

# Workshare Protect Routing Agent

---

## Admin Guide

# Table of Contents

Chapter 1: Introduction.....	4
Overview .....	5
About Workshare Protect Routing Agent .....	5
Mail Flow .....	6
Default mail flow .....	6
Adding Protect Server to your mail flow .....	7
Chapter 2: Installation .....	9
Prerequisites.....	9
Software .....	9
Installation Sequence .....	9
1. Ensure all Protect Server machines are ready.....	10
2. Install the Workshare Protect Routing Agent on all Exchange hub transports.....	11
3. Manually enable Workshare Protect Routing Agent (if necessary).....	12
4. Ensure that all Exchange hub transports handle final delivery .....	13
5. Ensure all Protect Servers send email back to Exchange hub transports .....	13
Performing the Installation .....	14
Routing Agent installation on first Exchange hub transport.....	14
Routing Agent installation on subsequent Exchange hub transports.....	22
Uninstalling Workshare Protect Routing Agent.....	22
Upgrading.....	23
Chapter 3: Configuration Options.....	24
Configuration File .....	25
Working with Third Party Transport Agents.....	25
Mail flow .....	25
Configuration.....	26
Restrict Routing Agent to Specified Users .....	30
Changing the Routing Domain.....	30
Whitelist iManage EMM Email Addresses.....	31
Support Exchange Server Journaling .....	31
Chapter 4: Diagnostics and Maintenance.....	33
Enabling/Disabling the Routing Agent.....	33

Logging..... 33  
Performance Counters..... 34

# Chapter 1: Introduction

- *Overview*
- *Mail Flow*

## Overview

The Workshare Protect Routing Agent is a transport hub agent that interfaces Exchange Server with Workshare Protect Server.

Protect Server is a legal data loss prevention (DLP) and metadata removal server. It enables organizations to define and enforce security policies preventing harmful metadata from leaking to the outside world.

## About Workshare Protect Routing Agent

The Routing Agent routes emails to Protect Server for processing before they are delivered to any recipients. This ensures that both internal and external recipients receive the same versions of attachments.

Only emails that match the following criteria are re-routed to Protect Server:

- At least one external recipient; and
- At least one non-image attachment; and
- Not already been cleaned by Protect Server; and
- (configurable) Not been processed by Workshare Protect or other cleaning software. This is determined by the presence of an email header.

The Routing Agent requires Exchange 2010, 2013 or 2016 servers that have the hub transport role.

You can control whose emails get processed by adding their email addresses to a distribution list and specifying that distribution list in the Routing Agent. If you choose to do this, only emails that meet the above criteria AND have been sent by a user from the distribution list will be processed by Protect Server.

This is also useful when testing Protect Server so you can start by processing only emails from a limited group of people.

# Mail Flow

## Default mail flow

In normal Microsoft Exchange environments, servers are configured to deliver mail destined to external recipients to a mail gateway, or in rare cases to perform final delivery based on DNS lookups.

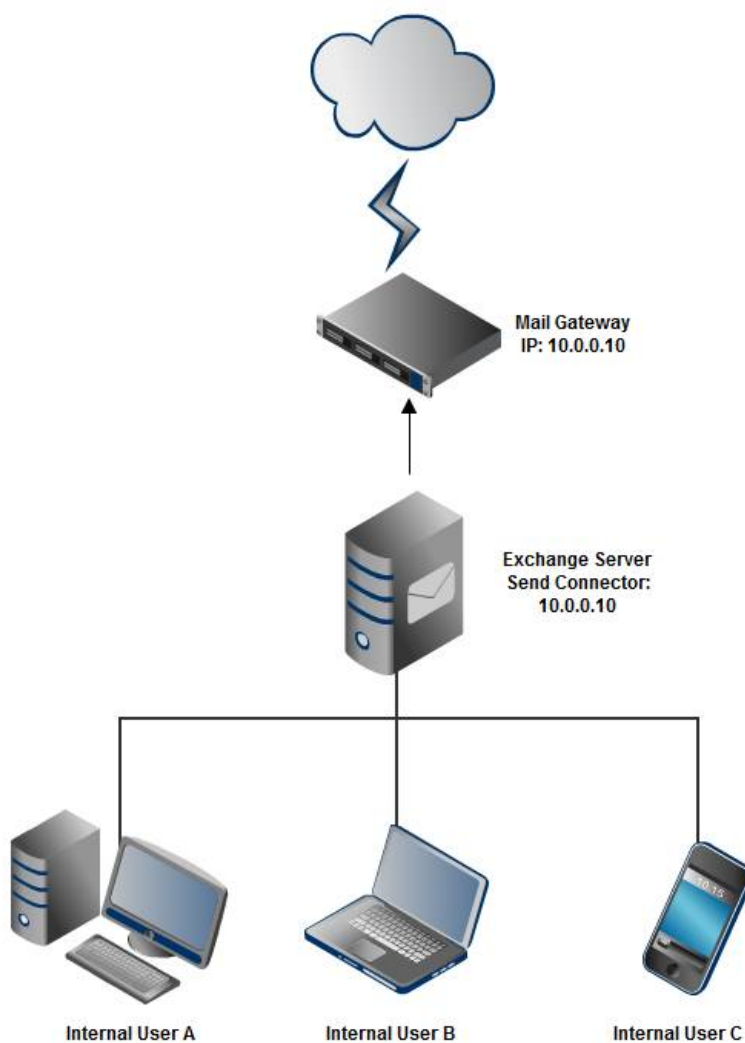
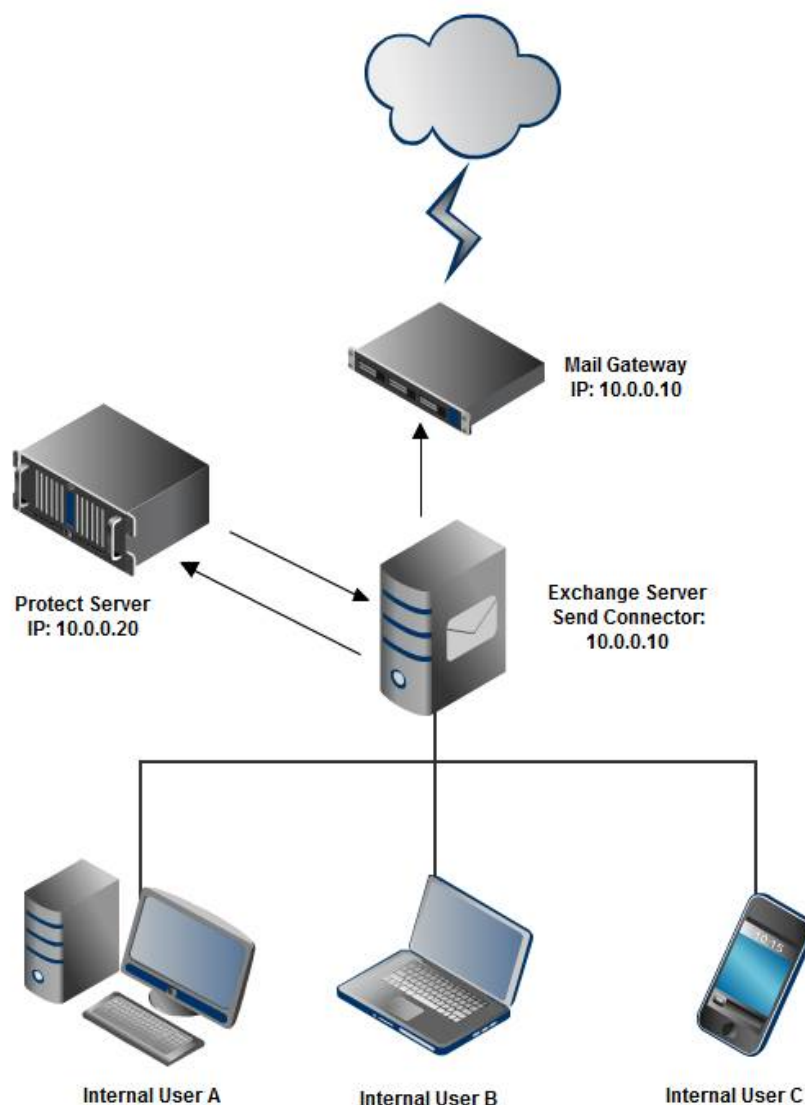


