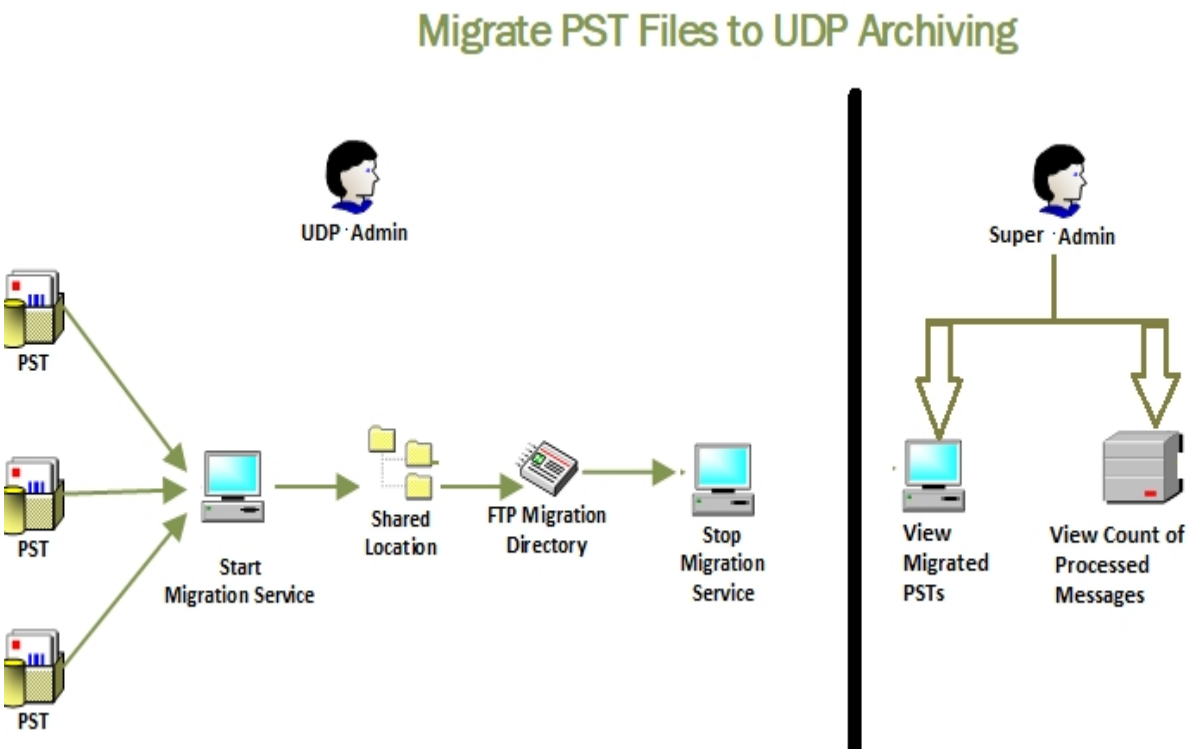
- When using WinSCP as FTP tools, you must update settings. For more information, see link.
- To export mailbox data to .PST files, see link.
- To export Gmail data to .MBOX files, see link.

Considerations

- For IBM Lotus Domino email service, first convert .nsf files to .pst file.
- Deduplication: When migrating a PST file again, the migration service imports only new messages of those files. Messages already imported during previous migration are not included.
- Policies: As message processes through migration all the existing retention, exception, and legal hold policies are applied.
- Avoid delays in migration process: As large size of .pst files delay the migration process, we recommend to use .pst files of size 5-10 GB.
- Verify .pst files for faster migration: Type of .pst file used for migration may make the migration slower. To complete migration faster, we recommend to verify the fasimport.log file and find the reason.
- When migrating the .pst, .zip, or .tar.gz files, the available disk space in the target machine must be twice the size of the source file.
- To migrate historical .eml and .pst files, you can also use .zip or .tar or tar.gz formats for compression and can place them in the migration folder for migration.

Important! Only import or migration of emails does not make the user licensed. Only licensed user can view the emails. To view the emails in Auditor/Employee user roles, the user (Auditor/Employee) must send at least one email.

Migration Process Flow



Follow these steps:

1. Using UDP Admin login, start Migration services in Command Line using the following:

   sudo /etc/init.d/rc.migration start

   Note: Verify the service status when desired using the following command:

   sudo /etc/init.d/rc.migration status

2. Using FTP Client, upload the .pst file that you want to migrate to the following path on the default volume at the UDP Archiving server:

   /var/fas/www/migration/

   Note: To upload files, administrators must have completed prerequisite.

   Important! After adding the new volume, upload the .pst file that you want to migrate only to the following path on the new volume:

   /archiving/migration/

Any files uploaded to the path */var/fas/www/migration/* on the default volume will not migrate.

3. Stop the Migration service using the following command:

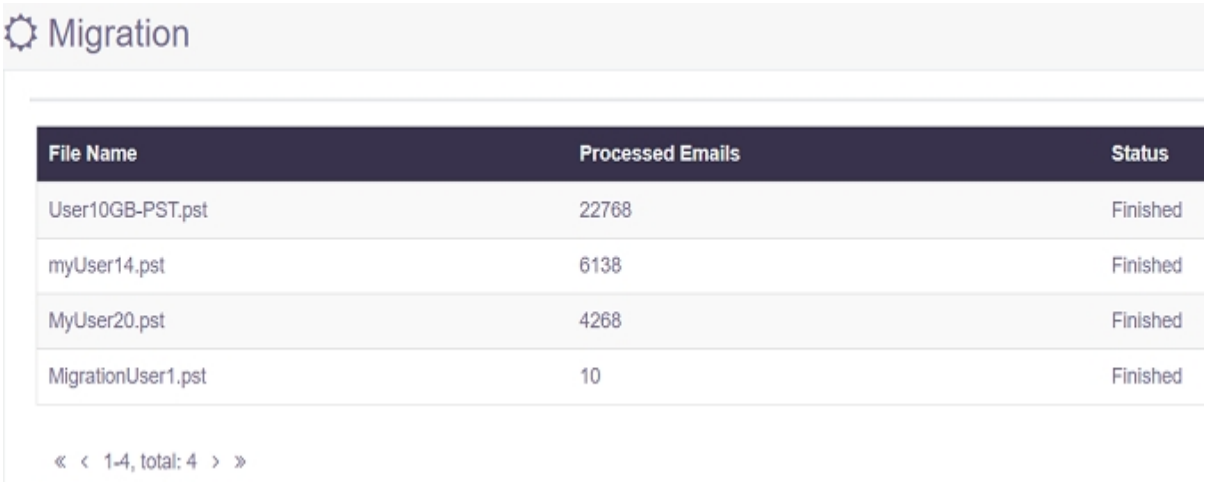
   sudo /etc/init.d/rc.migration stop

   Note: If not stopped after completion of migration, the service continues searching for files to migrate.

   The emails present in the .pst file are archived with the existing emails. Migration screen displays the name of .pst files and the status displays **Finished**.

4. To verify, log into UDP Archiving Console as Super Admin.
5. To view migrated .pst files, from the left pane of UDP Archiving Console click Administration>**Migration**.

   Migration screen is displayed.



6. To view count of processed emails, click Monitor>**Health** and the dashboard displays updated number of emails in the processed emails.

   Note: Apart from Super Admin, Administrator can also verify the count of messages using the **Dashboard** option.

After successful migration, all the migrated .pst files are deleted from the UDP Archiving server.

Migrate using WinSCP

When using WinSCP for transferring the files onto Migration folder, you need to update WinSCP settings before starting the migration process.

Follow these steps:

1. Navigate to **Options**, **Preferences**.
2. From Preferences, click **Transfer, Endurance**.
3. From Endurance screen, disable the option **Enable transfer resume/transfer to temporary filename for**.

   After saving the updates, continue with the migration process.

Export Mailbox Data to .PST Files

Before starting migration from the UDP Archiving Console, administrators need to complete the prerequisite of exporting mailbox data to .PST files. Administrators can export the mailbox data into .PST files either by using Outlook or by using Exchange PowerShell commands.

Requirements:

- The shared folder should have Full Control rights granted for the *Exchange Trusted Subsystem* security group.
- The Organization Management role group should have the *Mailbox Import-Export*" role assigned. To assign, use using the following PowerShell command:

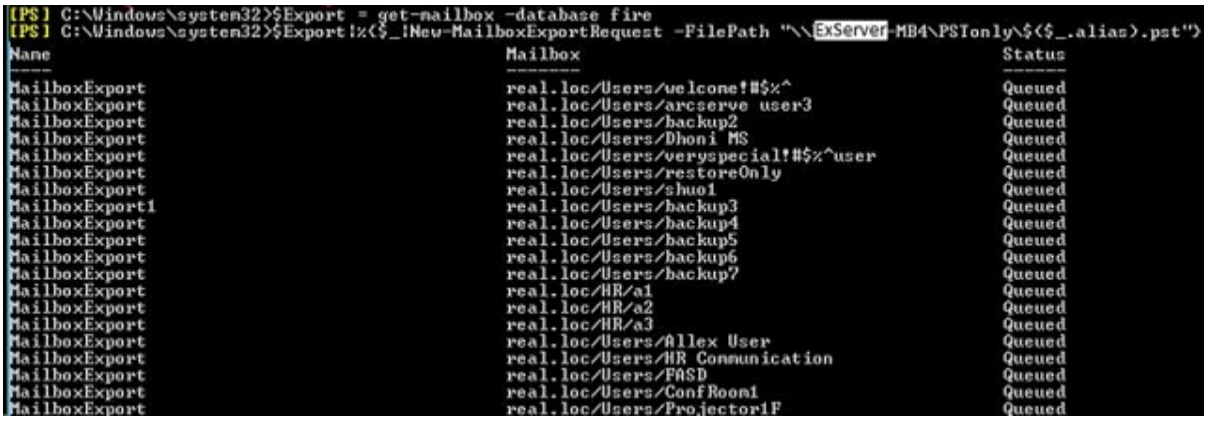
  New-ManagementRoleAssignment -Name "Import Export_Support" -SecurityGroup "Organization Management" -Role "Mailbox Import Export"

Exporting .pst files using Exchange PowerShell commands

To export all mailboxes to the .PST files, use exchange PowerShell commands. This option is allowed only in an On-Premise Exchange server. For more information, see link.

Example: The example below exports all the mailboxes from the database *Fire* to a shared location PSTOnly on the server *ExServer-MB4*.

1. Export .PST files.



2. View status of the exported .PSTs.

```
[PS] C:\Windows\system32>Get-MailboxExportRequest

Name                                               Mailbox                                            Status
----                                               -------                                            ------
MailboxExport                                      real.loc/Users/FASD                                InProgress
MailboxExport                                      real.loc/HR/a1                                     InProgress
MailboxExport                                      real.loc/Users/Allex User                          InProgress
MailboxExport                                      real.loc/Users/ConfRoom1                           InProgress
MailboxExport                                      real.loc/Users/backup2                             InProgress
MailboxExport                                      real.loc/Users/HR Communication                    InProgress
MailboxExport                                      real.loc/Users/veryspecial!#$%^user                InProgress
MailboxExport                                      real.loc/Users/backup7                             InProgress
MailboxExport                                      real.loc/Users/Projector1F                         InProgress
MailboxExport                                      real.loc/HR/a2                                     InProgress
MailboxExport                                      real.loc/HR/a3                                     InProgress
MailboxExport                                      real.loc/Users/welcome!#$%^                        InProgress
MailboxExport                                      real.loc/Users/backup5                             InProgress
MailboxExport                                      real.loc/Users/backup3                             Completed
MailboxExport1                                     real.loc/Users/backup3                             InProgress
MailboxExport                                      real.loc/Users/restoreOnly                         InProgress
MailboxExport                                      real.loc/Users/Dhoni MS                            InProgress
MailboxExport                                      real.loc/Users/backup4                             InProgress
MailboxExport                                      real.loc/Users/arcserve user3                      InProgress
MailboxExport                                      real.loc/Users/backup6                             InProgress
MailboxExport                                      real.loc/Users/shuo1                               InProgress
```

.PST files are exported.

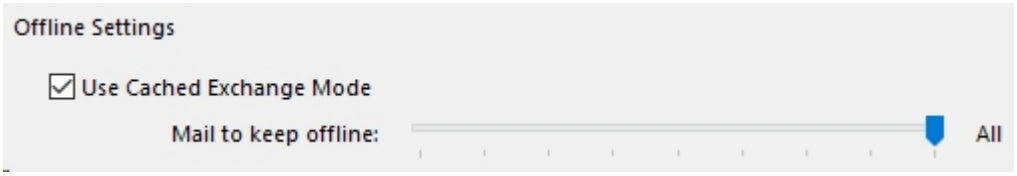
Exporting .PST files using Microsoft Outlook

For Exchange-Online, administrators need to manually export respective .PST files to the shared location.

Before exporting Exchange Online mailbox to the .PST, verify that the option *Use Cached Exchange Mode* is selected in Microsoft Outlook. If the option is selected, then the Offline settings to is set to cache All mails. Skip this step if the option of *Use Cached Exchange Mode* is not selected.

1. Navigate to the following location in Microsoft Outlook to verify if the option is selected:

   File>Info>Account Settings>Highlight Account>Change



2. (Optional) If the slider is currently not set to *All*, perform the following steps to create a new Microsoft Outlook profile with the *Cached Mode* set to *All* and wait till all the folders of the Mailbox gets updated completely.
   a. Navigate to File, Add Account.
   b. Enter account details and click **Next**,
   c. Once connected, click **Change settings** and in the Offline Settings dialog select *All*, and click **Finish**.
3. Perform the following steps to export the entire mailbox to a .PST File:

a. In Export, navigate to Import-Export, Export to a File, Outlook Data File (.PST).

b. Highlight the account name and click **Next**.

c. Enter a location for the .PST file and click **Finish**.

   Note: Password is optional.

.PST files are exported.

Export Gmail Data to .MBOX Files

Before starting migration from the UDP Archiving Console, administrators need to complete the prerequisite of exporting Gmail data to .MBOX files. Administrators can export the Gmail data into .MBOX files using Gmail account.

Follow these steps:

1. Navigate to https://takeout.google.com/.

   Gmail login page appears.

2. Log into Gmail using appropriate credentials.

   Download your data page appears.

3. Under the **Select data to include** section, select the **Mail** option and click **Next**.

   The Customize archive format page appears.

4. Select **.zip** as File type and click **CREATE ARCHIVE**.

   When the archive is created, **Download your data: downlaods** page appears to display the **Download** link. You also receive a mail into your Inbox of the Gmail account.

5. Click **Download** to import the .zip file.

6. Extract the folders and files from the downloaded .zip file.

   The extracted folder includes the .MBOX file.

Chapter 4: Using Arcserve UDP Archiving as Administrator or Master Admin

Super Admin creates administrator associated with one or more Domains. by selecting Master admin as the role while creating a user. The Master admin role is designed to manage the archive without access to any messages. The administrator can monitor, make configuration changes and set corporate policy such as retention rules, exception rules, legal holds, and add auditors and employees.

This section contains the following topics:

Settings for Administrator

Clicking your user name on the top-right corner of the UDP Archiving Console displays the **Settings** option. Using the Settings option, you can view access details.

The Settings page lets you update the following details:

Display Settings

Lets you define how content appears on your UDP Archiving Console.

Results Per page

Lets you define the number of results displayed on every page.

Language

Lets you set the preferred language for display.

Date Format

Lets you set the preferred display format of date.

Profile Picture

Lets you add a picture for your profile. Select a picture using the **Choose file** option and click **Upload**.

Change Password

Lets you reset your password. Enter the new password twice and click **Submit**.

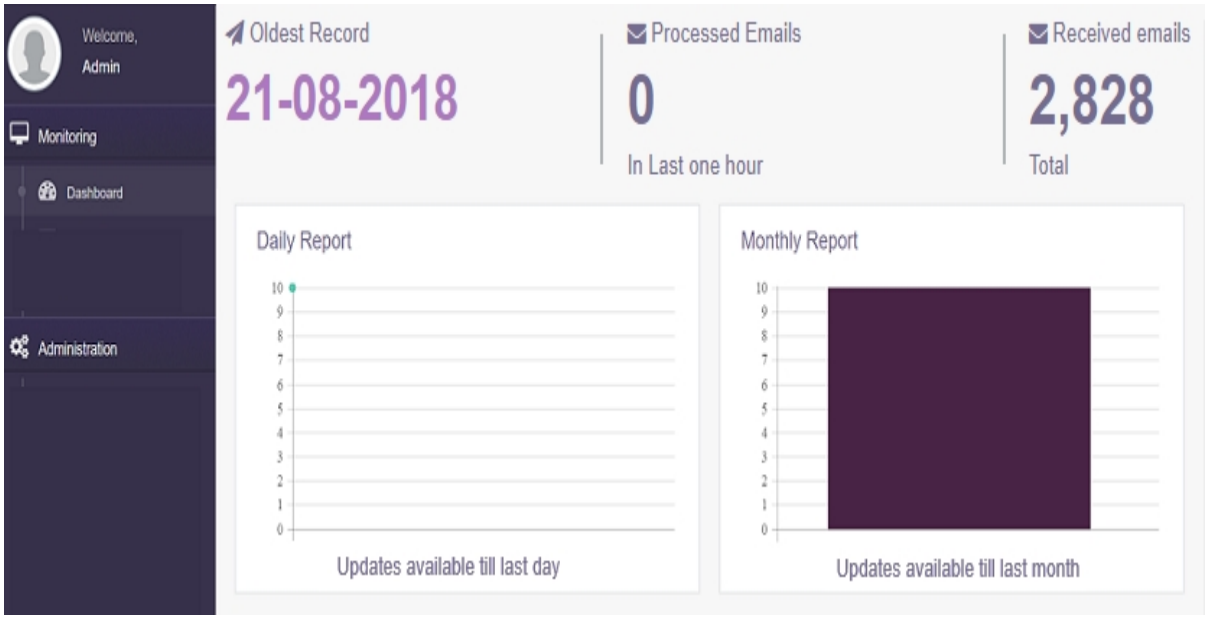
Using the Settings tab, you can also download UDP Archiving as Outlook plug-in. To configure, view add UDP Archiving as Outlook plug-in.

Monitor

UDP Archiving lets administrator monitor Dashboard, Archive accounting, and Audit log.

View Dashboard

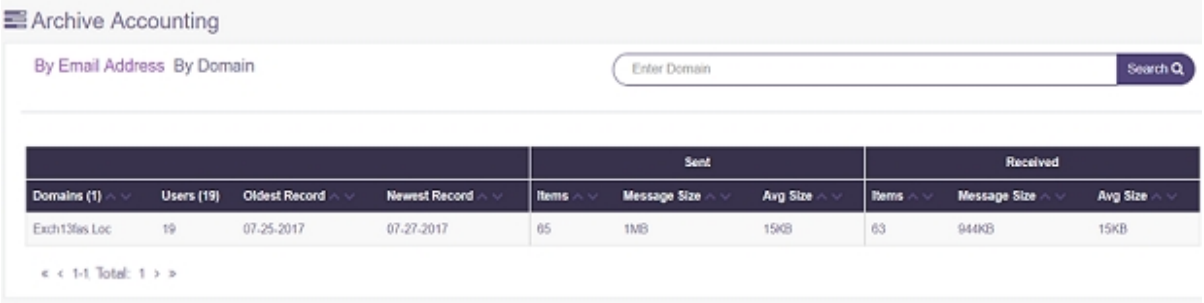
From the dashboard, administrator monitors the history of the daily and monthly flow of messages into the UDP Archiving. The Oldest Record option displays the date on which the oldest record was received for the corresponding profile.



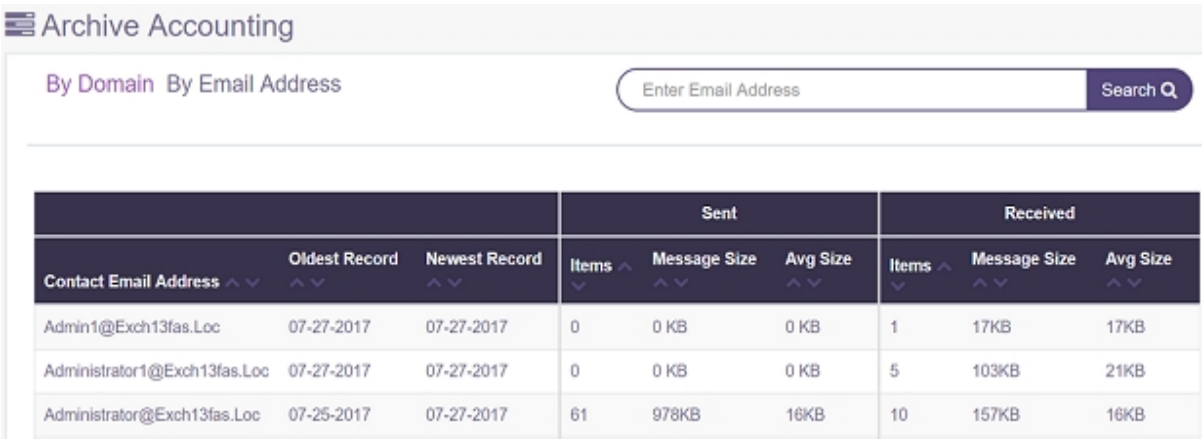
View Archive Accounting

Using Archive Accounting, you can monitor the count and date range of all messages that UDP Archiving receives from an email address or a domain.

View by Domain

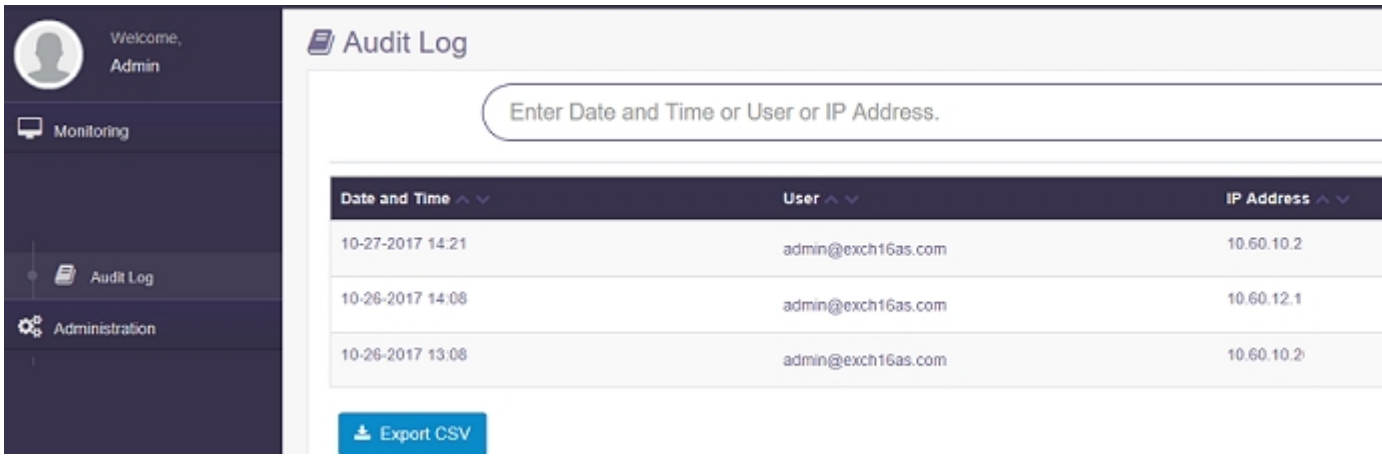


View by Email Address



View Audit Log

Using Audit log, administrator can track all activities that the users perform on the system. You can export the log in .csv format.



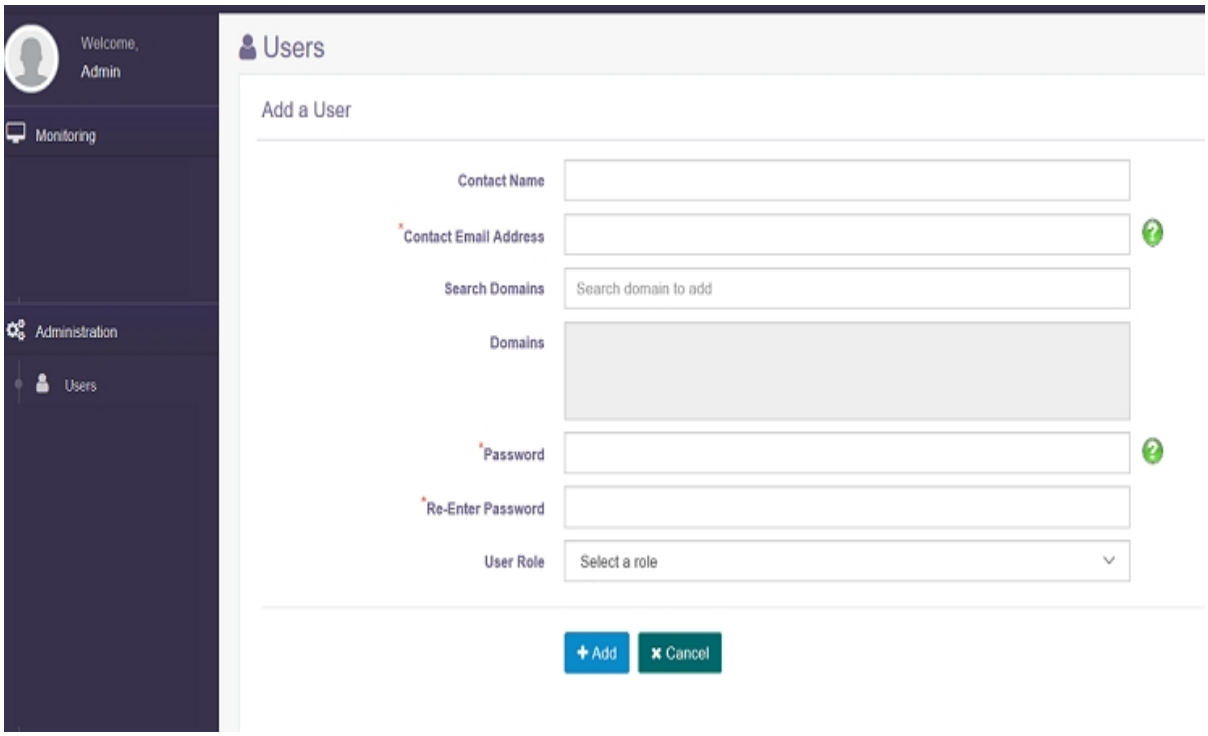
Administration

The administrator can perform multiple administrative functions. For example, manage users, groups, LDAP, import, manage exception rules, retention rules, legal hold, and license management.

Manage Users

The Administrator can create new users in the system as additional administrators, Auditors or Employee. An Auditor can view and manage all messages in the system, but an employee can only view their own messages. Users can be added to groups and the administrator will select the domain name for each employee. This function helps a large company with multiple domains to be managed in one archive and assign users appropriately. The administrator can also add users from Active Directory and LDAP queries.

