

# Deployment and Configuration Guide

*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.

© 2018 Arcserve, including its affiliates and subsidiaries. All rights reserved. Any third party trademarks or copyrights are the property of their respective owners.

## 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 product.

---

# Contents

---

<b>Chapter 1: Documentation Overview</b>	<b>1</b>
About This Document	2
Related Documentation	3
Language Support	4
<b>Chapter 2: Understanding UDP Archiving</b>	<b>5</b>
How Deployment and Configuration Works	6
Deployment Options	7
Configuration Options	8
Management Hierarchy	9
Single Company Deployment	10
Multiple Company or Multiple Organizational Unit Deployment	12
Best Practices for UDP Archiving	14
<b>Chapter 3: How to Deploy UDP Archiving</b>	<b>17</b>
Review Prerequisites	18
Deploy UDP Archiving in VMware	19
Deploy UDP Archiving in Hyper-V 2016 and Hyper-V 2012 R2	26
Modify DHCP to Static IP for Hyper-V/VMware/AMI after Deployment	31
Deploy UDP Archiving in Hyper-V 2008 R2	34
Deploy UDP Archiving in Microsoft Azure	39
Add UDP Archiving Virtual Hard Disk to Microsoft Azure	40
Create Virtual Machine and Deploy UDP Archiving	42
Enable UDP Archiving for Public Access	44
Deploy UDP Archiving in Amazon Web Services (AWS)	45
Finding Amazon Machine Image	49
Configure to Access UDP Archiving	50
<b>Chapter 4: How to Configure UDP Archiving</b>	<b>53</b>
Review Prerequisites and Considerations	54
Log into UDP Archiving	56
Configure Settings of UDP Archiving	57
Enter Domain for Mail Server	58
Add Profiles for Each Domain	60
Create Archiving Administrators for Each Domain	62
Set the Forwarding Mail Server	65
<b>Chapter 5: How to Configure Email Services</b>	<b>67</b>



---

Configuring Microsoft Office 365 .....	68
Create a Non-routable New Remote Domain .....	69
Create a Fake Mail Contact using New Domain .....	72
Creating Mail Contact .....	75
Create a Send Connector for the Remote Domain .....	78
Add a Journaling Rule to direct Messages .....	84
Setting up Access to UDP Archiving from Outlook Web Access .....	86
Configuring Microsoft Exchange 2007 .....	87
Creating New Remote Domain .....	88
Creating Mail Contact .....	90
Creating Send Connector .....	93
Setting up the Journal Rule .....	98
Configuring Microsoft Exchange 2010 .....	100
(Optional) Create new Distribution Group to Archive Selective Users .....	101
Create a Non-routable New Remote Domain .....	105
Create a Mail Contact using New Domain .....	107
Create a Non-deliverable Mailbox .....	110
Create Send Connector .....	112
Create the Journaling rule .....	118
Configuring Microsoft Exchange 2013 and 2016 .....	122
(Optional) Create new Distribution Group (Using EAC) .....	123
Create a Non-routable New Remote Domain .....	124
Create a Fake Mail Contact using New Remote Domain .....	125
Create a Non-deliverable Mailbox .....	127
Create a Send Connector for the Remote Domain .....	129
Add a Journaling Rule to direct Messages .....	134
Configuring G Suite Email .....	136
Configuring IBM Lotus Domino .....	141
Configure UDP Archiving for Lotus Domino .....	142
Set up Email Services of Lotus Domino .....	143
Configuring Zimbra .....	157
Configuring Sendmail .....	158
Configuring Postfix .....	160
Configuring Kerio .....	162
<b>Chapter 6: Frequently Asked Questions .....</b>	<b>163</b>
How to Modify the Host name? .....	164

---

---

How to Archive historic emails? .....	165
Can I increase the storage capacity anytime? .....	166
Can I view my archived emails from Web browser? .....	167
What type of licenses are required to use UDP Archiving? .....	168
Can Windows user credentials help search/recover emails? .....	169
Can I archive calendar, tasks, and contacts? .....	170

---

# Chapter 1: Documentation Overview

This section provides an overview about this guide and 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:

---

<a href="#">About This Document</a> .....	2
<a href="#">Related Documentation</a> .....	3
<a href="#">Language Support</a> .....	4

## About This Document

Deployment and Configuration guide assists to complete deployment in multiple environments and configuration of desired email services. The guide provides details about setup and configuration for both On-premise and cloud deployments.

### Key sections of this document:

- *Chapter 2* outlines the management hierarchy, flow of deployment and configuration and the options available to complete set up.
- *Chapter 3* describes how to complete the first step of setting up UDP Archiving by providing detailed steps of deployment in multiple environments.
- *Chapter 4* describes how to configure the UDP Archiving Console for your company.
- *Chapter 5* describes how to configure your required email services.
- *Chapter 6* provides answers through Frequently Asked Questions (FAQs).

## Related Documentation

- 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® Unified Data Protection 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. Simple configurations after deployment lets you archive mails using UDP Archiving.

This section contains the following topics:

---

<a href="#">How Deployment and Configuration Works</a>	6
<a href="#">Deployment Options</a>	7
<a href="#">Configuration Options</a>	8
<a href="#">Management Hierarchy</a>	9
<a href="#">Best Practices for UDP Archiving</a>	14

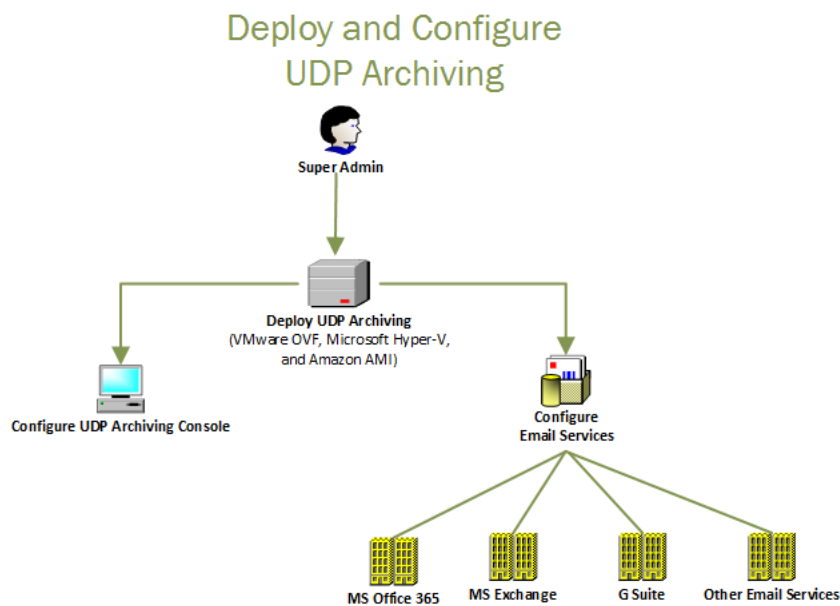
## How Deployment and Configuration Works

Getting started with archiving emails using UDP Archiving is possible in just three short steps:

- **Deployment of UDP Archiving:** As UDP Archiving supports deployment on multiple environments, select the most suitable options to start deployment. For more information, see [Deployment Options](#).
- **Configuration of UDP Archiving:** After deployment, access the UDP Archiving Console to configure for your organization. For details, view [How to Configure UDP Archiving](#).
- **Configuration of Email Service(s):** After deployment, configure desired email service(s) to sync up with UDP Archiving. For the list of supported Email services, view [How to Configure Email Services](#).

**Note:** After deployment, you can start with the two configurations in any sequence.

The flow diagram below explains the deployment and configuration process.





## Deployment Options

UDP Archiving is installed as a Virtual Machine quickly and easily using the following deployment options:

- **VMware OVF:** Designed for deployment in any vSphere environment either on-premise or in any cloud environment that uses vSphere such as VMware vCloud Air, Rackspace and a high percentage of public cloud providers.
- **Microsoft Hyper-V:** Designed for deployment in any Hyper-V environment either on-premise or in any cloud environment that uses Hyper-V such as the Microsoft Azure Cloud and other leading cloud providers.
- **Amazon AMI:** Designed for the EC2 instance in your Amazon Web Services (AWS) account.

## Configuration Options

After deployment, UDP Archiving requires the following two different configurations to start the archiving process:

**Important!** The two types of configuration do not require any specific sequence. After deployment, you can start with either of the following two configurations:

- **Configure UDP Archiving:** In this process, super admin configures the UDP Archiving Console, setting up mandatory information and also creates administrator.
- **Configure Email Services:** In this process, super admin configures email services. UDP Archiving supports multiple email services. For example: Microsoft Exchange, G Suite email, and IBM Lotus Domino.

## 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. When used as a single tenant solution, the Super Admin defines one customer and the first Admin for that organization. In a multi-tenant environment, the Super Admin defines multiple customers and the first admin for each organization or organizational group of an Enterprise.

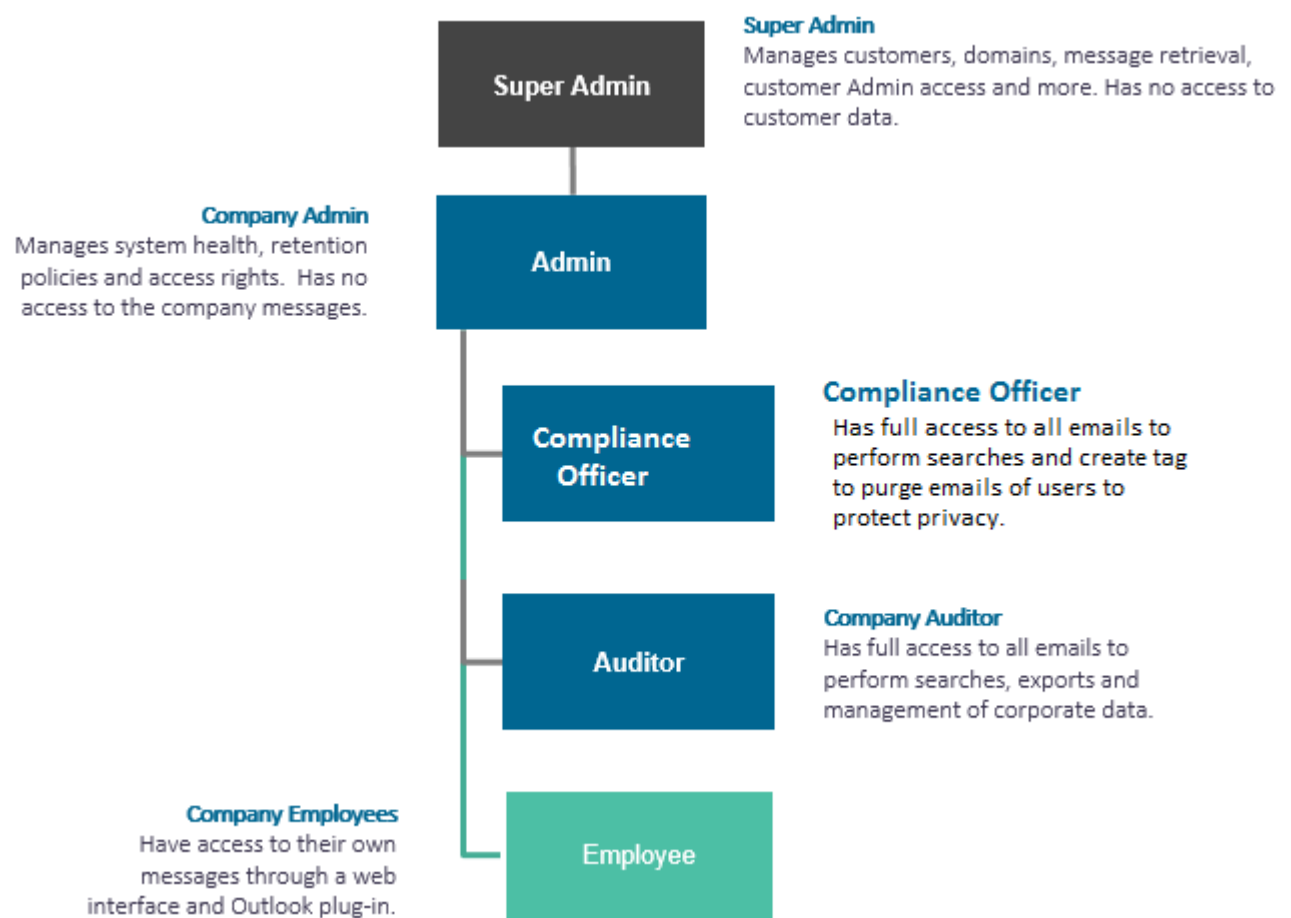
This section contains the following topics:

- [Single Company Deployment](#)
- [Multiple company or Multiple Organizational Unit Deployment](#)

## 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.



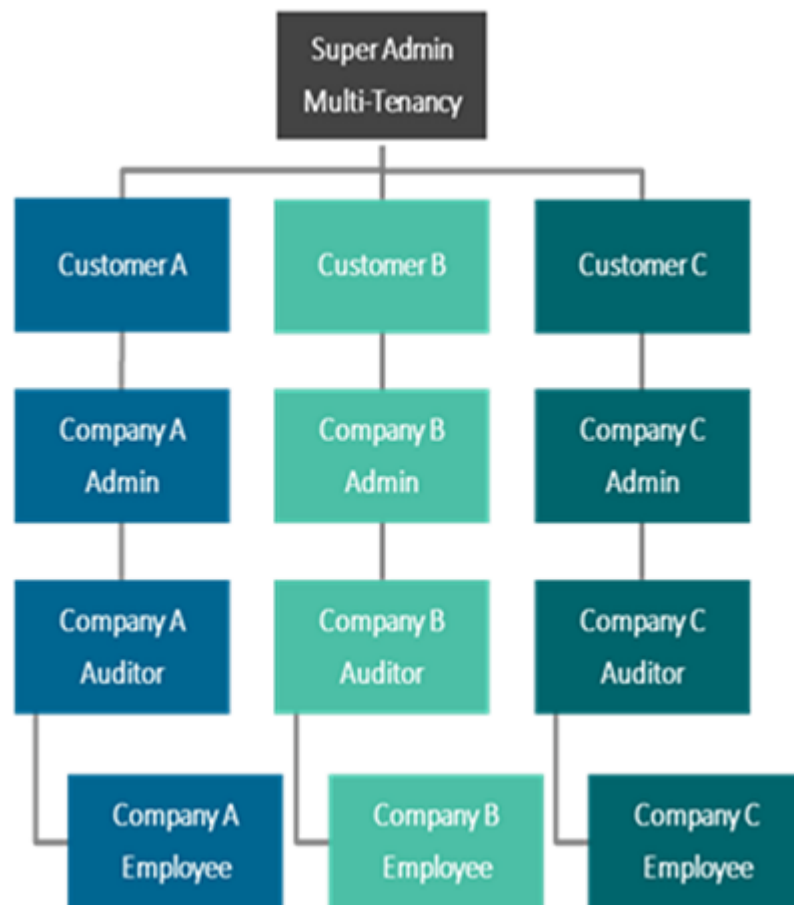
### Roles Assigned:

- **Super admin:** In UDP Archiving, this role assists to manage domains, create and manage administrators who would interact with the system, and more. This role does not have access to the end user data and is more useful in management.

- **Administrator:** In UDP Archiving, this role handles reporting and monitoring, setting up retention policies, providing access rights, 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 everyone 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:** In UDP Archiving, this role assists to manage domains, create and manage administrators who would interact with the system, and more. This role does not have access to the end user data and is more useful in management.

- **Administrator:** In UDP Archiving, this role handles reporting and monitoring, setting up retention policies, providing access rights, 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 everyone 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.

## 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.
- **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.
- **Hassle-free Import:** Use POP3S, IMAP3S protocols for importing mails from Google professional mail boxes for hassle free operations
- **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 smoother 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.



---

## Chapter 3: How to Deploy UDP Archiving

Deploy UDP Archiving in your environment from the list of multiple supported options and then complete the basic configuration to access the Console. The two-step process completes deployment in less than an hour.

This section contains the following topics:

---

<a href="#">Review Prerequisites</a>	18
<a href="#">Deploy UDP Archiving in VMware</a>	19
<a href="#">Deploy UDP Archiving in Hyper-V 2016 and Hyper-V 2012 R2</a>	26
<a href="#">Deploy UDP Archiving in Hyper-V 2008 R2</a>	34
<a href="#">Deploy UDP Archiving in Microsoft Azure</a>	39
<a href="#">Deploy UDP Archiving in Amazon Web Services (AWS)</a>	45
<a href="#">Configure to Access UDP Archiving</a>	50

## Review Prerequisites

- Verify if UDP Archiving is downloaded.
  - Verify if you have following minimum system requirements:
    - ◆ 8 GB of RAM
    - ◆ 2 CPUs
    - ◆ 20 GB of storage for Microsoft Azure and 16 GB of storage for others
- Note:** You can add a new disk to increase volume.
- Verify if you have supported versions available for required deployment:
    - ◆ ESX/VMware Versions: 5.5 and above
    - ◆ Hyper-V versions: 2016 / 2012 R2 and 2008 R2

Select your deployment option and follow the related steps:

**Important!** After deployment, take a backup of UDP Archiving to avoid loss of data later.

- [VMware OVF](#)
- [Amazon Web Services AMI](#)
- [Microsoft Hyper-V 2016 and 2012 R2](#)
- [Microsoft Hyper-V 2008 R2](#)
- [Microsoft Azure](#)
- [AWS](#)

## Deploy UDP Archiving in VMware

This topic describes how to deploy UDP Archiving on the ESX server using Web client with 8 GB of RAM, 2 CPUs, and 16 GB of storage. You can also deploy UDP Archiving at vCenter level or vSphere Web Client. After deployment, you can modify RAM and CPU depending upon your requirement. You cannot modify storage of the initial volume. However, adding a new disk to increase the storage space is possible.

For viewing steps in video, click [How to Deploy UDP Archiving in VMware](#).

### Important!

Do not modify the initial volume. Modifying the initial volume using web vSphere client makes the volume inconsistent.

UDP Archiving supports only VMware versions 5.5 and above.

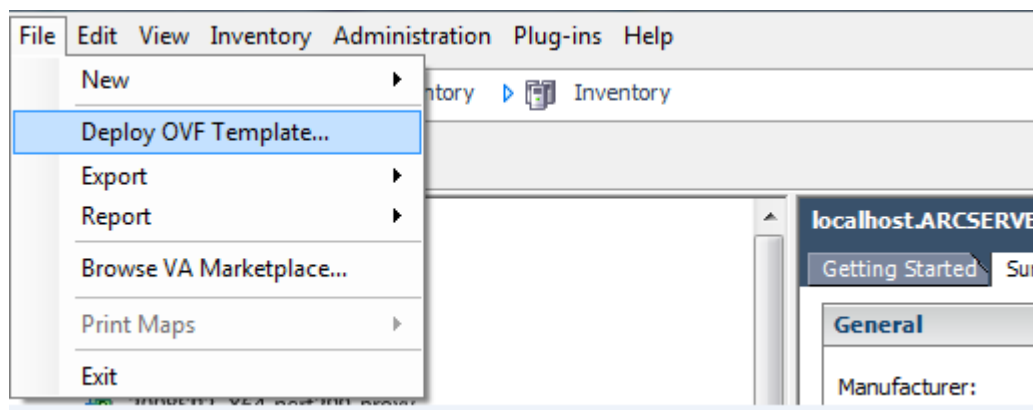
### Follow these steps to set up and configure UDP Archiving:

1. Download the UDP Archiving software (VMware OVF) to deploy in a VMware.

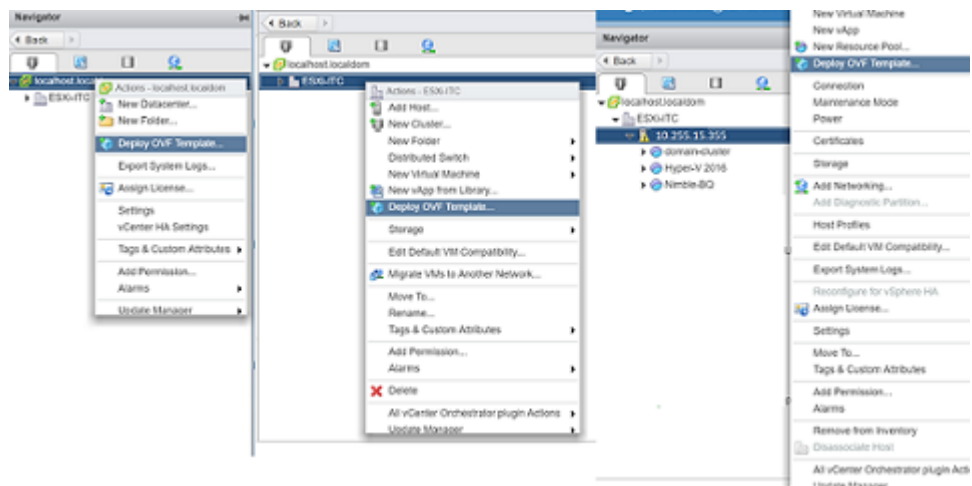
The operating system is Linux Debian 8.0 and the software runs in any VMware environment.

2. Set up and deploy the UDP Archiving VM using the following steps:

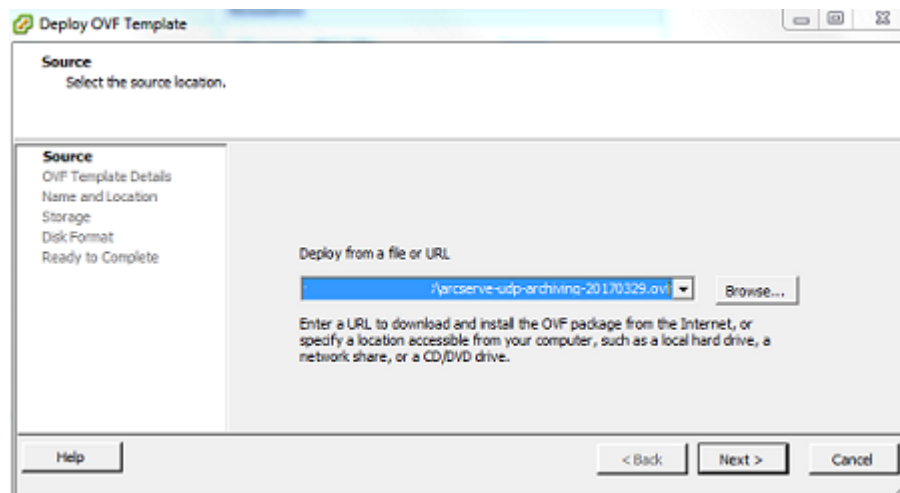
- a. Open the VM client and connect to your ESX host.
- b. From the VM client, Click File> **Deploy OVF Template**.



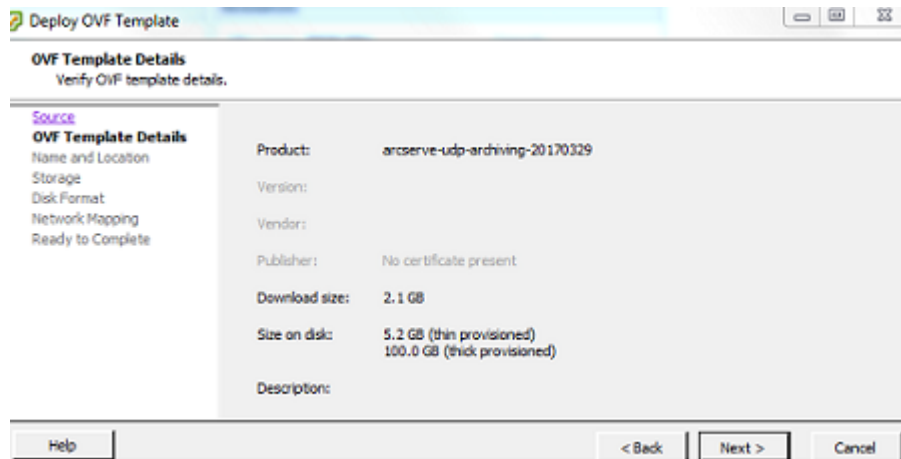
**Note:** You can import OVF files into vSphere through the vSphere Web client at the vCenter, Host, or Cluster Level.



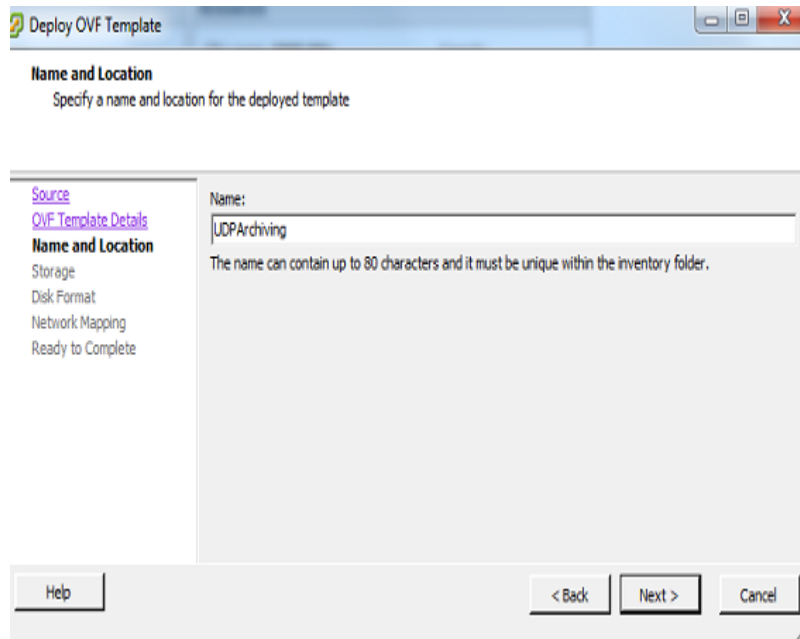
- c. From the **Source** tab, browse to the location where the .ovf file is stored and click **Next**.



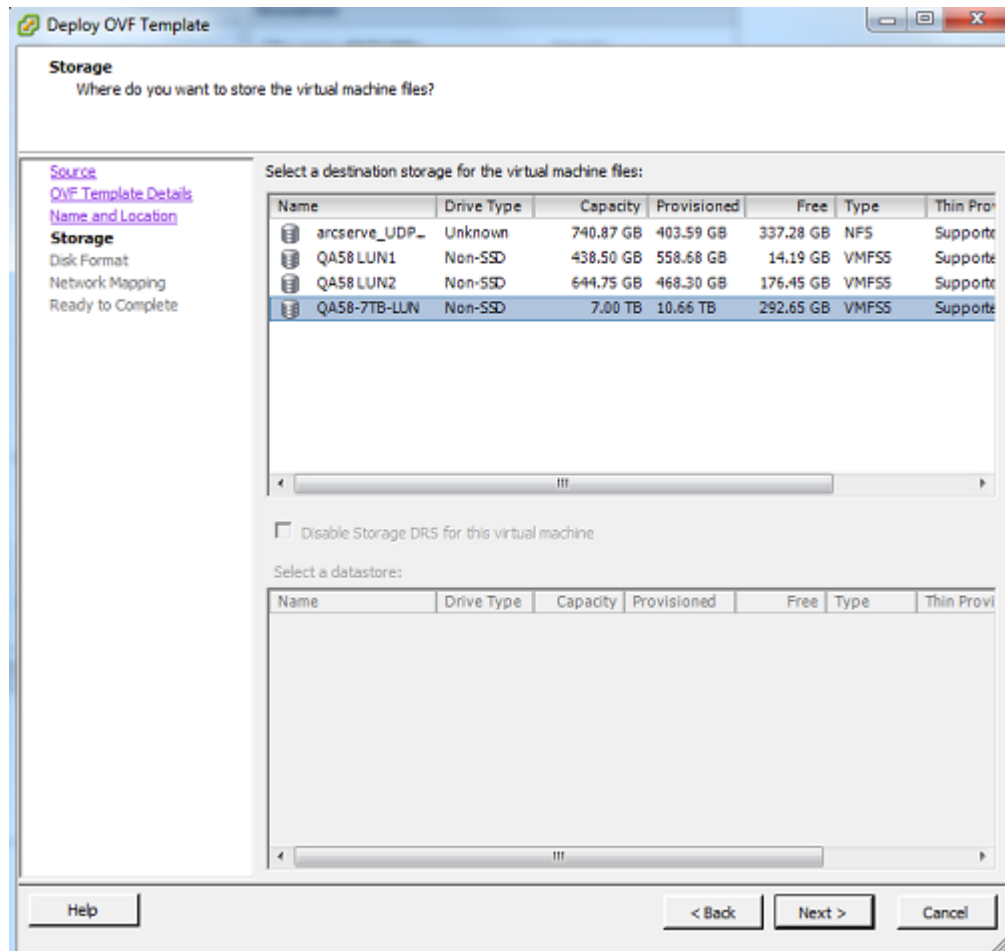
- d. From the **OVF Template Details** tab, review the product details and click **Next**.



- e. From the **Name and Location** tab, enter the display name of VM and click **Next**.



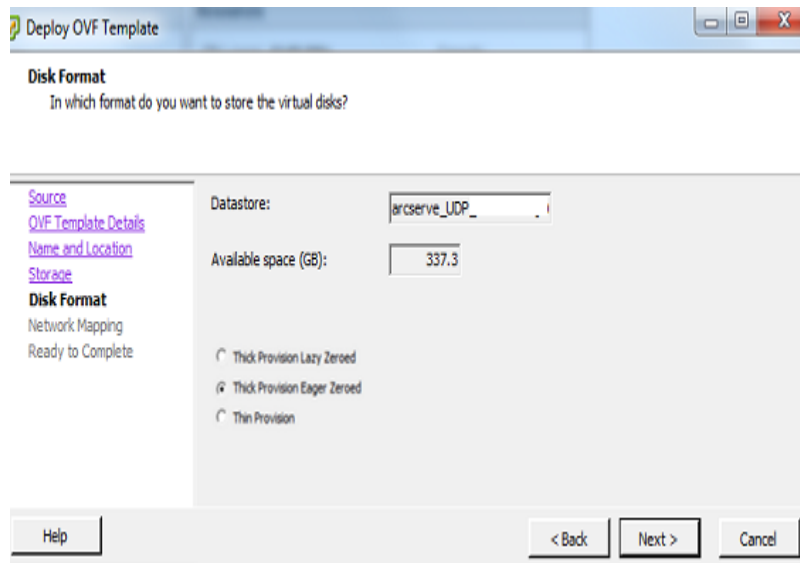
- f. From the **Storage** tab, select one of the available disks as destination storage, and click **Next**.



- g. Select the disk format (one of the options of Thick Provision) that you want the new VM to use and click **Next**.

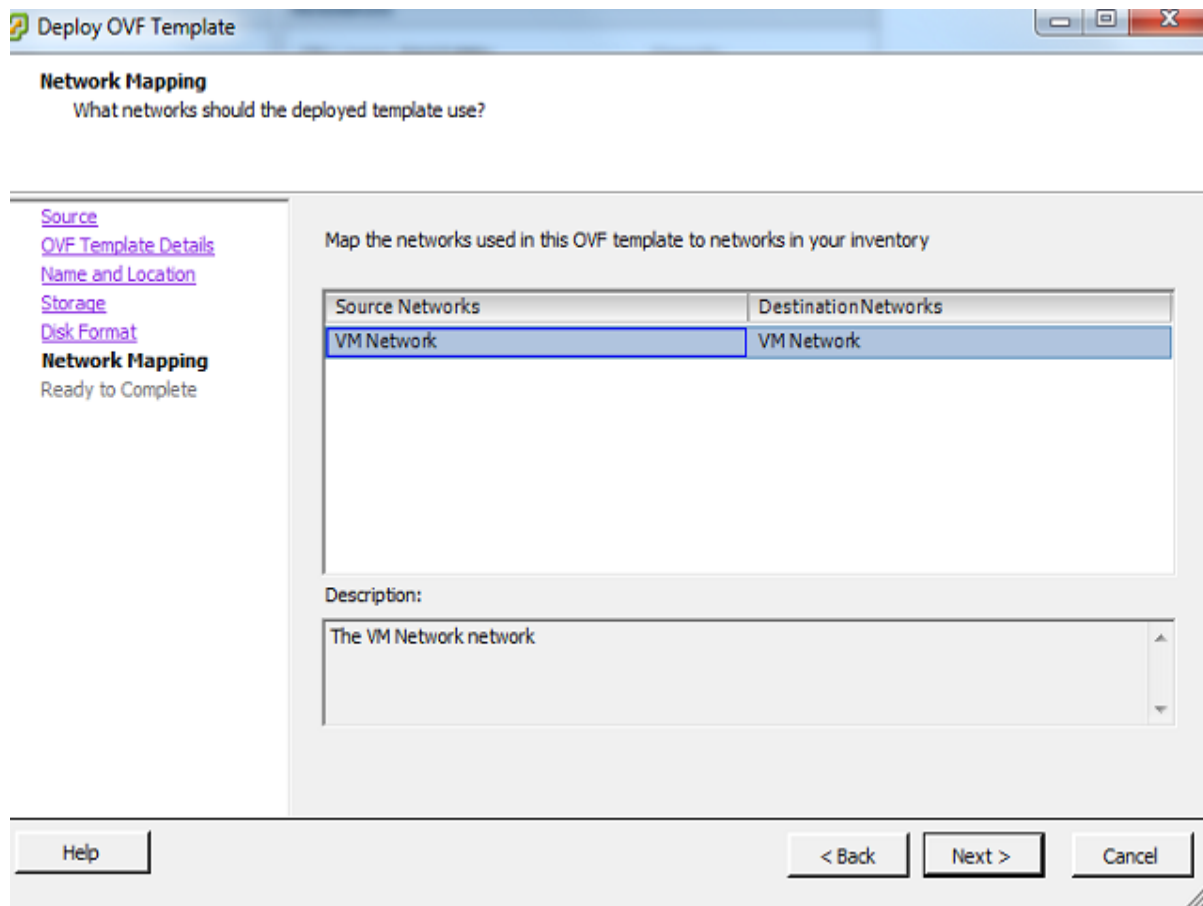
**Note:** We recommend thick provision to ensure that space is allocated to the new VM.