Figure 1: Typical Exchange setup – Exchange server has a send connector configured to send outgoing mail to the mail gateway at 10.0.0.10.

## Adding Protect Server to your mail flow

The mail flow changes when the Protect Routing Agent is installed to route email to Protect Server. Mail matching the routing criteria is routed to Protect Server, which is configured to send traffic back to Exchange after it has processed the mail.

Exchange then does the final routing of the mail, similar to the typical Exchange server setup of Figure 1. This custom routing also ensures that mail coming back from Protect Server does not get re-routed back to Protect Server causing a mail loop.



*Figure 2: Workshare Protect Routing Agent setup – Exchange server's external send connector is configured once again to send outgoing mail to the mail gateway at 10.0.0.10 (same as Figure 1). The Workshare Protect Routing Agent on Exchange will direct mail with attachment(s) and external recipient(s) to Protect Server at 10.0.0.20 by using a special send connector created during the installation of the Protect Routing Agent (network name: workshareprotectserver.com) that points to Protect Server at 10.0.0.20. Protect Server's smart host is configured to point back to Exchange where normal routing of the mail continues.*

The detailed mail flow for the Workshare Protect Routing Agent is as follows:

1. Mail sent by an internal user reaches the Exchange server with the Workshare Protect Routing Agent installed.
2. Before Exchange delivers the mail, it gets processed by the Workshare Protect Routing Agent. If the Routing Agent decides the email should be processed by Protect Server, the Routing Agent will set the routing domain on the email to `workshareprotectserver.com`.
3. The Routing Agent also adds a MIME header to the mail to avoid a mail loop.
4. The email is routed by Exchange via the Workshare Protect send connector (created during installation). The send connector is scoped for "workshareprotectserver.com" emails.
5. Protect Server will receive, inspect and possibly clean or convert the email attachment(s). It will then send the mail back to Exchange for final delivery. Protect Server will need to be configured to route all traffic back to Exchange by setting its SMTP server smart host to Exchange on all domains in IIS Manager.
6. Exchange will receive the mail back from Protect Server. This is allowed by a receive connector created during installation. The Workshare Protect Routing Agent will see that the mail came from Protect Server and allow Exchange to route the mail normally (to the mail gateway for external recipients and into the appropriate mailbox for internal recipients).



## Chapter 2: Installation

- *Prerequisites*
- *Installation Sequence*
- *Performing the Installation*
- *Upgrading*

### Prerequisites

#### Software

The software prerequisites for the Workshare Protect Routing Agent are as follows:

- Microsoft Exchange 2010 SP3 to Microsoft Exchange 2016
- Hub Transport role installed (Exchange 2010) or Mail Server role installed (Exchange 2013 and above)
- Microsoft Exchange Management Shell
- Microsoft .NET Framework 3.5 (for Exchange 2010 SP3), Microsoft .NET Framework 4.0+ (for Exchange 2013 and 2016)
- Workshare Protect Server 3.8 or later, reachable from but not installed on the Microsoft Exchange server

**Note:** *The account used to install the Workshare Protect Routing Agent must have administrative rights in the top level domain to create an Exchange impersonation user account.*

To enable distribution list-based control, a distribution list needs to be created (or already exist) in Microsoft Exchange before install of the Protect Routing Agent. The distribution list must include at least one email address. You must retain the email address of this distribution list for use during the installation procedure.

### Installation Sequence

The sequence described below has been designed to reduce potential down time. This is achieved as follows:

- Each step consists of a small, iterative change to a production environment; expected effects on mail flow are described for each step.
- Each step has a set of tests that can be performed to validate execution.

- Each step can easily be reversed if necessary.

For the purposes of this example sequence, it is assumed that there are no issues with production mail flow prior to installation, and that no previous version of the Workshare Protect Routing Agent is currently installed. Allowances have been made for environments that already have Protect Server in the mail flow so it is not necessary to remove or alter that which is already working.

**Note:** *Upgrades are supported and are described in [Upgrading](#).*

## 1. Ensure all Protect Server machines are ready

<b>Action</b>	<p>Start by installing and configuring the instances of Protect Server. The aim is to have all of them able to process and relay mail for final delivery.</p> <ul style="list-style-type: none"> <li>• Configure the SMTP server on each Protect Server so that: <ul style="list-style-type: none"> <li>▫ All Exchange hub transports may connect to the SMTP server and relay mail.</li> <li>▫ The SMTP server either performs final delivery or forwards mail to the final delivery smart host. <b>Do not configure the Exchange hub transport as the final delivery smart host at this stage.</b></li> <li>▫ Message size limits are consistent with the organization's size limits.</li> </ul> </li> <li>• From the Workshare Protect Server web console, check that bounce settings are as desired. Bounce settings are not shared amongst servers. The bounce settings are also system-wide settings, pre-empting profile settings.</li> </ul>
<b>Impact</b>	<p>There should be no effects on mail flow at this stage – Protect Server is either disconnected or, if connected, it is already configured and changes in configuration are unlikely to be necessary.</p>
<b>Next steps</b>	<p>Test that each Protect Server is able to relay email to internal and external email addresses before proceeding.</p>