From the **Users** page, click **Add a User** to create a profile for Compliance Officer, Master Admin, Auditors, and Employees.



Contact Name

Refers to the contact name of the email address that you enter.

Contact Email address

Refers to the email address of the auditor or employees. The email address must belong to one of the available domains.

Domains

Refers to the domain associated with that employee.

Search Domains

Refers to the domain for the employee. You can type initial alphabets and select from the drop-down list.

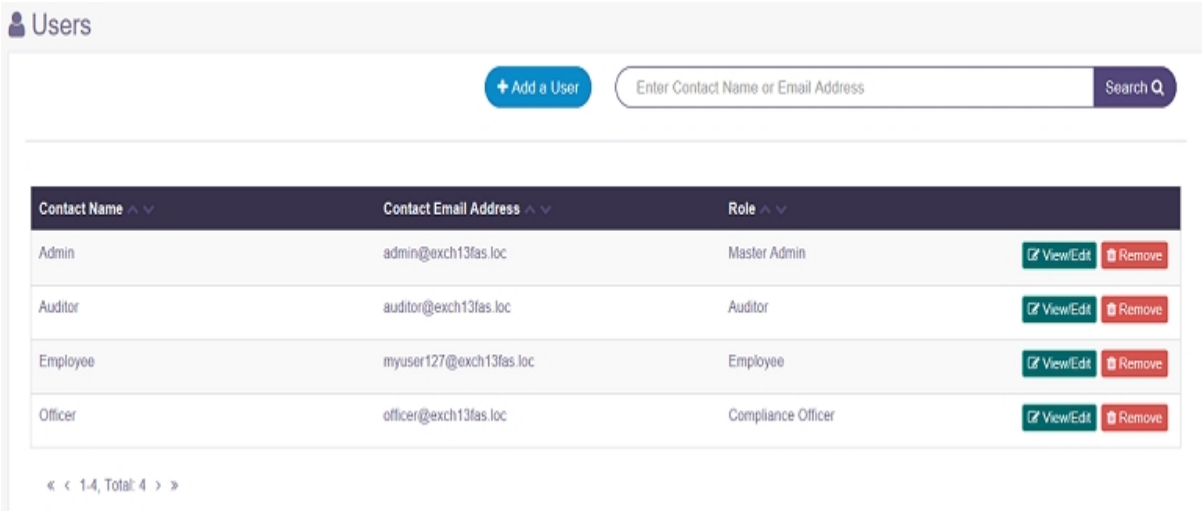
Password

Refers to the password that you need to enter twice to confirm.

User role

Refers to the role of the user.

Summary list of all system users

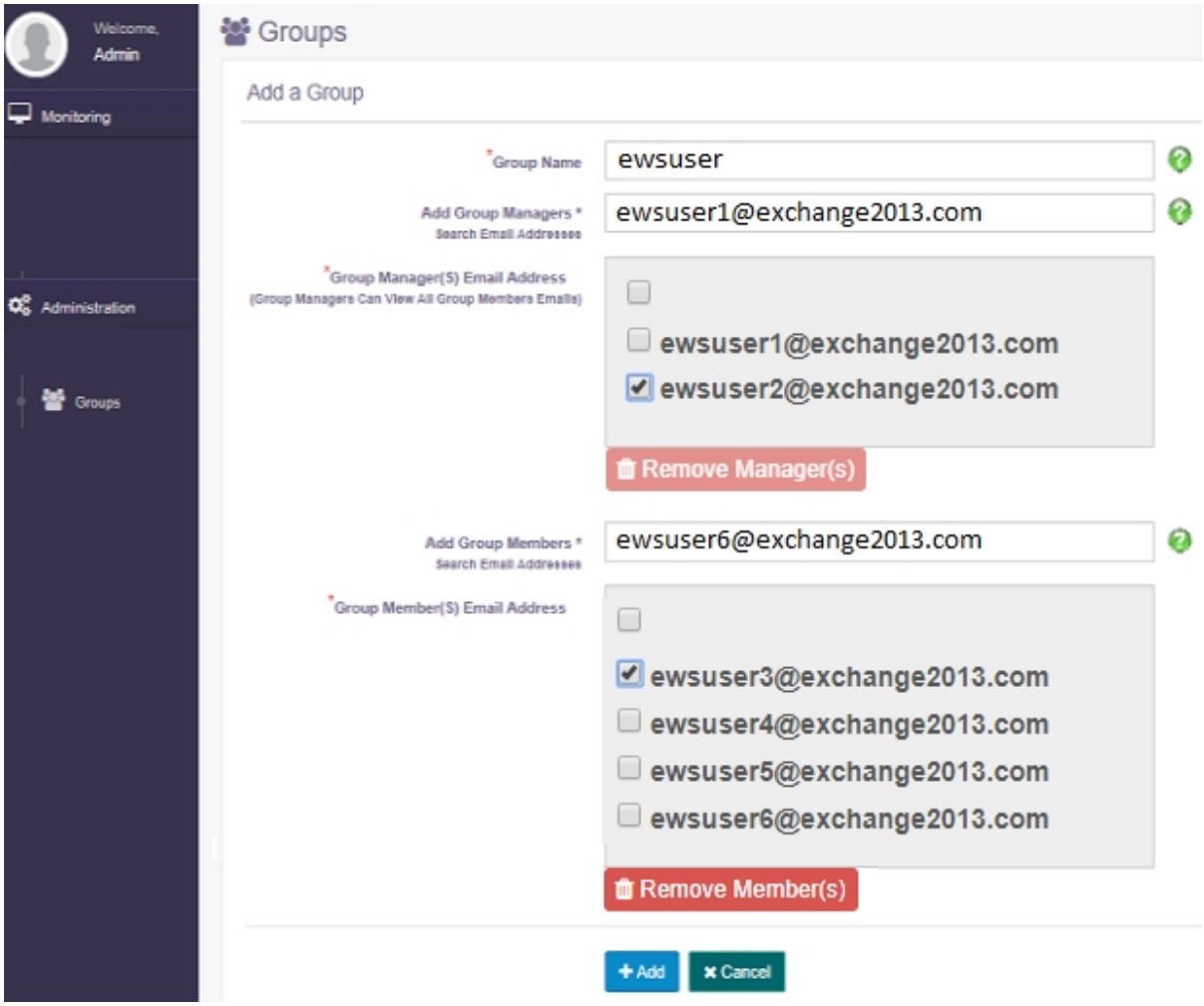


You can view, edit, or delete any user.

Manage Groups

Using Groups, administrator provides permission to one or more group managers to see all messages from group members. For example, a manager of a department to see subordinate's messages, access to a general email address by a group of employees such as a support email or giving someone access to messages of former employee.

To create new groups, from **Groups** page, click **Add a Group**.



Enter the following details:

Group Name

Refers to the name of a group. Enter a name for the group.

Add Group Managers

Refers to the manager for a group. Find an email ID from the same domain and assign as the manage of the group. The email ID assigned as manager can access messages of all the members of that group.

Note: Group managers are anyone who have access to these messages.

You can remove a group manager from the list. Select **Group Manager(s) Email Address** from the list and click **Remove Manager(s)**.

Add Group Members

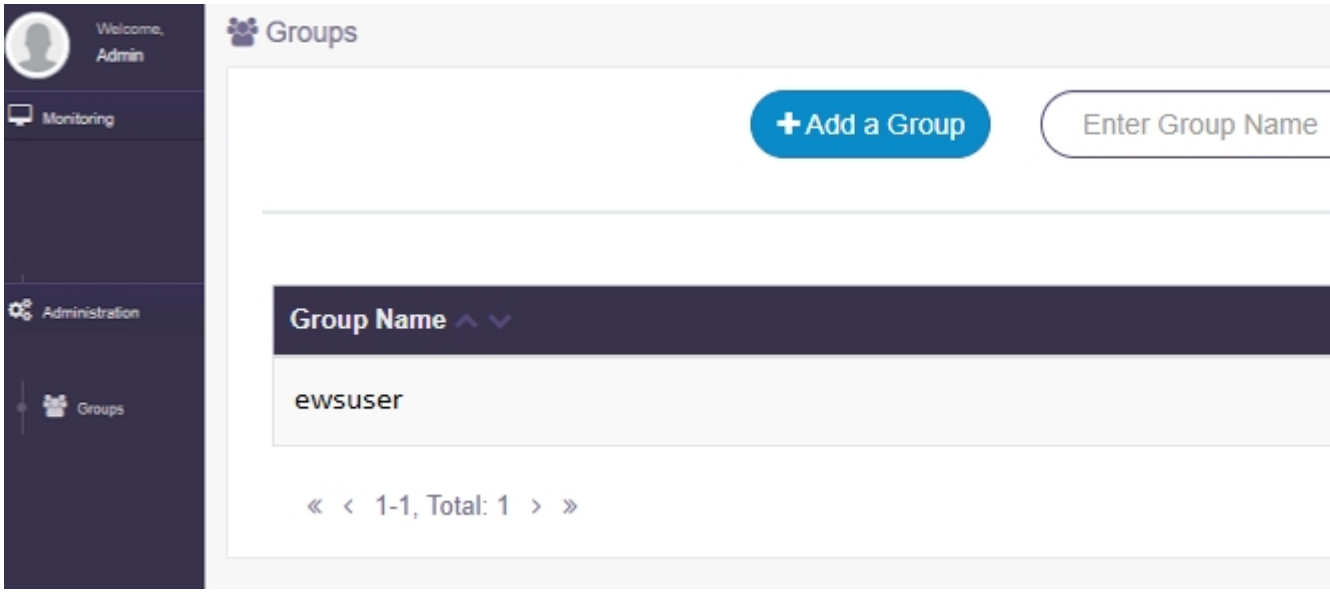
Refers to the list of employees in the group. Group members can view only their own messages:

Example: Company has a distribution group like *marketing@arc.com* that serves as the email address of the group.

You can remove a group member from the list. Select **Group Member(s) Email Address** from the list and click **Remove Member(s)**.

Summary list of all groups

Refers to the list of groups that you created in the system.



You can view, edit, or delete any group.

Manage LDAP

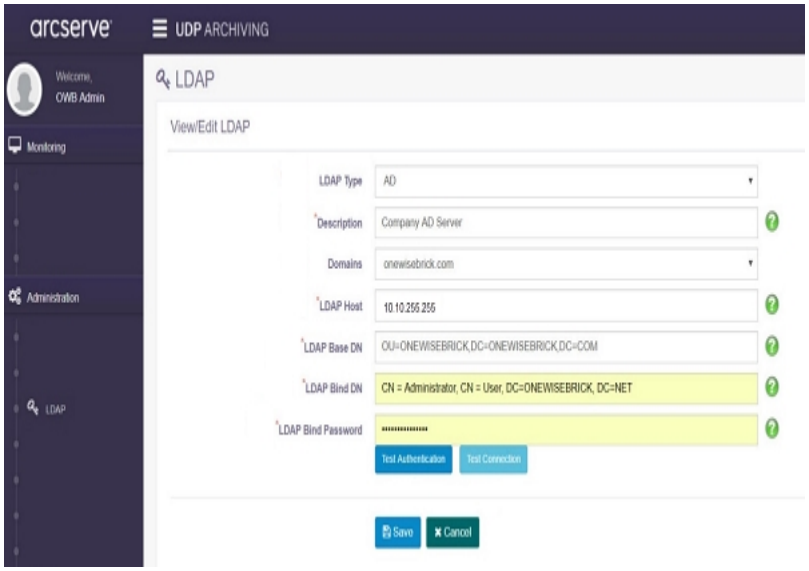
Using LDAP option, the UDP Archiving Administrators can add, edit, and remove an existing LDAP configuration available in the UDP Archiving server. To setup a working LDAP connection using Active Directory service, log into UDP Archiving as an Administrator.

Click **Add a Server** on the **LDAP** page to add LDAP.

Note: To use the **Add a Server** option, you must click **Enable LDAP**.

For more information on LDAP, refer Understanding LDAP.

To allow Active directory users to log into UDP Archiving, the following configurations are required:



LDAP Type

Refers to the type of LDAP authentication.

Note: The default value set is AD.

Description

Refers to the short description about the Active Directory(AD) server connection.

Domains

Refers to the domain where the Primary Active Directory (AD) services are running.

LDAP Host

Refers to the IP address of the Primary Active Directory(AD).

LDAP Base DN

Refers to the domain name used for searching users/groups entries in the Active Directory server having the following syntax :

CN=Users,DC=<Your Domain>,DC=com

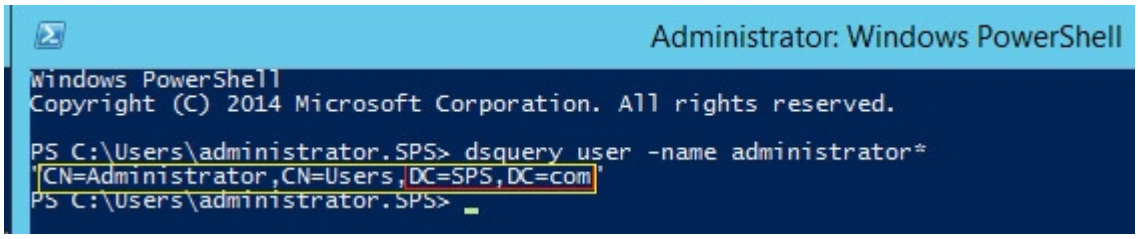
Note: To configure multiple organization units within one domain, separate the names using semicolon (;). For example, *OU= OU1,DC=<YourDomain>,DC=com; OU=OU2,DC=<Your Domain>,DC=com*.

LDAP Bind DN

Refers to the location in AD where your user account lies. This detail is used to allow LDAP calls to work from UDP Archiving. In the above screenshot, the domain administrator account is Administrator that lies in the default AD users bin. To get your bind DN, run the following command in PowerShell on the LDAP server:

*dsquery user –name Administrator**

Note: If you are using an account other than Administrator, replace the account name in your command.



In the PowerShell screen, the whole string highlighted in yellow is the Bind DN and the box in red at the end is the Base DN.

LDAP Bind Password

Refers to the Active Directory (AD) administrator password for the LDAP Bind.

Test Connection

Allows to validate whether the Bind DN credentials of user is able to authenticate using LDAP.

Test Authentication

Allows to test whether the connection established to the server is successful for the provided configuration details.

Manage Import

If you need to bring over existing messages from your mail server, create an import configuration using POP3 or IMAP and the admin credentials for your mail server. UDP Archiving finds and retrieves all the messages. This option is designed to pull in historical messages. Primary messages are send to the archiving using SMTP configurations. The O365 and Exchange customers must use only the EWSImport option.

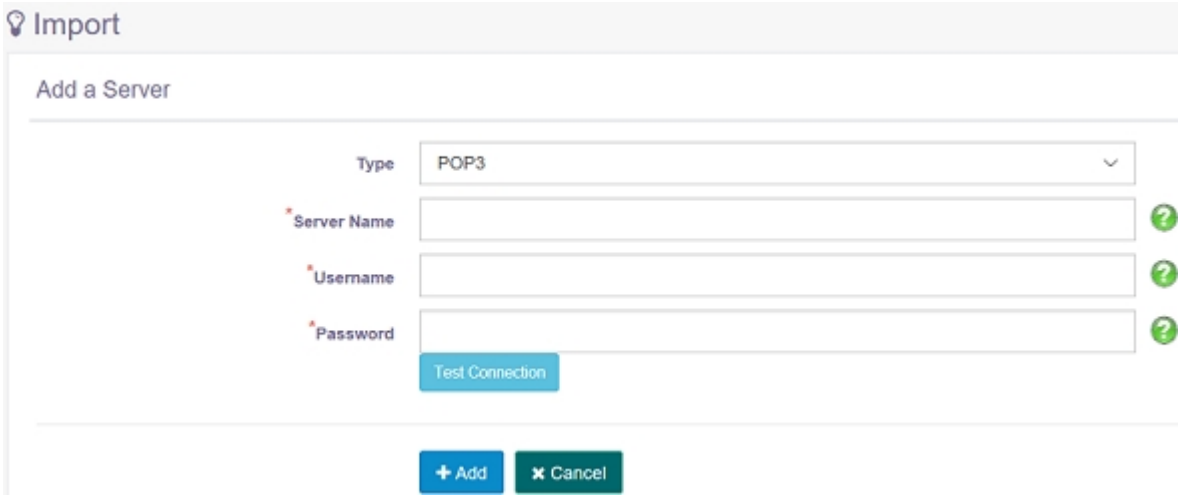
Note:

- To manage import for Gmail users, view link.
- To manage import of Exchange and Office 365 messages using Microsoft Exchange Web Services, view link.
- If import fails, view Troubleshooting.

Important! Only import or migration of emails does not make a user licensed. Only licensed user can view the emails. To view the emails in Employee user role, the Employee must send at least one email.

Follow these steps:

1. Navigate to Administration>**Import**.
2. From the Import screen, click **Add a Server**.



3. From Add a Server screen, provide the following details:

   Note: Import does not function if the name of server and credentials for server do not match.

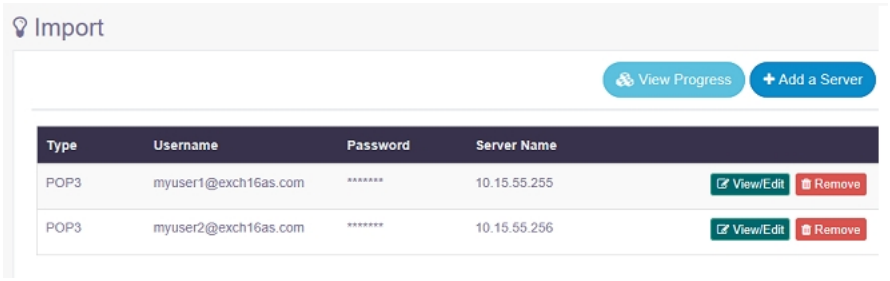
- **Type:** Select one of the options that applies.
- **Server Name:** Provide the name of server.
- Credentials: Provide user name and password to access the server.

4. Click **Test Connection**.

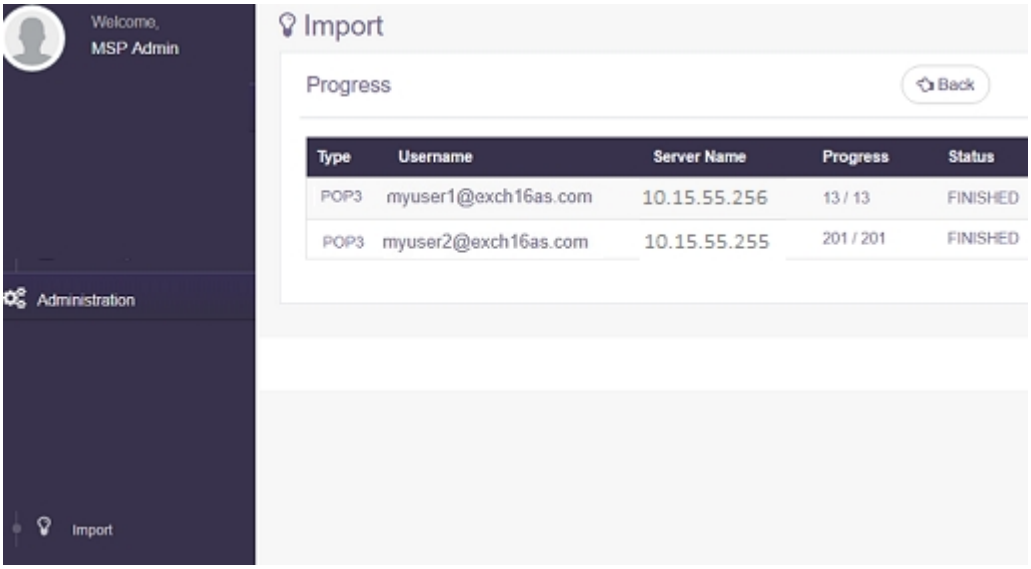
   Successful test provides the confirmation message: *Success*.

5. Click **Add**.

   The imported mailboxes appear on the main screen. You can bring over messages from each employee's mailbox or the entire mail server.



6. View status of the import by clicking **View Progress**.



Note: Import can take from few seconds to minutes depending upon the volume of mailbox and network speed.

The import process is complete.

More Information:

For Microsoft Exchange Server after importing the mail boxes, you must configure the Message MIME Format in Exchange Admin Center for the Search and Advanced Search functionality work properly. For more information, view Troubleshooting.

In case of network latency issues, you may observe that the fasimport.log file size may increase when POP3S and IMAPS protocols are configured.

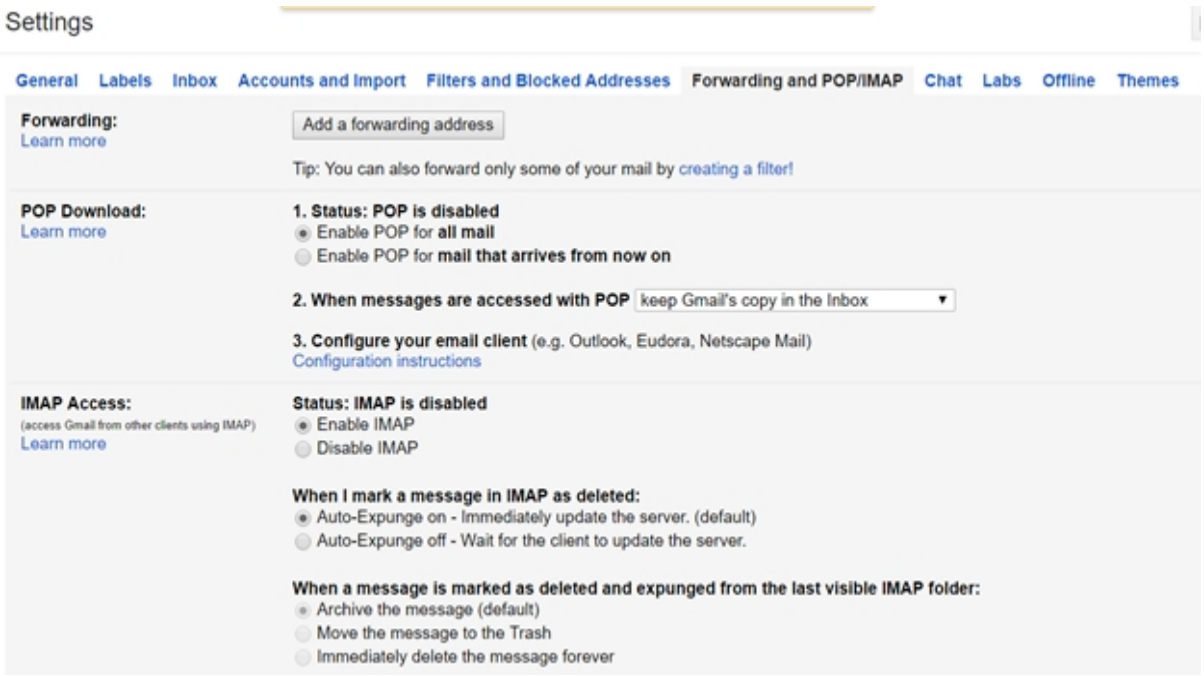
Manage Import from Gmail

UDP Archiving lets administrators import existing messages from the Gmail server. Create an import configuration using POP or IMAP3 and provide the admin credentials for your mail server. UDP Archiving finds and retrieves all the messages. This option is designed to pull in historical messages. Primary messages are send to the archiving using SMTP configurations.

Prerequisites

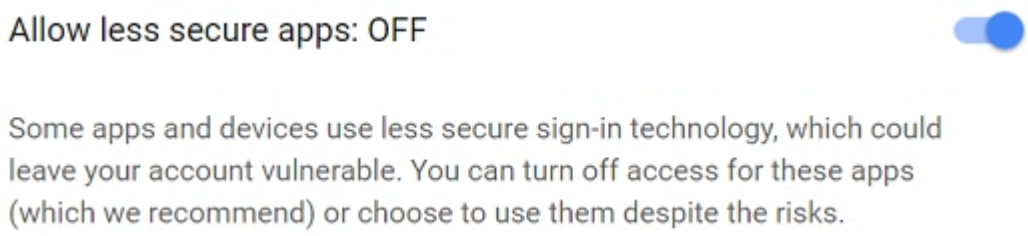
Before configuring UDP Archiving Console, verify if you have completed the following prerequisites for your gmail account:

- Configure your Gmail to enable POP or IMAP. From Settings , enable options as displayed below.



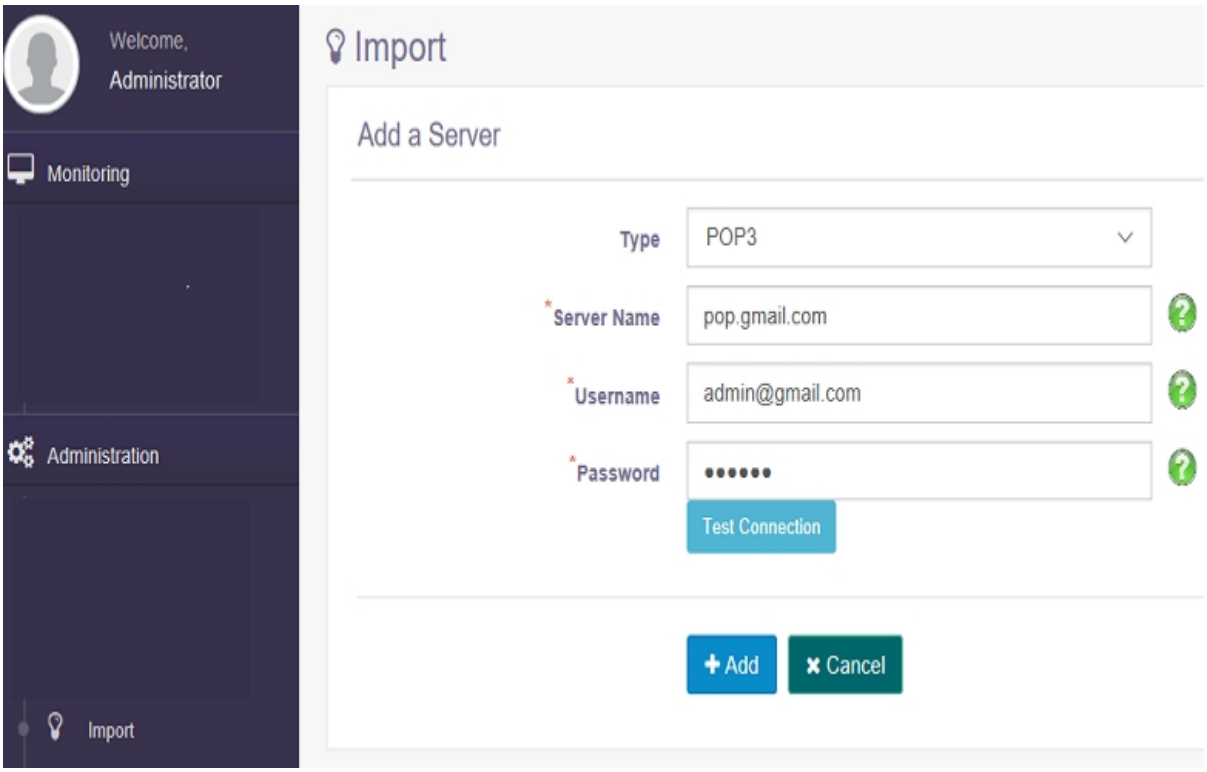
- In some cases, you also need to allow access to less secure apps. For more information, see link.
- Unlock captcha. For more information, see link.
- Verify that **Allow Less Secure apps** is enabled. To reach in Gmail, navigate to

My Account, Sign-in Security and scroll down towards the bottom of page.