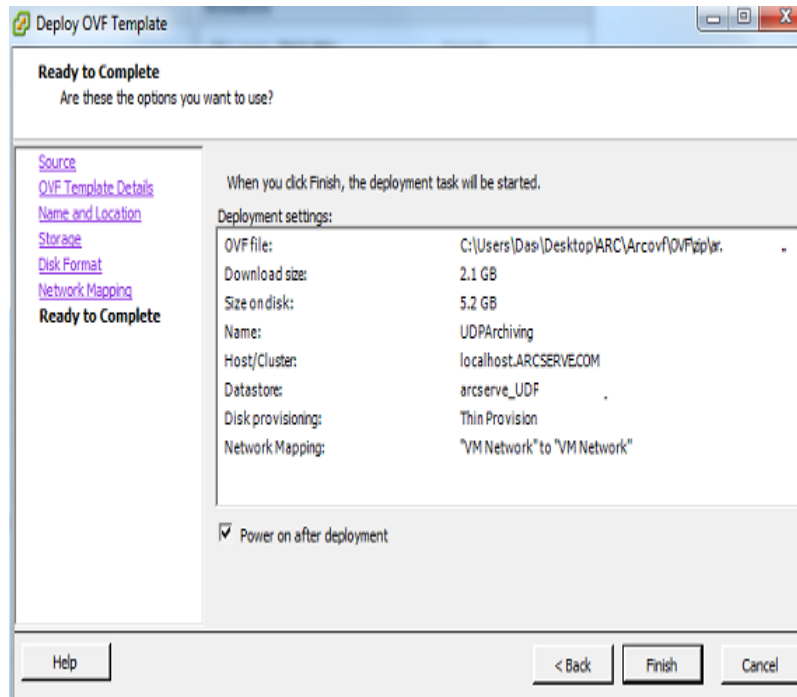


- h. From the **Network Mapping** tab, select one of the available options, and click **Next**.

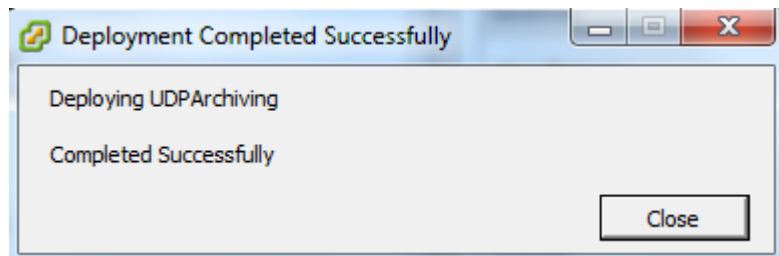
**Note:** Select any network adapter that can communicate to machines across your domain.



- i. Review the summary of selections made in previous steps, select the check box of **Power on after deployment**, and click **Finish**.



Successful deployment results in the following message:



3. Perform the following steps to assign the IP address:
  - a. Navigate to the ESX server and open the VM Console where you deployed UDP Archiving.

**Note:** If you have not selected above the check box option to Power on after deployment before clicking Finish, then first start the UDP Archiving machine on the ESX server before opening the VM Console.
  - b. Locate the IP address assigned to your new VM.
    - ◆ *Using DHCP:* By default, UDP Archiving VM gets an IP Address from DHCP. You can view this IP Address on the VM Console.

**Note:** You can also run **sudo ifconfig** on VM on Console, or navigate to Summary to find the IP address.

- ♦ *Using Static IP:* You can also assign a static IP Address. For details, see [link](#).

4. To complete deployment, follow the steps described in [configuring UDP Archiving](#).

## Deploy UDP Archiving in Hyper-V 2016 and Hyper-V 2012 R2

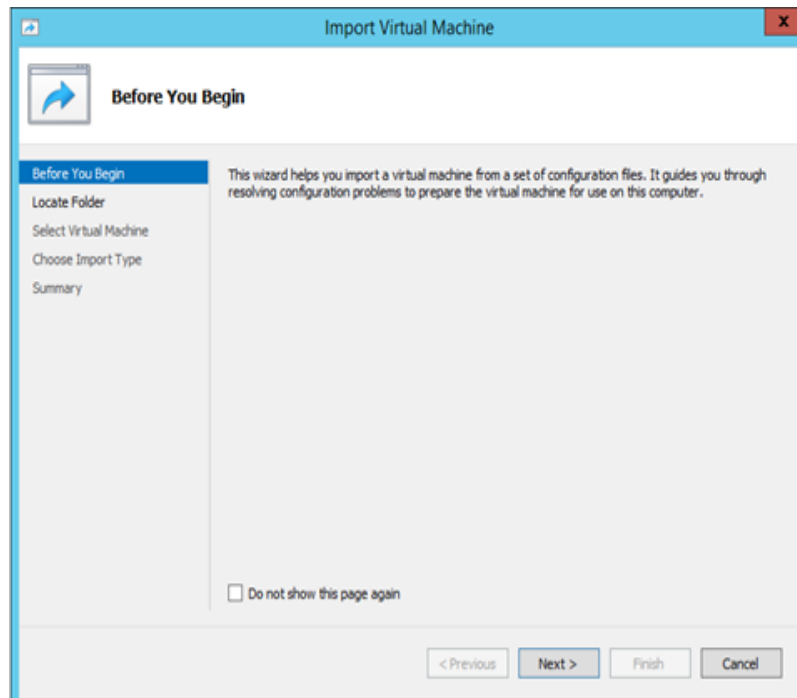
This section describes how to deploy UDP Archiving in Hyper-V. The UDP Archiving is installed with 8 GB of RAM, 2 CPUs, and 16 GB of storage. You can modify RAM and CPU later, but cannot modify storage of the initial volume after deployment. However, adding a new disk to increase storage after installation is possible.

**Troubleshooting:** [Modify DHCP to Static IP for Hyper-V/VMware/AMI after Deployment](#)

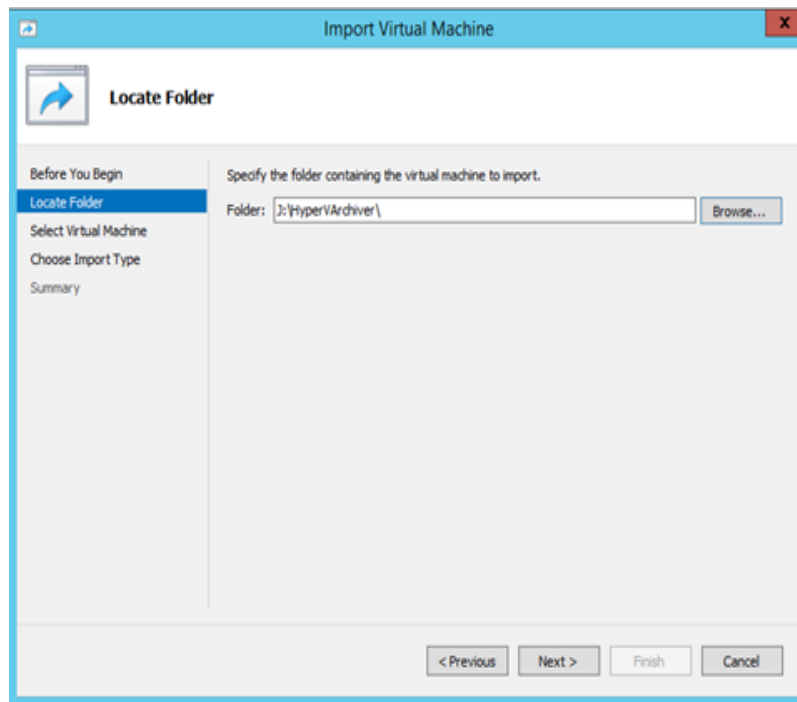
For viewing steps in video, click [How to Deploy UDP Archiving in Hyper-V 2012 R2 and Hyper-V 2016](#).

**Follow these steps to set up and configure UDP Archiving software:**

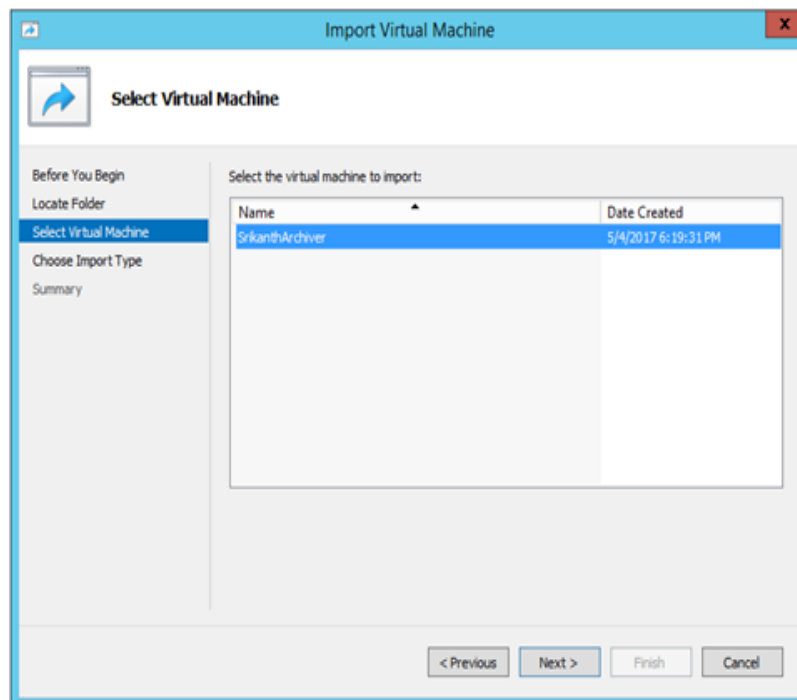
1. Download the UDP Archiving software and store at a folder in your local machine.
2. Set up and deploy the VM using the following steps:
  - a. In Hyper-V Manager, right click your VM host, select **Import Virtual machine**, and click **Next**.



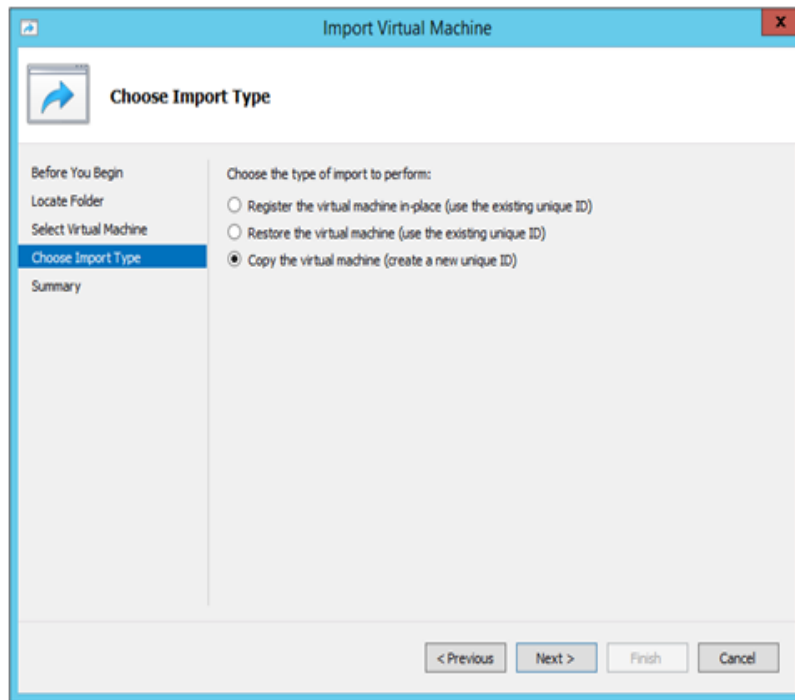
- - b. Browse to the Hyper-V folder where you have downloaded UDP Archiving and click **Next**.



- c. From **Select Virtual Machine**, select the Virtual machine to import and click **Next**.

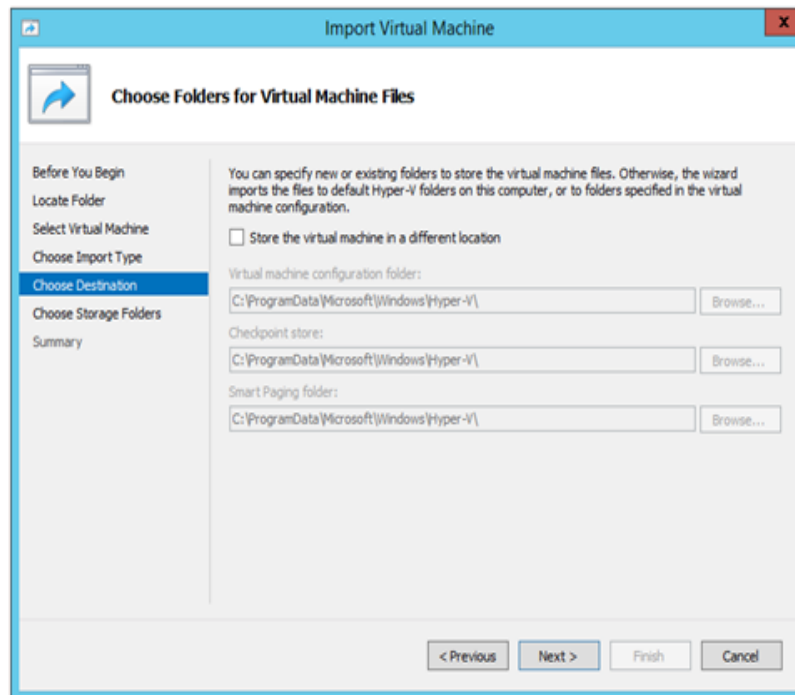


- d. From **Choose Import Type**, select the option: **Copy the virtual machine (create a new unique ID)**, and click **Next**.



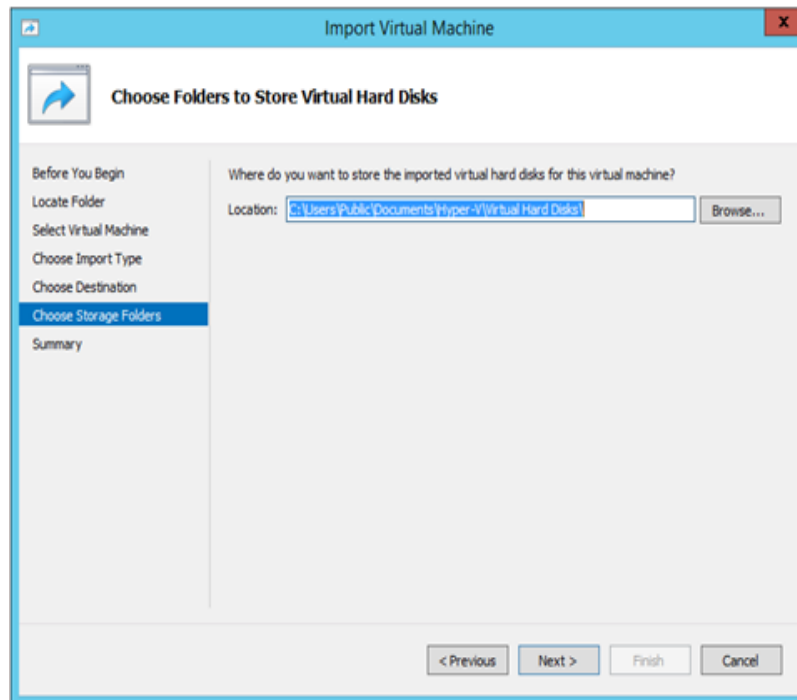
- e. From **Choose Folder for Virtual Machine Files**, select a folder and click **Next**.

**Note:** You can change folders when required.

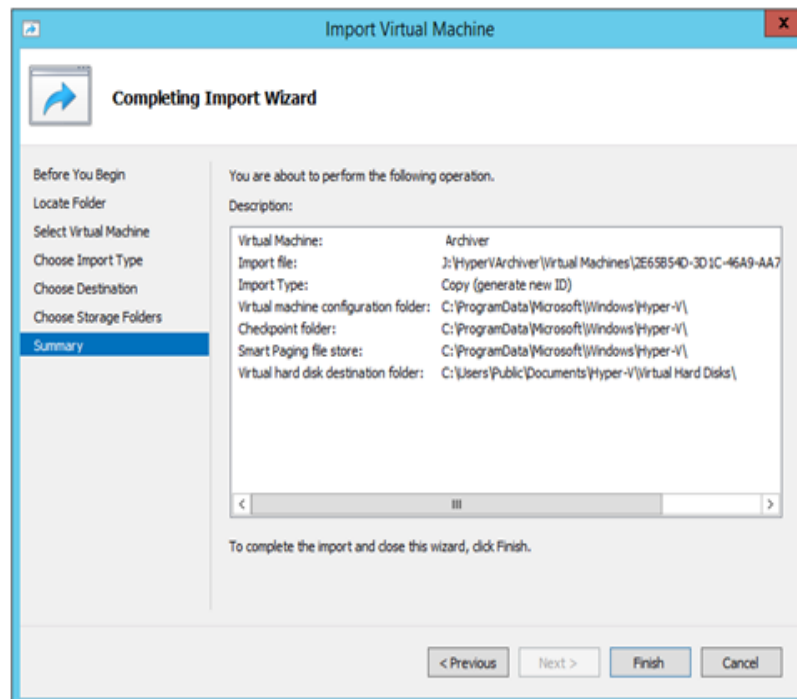


- f. From **Choose Folders to Store Virtual Hard Disks**, select a folder and click **Next**.

**Note:** You can change folders when required.



- g. From Completing Import Wizard, review the complete summary and click **Finish**.



You have deployed Hyper-V successfully.

3. Perform the following steps to configure UDP Archiving:

- a. Navigate to the Hyper-V server and open the VM Console where you deployed UDP Archiving.

**Note:** During set up before clicking **Finish**, if you have not selected the check box option to power on, then first you need to start the UDP Archiving machine on the Hyper-V server, and then open VM Console.

- b. To finish the configuration, locate the IP address assigned to your new VM.

**Note:** The IP address may appear on the command line when you run **sudo ifconfig**. Otherwise, navigate to Summary to find the address.

- ◆ *Using DHCP:* By default, UDP Archiving VM gets an IP Address from DHCP. You can view this IP Address on the VM Console.

**Note:** You can also run **sudo ifconfig** on VM on Console, or navigate to Summary to find the IP address.

- ◆ *Using Static IP:* You can also assign a static IP Address. For details, see [link](#).

- c. Follow the steps of [configuring](#) to complete the installation.



## Modify DHCP to Static IP for Hyper-V/VMware/AMI after Deployment

At times after deployment, IP address is not displayed for Hyper-V or VMware.

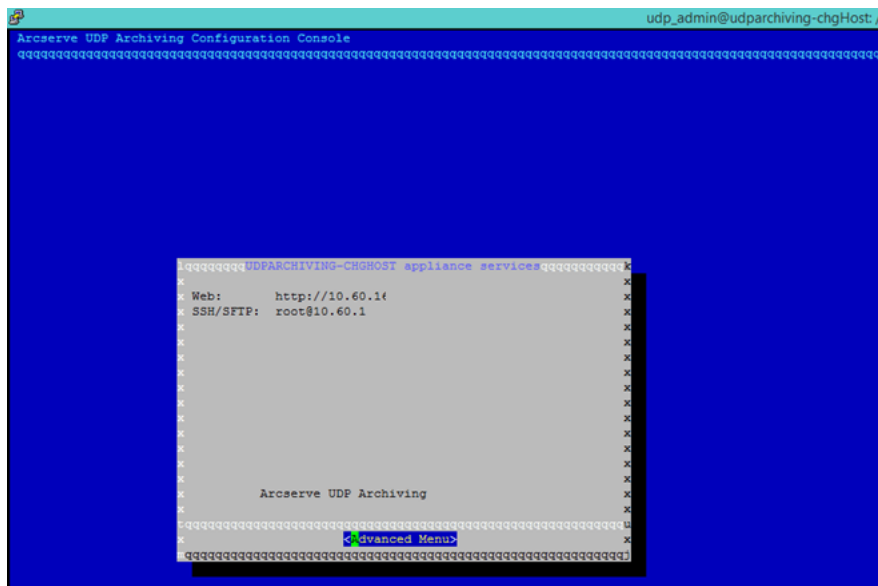
### Symptom

Unable to get DHCP IP address for the Hyper-V or VMware machine after deployment.

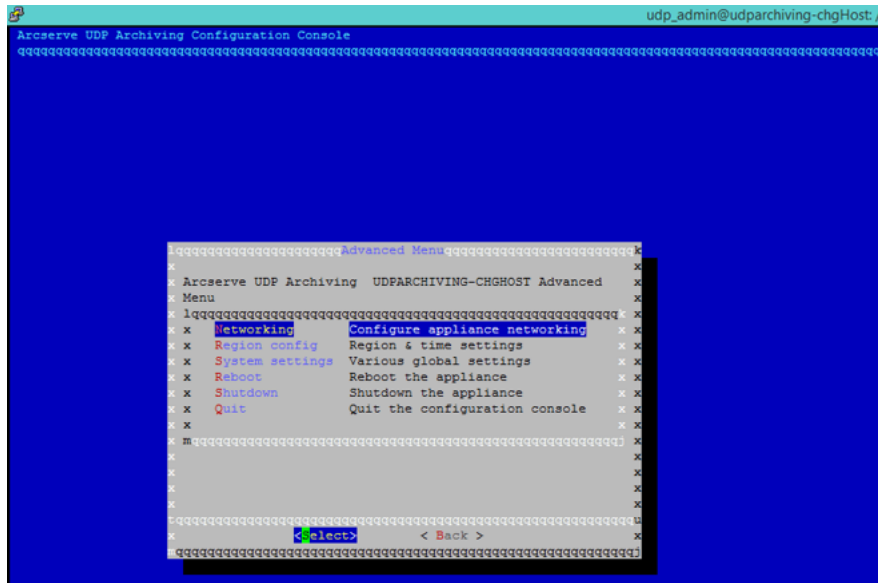
### Solution

As a workaround, perform the following steps:

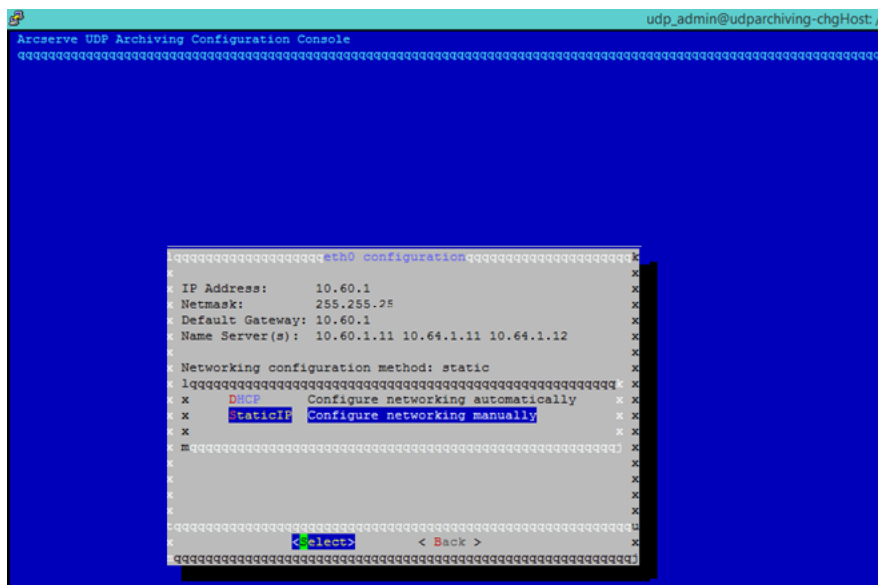
- Log in using `udp_admin` as user name and `sa@#$43` as password.
- In the UDP Archiving VM machine, enter the command `sudo setbox`.



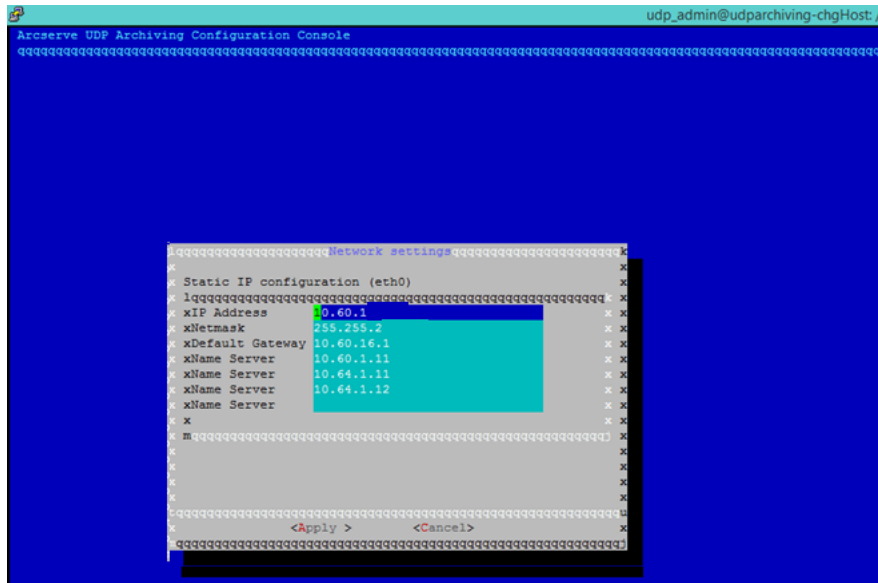
- Select Networking option using arrow keys (up or down) and press spacebar / Enter key, to open the eth0 Configuration screen.



- Select Static IP option and press spacebar / Enter key and navigate to the Network settings screen.

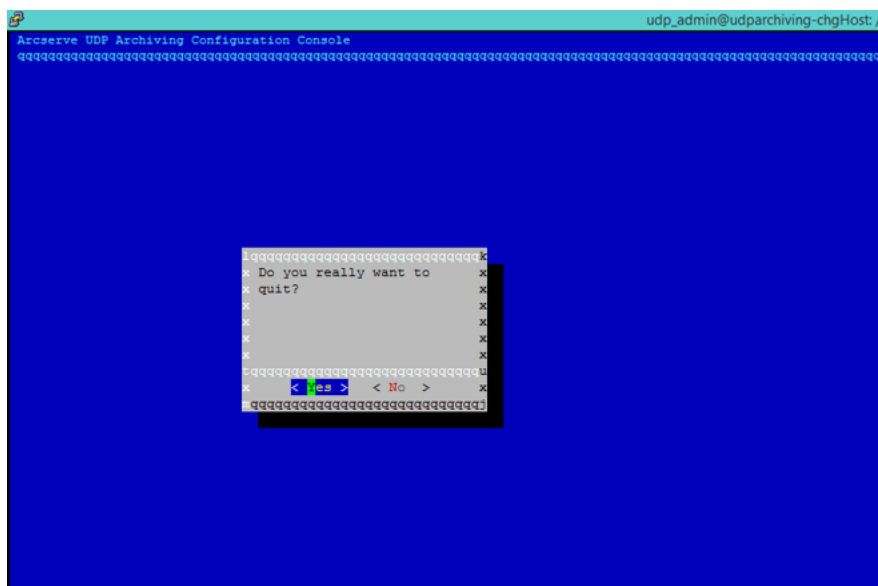


- Provide the static IP information in *IP Address*, *Netmask*, *Default Gateway* and press the Tab button to move to the **Apply** option and press spacebar / Enter key.



The eth0 Configuration screen appears.

- Press ESC button.
- Press spacebar / Enter key on **Yes** options.



## Deploy UDP Archiving in Hyper-V 2008 R2

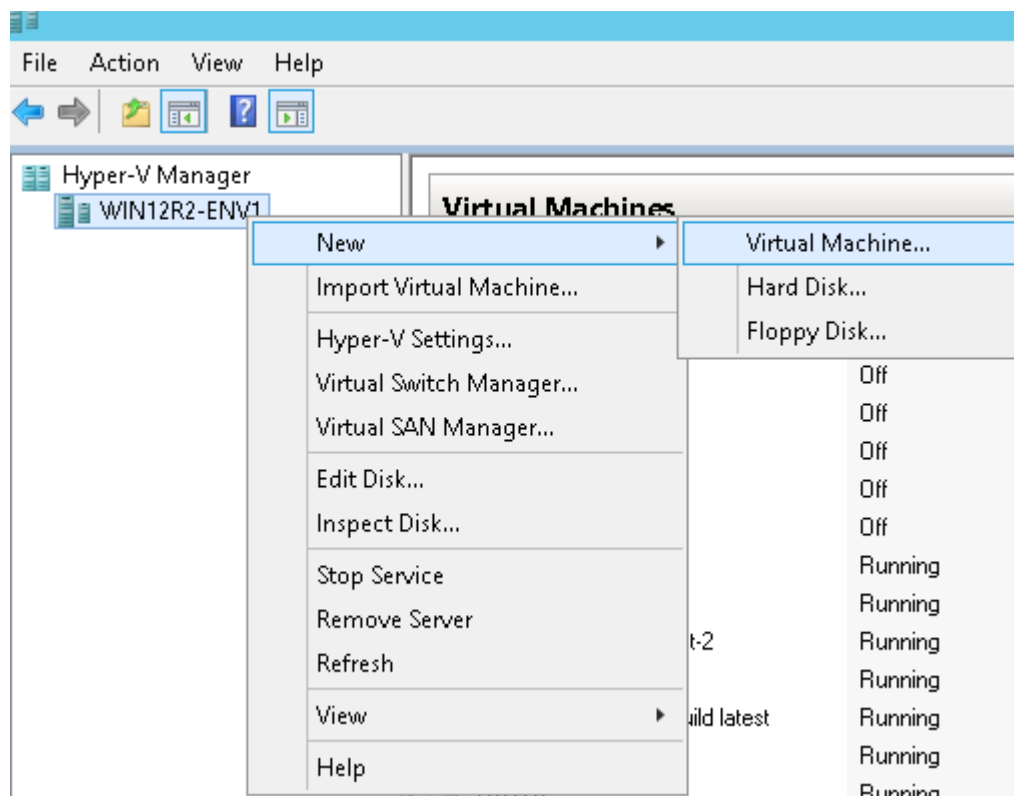
You can deploy UDP Archiving in Hyper-V 2008 R2. UDP Archiving is installed with 8 GB of RAM, 2 CPUs, and 16 GB of storage. You can configure RAM during deployment and modify CPU later. But, modifying storage of the initial volume is not possible after deployment. However, to increase the storage adding a new disk is possible after installation.

For viewing steps in video, click [How to Deploy UDP Archiving in Hyper-V 2008 R2](#).

**Troubleshooting:** [Modify DHCP to Static IP for Hyper-V/VMware/AMI after Deployment](#)

**Follow these steps to set up and configure UDP Archiving software:**

1. Download the UDP Archiving software and store at a folder in your local machine.
2. Set up and deploy the VM using the following steps:
  - a. In Hyper-V Manager, right click your VM host, first select **New**, and then select **Virtual machine**.



New Virtual Machine Wizard is displayed.

- b. From the Wizard, in the **Specify Name and Location** tab, enter a name for the virtual machine, and click **Next**.

- c. From the **Specify Generation** tab, select the check box of Generation 1, and click **Next**.

- d. From the **Assign Memory** tab, assign 4096 to startup memory and click **Next**.

- e. From the **Configure Networking** tab, configure Network connection with the available network adapter and click **Next**.

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected ▼

Not Connected  
 External  
 Hyper-V Virtual Switch

- f. From the **Connect Virtual Hard Disk** tab, select the check box of *Use an Existing virtual hard Disk* option, browse the VHD file in the provided UDP Archiving, and click **Next**.

**Connect Virtual Hard Disk**

Before You Begin  
Specify Name and Location  
Specify Generation  
Assign Memory  
Configure Networking  
**Connect Virtual Hard Disk**  
Summary

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

☐ Create a virtual hard disk  
Use this option to create a VHDX dynamically expanding virtual hard disk.

Name:   
 Location:   
 Size:  GB (Maximum: 64 TB)

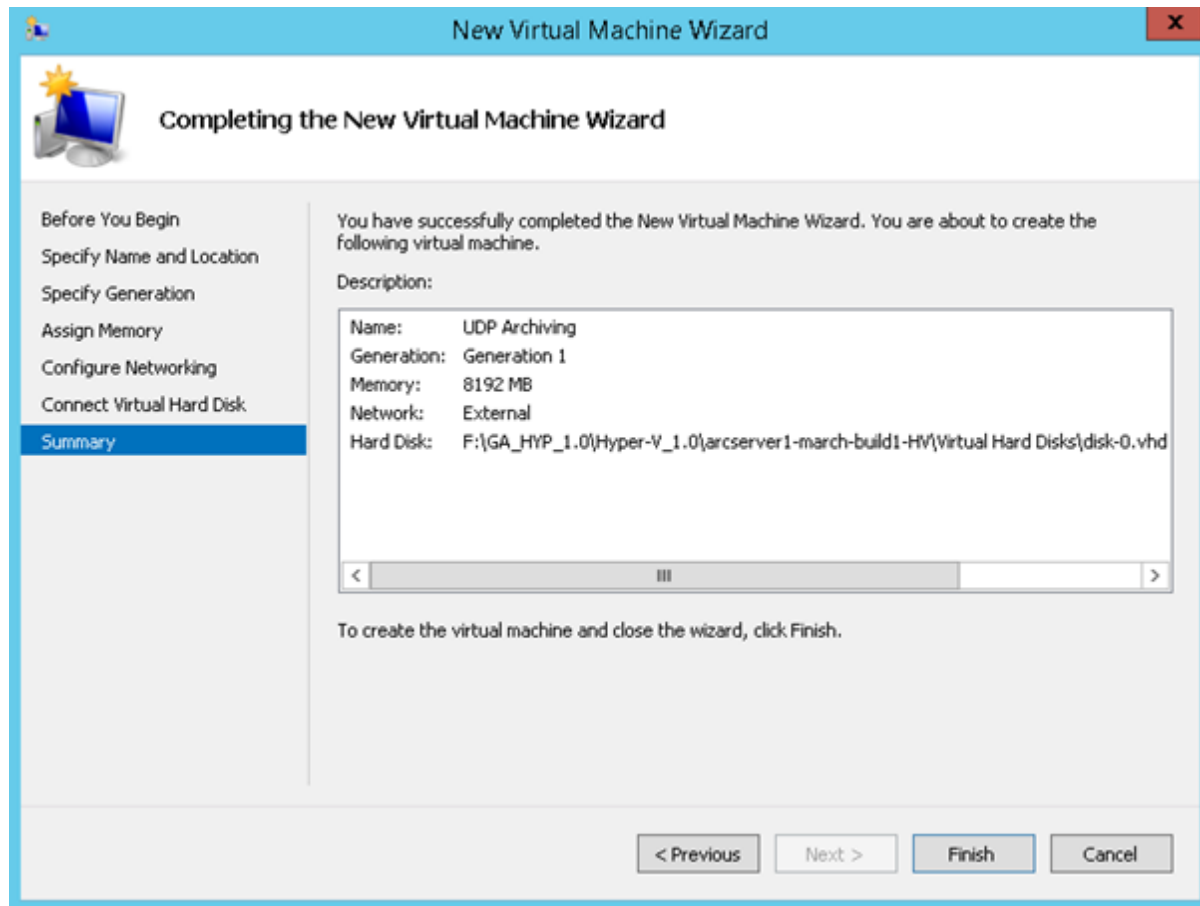
☒ Use an existing virtual hard disk  
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location:

☐ Attach a virtual hard disk later  
Use this option to skip this step now and attach an existing virtual hard disk later.