## 2. Install the Workshare Protect Routing Agent on all Exchange hub transports

<b>Action</b>	<p>The second step is to install and configure the Workshare Protect Routing Agent software on each Exchange hub transport. An installation wizard will guide you through this process and is described in <i>Performing the Installation</i>.</p> <p>The installation wizard will:</p> <ul style="list-style-type: none"> <li>• Add and (optionally) enable the transport agent “Workshare Protect Routing Agent”.</li> <li>• Add the send connector “Workshare Protect Send Connector” that points to Protect Server. It has a special address space “workshareprotectserver.com”, which is only used internally by the Workshare Protect Routing Agent. <b>Do not change the value of this address space.</b> Also note that if you change the IP address of Protect Server, you must update the smart host of this send connector.</li> <li>• Add the receive connector “Workshare Protect Receive Connector” that allows Protect Server’s IP address the rights to relay mail back into Exchange. By default, this receive connector allows anonymous access from the one IP address. As with the send connector, you must update the allowed IP address if the Protect Server’s IP address changes.</li> <li>• Add a system account with a mailbox used for updating Sent Items. This system account is set up with impersonation rights so the Workshare Protect Server mail updater service can access and update items in users’ Sent Items folders.</li> </ul>
<b>Impact</b>	<p>The installation wizard will perform tests to ensure that the hub transport is able to correctly relay email to nominated Protect Servers. By default, the Workshare Protect Routing Agent is enabled after install. Mail flow will be altered as described in the next section, otherwise, mail flow should not be affected.</p> <p>This will have the following effects on mail flow:</p> <ul style="list-style-type: none"> <li>• There will be momentary down time for Exchange users while the MExchangeTransport service restarts.</li> <li>• After restart, emails that match the Workshare Protect Routing Agent routing criteria will be routed to Protect Server which will handle final delivery for these emails.</li> <li>• Emails that do not match the criteria will be delivered as before.</li> </ul>

### 3. Manually enable Workshare Protect Routing Agent (if necessary)

<b>Action</b>	<p>If the Routing Agent was not enabled after install in step 2, you may enable the Routing Agent with the following commands in the Exchange Management Shell:</p> <pre>Enable-TransportAgent "Workshare Protect Routing Agent" Set-SendConnector "Workshare Protect Send Connector" - enabled \$true Restart-Service MExchangeTransport</pre>
<b>Impact</b>	<p>The installation wizard will perform tests to ensure that the hub transport is able to correctly relay email to nominated Protect Servers. By default, the Workshare Protect Routing Agent is enabled after install. Mail flow will be altered as described in the next section, otherwise, mail flow should not be affected.</p> <p>This will have the following effects on mail flow:</p> <ul style="list-style-type: none"> <li>• There will be momentary down time for Exchange users while the MExchangeTransport service restarts.</li> <li>• After restart, emails that match the Workshare Protect Routing Agent routing criteria will be routed to Protect Server which will handle final delivery for these emails.</li> <li>• Emails that do not match the criteria will be delivered as before.</li> </ul>
<b>Risk mitigation</b>	<p>While this configuration is workable, it is undesirable for the following reasons:</p> <ul style="list-style-type: none"> <li>• Emails to internal recipients may take an inefficient route back to the Exchange mailbox.</li> <li>• Exchange will not have an opportunity to journal the processed version of emails.</li> </ul> <p>If an issue does occur, you may restore the previous mail flow with the following commands in the Exchange Management Shell:</p> <pre>Disable-TransportAgent "Workshare Protect Routing Agent" Set-SendConnector "Workshare Protect Send Connector" - enabled \$false Restart-Service MExchangeTransport</pre>

## 4. Ensure that all Exchange hub transports handle final delivery

<b>Action</b>	<p>Prepare Exchange hub transports for mail delivery of items that will be relayed back from Protect Server in the next step.</p> <ul style="list-style-type: none"> <li>• Ensure each Exchange hub transport has a send connector handling final delivery for emails not scoped to “workshareprotect.com”.</li> <li>• Ensure that only the “Workshare Protect Send Connector” has its smart host set to Protect Server by removing or disabling any other send connectors pointing to Protect Server.</li> </ul>
<b>Impact</b>	<p>The mail flow will change if all mail was previously routed through Protect Server; now only items matching the routing criteria will be relayed to Protect Server. You may test your changes by sending an email without attachment to an external recipient. Check the email headers on the recipient’s copy of the email. Protect Server machines should not appear in the “Received by” headers.</p>

## 5. Ensure all Protect Servers send email back to Exchange hub transports

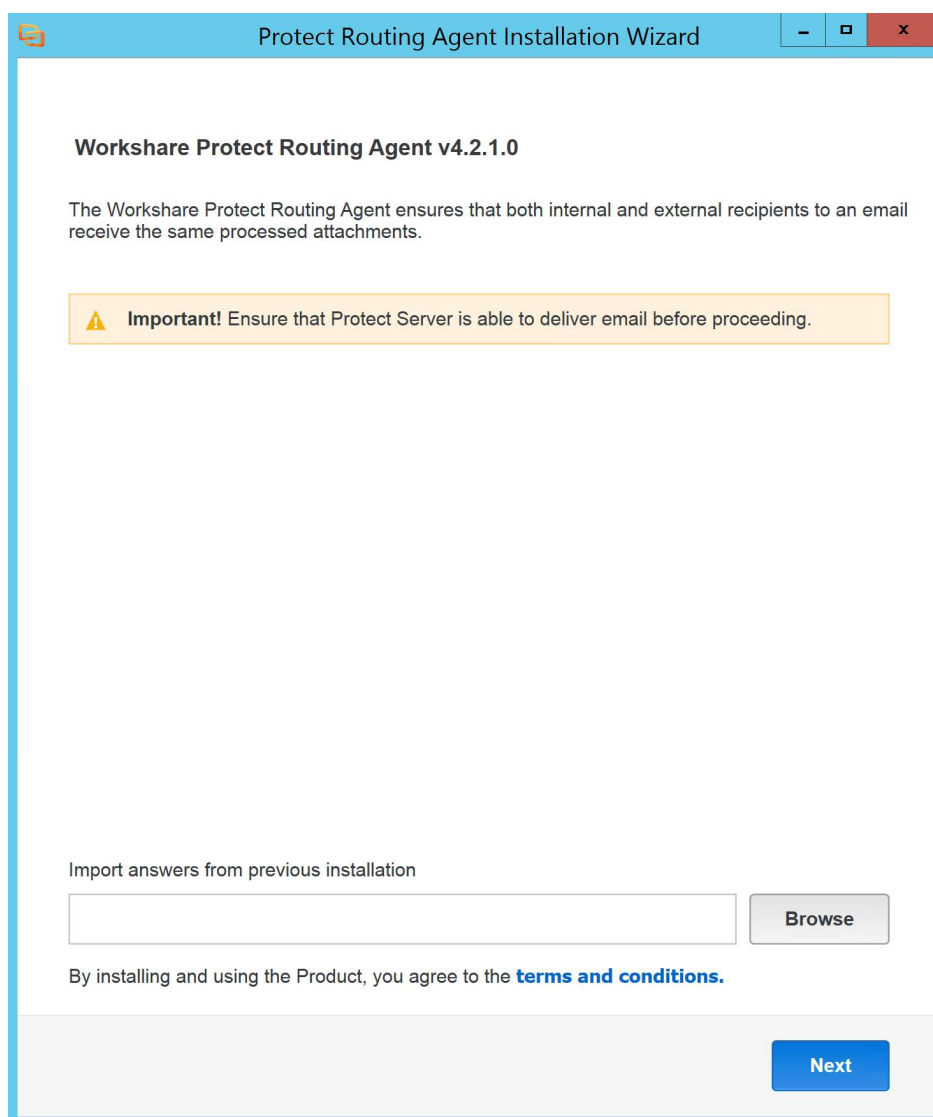
<b>Action</b>	<p>Complete installation by configuring each Protect Server’s smart host to the Exchange hub transports. This will route all emails back to Exchange after being processed by Protect Server.</p>
<b>Impact</b>	<p>Test that emails containing attachments to internal and external recipients are processed by Protect Server as follows:</p> <ul style="list-style-type: none"> <li>• Emails should appear as processed in message logs.</li> <li>• Internal and external recipients should receive the same processed email.</li> </ul>

## Performing the Installation

You will have two executables for installing Workshare Protect Routing Agent – one for Exchange 2010 and one for Exchange 2013/2016.