Follow these steps:

1. To import mailbox of a user, login to the Gmail account of the respective user.
2. Launch Arcserve UDP Archiving in another tab of the same browser and login as Administrator or Master Admin.
3. Navigate to Administration>**Import**.
4. From the Import screen, click **Add a Server**.



5. Provide the following details on the Add a Server screen:
   a. Select Type.
   b. Enter Server Name.

For IMAPS: imap.gmail.com

For POP3S: pop.gmail.com

c. Enter the username and Password of Gmail account.

Note: Import will not happen if the name of server do not match with credentials for server.

6. Click **Test Connection**.

   Successful test provides the confirmation message: *Connection OK*.

7. Click **Add**.

   The imported mailboxes appear on the main screen. You can bring over messages from each employee's mailbox or the entire mail server.

8. View status of the import by clicking **View Progress**.

   Note: Import can take from few seconds to minutes depending upon the volume of mailbox and network speed.

The import process is complete.

Manage Import using Microsoft Exchange Web Services

UDP Archiving lets administrators import the mails of the individuals from the mail server. Administrators can create an impersonation user in mail server and import the historic mails of all individuals that exist in mail server. Microsoft Exchange Web Service supports impersonation and enables the UDP Archiving to communicate with mail server and allows to retrieve all the mails, folders and any required item of specific user / all users using the credentials of impersonation user.

- UDP Archiving supports importing mails using Microsoft Exchange Web Service only through *ewsImport* command line utility.
- UDP Archiving supports importing mails only from Microsoft Exchange Server and Microsoft Office 365 using Microsoft Exchange Web Services. Microsoft Exchange Server 2010, 2013 and 2016 are the supported versions.
- UDP Archiving does not import the non email items such as drafts, outbox mails, calendar, and contacts.

What To Do Next?

1. Review Prerequisites and Considerations
2. Import Mails using Microsoft Exchange Web Services

Prerequisites

You must complete the following prerequisite tasks before importing the mails from Microsoft Exchange Server / Microsoft Exchange Online (Office 365) using Microsoft Exchange Web Services (EWS):

1. Create the Journaling Rule in Microsoft Exchange Server / Microsoft Exchange Online (Office 365). For more information, see UDP Archiving Deployment and Configuration guide.
2. Add an impersonation user in Microsoft Exchange Server. For more information, see Add Impersonation User in Microsoft Exchange Server.
3. Download and install Java Development Kit (JDK) on the UDP Archiving server if you upgraded to UDP Archiving v6.0 Update 4 in offline mode. For more information, see Download and install Java Development Kit (JDK).
4. On the UDP Archiving server run the following command and enter the host name and IP address of Microsoft Exchange Server in the hosts file:

   sudo vim /etc/hosts

   This step is not required if you are using Microsoft Exchange Online (Office 365).

Add Impersonation User in Microsoft Exchange Server

You must add an impersonation user before importing the mails from Microsoft Exchange Server / Microsoft Exchange Online (Office 365) using Microsoft Exchange Web Services (EWS).

Follow these steps:

Using Microsoft Exchange Admin Center:

1. Log into Microsoft Exchange admin center as administrator.
2. Navigate to **permissions** and click **Discovery Management**.
3. In the Discovery Management window, specify the following details and click **Save**:
   - Select **Default** as **Write scope**.
   - From **Roles**, click **+** and select **ApplicationImpersonation**.
   - From the **Members**, click **+** and select a member to whom you want to assign the impersonation user.

   You have successfully added impersonation user in Microsoft Exchange Server.

Using Remote Powershell:

1. Connect to Microsoft Exchange Online using PowerShell or Connect to Microsoft Exchange Server using PowerShell based on your mail server.
2. Run the following command to add a user as a member of Discovery Management role group:

   "Add-RoleGroupMember" cmdlet

   For example: Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.
3. Run the following command to assign application impersonation role to the user:

   "New-ManagementRoleAssignment" cmdlet

   For example: New-ManagementRoleAssignment Name: impersonationAssignmentName -Role:ApplicationImpersonation - User: "username@domain.onmicrosoft.com"

The ApplicationImpersonation role and Members group are added successfully.

Download and Install Java Development Kit

If you upgraded to UDP Archiving v6.0 Update 4 in offline mode, you must install Java Development Kit (JDK) on the UDP Archiving server.

Follow these steps:

1. Click link and download *java.tar.gz* file.
2. Copy the *java.tar.gz* file to the UDP Archiving server.
3. Run the following command to extract files and folders:

   tar -zxvf java.tar.gz
4. Open the folder named java from the extracted files and folders.
5. Run the following command to install the package:

   *sudo dpkg -i *.deb*

   Java is successfully installed on UDP Archiving server.

Import Mails using Microsoft Exchange Web Service

After adding the impersonation user in Microsoft Exchange Server / Microsoft Exchange Online (Office 365), you can import the mails of all the individual users using the credentials of impersonation user.

Follow these steps:

1. Navigate using one of the following options:
   - If you have added a volume from UDP Archiving Console navigate to the following path:

     /archiving/ewsimport
   - If you have not added a volume from UDP Archiving Console navigate to the following path:

     /var/fas/www/ewsimport
2. Run the following command with the mandatory options to execute the import job:

   ewsImport -b <bind URL of Microsoft Exchange Server> -u < impersonated user name on the Microsoft Exchange Server> -t <to date> -T <time zone> -a

   Important! The -a option is not supported in Microsoft Exchange Server 2010. You can use one of the options from -D, -L or -s instead of -a.

   Example: ewsImport -b https://WIN-T1I7830GB32.per-fexch16.com/EWS/Exchange.asmx -u impersonation@perfexch16.com -t 2019-09-10 -T +05:30 -a

   -b

   Refers to the bind URL of Microsoft Exchange Server.

   If you want to import mails from Microsoft Office 365, the bind URL is *https://outlook.office365.com/EWS/Exchange.asmx*.

   If you want to import mails from Microsoft Exchange Server, perform the following steps to find the bind URL in Microsoft Exchange Server:

   Follow these steps:

   a. Log into ExchangeAdmin center as administrator.

   b. Navigate to **servers** and click the **virtual directories** tab.

   c. From the list of virtual directories, double click **EWS (Default Web**

Site).

Internal URL field displays the bind URL.

-u

Refers to the impersonated user name on the Microsoft Exchange Server.

-t

Refers to the date till when to import the mails.

-T

Refers to the time zone of the Microsoft Exchange Server.

-a

Refers to all the mailboxes present in an organization. You can replace the -a option with one of the following options:

-D

Refers to the path of the file that includes the Distribution Lists.

-L

Refers to the path of the file that includes the list of users.

-s

Refers to the email address of a single user.

Example: ewsImport -b https://WIN-T1I7830GB32.per-fexch16.com/EWS/Exchange.asmx -u impersonation@perfexch16.com -t 2019-09-10 -T +05:30 -L list.txt

Following are the additional options available that you can optionally append with command:

-f

Refers to the date from when to import the mails.

-B

Refers to the start time of the scheduler.

-E

Refers to the end time of the scheduler.

3. Enter the password of the impersonation user and press **Enter** on the key board.

   The ewsImport job is successfully started.

   Notes:

- After the ewsImport job is completed if any users / mails are not processed, run the command again to resume the import job.
- If ewsImport is a scheduled job and the import is not completed by end time, the job resumes at start time next day. For more information, see Schedule EWS Import.
- You can specify maximum 23 hours duration between start time and end time to schedule ewsImport job. For example, 5 am to 4 am.
- The ewsImport and ewsSchedule logs include the details of ewsImport job. Perform the following steps, to access the ewsImport and ewsSchedule logs:

  a. Log into UDP Archiving as udp_admin using PuTTY.

  b. Navigate to the path */var/fas/www/log*.

  c. Open the following log files using a text editor:

  ewsImport.log

  Contains the details of all the mailboxes and the folders that are imported from the mail server to UDP Archiving server.

  ewsSchedule.log

  Contains the details related to the scheduled ewsImport job.

You can Pause/Resume EWS Import and Configure the EWS Import Utility.

Schedule EWS Import Job

You can schedule ewsImport job to run during the specified start and end time. You can schedule only one ewsImport job to run at a time.

Notes:

- You cannot schedule the ewsImport job to start and end at the same time.
- When ewsImport job is scheduled, do not run any other ewsImport job manually before, during or after the scheduled time.

Follow these steps:

1. Navigate using one of the following options:
   - If you have added a volume from UDP Archiving Console navigate to the following path:

     /archiving/ewsimport
   - If you have not added a volume from UDP Archiving Console navigate to the following path:

     /var/fas/www/ewsimport
2. Run the *ewsImport* command appended with the mandatory options. For more information about the mandatory options, see Import Mails using Microsoft Exchange Web Service.

   Example: The below example command schedules ewsImport job to run between 5pm and 6 pm and import the mails sent or received from 2015-08-08 to 2019-09-10 based on the GMT+5.30 time zone. The scheduled job runs every day between the specified time till all the mails are imported.

   ewsImport -b https://WIN-T1I7830GB32.perfexch16.com/EWS/Exchange.asmx -u impersonation@perfexch16.com -f 2015-08-08 -t 2019-09-10 -T +05:30 -B 5pm -E 6pm -L list.txt

   Notes:
   - If the import job is not completed by end time, the current job is paused and resumed at start time next day.
   - You can specify maximum 23 hours duration between start time and end time to schedule ewsImport job. For example, 5 am to 4 am.
3. Type the password of impersonation user and press **Enter** on the keyboard.

   ewsImport job is scheduled successfully.

Note: If you run the command with modified parameters before completing the scheduled ewsImport job, the previously scheduled job stops and new job takes place based on the latest command passed.

You can stop the scheduled ewsImport job any time before the specified start time or after the specified end time. You cannot stop the job when in progress.

Follow these steps to stop the scheduled ewsImport job:

1. Navigate using one of the following options:
   - If you have added a volume from UDP Archiving Console navigate to the following path:

     /archiving/ewsimport
   - If you have not added a volume from UDP Archiving Console navigate to the following path:

     /var/fas/www/ewsimport
2. Run the following command to delete the ews_command file:

   rm -rf ews_command

   The scheduled ewsImport is successfully stopped.

Pause/Resume EWS Import

You can pause the ewsImport job that is manually started, and resume ewsImport job that is paused.

Follow these steps:

1. To pause the ewsImport job, press Ctrl+C on the keyboard while the ewsImport is running.

   Notes:

   - When you resume the manually paused ewsImport, the job starts to import the mails of the user that was in progress at the time you paused the job.
   - When you resume ewsImport job that is terminated due to any other reason such as network outage or required services stopped, the job starts to import from the mail that was getting imported when you paused the job.

2. Perform the following steps to resume ewsImport job:

   a. Navigate using one of the following options:

      - If you have added a volume from UDP Archiving Console navigate to the following path:

        /archiving/ewsimport

      - If you have not added a volume from UDP Archiving Console navigate to the following path:

        /var/fas/www/ewsimport

   b. Run the following command:

      ewsImport -b <bind URL of Microsoft Exchange Server> -u <impersonated user name on the Microsoft Exchange Server> -t <end date> -T <time zone> -L <path of the file that includes the list of users>

      Note: You can also use -a, -D, or -s option instead of -L. For more information about the options, see Import Mails using Microsoft Exchange Web Service.

   c. Enter the password of impersonation user and press **Enter** on the keyboard.

   The ewsImport job is successfully paused and resumed.

Configuring ewsImport Utility

You can configure the *ewsImport utility* to specify the number of retries, wait time, number of mails to fetch at once and number of threads to run at a time.

Follow these steps:

1. Navigate to the following path and open the *ews_config.properties* file:

   /usr/local/etc/

2. Find the following parameters and modify the values as required:

   number_of_retries

   Refers to the number of times that the UDP Archiving instance must try to reconnect with the Exchange Server. Specify a number between 1 to 50.

   Default: 20

   wait_time

   Refers to duration that UDP Archiving instance must wait between the attempts to reconnect with the Exchange Server. Specify the wait time in milliseconds between 1 to 120000.

   Default: 60000

   mails_to_be_fetched_per_request

   Refers to the number of mails to fetch at once. Specify the number between 1 to 1000.

   Default: 40

   number_of_threads

   Refers to the number of users to process at a time for importing mails.

   Default: 2

3. Save and close the file.

Manage Exception Rules

When a company does not want to archive certain messages, an administrator can set rules for their organization to remove these messages as they are being processed in the archive. Some examples include known spam messages, system generated emails and more including messages to or from an email address, text in a subject field and more. For each new rule you complete the form below with just the information needed for the rule. The remaining fields are left blank.

Important! You cannot modify an Exception rule.

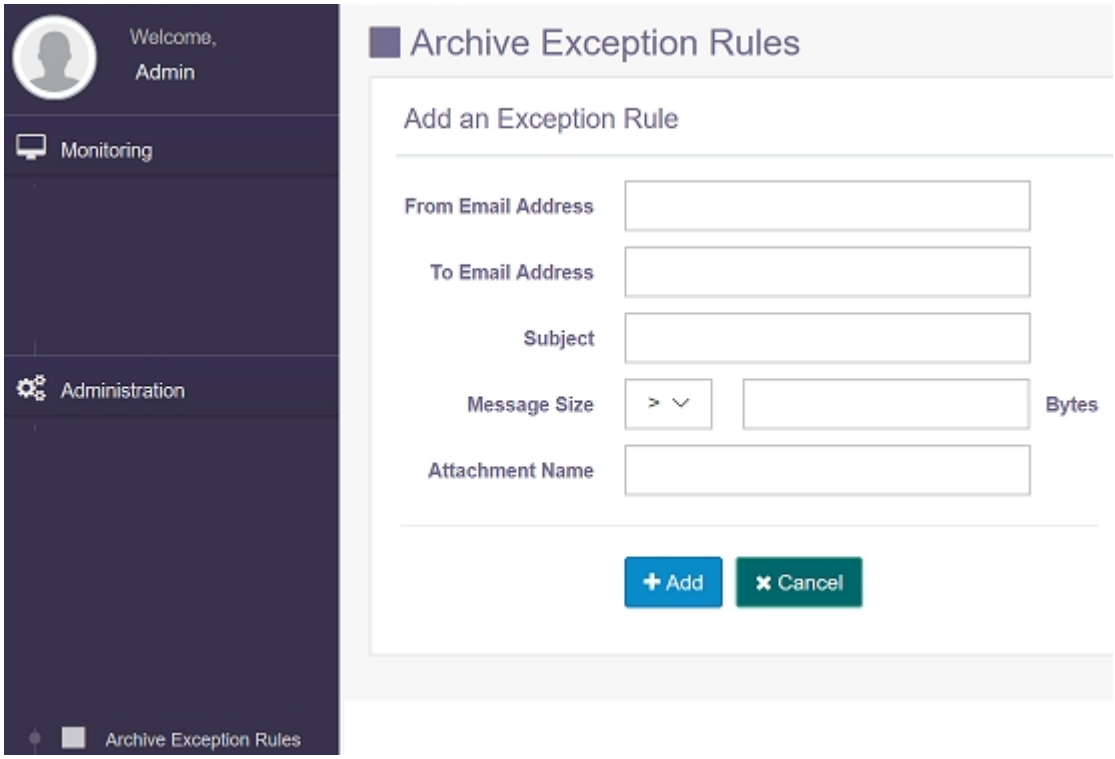
You can remove Exception rules.

For viewing steps in video, click How to Manage Archive Exception Rules.

Considerations:

- Administrator must determine and configure the Retention Rules \ Settings and Archive Exception Rules before configuring the Email Archiving on the Mail Server. If not configured, then emails are archived based on the default Retention Settings and purged only after meeting the number of days mentioned in the Retention Settings at the time of Archiving.
- Any new Exception and Retention Rules are applied for the messages moving forward and are not applicable to the email messages that are archived already.
- For text in Subject field, the Exception Rules do not support the following characters:

  ':', ';', '<', '=', '>', '?', '@', ', '', '#', '%', '&', '(', ')', '*', '+', '/', '[', '\\', ']', '^', '_', '{', '|', '}', '~'



To add an exception rule, enter detail in one of the fields and click **Add**.

Manage Retention Rules

Administrator must always set the retention rules even if the rule matches the global policy. For more information about retention rules, see Considerations.

Before configuring the email archiving on the Mail Server, the administrator must determine and configure Retention Rules and Archive Exception Rules. If not configured, then the emails are archived based on the default Retention Settings and purged only after meeting the number of days mentioned in the Retention Settings at the time of Archiving.

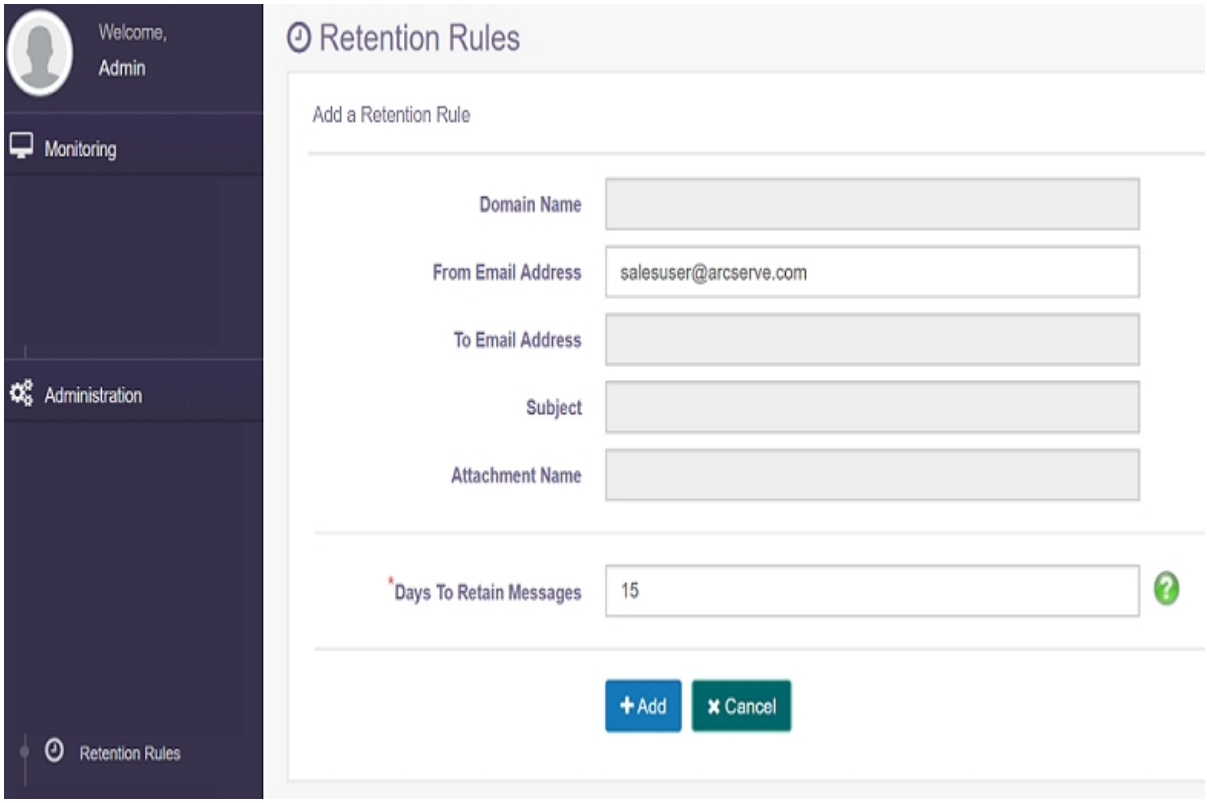
From the Console, you can add multiple retention rules based on different parameters. You can set retention rules using one of the parameters such as the From or To email address, subject line, and other options. An organization may want management emails to be kept longer than the emails of other employees or may want to have employees add a specific subject line text.

For viewing steps in video, click How to Manage Retention Rules.

Retention Rules are applicable to the specific domain and override the Global Email Retention settings. Administrator must always set the Retention rules even if the rule matches the global policy. From the Console, you can add multiple Retention Rules based on different parameters. The system holds messages based on the longest retention policy applied.

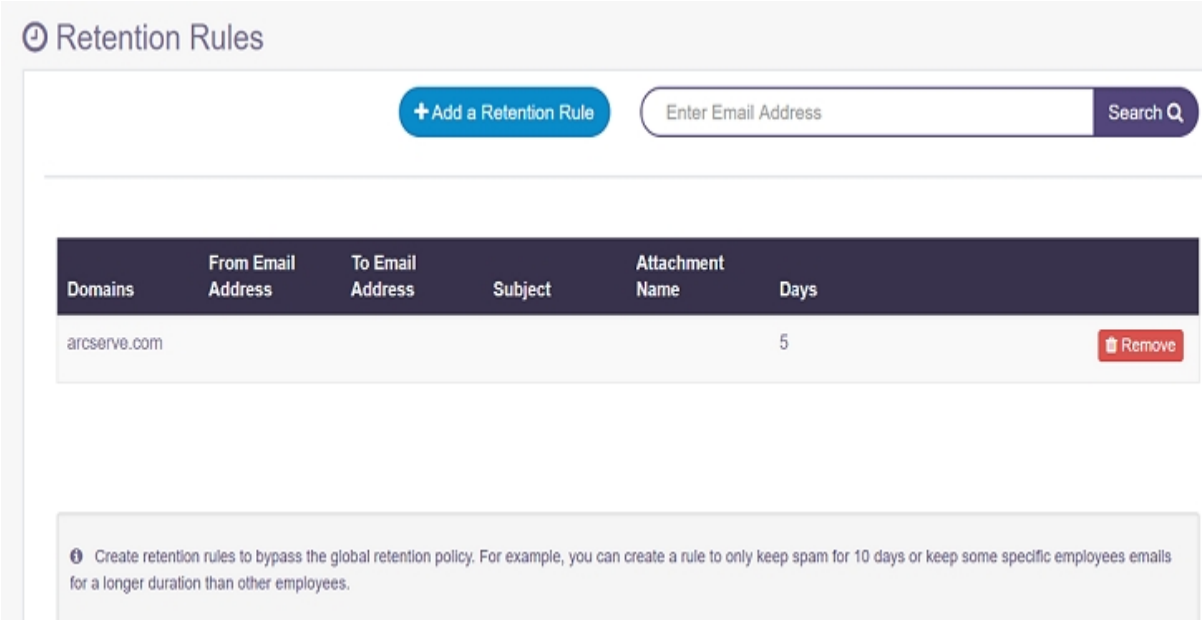
Note: Retention rule is applicable to messages archived only after setting the retention rule.

For example, you can start by setting a general rule for your domain. Such as entering <domain>.com on the domain line and days to retain to 365 for a one year retention. You can enter detail only in one field.



To add retention rule, enter details in a field, provide a number for **Days to Retain Messages**, and click **Add**.

Below is a summary of rules that have been set. You can also remove retention rules.



Considerations

A company's retention policy defines the period within which the emails are retained in their archive. In UDP Archiving, the Super Admin and Master Admin configure the email retention settings. The responsibilities are defined as follows:

- The Super Admin configures the Global Email Retention.
- The Master Admin configures the retention rules based on their corporate policies.

A retention rule is applied based on the sent date of the email message. This rule applies to all email messages that are being archived, which includes the migrated and imported historical email messages.

Note: The imported or migrated email messages remain archived only if the age of the email message is lesser than the retention days applied to the email message.

For example:

Days to retain: 3650 (~10 years)

Current date: August 15, 2019

Email messages sent on or after Aug 15, 2019: Retained for 10 years.

Imported email messages sent on Aug 15, 2014: Retained for 5 years.

Imported email messages sent on or before Aug 14, 2009: Will be purged in the next scheduled purge

Other considerations include:

- When the Master Admin configures the retention rules, it overrides the Global Email Retention settings. If the administrators do not set the retention policy, the Global Email Retention is applied by default.
- Although many retention rules may be defined, only the longest rule is applied to the email message. The system retains email messages based on the longest retention policy.
- Any new retention rule is applied to the email messages only from the time the new rule is created. The new rule is not applicable to the existing archived email messages.

  For example:

  Initially, message 1 from domain.com gets archived and its retention or purge date is set as 3000 days.

Later, the Master Admin creates a retention rule based on the corporate policies of domain.com to retain messages for 4000 days.

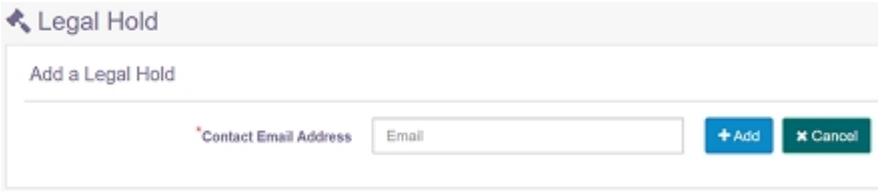
Subsequent to the creation of new retention rule, when a new message from domain.com gets archived, the retention or purge date is set to 4000 days, by default.

Note: The purge date for message 1 stays as 3000 days and it does not change as these messages were archived before the Master Admin created the retention rule for 4000 days.