< Previous   Next >   Finish   Cancel

- g. From the **Summary** tab, review the complete summary and click **Finish**.



Hyper-V 2012 R2 is deployed successfully.

3. Perform the following steps to configure UDP Archiving:

- a. Navigate to the Hyper-V server and open the VM Console where you deployed UDP Archiving.

**Note:** During set up before clicking **Finish** if you have not selected the check box option to power on, then first you need to start the UDP Archiving machine on the Hyper-V server, and then open the VM Console.

- b. To finish the configuration, locate the IP address assigned to your new VM.

**Note:** The IP address may appear on the command line when you run **sudo ifconfig**. Otherwise, navigate to Summary to find the address.

- ♦ *Using DHCP:* By default, UDP Archiving VM gets an IP Address from DHCP. You can view this IP Address on the VM Console.

**Note:** You can also run **sudo ifconfig** on VM on Console, or navigate to Summary to find the IP address.

- ◆ *Using Static IP:* You can also assign a static IP Address. For details, see [link](#).

- c. Follow the steps of [configuring](#) to complete the deployment.



## Deploy UDP Archiving in Microsoft Azure

You can deploy UDP Archiving in Microsoft Azure. UDP Archiving is installed with 8 GB of RAM, 4 CPUs, and a minimum 20 GB of storage. You can configure RAM and modify CPU any time after deployment. You can modify the storage of initial volume after deployment by adding a new disk.

**Follow these procedures:**

---

<a href="#">Add UDP Archiving Virtual Hard Disk to Microsoft Azure</a>	40
<a href="#">Create Virtual Machine and Deploy UDP Archiving</a>	42
<a href="#">Enable UDP Archiving for Public Access</a>	44

## Add UDP Archiving Virtual Hard Disk to Microsoft Azure

UDP Archiving Virtual Hard Disk (VHD) is required to deploy the UDP Archiving solution in Azure. You can add the UDP Archiving solution software to Microsoft Azure and then deploy in a virtual machine.

### Follow these steps:

1. Download **UDP Archiving VHD for Azure** from the [link](#) to the local machine where you access Microsoft Azure.

**Note:** The md5 for UDP Archiving VHD download is  
*46c42b9ee664cab9da113dc4b3a63dec*.

2. Log into the **Microsoft Azure** portal at <https://portal.azure.com> with valid user credentials.
3. On the home page, click **All services** from the left-hand navigation.
4. Under the **General** category, click **Resource groups**.
5. From the **Resource groups** panel, click **Add**.

Create Resource group panel opens.

6. In the **Create Resource group** panel, specify the required information and click **Create**.

For more information, see [Resource Group in Azure](#).

7. Navigate to **All services** page, and click **Storage accounts** under the **Storage** category.

Storage accounts panel opens. For more information, see [Storage Account in Azure](#).

8. From the **Storage accounts** panel, click **Add**.
9. In the **Create storage account** panel, perform the following steps and click **Create**:
  - a. Select the **Resource group** that you created in the previous steps.
  - b. Select the **Account kind** as **storage(general purpose v1)**.
  - c. Specify other details as required.
10. From the Storage account panel, click the **Storage account** name that you created.

11. From the Storage account details panel, click **Blobs** under the **Blob service** category.
12. Click the **+Container** button, enter a name for the new container and click **OK**.
13. From the Blobs screen, click the **Container** that you created.
14. From the Container details screen, click the **Upload** button.
15. From the **Upload blob** panel, click the **Browse** button.
16. Select **UDP Archiving virtual hard disk (VHD) for Azure**.
17. Select SAS as **Authentication type** and click **Upload**.

UDP Archiving VHD for Azure is successfully added to Microsoft Azure.

**Next Steps:**

- [Create Virtual Machine and Deploy UDP Archiving](#)
- [Enable UDP Archiving for Public Access](#)

## Create Virtual Machine and Deploy UDP Archiving

After adding the UDP Archiving VHD, you must create a virtual machine to deploy the UDP Archiving solution.

**Follow these steps:**

1. On the Microsoft Azure home page, click **All services** from the left-hand navigation.
2. Navigate to **All Services**, and click **Disks** from **COMPUTE** category.
3. On the Disks screen, click **Add** to create a new disk.
4. In the Create managed disk panel, perform the following steps and click **Create**.
  - a. Select the **Resource group** that you created for UDP Archiving VHD.
  - b. Select the **Account type** as **Standard HDD** or **Premium SSD** as per your requirement.
  - c. Select the **Source type** as **Storage Blob**.
  - d. In the **Source blob** field, click **Browse** and select the **UDP Archiving VHD** that you uploaded as explained in [Add UDP Archiving VHD to Microsoft Azure](#).
  - e. Select **Linux** as **OS type**.
  - f. Specify **20 GB** as **Size**.
  - g. Specify other details as required.
5. From the list of available disks on the Disks screen, click the newly added **Disk** name.
6. In the Disk details panel, click **Create VM**.
7. In the **Create virtual machine** wizard, perform the following steps:
  - a. In the **Basics** step, select the **Resource group** that you created for UDP Archiving VHD, and click **OK**.
  - b. Click **Change Size**, select a package that includes a minimum of 2 CPUs and 8 GB RAM, and click **Select**. Depending on the package that you select, the number of disks are available.

**Note:** The required number of CPUs and RAM vary depending on the number of mailboxes you want to archive. For more information, view [UDP Archiving Configuration Considerations](#).

- c. From the **Public inbound ports** options, select **Allow selected ports**.
- d. From **Select inbound ports** drop-down list, select all the four options - **HTTP, HTTPS, SSH(22)** and **RDP(3389)**.
- e. Click **Review+create**.
- f. Review the options that you selected and click **Create**.

The Virtual Machine is created and UDP Archiving is successfully deployed.

**Next Step:**

- [Enable UDP Archiving for Public Access](#)

## Enable UDP Archiving for Public Access

After creating the virtual machine and deploying UDP Archiving, you must enable network ports. The enabled ports help to access UDP Archiving using the virtual machine IP address.

### Follow these steps:

1. On the Microsoft Azure home page, click **All services** from the left-hand navigation.
2. Navigate to **All Services**, and click **Virtual machine** from **COMPUTE** category.
3. On the Virtual machines screen, click **Virtual machine name** where you deployed UDP Archiving as explained in [Create Virtual Machine and Deploy UDP Archiving](#).
4. On the Virtual machine details screen, click **Networking** under **Settings**.
5. From the Networking settings, click **Add inbound port rule** and create the ports as follows:
  - a. Create a port with the port range 80 and priority 100.
  - b. Create a port with the port range 25 and priority 370.
  - c. Create a port with the port range 22 and priority 380.

**Note:** For more information about the required open ports, view [UDP Archiving Configuration Considerations](#).

6. If you deployed UDP Archiving v6.0 Update 3, download the patch from [link](#) and apply. For more information about how to apply the patch refer to the documentation available along with the patch.

UDP Archiving is successfully deployed in Microsoft Azure.

## Deploy UDP Archiving in Amazon Web Services (AWS)

You can set up and configure AWS for UDP Archiving using an Amazon Machine Image (AMI).

For viewing steps in video, click [How to Deploy UDP Archiving in AWS](#).

### Follow these steps:

1. Find and select Amazon Machine Image (AMI).

To find AMI, see [Finding Amazon Machine Image \(AMI\)](#).

2. Set up and configure AWS using the following steps:
  - a. From Choose an Instance Type screen, select the server to launch and click **Configure Instance Details**.

Step 2: Choose an Instance Type

amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more about instance types and how they can meet your computing needs.](#)

Filter by: All instance types | Current generation | Show/Hide Columns

Currently selected: t2.large (Variable ECUs, 2 vCPUs, 2.4 GHz Intel Xeon Family, 8 GB memory, EBS only)

	Family	Type	vCPUs	Memory (GB)	Instance Storage (GB)	EBS Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes
<input type="checkbox"/>	General purpose	m4.2xlarge	8	32	EBS only	Yes	High	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

**Note:** Minimum configuration is T2 Large with 2 CPUs and 8 GB of memory. More number of CPUs is always better. For a large migration of legacy messages move to a larger server.

- b. From the Configure Instance Details screen:
  - ◆ Select Use subnet setting (Enable) option for Auto-assign Public IP.
  - ◆ Select the check box of **Enable termination protection**.

### Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances  [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot Instances

Network  [Create new VPC](#)

Subnet  [Create new subnet](#)

Auto-assign Public IP

IAM role  [Create new IAM role](#)

Shutdown behavior

Enable termination protection ☒ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring  
[Additional charges apply.](#)

Tenancy   
[Additional charges will apply for dedicated tenancy.](#)

Advanced Details

- c. From the Add Storage screen, add more storage now or expand the volume later. Change the root volume to desired size for archiving.

Consider the existing message to move to UDP Archiving as well as the existing messages that you need later. An ideal ratio is 1 GB per mailbox per year. For example, 100 GB per year for 100 mailboxes.

Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/sda1	snap-06d4c192061e0c37b	100	General Purpose SSD (GP2)	300 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

- d. (Optional) From Add Tags, you have the option to assign tags.
- Note:** Do not assign tags at present.
- e. From Configure Security Group, open ports as required and click **Review and launch**.



**Step 6: Configure Security Group**

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☐ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source
SSH	TCP	22	Custom <input type="text" value="CIDR, IP or Security Group"/>
HTTP	TCP	80	Custom <input type="text" value="CIDR, IP or Security Group"/>
HTTPS	TCP	443	Custom <input type="text" value="0.0.0.0:::0"/>
LDAP	TCP	389	Custom <input type="text" value="CIDR, IP or Security Group"/>
IMAP	TCP	143	Custom <input type="text" value="CIDR, IP or Security Group"/>
IMAPS	TCP	993	Custom <input type="text" value="CIDR, IP or Security Group"/>
POP3	TCP	110	Custom <input type="text" value="CIDR, IP or Security Group"/>
POP3S	TCP	995	Custom <input type="text" value="CIDR, IP or Security Group"/>
SMTP	TCP	25	Custom <input type="text" value="CIDR, IP or Security Group"/>
Custom TCP Rule	TCP	587	Custom <input type="text" value="CIDR, IP or Security Group"/>
Custom TCP Rule	TCP	465	Custom <input type="text" value="CIDR, IP or Security Group"/>

[Add Rule](#)

[Cancel](#) [Previous](#) [Review and Launch](#)

- f. From **Review Instance Launch** screen, create a new key pair.

**Step 7: Review Instance Launch**

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**Note:** Create the new pair and keep safely.

**Select an existing key pair or create a new key pair**

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Create a new key pair

**Key pair name**

[Download Key Pair](#)

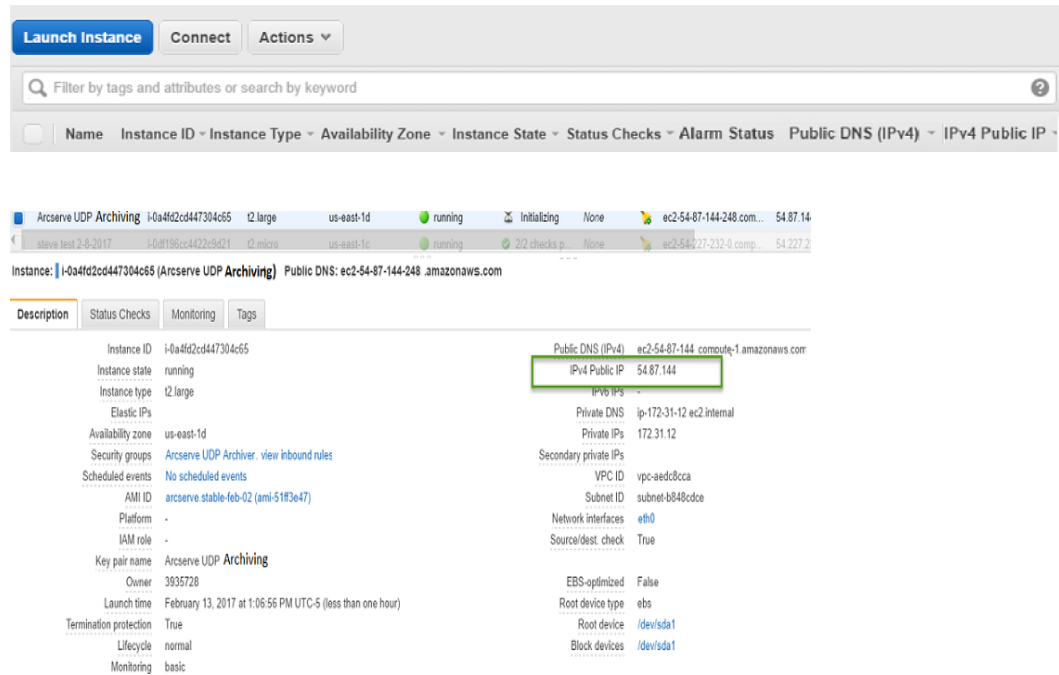
You have to download the **private key file** (\*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

**Recommended to create a new key pair**

[Cancel](#) [Launch Instances](#)

Your UDP Archiving is now configured in AWS.

3. Perform the following steps to configure the UDP Archiving software in a browser:
  - a. First, find your public IP address as shown below.
  - b. Next, map a URL you want to use for your UDP Archiving. For example: email\_archive.acme.com
  - c. Then, navigate to your new URL/welcome.php. For example: email\_archive.acme.com/welcome.php



**Note:** Although you can use the IP address to configure your UDP Archiving, for better results we recommend to redirect a URL to this address.

Important! In AWS, restarting your server changes the IP address. After configuring your system, you can use an Elastic IP.

## Finding Amazon Machine Image

Amazon Machine Image (AMI) is required to deploy UDP Archiving in AWS.

**Follow these steps:**

1. Log into the AWS Console with valid user credentials.
2. From the Services page, click **EC2** available under Compute in the centre pane.
3. Click **Launch Instance** available below Create Instance..
4. From the left pane of Choose an Amazon Machine Image (AMI) perform the following steps:
  - a. Select Community AMIs.
  - b. Enter UDP Archiving AMI name / AMI ID.
  - c. Click Enter to search.
  - d. Select the AMI from the search results and proceed to [configure your instance](#).

## Configure to Access UDP Archiving

After deploying UDP Archiving, complete the basic configuration to access the UDP Archiving Console.

For viewing steps in video, click [How to Setup UDP Archiving after Deployment](#).

**Prerequisites:** Identify one of the following requirements before starting configuration:

- Your hostname (to find, use hostname command)
- The IP address assigned by your network for the UDP Archiving (view from the VM console)
- Verify if the UDP Archiving server is reachable over the network using host-name (FQDN) and the IP address.

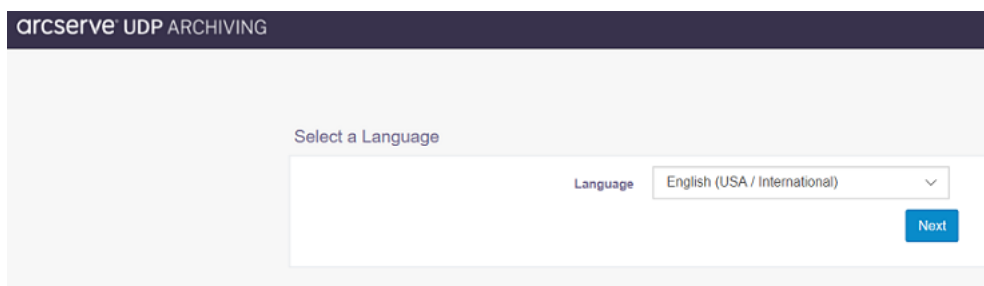
**Note:** If the server is not reachable, you may need to create *A record* on your DNS server for the UDP Archiving server. For details, contact your administrator or click [link](#).

### Follow these steps:

1. Enter the Host name or the IP address in a browser.

**Note:** Modify the host name later for security reasons. For details, see [how to modify the host name](#).

The UDP Archiving window appears. As part of configuration, the first step is to select your preferred language.



2. From the Select a Language screen, select an option from the drop-down menu of **Language**, and click **Next**.

The UDP Archiving Console is displayed in the language that you select here.

The UDP Archiving License Agreement screen appears.

arcserve' UDP ARCHIVING

### End User License Agreement

Please read the following License Agreement carefully.

Arcserve (USA), LLC and/or its affiliates or subsidiaries ("Arcserve")

End User License Agreement (the "Agreement") for the Arcserve software product that is being installed as well as the associated documentation and any SDK, as defined below, included within the product ("the Product").

Carefully read the following terms and conditions regarding your use of the Product before installing and using the Product. Throughout this Agreement, you will be referred to as "You" or "Licensee."

By selecting the "I accept the terms of the License Agreement" radio button below, and then clicking on the "Next" button, you are

☒ I accept the terms of the License Agreement  
☐ I DO NOT accept the terms of the License Agreement

Back Next Cancel

3. Read the license content, select the check box of *I accept the terms of license agreement*, and click **Next**.

The UDP Archiving configuration window appears.

**Note:** If you do not accept the license agreement, select the other checkbox. A confirmation prompt appears. Click **Decline** and the configuration window closes.

## Configuration

\* Fully Qualified Domain Name / IP Address 10.10.10.10

Time Zone Europe/Budapest

Date Format mm-dd-yy

Back Finish

4. Review the following fields, enter the details as necessary, and click **Finish**.

**Fully Qualified Domain Name/IP Address**

Refers to the FQDN or IP address of the UDP Archiving server. The FQDN / IP address details are auto populated. If FQDN is used, the value appears in the following format:

*<host name>.<domain name>*

**Example:** If the host name is *email\_archive* and the domain name is *acme.com*, the FQDN is *email\_archive.acme.com*.

**Note:** FQDN helps mail servers to communicate with UDP Archiving and send journaling emails. The FQDN consists of two parts - the host name and the domain name.

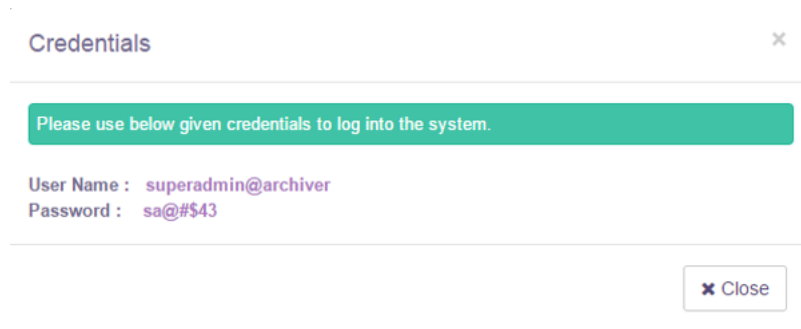
### Time zone

Refers to your preferred time zone. The UDP Archiving Console reflects the time zone that you select here.

### Date format

Refers to your preferred date format. The UDP Archiving Console reflects the date format that you select here.

A **Credentials** pop-up message appears with login credentials.



5. Make a note of the credentials and click **Close**.

The login screen of UDP Archiving appears.

The deployment and basic configuration of UDP Archiving is complete. Now, start with configuration of the UDP Archiving Console and email services, in any order.

To configure the UDP Archiving Console, see [How to Configure Arcserve UDP Archiving](#).

To configure desired email service(s), see [How to Configure Email Services](#).

---

# Chapter 4: How to Configure UDP Archiving

After deployment, Super Admin needs to complete multiple configurations in UDP Archiving. The configuration process starts just after deployment when you are automatically directed to the login screen of UDP Archiving.

For viewing steps in video, click [How to Configure UDP Archiving after Deployment](#).

This section contains the following topics:

---

<a href="#">Review Prerequisites and Considerations</a>	54
<a href="#">Log into UDP Archiving</a>	56
<a href="#">Configure Settings of UDP Archiving</a>	57

## Review Prerequisites and Considerations

Before configuring the settings of UDP Archiving, verify the prerequisites and considerations.

### Considerations

- Based on your requirement, configure RAM and CPU.  
The minimum requirement is 8 GB RAM and 2 dual core CPUs.  
Some considerations:
  - ◆ Up to 1,000 employees: 8 GB of RAM and 2 dual core CPUs
  - ◆ 1,000 – 2,500 employees: 12 GB of RAM and 4 dual core CPUs
  - ◆ 2,500 – 5,000 employees: 12 GB of RAM and 6 dual core CPUs
  - ◆ 5,000 – 10,000 employees: 12 GB of RAM and 8 dual core CPUs
- For cloud deployments, select a server with the above minimum CPUs (more CPU is better).
- Exception, Retention rules, and Legal hold policies are applicable to all emails getting into UDP Archiving server through Historic Email Ingestion (Migration and Import).
- Email Retention (Days to Retain Messages): Super Admin has the option to set Global Email Retention. Number of days entered by Super Admin is the default setting for Global Email Retention unless administrator later overrides by setting the Domain Level Retention Policy.

### Prerequisites

- Set security setting

Verify if required ports are available. Open the following ports depending upon your network requirements:

- ◆ HTTP/HTTPS 80, 443
- ◆ IMAP/IMAPS 143, 993
- ◆ POP/POPS 110, 995
- ◆ SMTP 25
- ◆ TLS Secure 587

**Note:** Even when mail servers are configured with encryptions such as TLS 1.2 / 1.1; UDP Archiving communicates only through TLS 1.0.



- ◆ SSL Secure 465
- ◆ SSH port 22
- ◆ LDAP 389

- Storage

Verify if UDP Archiving is set up with minimum 20 GB of storage for Microsoft Azure and 16 GB of storage for others as initial configuration. You can add new disks to increase storage. For more details, refer to UDP Archiving *Administration Guide*.

## Log into UDP Archiving

Open a browser and enter the IP address assigned to your UDP Archiving server.  
For the first login, use the following credentials:

- User name: superadmin@archiver
- Password: sa@#\$43

**Important!** Change the password after logging into UDP Archiving.

After login, the health dashboard of UDP Archiving appears.

## Configure Settings of UDP Archiving

Configuration of UDP Archiving is required to accept incoming messages from corresponding domains. To configure the settings, super admin follows four mandatory steps:

1. [Add Domain](#)
2. [Add Profile for Each Domain](#)
3. [Create Archiving Administrators for Each Domain](#)
4. [Set the Forwarding Mail Server](#)

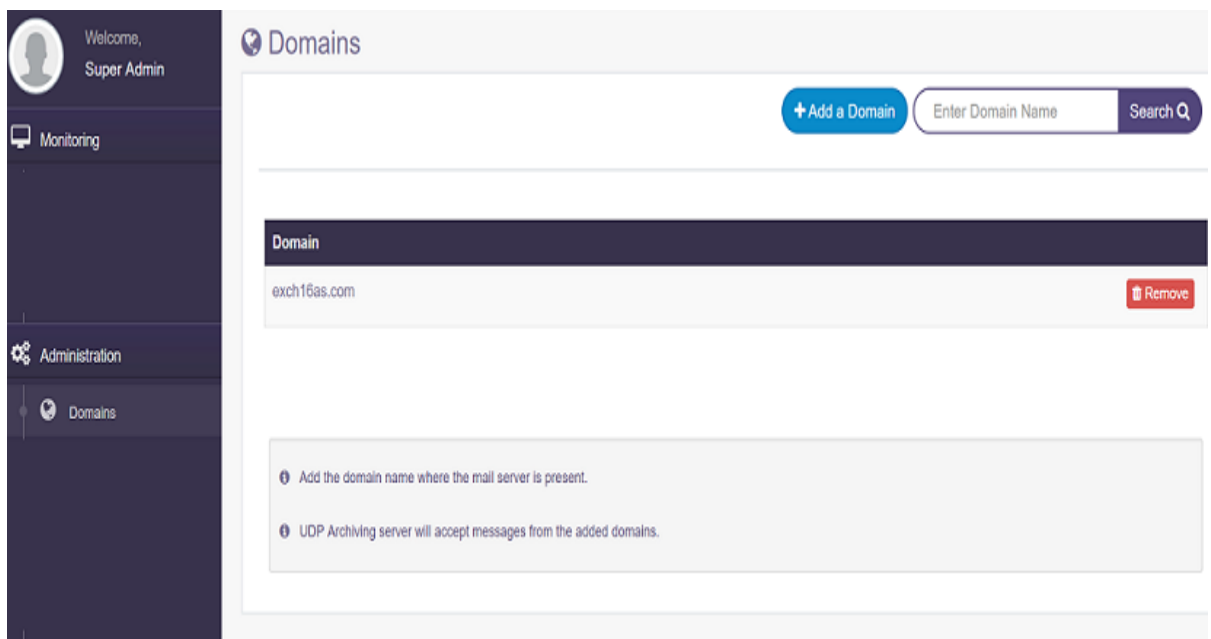
## Enter Domain for Mail Server

Adding domain is the first step in configuring UDP Archiving. For a service provider, super admin would add domains for every archiving customers. For example: If you have a domain of exchps.com and mails are coming from this domain Super Admin sets up this domain in the system.

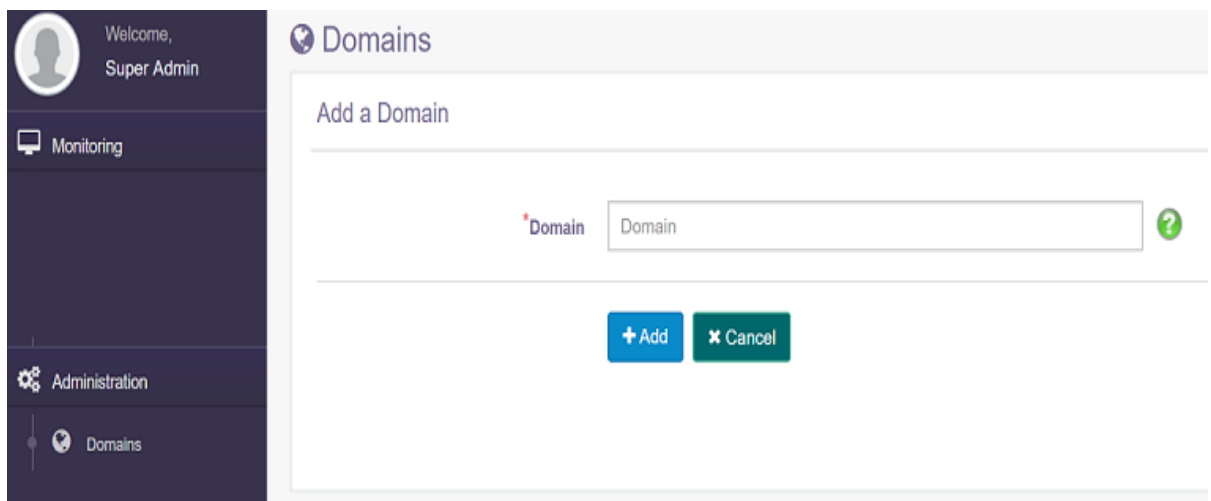
Add more than one domain depending upon the requirement.

### Follow these steps:

1. From the left pane, click **Domains** under *Administration*.



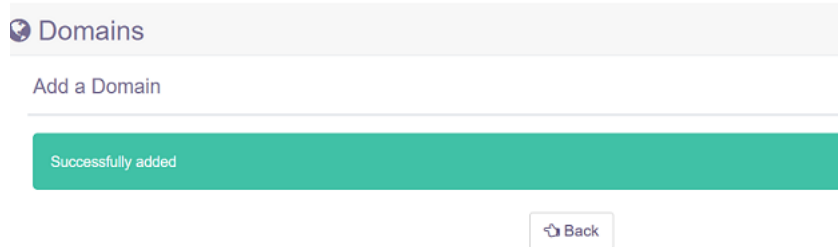
2. From the Domains page, click **Add a Domain**.



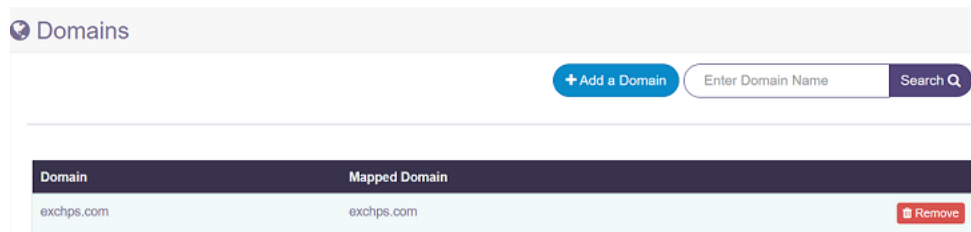
3. For Domain, enter the mail server domain address for mails coming to UDP Archiving.

The domain information is available at *Mail Server > System Properties*.

4. Click **Add**.



5. From the confirmation message, click **Back**.



Added domain is displayed on the Domains page.

The domain is added for the mail server. Now, [create contacts](#) using the Profile option.

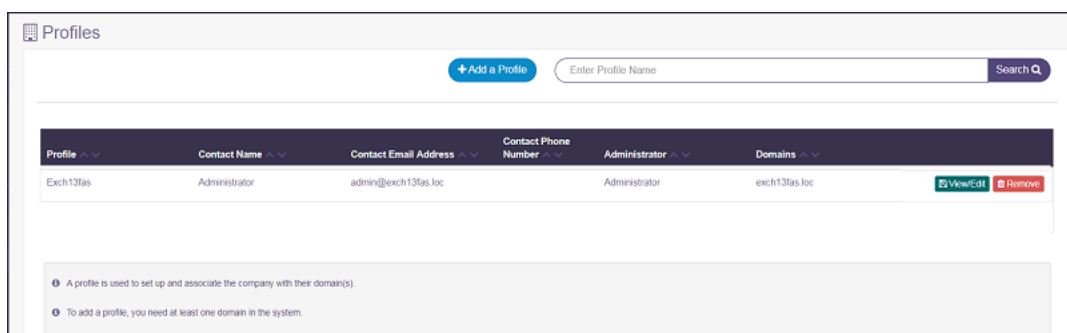
## Add Profiles for Each Domain

Adding profile is the second step in configuring UDP Archiving. A profile is used to set up the company information and associates a company with the domain(s). Super Admin can add a profile to the system for a company or a separate profile for each customer domain of service provider.

**Note:** UDP Archiving must have a domain configured before adding a profile.

**Follow these steps:**

1. From the left pane, click **Profiles** under *Administration*.



2. Click **Add a profile**.

The screenshot shows the 'Add a Profile' form. It includes the following fields:
 

- Profile Name:** Arcserve
- Contact Name:** Arcserve Admin
- Contact Email Address:** admin@arcserve.com
- Contact Mailing Address:** (empty)
- Contact Phone Number:** (empty)
- Domain(s):** A dropdown menu showing 'arcserve.com' (selected) and 'exch13fas.loc'.

 At the bottom of the form are '+ Add' and 'Cancel' buttons. A note at the very bottom states: 'Hold the Ctrl (Windows) / Command (Mac) button to select multiple options for domains.'

3. Enter the following details and click **Add**:

### Profile

Enter a name for the profile.

**Contact Name**

Enter the contact name of profile.

**Email Address**

Enter the email address of the contact.

**Contact Address**

Enter address of the contact.

**Contact Phone Number**

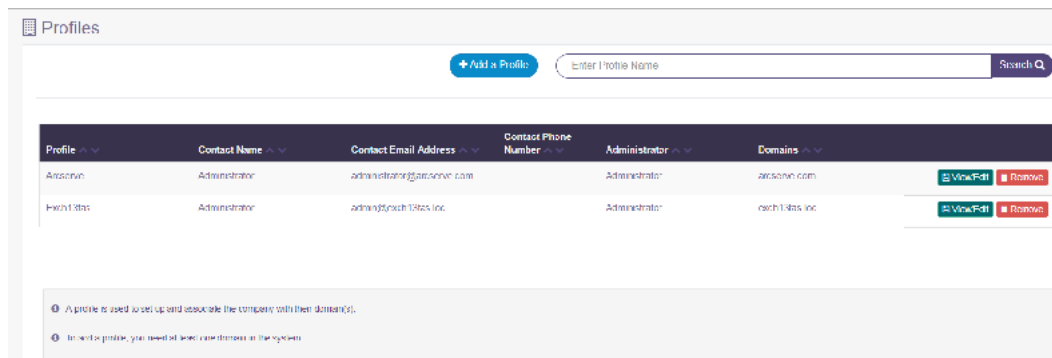
Enter phone number of the contact.

**Domain(s)**

Select one domain from the available list of domains. The list displays only those domains that super admin added before using [Add a domain](#).

The profile is added. A confirmation message appears.

4. Click **Back** and view the added contact in the Profiles page.



The profile is created. In the screen above, the detail under Administrator column appears when you assign the profile to an administrator.

Now, [create administrator](#) to manage users.

## Create Archiving Administrators for Each Domain

Creating an administrator is the third step in completing configuration of UDP Archiving. Super Admin creates an Administrator for each domain. The credentials are set for the administrator to access the system and manage settings that are specific to the archiving requirements for a domain. The administrator can create more administrators with similar access rights.

### Follow these steps:

1. From the left pane, click **Administrators** under *Administration*.

The screenshot shows the 'Administrators' management page. At the top, there is a header with a user icon and the title 'Administrators'. Below the header, there is a blue button labeled '+ Add an Administrator' and a search bar with the placeholder text 'Enter Contact Name or Email Address' and a 'Search' button. The main content area features a table with the following columns: 'Contact Name', 'Contact Email Address', 'Role', 'Profile', 'Domains', and 'Status'. The table contains one row with the following data: 'Adminjp', 'administrator@exch13fas.loc', 'Master Admin', 'Jpr', 'exch13fas.loc', and a green checkmark status. To the right of the status is a 'View/Edit' button and a 'Remove' button. Below the table, there is a pagination control showing '<< < 1-1, total: 1 > >>'. At the bottom, there is a box containing four informational messages:

- 1 Create an administrator to associate with each profile.
- 1 Administrator can login using the email address and password provided here.
- 1 Administrator can access the system and manage policies for their domain(s).
- 1 One Administrator can be associated with multiple profiles.

2. Click **Add an Administrator**.



The screenshot shows a web interface titled 'Administrators' with a sub-header 'Add an Administrator'. The form contains five input fields: 'Contact Name' (text), '\*Email Address' (text with a green question mark icon), 'Profile' (a dropdown menu showing 'exch 16 UDP com'), '\*Password' (text with a green question mark icon), and '\*Re-Enter Password' (text). At the bottom of the form are two buttons: a blue '+ Add' button and a green 'X Cancel' button.

3. In the **Add an Administrator** screen, enter the following details and click **Save**.

**Contact Name**

Enter a name for administrator.

**Email Address**

Enter the email address of administrator. The email address must belong to the domain that is linked with the profile selected in the Profile field.

**Profile**

Select a profile for which you want to add the administrator.

**Password**

Enter a password for the first login of Administrator to UDP Archiving. The administrator can change the password after logging for the first time.

**User Role**

Assign a user role from the drop-down option.

A confirmation message informs about successful creation of the administrator.