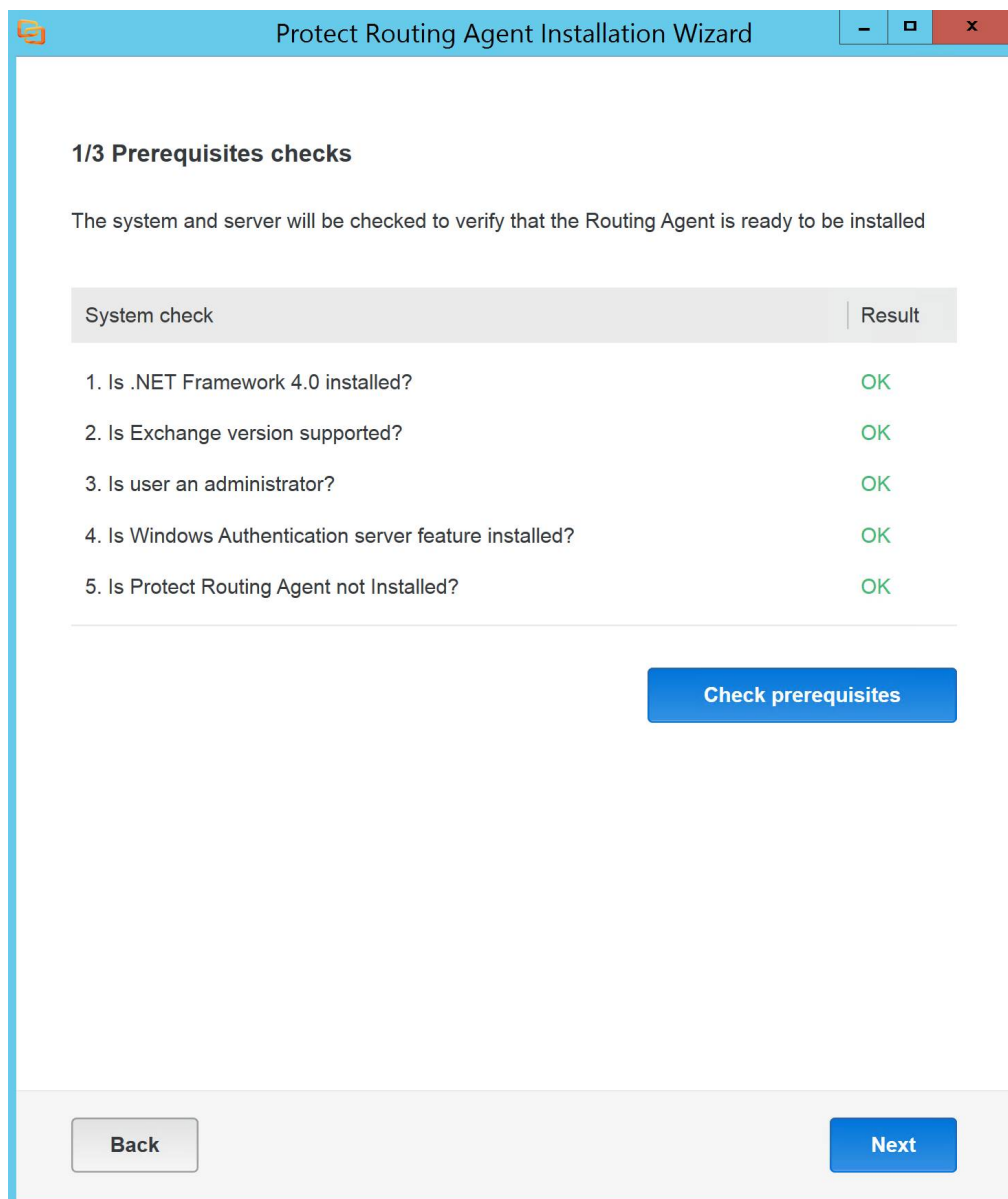
### Routing Agent installation on first Exchange hub transport

1. Run the relevant Workshare Protect Routing Agent setup executable for your environment.



Once the Installation Wizard has loaded, the screen above will appear, providing an opportunity to import an answer file from a previous installation.

2. Click **Next**.



The Prerequisites checks screen shows the necessary prerequisites required before installation can proceed.

**Note:** The screen may vary slightly according to your version of Exchange.

3. Click **Check prerequisites** to check if it is okay to start installation.

- Once all results are **OK**, click **Next** to proceed.

### 2/3 Routing Agent configuration

---

Enable Protect Routing Agent

---

Install location

---

Protect server IP address(es)

---

Create Workshare Receive Connector

Mail connector maximum email size

---

Enable Impersonation user creation

Impersonation user name

Impersonation user domain

Impersonation user password

Confirm password

Mailbox database

---

Protected Senders Distribution List

Internal addresses

---

Client Message Processing

Skip processing on messages processed by Workshare Protect Client

Skip processing on messages processed by Payne Metadata Assistant

---

Enable Third Party Distribution List Resolution

---

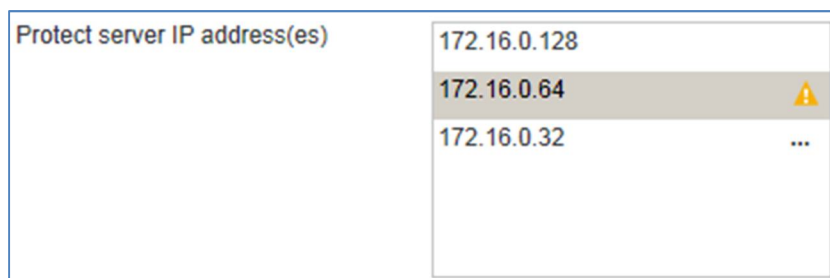


The Routing Agent configuration screen provides the ability to set the configuration of the Routing Agent prior to installation.