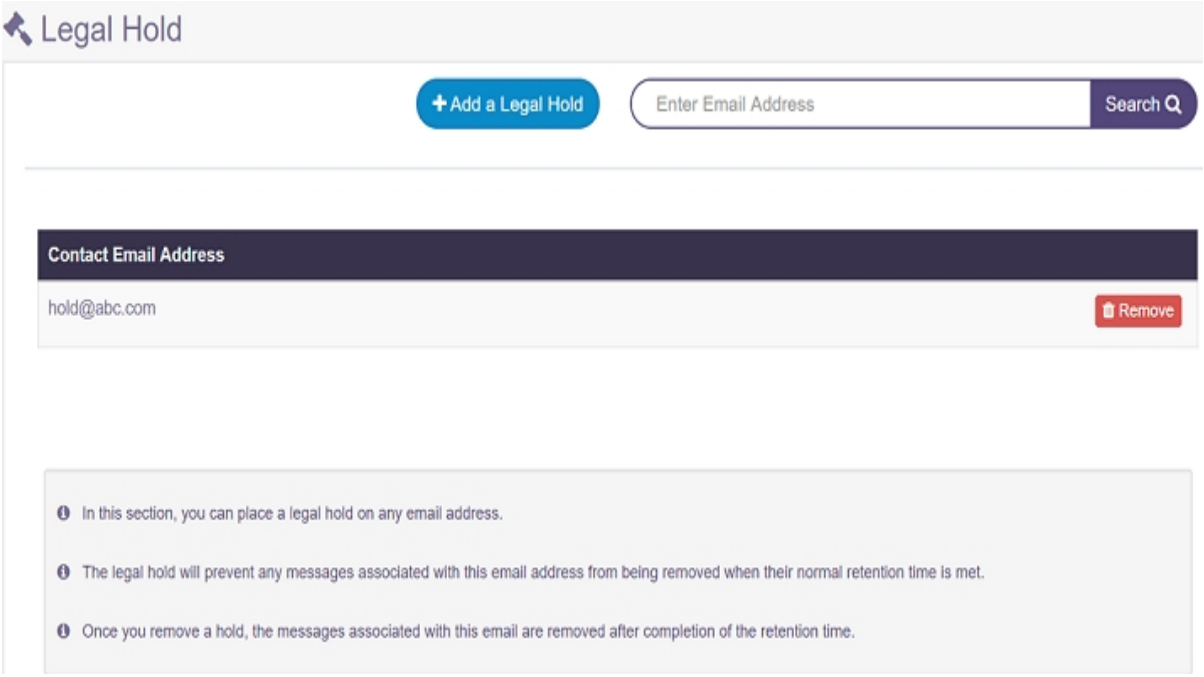
Legal Hold

In an organization, Legal Holds are applied to individual email addresses to preserve all the messages during a litigation, regulatory inquiry or internal review. When a legal hold is placed, all associated messages are not removed during the normal purging of expired messages that reach their longest retention date.

Administrators can use Legal Hold to add email addresses for each employee on hold. Identify the email address of any employee whose messages should never be deleted or are on legal hold due to a litigation.



Below is a list of the holds. All messages are held until the hold is removed.



Manage Licenses

Administrator can manage licenses of employees using the **License Management** tab. Administrator can assign or unassign licenses to employees.

For detailed steps, view Arcserve Licensing User Guide.

For viewing steps in video, click How to Manage UDP Archiving Licenses.

Chapter 5: Using Arcserve UDP Archiving as Compliance Officer

The Compliance Officer role provides the flexibility to create and manage policies in support of compliance regulations. The Compliance Officer has all capabilities of a regular auditor but can additionally set scheduled purge policies.

This section contains the following topics:

Personal Settings

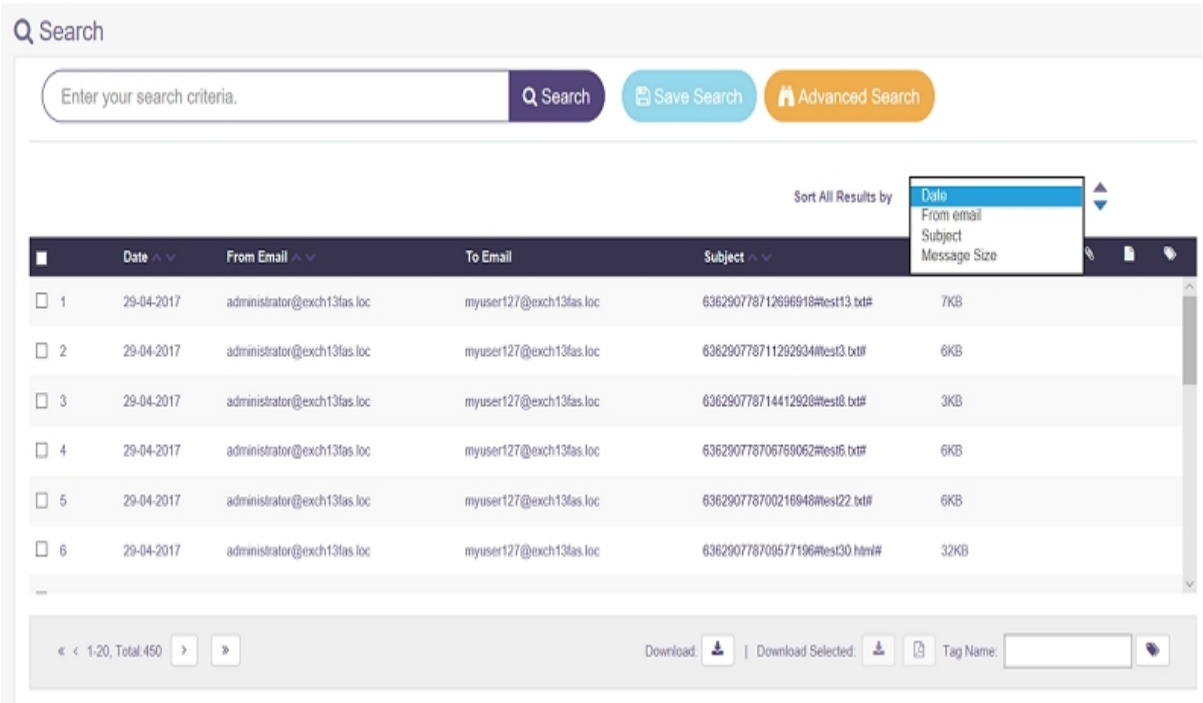
From the UDP Archiving Console, click **Settings** on the top-right corner under your login name to view and modify your personal settings. The settings page has four sections:

- **Access Settings:** Lets you view your access details that the administrator created. You cannot modify details of Access Settings.
- **Profile Picture:** Lets you upload desired picture for your profile.
- **Display Settings:** Lets you manage emails that appear on your dashboard. You can set the number of emails that can appear on one screen. You can also set the language and date format for the emails.

  Note: For **Results per page**, you can select only one of the four options: 10,20,30, and 50.
- **Change Password:** Lets you update your password. You use this option after your first login. Later also you can change password when desired.

Using the Settings tab, you can also download UDP Archiving as Outlook plug-in. To configure, view add UDP Archiving as Outlook plug-in.

Search



After logging into UDP Archiving as an employee, you land into the dashboard. The landing screen is the same screen that appears when you click **Search** from the left pane. Use Simple search only to search content of Subject and Body of an email. For more specific search, use Advanced Search.

For viewing steps in video, click How to Search in UDP Archiving.

The Search page is divided into four parts as per information displayed:

1. **Header:** Includes Search and Advanced Search activities. Comma separated text, Boolean connectors and other functions such as wild cards help you perform simple and advanced search. For Simple search, you can save search term with results. For Advanced Search, you can save only the search terms.
2. **Body:** Displays all the archived emails and their details. Details include the from and to addresses, date of email received, subject, and message size. Some details are marked with symbols. For example, every email has symbols to displays if the mail contains notes and attachment, or has a tag associated.
3. **Footer:** This area of dashboard (or search page) includes multiple options to perform on emails. For example, you can Download all or some messages either as PDF or Email. You can also assign tag to one or more emails.

4. **Result:** Displays the result of any action that you perform in Body or Footer area. For example, if you click a message, the content appears in this area. You can add Notes to the displayed email message. From Footer area if you download any email, the progress appears in this area.

In the dashboard you have many options that include:

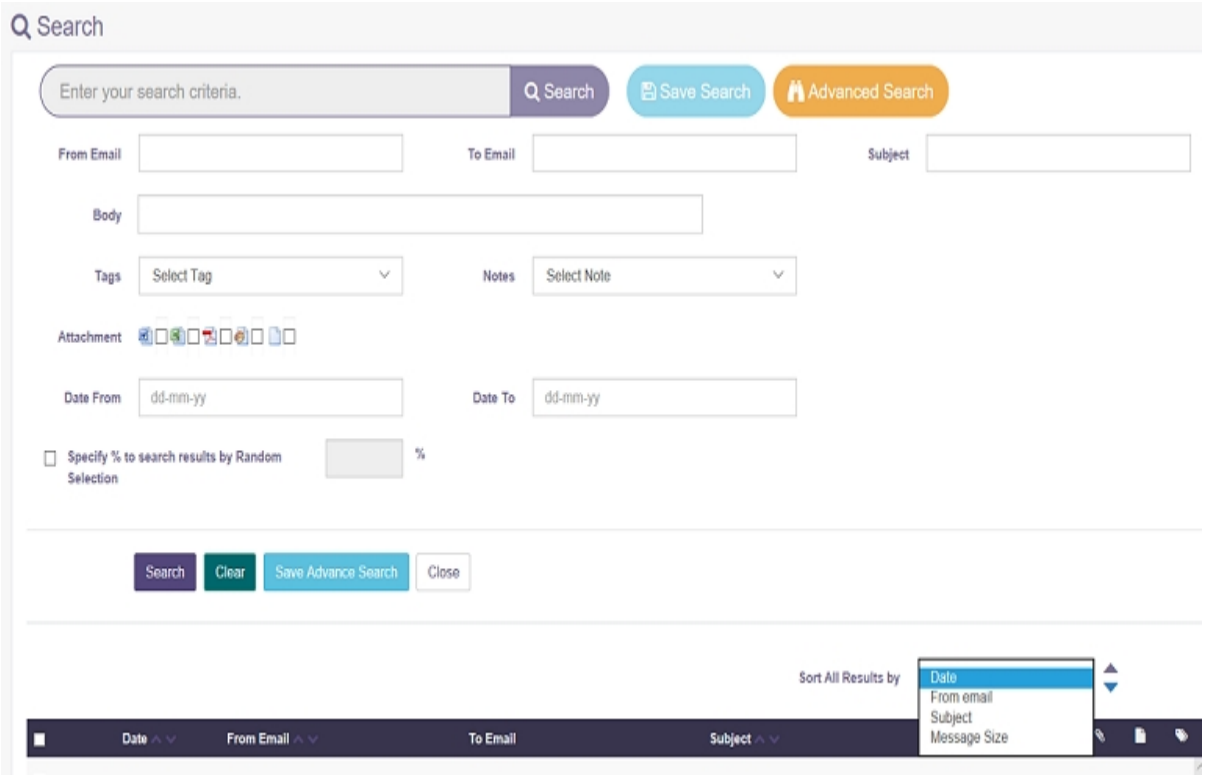
- **View a message:** Click the subject line of any message to view the message inline below the search screen or double click a subject line to view the message full screen in a different tab. To the right an icon each appears to indicate if the email has attachments, notes, and tags. You can download the message or Print. You can also view only the Headers.
- Sorting: Click the arrow icons beside the respective column heading to sort each column.
- **Messages to View:** From the Settings option, you can adjust the number of messages displayed.
- **Tag:** Select one or more messages and apply a tag by typing the tag name on the footer area (see tag icon). To search all messages with the same tag, click **Advanced Search**. From the left pane, click the **References** option to view a list of all registered tags.

  Notes: After opening a message, you can add a note or use an existing note. Apply a note by typing the name in the notes field (see note icon). To search all messages with the same note, click **Advanced Search**. To view a list of all registered notes, from the left pane, click the **References** option.
- **Sort All Results by:** After completing the search, you can filter search results further using the drop-down option of Sort All Results by. The available options are:
  - **Date:** Sort by date of email received.
  - **From email:** Sort by email ID of sender.
  - **Subject:** Sort by Subject of email message.
  - **Message Size:** Sort by size of message.

Advanced Search

The advanced Search gives you more options for finding exactly what you need. For entering query, UDP Archiving lets you use Boolean connector.

For viewing steps in video, click How to Search in UDP Archiving.



When you select advanced search, an expanded set of fields appears. You can query for one or multiple fields to run a search.

Note: You can save query name of search criteria too. After entering the field, click **Save Advance Search** before clicking **Search**.

From Email

Lets you search using sender's email address.

To Email

Lets you search using receiver's email address.

Subject

Lets you search using the text in the subject line of an email message.

Body

Lets you search using the text in the body of an email message.

Tags

Lets you search using the drop-down option that displays existing tags.

Notes

Lets you search using the drop-down option that displays existing notes.

Random Sample

Lets you search desired percentage of available emails. For example, if you enter 10 (%) as random sample and the related available results count is 150, then only 15 random samples of total available results are displayed as search result.

Attachment

Lets you search email by type of attachments.

Date From and **Date To**

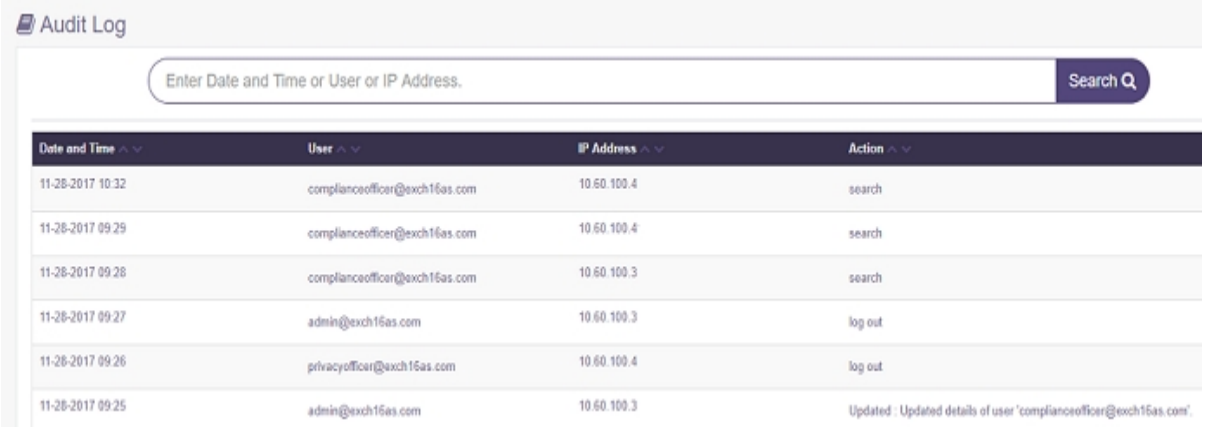
Lets you search using a specific date range.

Sort All Results by: After completing the search, you can filter search results further using the drop-down option of Sort All Results by. The available options are:

- **Date:** Sort by date of email received.
- **From email:** Sort by email ID of sender.
- **Subject:** Sort by Subject of email message.
- **Message Size:** Sort by size of message.

Audit Log

Using Audit Log, Compliance Officer can view the action performed on respective archived email messages and export when required.

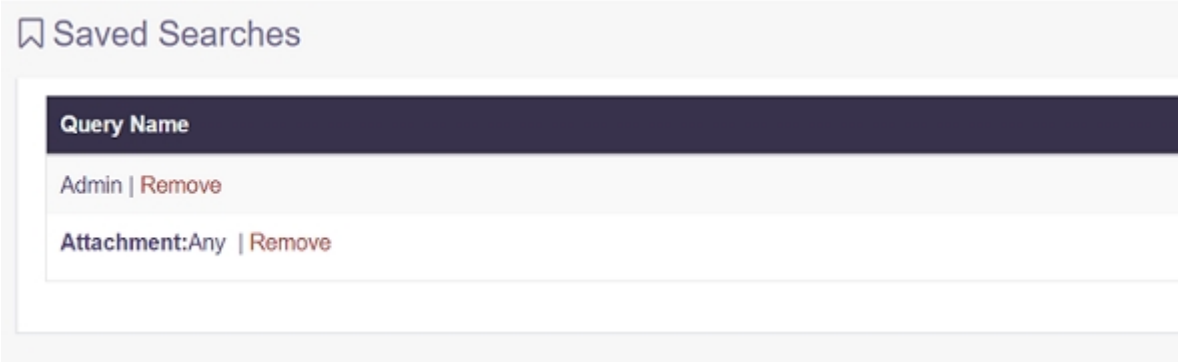


Saved Searches for Compliance Officer

From the left pane, click Saved Searches to view all the simple or advanced search that you have saved in the past. The Saved Searches page display list of searches by the query name that you saved either from Simple search or for Advanced search performed in the past. By clicking on a saved search, the fields are populated again and the search is performed exactly as you performed in the past.

Note: For Advanced search, you can only save the search criteria, not the results.

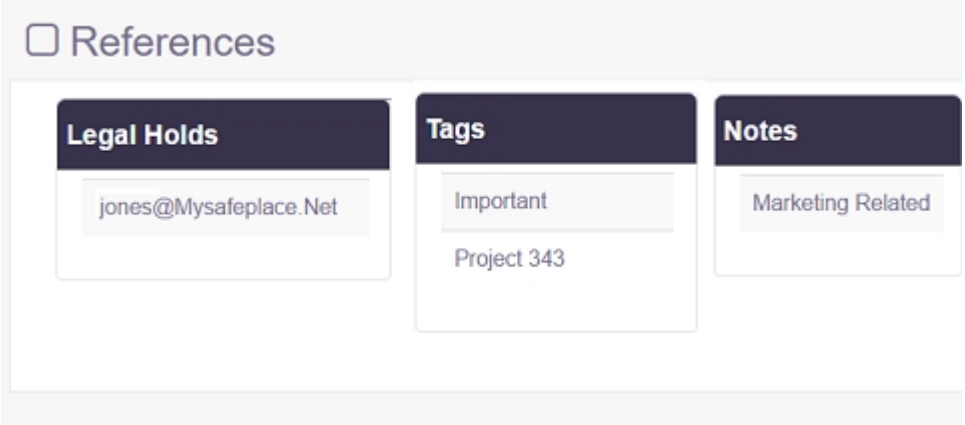
Remove: You can click Remove against the name of any Query Name to delete the search query from the list of Saved Searches.



References

The references page provides a summary of legal hold, all created tags and notes that were applied to messages. From the left pane, click **References** to reach this page. The references help you search and manage the UDP Archiving.

Note: The References page only displays information. You cannot click the displayed terms.



Legal Holds

Displays all email addresses that the administrator specified for legal hold.

Tags

Displays all the tags that you have created for messages.

Notes

Displays all the notes that you have added to messages.

Tags

The page displays all the tags attached to the messages. The page lets you view/edit and remove a tag.

To remove an existing tag, select the check box of tag and click **Remove Tag** placed against that tag. Removing tag deletes the tag from all the attached messages.

To view all messages of the tag, add or modify a description, and schedule purge, click **View/Edit** placed against that tag.

Important!

To purge a tag, you must select the messages associated. After purge, you cannot retrieve a message.

You cannot purge messages that are either put on Legal Hold or associated with other tags.

For more information, view how to add or remove messages from a tag.

Chapter 6: Using Arcserve UDP Archiving as Auditor

The Auditor role is designed for the person who needs access to all messages of the organization. The auditor can be an internal compliance person, Human Resources Administrator or internal or external legal counsel. Each messages are retained as a corporate record and all messages are retrieved as they are sent or received. Once received the messages are indexed (including attachments) to include as part of searchable records, and policies are applied. For example, retention, exception rules, and legal holds that are all set by the system administrator for the company.

This section contains the following topics:

Personal Settings

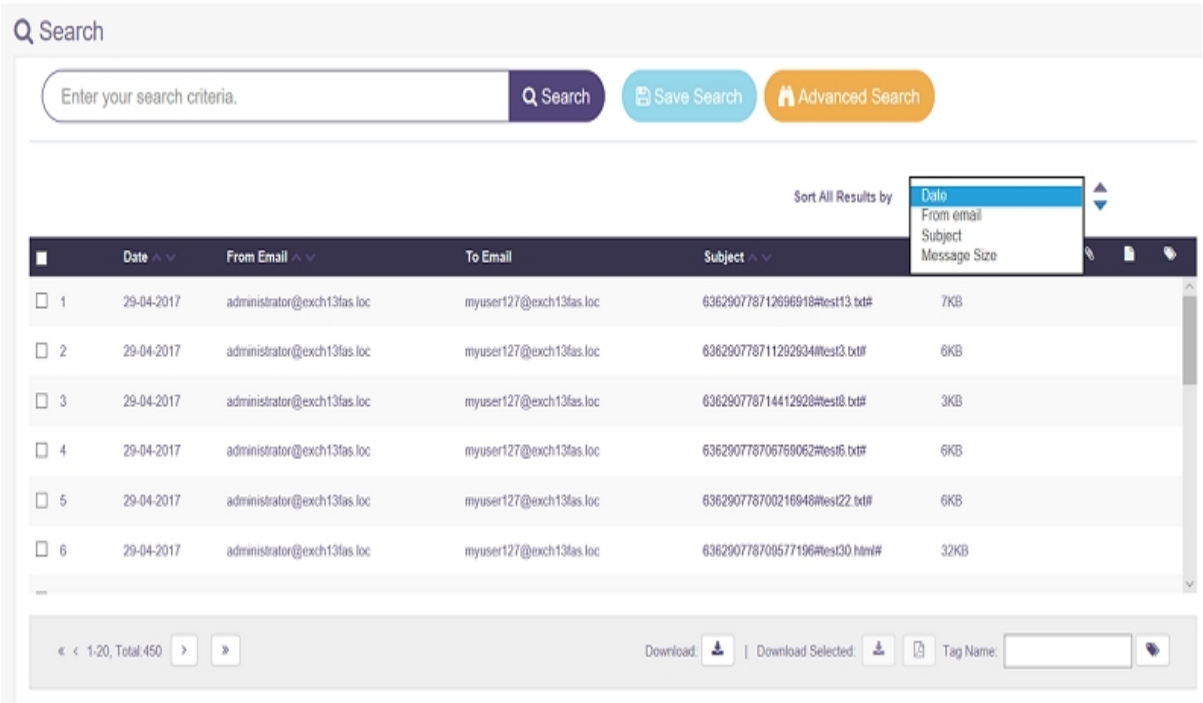
From the UDP Archiving Console, click **Settings** on the top-right corner under your login name to view and modify your personal settings. The settings page has four sections:

- **Access Settings:** Lets you view your access details that the administrator created. You cannot modify details of Access Settings.
- **Profile Picture:** Lets you upload desired picture for your profile.
- **Display Settings:** Lets you manage emails that appear on your dashboard. You can set the number of emails that can appear on one screen. You can also set the language and date format for the emails.

  Note: For **Results per page**, you can select only one of the four options: 10,20,30, and 50.
- **Change Password:** Lets you update your password. You use this option after your first login. Later also you can change password when desired.

Using the Settings tab, you can also download UDP Archiving as Outlook plug-in. To configure, view add UDP Archiving as Outlook plug-in.

Search



After logging into UDP Archiving as an employee, you land into the dashboard. The landing screen is the same screen that appears when you click **Search** from the left pane. Use Simple search only to search content of Subject and Body of an email. For more specific search, use Advanced Search.

For viewing steps in video, click How to Search in UDP Archiving.

The Search page is divided into four parts as per information displayed:

1. **Header:** Includes Search and Advanced Search activities. Comma separated text, Boolean connectors and other functions such as wild cards help you perform simple and advanced search. For Simple search, you can save search term with results. For Advanced Search, you can save only the search terms.
2. **Body:** Displays all the archived emails and their details. Details include the from and to addresses, date of email received, subject, and message size. Some details are marked with symbols. For example, every email has symbols to displays if the mail contains notes and attachment, or has a tag associated.
3. **Footer:** This area of dashboard (or search page) includes multiple options to perform on emails. For example, you can Download all or some messages either as PDF or Email. You can also assign tag to one or more emails.

4. **Result:** Displays the result of any action that you perform in Body or Footer area. For example, if you click a message, the content appears in this area. You can add Notes to the displayed email message. From Footer area if you download any email, the progress appears in this area.

In the dashboard you have many options that include:

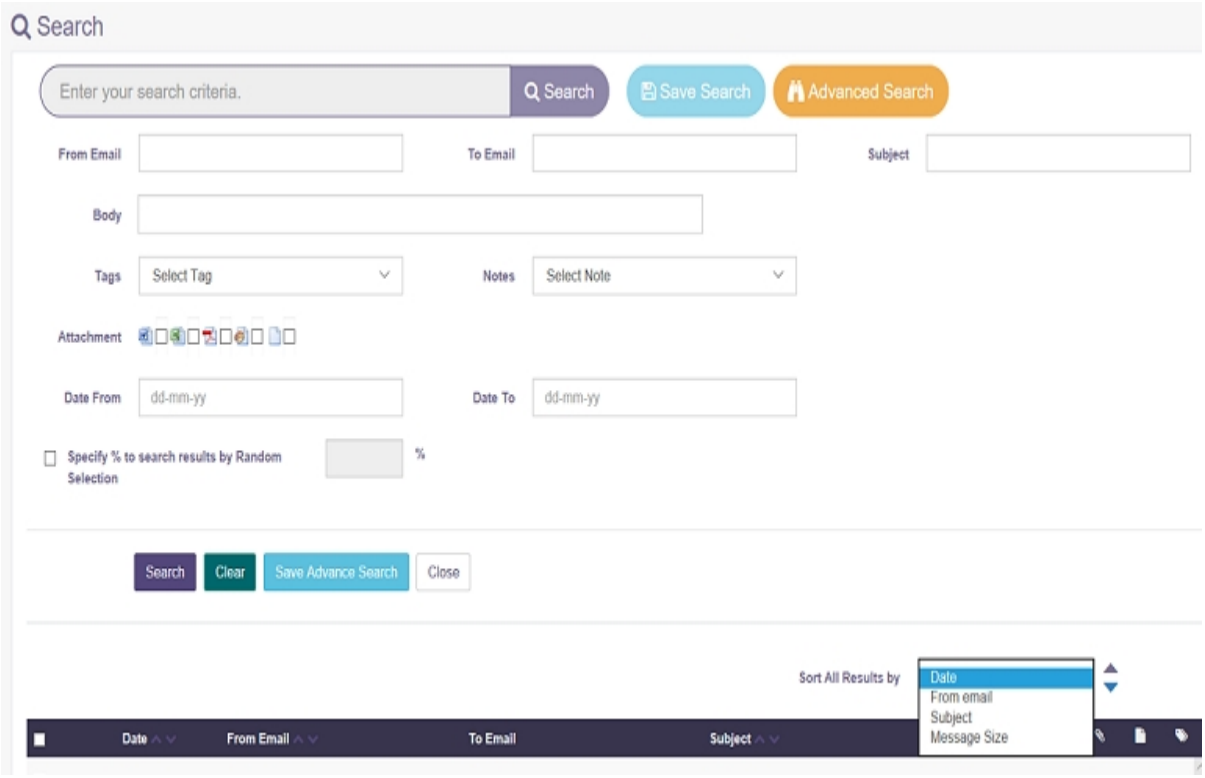
- **View a message:** Click the subject line of any message to view the message inline below the search screen or double click a subject line to view the message full screen in a different tab. To the right an icon each appears to indicate if the email has attachments, notes, and tags. You can download the message or Print. You can also view only the Headers.
- Sorting: Click the arrow icons beside the respective column heading to sort each column.
- **Messages to View:** From the Settings option, you can adjust the number of messages displayed.
- **Tag:** Select one or more messages and apply a tag by typing the tag name on the footer area (see tag icon). To search all messages with the same tag, click **Advanced Search**. From the left pane, click the **References** option to view a list of all registered tags.