4. From the confirmation screen click **Back**.

The administrator details appear on the Administrators page.

Administrators

+ Add an Administrator

Search

Contact Name ^ v	Email Address ^ v	Role ^ v	Profile ^ v	Domains ^ v	Status	
Admin Exch 16	admin@exch16as.com	Master Admin	Exch 16 UDP Com	exch16as.com	<div></div>	<div>View/Edit</div> <div>Remove</div>

« < 1-2, total: 2 > »

Create an administrator to associate with each profile.

Administrator can login using the email address and password provided here.

Administrator can access the system and manage policies for their domain(s).

One Administrator can be associated with multiple profiles.

**Note:** Now, the [Profiles](#) tab displays the name of created administrator for the selected profile.

Now, set [forwarding mail server](#) to complete configuration.

## Set the Forwarding Mail Server

Setting the forwarding mail server completes the mandatory configuration of UDP Archiving. Forwarding email server is the server whose messages are to be accepted and archived by UDP Archiving. All messages from the added servers are always archived. On the other hand, messages of servers not set as forwarding mail server are not archived. For example, while using Microsoft Exchange to send message to UDP Archiving through SMTP you need to add the IP address of each Exchange server.

Provide an SMTP Forwarding Email Address that is used later to set up journaling on the mail servers. For specific configuration instructions, view configuration for each type of mail server.

**Important!** Save the SMTP Forwarding Email Address as the same information is required while creating Journaling rule.

**Follow these steps:**

1. From the left pane, click **Configuration** under **Administration**.

The Configuration page appears.

2. Review the following fields and enter the details as necessary:

### Fully Qualified Domain Name/IP Address

Refers to the FQDN or IP address of the UDP Archiving server. The FQDN / IP address details are auto populated. If FQDN is used, the value appears in the following format:

*<host name>.<domain name>*

**Example:** If the host name is *email\_archive* and the domain name is *acme.com*, the FQDN is *email\_archive.acme.com*.

**Note:** FQDN helps mail servers to communicate with UDP Archiving and send journaling emails. The FQDN consists of two parts - the host name and the domain name.

### SMTP Forwarding EMAIL Address

Refers to the email address used for alerts. The email address is used as forwarding email address through SMTP to UDP Archiving.

**Example:** archive@<IP Address> or archive @<FQDN of Archiving VM>.

### Time Zone

Select your preferred time zone.

3. Click **Save**.

The forwarding email address is configured.

Now, before starting to archive email ensure to [configure Email service](#).

---

## Chapter 5: How to Configure Email Services

UDP Archiving allows integration with multiple email services. Configure email services to suit your requirement and start archiving the emails.

**Important!** Hosted Archiving customers do not need to perform steps performed by Super Admin.

This section contains the following topics:

---

<a href="#">Configuring Microsoft Office 365</a>	68
<a href="#">Setting up Access to UDP Archiving from Outlook Web Access</a>	86
<a href="#">Configuring Microsoft Exchange 2007</a>	87
<a href="#">Configuring Microsoft Exchange 2010</a>	100
<a href="#">Configuring Microsoft Exchange 2013 and 2016</a>	122
<a href="#">Configuring G Suite Email</a>	136
<a href="#">Configuring IBM Lotus Domino</a>	141
<a href="#">Configuring Zimbra</a>	157
<a href="#">Configuring Sendmail</a>	158
<a href="#">Configuring Postfix</a>	160
<a href="#">Configuring Kerio</a>	162

## Configuring Microsoft Office 365

To configure Microsoft Office 365, perform the following steps:

1. [Review Prerequisite and View Mail Flow](#)
2. [Create a Non-routable New Remote Domain](#): UDP.int
3. [Create a Fake Mail Contact using New Domain](#):archive@UDP.int
4. [Create a Non-deliverable Mailbox](#): JournalNDR@<your domain>
5. [Create a Send Connector for the Remote Domain](#)
6. [Add a Journaling Rule to direct Messages](#)

### Prerequisite:

Verify if you have Fully Qualified Domain Name (FQDN) of your new UDP Archiving system set during the [initial deployment](#).

### Mail Flow Process After Configuring:

1. [Journal Rule](#) directs all messages to the [Mail Contact](#).
2. Report of any undelivered messages reach the [NDR mailbox](#).
3. The [Send Connector](#) forwards any messages going to the [fake remote domain](#) to your UDP Archiving(archive@<fqdn of Archive>).

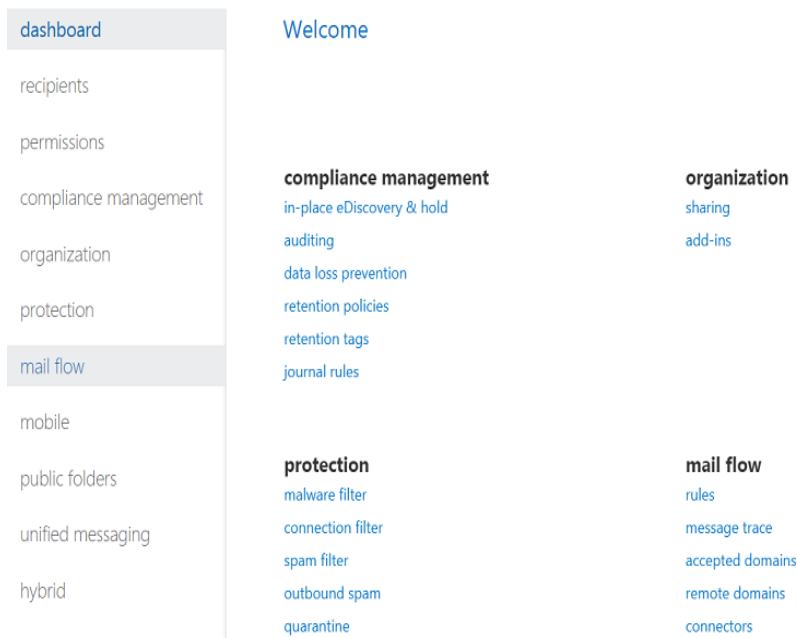
## Create a Non-routable New Remote Domain

Office 365 requires a remote domain to send the messages to the mail server (SMTP). The Remote Domain is not your regular email domain. The remote domain is a non-existent and non-routable/unresolvable domain from either inside or outside your organization (such as UDP.int). This domain is mandatory for the email address of the Mail Contact that is the recipient of the journaled message.

### Follow these steps:

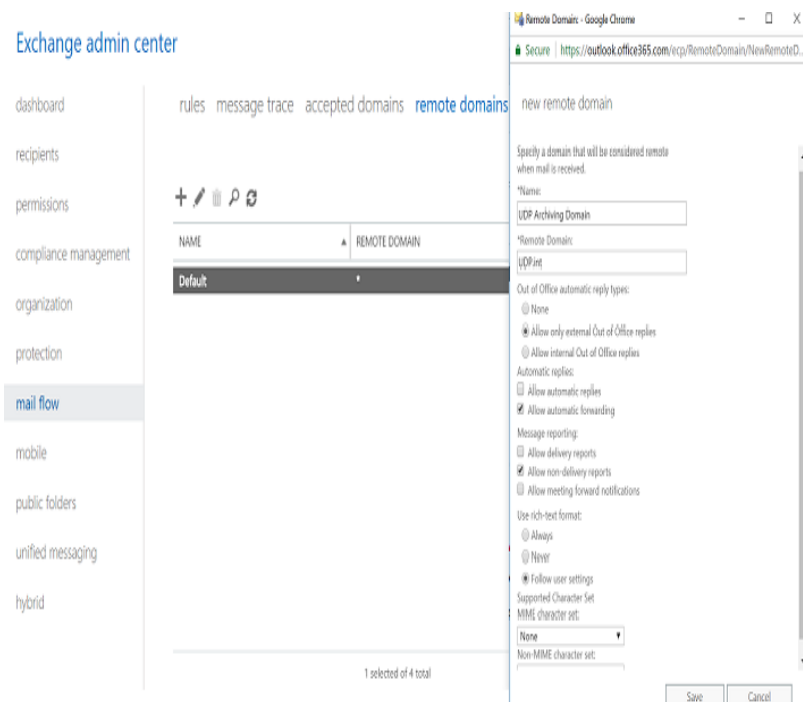
1. From **Exchange Admin Center** screen, select **mail flow**.

#### Exchange admin center



The **mail flow** screen opens.

2. Select remote domains and click + to add a new remote domain.



Enter the following details:

- **Name:** UDP Archiving Domain

- **Remote domain:** UDP.int

**Note:** You can enter name of an internal and non-routable domain. Make a note of the domain name as you need to use the same name later.

- **Other:**

- ◆ **Out of Office reply types:** Select **None**.
- ◆ **Use rich-text format:** Select **Never**.
- ◆ Clear selection for all other options.

3. Click **Save**.

The new domain is created and displayed.



## Exchange admin center

rules message trace accepted domains remote domains connectors

+ / [icon] [icon]

NAME	REMOTE DOMAIN
UDP Archiving Domain	UDP.int

UDP Archiving Domain

Fully qualified domain name:  
UDP.int

Out of Office replies configuration:  
External

Automatic replies:  
Disabled

Automatic forward:  
Enabled

Delivery report:  
Disabled

Non-delivery report (NDRs):  
Enabled

Meeting forward notification:  
Disabled

## Next Steps:

1. [Create a Fake Mail Contact using New Domain](#)
2. [Create a Non-deliverable Mailbox](#)
3. [Create a Send Connector for the Remote Domain](#)
4. [Add a Journaling Rule to direct Messages](#)

## Create a Fake Mail Contact using New Domain

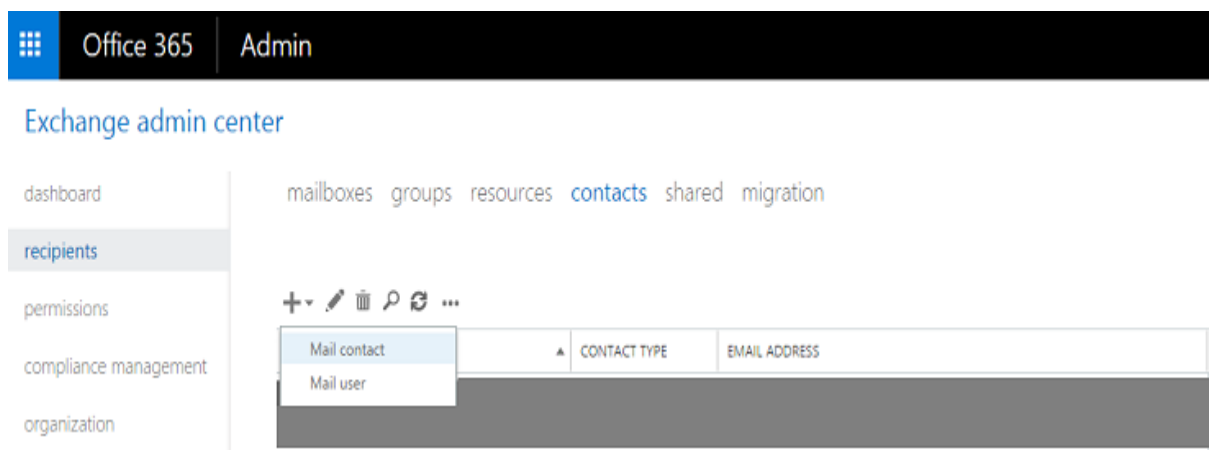
The Mail Contact is the account that acts as a *holding location* for journaled messages. The email address associated with this account is the designated recipient and must be associated with a non-existent, non-routable dummy Domain Name created in [previous step](#).

**Follow these steps:**

1. From **Exchange Admin Center** screen, select **recipients**.

The **recipients** screen opens.

2. Select **contacts** from the recipients screen.



3. Click **+** and select **Mail contact** to add.

The **new mail contact** screen opens.

4. Enter the following details:

- **First name:** Arcserve
- **Initials:** UDP
- **Last Name:** UDP Archiving
- **Display Name:** Arcserve UDP Archiving
- **Alias:** EmailArchive
- **External email address:** archive@UDP.int

**Note:** Make a note of the email address as you need to use the same ID later.

New Mail Contact - Google Chrome

Secure | <https://outlook.office365.com/ecp/UsersGroups/NewContact.aspx?...>

new mail contact

First name:

Initials:

Last name:

\*Display name:

\*Alias:

\*External email address:

5. Click **Save** to create the mail contact.

## Exchange admin center

dashboard

recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

unified messaging

mailboxes groups resources **contacts** shared migration

DISPLAY NAME	CONTACT TYPE	EXTERNAL EMAIL ADDRESS
Arcserve UDP Archiving	Mail contact	SMTP:archive@UDP.int

Arcserve UDP Archiving

Mail contact  
archive@UDP.int  
Office:  
Work phone:

The mail contact is successfully created.

**Next Steps:**

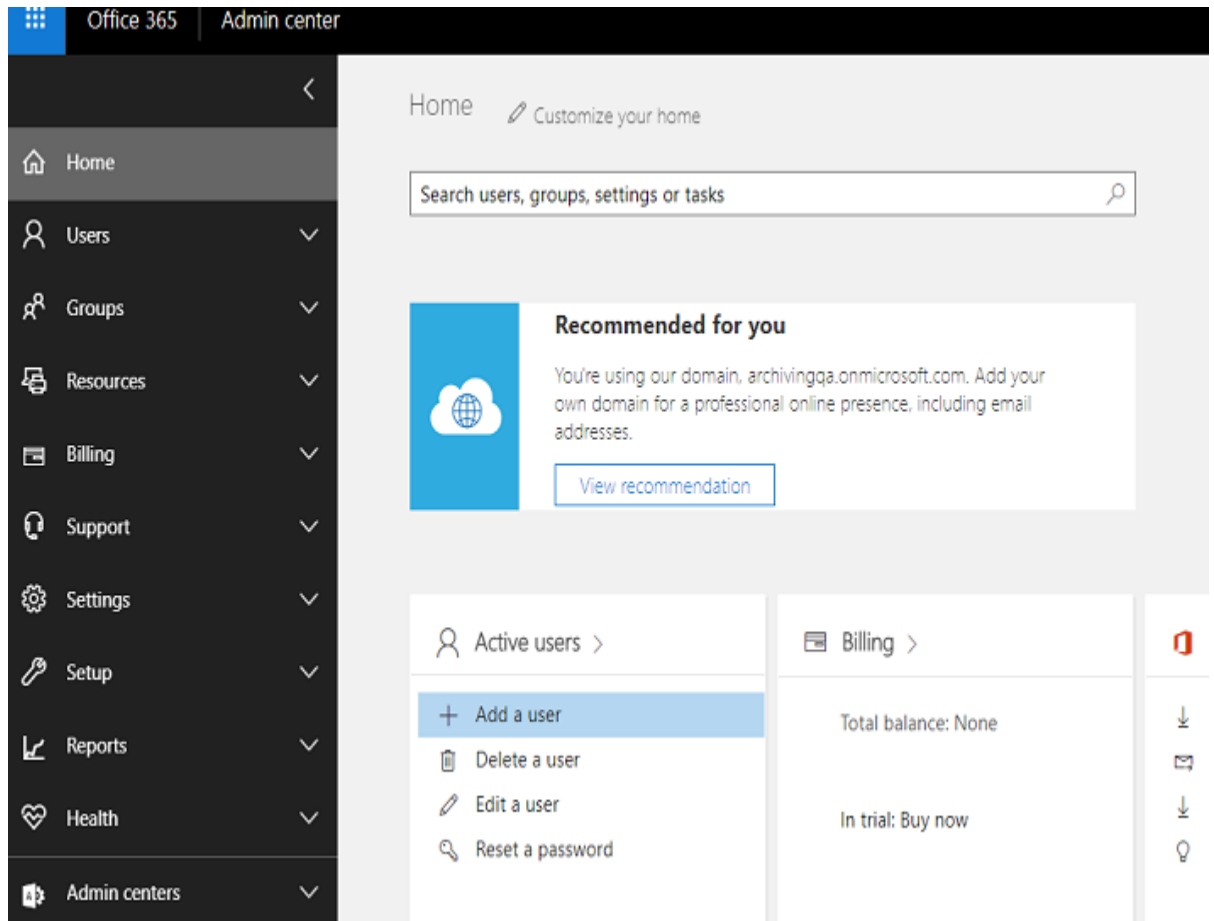
1. [Create a Non-deliverable Mailbox](#)
2. [Create a Send Connector for the Remote Domain](#)
3. [Add a Journaling Rule to direct Messages](#)

## Creating Mail Contact

Non-Delivery Report (NDR) mailbox helps you know about the message undelivered to the archive. The NDR is always a dedicated mailbox.

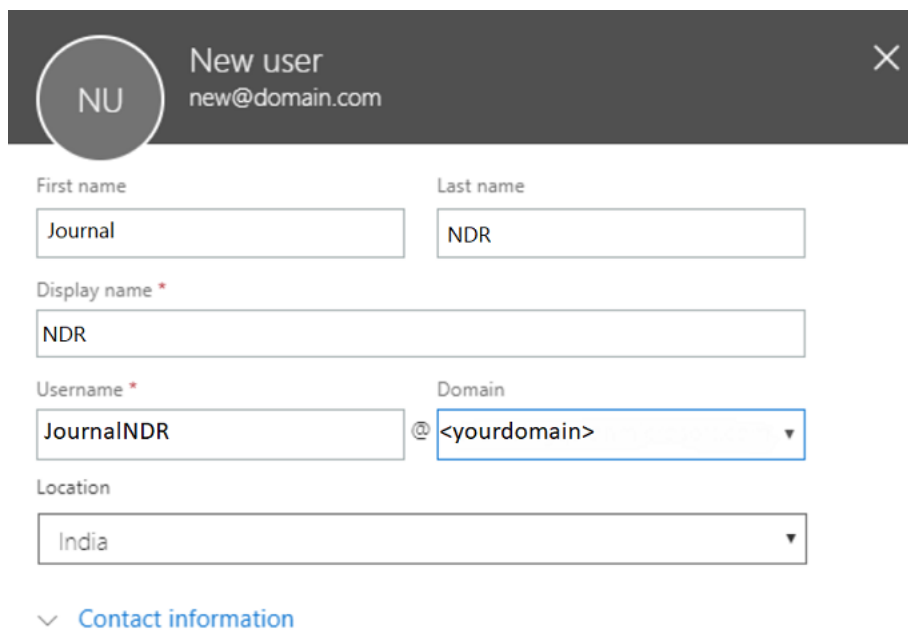
### Follow these steps:

1. From Home page of Admin Portal, click **Add a user**.



2. From Add a user, enter the following details and click **ADD**.

- **First name:** Journal
- **Last Name:** NDR
- **Display Name:** NDR
- **Username:** JournalNDR
- **Domain:** <yourdomain>



**New user** new@domain.com ×

First name: Journal

Last name: NDR

Display name \*: NDR

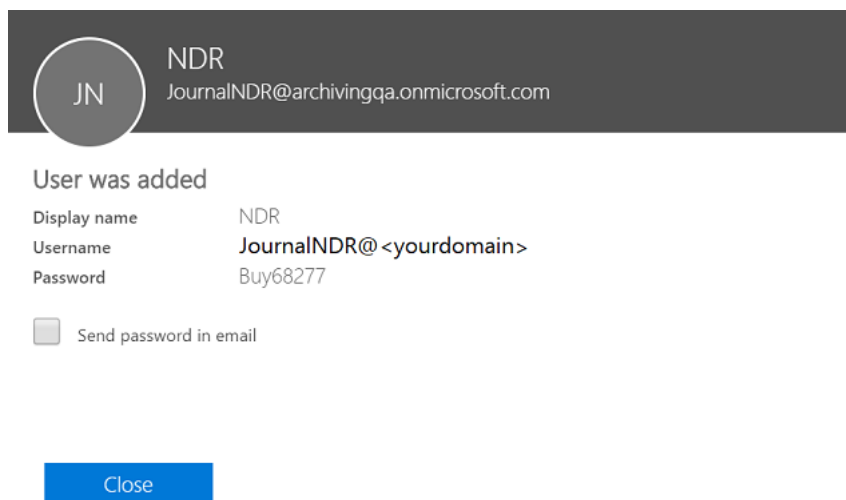
Username \*: JournalNDR

Domain: <yourdomain>

Location: India

[Contact information](#)

3. Close the Confirmation screen displays that user is added.



**User was added**

Display name: NDR

Username: JournalNDR@<yourdomain>

Password: Buy68277

☐ Send password in email

[Close](#)

4. From Exchange Admin Center, navigate to **recipients, mailboxes** and click the **Refresh** icon.

## Exchange admin center

The screenshot shows the Exchange Admin Center interface. On the left is a navigation pane with categories like recipients, permissions, compliance management, organization, protection, mail flow, mobile, public folders, unified messaging, servers, hybrid, and tools. The 'recipients' category is selected, and the 'mailboxes' sub-tab is active. Above the mailbox list are icons for adding, editing, deleting, and other actions. Below the icons is a table with three columns: DISPLAY NAME, MAILBOX TYPE, and EMAIL ADDRESS. One mailbox is listed: 'journal NDR' with type 'User' and email address 'journalNDR@ <your domain>'.

DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
journal NDR	User	journalNDR@ <your domain>

The added NDR mailbox is visible.

**Next Steps:**

1. [Create a Send Connector for the Remote Domain](#)
2. [Add a Journaling Rule to direct Messages](#)

## Create a Send Connector for the Remote Domain

Send Connector lets you route journaled mail sent from the Mail Contact to the UDP Archiving.

**To create new send connector, follow these steps:**

1. Navigate to **Mail Flow** and select connectors.
2. Click **+** to add a new connector.

The **Select your mail flow scenario** screen opens.

3. Select Office 365 from the **From:** drop-down list and your organizations email from the **To:** drop-down list, and click **Next**.

Select your mail flow scenario

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.  
[Learn more](#)

From:  
Office 365 ▼

To:  
Your organization's email server ▼

You need to create a connector for this mail flow scenario. Because your domain's MX record points to Office 365, you must set up an alternative server (called a smart host) so that Office 365 can send email to your organization's email server (also called on-premises server). To complete the scenario, you might need to configure your email server to accept messages delivered by Office 365. [Learn more about configuring your email server](#)

Next Cancel

The **New Connector** screen opens.

4. Enter information as provided below.



## New connector

This connector lets Office 365 deliver messages to your organization's email server.

\*Name:

Arcserve UDP Journal Send Connector

Description:

Send connector for Archiving emails to Arcserve UDP Archiving

What do you want to do after connector is saved?

☒ Turn it on

☒ Retain internal Exchange email headers (recommended)

Next

Cancel

- **Name:** Arcserve UDP Journal Send Connector
- **Description:** Send connector for Archiving emails to Arcserve UDP Archiving

5. Click **Next** to specify when to use this connection in the next screen.

New Connector - Google Chrome

Microsoft Corporation [US] | <https://outlook.office.com/ecp/Connectors/OutboundConnector.aspx?Conne>

New connector

When do you want to use this connector?

☐ Only when I have a transport rule set up that redirects messages to this connector

☐ For email messages sent to all accepted domains in your organization

☒ Only when email messages are sent to these domains

Use this connector only for email messages sent to domains listed below.

+ -

Back Next Cancel

6. Select *Only when emails are sent to this domain* option and click +.

The **add domain** dialog opens.

7. Enter the name of the created domain and click **OK**.

New Connector - Google Chrome

Secure | https://outlook.office365.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=OnPr...

### add domain

Specify the domain name, with or without wildcards.  
Example: \* or \*.contoso.com or \*.com

Specify the fully qualified domain name. Example: myhost.contoso.com

OK Cancel

You return to the New Connector screen.

8. Click **Next** to add host.

The **Add smart host** dialog opens.

9. Enter the details of the smart host and click **Save**.

You return to the New Connector screen.

Microsoft Corporation [US] | https://outlook.office.com/ecp/Connectors/OutboundConnector.aspx?Conne

### add smart host

Specify the smart host's fully qualified domain name (FQDN) or IPv4 address.  
Example: myhost.contoso.com or 192.168.3.2

Specify the fully qualified domain name or IPv4 address.

OK Cancel

**Note:** This host is the address of the UDP Archiving. Add the Fully Qualified Domain Name (FQDN) that you used during the [initial setup](#) of UDP Archiving. You can also use a static IP address if added.

**Example:** *myhost.contoso.com*

10. Click **Next** to specify how to connect to your email server.

The *How should Office 365 connect to your email server?* selection opens.

Microsoft Corporation [US] | <https://outlook.office.com/ecp/Connectors/OutboundConnector.aspx?Conne>

### New connector

How should Office 365 connect to your email server?

☒ Always use Transport Layer Security (TLS) to secure the connection (recommended)

Connect only if the recipient's email server certificate matches this criteria

☒ Any digital certificate, including self-signed certificates

☐ Issued by a trusted certificate authority (CA)

☐ And the subject name or subject alternative name (SAN) matches this domain name:

Example: contoso.com or \*.contoso.com

A digital certificate is an electronic 'passport' that allows your organization to exchange email securely. Just like a passport, a digital certificate provides identifying information, is forgery resistant, and can be verified because it was issued by an official, trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate authority (CA) so that a recipient can verify that the certificate is real.

Back Next Cancel

11. From *Always use Transport Layer Security (TLS) to secure the connection (recommended)* option, perform the following steps:
  - a. Select the checkbox of *Any digital certificate, including self-signed certificates*. By default the other one is selected.
  - b. Click **Next** to review the configuration.
12. After reviewing, click **Next**.

The **validate this connector** screen opens.

Microsoft Corporation [US] | <https://outlook.office.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=OnPremises#>

## New connector

Validate this connector

We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message.

Specify an email address for an active mailbox that's on your email server. You can add multiple addresses if your organization has more than one domain.

+ -

Specify the email address or addresses you want to use to validate this connector.

Back Validate Cancel

<https://outlook.office.com/ecp/Connectors/OutboundConnector.aspx?ConnectorType=OnPremises#>

13. Click +.

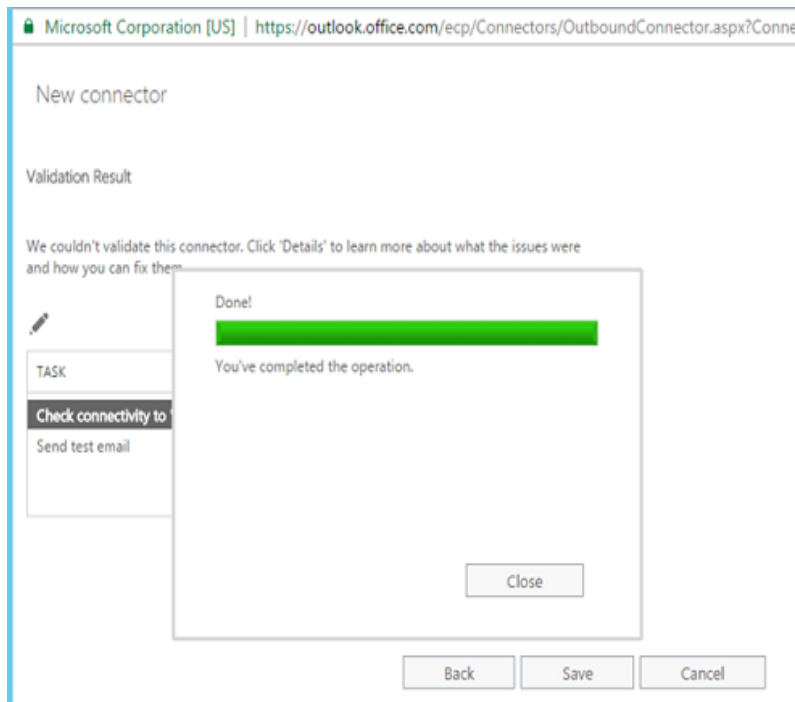
Add email dialog appears.

14. In the **add email** dialog, enter the email address and click **OK**

To validate, use the email address that you provided in [previous step](#).

The New Connector screen displays the added email address under Validation Result.

15. Click **validate**.



A successful validation test of email address and domain displays that the connector is configured properly and port 25 is open for UDP Archiving.

The send connector is created successfully.

**Next Step:**

[Add a Journaling Rule to direct Messages](#)

## Add a Journaling Rule to direct Messages

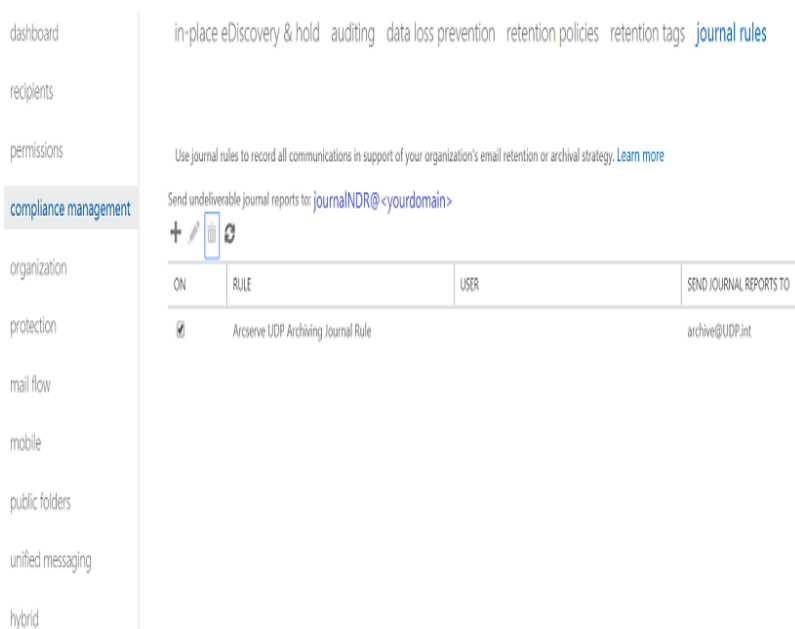
Journaling records inbound and outbound email communications to help organizations manage legal, regulatory, and organizational compliance requirements. From the journaling rule main page, you can enable or disable the journaling process. If there is a network outage and messages do not reach the archive, NDR mailbox (journalNDR@<your domain>) helps you knowing about the undelivered message.

To set up the journal rule, follow these steps:

1. Navigate to **compliance management** and select **journal rules**.

The **journal rules** screen opens.

Exchange admin center



2. Set your previously created [NDR mailbox](#) (journalNDR<your Domain>) to use in the area marked blue (send undelivered journal reports to).
3. Click **+** to add a new journal rule.

The **Journal Rule** screen opens.

4. Enter the required information, click **Save**.

new journal rule

Apply this rule...

\*Send journal reports to:  
archive@UDP.int

Name:  
Arcserve UDP Archiving Journal Rule

\*If the message is sent to or received from...  
[Apply to all messages]

\*Journal the following messages...  
All messages

Save Cancel

- **Send Journal Report to:** archive@UDP.int
- **Name:** Arcserve UDP Archiving Journal Rule
- **If messages sent or received from:** Apply to all messages or a selected Distribution Group.
- **Journal the following messages:** All messages or you can select a distribution group.

A Warning message appears.

5. Click **Yes** to apply the journal rule

All the settings are set and the mail starts flowing into the archive successfully.

## Setting up Access to UDP Archiving from Outlook Web Access

UDP Archiving allows access directly from Outlook Web Access (OWA) that is enabled on Microsoft Exchange Server 2010. You can launch UDP Archiving using any of the supported browsers. For more information, see [Compatibility Matrix](#).

### Follow these steps:

1. On the Microsoft Exchange Server 2010, navigate to the following path:  
*Exchange 2010 – C:\Program Files\Microsoft\Exchange Server-V14\ClientAccess\Owa\forms\Customization*
2. Copy the Arcserve logo (*arcserve.png*) to the Customization folder. You can download and extract the image [here](#).
3. Locate the *UIExtensions.xml.template* file and create a copy with the file name *UIExtensions.xml* in the Customization folder.
4. Open the *UIExtensions.xml* file in a text editor and locate the following entry:  
*MainNavigationBarEntry*
5. Add the following content below the entry *MainNavigationBarEntry*:

```
<MainNavigationBarExtensions>
<!--You can register your own entries to appear in Outlook Web Access navigation bar here-->
<MainNavigationBarEntry
  LargeIcon="arcserve.png"
  SmallIcon="arcserve.png"
  URL=" https://example.company.com " >
  <string language="en-us" text="UDP Archiving"/>
</MainNavigationBarEntry>
</MainNavigationBarExtensions>
```
6. Replace the URL value with your UDP Archiving URL including the protocol.
7. Restart Internet Information Service (IIS).  
**Note:** The users who already logged into OWA are disconnected while IIS is restarted.
8. After IIS is restarted, log into OWA.  
Arcserve icon is added at the end of the folders list.
9. Click Arcserve icon to open UDP Archiving in a web browser.  
You have successfully launched UDP Archiving from OWA.



## Configuring Microsoft Exchange 2007

For Microsoft Exchange, UDP Archiving ingests email using two methods. First, UDP Archiving ingests Exchange PST files into the archive. The PST files are created by the Exchange Server. Second, UDP Archiving is configured to receive journal email from Exchange Server via SMTP. Exchange journaling copies every email sent and received by a mailbox. Users configure journaling by mailbox and designate the UDP Archiving SMTP address as the destination. This process allows an organization to create a full set of both historical and future email records.

To configure the Microsoft Exchange 2007, you need to perform the following steps:

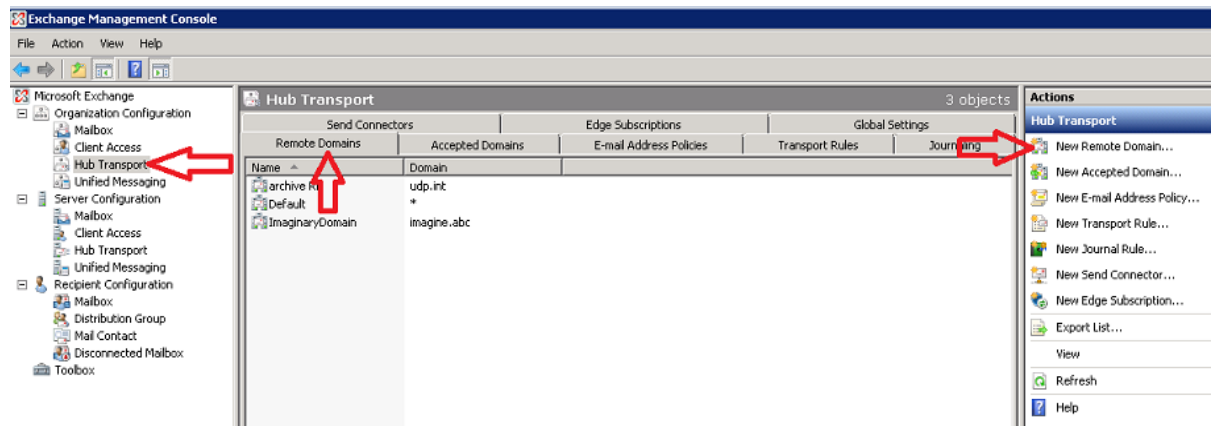
1. [Create a new remote domain](#): UDP.int
2. [Create a new mail contact](#): archive@UDP.int
3. [Create a Send Connector](#)
4. [Create a Journal Rule](#)

## Creating New Remote Domain

A remote domain is required to send the journaled messages to the mail server (SMTP). Use the same domain that you use for the mail contact.