5. Specify options as explained below:

Option	Description
<b>Enable Protect Routing Agent</b>	<p>Determines whether the transport agent in the Protect Routing Agent is enabled in Exchange immediately after installation.</p> <p>Default: Selected</p> <div style="border: 1px solid orange; padding: 5px; margin-top: 10px;"> <p><b>WARNING:</b> When the transport agent is enabled immediately after installation, this will add Protect Server to the mail flow and cause a restart of the Microsoft Exchange Transport service.</p> </div>
<b>Install location</b>	<p>The install location of the Routing Agent software.</p> <p>Default: %PROGRAMFILES%\Workshare\Protect for Exchange</p>
<b>Protect server IP address(es)</b>	<p>IP addresses for this Exchange hub transport to send mail to.</p> <p>The installation wizard will validate these IP addresses.</p>

6. Wait for the Installation Wizard to validate connectivity with the nominated Protect Server machines.



In the above example:

- Email was successfully relayed to Workshare Protect Server at 172.16.0.128.
- Email could not be relayed to Workshare Protect Server at 172.16.0.64. An error message can be viewed by hovering over the warning icon.
- Connectivity to Workshare Protect Server 172.16.0.32 is currently being validated.

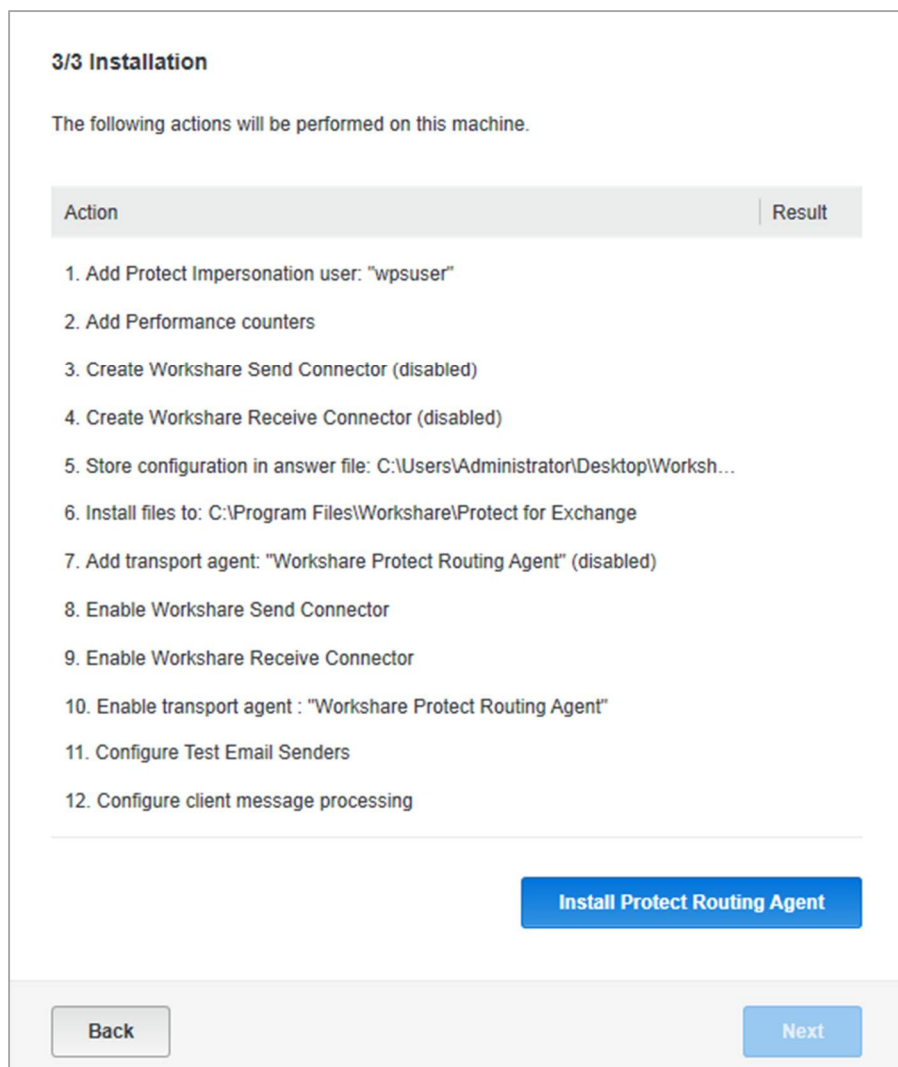
## 7. Continue specifying options as follows:

Option	Description
<b>Create Workshare Receive Connector</b>	Determines whether the installer creates receive connectors for the Protect Server IP addresses. The receive connectors allow Protect Server to send emails back through Exchange, for example user notifications such as clean receipts.
<b>Mail connector maximum email size</b>	The email size limit for both send and receive connectors. You must specify the same limit that you have set in Exchange. Look <a href="#">here</a> for a description of where to set email size limits. Default: 25MB
<b>Enable Impersonation user creation</b>	Determines whether the installer attempts to create an impersonation user to be used by the Workshare Protect Server mail updater feature. This only needs to be created once per network. Default: Selected
<b>Impersonation user name</b>	User name (alias) of the new impersonation user. You can change the default name to match your company's Active Directory policy. Default: wpsuser
<b>Impersonation user domain</b>	Domain of the new impersonation user.
<b>Impersonation user password</b>	Password of the new impersonation user. The password policy must match your company's Active Directory security policy.
<b>Confirm password</b>	Verify the new password for the new impersonation user.
<b>Mailbox database</b>	Mailbox database that will host the new impersonation user. By default, the Routing Agent will use the mailbox with the highest index. Select your preferred database.
<b>Protected Senders Distribution List</b>	The email address of the distribution list referenced on page 9. The Routing Agent will only route emails sent by the mailboxes included in this distribution list to Workshare Protect Server. Mail flow will be unaffected for all other senders. Adding a non-existent email address disables the Protect Server infrastructure from the mail flow. See also: <a href="#">Restrict Routing Agent to Specified Users</a> .

---

Option	Description
<b>Internal addresses</b>	If set, the Routing Agent will only consider recipients matching this pattern as an internal recipient. Use a comma or semicolon separated list of regular expressions. For example, <i>*@dms1.example.com</i> , <i>*@dms2.example.com</i> See also: <i>Whitelist iManage EMM Email Addresses</i> .
<b>Skip processing on messages processed by Workshare Protect Client</b>	If selected, the Routing Agent will not route emails previously processed by the Workshare Protect client to Workshare Protect Server.
<b>Skip processing on messages processed by Payne Metadata Assistant</b>	If selected, the Routing Agent will not route emails previously processed by Payne Metadata Assistant to Workshare Protect Server.
<b>Enable Third Party Distribution List Resolution</b>	This is a client-specific option. Please leave unselected.