  Notes: After opening a message, you can add a note or use an existing note. Apply a note by typing the name in the notes field (see note icon). To search all messages with the same note, click **Advanced Search**. To view a list of all registered notes, from the left pane, click the **References** option.
- **Sort All Results by:** After completing the search, you can filter search results further using the drop-down option of Sort All Results by. The available options are:
  - **Date:** Sort by date of email received.
  - **From email:** Sort by email ID of sender.
  - **Subject:** Sort by Subject of email message.
  - **Message Size:** Sort by size of message.

Advanced Search

The advanced Search gives you more options for finding exactly what you need. For entering query, UDP Archiving lets you use Boolean connector.

For viewing steps in video, click How to Search in UDP Archiving.



When you select advanced search, an expanded set of fields appears. You can query for one or multiple fields to run a search.

Note: You can save query name of search criteria too. After entering the field, click **Save Advance Search** before clicking **Search**.

From Email

Lets you search using sender's email address.

To Email

Lets you search using receiver's email address.

Subject

Lets you search using the text in the subject line of an email message.

Body

Lets you search using the text in the body of an email message.

Tags

Lets you search using the drop-down option that displays existing tags.

Notes

Lets you search using the drop-down option that displays existing notes.

Random Sample

Lets you search desired percentage of available emails. For example, if you enter 10 (%) as random sample and the related available results count is 150, then only 15 random samples of total available results are displayed as search result.

Attachment

Lets you search email by type of attachments.

Date From and **Date To**

Lets you search using a specific date range.

Sort All Results by: After completing the search, you can filter search results further using the drop-down option of Sort All Results by. The available options are:

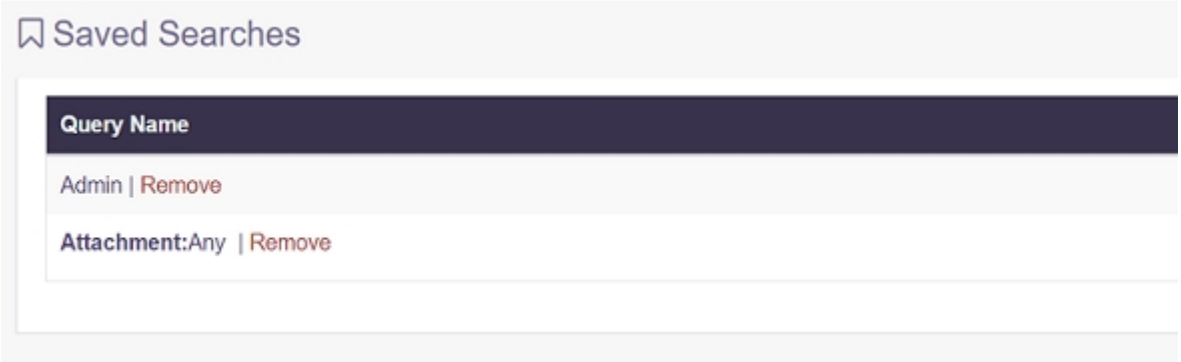
- **Date:** Sort by date of email received.
- **From email:** Sort by email ID of sender.
- **Subject:** Sort by Subject of email message.
- **Message Size:** Sort by size of message.

Saved Searches for Auditor

From the left pane, click Saved Searches to view all the simple or advanced search that you have saved in the past. The Saved Searches page display list of searches by the query name that you saved either from Simple search or for Advanced search performed in the past. By clicking on a saved search, the fields are populated again and the search is performed exactly as you performed in the past.

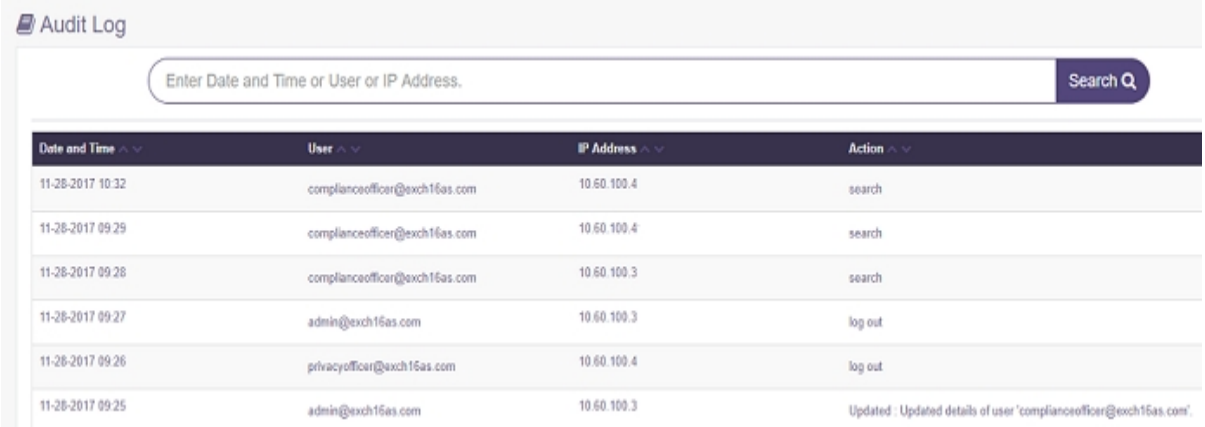
Note: For Advanced search, you can only save the search criteria, not the results.

Remove: You can click Remove against the name of any Query Name to delete the search query from the list of Saved Searches.



Audit Log

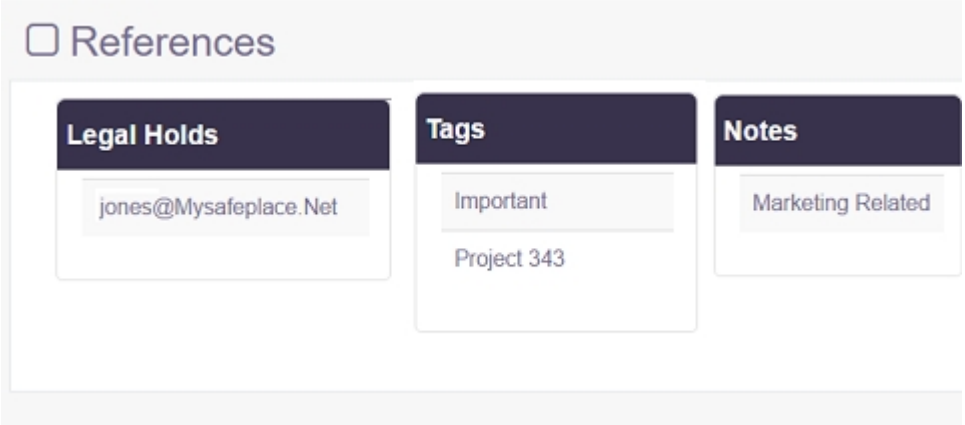
Using Audit Log, Auditor can view the action performed on respective archived email messages and export when required.



References

The references page provides a summary of legal hold, all created tags and notes that were applied to messages. From the left pane, click **References** to reach this page. The references help you search and manage the UDP Archiving.

Note: The References page only displays information. You cannot click the displayed terms.



Legal Holds

Displays all email addresses that the administrator specified for legal hold.

Tags

Displays all the tags that you have created for messages.

Notes

Displays all the notes that you have added to messages.

Tags

The page displays all the tags attached to the messages. The page lets you add a tag, view/edit and remove an existing tag.

To remove an existing tag, select the check box of tag and click **Remove Tag** placed against that tag. Removing tag deletes the tag from all the attached messages.

To view all messages of the tag, add or modify a description, click **View/Edit** placed against that tag.

For more information, view how to add, view/modify or remove a tag.

Chapter 7: Using UDP Archiving as Employee

An administrator provides access to employees to use UDP Archiving. Some of the employees are also assigned the role of a group manager. Depending upon the type of access, employees can view:

- Own messages.
- Messages of all the group members.

  Note: To view messages of others, the administrator must assign the employee role of a group manager.

The employee can access the system through the web interface or through a folder in Outlook. On accessing UDP Archiving, an employee lands at the dashboard. Using search function, an employee can find own messages or of group members.

This section contains the following topics:

Personal Settings

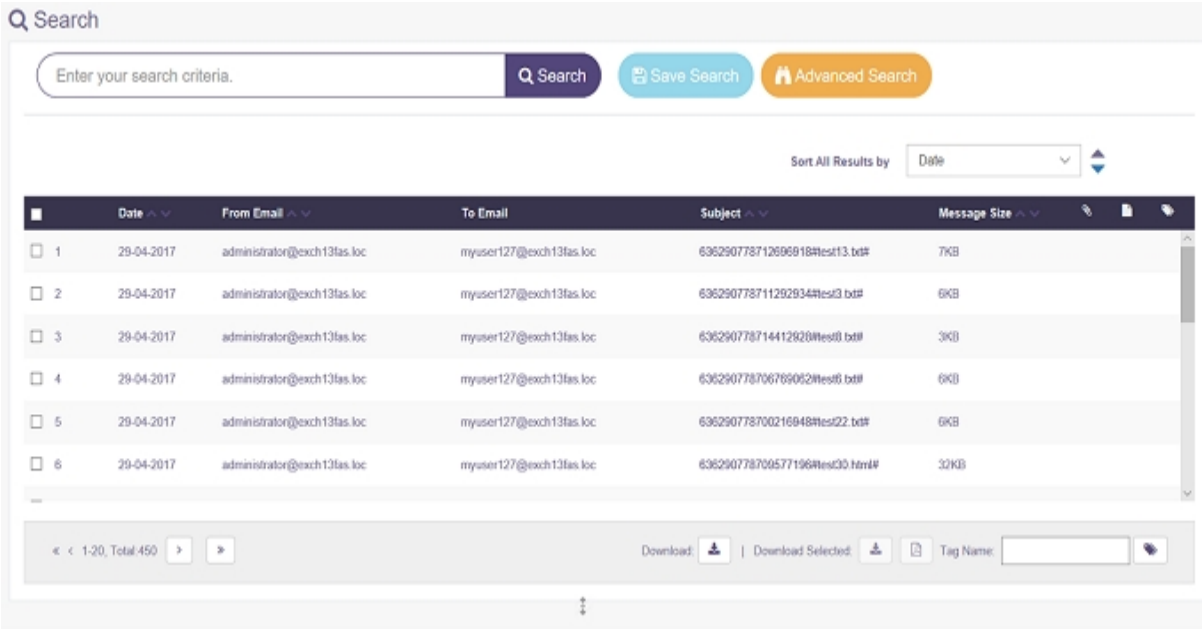
From the UDP Archiving Console, click **Settings** on the top-right corner under your login name to view and modify your personal settings. The settings page has four sections:

- **Access Settings:** Lets you view your access details that the administrator created. You cannot modify details of Access Settings.
- **Profile Picture:** Lets you upload desired picture for your profile.
- **Display Settings:** Lets you manage emails that appear on your dashboard. You can set the number of emails that can appear on one screen. You can also set the language and date format for the emails.

  Note: For **Results per page**, you can select only one of the four options: 10,20,30, and 50.
- **Change Password:** Lets you update your password. You use this option after your first login. Later also you can change password when desired.

Using the Settings tab, you can also download UDP Archiving as Outlook plug-in. To configure, view add UDP Archiving as Outlook plug-in.

Search



After logging into UDP Archiving as an employee, you land into the dashboard. The landing screen is the same screen that appears when you click **Search** from the left pane. Use Simple search only to search content of Subject and Body of an email. For more specific search, use Advanced Search.

For viewing steps in video, click How to Search in UDP Archiving.

The Search page is divided into four parts as per information displayed:

1. **Header:** Includes Search and Advanced Search activities. Comma separated text, Boolean connectors and other functions such as wild cards help you perform simple and advanced search. For Simple search, you can save search term with results. For Advanced Search, you can save only the search terms.
2. **Body:** Displays all the archived emails and their details. Details include the from and to addresses, date of email received, subject, and message size. Some details are marked with symbols. For example, every email has symbols to displays if the mail contains notes and attachment, or has a tag associated.
3. **Footer:** This area of dashboard (or search page) includes multiple options to perform on emails. For example, you can Download all or some messages either as PDF or Email. You can also assign tag to one or more emails.
4. **Result:** Displays the result of any action that you perform in Body or Footer area. For example, if you click a message, the content appears in this area.

You can add Notes to the displayed email message. From Footer area if you download any email, the progress appears in this area.

In the dashboard you have many options that include:

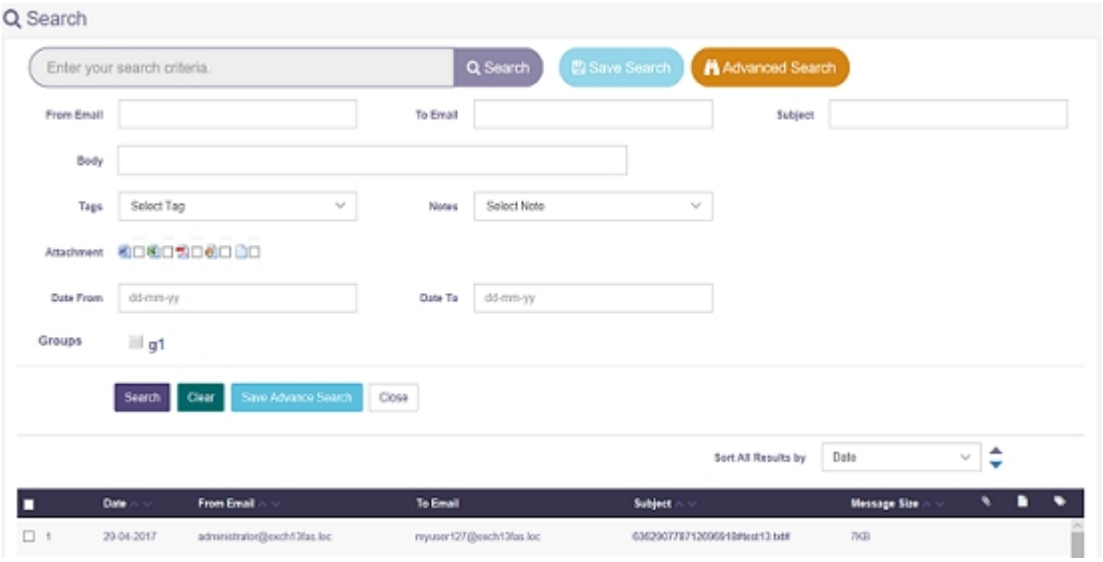
- **View a message:** Click the subject line of any message to view the message inline below the search screen or double click a subject line to view the message full screen in a different tab. To the right an icon each appears to indicate if the email has attachments, notes, and tags. You can download the message or Print. You can also view only the Headers.
- Sorting: Click the arrow icons beside the respective column heading to sort each column.
- **Messages to View:** From the Settings option, you can adjust the number of messages displayed.
- **Tag:** Select one or more messages and apply a tag by typing the tag name on the footer area (see tag icon). To search all messages with the same tag, click **Advanced Search**. From the left pane, click the **References** option to view a list of all registered tags.

  Notes: After opening a message, you can add a note or use an existing note. Apply a note by typing the name in the notes field (see note icon). To search all messages with the same note, click **Advanced Search**. To view a list of all registered notes, from the left pane, click the **References** option.
- **Sort All Results by:** After completing the search, you can filter search results further using the drop-down option of Sort All Results by. The available options are:
  - **Date:** Sort by date of email received.
  - **From email:** Sort by email ID of sender.
  - **Subject:** Sort by Subject of email message.
  - **Message Size:** Sort by size of message.

Advanced Search

Using advanced Search, employee can use multiple options to search emails. Employee can also access a group using the Advanced Search option. For entering search terms, UDP Archiving lets you use Boolean connector.

For viewing steps in video, click How to Search in UDP Archiving.



When you select advanced search, an expanded set of fields appears. You can query for one or multiple fields to run a search.

Note: You can save query name of search criteria too. After entering the field, click **Save Advance Search** before clicking **Search**.

From Email

Lets you search using sender's email address.

To Email

Lets you search using receiver's email address.

Subject

Lets you search using the text in the subject line of an email message.

Body

Lets you search using the text in the body of an email message.

Tags

Lets you search using the drop-down option that displays existing tags.

Notes

Lets you search using the drop-down option that displays existing notes.

Attachment

Lets you search email by type of attachments.

Date From and **Date To**

Lets you search using a specific date range.

Groups

Lets you search emails of a specific group.

Sort All Results by: After completing the search, you can filter search results further using the drop-down option of Sort All Results by. The available options are:

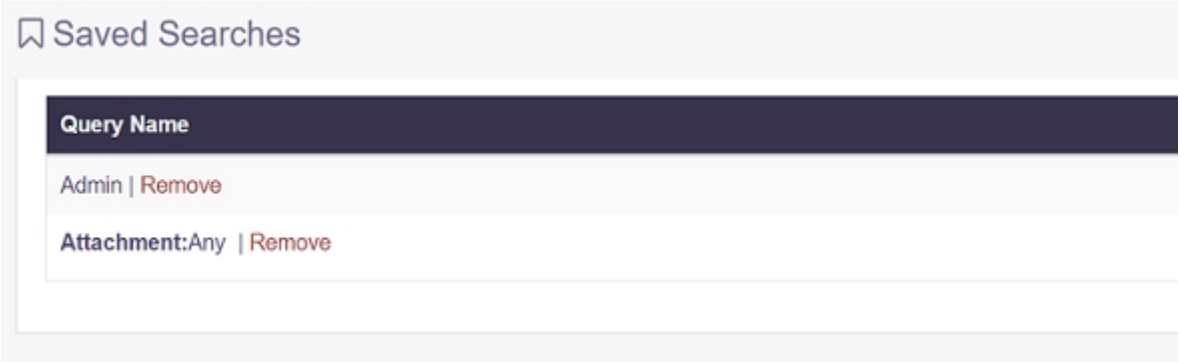
- **Date:** Sort by date of email received.
- **From email:** Sort by email ID of sender.
- **Subject:** Sort by Subject of email message.
- **Message Size:** Sort by size of message.

Saved Searches

From the left pane, click Saved Searches to view all the simple or advanced search that you have saved in the past. The Saved Searches page display list of searches by the query name that you saved either from Simple search or for Advanced search performed in the past. By clicking on a saved search, the fields are populated again and the search is performed exactly as you performed in the past.

Note: For Advanced search, you can only save the search criteria, not the results.

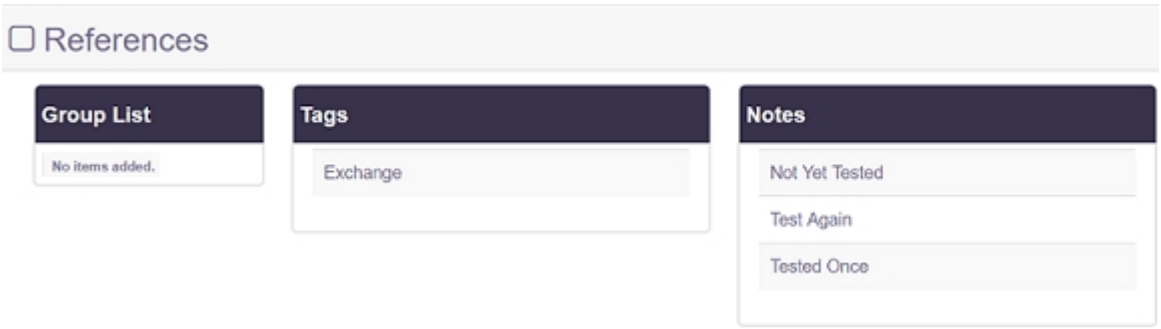
Remove: You can click Remove against the name of any Query Name to delete the search query from the list of Saved Searches.



References for Employee

The references page provides a summary of existing Group Lists, created tags, and notes already added to messages. From the left pane, click **References** to reach this page. The references help you search and manage the UDP Archiving.

Note: The References page only displays information. You cannot click the displayed terms.



Group List

Displays name of all the groups to which the administrator has added the employee.

Tags

Displays all the tags that you have created for messages.

Notes

Displays all the notes that you have added to messages.

Chapter 8: Working With UDP Archiving

The section contains the following topics:

How to Add UDP Archiving as Outlook Plug-in

UDP Archiving allows access directly from Microsoft Outlook. Installing a plug-in at your machine lets you access and import archived emails of any valid user without opening the UDP Archiving Console. You can also launch the Console directly from Outlook.

For viewing steps in video, click How to Add UDP Archiving as Outlook Plug-in.

Prerequisites:

- .NET Framework 4.5.2 (To download, click link)
- Visual Studio 2010 Tools for Office Runtime (To download, click link)

  Note: On detecting that the components are not installed, the plug-in installer automatically installs the components. But, in Windows 7 or earlier editions you may need to manually install the dependencies.
- Windows 7 or later with .Net Framework 4.5.2
- Windows Server 2012 or higher version
- Microsoft Office 2010 or higher version

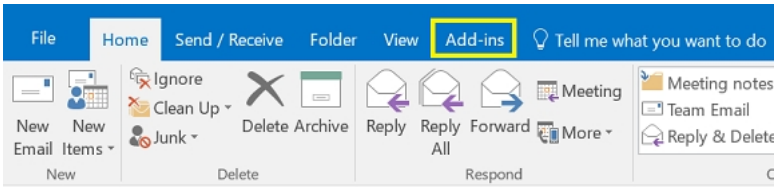
Follow these steps:

1. Install UDP Archiving Plugin .exe file.

   Select the Plug-in option according to your available outlook versions (x-86 or x-64)

   Note: Request your administrator for the Plug-in.
2. Open your outlook *AFTER* installing the plug-in.

   The Outlook menu displays Add-ins as a tab.



3. Click Add-ins.

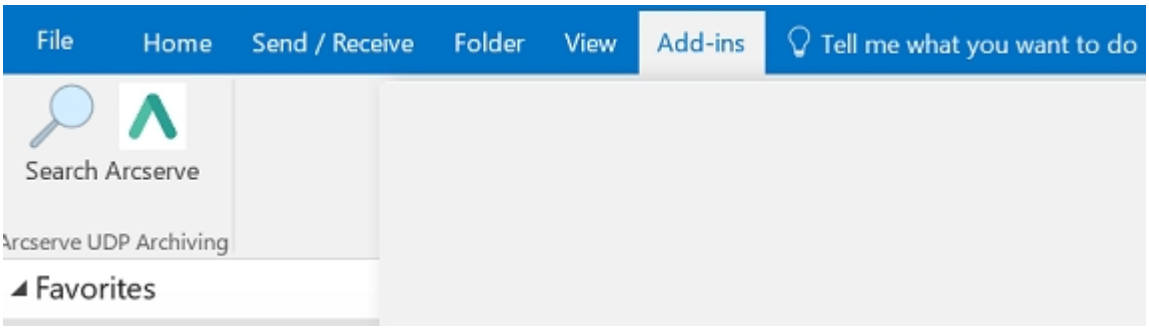
   Add-ins for UDP Archiving plug-in displays icons for Arcserve and Search.

   Arcserve

   Leads to the login page of UDP Archiving URL that you provide in Settings. Provide credentials and login.

Search

Opens Arcserve UDP Archiving dialog displaying two tabs, Settings and Search. First time user needs to enter details using Settings.



4. Click Settings and enter the following details:

UDP Archiving Address

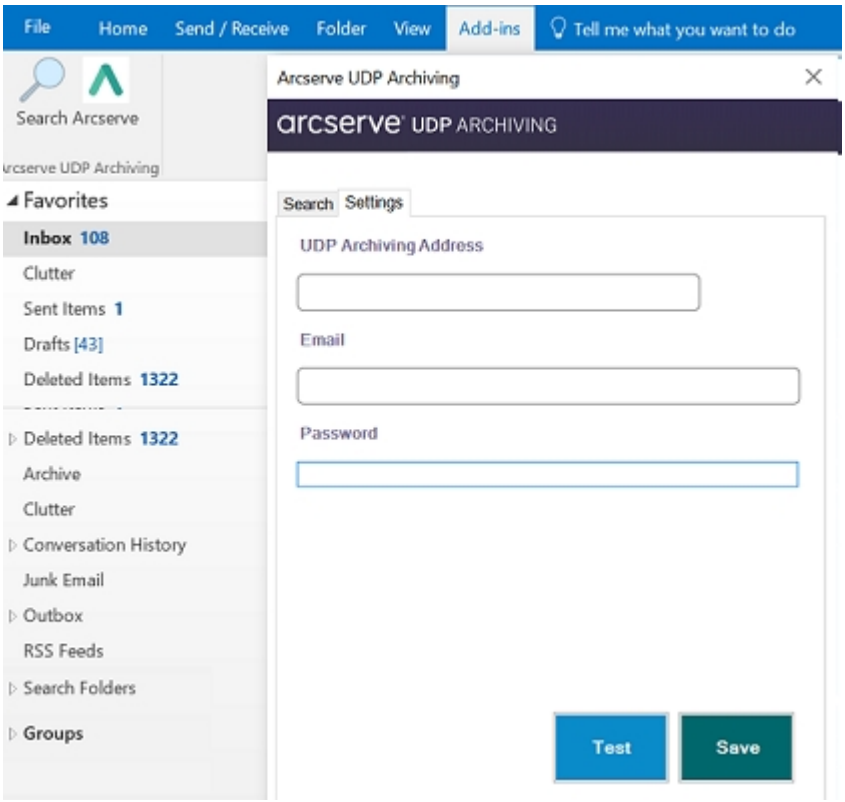
Enter the URL to access UDP Archiving.

Email

Enter the email of the user whose email messages you want to view and download.

Password

Enter password for the email provided.



5. Click **Test**.

   Valid details display the following message:

   Login Success.