**Follow these steps:**

1. From the **Exchange Management Console**, navigate to **Organization Configuration, Hub Transport, Remote Domains**, and click **New Remote Domain**.



The New Remote Domain wizard opens.

2. From the wizard, enter details in the **New Remote Domain** tab. For example:

**New Remote Domain**

☒ New Remote Domain  
☐ Completion

**New Remote Domain**  
When you create a remote domain, you can control mail flow with more precision, apply message formatting and messaging policies, and specify acceptable character sets for messages that are sent to and received from the remote domain. After you create a remote domain, you can specify more advanced security, policy, and permission configurations for messages that you exchange with the remote domain.

Name:  
Arcserve UDP Archiving Domain

Domain name:  
UDP.int

☐ Include all subdomains

Help < Back New Cancel

- **Name:** Arcserve UDP Archiving Domain
  - **Remote domain:** UDP.int
3. Click **New**.
  4. Click **Finish**.

New remote domain is successfully created.

#### Next Steps:

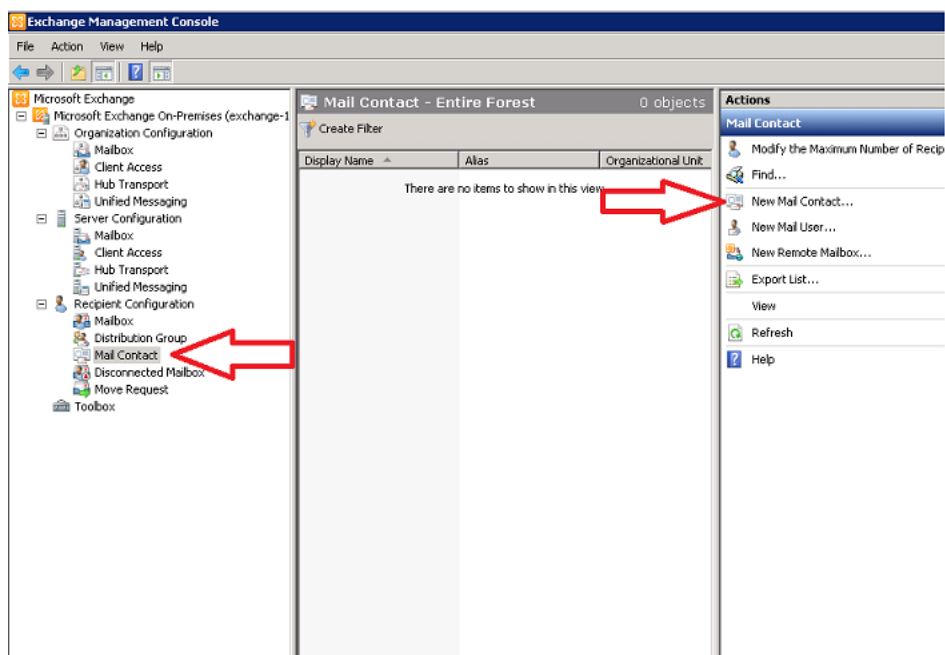
1. [Create a new mail contact](#)
2. [Create a Send Connector](#)
3. [Create a Journal Rule](#)

## Creating Mail Contact

The mail contact is the external email address of the mailbox that receives the journal report first. Use the same domain that you used to [create a new remote domain](#).

**Follow these steps:**

1. From **Exchange Management** Console, navigate to Recipient Configuration, and click **Mail Contact**.
2. Click **New Mail Contact**.



The new mail contact wizard opens.

3. From the **Introduction** tab of the wizard, select **New contact**, and click **Next**.

The Contact Information screen opens.

The screenshot shows the 'New Mail Contact' wizard with the 'Contact Information' tab selected. The left sidebar shows the progression: Introduction (completed), Contact Information (current), New Mail Contact, and Completion. The main area contains the following fields:

- Organizational unit:** exch07.com/Users (with a 'Browse...' button)
- First name:** UDP
- Initials:** (empty)
- Last name:** Journaling
- Name:** UDP Journaling
- Alias:** UDPJournaling
- External e-mail address:** (empty, with an 'Edit...' button)

At the bottom are buttons for 'Help', '< Back', 'Next >', and 'Cancel'.

4. Enter details in the **Contact Information** tab and click **Edit** for **External e-mail address**:

For example:

- **First name:** UDP
  - **Last Name:** Journaling
  - **Name:** UDP Journaling
  - **Alias:** UDPJournaling
5. For SMTP Address, enter archive@UDP.int as the external E-mail address and click **OK**.

The screenshot shows the 'SMTP Address' dialog box with the following fields:

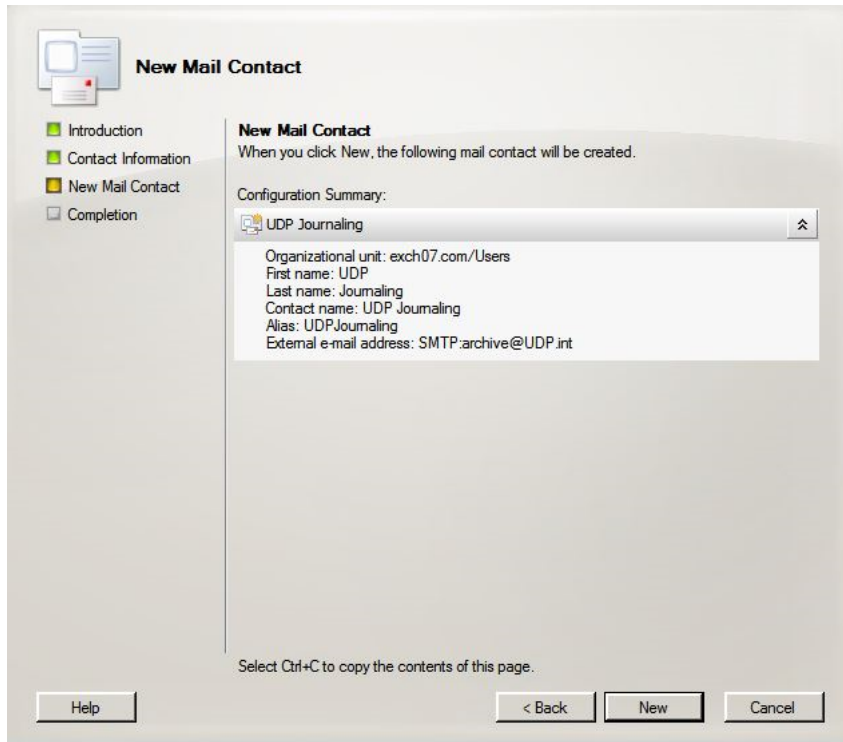
- E-mail address:** archive@UDP.int
- E-mail type:** SMTP

At the bottom are 'OK' and 'Cancel' buttons.

The email address is displayed in the Contact Information tab.

6. Click **Next**

The New Mail Contact tab displays the summary.



7. Review the summary and click **New**.
8. From the Completion tab, click **Finish**.

The wizard is closed and the created mail contact is displayed.

#### Next Steps:

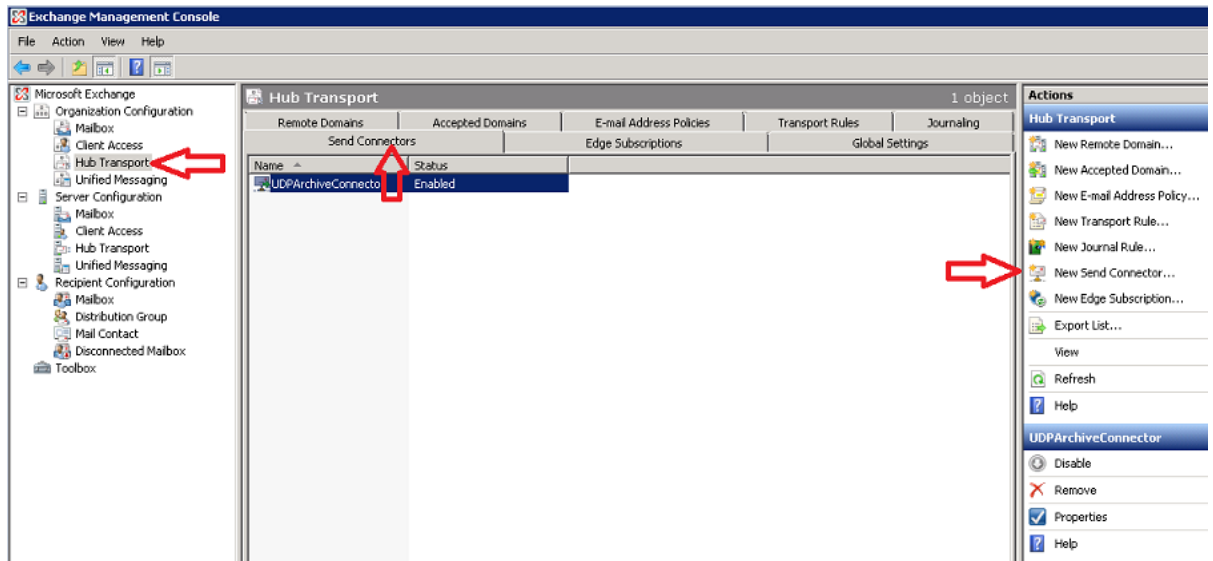
1. [Create a Send Connector](#)
2. [Create a Journal Rule](#)

## Creating Send Connector

The connector sends the journal report to the mail server (SMTP).

To create new send connector, follow these steps:

1. Navigate to Organization Configuration, Hub Transport, Send Connectors and click **New Send Connector**.



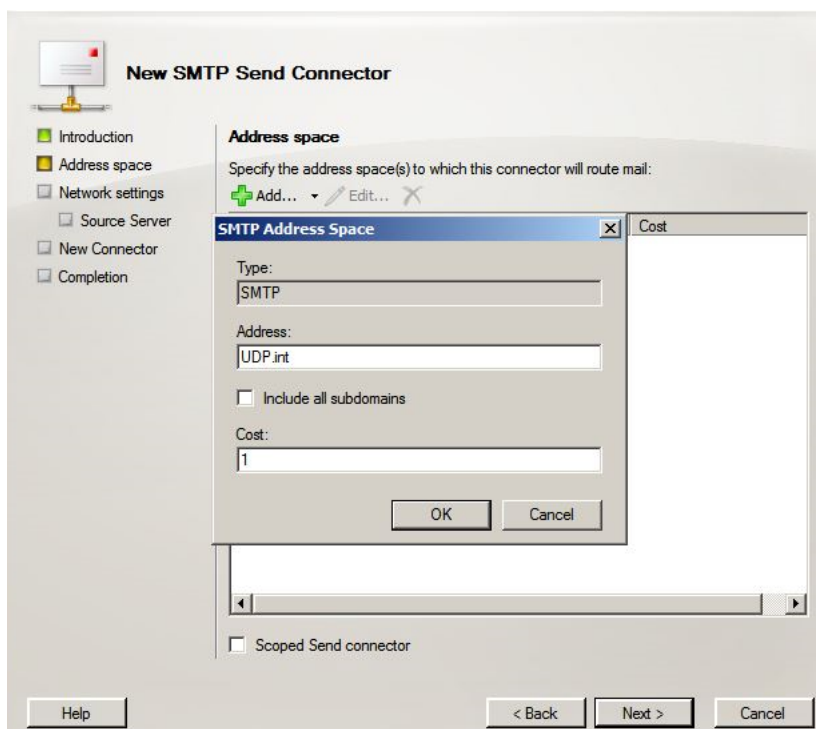
The **New SMTP Send Connector** wizard is displayed.

2. In the Introduction tab, perform the following steps and click **Next**.
  - Enter the name of connector. For example: UDP Journal Send Connector.
  - Select **Custom** as the **intended use for this Send connector**.



The **Address space** tab is displayed.

3. From the Address Space tab, perform the following steps and click **Next**.



- a. Click the **Add** button to specify the Address space.

The SMTP Address Space dialog is displayed.

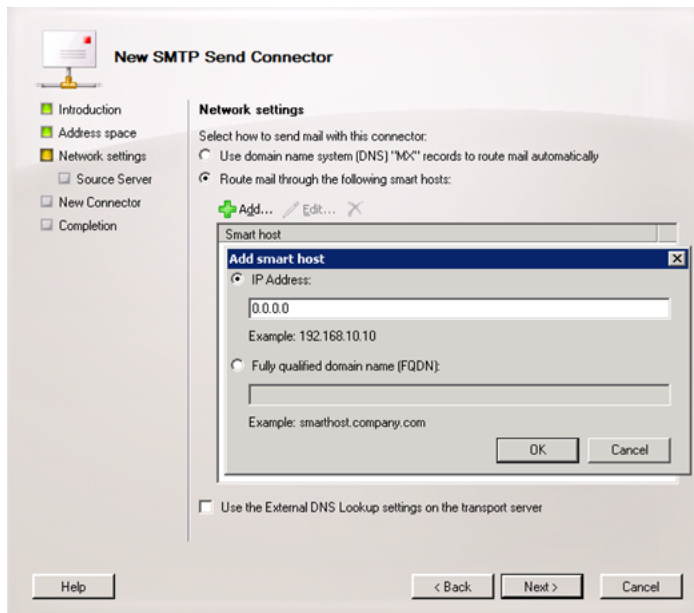


- b. Enter the remote domain name in the **Address** field. For example, UDP.int.
- c. Click **OK**.

The SMTP Address Space dialog is closed.

The Network settings tab is displayed.

4. For Network Settings, perform the following steps, and click **Next**:



- a. Click **Add** for the option **Route mail through the following smart hosts**.

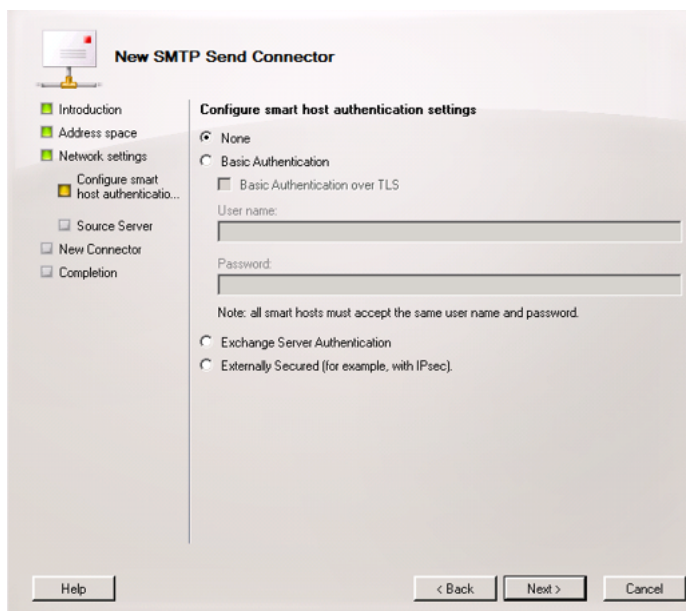
The Add Smart Host dialog is displayed.

- b. Enter the IP address or FQDN of the UDP Archiving server.
- c. Click **OK**.

The Add Smart Host dialog is closed.

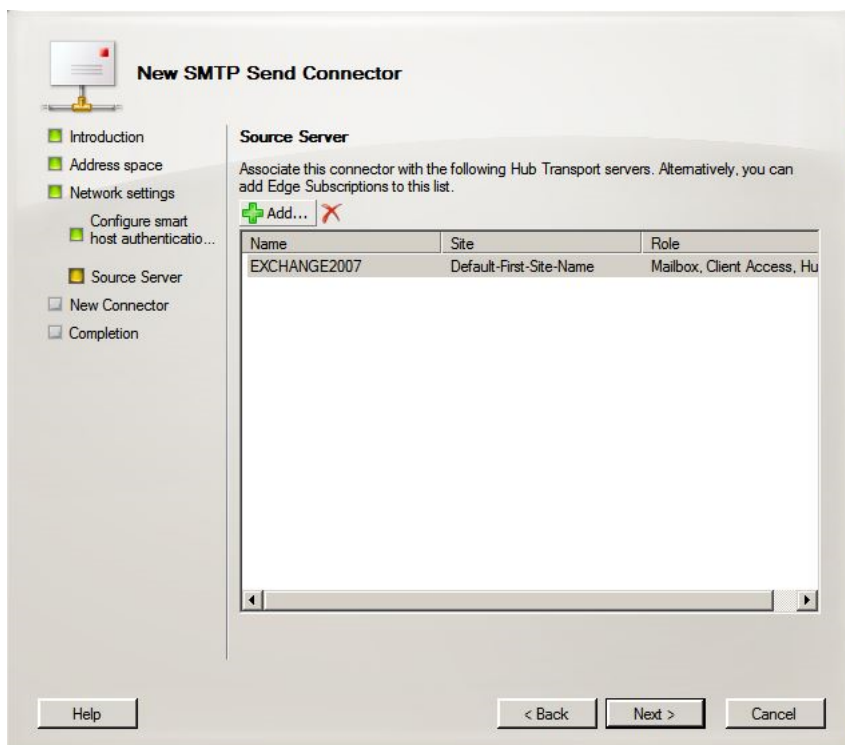
The Configure smart host authentication settings tab is displayed.

5. Select **None** and click **Next**.

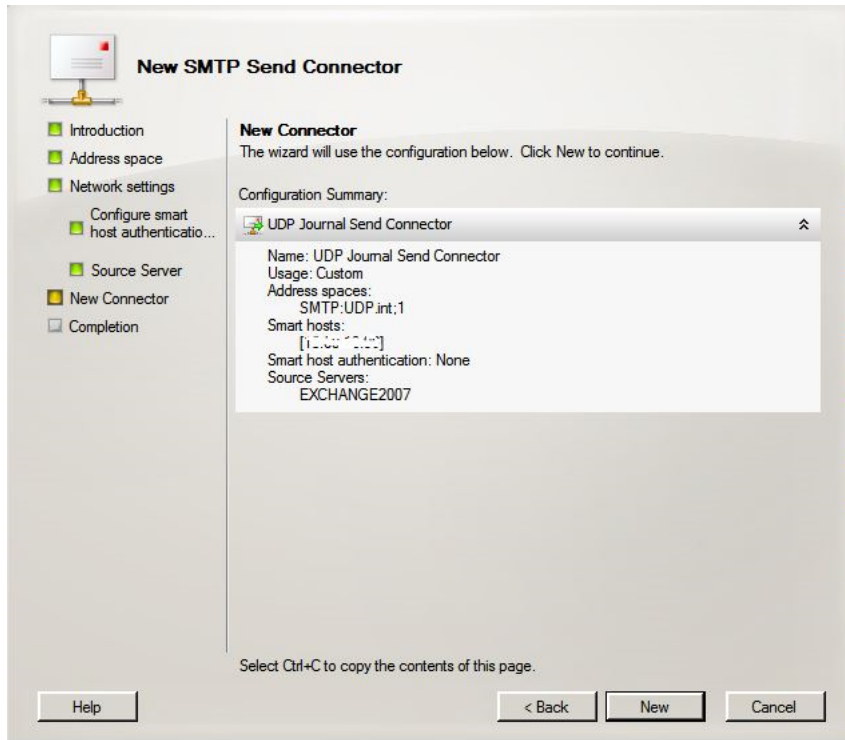


The **Source Server** dialog is displayed.

6. Select the source server and click **Next**.



7. From the New Connector tab, click **New**.



The send connector is created successfully.

**Next Step:**

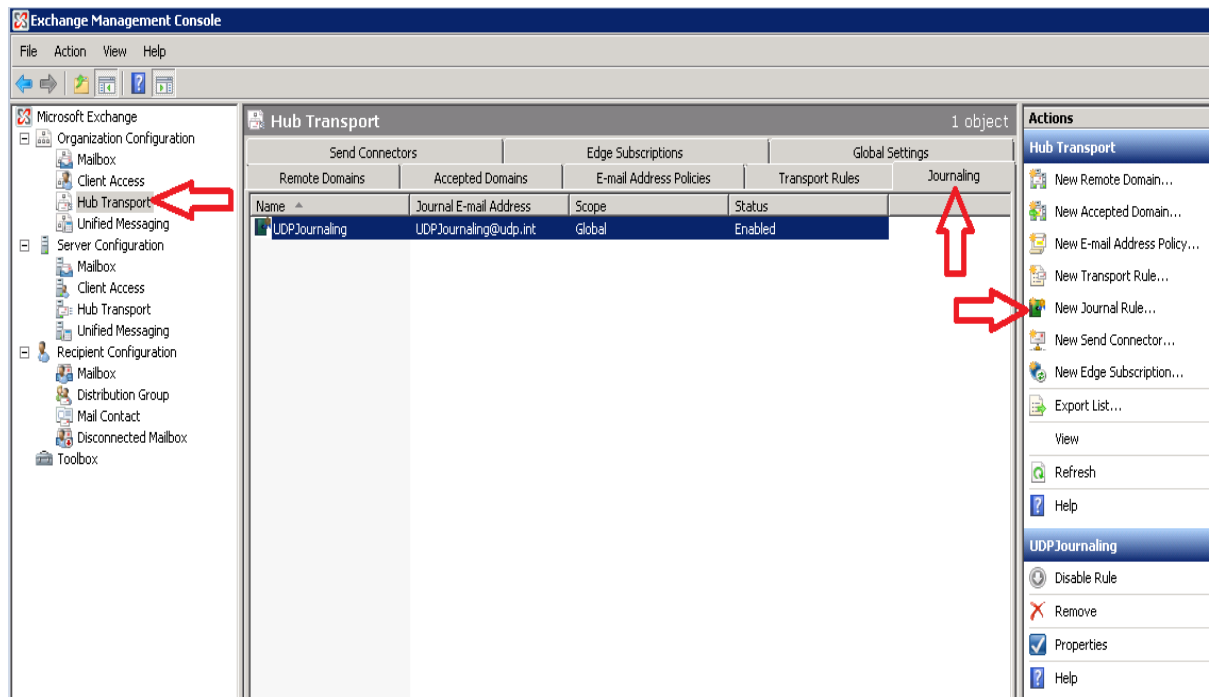
[Create a Journal Rule](#)

## Setting up the Journal Rule

Journaling records inbound and outbound email communications to help organizations manage legal, regulatory, and organizational compliance requirements.

To set up the journal rule, follow these steps:

1. Navigate to **Organization Configuration, Hub Transport, Journaling**.

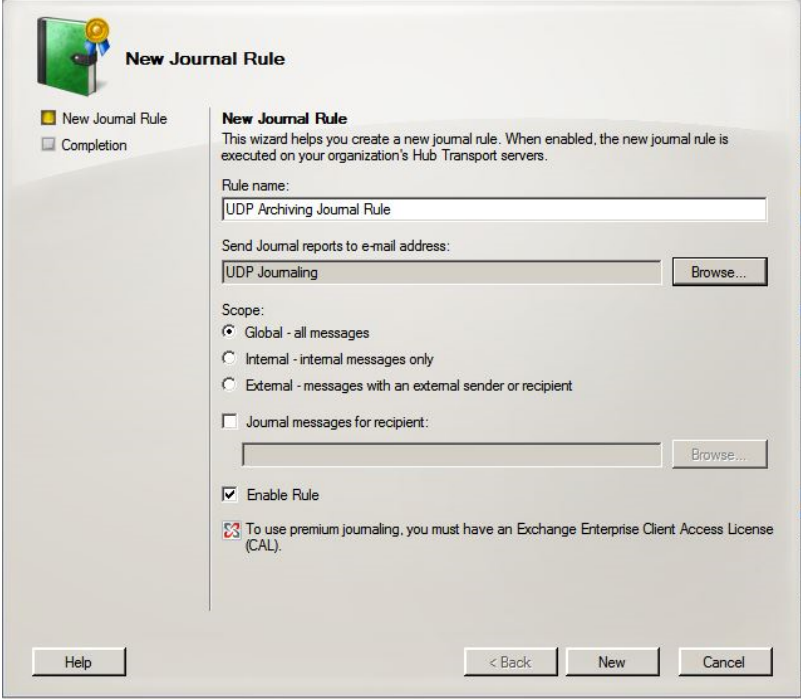


2. Under Actions, click **New Journal Rule**.

New Journal wizard is displayed.

3. From the Wizard in the **New Journal Rule** tab, perform the following steps and click **New**.
  - a. Enter the rule name. For example: UDP Archiving Journal Rule.
  - b. For **Send Journal reports to e-mail address**, click **Browse** to select the

mail contact that you [created](#) before.



The screenshot shows the 'New Journal Rule' wizard in Microsoft Exchange 2007. The wizard is titled 'New Journal Rule' and has a progress bar at the top. The first step, 'New Journal Rule', is selected, and the second step, 'Completion', is also visible. The main content area contains the following fields and options:

- Rule name:** A text box containing 'UDP Archiving Journal Rule'.
- Send Journal reports to e-mail address:** A text box containing 'UDP Journaling' and a 'Browse...' button.
- Scope:** Three radio button options: 'Global - all messages' (selected), 'Internal - internal messages only', and 'External - messages with an external sender or recipient'.
- Journal messages for recipient:** A checkbox that is unchecked, with a text box and a 'Browse...' button below it.
- Enable Rule:** A checkbox that is checked.
- License:** A red 'X' icon and a note: 'To use premium journaling, you must have an Exchange Enterprise Client Access License (CAL)'.

At the bottom of the wizard, there are three buttons: 'Help', '< Back', and 'New', and a 'Cancel' button on the right.

All the settings are set and the mail starts flowing successfully.

## Configuring Microsoft Exchange 2010

For Microsoft Exchange, UDP Archiving ingests email using two methods. First, UDP Archiving ingests Exchange PST files into the archive. The PST files are created by the Exchange Server. Second, UDP Archiving is configured to receive journal email from Exchange Server via SMTP. Exchange journaling copies every email sent and received by a mailbox. Users configure journaling by mailbox and designate the UDP Archiving SMTP address as the destination. This process allows an organization to create a full set of both historical and future email records.

To configure the Microsoft Exchange 2010, you need to perform the following steps:

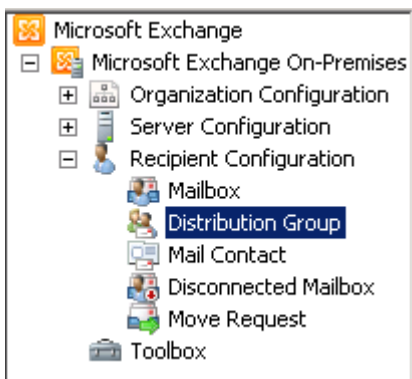
1. [\(Optional\) Create a new Distribution Group to archive selective users](#)
2. [Create a Non-routable New Remote Domain](#)
3. [Create a Fake Mail Contact using New Domain](#)
4. [Create a Non-deliverable Mailbox](#)
5. [Create Send Connector](#)
6. [Create the Journaling rule](#)

## (Optional) Create new Distribution Group to Archive Selective Users

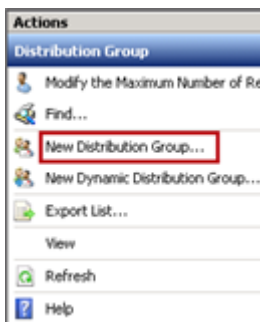
**Note:** Skip creating new distribution group if you intend to set archiving for all users in your exchange organization.

To create new distribution group for some users, you need to follow these steps:

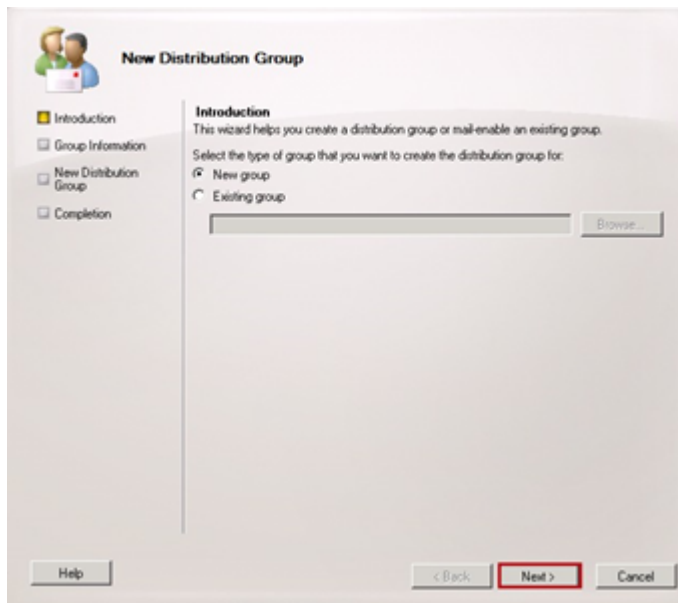
1. From the **Exchange Management Console**, navigate to **Distribution Group** from the **Recipient Configuration** drop-down list.



2. Select **New Distribution Group** from the **Actions** menu available on the right.

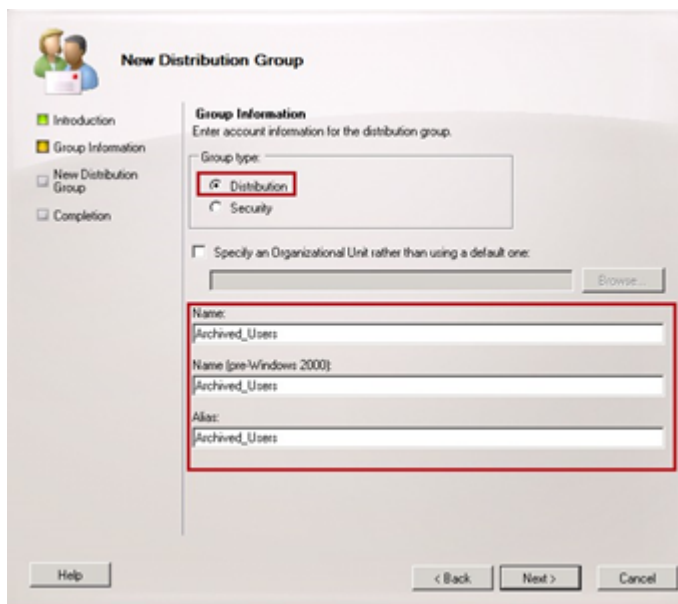


The **New Distribution Group** dialog opens.



3. Click **Next**.

The **Group Information** dialog appears.



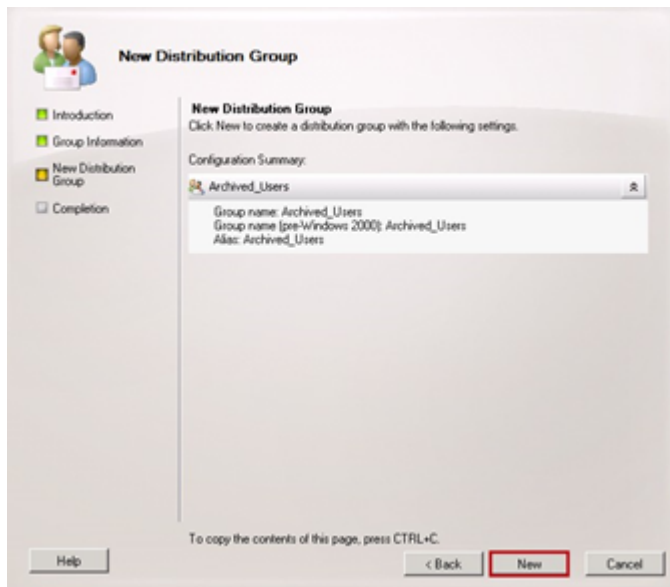
4. Select the Group type as required and fill the following fields:

- Name
- Name (pre-Windows 2000)
- Alias

5. Click **Next**.

The **New Distribution Group** dialog appears.





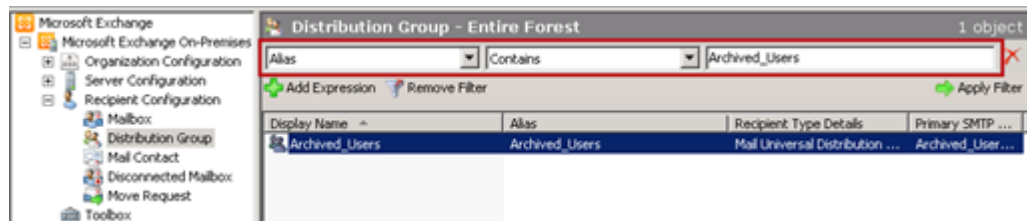
6. Click **New**.

The **Distribution Group** screen appears.

You can find the Distribution Group using the following steps:

- a. Navigate to **Distribution Group** from the **Recipient Configuration** drop-down list.

**Note:** Use **Apply Filter** to find newly created group.



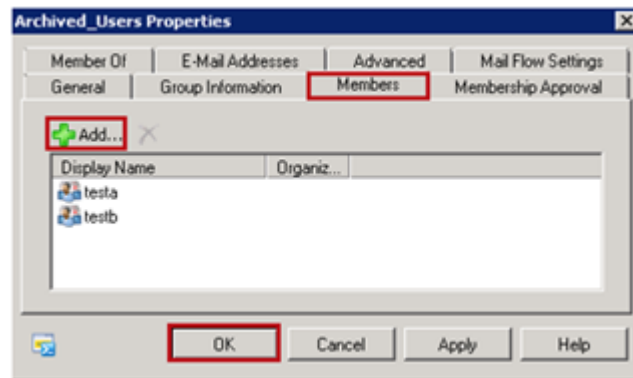
- b. Now, double click on the distribution group.

The distribution group properties screen appears.



- c. Navigate to **Members** tab.
  - i. Find the Member(s) you wish to add to be a part of Archiving journaling rule.

- ii. Click **Add** and Repeat for additional members.



- d. Click **OK** after listing your member(s).

The new Distribution Group to Archive Selective Users is created successfully.