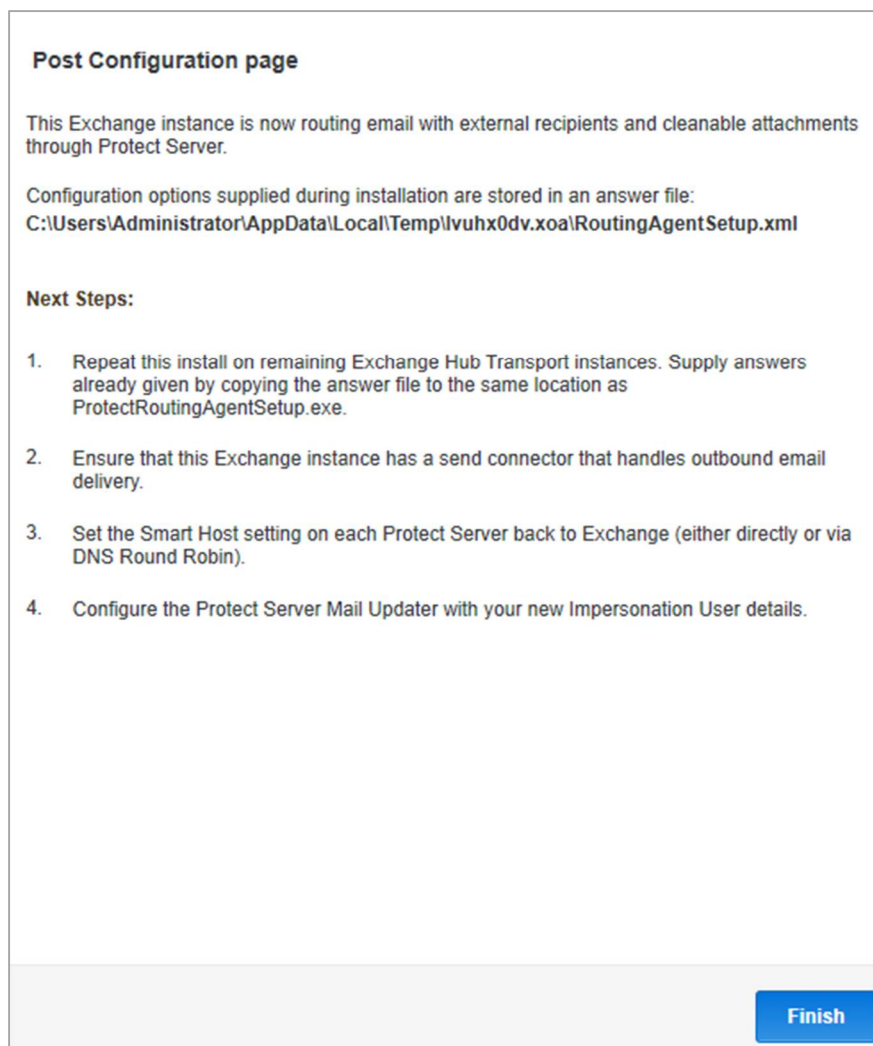
- Click **Next** to proceed to the Installation screen.



The Installation screen allows administrators to review the steps that the Installation Wizard will perform before beginning an install.

- Review that these actions are in line with expectations, and click **Install Protect Routing Agent**.

10. Review the results of the installation. Click **Next** to proceed.



On the Post Configuration page, you can see the location of an answer file containing the answers provided during this installation. Clicking on the link will open an Explorer window at the location of the file. Retain this file for use in future installations.

This page also contains the post configuration steps to perform (as described in *Installation Sequence*) to complete the Routing Agent installation.

11. Click **Finish** to complete installation.

---

## Routing Agent installation on subsequent Exchange hub transports

1. Run the relevant Workshare Protect Routing Agent setup executable for your environment.
2. Click **Browse**, locate and select the answer file created during the first installation.
3. Click **Next** to go to the next screen.
4. On the Prerequisites checks screen, click **Check prerequisites** to confirm the Exchange hub transport has the necessary prerequisites.
5. Click **Next** to proceed once all results are **OK**.
6. The Routing Agent configuration screen should already be pre-populated with the values from the first install. Wait for the installation wizard to confirm connectivity to Protect Server.
7. Review that settings are in line with expectations, and click **Next** to continue to the Installation screen.
8. As before, review the actions the installation wizard will perform are in line with expectations. Click **Install Protect Routing Agent**.
9. Click **Next** to go to the Post Configuration page.
10. Click **Finish** to complete the installation.

## Uninstalling Workshare Protect Routing Agent

### To uninstall the Routing Agent:

1. Navigate to the install location for the Workshare Protect Routing Agent (default: C:\Program Files\Workshare\Protect for Exchange).
2. Navigate to the scripts folder.
3. Right-click **Uninstall-RoutingAgent.ps1**
4. Select **Run with Powershell**.

## Upgrading

The Routing Agent can be upgraded to the latest version without having to uninstall the previous version.

### To upgrade the Routing Agent:

1. Back up the “Workshare.ProtectServer.Exchange.dll.config” file. The upgrade script will read this file and ensure settings are migrated sensibly.
2. Download the Routing Agent install exe appropriate for your Exchange version (for example, WorkshareProtectRoutingAgent2010-v.v.v.v.exe or WorkshareProtectRoutingAgent2013OrGreater-v.v.v.v.exe).
3. If this file was downloaded from the internet, ensure that Windows has not blocked access to this file. Right click the .exe file, and view its properties. In the General tab, click the Unblock button if it is present.
4. Extract this zip file to disk.
5. Open a command window as administrator, and navigate to the “scripts” folder that you have just extracted.
6. Run powershell .\Upgrade-RoutingAgent.ps1.
7. When the upgrade is complete, compare the “Workshare.ProtectServer.Exchange.dll.config” file with your backup to confirm settings have been applied correctly.

**Note:** *The MExchangeTransport service will be restarted during upgrade. Existing receive and send connectors are not modified.*

## Chapter 3: Configuration Options

- *Configuration File*
- *Working with Third Party Transport Agents*
- *Restrict Routing Agent to Specified Users*
- *Changing the Routing Domain*
- *Whitelist iManage EMM Email Addresses*
- *Support Exchange Server Journaling*



## Configuration File

Configuration of the Workshare Protect Routing Agent is via the configuration file:

- **Workshare.ProtectServer.Exchange.dll.config**

This is located, by default, at C:\Program Files\Workshare\Protect for Exchange.

You do not need to restart MExchangeTransport service to apply changes.

## Working with Third Party Transport Agents

Workshare Protect Server enforces the metadata policies of an organization on all outgoing mail. This means where an email has internal and external recipients, the internal recipients may receive one version of an attachment and the external recipients may receive a different cleaned version of an attachment.

To ensure that both internal and external recipients will receive the same attachment, the Protect Routing Agent routes all emails that include an external recipient to Protect Server.

When there are other transport agents installed on Exchange, they may disrupt the role of the Protect Routing Agent.

For example, Exclaimer is an Exchange transport agent that adds a legal disclaimer to outbound emails. If an email is addressed to multiple recipients, Exclaimer can be configured to add a disclaimer for some recipients but not for others. When this happens, Exclaimer bifurcates the email. In mail processing, Exchange forks the original email into two emails - one with a disclaimer, and one without. This could cause confusion as the Protect Routing Agent processes these emails one at a time. It cannot know what the original recipient list was, so internal and external recipients may not receive the same versions of attachments.