6. Click **Save**

   The following message confirms that you can search and access messages of the entered email id:

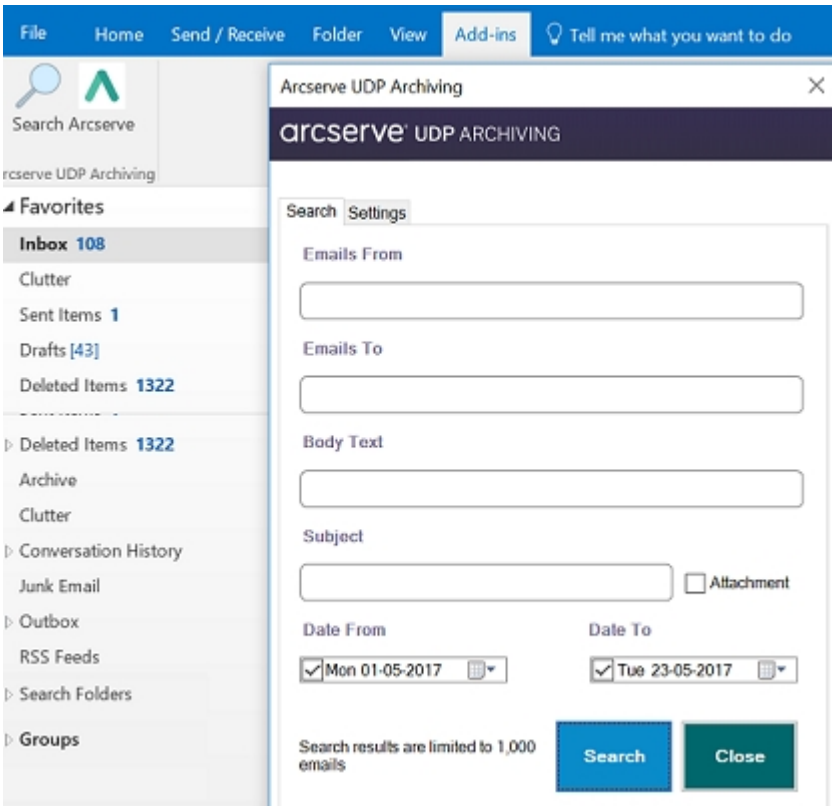
   Successfully Saved.

   The UDP Archiving plug-in is configured for outlook. Now, you can start searching the emails.

7. Click the **Search** tab.

   The screen contains multiple parameters to search email.

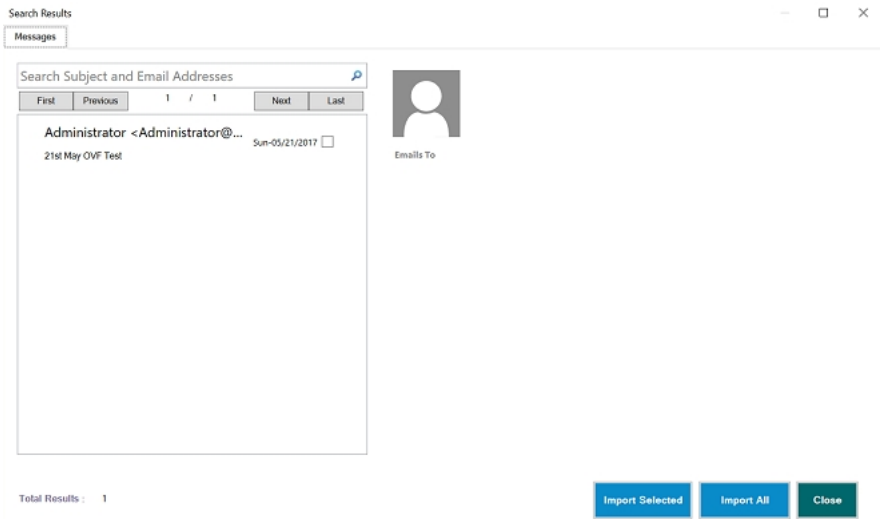
   Note: Auditor can access email messages of all while employees can access own email.



8. From the Search screen, select one or more parameters and click **Search**.

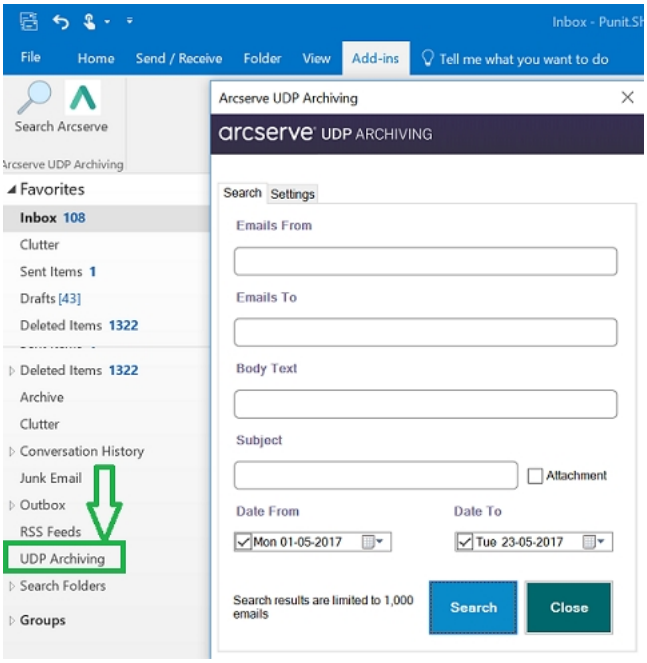
   The matching results appear in the **Search Results** dialog. You can import all or some messages.

   Note: Only the latest 1000 results appear.



9. Click **Import All** or select some emails and click **Import Selected**.

A confirmation message appears and the emails are imported to a folder named UDP Archiving. The folder is created by default.



How to protect UDP Archiving using UDP Linux Agent

Using UDP Linux Agent, you can protect the UDP Archiving server. Once the UDP Archiving machine is protected by UDP, you can recover the machine in case of a crash or when machine connectivity is lost due to any circumstances. Following backup destinations are supported:

- RPS (Deduplication Data store/Non-Deduplication Data store)
- CIFS

To protect UDP Archiving using UDP Linux agent, perform the following steps:

- Review the Prerequisites and Considerations
- Add UDP Archiving as Linux Node
- Create and Run a Backup Plan
- Perform Bare Metal Recovery (BMR)

Review the Prerequisites and Considerations

Prererquisites:

- Arcserve UDP v6.5 Update 1 is installed on the Console /Server where UDP Archiving machine serves as Client.
- Arcserve UDP Linux Agent is installed on UDP Archiving machine, if you want to add the UDP Archiving machine using either of the two options: Add Linux Backup Server or Add UDP Archiving node.

  To install Arcserve UDP Linux Agent, click link.
- To perform BMR, at least 1024 MB free memory is available on your machine to boot and run the Live CD.
- The CIFS utility is installed on the UDP Archiving node to run backup.

  Note: Use the command **apt-get install cifs-utils** to install the utility.
- Linux Backup proxy.

  Note: Supports all the supported platforms of Arcserve UDP Linux backup Server.

Considerations:

- Before adding Linux node, Linux Backup server must be available.
- Agentless Backup is supported for both VMware and Hyper-V. For details, view Arcserve UDP v6.5 Update 1 Compatability Matrix. From the *Select Component* drop-down option, *select Supported Hypervisors for Host-Based Agentless Backup*.

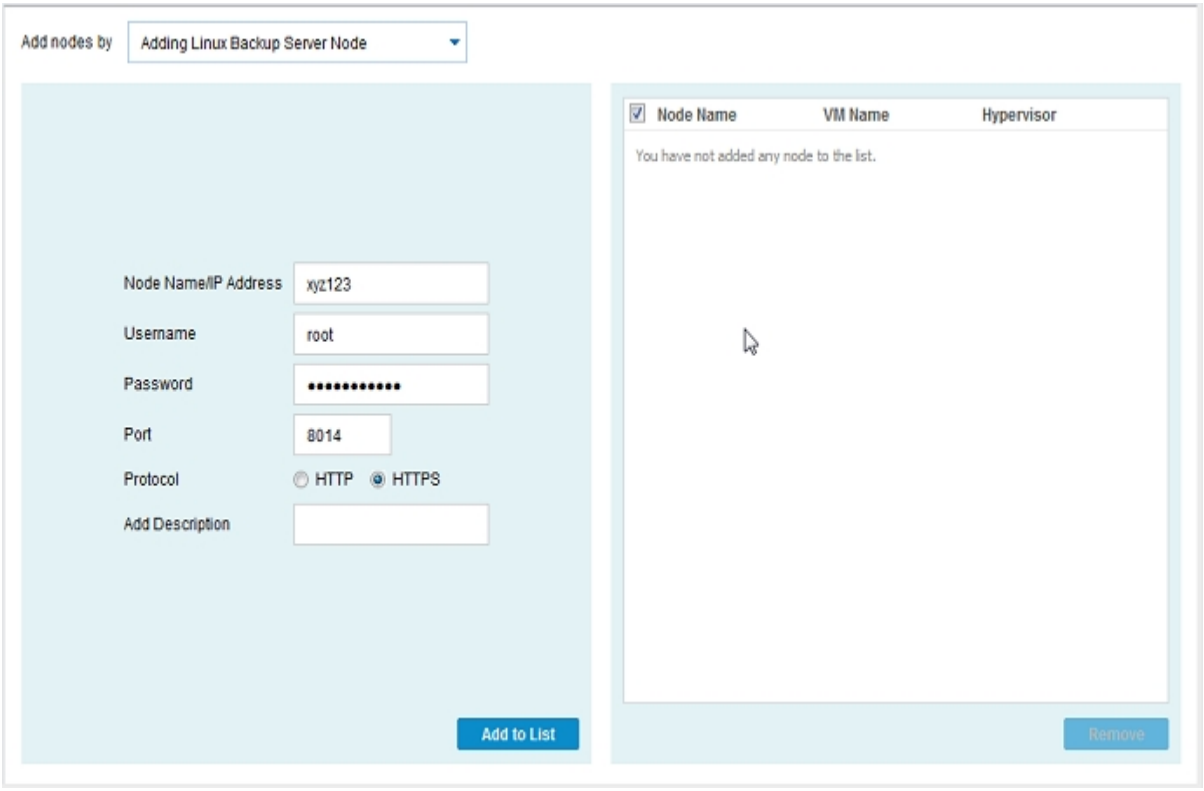
Add UDP Archiving as Linux Node

To protect UDP Archiving, creating a node and running the backup job are primary requirements. Use UDP Archiving Super Admin credentials to add as a Linux node in the Arcserve UDP Console.

Important! Add Linux Backup server first before adding Linux node.

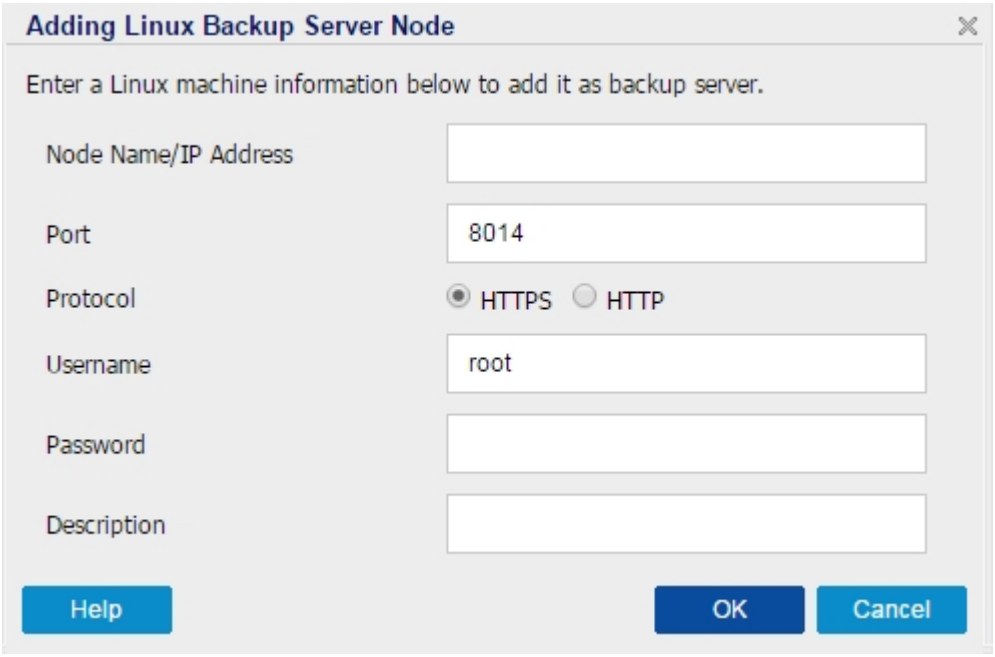
Follow these steps:

1. Perform the following steps to add Linux Backup Server Node:
    a. From UDP Console v6.5 Update 1, click Add Node.
    b. From the Add Node dialog, select Adding Linux Backup Server node.



    c. Enter the details and add.

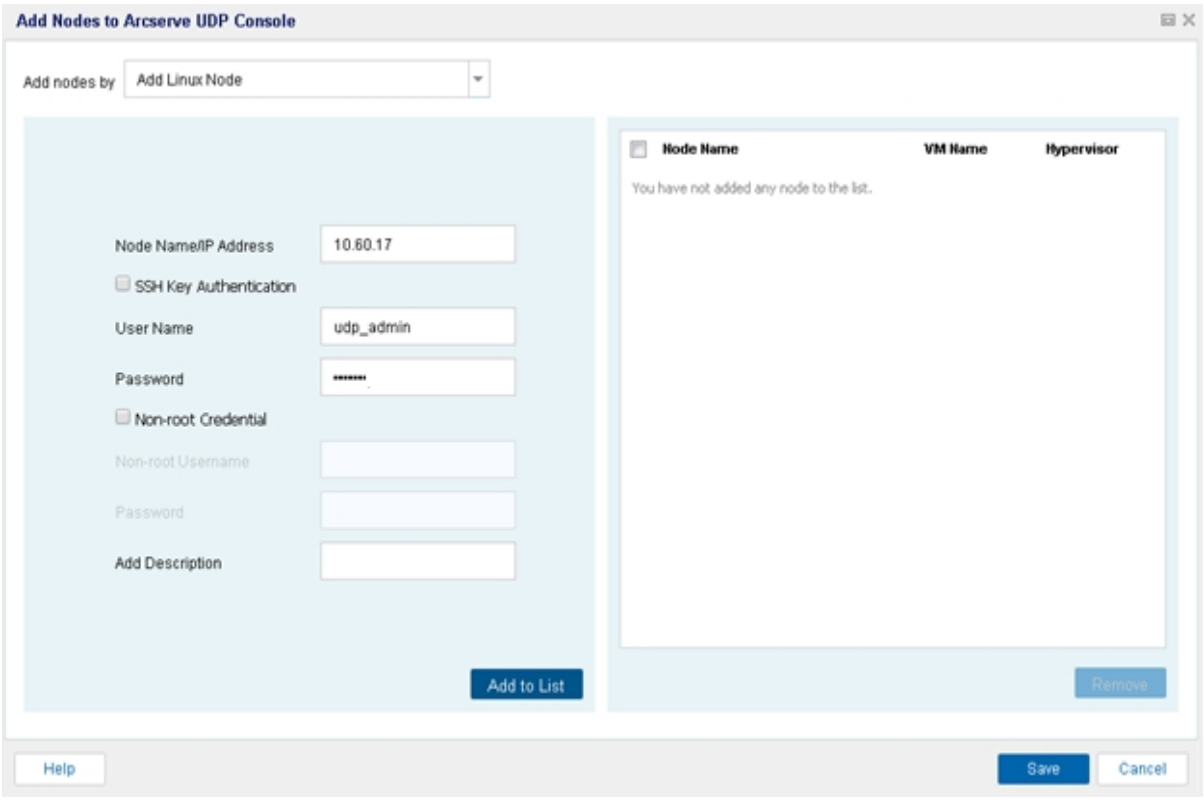
    The following dialog appears when you add Linux Backup Server node from the Backup: Agent-Based Linux task, while configuring Plan:



The details of the selected option are displayed.

You can log into the Linux Backup Server from the Arcserve UDP Console v6.5 Update 1 only when you perform a BMR.

2. Perform the following steps to Add Linux node.
    a. From UDP Console v6.5 Update 1, click Add Node.
    b. From the Add Node dialog, select Add Linux node.



c. Enter details of UDP Archiving Super Admin and add the node.

Create and Run a Backup Plan

To protect nodes, you need to create a plan. A backup plan for Linux nodes consists of a backup task. This backup task lets you specify the nodes you want to protect, the backup destination, and the backup schedule. The backup destination supported for protecting UDP Archiving can be a data store in a recovery point server or a CIFS destination on Windows or NAS.

The section contains the following topics:

Add a Backup Plan

A backup plan includes a backup task that performs a backup of the UDP Archiving node and stores the data to the specified supported destination.

Follow these steps:

1. Click the resources tab.
2. From the left pane, navigate to Plans, and click All Plans.

   If you have added any plans, these plans will be displayed in the center pane.
3. On the center pane, click Add a Plan.

   The Add a Plan page opens.
4. Enter a plan name.
5. (Optional) Select Pause this plan check box.

   The plan will not run until you clear the check box to resume the plan.

   Note: When a plan is paused, the running job is not paused. All corresponding scheduled jobs associated with that plan are paused. However, you can manually run the paused jobs. For example, backup job for a node can be run manually even if the respective plan is paused. When you resume the plan, the pending jobs will not resume immediately. After you resume the plan, the pending jobs will run from the next scheduled time.
6. From the Task Type drop-down menu select Backup: Agent-Based Linux.

Now, specify the Source, Destination, Schedule, and Advanced settings.

Specify the Source

The Source page lets you specify the source nodes that you want to protect. You can select more than one nodes in a plan. If you have not added any nodes to the Console, you can add nodes from the Source page.

Note: You can save a plan without adding any source nodes but the plan will not be deployed unless you add any nodes.

Follow these steps:

1. Click the **Source** tab.
2. Select the Linux Backup Server from the drop-down list
3. (Optional) Click **Add** to add a new Linux Backup Server to the list.
4. Click **Add Nodes** and select one of the following options:

   Select Nodes to Protect

   Opens the Select Nodes to Protect dialog and you can select the nodes from the displayed list. Select this option if you have already added the nodes to the Console.

   Adding Linux Nodes

   Opens the Add Nodes to Arcserve UDP Console dialog. Select this option to manually add the nodes to protect.

5. Select the nodes from the Available Nodes column and click the **Add all nodes or Add selected nodes** button.

   The selected nodes are displayed in the Selected Nodes column.

6. Click **OK** to close the dialog.
7. (Optional) Provide the details for the following options:

   Filter volumes for backup

   Select either Include or Exclude from the drop-down list. Include specifies that only the specified volumes will be included for backup. Any volume that is not specified will not be backed up. Excluded specifies that the volumes will be excluded from the backup.

   Files/folders to be excluded

   Specify the files and folders that you do not want to backup for all the listed nodes. If you do not want to backup multiple files and folders, separate each file and folder using a colon (:). Provide the full path of the file and folder that you want to exclude.

The source is specified.

Specify the Destination

The destination is a location where you store the backup data. You must at least specify the destination to save the plan.

Follow these steps:

1. Click the **Destination** tab.
2. Select one of the following as Destination Type:

   Local disk or shared folder

   Specifies that the backup data is stored at a local disk or shared folder.

   Arcserve UDP Recovery Point Server

   Specifies that the backup destination is a recovery point server. If you select this option, then data is stored as recovery points. You cannot store data as recovery sets.
3. If you have selected Local disk or shared folder, then provide the following details:
   - If you have selected CIFS share, then type the Backup Destination detail in the following format:

     //hostname/share_folder

     Note: The shared folder name cannot contain any spaces.

     Arcserve currently supports protecting UDP Archiving node to CIFS destinations on Windows and NAS.

     a. Select a compression level from the Compression drop-down list to specify a type of compression that is used for backup.

        Standard Compression

        Specifies that this option provides a good balance between the CPU usage and the disk space usage. This compression is the default setting.

        Maximum Compression

        Specifies that this option provides the highest CPU usage (lowest speed), but also has the lowest disk space usage for your backup image.

     b. Select an algorithm from the Encryption Algorithm drop-down list and type the encryption password, if necessary.

c. Select the type of encryption algorithm that you want to use for backups.

d. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. The Arcserve UDP Agent (Linux) data protection solution uses secure, AES (Advanced Encryption Standard) encryption algorithms to achieve the maximum security and privacy of your specified data.

- A full backup and all its related incremental backups must use the same encryption algorithm.
- The encryption algorithm for an incremental backup has changed, you must perform a full backup.

For example, if you change the algorithm format and then you run an incremental backup, then the backup type automatically converts to a full backup.

e. When an encryption algorithm is selected, you must provide (and confirm) an encryption password.

- The encryption password is limited to a maximum of 23 characters.
- A full backup and all its related incremental backups use the same password to encrypt data.

4. If you have selected Arcserve UDP Recovery Point Server as Destination Type, provide the following details:

a. Select a recovery point server.

b. Select a data store. The list displays all data stores that are created at the specified recovery point server.

c. Provide a session password. The session password is optional when the backup destination is an unencrypted RPS data store.

d. Confirm the session password.

The destination is specified.

Specify the Schedule

From the Schedule tab, specify a schedule for the job to run.

Specify the Advanced Settings

Advanced Settings lets you include additional settings to the plan. Include the options applicable.

Perform a Manual Backup

Typically, backups are performed automatically and are controlled by the schedule settings. A manual backup provides you the option to back up your nodes on a need basis.

Follow these steps:

1. From the Console, click the **resources** tab.

   Nodes are displayed in the center pane.
2. Select the nodes that you want to backup and that has a plan assigned to it.
3. On the center pane, click **Actions**, **Backup Now**.

   The Run a backup now dialog is displayed.
4. Select a backup type and optionally provide a name for the backup job.
5. Click **OK**.

   The backup job runs.

The manual backup is successfully performed.

Verify the Backup

To verify your backup, confirm that you have successfully created the backup plan. After you verify that the plan is created successfully, confirm whether the backup job is running once it gets triggered. You can verify the status of backup jobs from the jobs tab.

Follow these steps to verify plans:

1. Click the **resources** tab.
2. From the left pane, navigate to Nodes, and click **All Nodes**.

   A list of all nodes is displayed on the center pane.
3. Verify that plans are mapped with nodes.

Follow these steps to verify backup jobs:

1. Click the **jobs** tab.
2. From the left pane, click **All Jobs**.

   The status of each job is listed on the center pane.
3. Verify that the backup job is successful.

The backup job is verified.

Troubleshooting: Job Status, Job History, and Activity Log are Not Visible

Symptom

I cannot see the job status, job history, and activity log for Linux nodes in Arcserve UDP Console.

Solution

Linux Backup Server is unable to connect to Arcserve UDP using the host name.

Follow these steps:

1. Create the server_ip.ini file at the following location of Arcserve UDP:

   "UDP installation path"\Management\Configuration\server_ip.ini

2. Enter the IP address of Arcserve UDP in this file.
3. Log into the Arcserve UDP Console and update Linux Backup Server and Linux nodes.

   Note: Linux Backup Server can be updated only from Linux Backup Server Groups, where all the Linux backup servers are listed.

   The job status, job history, and activity log are visible.

Perform Bare Metal Recovery (BMR)

A BMR restores the operating system and software applications, and recovers all the backed-up data. BMR is the process of restoring a computer system from bare metal. Bare metal is a computer without any operating system, drivers, and software applications. After the restore is complete, the target machine automatically reboots in the same operating environment as the backup source node and all data is restored.

Note: Only the normal BMR is supported. Instant BMR, Instant BMR with auto-recovery of data, and Migration BMR are not supported.

A complete BMR is possible because when you back up data, the backup also captures information related to the operating system, installed applications, drivers, and so on.

You can perform a BMR using the IP address of the target machine. Once you boot the target machine using the Arcserve UDP Agent (Linux) Live CD, you can get the IP address of the target machine.

Note: Machine can boot up. Only one NIC is configured.

The section contains the following topics:

- Review the BMR Prerequisites
- Open BMR Wizard
- Create a Bootable Live CD
- Select Session to Run BMR
- Select Target Machine
- Select Advance Settings
- Review Summary and Run BMR job

Review the BMR Prerequisites and Considerations

Consider the following prerequisites and considerations before starting BMR:

- Only Backups and normal BMR are supported.
- A valid recovery point and the encryption password, if any, to perform BMR is available.
- A valid target machine for BMR is available.
- The Arcserve UDP Agent (Linux) Live CD is created.
- To perform a BMR using the IP address, the IP address of the target machine using the Live CD is available.
- The recovery point is from the Linux Agent-based backup.
- When a BMR is performed, ensure that the machine is recovered with the same hostname and IP address as that of the UDP Archiving server.

Note: Restore options are not supported for the current release. When selected as the source node, you need to add UDP Archiving node using the option Add Linux node.

Navigate to BMR Wizard

As the first step, from UDP Console v6.5 Update 1 you need to open the BMR wizard.

Follow these steps:

1. From Arcserve UDP Console v6.5 Update 1, right-click the desired UDP Archiving node and click **Restore**.

   The Linux Backup server interface opens with a pop-up message.

2. From the pop-up message, select BMR.

   The BMR Wizard opens.

Create a Bootable Live CD

Before performing a BMR using the IP address, you need to get the IP address of the target machine. A BMR does not have any IP address initially. You need to boot BMR using the default Live CD that is Arcserve UDP Agent (Linux) v6.5 Update 1 Live CD. After getting the IP address of the target machine, you can configure the static IP of the target machine.

The target machine boots into the Arcserve UDP Agent (Linux) v6.5 Update 1 Live CD environment. On the screen, the IP address of the target machine is displayed.

To create bootable live CD, you need to download the live CD from BMR wizard on Arcserve UDP v6.5 Linux Agent interface and then use on your target machine.

Follow these steps:

1. From the **Backup Server** tab of BMR Wizard, click the link: **Click here to download Live CD**.

   Live CD is downloaded. After that you can perform a Bare Metal Recovery (BMR). Use this Live CD to get the IP address of the target machine, required during the BMR job.

2. Insert the Live CD into the CD-ROM drive of the target node.
3. Boot the target machine from CD-ROM.

As a storage manager, you can create a bootable Live CD. When created, this bootable Live CD contains a complete read-only image of the computer operating system, and can be used to provide a temporary operating system functionality. This Live CD includes all your system settings and operating system files.

After getting the IP address, proceed to the next step at BMR Wizard.

Select Session to Run BMR

The **Recovery Point** tab lets you assign a session to run BMR. Before selecting a session, consider whether the type of session associated is full, incremental or verify. For more information about backup types, click link.

Considerations:

- Incremental backup is converted to Full backup if the UDP Archiving machine is rebooted and destination is deduplication data store.
- Full / Incremental backup is converted to Verify backup when:
  - the UDP Archiving machine has been rebooted and destination is non-deduplication data store / CIFS.
  - the backup destination is changed from deduplication to non-deduplication data store or vice-versae.

Full Backup Session

When you perform BMR of UDP Archiving machine selecting Full backup session as **Type**, the same count of licenses consumed on the UDP Archiving server at the time of full backup is reflected on the recovered machine.

For example, when you perform Full backup of UDP Archiving that has consumed 100 licenses, the same number of licenses are reflected after the BMR job is completed using that session.

Incremental Backup Session

When you perform BMR of a UDP Archiving machine selecting incremental backup session as **Type**, the same count of licenses consumed on the UDP Archiving server at the time of an incremental backup is reflected on the recovered machine.

For example, when you perform the incremental backup of UDP Archiving that has consumed an additional 50 licenses with 100 licenses consumed in the Full backup session, then the same number of licenses are reflected after the BMR job is completed using that session.