**Next Steps:**

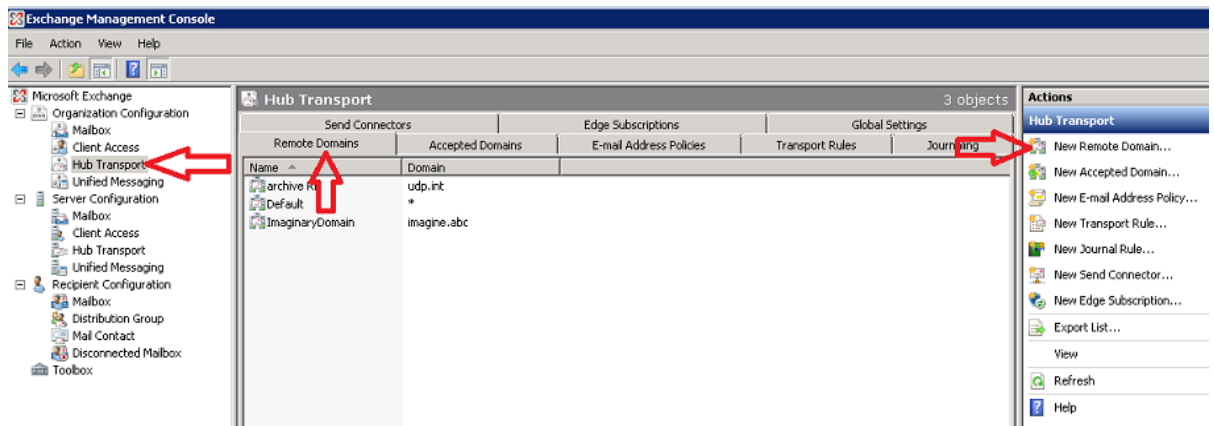
1. [Creating the Journaling rule](#)
2. [Creating Send Connector](#)

## Create a Non-routable New Remote Domain

A remote domain is required to send the journaled messages to the mail server (SMTP). Use the same domain that you use for the mail contact.

**Follow these steps:**

1. From the **Exchange Management Console**, navigate to **Organization Configuration, Hub Transport, Remote Domains**, and click **New Remote Domain**.



The New Remote Domain dialog opens.

2. From New Remote Domain, enter the following details:

**New Remote Domain**

☒ New Remote Domain  
☐ Completion

**New Remote Domain**  
When you create a remote domain, you can control mail flow with more precision, apply message formatting and messaging policies, and specify acceptable character sets for messages that are sent to and received from the remote domain. After you create a remote domain, you can specify more advanced security, policy, and permission configurations for messages that you exchange with the remote domain.

Name:  
Arcserve UDP Archiving Domain

Domain name:  
UDP.int

☐ Include all subdomains

Help < Back New Cancel

- **Name:** Arcserve UDP Archiving Domain
- **Domain name:** UDP.int

3. Click **New**.

New remote domain is successfully created.

#### Next Steps:

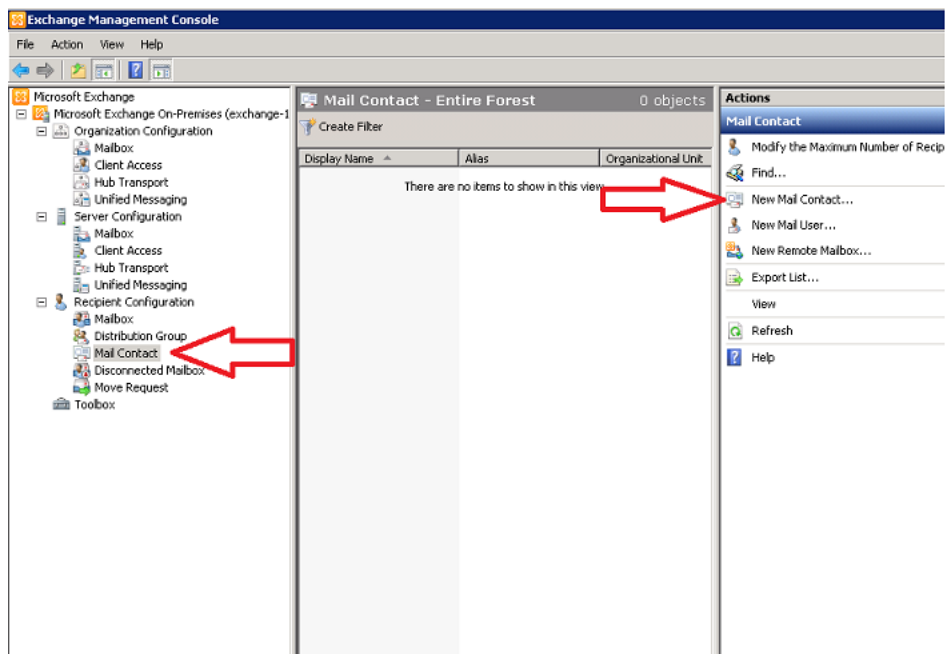
1. [Create a Mail Contact using New Domain](#)
2. [Create a Non-deliverable Mailbox](#)
3. [Create Send Connector](#)
4. [Create the Journaling rule](#)

## Create a Mail Contact using New Domain

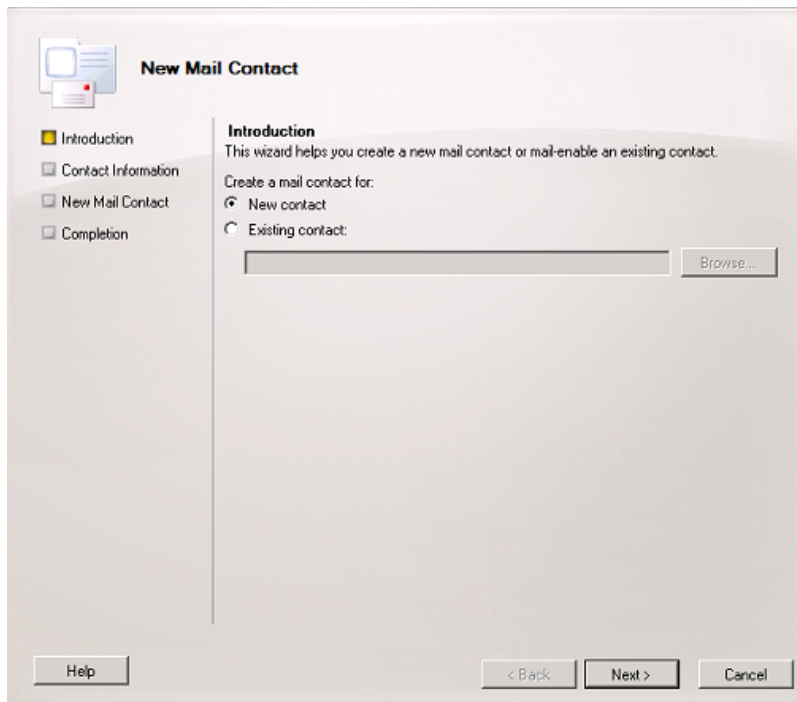
The Mail Contact is the account that acts as a *holding location* for journaled messages. The email address associated with this account is the designated recipient and must be associated with a non-existent, non-routable Domain Name created in [previous step](#).

**Follow these steps:**

1. From **Exchange Management Console**, navigate to Recipient Configuration, and click **Mail Contact**.
2. Click **New Mail Contact**.

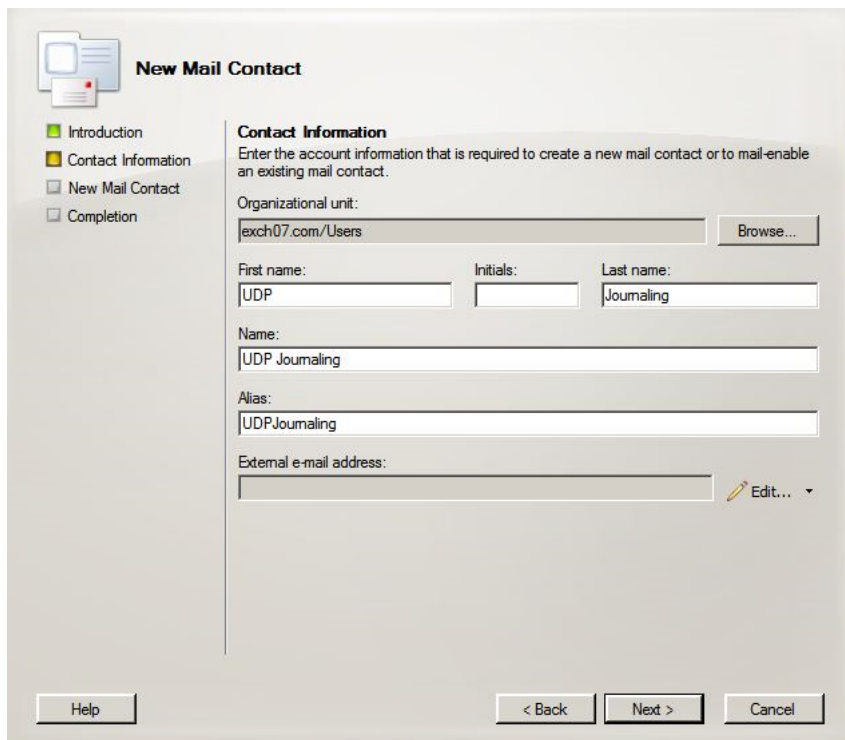


The New Mail Contact wizard is displayed.



- From the Introduction tab of New Mail Contact dialog, verify if the option for **New contact** is selected, and click **Next**.

The Contact Information screen opens.



- Enter required details and click **Edit** placed for **External e-mail address**. For example,

- **First name:** Arcserve
- **Initials:** UDP
- **Last Name:** Archiving
- **Name:** Arcserve UDP Archiving
- **Display Name:** UDP Journaling

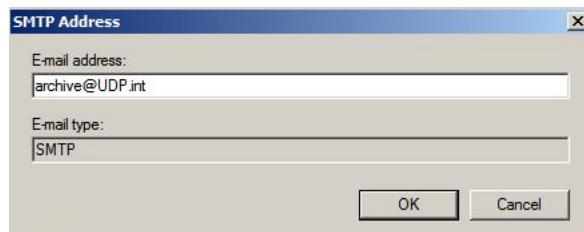
5. Perform the following steps to enter external e-mail address:

- a. Click **Edit**

SMTP Address dialog is displayed.

- b. Enter the e-mail address archive@udp.int for E-mail address

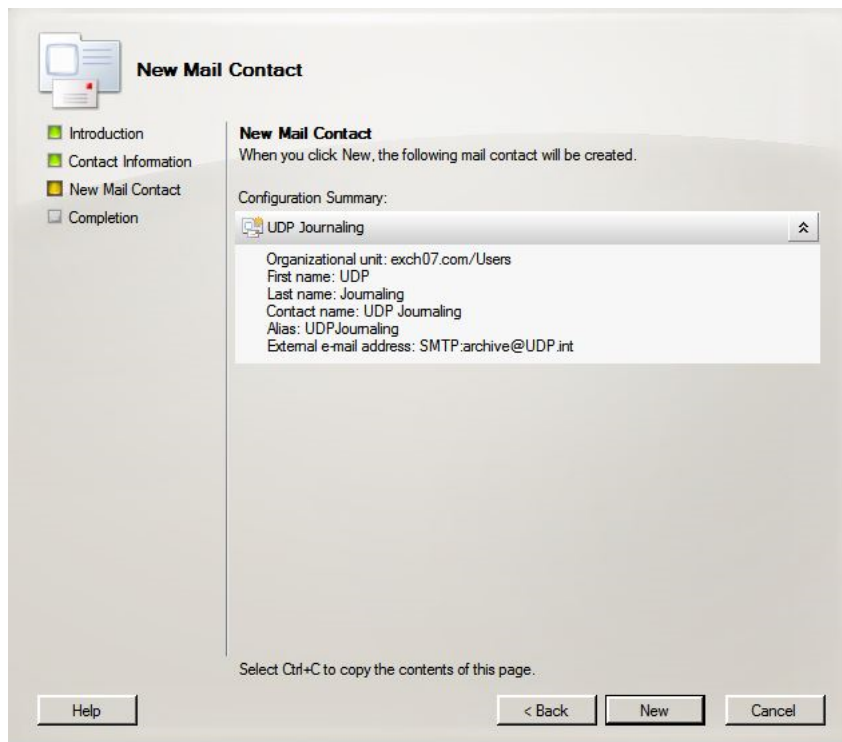
- c. Click **OK**.



The Contact Information pane displays the email address.

6. Click **Next**

The screen displays the configuration summary of new contact.



7. Click **New**.

The mail contact is successfully created.

#### Next Steps:

1. [Create a Non-deliverable Mailbox](#)
2. [Create Send Connector](#)
3. [Create the Journaling rule](#)

## Create a Non-deliverable Mailbox

Non-Delivery Report (NDR) mailbox helps you know about the messages that are not delivered to the UDP Archiving. Generally, the NDR is always a dedicated mailbox.

#### Follow these steps:

1. From ExchangeAdmin center, navigate to **Recipient Configuration, Mailbox**, and then click **New Mailbox** from the Actions pane.  
The New Mailbox window opens.
2. Select **User Mailbox** option and click **Next**.
3. Select **New user** as **User Type** and click **Next**.
4. Enter **User Information** details as desired and click **Next**.

For example:

- **First name:** Journal
- **Last Name:** NDR
- **User logon name:** JournalNDR

The Mailbox Settings screen appears.

5. Keep the default values and click **Next**.

The Archive Settings screen appears.

6. Keep the default values and click **Next**.

Configuration Summary screen appears.

7. Review the Configuration Summary and click **New**.

The NDR Mail Box is successfully created.

#### Next Steps:



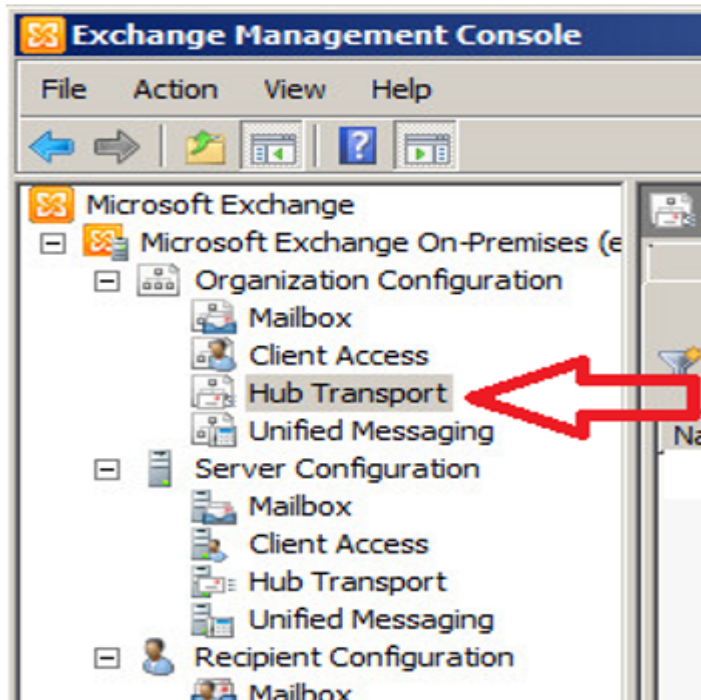
1. [Create a Send Connector for the Remote Domain](#)
2. [Add a Journaling Rule to direct Messages](#)

## Create Send Connector

The connector sends the journal report to the mail server (SMTP).

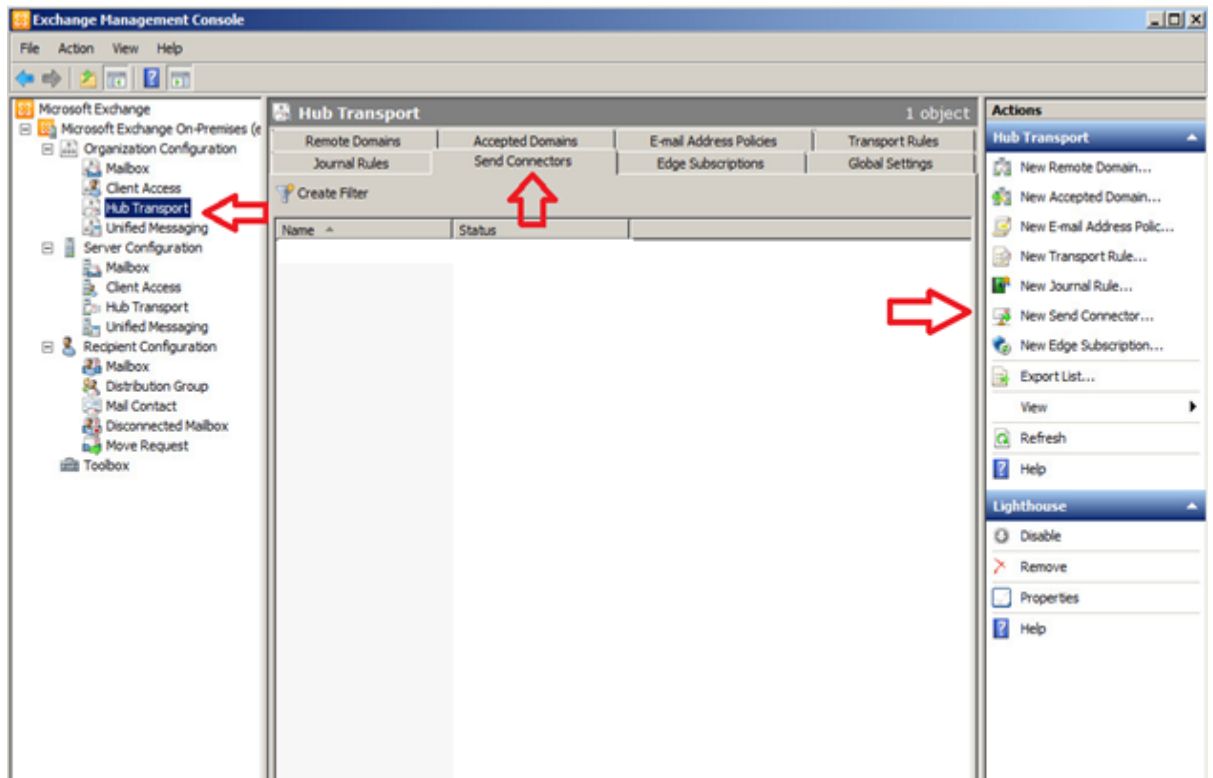
To create Send Connector, follow these steps:

1. From the **Exchange Management Console**, navigate to **Organization Configuration** drop-down list and select **Hub Transport**.



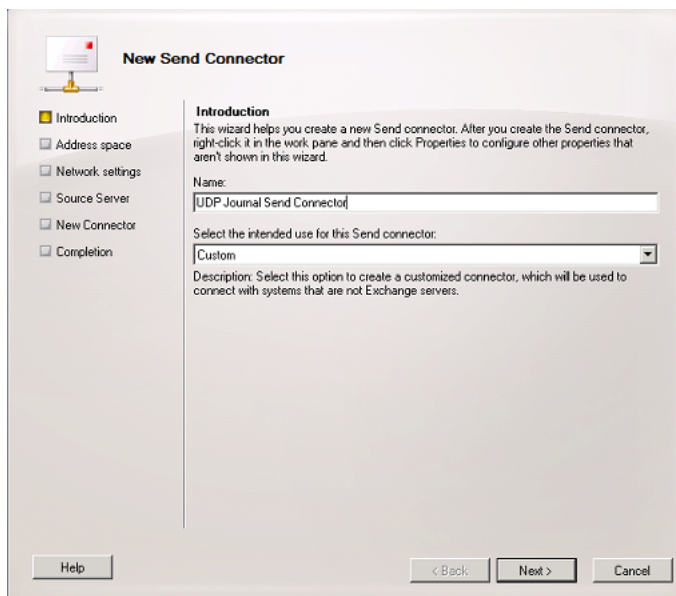
The **Hub Transport** screen opens.

2. Select the **Send Connectors** tab from the **Hub Transport** screen.



3. Select **New Send Connector** from the **Actions** menu.

The **New Send Connector** Wizard is displayed.

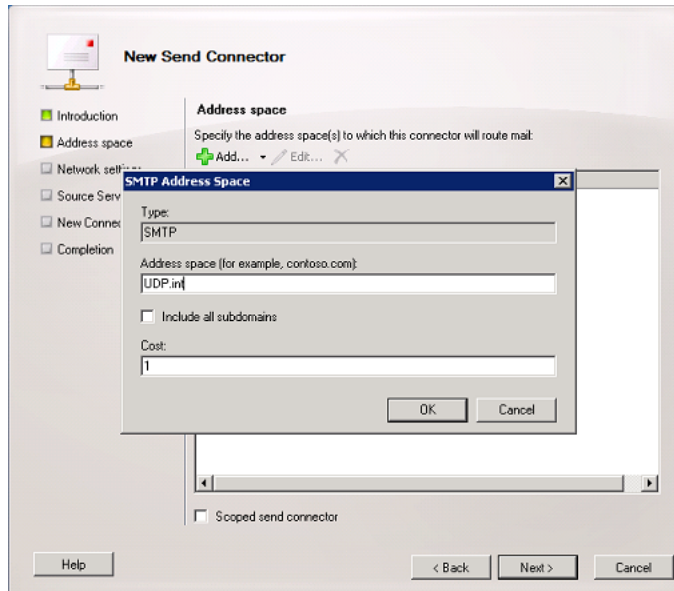


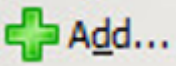
4. In the **Introduction** tab, enter a name for the New Send Connector.

For example: UDP Journal Send Connector

5. Select **Custom** for *Select the intended use for this Send connector* and click **Next**.

The **Address Space** tab is displayed.



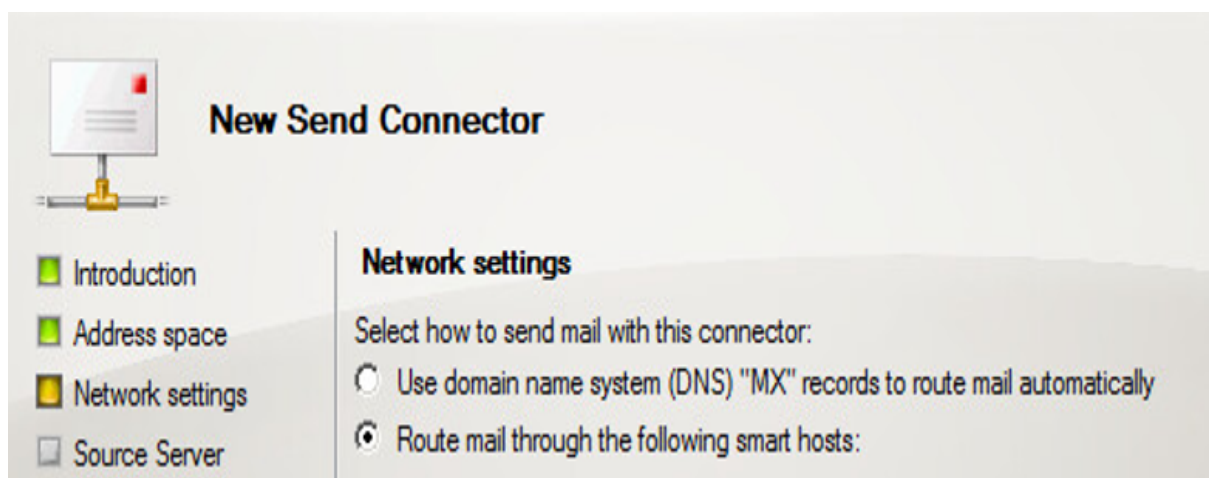
6. Click  to provide the address space for this send connector.
7. Enter the created remote domain in the Address Space and click **OK**.

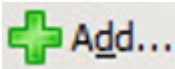
For example: UDP.int

The SMTP address space is added.

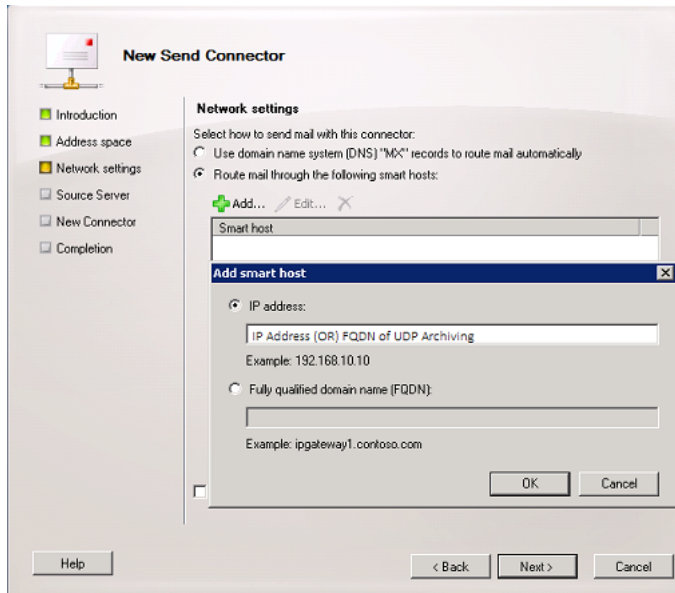
8. Click **Next**.

The **Network settings** screen opens.



9. From the Network settings, select the **Route mail through the following smart hosts:** option and click .

The **Add smart host** screen opens.

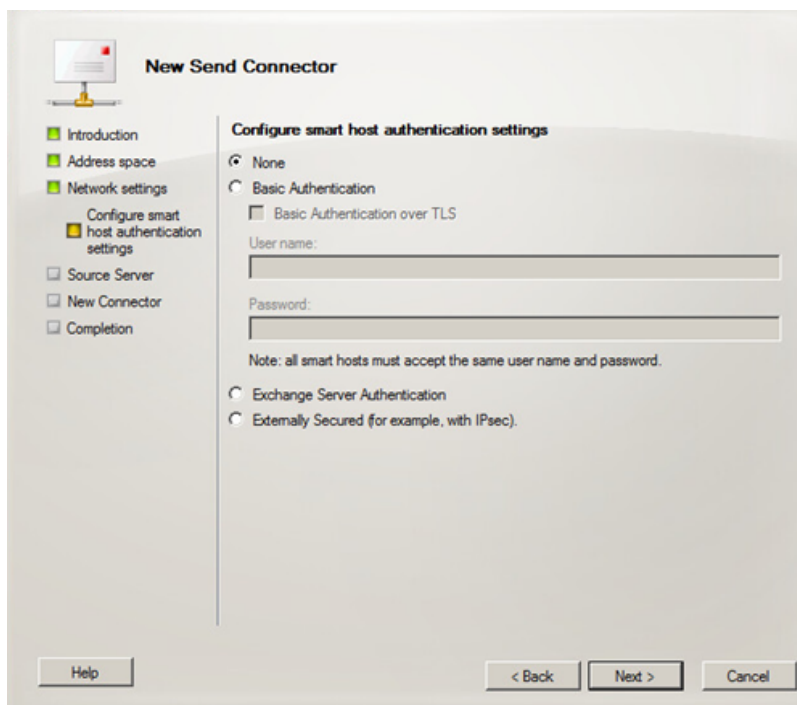


10. Enter either the IP address or the FQDN of the UDP Archiving host machine and click **OK**.

The address is added in the Network setting pane.

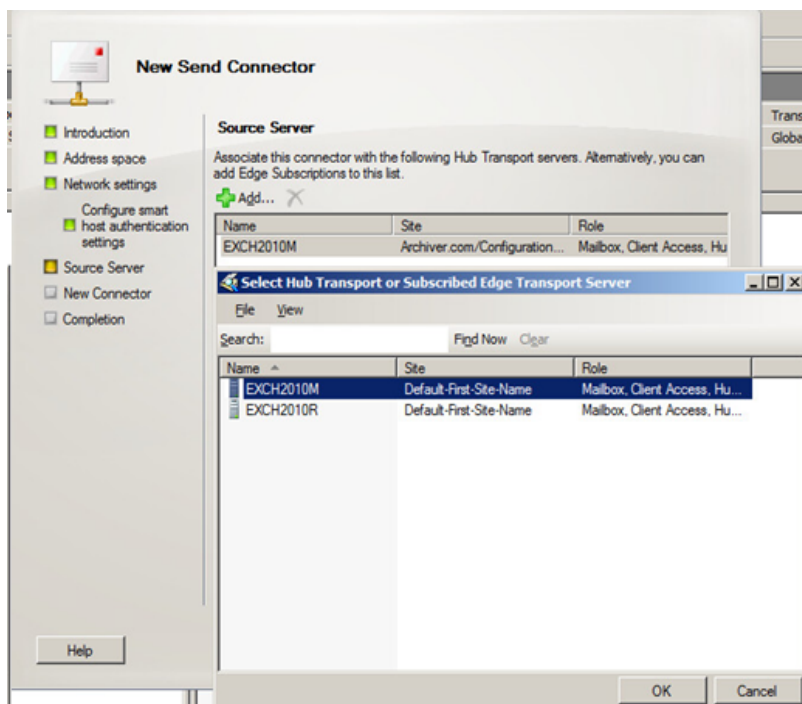
11. Click **Next**.

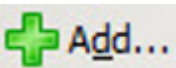
Network setting tab expands and the **Configure smart host authentication settings** pane appears.



12. Enable the authentication if required and click **Next**.

The **Source Server** screen opens.

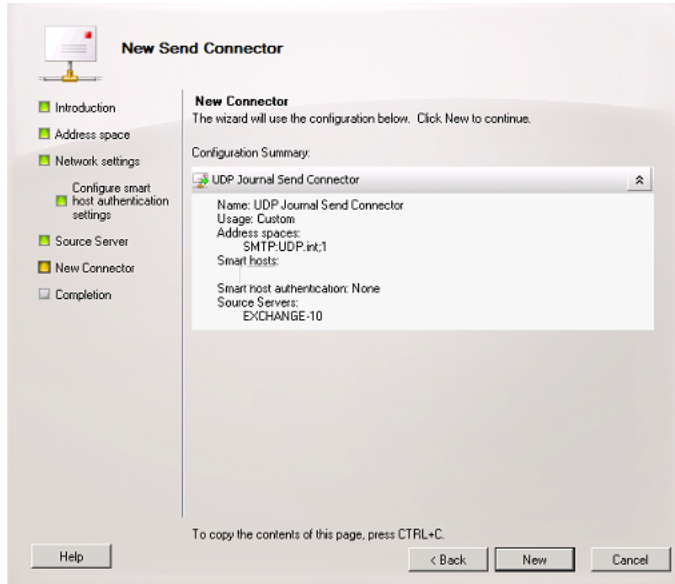


13. Click  to add the Exchange 2010 server used for routing mail to UDP Archiving and click **OK**.

The server is added to the Source server tab.

14. Click **Next**.

The **New Connector** screen displays the summary.



15. Review details and click **New** to create the send connector.

You have created Send Connector successfully and the Completion tab is displayed.

16. Click **Finish** on the Completion tab.

### Next Step:

#### [Create the Journaling rule](#)

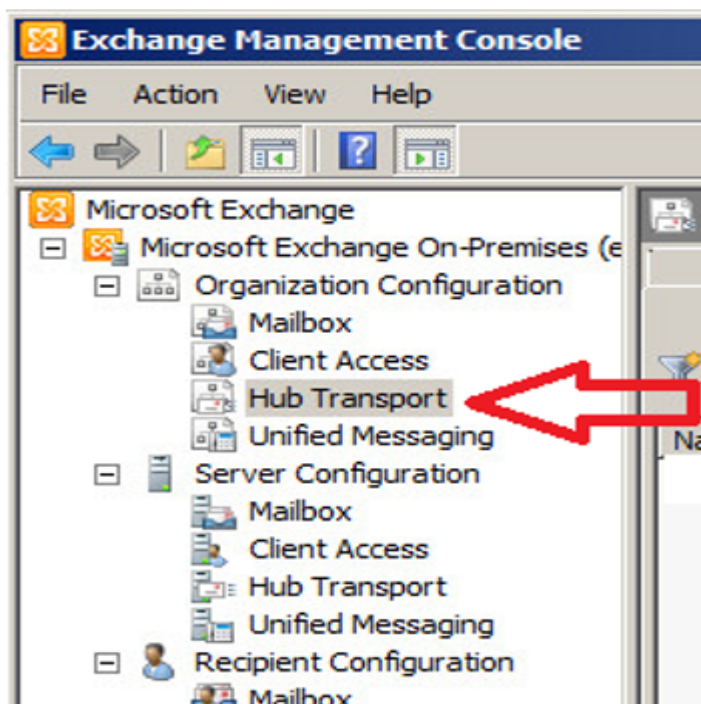


## Create the Journaling rule

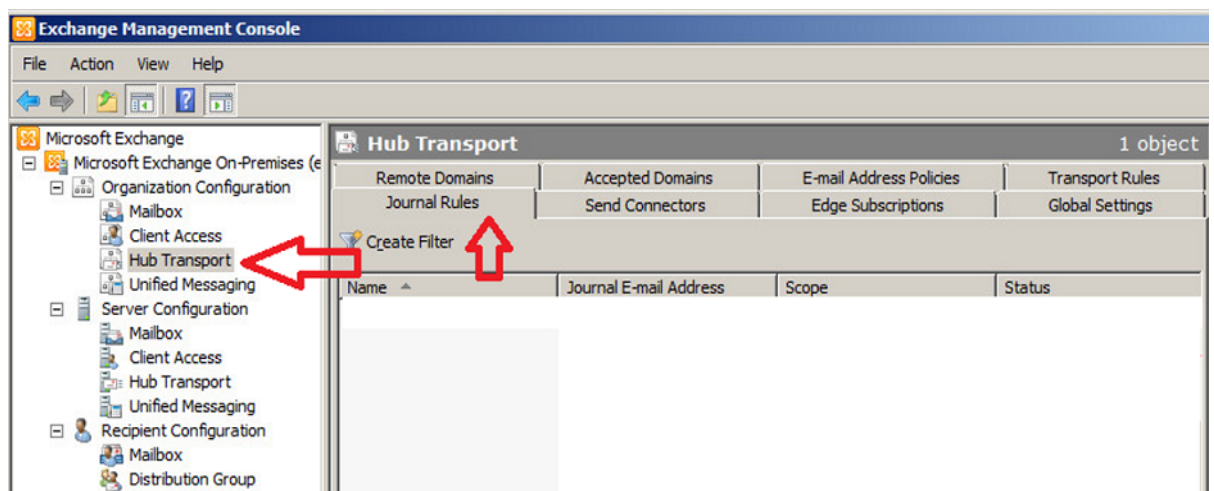
Journaling records inbound and outbound email communications to help organizations manage legal, regulatory, and organizational compliance requirements.

To create the journaling rule, follow these steps:

1. From the **Exchange Management Console**, navigate to **Organization Configuration** drop-down list and select **Hub Transport**.