## Mail flow

Exchange transport agents are ranked by priority and transport agents with a higher priority run before transport agents with a lower priority. Additionally, the Exchange transport pipeline has multiple stages and transport agents may perform actions at different times during this process. So even if the Protect Routing Agent has the highest priority, this does not ensure it will be able to process the emails correctly.

For example, where the Protect Routing Agent has a priority of 1 and the Exclaimer Routing Agent has a priority of 2, Exchange mail processing will occur in the following order:

- Protect Routing Agent process the "OnSubmitted" event
- Exclaimer Routing Agent process the "OnSubmitted" event
- Protect Routing Agent processes the "OnResolved" event
- Exclaimer Routing Agent process the "OnResolved" event

By default, the Protect Routing Agent determines if an email is internal or external during the OnResolved event by looking at the recipients. However, the original email may have been bifurcated by Exclaimer in the OnSubmitted event. When this happens, the full recipient list is not available. Without the full list, the Protect Routing Agent cannot reliably determine if one of the recipients is external and whether the email should be sent to Protect Server for cleaning.

There are two possible ways to ensure emails are routed to Protect Server correctly:

- **Third party transport agent pre-emption**

The Protect Routing Agent can check the email recipients before any other transport agents fork the email. This must be done during the Exchange OnSubmitted event. During this stage of processing, Exchange has not resolved the members of distribution lists, so the Protect Routing Agent must check each recipient, including those in distribution lists, to see if they are internal or external. To use pre-emption, the Routing Agent must be configured to resolve email addresses with Active Directory. Refer to [ResolveWithActiveDirectory](#).

**Note:** You can specify whether a distribution list is external or internal to avoid large distribution lists impacting performance. Refer to [PreresolvedInternalDistList/PreresolvedExternalDistList](#).

The Protect Routing Agent must have the highest Exchange transport agent priority for pre-emption to work.

- **Third party transport agent cooperation**

If the third party transport agent supports this, a header is set in the email which indicates to the Protect Routing Agent that the email should be treated as an internal or external email. This is not a feature that Exclaimer supports. Refer to [RoutingOverrideHeader](#).

## Configuration

To configure the Protect Routing Agent to resolve email addresses or set a routing override header, you modify the Workshare.ProtectServer.Exchange.dll.config file.

```
<configuration>

  <!-- ... -->

  <applicationSettings>
    <Workshare.ProtectServer.Exchange.Properties.Settings>

    <!-- ... -->
```

```

<setting name="RoutingOverrideHeader" serializeAs="String">
  <value>x-wps-routingoverride</value>
</setting>

<setting name="ResolveSettings" serializeAs="Xml">
  <value>
    <ResolveSettings xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <ResolveWithActiveDirectory>false</ResolveWithActiveDirectory>
      <PreresolvedInternalDistList></PreresolvedInternalDistList>
      <PreresolvedExternalDistList></PreresolvedExternalDistList>
      <PreresolvedExpiryTimeMinutes>60</PreresolvedExpiryTimeMinutes>
    </ResolveSettings>
  </value>
</setting>
<setting name="ProtectedSenderDistributionList"
serializeAs="String">
  <value></value>
</setting>
</Workshare.ProtectServer.Exchange.Properties.Settings>
</applicationSettings>
</configuration>

```

## RoutingOverrideHeader

The default RoutingOverrideHeader is named **x-wps-routingoverride**. This header is inserted into emails by the Protect Routing Agent once it has resolved the email address. It is given a value of internal or external.

For third party transport agent cooperation, the third party transport agent inserts this header into emails with a value of internal or external.

You can change the default name but the `RoutingOverrideHeader` must have a value of `internal` or `external`. Once this header is present, the Routing Agent will route the email as follows:

Value	Routing
Internal	Email is treated as internal. Overrides all other checks.
External	Email is treated as external. Overrides all other checks.
Other/not present	No change to existing behavior.

## ResolveWithActiveDirectory

In order for the Protect Routing Agent to resolve email recipients during the Exchange `OnSubmitted` event (before any other transport agents fork the email) `ResolveWithActiveDirectory` must have the value **true**.

Value	Behavior
True	Query Active Directory to determine if all recipients have a mailbox account. Recurse through distribution lists. This check is performed during the <code>OnSubmitted</code> event. Assuming that the Protect Routing Agent has a priority of 1, this check will occur before any other transport agent processes the email.
False (default)	Do not check Active Directory.

## PreresolvedInternalDistList/PreresolvedExternalDistList

To avoid large distribution lists impacting performance, you can specify whether a distribution list is external or internal.

The values for the `PreresolvedInternalDistList` or `PreresolvedExternalDistList` settings are distribution group email addresses.

If a distribution list is added to one of these settings, then only the distribution list is overridden. Members of the distribution list are not overridden.

For example:

`_legalteam@mintonslaw.com` is the email address of a distribution list with the following members:

- `elizabeth.morris@mintonslaw.com`
- `jonas.herzog@mintonslaw.com`
- `anna.wood@mintonslaw.com`
- `_itteam@mintonslaw.com` (a distribution list that includes `nick.phillips@mintonslaw.com` and `ahmed.fares@mintonslaw.com`)

If `PreresolvedInternalDistList` is set as follows:

```
<PreresolvedInternalDistList> _legalteam@mintonslaw.com</PreresolvedInternalDistList>
```

The Routing Agent will route emails as follows:

Email to:	Routing
_legalteam@mintonslaw.com	Treated as an internal email address. No Active Directory lookup performed. Email not sent to Protect Server.
anna.wood@mintonslaw.com	Treated as an internal email address. No Active Directory lookup performed. Email not sent to Protect Server.
ahmed.fares@mintonlaw.com	This address has not been preresolved so Active Directory lookup is performed to determine if email address is internal or external.

If an email address appears in both `PreresolvedInternalDistList` and `PreresolvedExternalDistList` then that email address is considered to be external.

**Note:** If `<ResolveWithActiveDirectory>` is false, the Protect Routing Agent will use the resolved recipient list from Exchange, which does not contain distribution lists.

## PreresolvedExpiryTimeMinutes

This setting determines how often the preresolved distribution lists are refreshed. The default setting is 60 minutes.

The members of `<PreresolvedInternalDistList>` and `<PreresolvedExternalDistList>` are cached in memory.

## Restrict Routing Agent to Specified Users

You can restrict the Routing Agent to specified senders. This can allow for testing, for example, so you can try the Routing Agent on a small sample set before turning it on for the whole organization.

### To limit the Routing Agent to one or more senders:

Add the test email addresses to the distribution list set up before installation of the Routing Agent (see page 9). If you don't specify the email address of this distribution list during installation (see page 18), edit the config file as follows:

Find `ProtectedSenderDistributionList` and set a value, for example:

```
<setting name="ProtectedSenderDistributionList" serializeAs="String">  
  <value>protectedsendeer@domain</value>
```

If there is no value for `ProtectedSenderDistributionList` or if the distribution list specified is an empty distribution list, a mailbox or doesn't exist, then all email is routed to Protect Server.