From the Recovery Point tab, select details and assign a session.

Follow these steps:

1. Select a session location (RPS/CIFS).
2. Select a data store and click **Connect**.

   List of nodes related to the selected data store is populated.

3. Select a node from the drop-down list of Machine.
4. Select date range from Date filter and click Search.

   Note: By default the current date range appears.

   List of sessions running for the selection made appear with details.
5. From the list of sessions, select a session and enter password.
6. Disk name and disk size appear.

   Note: If the disk size is less than 16 GB, modify your target machine to increase the size to 16 GB or more before clicking Next. If the disk size is less than 16 GB, CD does not boot up.
7. Click **Next**.

   The Target Machine screen appears.

Select Target Machine

The Target Machine tab lets you define network details for the target.

Follow these steps:

1. Enter IP address and Host Name.

   Note: To modify host name or IP later, see Assigning a Static IP Address/ Host Name.

2. Select one of the following network options:

   - DHCP: Enter the IP address received after running Live CD.
   - Static IP: Enter details for IP Address, Subnet Mask, and Default Gateway.

   Note: Do not select checkboxes for Instant BMR as current version of UDP Archiving supports only normal BMR.

Assigning an IP Address / Host Name

Use one of the three options mentioned below to get the IP address or host name.

Assign a DHCP IP Address to the recovered machine

You can opt to assign a DHCP IP Address to the recovered machine while configuring for the BMR on the Arcserve UDP Agent (Linux).

To assign the Static IP use the following steps:

1. Open Putty.
2. Login using UDP Archiving Console Super Admin credentials.
3. Type *sudo setbox*.
4. Type *sudo reboot* to restart.

Assign a Static IP Address/ Host name to the recovered machine

You can opt to assign a Static IP Address / Host name to the recovered machine while configuring for the BMR on the Arcserve UDP Agent (Linux) v6.5 Update 1.

Assign a Static IP Address/ Host Name after the recovered machine is up

To modify the host name or IP address after the recovery is performed, contact Arcserve Support.

Select Advanced Settings

The Advanced Settings tab helps you customize settings when required. The option Run Now is selected by default.

Use the default **Run Now** option and click Next.

Review Summary and Run BMR Job

The Review Summary tab lets you verify the details to help you modify when required before running the job.

Click Submit after verifying the details and the BMR Job runs.

After a successful job run, the target machine is ready to use UDP Archiving.

How to Modify Host Name of UDP Archiving Server

You can modify the host name of the UDP Archiving server that is assigned when UDP Archiving is installed.

Follow these steps:

1. Create a .sh file and add the following content:

   ```
   #!/bin/bash
   sudo -- sh -c 'echo "<hostname.domain.com>" > /etc/hostname'
   sudo -- sh -c 'echo "127.0.0.1 hostname.domain.com " >> /etc/hosts'
   sudo invoke-rc.d <hostname>.sh start
   sudo invoke-rc.d networking force-reload
   sudo invoke-rc.d network-manager force-reload
   ```

   Note: Replace the *<hostname.domain.com>* and *<hostname>* with appropriate values based on the requirements of your organization.

2. Save the file and run the below command to grant permissions to the file:

   sudo chmod 777 <file name>.sh

3. Run the following command to execute the file:

   ./<filename>.sh

4. Run the below command to verify if the host name of the UDP Archiving server is modified:

   hostname

   The modified host name appears. You have successfully modified the host name of the UDP Archiving server.

How to Protect UDP Archiving using Agentless Backup

Using Agentless backup, you can protect UDP Archiving server. For details, view How to Create a Host-Based Virtual Machine Backup Plan in Arcserve UDP Solutions Guide.

Agentless or host-based backup does not need any agent on the computer that is being backed up. As a result, restarting an operating system is not required when setting up a agentless backup. We recommend to perform Agentless backup only if your local network bandwidth is more. If the bandwidth is just barely enough to meet your needs, then the additional network traffic from agent-less backups could impact local network performance.

How to Protect User Privacy Using UDP Archiving

Arcserve® UDP Archiving helps you protect user privacy. If some users from the organization opt not to share personal data, Compliance Offer can use UDP Archiving to purge the messages of those users.

Using the Search and Tag feature, compliance officer can add and remove messages to tag and then purge. Compliance officer can use one of the two options to tag and then purge.

1. Assign a Tag to Messages
2. Schedule Purge

Search Messages and Create a Tag

Protecting the user data requires assigning a tag to the search key terms that you use to find messages. This option is the first step for user security in UDP Archiving.

Using UDP Archiving, you can complete the step by using either of the following two steps:

- Search Messages and Create Tag to Assign
- Create a Tag and Assign to Search Results

If you want to modify the list of messages within a tag, you can perform either of the following options:

- Add Message to an Existing Tag
- Remove Message from an Existing Tag

Search Messages and Create Tag to Assign

Using this method, Compliance Officer can first search messages using a key term and then create a tag to assign to the messages from the search results.

Using a Search key term, Compliance officer can tag all the results.

Note: After attaching a tag to message, you can add more messages later to the same tag.

Follow these steps:

1. Log into UDP Archiving as a Compliance officer.

   The UDP Archiving Dashboard appears and you can view the Search box.

2. Using Search or Advanced Search option, enter a search key term.

   The matching results are displayed.

3. From the list of search results, select check boxes of messages from the search results that you want to tag.

   Note: If you do not select any message, then all the messages of search results are automatically tagged when you apply Tag.

4. Enter name of the tag in the Tag Name box and click the icon of **Tag**.

   The tag is created and assigned to all the selected messages of search results. To view tags, click Tags. To view details of a tag, click View/Edit button in front of a tag name.

With messages tagged, compliance officer can schedule a purge to remove all tagged messages from the system.

Create a Tag and Assign to Search Results

Using this method, Compliance Officer can first create a tag and then assign to the messages in the search results of a specific search key term.

Using a Search key term, Compliance officer can tag all the results. You can assign the same tag to different messages later.

Note: After attaching a tag to message, you can add more messages later to the same tag.

Follow these steps:

1. Log into UDP Archiving as a Compliance office.

   The UDP Archiving Dashboard appears and you can view the Search box.

2. From the left pane, click **Tag**.

   The matching results are displayed.

3. From Tags page, click **Add a Tag**.

4. From Add a Tag page, enter a name for tag and click **Add**.

   The Tags page displays all the added tags.

5. Using Search or Advanced Search option, enter a search key term.

   The matching results are displayed.

6. From the list of search results, select check boxes of messages from the search results that you want to tag.

   Note: If you do not select any message, then all the messages of search results are automatically tagged when you apply Tag.

7. Enter name of the tag in the Tag box and click the icon of **Tag**.

   The tag that you created before is assigned to all the selected messages of search results. To view tags, click Tags. To view details of a tag, click View/Edit button in front of a tag name.

With messages tagged, compliance officer can schedule a purge to remove all tagged messages from the system.

Add Tag to Message

Auditors and compliance officer can tag messages either by selecting specific messages and then creating a tag or by adding a tag first directly using the Tag tab and then assigning specific messages to the existing tab.

Note: After attaching a tag to search results, you can add more messages later to the same tag. You can assign the same tag to different search terms.

Follow these steps:

1. Log into UDP Archiving as an Auditor / Compliance Officer / Employee.

   The UDP Archiving Dashboard appears and you can view the Search box.

2. To add a tag before performing a search, from the left pane click **Tags**.
   a. From the Tags page, click **Add a Tag**.
   b. From Add a Tag page, enter a name in the field of **Tag Name**.
   c. Click **Add**.
3. To create and assign a tag to messages in the search result, perform the following steps:
   a. From the Search/Advanced Search page, perform a search.
   b. From the matching results, select messages that you want to tag.
   c. Enter a name for the tag in the **Tag Name** field to create a new tag and click the Tag icon  .

      The messages are assigned to the new tag.

      Now, you can use the search feature to find messages and assign the created tag. From the Tags page, you View/Edit/Remove the existing tag.

View/Edit or Remove a Tag

Auditors / Compliance Officer / Employee can remove either a tag with all the messages attached to it or remove some mesages from a tag.

Follow these steps:

1. Log into UDP Archiving as an Auditor or Compliance Officer.

   The UDP Archiving Dashboard appears.

2. From the left pane, click **Tag**.

   List of tags attached before appears. Every tag name has **View/Edit** and **Remove** options.

3. To remove a tag, click **Remove** against the name of desired tag and confirm.

   When you remove a tag, all the associated messages become untagged unless some messages are also associated with some other existing tag.

4. To Edit a tag or to remove some messages from an existing tag, perform the following steps:

   a. From the Tags page, click **View/Edit** against the name of the desired tag.

      The View/Edit Tag page appears with all the messages attached with the tag.

   b. From the list of messages, select check box of only those messages that you want to remove from the tag.

   c. Click **Untag Selected Messages**.

   d. Click **Yes** in the *Confirm* dialog.

      Selected messages are removed from the list of messages associated with that tag.

Schedule Purge

Using this method, Compliance Officer can first create a tag and then assign to messages.

Note: After attaching a tag to message, you can add more messages later to the same tag.

Follow these steps:

1. Log into UDP Archiving as a Compliance office.

   The UDP Archiving Dashboard appears and you can view the Search box.

2. From the left pane, click **Tags**.

   The matching results are displayed.

3. From the displayed results, click the **View/Edit** button for the Tag term that you want to purge.

   View/Edit tag page displays details of that tag and also displays Schedule Purge field.

4. Select the check box of Schedule Purge.

   Other field below Schedule Purge become editable.

5. Enter a duration in numbers for **Hold Period**.

   Hold Period defines the number of days after which Purge is completed. For example, when the value entered in Hold Period field is 30, then purge action for that tag is completed after 30 days from the date on which you schedule purge.

   Default Value of Hold Period: 3 (days)

6. Click **Save**.

   Purge is scheduled for all the messages of the tag.

   Note: You can reschedule the purge date. Rescheduling does not impact existing messages in the tag. Only those messages that you add to the tag after rescheduling are purged on the new date.

   Important! You cannot purge messages that are either put on Legal Hold or associated with other tags.. For details, view logs after purge.

Modify Scheduled Purge

After scheduling a purge for a tag with multiple messages, you may want to extend the purge date. UDP Archiving lets you modify the purge date of a tag. But, the modified date is applicable only to those messages that are added to that tag after rescheduling the purge date.

Follow these steps:

1. Log into UDP Archiving as a Compliance office.

   The UDP Archiving Dashboard appears and you can view the Search box.

2. From the left pane, click **Tag**.

   All the available tags are displayed.

3. From the Tags page, click **View/Edit** button for the tag name that you want to reschedule.

   The View/Edit page of that tag is displayed. You can view the number of messages and purge date scheduled.

4. From the **Hold Period** field, replace the existing duration with the revised duration.

5. Click **Save**.

   Important! All the messages added to that tag after rescheduling follow the rescheduled purge duration. Existing messages purge according to the previous hold period.

Auditor

The section contains the following topics:

How to Use Boolean Connector for Search

UDP Archiving supports Boolean connectors such as OR, AND, NOT.

For viewing steps in video, click How to Search in UDP Archiving.

Considerations

- For Auditors, the **Search** feature does not support the following characters:

  ':', ';', '<', '=', '>', '?', '@', ', '', '#', '%', '&', '(', ')', '*', '+', '/', '[', '\\', ']', '^', '_', '{', '|', '}', '~'

  Only when included with the following options, you can perform a search using the special characters mentioned above:

  - Include double quotes on the search term. For example, to use the special character **/**, apply double quotes (“25/09/2017”) on the search term.
  - Separate using space instead of using the special character. For example, enter the term HOME_LAND as HOME LAND.
- When using as the search term, search Half-width Kana characters as Full-width Kana characters.

Examples of Boolean Connectors supported for search

Important! You must enclose the search string with double quotes ("").

- cat dog = having cat and dog (order is not important)

  Note: Double-byte space is recognized as a search character, not as a search connector.
- cat OR dog = having cat or dog in different emails
- cat or dog = having cat and dog in the same email
- "cat dog" = having the expression "cat dog"
- !dog = not having dog
- -dog = not having dog
- "cat dog"~10 = proximity search – cat within 10 words of dog
- cat << dog = before operator: cat has to precede dog
- encryp* is a wild card search and will find emails such as “encrypt”, “encrypted” or “encryption”, and so on. By default, you need 5 characters and then *.

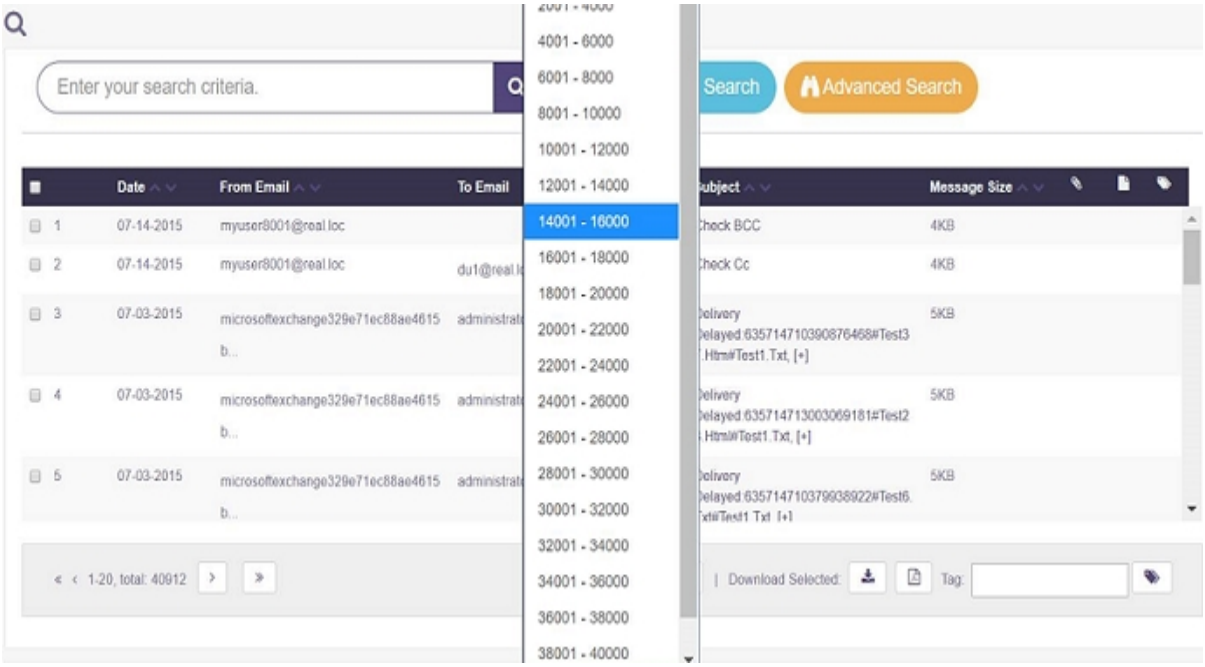
Note: In Japanese/Chinese, only one word with wild card * can perform a search. Do not use 6 characters.

How to View Email Message

Important! Only import or migration of emails does not make the user licensed. Only licensed user can view the emails. To view the emails in Auditor/Employee user roles, the user (Auditor/Employee) must send at least one email.

You can view the message either on the dashboard or in a separate screen. To view on the dashboard, click the subject of message once. To view the message in a separate screen, click the subject of message twice.

Using other options in the open message, you can view headers, and print.



You can perform the following functions on the message:

Download Messages

You can download a bulk message.

Note: Clicking **Download** display a drop down to select range of messages to download

Bulk Download

From the landing page, you can download more than one or all messages. To download multiple, select those messages and click **Download Selected**. To download all messages, select all the messages and click **Download**. The messages are downloaded in multiple zip files.

Tag Messages

From the main screen you can select a message and add a tag. The tag icon appears in front of that message in 15 minutes. To view the description, hover over a tag. To view list of tags assigned, from left pane click **references**. To manage messages having similar tag, from the **Advanced Search** section select desired Tag from the Tags drop-down option and click **Search**.

Apply Notes

From the main screen you can select a message and add a note. The Notes icon appears in front of that message in 15 minutes. To view the description, hover over a Note icon. To view list of Notes assigned, from left pane click **references**. To manage messages having similar tag, from the **Advanced Search** section select desired Notes from the Notes drop-down option and click **Search**.

PDF

From the main screen you can select any message and download as a PDF file.

Print

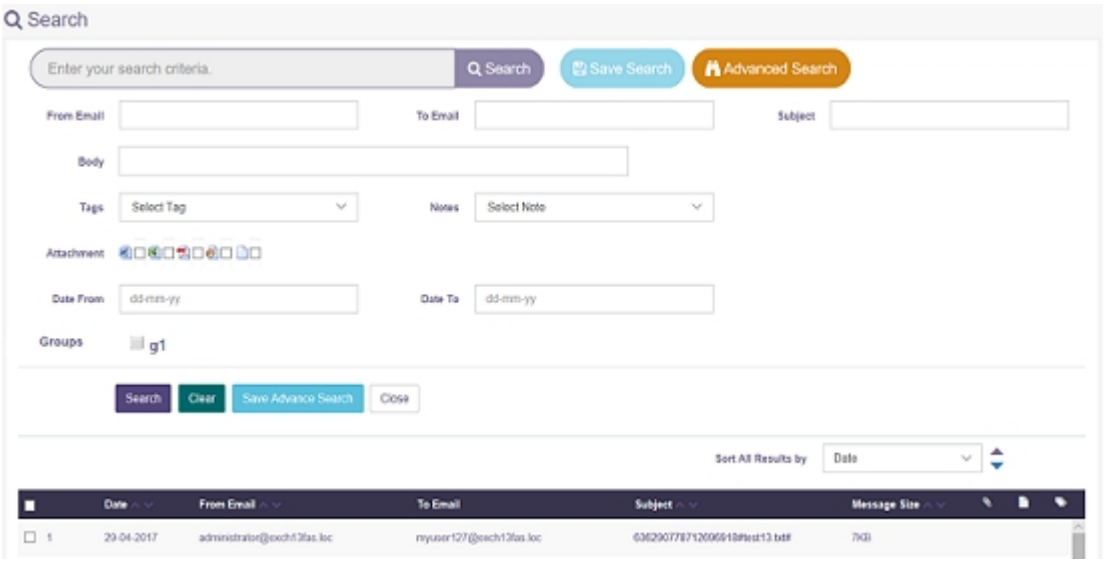
You can click a message to open and then click **Print** option.

Employees

The section contains the following topics:

How to Access a Group

If access to a group is provided, an employee can switch to the group access in the Advanced Search section. For example, the screenshot below displays an option for the Marketing Group. Selecting this group lets you view all messages of the group.

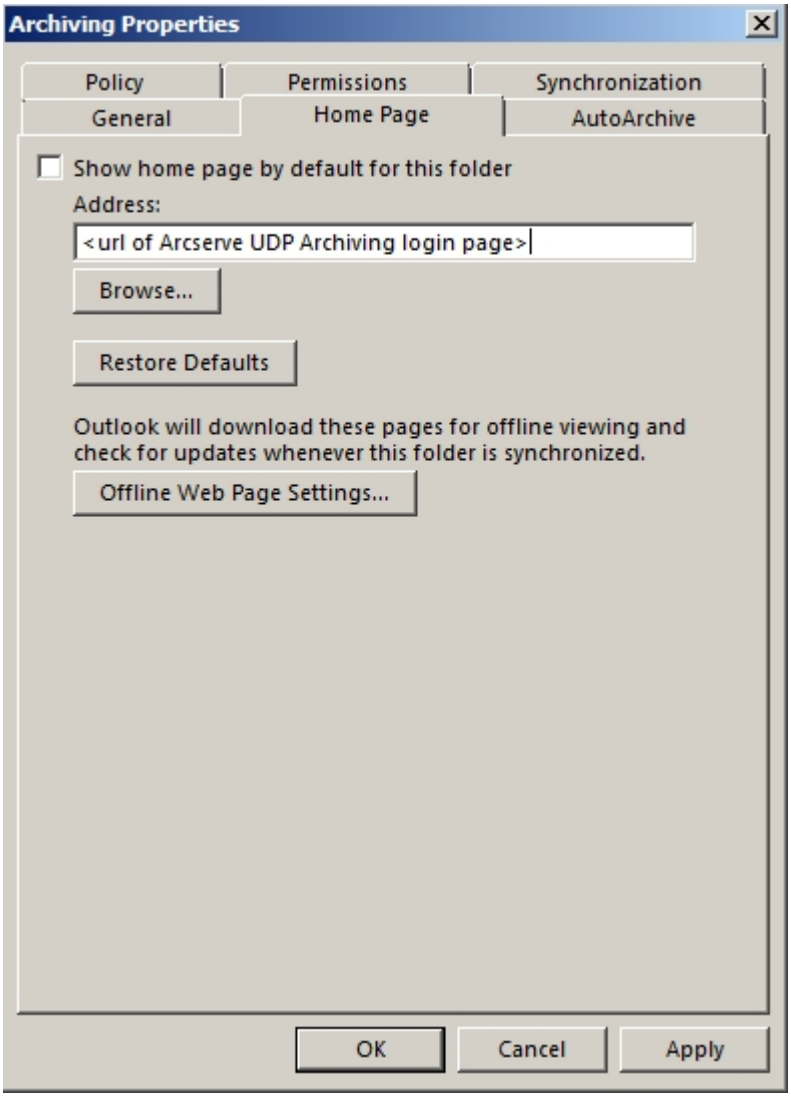


How to Access UDP Archiving Using Outlook

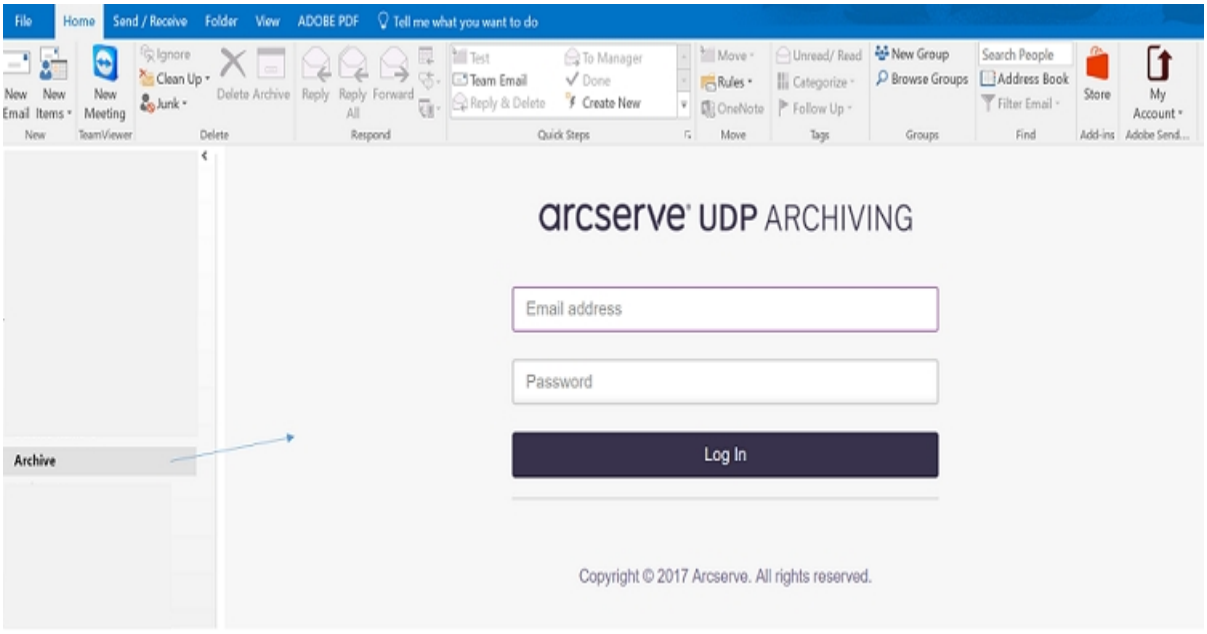
The employees can access UDP Archiving directly through an Outlook folder.

Follow these steps:

1. In your Outlook, add a new folder.
2. Right click on the folder, and click **Properties**.
3. From the Properties option, click the **Home Page** tab.
4. In the Home Page tab, provide the domain name of the UDP Archiving login page.
5. Click **Apply**.

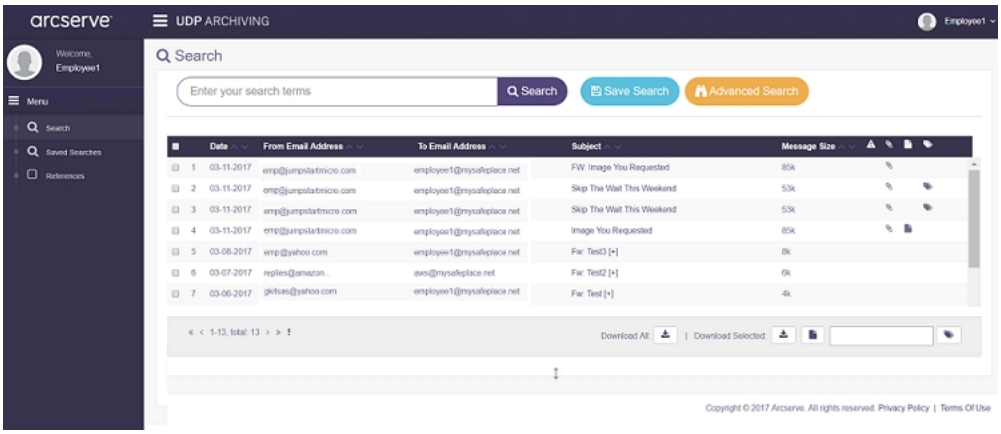


After applying the settings, accessing the folder directly logs you into UDP Archiving.