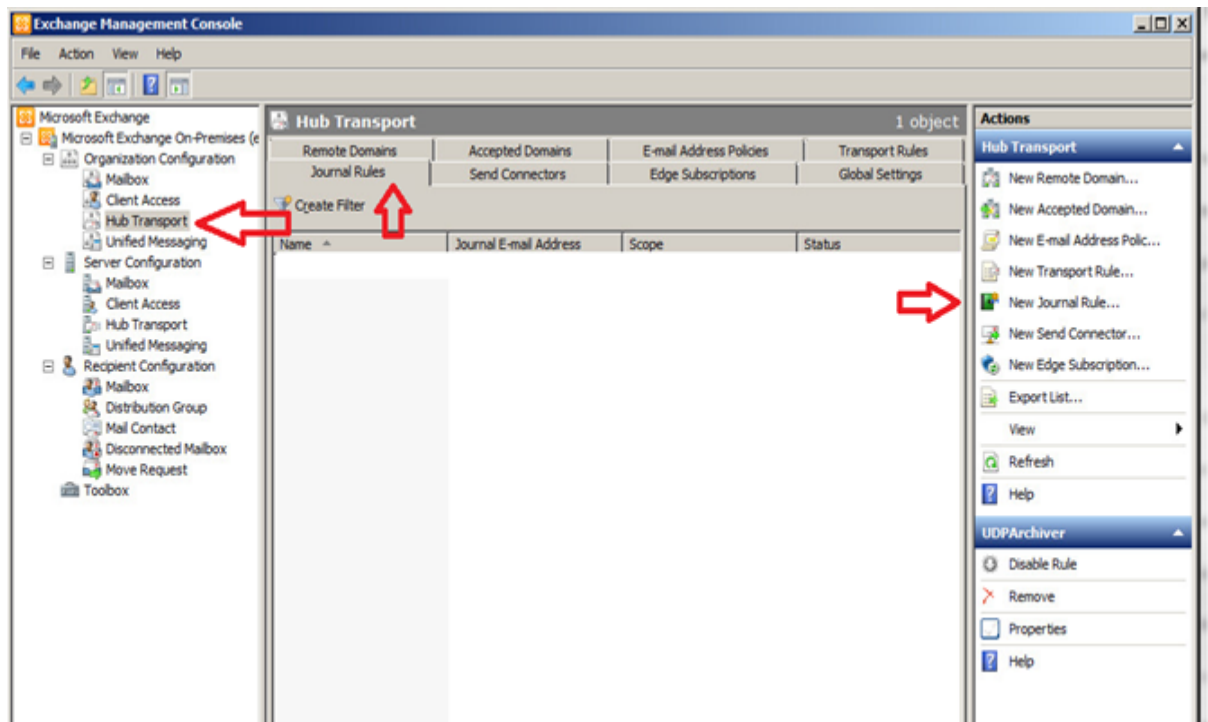


The **Hub Transport** screen opens.



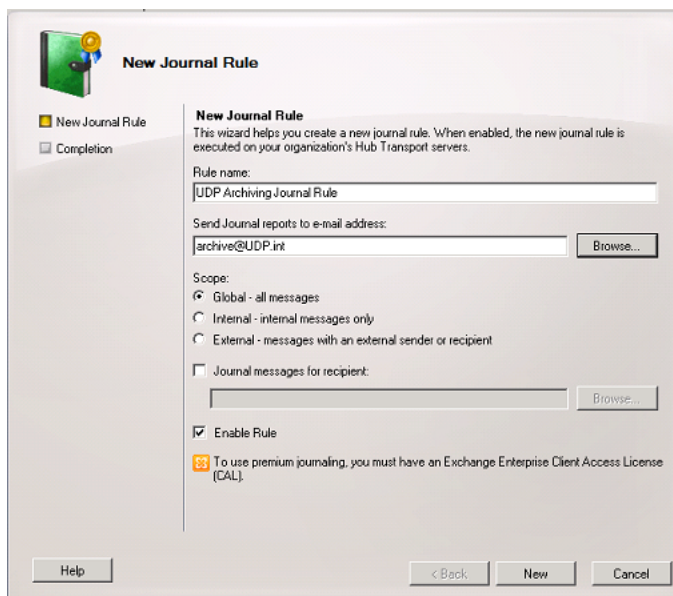
2. Select **Journal Rules** tab from the **Hub Transport** screen.





3. Click **New Journal Rule** from the **Actions** menu.

The **New Journal Rule** wizard is displayed.



Enter details:

### Rule name

Enter a name for your journal rule. For example: UDP Archiving Journal Rule

### Send Journal report to e-mail address

Select the forwarding e-mail address details. This email address is formed using the word “Archive” @FQDN of the UDP Archiving VM.

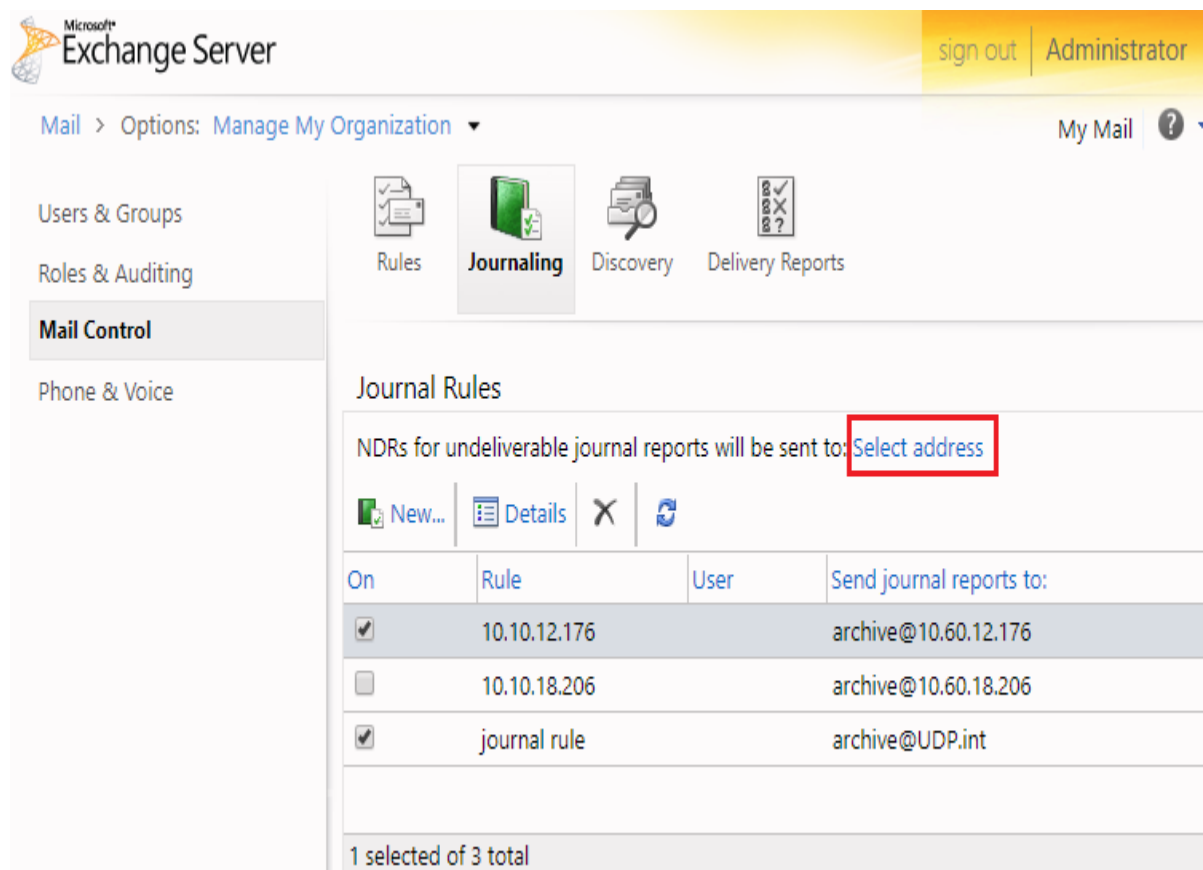
For example: archive@UDP.int.

### Journal message for recipient

**Important!** This option is required if you want to archive only a selected set of users.

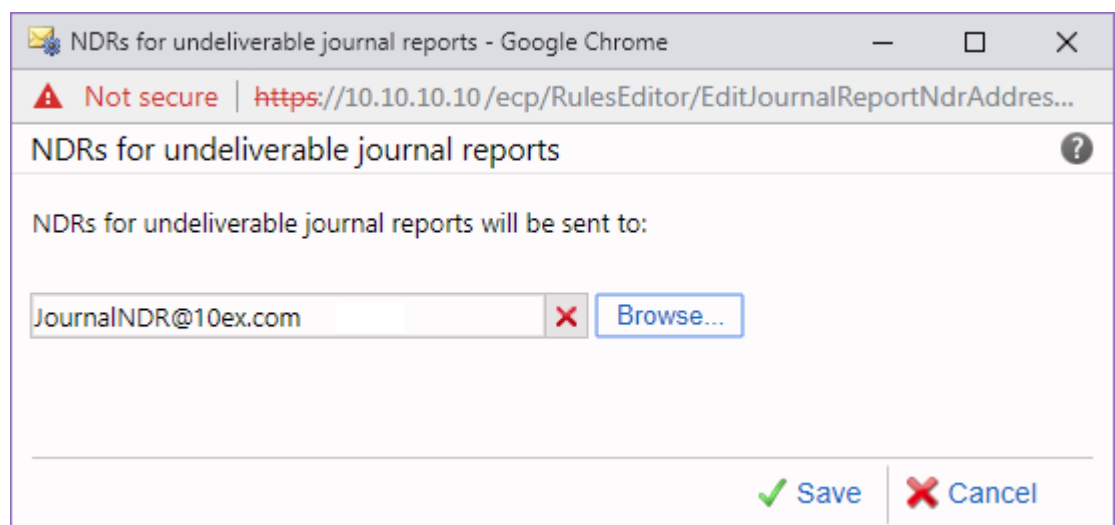
To enter Journal message for recipient, browse and select the distribution group created before.

4. Click **New**.
5. From the Completion tab, click **Finish**.  
The journaling rule is created.
6. Perform the following steps to configure the NDR mailbox
  - a. Open ECP in a web browser and login as administrator.
  - b. Navigate to the **Journal Rules** under Journaling tab of Mail Control and click **Select address**.



The NDRs for undeliverable journal reports screen pops up where you can select the NDR mailbox.

- c. Click **Browse**, select the NDR mailbox that you have created and click Save.



- d. Click **Save**.

The NDR mailbox you have added is visible at Recipients, Mail Boxes.

## Configuring Microsoft Exchange 2013 and 2016

For Microsoft Exchange, UDP Archiving ingests email using two methods. First, UDP Archiving ingests Exchange PST files into the archive. The PST files are created by the Exchange Server. Second, UDP Archiving is configured to receive journal email from Exchange Server via SMTP. Exchange journaling copies every email sent and received by a mailbox. Users configure journaling by mailbox and designate the UDP Archiving SMTP address as the destination. This process allows an organization to create a complete set of both historical and future email records.

To configure the Microsoft Exchange 2013 and 2016, you need to perform the following steps:

1. [\(Optional\) Create new Distribution Group \(Using EAC\)](#)
2. [Create a non-routable Remote Domain](#)
3. [Create a Fake Mail Contact using New Remote Domain](#)
4. [Create a non-deliverable Mailbox](#)
5. [Create a Send Connector for the Remote Domain](#)
6. [Add a Journaling Rule to direct Messages](#)

## (Optional) Create new Distribution Group (Using EAC)

**Note:** You can skip creating new distribution group, if you intend to set archiving for all users in your exchange organization.

Use the Exchange Admin Center (EAC) to create a distribution group for all the users to be archived.

### Follow these steps:

1. In the EAC, navigate to Recipients, Groups.
2. Click New, Distribution group.
3. On the New distribution group page, complete the following boxes:
  - **\*Display name:** Use this box to type the display name.
  - **\*Alias:** Use this box to type the name of the alias for the group.
  - **Description:** Describe the group.
  - **Organizational unit:** Select an organizational unit.
  - **\*Owners:** By default, the person who creates a group is the owner. All groups must have at least one owner. You can add owners by clicking Add.
  - **Members:** Use this section to add members.

To add members to the group, click Add . When you finish adding members, click OK to return to the New distribution group page.
4. Click **Save** to create the distribution group.

For more information on creating a new distribution group using EAC, refer the [link](#).

## Create a Non-routable New Remote Domain

Microsoft Exchange 2013 and 2016 require a remote domain to send the messages to the mail server (SMTP). The Remote Domain is not your regular email domain. The remote domain is a non-existent and non-routable/unresolvable domain from either inside or outside your organization (such as UDP.int). This domain is mandatory for the email address of the Mail Contact that is the recipient of the journal message.

### Follow these steps:

1. Open the Exchange Management Shell.
2. Run the following command to create the remote domain:

```
New-RemoteDomain -DomainName UDP.int -Name "Arcserve UDP Archiving Domain"
```

```
Get-RemoteDomain | Where {$_.DomainName -eq "UDP.int"} | Set-RemoteDomain -TNEFEnabled $false -AutoForwardEnabled $true
```

The command ensures that the TNEF encoding is disabled and auto-forwarding is enabled.

3. Run the following command to verify the settings:

```
Get-RemoteDomain | Where {$_.DomainName -eq "UDP.int"} | Format-table Name, DomainName, TNEFEnabled, AutoForwardEnabled
```

The new domain is created. For example: UDP.int.

### Next Steps:

1. [Create a Fake Mail Contact using New Domain](#)
2. [Create a Non-deliverable Mailbox](#)
3. [Create a Send Connector for the Remote Domain](#)
4. [Add a Journaling Rule to direct Messages](#)

## Create a Fake Mail Contact using New Remote Domain

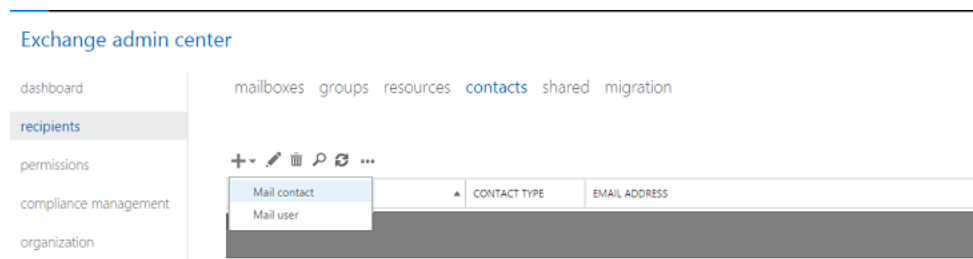
The Mail Contact is the account that acts as a *holding location* for journaled messages. The email address associated with this account is the designated recipient and must be associated with a non-existent, non-routable dummy Domain Name created in [previous step](#).

**Follow these steps:**

1. From **Exchange Admin Center** screen, select **recipients**.

The **recipients** screen opens.

2. Select **contacts** from the recipients screen.



3. Click **+** and select **Mail contact** to add.

The **new mail contact** screen opens.

4. Enter the required details. For example:

- **First name:** Arcserve
- **Initials:** UDP
- **Last Name:** UDP Archiving
- **Display Name:** Arcserve UDP Archiving
- **Alias:** EmailArchive
- **External email address:** archive@UDP.int

**Note:** Make a note of the email address as you need to use the same

ID later.

new mail contact [Help](#)

First name:

Initials:

Last name:

\*Display name:

\*Name:

\*Alias:

\*External email address:

Organizational unit:

5. Click **Save** to create the mail contact.

The mail contact is successfully created.

#### Next Steps:

1. [Create a Non-deliverable Mailbox](#)
2. [Create a Send Connector for the Remote Domain](#)
3. [Add a Journaling Rule to direct Messages](#)



## Create a Non-deliverable Mailbox

Non-Delivery Report (NDR) mailbox helps you know about the message that are not delivered to the UDP Archiving. Generally, the NDR is always a dedicated mailbox.

### Follow these steps:

1. From Exchange Admin Center, navigate to **recipients, mailboxes**, and then click the **+** symbol to create a new mailbox.
2. Enter the details as desired and click **save**. For example:
  - **First name:** Journal
  - **Last Name:** NDR
  - **Display Name:** NDR
  - **User logon name:** JournalNDR
  - **Domain:** <yourdomain>

### Exchange admin center

The screenshot shows the Exchange Admin Center interface. On the left is a navigation pane with links to recipients, permissions, compliance management, organization, protection, mail flow, mobile, public folders, unified messaging, servers, hybrid, and tools. The main area shows the 'mailboxes' section with a '+', edit, delete, and other icons. A 'new user mailbox' form is open in a browser window titled 'User Mailbox - Google Chrome'. The form fields are as follows:

- First name: Journal
- Initials: (empty)
- Last name: NDR
- \*Display name: Journal NDR
- \*Name: Journal NDR
- Organizational unit: (empty) with a 'browse...' button
- \*User logon name: JournalNDR @ <your domain> (with a tooltip: 'Type the user's alias here. The user will use this name to log on to the domain.')
  - \*New password: (empty)
  - \*Confirm password: (empty)
- ☐ Require password change on next logon
- More options... (link)
- Buttons: save, cancel

The added NDR mailbox is visible at **recipients, mailboxes**.

### Exchange admin center

recipients	mailboxes	groups	resources	contacts	shared	migration
permissions	+ - ✎ 🗑 🔍 ↺ ...					
compliance management						
organization						
protection						
mail flow						
mobile						
public folders						
unified messaging						
servers						
hybrid						
tools						

DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS
journal NDR	User	journalNDR@ <your domain>

### Next Steps:

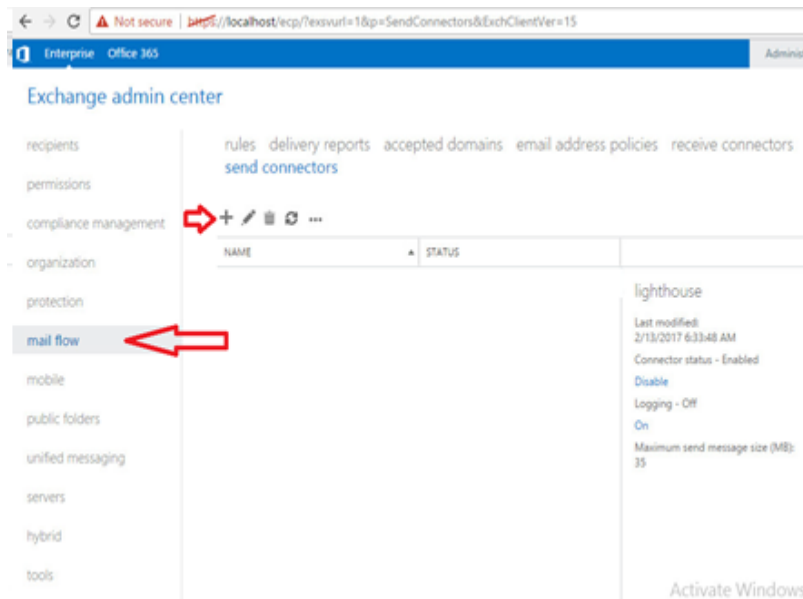
1. [Create a Send Connector for the Remote Domain](#)
2. [Add a Journaling Rule to direct Messages](#)

## Create a Send Connector for the Remote Domain

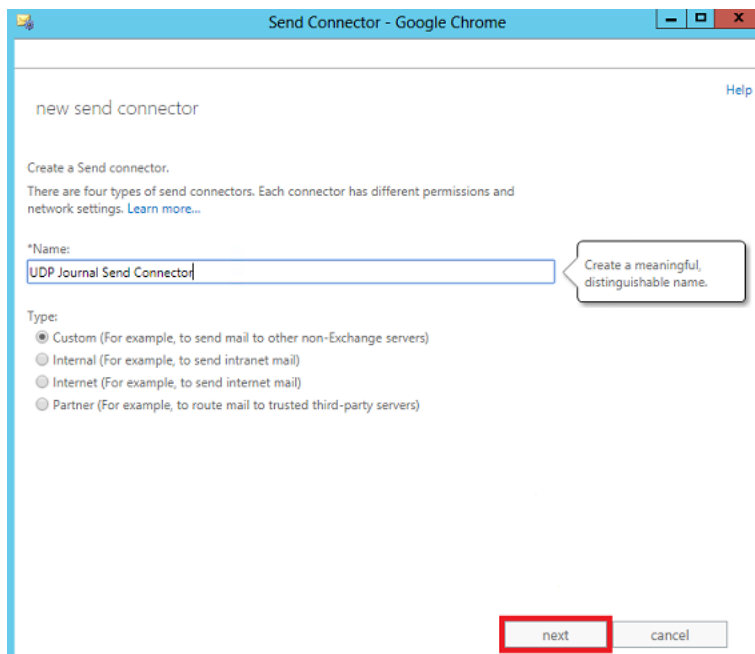
The connector sends the journal report to the mail server (SMTP).

To create a send connector, follow these steps:

1. From the **Exchange admin center**, navigate to **mail flow**, select **send connectors** and click **+**.



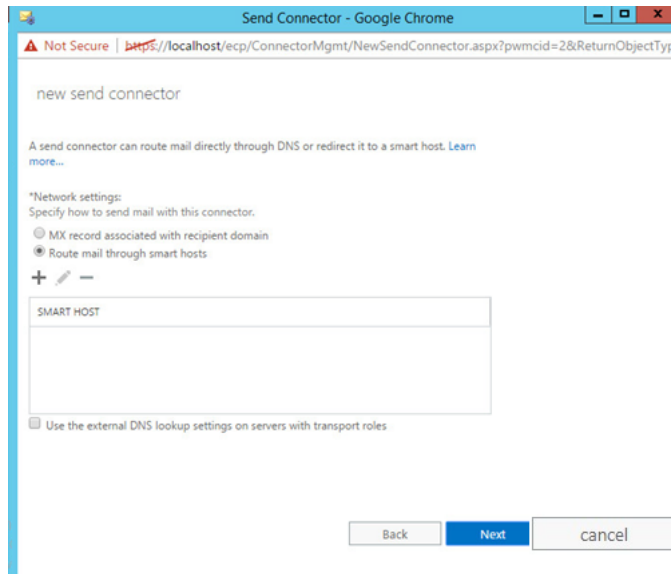
The **Send Connector** screen opens.



2. Enter a name for Send Connector and click **Next**.

Example of name: UDP Journal Send Connector

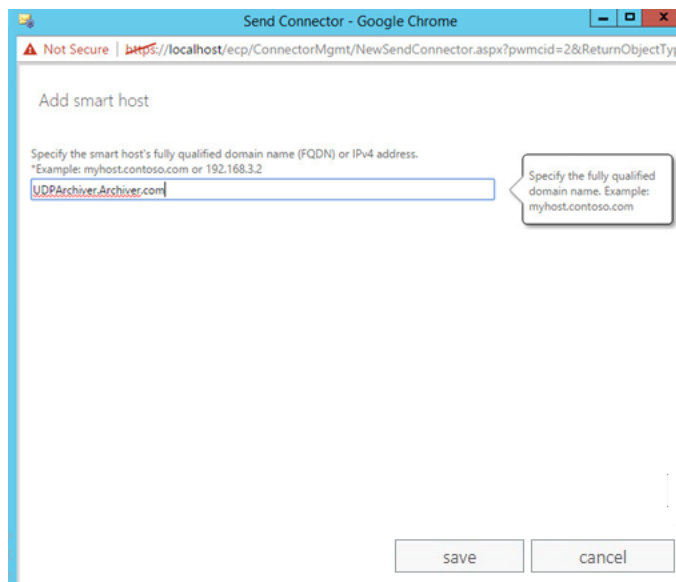
The **Network settings** screen appears.



The screenshot shows the 'new send connector' screen in a web browser. The title bar says 'Send Connector - Google Chrome'. The address bar shows a URL starting with 'https://localhost/ecp/ConnectorMgmt/NewSendConnector.aspx?'. The page has a header 'new send connector'. Below it, there is a description: 'A send connector can route mail directly through DNS or redirect it to a smart host. Learn more...'. Under '\*Network settings: Specify how to send mail with this connector.', there are two radio buttons: 'MX record associated with recipient domain' (unselected) and 'Route mail through smart hosts' (selected). Below the radio buttons, there is a '+ -' icon and a text box labeled 'SMART HOST'. At the bottom, there is a checkbox 'Use the external DNS lookup settings on servers with transport roles' which is unchecked. At the very bottom, there are three buttons: 'Back', 'Next', and 'cancel'.

3. Select the *Route mail through smart hosts* check box and click + to add a smart host.

The **Add smart host** screen appears.



The screenshot shows the 'Add smart host' screen in a web browser. The title bar says 'Send Connector - Google Chrome'. The address bar shows a URL starting with 'https://localhost/ecp/ConnectorMgmt/NewSendConnector.aspx?'. The page has a header 'Add smart host'. Below it, there is a description: 'Specify the smart host's fully qualified domain name (FQDN) or IPv4 address. \*Example: myhost.contoso.com or 192.168.3.2'. There is a text box containing 'UDPArchiver.Archiver.com'. To the right of the text box, there is a callout box that says 'Specify the fully qualified domain name. Example: myhost.contoso.com'. At the bottom, there are two buttons: 'save' and 'cancel'.

4. Enter the FQDN or the IP address of the new UDP Archiving VM and click **Save**.

The added host name appears on the **Network settings** screen.

- From the Network settings screen, click **Next**.

The **Smart host authentication** screen appears.

new send connector

Configure smart host authentication. [Learn more...](#)

Smart host authentication:

☒ None

☐ Basic authentication

☐ Offer basic authentication only after starting TLS

\*User name:

\*Password:

Note: all smart hosts must accept the same username and password.

☐ Exchange Server authentication

☐ Externally secured (for example, with IPsec)

Back Next Cancel

- Click **Next**.

The **\*Address space** screen appears.

new send connector

A Send connector routes mail to a specified list of domains. These domains can be an SMTP address space or a custom type. [Learn more...](#)

\*Address space:  
Specify the address space or spaces to which this connector will route mail.

+ -

TYPE	DOMAIN	COST
------	--------	------

☐ Scoped send connector

Back Next cancel

- Click **+** to add the Address space and click **Next**.

The **add domain** screen appears.

Send Connector - Google Chrome

Not secure | https://localhost/ecp/ConnectorMgmt/NewSendConnector.aspx?pwmcid=14&ReturnObject...

add domain [Help](#)

\*Type:  
SMTP

\*Full Qualified Domain Name (FQDN):  
UDP.int

\*Cost:  
1

save cancel

8. In the FQDN field, enter the full name of the remote domain and click **Save**.

For example: udp.int

The **\*Source server** screen appears.

Send Connector - Google Chrome

Not Secure | https://localhost/ecp/ConnectorMgmt/NewSendConnector.aspx?pwmcid=2&ReturnObjectType...

new send connector

A send connector sends mail from a list of servers with transport roles or Edge Subscriptions. [Learn more...](#)

\*Source server:  
Associate this connector with the following servers containing transport roles. You can also add Edge Subscriptions to this list.

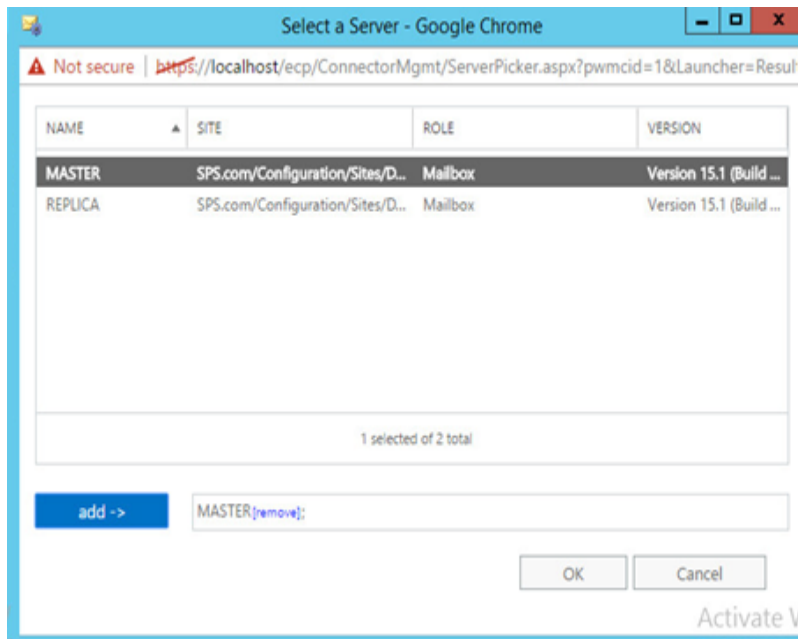
+ -

SERVER	SITE	ROLE
--------	------	------

Back Finish cancel

9. Click + to add an Exchange server with the transport role.

The **Select a Server** screen appears.



10. Select the Exchange 2013/2016 server that you need to use for routing mail to UDP Archiving and click **add->**.
11. Click **OK** to add the selected Exchange 2013/2016 server.
12. Click **Finish**.

The Send Connector is created successfully.

**Next Step:**

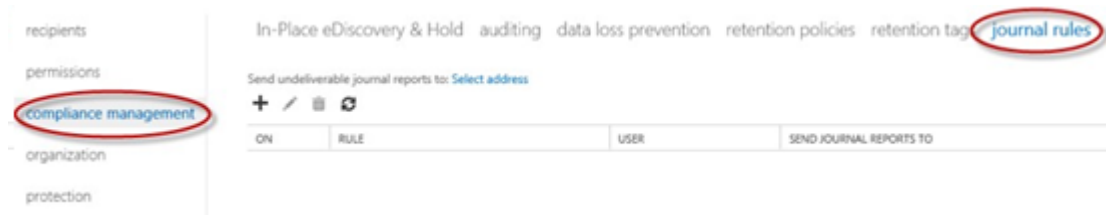
[Add a Journaling Rule to direct Messages](#)

## Add a Journaling Rule to direct Messages

Journaling records inbound and outbound email communications to help organizations manage legal, regulatory, and organizational compliance requirements.

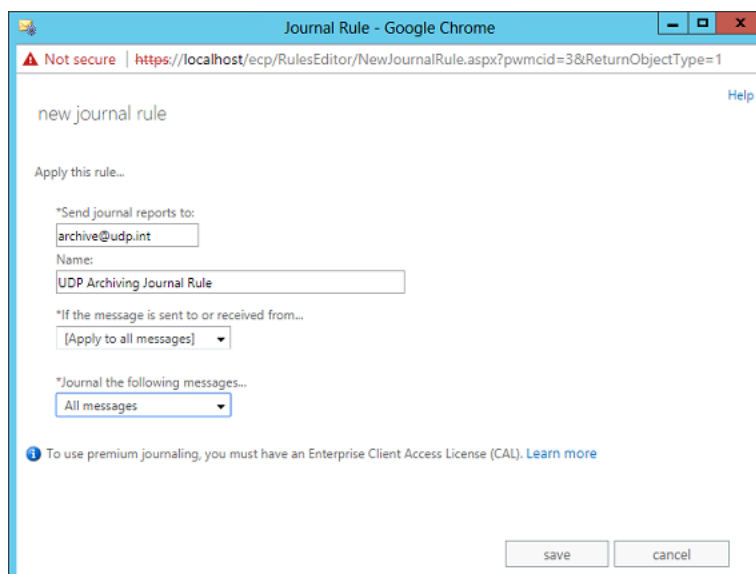
To enable the Exchange Journaling rule, follow these steps:

1. Select **compliance management** and click **journal rules**.



2. Click **+** to add a new journal rule.

The **Journal Rule** screen appears.



3. In the **Send Journal Reports to:** field, enter the email address of the contact created. For example, archive@UDP.int
4. Enter a name for the rule in Name field. For example, UDP Archiving Journal Rule.
5. Select **Apply to all messages** from the *If the message is sent or received from* list drop-down menu.
6. Select **All Messages** from the **Journal the following messages...** drop-down menu.

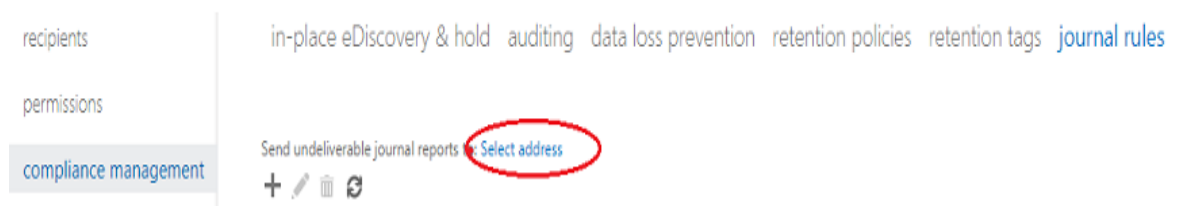


7. Click **save**.
8. Click **Yes** for the warning message **Do you want this rule to apply to all future messages**.

The journal rule displays as enabled on the journal rules page. Now, you need to configure the NDR mailbox.

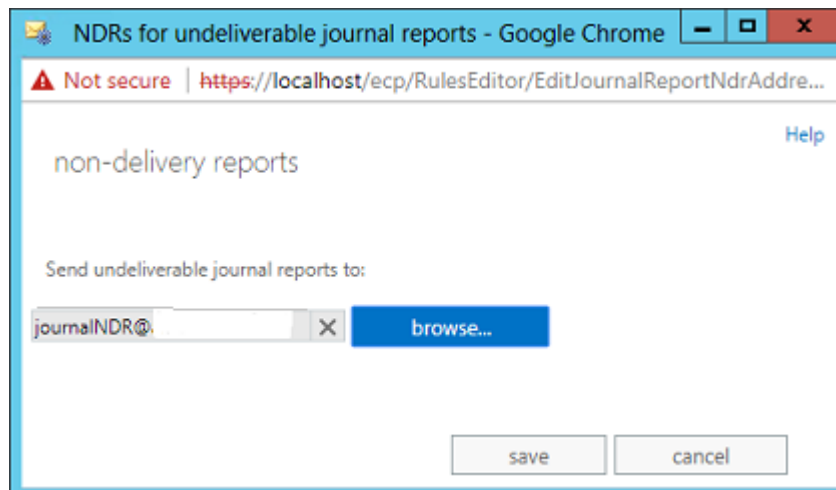
9. Perform the following steps to configure the NDR mailbox
  - a. Navigate to the **journal rules** tab of Compliance management and click **Select address**.

#### Exchange admin center



The non-delivery reports screen pops up where you can select the NDR mailbox.

- b. Click **browse** and select the created NDR mailbox "JournalNDR@<your domain>"



- c. Click **save**.

You have successfully set up Email Journaling.

## Configuring G Suite Email

UDP Archiving lets you configure G Suite Email. To start, configure UDP Archiving Console for G Suite and then configure G Suite for archiving.

### Follow these steps:

1. Log into UDP Archiving as Super admin and add the mail domain of G Suite.

For information about how to add mail domain, view [adding mail server domain](#).

2. Create a profile and administrator for the domain.

For information about how to add profile and administrator, view [configure settings](#).

The G suite email is configured in UDP Archiving. Now, you need to configure G Suite.

3. Navigate to <https://admin.google.com>.

Google Admin Console login page is displayed.

4. Enter G Suite administrator user credentials to login.

Admin Console displays multiple options including Apps.

5. Click **Apps**.

Apps Setting page displays multiple options including G Suite.

6. Click **G Suite**.

List of G Suite options including Gmail appear.

7. Click **Gmail**.

Gmail settings page displays multiple options including Advanced Settings.

8. Click **Advanced Settings**.

The Advanced Settings page opens with details of the General Settings tab.

9. Scroll down the General Settings tab to Routing section and place your mouse over **Routing**.

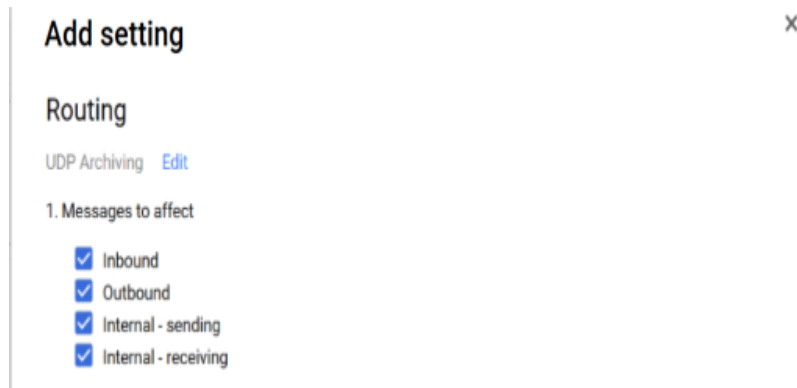
The Configure button appear in front of Routing.

**Note:** Configure button appears only when you have not configured Routing before. If already configured before, from the multiple options that appear select *Add Another* to reach the Add Setting page.

10. Click **Configure**.

The Add setting page displays.

11. Enter details in the **Add setting** page using the following options:
  - a. Name the rule as UDP Archiving.
  - b. Select the check boxes of all messages to affect. For example, **Inbound**, **Internal - receiving** and so on.



- c. (Optional) Select the required option under **Envelope Filter**.

Filters let you select specific users or predefined groups to archive. Consider the scenarios before selecting this option.

- ◆ If you select checkboxes of envelope senders and recipients both, then do not provide same Email address under Group Membership.
- ◆ Only those recipients can view emails whose email ID is entered under envelope recipients.

- d. Perform the following steps for **Also deliver to**:

**Add setting** ×

**Headers**

- ☐ Add X-Gm-Original-To header
- ☐ Add X-Gm-Spam and X-Gm-Phishy headers
- ☐ Add custom headers

**Subject**

- ☐ Prepend custom subject

**Route**

- ☐ Change route

**Envelope recipient**

- ☐ Change envelope recipient

**Spam**

- ☐ Bypass spam filter for this message

**Attachments**

- ☐ Remove attachments from message

**Also deliver to**

- ☒ Add more recipients

**Recipients** ADD

**Advanced** ▾

**Recipient address:**

Enter an additional recipient email address

CANCEL SAVE

CANCEL ADD SETTING

- Select **Add more recipients**.
- From the **Recipients** box, click **Add**.
- From the drop-down list, select **Advanced**.

**Add setting** [X]

**Recipients** [ADD]

Advanced ▾

Apply the above modifications, plus the following:

**Route**

☐ Change route

**Envelope recipient**

☒ Change envelope recipient

☒ Replace recipient: archive@f4b3c1d2e3

☐ Enter new username @ existing-domain

☐ Existing-username @ Enter new domain

**Spam and delivery options**

☒ Do not deliver spam to this recipient

☒ Suppress bounces from this recipient

**Headers**

☐ Add X-Gm-Original-To header

☐ Add X-Gm-Spam and X-Gm-Phishy headers

☐ Add custom headers

**Subject**

☐ Prepend custom subject

**Attachments**

☐ Remove attachments from message

CANCEL SAVE

CANCEL ADD SETTING

- From the displayed options, select **Change envelope recipient** option.
- Enter email address for **Replace recipient**. For example, archive@FQDN where FQDN refers to the public address of the UDP Archiving system. You can also use the SMTP Forwarding Address from the UDP Archiving Console.
- Click **SAVE**.
- Click **Show options** and scroll down to select all options available under **Account types to affect**.

×

Add setting

Spam

☐ Bypass spam filter for this message

Attachments

☐ Remove attachments from message

Also deliver to

☒ Add more recipients

Recipients

ADD

Deliver to: archive@udp.archiving.com

Do not deliver spam to this recipient

Suppress bounces from this recipient

Encryption (onward delivery only)

☐ Require secure transport (TLS)

Hide options

A. Address lists

☐ Use address lists to bypass or control application of this setting

Apply address lists to correspondents

☐ Bypass this setting for specific addresses / domains

☐ Only apply this setting for specific addresses / domains

B. Account types to affect

☒ Users

☒ Groups

☒ Unrecognized / Catch-all

CANCEL

ADD SETTING

e. Click **Add Setting**.

Routing is configured.

12. Click **Save** at the end of the General settings page.

G Suite email is configured for UDP Archiving. You can send a copy of all messages to UDP Archiving.

13. Send a test email to an email account on G Suite.

14. Log into UDP Archiving as super admin and click **Message audit** to view the message. You can also login as administrator and view message count from Dashboard.

## Configuring IBM Lotus Domino

For viewing steps in video, click [How to Configure IBM Lotus Domino](#).

Configuring email services of IBM Lotus Domino (referred ahead as Lotus Domino) for UDP Archiving involves the following steps:

- [Configure UDP Archiving for Lotus Domino](#)
- [Set up Lotus Domino for UDP Archiving](#)

## Configure UDP Archiving for Lotus Domino

Configuring UDP Archiving Console for Lotus Domino is the first step towards archiving message using Lotus Domino email service.

**Follow these steps:**

1. Log into UDP Archiving as super admin and add the mail domain of Lotus Domino.

For information about how to add mail domain, view [adding mail server domain](#).

2. Create a profile and administrator for the domain.

For information about how to add profile and administrator, view [configure settings](#).

The Lotus Domino email is configured in UDP Archiving. Now, you need to configure Lotus Domino by [setting up journal rule](#).



## Set up Email Services of Lotus Domino

After configuring UDP Archiving Console, set up email service to complete configuration of Lotus Domino. Setting up email services involves the following steps in Lotus Domino:

1. [Set up a journal rule](#)
2. [Enable journaling](#)
3. [Set Advanced Outbound Message options](#)
4. [Set up a smart host for outbound mail](#)

## Set up the Journal Rule

Journaling records inbound and outbound email communications to help organizations manage legal, regulatory, and organizational compliance requirements.

**To set up the journal rule, follow these steps:**

1. Open Domino Administrator Client and navigate to Configuration, Messaging, Configurations.

The screen displays available configuration document(s).

2. Open the configuration document for the server that you want to configure.

**Note:** Open the configuration document in the Edit mode.

3. Navigate to Router/SMTP, Restrictions and Controls, Rules.



The **journal rules** screen is displayed.

4. Click **Edit Server Configuration**.
5. Click **New Rule**.

The New Rule dialog is displayed with by default selected details in two fields: Specify Conditions and Specify Actions.

6. Perform the following options to create a rule that journals messages to UDP Archiving and click OK.
  - a. In the Specify Conditions field, perform the following steps and click **Add**:
    - ◆ Replace sender option and select all documents option from the drop-down option. Selecting all documents helps you archive all messages

**Note:** You can also select one of the available conditions from the drop-down option. For example, Subject, Body, To, CC, BCC, and so on.

Based on your selection the conditions field displays sender or other option.

- ◆ Click **Add**.

Server Mail Rule - New Rule

This rule is: ☒ On ☐ Off

Specify Conditions

Create: ☒ Condition ☐ Exception

AND sender contains

When mail messages arrive that meet these conditions:

When:  
All Documents

Specify Actions

journal this message

Perform the following actions:

Add Action  
Remove  
Remove All

OK Cancel

- In the Specify Actions field, perform the following steps:
  - ◆ Verify if **journal this message** is selected from the drop-down options.
  - ◆ Click **Add Action** and then click **OK**.

Server Mail Rule - Edit Rule

This rule is: ☒ On ☐ Off

Specify Conditions

Create: ☒ Condition ☐ Exception

AND sender contains

When mail messages arrive that meet these conditions:

When:  
All Documents

Specify Actions

journal this message

Perform the following actions:  
Journal this Message

Add Action  
Remove  
Remove All

OK Cancel

The New Rule dialog closes and the created rules are displayed.



The New Rule dialog closes and the created rules are displayed. The New Rule dialog closes and the created rules are displayed.

7. Click **Save & Close**.

To apply the created rules, you need to enable to journal.

## Enable Journaling

Journaling records inbound and outbound email communications to help organizations manage legal, regulatory, and organizational compliance requirements.

To set up the journal rule, follow these steps:

1. Open Domino Administrator Client and navigate to Configuration, Messaging, Configurations.

The screen displays available configuration document(s).

2. Open the configuration document for the server that you want to configure.

**Note:** Open the configuration document in the Edit mode.

3. Navigate to **Router/SMTP, Advanced**.

Configuration Settings : domino9itc/ARCSERVE

Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings | IBM iNotes | IMAP | SNMP | Activity Logging | Diagnostics | Administration

Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Message Recall | Advanced...

Journaling | Commands and Extensions | Controls

**Basics**

Journaling: ☒ Enabled ▾

Field encryption exclusion list: ☒ Form; From; Principal; PostedDate ▾

Method: ☒ Copy to local database ▾

Database Name: ☒ mailjm.nsf ▾

Encrypt on behalf of user: ☒ LocalDomainServers ▾

Journal Recipients: ☒ Enable ▾

**Database Management**

Method: ☒ Periodic Rollover ▾

Periodicity: ☒ 1 ▾ days

\*\*\*Reminder: A journaling mail rule is needed to properly enable message journaling.

4. Perform the following steps:

- a. For **Journaling**, select **Enabled**.
- b. For **Method**, select **Send to mail-in database** from the drop-down list.

Select this option to route emails to UDP Archiving without saving the messages in the database. If you select this option, also specify mail destination.

- c. For **Mail Destination**, specify the same SMTP address of the UDP Archiving that is provided in the **Configuration** tab of Super admin.
- d. For Journal Recipients, select **Enable**.



Save & Close Cancel

**Configuration Settings : Inode9/lot**

Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings | IBM iNotes | IMAP | SNMP | Activity Logging | Diagnostics | Administration

Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Message Recall | Advanced...

Journaling | Commands and Extensions | Controls

**Basics**

Journaling: ☒ Enabled

Field encryption exclusion list: ☒ Form; From; Principal; PostedDate

Method: ☒ Send to mail-in database

Mail Destination: ☒ archive@arc-ga.arcserve.com

Journal Recipients: ☒ Enable

\*\*\*Reminder: A journaling mail rule is needed to properly enable message journaling.

5. Click **Save & Close**.

With journal enabled, you need to provide advanced settings for outbound messages.

## Set Advanced Outbound Message Options

Setting advanced options for outbound message lets organizations help auditing. Use this option to set desired settings required for auditing. For example, add settings to record email addresses added in BCC field of emails or add group settings to identify all email addresses in group messages.

### Follow these steps:

1. Navigate to MIME > Advanced > Advanced Outbound Message Options.
2. Specify the following information in the option **Always send the following Notes items in headers**.

*\$JournalRecipients*

*RecipientGroupsExpanded*

*OriginalBcc*

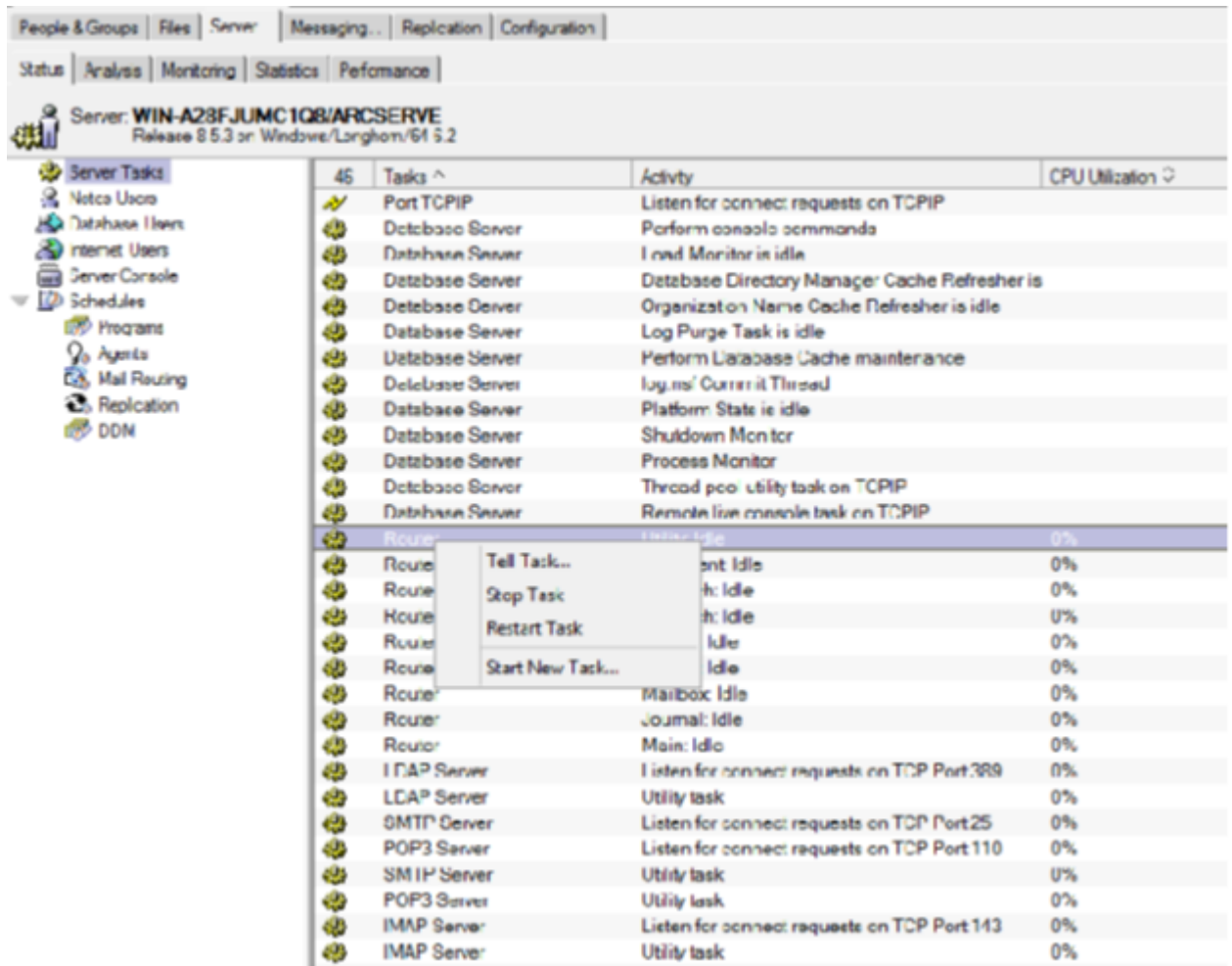
The screenshot shows the 'Configuration Settings : domino/ARCSERVE' dialog box. The 'MIME' tab is selected, and the 'Advanced Outbound Message Options' sub-tab is active. The settings are as follows:

- Macintosh attachment conversion: ☒ AppleDouble (base64 only)
- RFC822 phrase handling: ☒ Do not add phrase
- Internet Mail server sends Notes private items in messages: ☒ Disabled
- Always send the following Notes items in headers: ☒ \$JournalRecipients, RecipientGroupsExpanded, OriginalBcc
- Notes items to be removed from headers: ☐ (empty)
- When converting a multilingual message to MIME: ☐ Send it in Unicode (UTF8), ☒ Send it in most representable charset
- Character set name aliases: Two empty text boxes, each with a 'maps to' label and a dropdown arrow.

3. For the field *When connecting a multilingual message to MIME*, select the option **Send it in most representable charset**.
4. Click Save & Close.



5. To apply the journaling updates, restart the Router task from the server tasks option of IBM Lotus Domino.



The configuration of Lotus Domino email services is complete and you are set to use UDP Archiving.

If your organization uses Smarthost option in Lotus domino, move to next [step](#).

## Set up Host for Outbound Email

When using outbound filtering, you need to configure a smart host to route mails to UDP Archiving Server. Using IBM Lotus Domino, some customers use third-party relay server to communicate to hosts and some connect directly to the hosts. The topics below describe how to set up host for outbound email to single or multiple hosts.

- [Set up Host for Outbound Email to Single Host](#)
- [Set up Host for Outbound Email to Multiple Hosts](#)

## Set up a Smart Host for Outbound Email to Single Host

When using outbound filtering, you need to configure a smart host to route mails to UDP Archiving Server.

### Follow these steps:

1. From the Domino Administrator, perform the following steps:
  - a. Navigate to the **Configuration** tab.
  - b. Expand the **Messaging** section.
  - c. Select **Configurations**
  - d. Select the Configuration Settings document.
2. Click Edit Configuration and perform the following steps:
  - a. Navigate to Router/SMTP, Basics.
  - b. Select **Enabled** for the field **Smarthost is used for all local internet domain recipients**.

The screenshot shows the 'Edit Server Configuration' dialog box for 'WIN-A28FJUMCTQ8/ARCSERVE'. The 'Router/SMTP Basics' tab is selected. The 'Smart host is used for all local internet domain recipients' field is set to 'Enabled'. Other fields include 'Number of mailboxes', 'SMTP used when sending messages outside of the local internet domain' (Enabled), 'SMTP allowed within the local internet domain' (Disabled), 'Servers within the local Notes domain are reachable via SMTP over TCP/IP' (Always), 'Address lookup' (Fullname then Local Part), 'Exhaustive lookup' (Disabled), 'Relay host for messages leaving the local internet domain' (10.60.21.8), 'Use authentication when sending messages to the relay host' (Disabled), 'Local Internet domain smart host' (WIN-A28FJUMCTQ8), and 'Host name lookup' (Dynamic then local).

Router/SMTP Basics	
Number of mailboxes:	
SMTP used when sending messages outside of the local internet domain:	Enabled
SMTP allowed within the local internet domain:	Disabled
Servers within the local Notes domain are reachable via SMTP over TCP/IP:	Always
Address lookup:	Fullname then Local Part
Exhaustive lookup:	Disabled
Relay host for messages leaving the local internet domain:	10.60.21.8 SMTP Enabled relay host IP address as Gateway
Use authentication when sending messages to the relay host:	Disabled
Local Internet domain smart host:	WIN-A28FJUMCTQ8 Domino Server name with FQDN
Smart host is used for all local internet domain recipients:	Enabled
Host name lookup:	Dynamic then local

3. Click **Save & Close**.

The smart host is set for outbound emails.

The configuration of Lotus Domino email services is complete and you are set to use UDP Archiving.

## Set up a Host for Outbound Email to Multiple Hosts

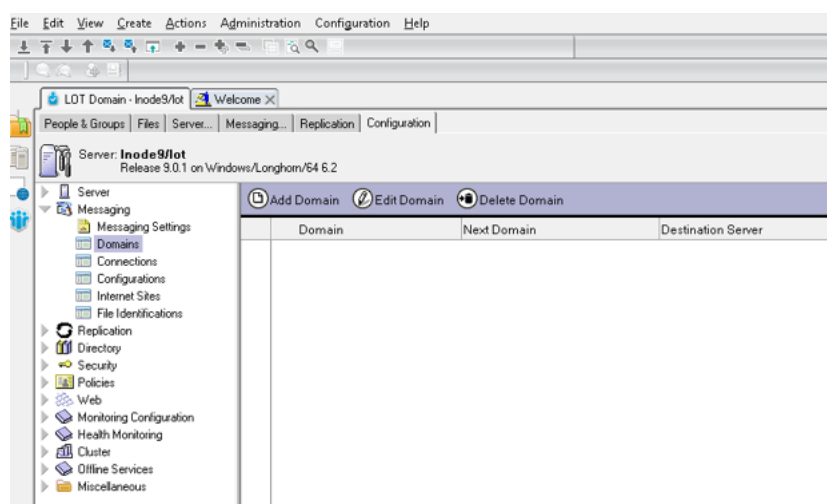
UDP Archiving does not receive journaling data if your environment is using a third-party relay server to send messages. By default, IBM Lotus Domino can only communicate with one server at a time on any given server. As a result, the outbound email reaches only one host. If you are not using the host server of UDP Archiving, then the data does not reach any other server except the one that you have specified in your environment. In such scenario, you need to set up host for outbound email to multiple hosts.

**To send data to UDP Archiving, use one of the following options:**

1. Configure the third-party relay server to automatically forward or send a copy of the journal data to UDP Archiving.
2. Foreign SMTP is configured externally to split the routing and send mails to all multiple hosts that are configured. This applies only to third-party archiving servers. To perform the update, mention Engineering IP host as relay host in Lotus Domino configuration. As a result, Lotus Domino routes mails to the journal at Mail destination.
3. Configure Lotus Domino server to send mail directly without using the third-party relay server.

**To configure Lotus Domino server, perform the following steps:**

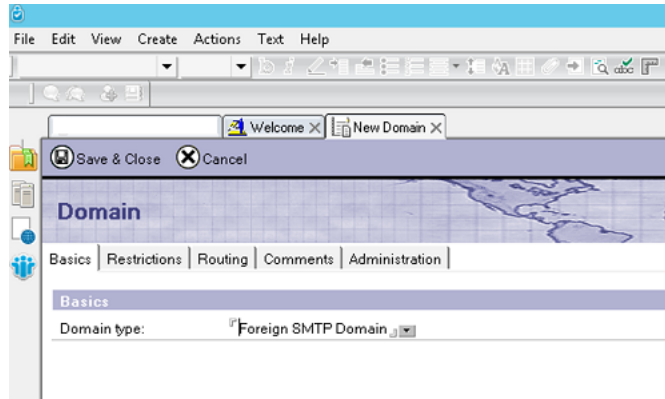
1. Open Lotus Domino **Configuration** window.
2. Click **Messaging** and navigate to Domains.



3. Click **Add Domain**.

The New Domain dialog box is displayed. From the New Domain window, you need to configure Foreign SMTP Domain and Global Domain.

4. Perform the following steps to configure Foreign SMTP Domain:
  - a. From the **Domain type** field of the **Basics** tab, select **Foreign SMTP Domain**.

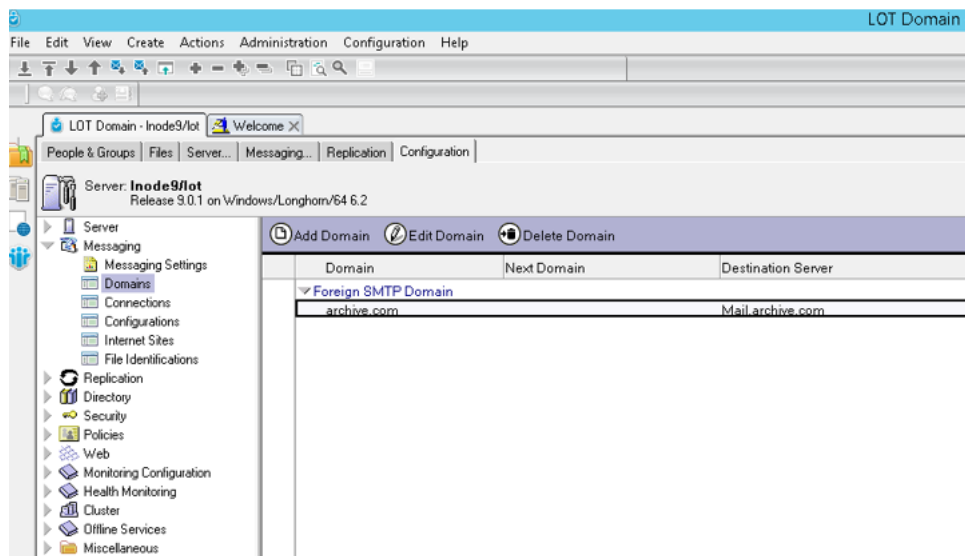


- b. From the **Routing** tab, enter the information for the following fields
 

**Internet Domain:** Refers to the Internet domain used as UDP Archiving forwarding address

**Internet host:** IP or FQDN of the UDP Archiving server.
    - c. Click **Save & Close**.

The Foreign SMTP Domain appears as displayed below.



5. Perform the following steps to configure Global Domain:

- a. From the **Domain type** field of the **Basics** tab, select **Global Domain**.

Domain

Basics | Restrictions | Conversions | Comments | Administration

**Basics**

Domain type: Global Domain

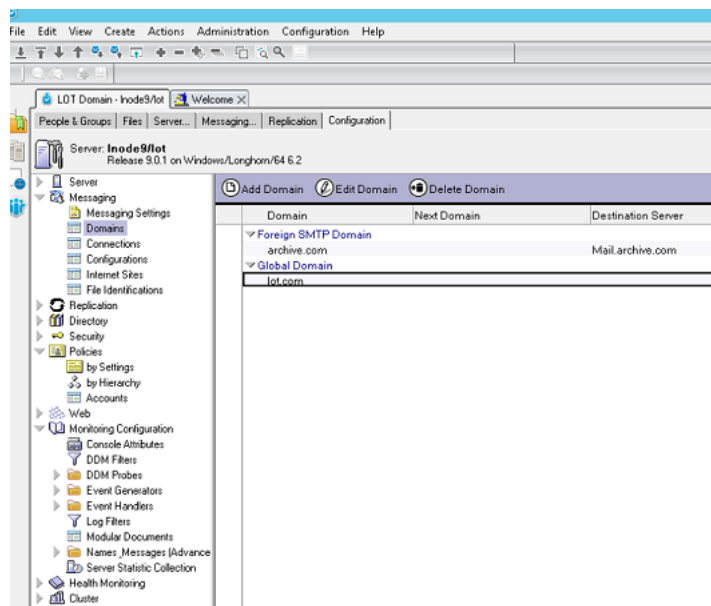
Global domain name:

Global domain role: R5/R6/R7/R8 Internet Domains or R4xSMTP MTA

Use as default Global Domain (for use with all Internet protocols except HTTP): ☐ Yes

- b. In the field of **Global domain name**, enter related domain name for your Lotus Domino.
- c. For **Global domain role** drop-down options, select **R5/R6/R7/R8 Internet Domains or R4xSMTP MTA**.
- d. Click **Save & Exit**.

The smart host is configured and the domain screen appears as displayed below.



## Configuring Zimbra

UDP Archiving lets you configure Zimbra. To start, configure UDP Archiving Console for Zimbra and then configure Zimbra for archiving.

### Follow these steps:

**Important!** Hosted Archiving customers do not need to perform first two steps.

1. Log into UDP Archiving as Super admin and add the mail domain of Zimbra.

For information about how to add mail domain, view [adding mail server domain](#).

2. Create a profile and administrator for the domain.

For information about how to add profile and administrator, view [configure settings](#).

Zimbra is configured in UDP Archiving. Now, you need to configure journaling of the Zimbra mail server.

3. Log into Zimbra email Server using any console client, such as Putty.

4. Enable archiving on the MTA server using the following command:

```
zmprov ms <zmlhostname> +zimbraServiceEnabled archiving
```

5. Restart the Zimbra server using the following command to enable archiving on Zimbra.

```
zmcontrol restart
```

Now, you need to start archiving emails of individual user in UDP Archiving.

**Note:** If the archive account is not maintained within Zimbra, you do not need to set a password, COS, or other attributes.

6. In the Zimbra console, run the following command:

```
zmarchiveconfig enable <account@example.com> archive-address account-  
archive@offsiteserver.com archive-create false
```

**account@example.com** is Zimbra user account email address

**account-archive@offsite.com** is the third party address. For example, UDP Archiving deployed host address.

**Note:** To archive emails of all users by default, configure Zimbra relay host IP to UDP Archiving console IP address.

Zimbra is configured for UDP Archiving.

7. Log into UDP Archiving and click **Message audit** to view the message count.

## Configuring Sendmail

UDP Archiving lets you configure Sendmail. To start, configure UDP Archiving Console for Sendmail and then configure Sendmail for archiving.

### Follow these steps:

**Important!** Hosted Archiving customers do not need to perform first two steps.

1. Log into UDP Archiving as Super admin and add the mail domain of Sendmail.

For information about how to add mail domain, view [adding mail server domain](#).

2. Create a profile and administrator for the domain.

For information about how to add profile and administrator, view [configure settings](#).

Sendmail is configured in UDP Archiving. Now, you need to configure journaling of the Sendmail mail server.

3. Log into Sendmail.
4. Modify following content in the file `/etc/mail/sendmail.mc` to synchronize with UDP Archiving as shown below:

```
define(`SMART_HOST', `smtp:[<Archiving machine IP Address/ Archiving machine hostname>]')dnl
```

```
LOCAL_DOMAIN(`<sendmail server domain>')dnl
```

```
MASQUERADE_AS(`<sendmail server domain>')dnl
```

Uncomment the below line

```
DAEMON_OPTIONS(`Port=smtps, Name=TLSMTPA, M=s')dnl
```

5. Execute below command and restart the Sendmail service.

```
m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
```

6. Add following lines in the file `vi /etc/procmailrc`:

```
:0c # Copy everything
```

```
! archive@<Archiving hostname / IP> # Send the copies to this address
```

Configuring of Sendmail is complete.

7. Log into UDP Archiving and click **Message audit** to view the message count.

**Note:** If you want to use the Import feature, perform the steps provided below.



1. To enable import, add the following content in the file `/etc/dovecot/dovecot.conf`:

```
protocols = imap pop3 imaps pop3s  
listen = *  
!include_try /usr/share/dovecot/protocols.d/*.protocol  
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

**Note:** The mail location depends on the location of mailbox.

2. Add following content in the file `/etc/dovecot/conf.d/10-mail.conf`:

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

**Note:** The mail location depends on the location of mailbox.

3. Modify following content in the file `/etc/dovecot/conf.d/10-ssl.conf` as shown below:

```
ssl = yes
```

4. Change permission for the following folder:

```
chmod 777 /var/mail*
```

5. Restart the dovecot service.
6. Execute the following command:

```
iptables -flush.
```

7. Restart the iptables service

## Configuring Postfix

UDP Archiving lets you configure Postfix. To start, configure UDP Archiving Console for Postfix and then configure Postfix for archiving.

### Follow these steps:

**Important!** Hosted Archiving customers do not need to perform first two steps.

1. Log into UDP Archiving as Super admin and add the mail domain of Postfix.  
For information about how to add mail domain, view [adding mail server domain](#).
2. Create a profile and administrator for the domain.  
For information about how to add profile and administrator, view [configure settings](#).  
  
Postfix is configured in UDP Archiving. Now, you need to configure journaling of the Postfix mail server.
3. Log into Postfix.
4. Modify following content in the file `/etc/postfix/main.cf` to synchronize with UDP Archiving:  
  
Add the **always\_bcc** parameter and enter the value as **archive@[your ip]** to get the mails archived to your archiving system. For example, `always_bcc = archive@[10.15.55.255]`
5. Log into UDP Archiving and click **Message audit** to view the message count.
6. For migration of emails, convert your mails into .eml or .pst format using any third-party tools.
7. For import, make sure the following values are uncommented or written into the respective files:

- In `/etc/postfix/main.cf`  
`smtpd_tls_cert_file = </etc/dovecot/private/mykey.key`  
`smtpd_tls_key_file = </etc/dovecot/mycert.pem`  
`smtpd_use_tls=yes`
- In `/etc/dovecot/dovecot.conf`  
`protocols = imap pop3 imaps pop3s`
- in `/etc/dovecot/conf.d/10-mail.conf`  
`mail_location = maildir:~/Maildir`

- in `/etc/dovecot/conf.d/10-auth.conf`  
*disable\_plaintext\_auth = no*  
*ssl=required*  
*auth\_mechanisms = plain login*
- in `/etc/dovecot/conf.d/10-ssl.conf`  
*ssl = yes*  
*ssl\_key = </etc/dovecot/private/mykey.key*  
*ssl\_cert = </etc/dovecot/mycert.pem*

**Notes:**

- ◆ Make sure that the SSL certificate is present for using the POP3S and IMAPS protocols.
- ◆ The `ssl_key` and `ssl_cert` parameter path might vary.

## Configuring Kerio

UDP Archiving lets you configure Kerio. To start, configure UDP Archiving Console for Kerio and then configure Kerio for archiving.

### Follow these steps:

**Important!** Hosted Archiving customers do not need to perform first two steps.

1. Log into UDP Archiving as Super admin and add the mail domain of Kerio.  
For information about how to add mail domain, view [adding mail server domain](#).
2. Create a profile and administrator for the domain.  
For information about how to add profile and administrator, view [configure settings](#).  
  
Kerio is configured in UDP Archiving. Now, you need to configure journaling of the Kerio mail server.
3. Log into Kerio.
4. Navigate to configurations, archiving and backup and click the **archiving** tab.
5. From the email archiving section, enter the SMTP forwarding email address of your archiving machine.
6. Enable the archiving to remote email address section.
7. Navigate to configurations, SMTP server and click the **SMTP Delivery** tab.
8. Add your archiving system host as a relay server.  
  
Now, email archiving starts.
9. Log into UDP Archiving and click **Message audit** to view the message count.
10. For migration of emails, convert your mails into .pst format using any third-party tools.
11. For import, log into UDP Archiving as admin, navigate to Import and enter details.

**Note:** You must allow the HTTPS service on port 4040 if Kerio Connect is behind firewall.

---

## Chapter 6: Frequently Asked Questions

This section contains the following topics:

---

<a href="#"><u>How to Modify the Host name?</u></a> .....	164
<a href="#"><u>How to Archive historic emails?</u></a> .....	165
<a href="#"><u>Can I increase the storage capacity anytime?</u></a> .....	166
<a href="#"><u>Can I view my archived emails from Web browser?</u></a> .....	167
<a href="#"><u>What type of licenses are required to use UDP Archiving?</u></a> .....	168
<a href="#"><u>Can Windows user credentials help search/recover emails?</u></a> .....	169
<a href="#"><u>Can I archive calendar, tasks, and contacts?</u></a> .....	170

## How to Modify the Host name?

UDP Archiving provides default host name to set up basic [configuration](#) during deployment. For security reasons, super admin must modify the host name after accessing the UDP Archiving Console. The default host name is UDP Archiving.

To customize open command line prompt and enter the following details:

```
# sudo -- sh -c 'echo "example-hostname" > /etc/hostname'

# sudo -- sh -c 'echo "127.0.0.1 example-hostname" >> /etc/hosts'

# sudo invoke-rc.d hostname.sh start

# sudo invoke-rc.d networking force-reload

# sudo invoke-rc.d network-manager force-reload
```

## How to Archive historic emails?

UDP Archiving helps archiving of historic emails using migration and import features. Using migration feature, Super 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 UDP Archiving Console.



## 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.

## What type of licenses are required to use UDP Archiving?

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

## Can Windows user credentials help search/recover emails?

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

## 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.