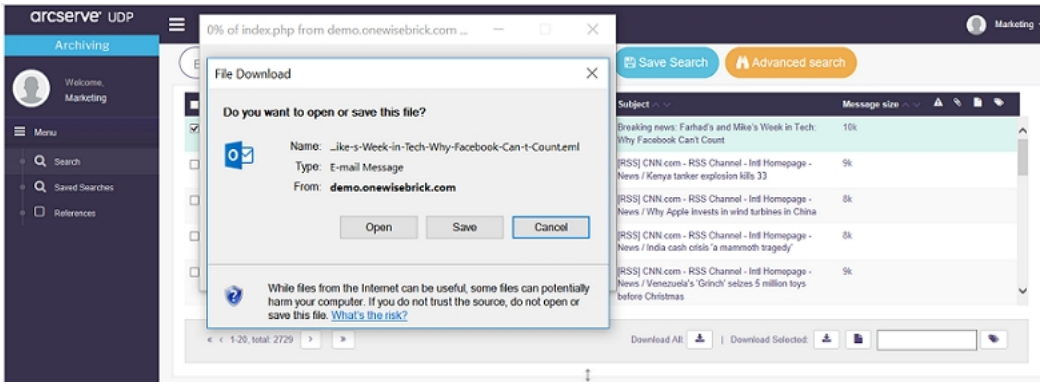


You can perform the following action:

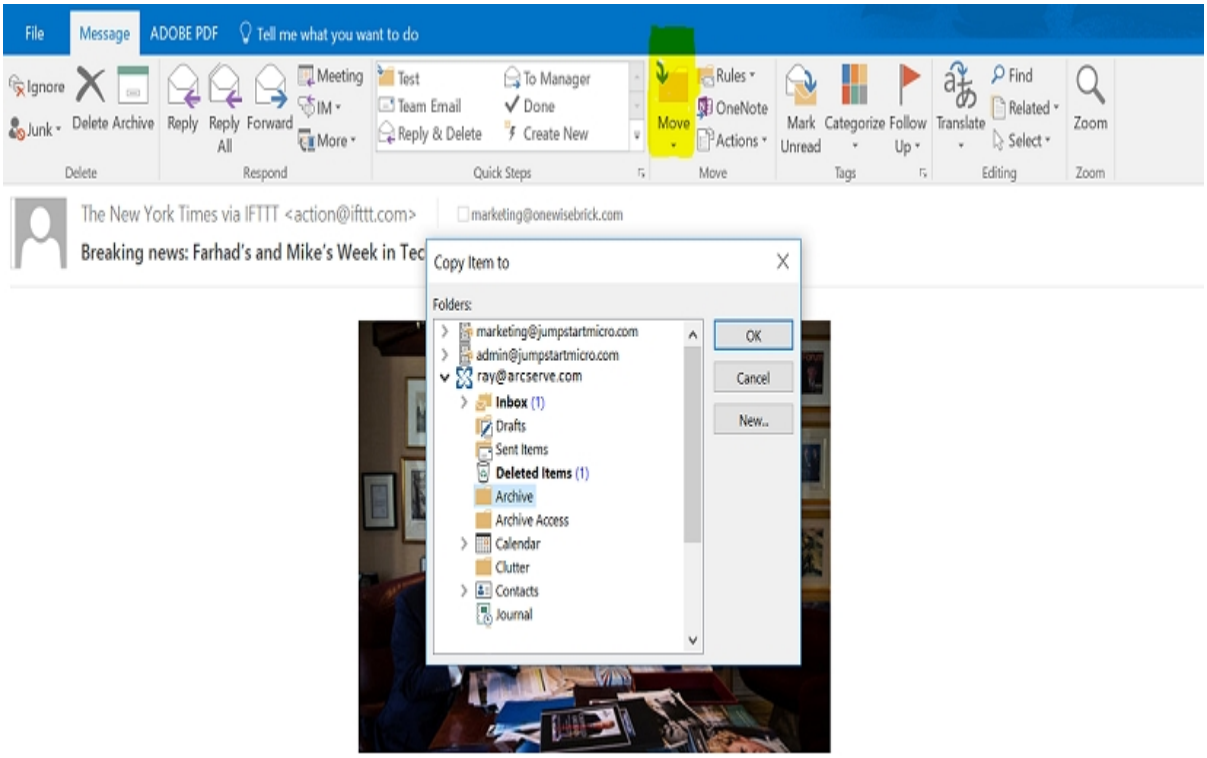
- View all the messages.



- Select download to open the message and view.



- Perform any general Outlook action including forward, reply, save and move. You can move the message into any Outlook folder for future access as shown below.

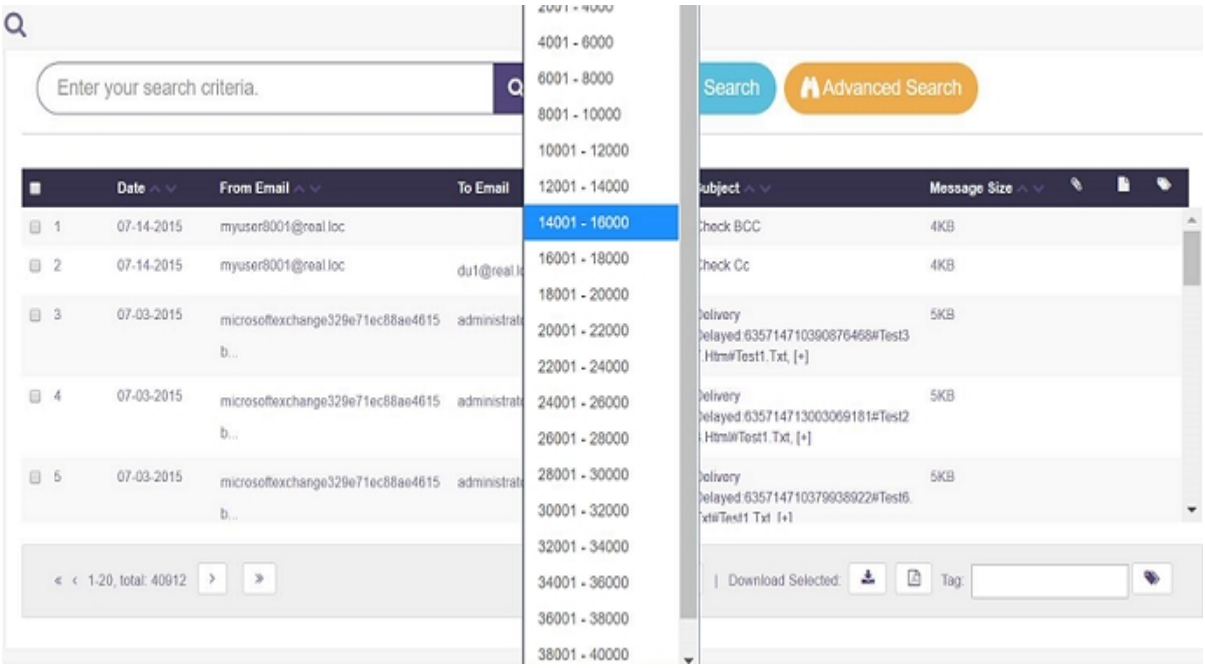


How to View Email Message

Important! Only import or migration of emails does not make the user licensed. Only licensed user can view the emails. To view the emails in Auditor/Employee user roles, the user (Auditor/Employee) must send at least one email.

You can view the message either on the dashboard or in a separate screen. To view on the dashboard, click the subject of message once. To view the message in a separate screen, click the subject of message twice.

Using other options in the open message, you can view headers, and print.



You can perform the following functions on the message:

Download Messages

You can download a bulk message.

Note: Clicking **Download** display a drop down to select range of messages to download

Bulk Download

From the landing page, you can download more than one or all messages. To download multiple, select those messages and click **Download Selected**. To download all messages, select all the messages and click **Download**. The messages are downloaded in multiple zip files.

Tag Messages

From the main screen you can select a message and add a tag. The tag icon appears in front of that message in 15 minutes. To view the description, hover over a tag. To view list of tags assigned, from left pane click **references**. To manage messages having similar tag, from the **Advanced Search** section select desired Tag from the Tags drop-down option and click **Search**.

Apply Notes

From the main screen you can select a message and add a note. The Notes icon appears in front of that message in 15 minutes. To view the description, hover over a Note icon. To view list of Notes assigned, from left pane click **references**. To manage messages having similar tag, from the **Advanced Search** section select desired Notes from the Notes drop-down option and click **Search**.

PDF

From the main screen you can select any message and download as a PDF file.

Print

You can click a message to open and then click **Print** option.

Chapter 9: Troubleshooting

This section contains the following topics:

LDAP Related

Fails to Authenticate

For some scenarios, LDAP authentication fails during test connection.

Solution

To resolve such scenario, verify LDAP credentials with mail server LDAP credentials. LDAP credentials include LDAP Hostname or IP address, LDAP Base DN, and LDAP Bind DN parameters.

Login Related

Unable to log into UDP Archiving

Fail to log into UDP Archiving system.

Solution

Expiration of license / trial expires leads to the issue where login fails in the UDP Archiving system. Clicking **Refresh** fails to get count of License. To verify the status of license / trial, log into UDP Archiving as SuperAdmin, navigate to **Health** and verify related notifications.

Unable to log into UDP Archiving server from Web Interface

When the UDP Archiving machine disk space reaches 100%, irrespective of roles all the users are unable to log into the Archiving server using web interface.

Solution

Increase or empty the disk space to login again using the web interface of UDP Archiving. Follow the workarounds given below to increase the disk storage.

Workaround 1: Applicable to VMware Deployment only

Follow these steps:

1. Add a new disk to the UDP Archiving machine from the vSphere client / Web-client/ VCenter server.
2. Log into UDP Archiving Debian console specifying **udp_admin** credentials.
3. Navigate to *cd /home/udp_admin/*, create a file named as *scan* (command: vi scan), and paste below commands before saving that file (command: Press Escape and type :wq!)

   #!/bin/bash

   for HOST in $(cd /sys/class/scsi_host; ls -d host)*

   do

   echo $HOST

   sudo bash -c "echo '- - -' > /sys/class/scsi_host/$HOST/scan"

   done
4. Run the following command:

   sudo runuser -l udp_admin -c "bash /home/udp_admin/scan”

   Note: You can skip steps 3 and 4 if you reboot the machine after step 1.
5. Run the following commands:

   sudo runuser -l fas -c "bash /var/fas/www/utils/disk/lvmDisk"

   sudo runuser -l fas -c "bash /var/fas/www/utils/disk/incDiskAuto"

Now, you can log into the UDP Archiving server from web interface using all the user roles.

Workaround 2: Applicable to Hyper-V and AMI Deployments only

Follow these steps:

1. Add a new disk to the UDP Archiving machine.
2. Log into UDP Archiving Debian console specifying **udp_admin** credentials.
3. Run the following commands:

   sudo runuser -l fas -c "bash /var/fas/www/utils/disk/lvmDisk"

   sudo runuser -l fas -c "bash /var/fas/www/utils/disk/incDiskAuto"

Now, you can log into the UDP Archiving server from web interface using all the user roles.

Unable to log into Administrator or Other Accounts

Cannot log into UDP Archiving using administrator or other roles.

Solution

Verify if license is active and available. If in trial, verify if the trial duration is still running. If the license is active, clear browser cookies and try to log in again.

Important! Only import or migration of emails does not make a user licensed. Only licensed user can view the emails. To view the emails in Employee user role, the Employee must send at least one email.

Migration and Import Related

Note: While importing emails using EWSImport, the following message displays, "Retrying messages on terminal. This is because, O365 or Exchange tries to control network traffic between Application and itself/O365/Exchange."

Unable to Import Emails

When using import, emails are not getting imported.

Solution

Multiple reasons can lead to such an issue. Verify the list below to find out the exact reason and resolve.

- When the import functionality fails to import mails from mail server, verify the provided import credentials and connection.
- Before saving Import user credentials, always select the **test connection** option in the **Import** page. If Test connection fails with an error, then Archiving instance is not able to communicate with mail server credentials provided in the Import page.
- Verify if required ports are enabled on the mail server so that Archiving can communicate successfully.
- Verify if the mail server is running firewall environment. Then, allow access to required ports for the archiving system to access.
- Verify if the relevant import protocols (POP3, IMAP, POP3S, IMAP3S) are enabled on the mail server.
- Verify if the mailbox is having mails to import.
- When using Sendmail / Postfix, verify if the mail directory path is available in the configuration file of your mail server.
- Verify the syslog for any additional information.

  Note: Syslog is available in the support logs downloaded from the Super Admin account

Test connection Fails

Test connection fails and an error message appears.

Solution

Multiple reasons can lead to such an issue. Verify the list below to find out the exact reason and resolve.

- Verify if the import protocols (POP3, IMAP, POP3S, IMAPS) are enabled on the mail server.
- Verify if required ports are enabled on the mail server for UDP Archiving to communicate successfully.
- If mail server is running firewall, then allow access to required ports to let UDP Archiving access.
- Review the syslogs present in the Super Admin account's support logs.

Unable to Import Emails Despite Running State

The import job is in running state for a long time, but emails are not imported.

Solution

Multiple reasons can lead to such an issue. Verify the list below to find out the exact reason and resolve.

- Verify if the mailbox that is being imported has emails in Inbox.
- For Sendmail / Postfix mail servers, verify if the mailbox directory path is available in the configuration file of your mail server.

Migration Status is not Visible

In the Migration page, the status of migration is not displayed.

Solution

The issue occurs when the UDP Archiving migration service is not running. Before starting migration of emails, verify if the migration service is running. To start the service and verify for migration status in the Migration page of UDP Archiving, add command to start the service.

Test Connection Fails for Sendmail / Postfix

On the Import page, the Test Connection fails.

Solution

If the user credentials are correct then as a workaround provide user name without domain. For example: If user1@domain.com is not working, try user1 in the user-name field.

Unable to Perform Search using Mail Content

No results are displayed when the mail content is used in the Search field after importing from Microsoft Exchange Server.

Solution

After importing the mail box from Microsoft Exchange Server, you must configure the Message MIME Format in Exchange Admin Center.

Follow these steps:

1. Launch **Microsoft Exchange Admin Center** and navigate to **Servers**.
2. From the Servers screen, select the **Client Access server** and click **Edit**.
3. On the Server Properties screen, click **POP3/IMAP**.
4. Under **Message MIME Format**, select one of the following options:
    - HTML
    - HTML and alternative text
5. Click **Save**.
6. Restart the following services on the server where UDP Archiving is installed:
    - Microsoft Exchange POP3
    - Microsoft Exchange POP3 Backend
    - Microsoft Exchange IMAP4
    - Microsoft Exchange IMAP4 Backend

Miscellaneous

This section contains the following topics:

Status of UDP Archiving displays Error

In the SuperAdmin Health page, the UDP Archiving Status displays status as Error.

Solution

Such a status indicates that UDP Archiving FAS service is not running. To archive emails properly, UDP Archiving FAS service needs to run always as daemon. Verify if the rc.fas service is running. To start the rc.fas service add command to start the service.

UDP Archiving Does Not Receive Mails from Email Server

Symptom:

UDP Archiving does not receive mails from Email server even after journaling is configured.

Solution:

Verify and ensure that the host name / IP Address specified in Email server is same as the current Archiving server IP address.

Note: When you modify the Archiving server IP address you must update Email server with the modified IP address. If you do not update the IP / host name of archiving server in Email server, the mails are not journaled. We recommend to use a static IP / hostname for UDP Archiving server.

Plug-in Related

Warning Appears After Installing Outlook Plug-in

After installing Outlook plug-in, MS Outlook displays an error message about Outlook slowing down.

Solution

In rare instances, this issue may appear. To resolve, uninstall the plug-in and install again.

Storage Related

UDP Archiving Machine Storage running out of Space

When the UDP Archiving machine storage reaches > 90% threshold, UDP Archiving services stop automatically.

Solution

The UDP Archiving services stop when the storage space consumed is less than 90% and start only when the storage disk is increased. To resolve, perform the following steps:

1. Add a new disk to VMware ESX or Hyper-V data store machine.
2. Restart the UDP Archiving machine to recognize the newly added disk.
3. Log into UDP Archiving Console as SuperAdmin and navigate to **Configuration**.
4. Click the **Increase disk** option.
5. Restart the UDP Archiving FAS services.

Updates Related

Unable to Update UDP Archiving

Unable to get latest updates as the option **Check for Updates** in UDP Archiving fails.

Solution

To resolve, perform the following steps:

1. Verify if the UDP Archiving instance is connected to Internet and not behind the firewall with port blocked.
2. If Archiving instance is not connected to Internet, install Update manually by downloading the .deb package from Arcserve UDP Archiving **Check for Updates** page.

Chapter 10: Frequently Asked Questions

This section contains the following topics:

Can I archive calendar, tasks, and contacts?

UDP Archiving lets you archive emails from Inbox and Sent folders. Calendar and tasks are archived only when included in Inbox and Sent folders. Contacts are not archived.

Can I view my archived emails from Web browser?

UDP Archiving lets you access archived emails using web console. Use your credentials to log into the UDP Archiving console to access archived emails. Outlook plug-in integration lets you open web console directly from Outlook.

Can Windows user credentials help search/recover emails?

Yes, UDP Archiving lets users search / recover their emails using Windows credentials.

What type of licenses are required to use UDP Archiving?

To use UDP Archiving, you need mailbox and capacity-based licenses.

How to Archive historic emails?

UDP Archiving helps archiving of historic emails using migration and import features. Using migration feature, UDP Admin can migrate. Using Import feature, administrator can migrate.

Can I increase the storage capacity anytime?

UDP Archiving lets you use the simple method of increasing storage by adding new disk using the Configuration tab in the UDP Archiving Console.

Which Backup Type Shall I Use?

Arcserve UDP allows three types of backup. Depending upon your preference you can use any or a mix of all three types.

Full Backup

Determines the backup schedule for Full Backups. As scheduled, Arcserve UDP performs a full backup of all used blocks from the source machine. A full backup typically consumes time depending on the backup size.

Verify Backup

Determines the backup schedule for Verify Backups.

Arcserve UDP verifies that the protected data is valid and complete by performing a confidence check of the stored backup image to the backup source. If necessary, the image is resynchronized. A Verify Backup looks at the most recent backup of each individual block and compares the content and information to the source. This comparison verifies that the latest backed up blocks represent the corresponding information at the source. If the backup image for any block does not match the source (possibly because of changes in the system since the last backup), Arcserve UDP refreshes (resynchronizes) the backup of the block that does not match. You can also use a Verify Backup (infrequently) to get the guarantee of full backup without using the space required for a full backup.

Advantages: Produces a small backup image when compared to full backup because only the changed blocks (blocks that do not match the last backup) are backed up.

Disadvantages: Backup time is long because all source blocks are compared with the blocks of the last backup.

Incremental Backup

Determines the backup schedule for Incremental Backups.

As scheduled, Arcserve UDP incrementally backs up only those blocks that have changed after the last successful backup. The advantages of Incremental Backups are that it is a fast backup and it produces a small backup image. This is the most optimal way to perform a backup.

APPENDIX: Understanding LDAP

This section contains the following topics:

Using LDAP in UDP Archiving

Using UDP Archiving LDAP (Lightweight Directory Access Protocol) option, users can log into the UDP Archiving Console using Active directory UPN (User Principal Name) credentials.

Administrator can restrict the authentication of users in a particular CN (Common Name) and/or OU (Organizational Units). UDP Archiving uses the Active Directory Administrator credentials to bind the Active Directory using LDAP protocol. Set the authentication using the following fields:

LDAP Base DN

Enter the CN's and OU's for search base.

LDAP Bind DN

Enter the Active Directory Administrator authentication details.

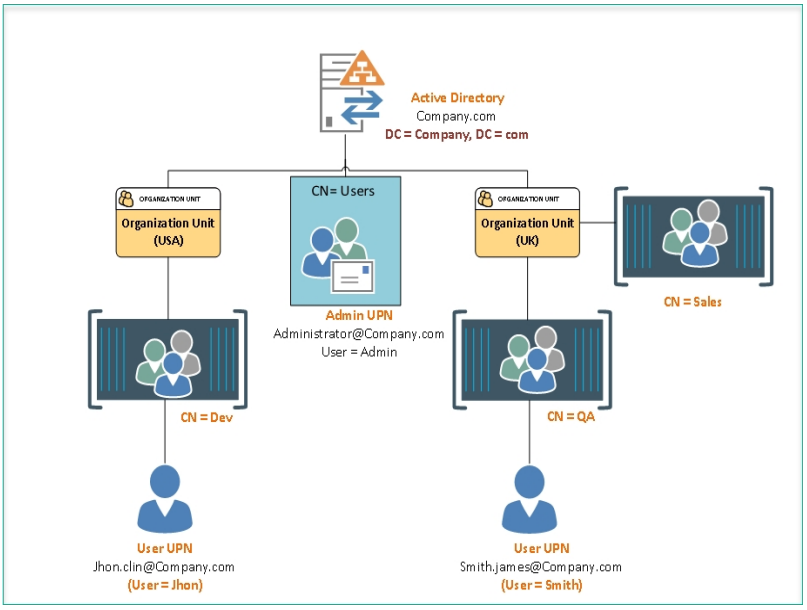
For more information, refer Manage LDAP.

Understanding Common Active Directory Scenarios

The following scenario explains the Common Active Directory functionality using multiple examples:

Scenario:

If Active Directory domain and UPN suffix domain are same.



In the above screenshot, consider Company.com as the Active directory server domain, different Organizational Units (USA and UK), and Containers (Dev, QA, and Sales) where a set of users (Jhon and Smith) are part of the containers.

Example 1:

To allow LDAP authentication for the users of USA Organizational Unit, the following configuration is applicable:

- **LDAP Base DN** *="OU=USA,DC=Company,DC=com"*
- **LDAP Bind DN** *="CN=Administrator,CN=Users,DC=Company,DC=Com"*

User details for the above configuration:

- user name: Jhon
- Organizational Unit: USA
- UPN Login credentials for the UDP Archiving Console: Jhon.clin@Company.com

Example 2:

To allow LDAP authentication for the users in the QA container available in the UK Organizational Unit, the following configuration is applicable:

- **LDAP Base DN**= " *CN=QA,OU=UK,DC=Company,DC=Com* "
- **LDAP Bind DN**= " *CN=Administrator,CN=Users,DC=Company,DC=Com*"

Example 3:

To allow LDAP authentication for the users available in specific containers (Dev, QA) present in multipleOrganizational Units ,the following configuration is applicable:

- **LDAP Base DN** = *"CN=Dev,OU=USA,DC=Company,DC=com;CN=QA,OU=UK,DC=Company,DC=com"*
- **LDAP Bind DN** = " *CN=Administrator,CN=Users,DC=Company,DC=Com*"

Using above configuration, the users in both organizational units can log into the UDP Archiving Console using their UPN credentials.

Note: Users of Sales container present in UK Organizational Unit cannot login using the above configuration.

Configuring LDAP for Different Scenarios

The following table provides an overview of the scenarios to configure LDAP:

	Domains		Employees/Users	
	Active Directory Domain	**Email Domain**	**Users in Main Folder**	**Users in Alternate or Multiple Folders**
Scenario 1	Same Domain		Available	NA
Scenario 2	Same Domain		NA	Available
Scenario 3	Different from Email Domain (UPN Suffix)	Different from AD Domain	Available	NA
Scenario 4	Different from Email Domain (UPN Suffix)	Different from AD Domain	NA	Available
Aliases	Managing Aliases			

Scenario 1

To allow LDAP authentication where Active Directory and UPN Suffix have same domain and employees are available in the single container, the following configuration is applicable:

- **LDAP Base DN:** *CN=Users,DC=domain,DC=com*
- **LDAP Bind DN:** *CN=Administrator,CN=Users,DC=Domain,DC=com*

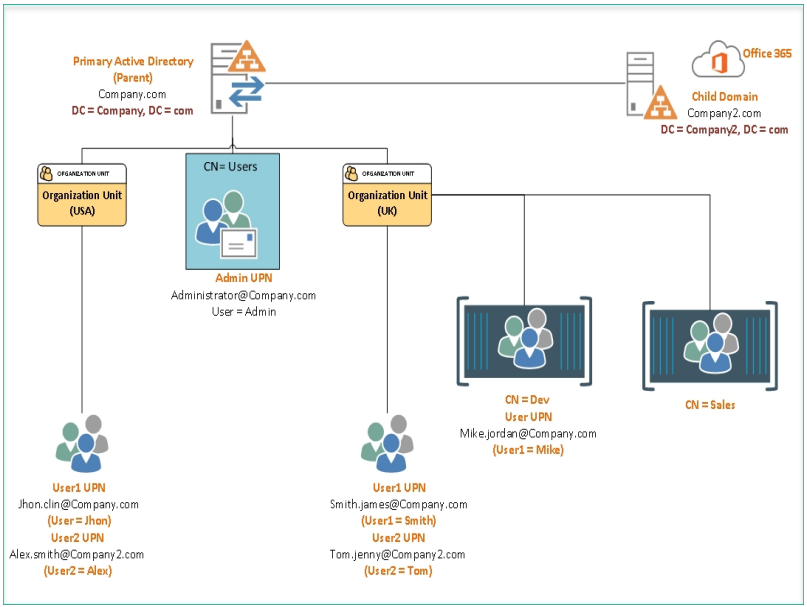
Scenario 2

To allow LDAP authentication where Active Directory and UPN Suffix have same domain and employees are in different or multiple Organization Units, the following configuration is applicable:

- **LDAP Base DN:**
  - For Single OU: *CN=users, OU=OUname,DC=domain,DC=COM*
  - For Multiple OU's: *OU=OUname,DC=domain,DC=COM; OU=OUname1,DC=domain,DC=COM; OU=OUname2,DC=domain,DC=COM*
- **LDAP Bind DN:** *CN=Administrator,CN=Users,DC=Domain,DC=com*

Scenario 3

Active Directory domain and UPN Suffix domain are different



In the above screenshot, *Company.com* is the Primary Active directory server domain and has a relationship with another domain name *Company2.com* (for example, Office 365/Child Domain). There are different Organizational Units (OU) and Containers (CN) having users.

Example 1:

To allow LDAP authentication for the users in USA Organizational Unit, the following configuration is applicable:

LDAP Base DN= *"OU=USA,DC=Company,DC=com"*

Using the above configuration, User1 and User2 of USA Organizational Unit can log into UDP Archiving Console using UPN names.

Example 2:

To allow LDAP authentication for the users in USA and UK Organizational Units, the following configuration is applicable:

LDAP Base DN = *"OU=USA,DC=Company,DC=com;OU=UK,DC=Company,DC=com"*

Using the above configuration, users of both: USA and UK Organizational Units can log into UDP Archiving Console using UPN names.

Scenario 4

When Active Directory and UPN Suffix domains are different, and employees are in single or multiple Containers/Organizational Units

In the above screenshot, *Test1.com* refers to the AD (Active Directory) domain configured for LDAP authentication and *Test2.com* refers to the UPN Suffix domain where the users can get access for UDP Archiving Console. In this case, two LDAP server configurations will have the similar Base DN/Bind DN and LDAP Host. After configuration, the Active Directory users having UPN suffix as *Test2.com* can log into UDP Archiving Console using the UPN credentials.

LDAP Configuration for Test1.com:

- **Domains:** AD domain
- **LDAP Base DN:** CN=Users,DC=domain,DC=com
- **LDAP Bind DN:** CN=Administrator,CN=Users,DC=Domain,DC=com

LDAP Configuration for Test2.com:

- **Domains:** UPN suffix domain of the User mail box
- **LDAP Base DN:** CN=Users,DC=domain,DC=com
- **LDAP Bind DN:** CN=Administrator,CN=Users,DC=Domain,DC=com

Note: The Active Directory domain and UPN Suffix domain should have the same Profile created in UDP Archiving.

For more information on multiple aliases, refer Adding Email Aliases to a Profile.