**Note:** *Of course the Routing Agent only routes emails to Protect Server when they include external recipients and attachments, and have not already been cleaned.*

By default, the protected sender distribution list cache is updated every minute so you can add a user to the protected sender distribution list and after a minute relevant emails sent by the user will be forwarded to Protect Server. If you want to change this cache update:

Find `ProtectedSenderDistributionListCachePeriodMinutes` and change the value.

## Changing the Routing Domain

By default, the installation of the Protect Routing Agent creates a send connector with the routing domain `workshareprotectserver.com`. If you want to change this routing domain:

Find `WorkshareRoutingDomain` and change the value.

If you change the default setting, you **must** modify the send connector on Exchange. The value for the `WorkshareRoutingDomain` setting and the send connector address space setting must match.

## Whitelist iManage EMM Email Addresses

The whitelist feature supports iManage EMM filing emails functionality ensuring that Protect Server treats the EMM email addresses as internal.

### To whitelist email addresses:

In the Routing Agent configuration file enter the domain part of the email address used by the EMM module to indicate that a message should be filed. The Routing Agent configuration file is: `Workshare.ProtectServer.Exchange.dll.config` (C:\Program Files\Workshare\Protect for Exchange).

At node: `AdditionalInternalAddresses`

Example:

```
<setting name="AdditionalInternalAddresses" serializeAs="String">
  <value>*@dms.emmfiling.com</value>
</setting>
```

This setting ensures that any email address ending `@dms.emmfiling.com` is treated as internal by the Workshare Protect Routing Agent and is not passed to Protect Server for cleaning.

## Support Exchange Server Journaling

The journaling feature reduces the number of emails journaled by Exchange when the Workshare Protect Routing Agent is installed. It is configured by 4 settings in the Routing Agent configuration file: `Workshare.ProtectServer.Exchange.dll.config` (C:\Program Files\Workshare\Protect for Exchange).

- **AllowJournalsOfEmailsFromProtectServer** – Boolean (True/False). When set to True, this will journal emails returning from Workshare Protect Server. The default is False.
- **AllowJournalsOfEmailsToProtectServer** – Boolean (True/False). When set to True, this will journal emails as they are going to Workshare Protect Server. The default is True.
- **AvoidCleanReportJournals** – Boolean (True/False). When set to True, the Workshare Protect Routing Agent ensures cleaning reports sent from Workshare Protect Server are not included in Exchange journaling.
- **AvoidBifurcatedJournals** – Boolean (True/False). When set to True, the Workshare Protect Routing Agent ensures emails that are bifurcated by Exchange before being processed by Workshare Protect Server will only generate a single Exchange journal entry.

**Example:**

```
<setting name="AllowJournalsOfEmailsFromProtectServer"
serializeAs="String">
<value>False</value>
</setting>
<setting name="AllowJournalsOfEmailsToProtectServer" serializeAs=
"String">
<value>True</value>
</setting>
<setting name="AvoidCleanReportJournals" serializeAs="String">
<value>True</value>
</setting>
<setting name="AvoidBifurcatedJournals" serializeAs="String">
<value>False</value>
</setting>
```



## Chapter 4: Diagnostics and Maintenance

- *Enabling/Disabling the Routing Agent*
- *Logging*
- *Performance Counters*

### Enabling/Disabling the Routing Agent

The Workshare Protect Routing Agent has been designed to be easily enabled and disabled. All changes in the normal Microsoft Exchange mail flow are performed in the Workshare Protect Routing Agent. Simply disabling the Routing Agent will return the Exchange mail flow from a scenario similar to Figure 2 (page 7) to Figure 1 (page 6), bypassing Workshare Protect Server and performing normal routing on all mail.

The easiest way to enable and disable the Routing Agent is by using Exchange Management Shell cmdlets:

```
Disable-TransportAgent "Workshare Protect Routing Agent"  
Enable-TransportAgent "Workshare Protect Routing Agent"
```

To view all transport agents and their current status run the following cmdlet:

```
Get-TransportAgent
```

Disabling the Workshare Protect Routing Agent can be useful when doing maintenance or upgrades to Protect Server or troubleshooting mail flow problems for example.

### Logging

By default, the Workshare Protect Routing Agent logs to the following locations:

- Windows Event Application Logs (see "Protect Server" event source)
- C:\Program Files\Workshare\Protect for Exchange\logs\wps-routing-agent.log

By default, log files do not exceed 1MB. Best effort is made to keep a maximum of 20 log files.

You may modify logging by modifying the following section in the logging.config file. The default location of this file is "C:\Program Files\Workshare\Protect for Exchange".

```

<add name="Rolling Flat File Trace Listener"
type="Microsoft.Practices.EnterpriseLibrary.Logging.TraceListeners
.RollingFlatFileTraceListener,
Microsoft.Practices.EnterpriseLibrary.Logging, Version=5.0.414.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35"
listenerDataType="Microsoft.Practices.EnterpriseLibrary.Logging.Co
nfiguration.RollingFlatFileTraceListenerData,
Microsoft.Practices.EnterpriseLibrary.Logging, Version=5.0.414.0,
Culture=neutral, PublicKeyToken=31bf3856ad364e35"
      fileName="C:\Program Files\Workshare\Protect for
Exchange\logs\wps-routing-agent.log"
      footer=""
      formatter="complete details"
      header=""
      rollFileExistsBehavior="Increment"
      rollInterval="None"
      rollSizeKB="1024"
      maxArchivedFiles="20"
      timeStampPattern="yyyy-MM-dd"
      traceOutputOptions="None"
      filter="Information" />


```

## Performance Counters

The following performance counters have been added.

Counter Category: "Workshare Protect Server for Exchange Counters"

Counter Name	Counter Description
Errors encountered in Protect Server Transport Agent	The number of unexpected errors encountered in Workshare Protect Routing Agent
Messages routed to Protect Server	The number of messages routed to Protect Server for processing from the OnRoutedMessage event
Messages received in OnRoutedMessage event	The number of messages entering the OnRoutedMessage event
Messages received in OnSubmittedMessage event	The number of messages entering the OnSubmittedMessage event

 Workshare Ltd.

© 2018. Workshare Ltd. All rights reserved.

#### **Copyright**

Workshare Professional and Workshare DeltaView are registered trademarks of Workshare Ltd. Workshare Compare, Workshare Protect, Workshare 3, Workshare DeltaServer, SafetyGain, and the Workshare logo are trademarks of Workshare Ltd. All other trademarks are those of their respective holders.

Trademarked names may appear throughout this guide. Instead of listing these here or inserting numerous trademark symbols, Workshare wishes to state categorically that no infringement of intellectual or other copyright is intended and that trademarks are used only for editorial purposes.

#### **Disclaimer**

The authors/publishers of this guide and any associated help material have used their best efforts to ensure accuracy and effectiveness. Due to the continuing nature of software development, it may be necessary to distribute updated help from time to time. The authors would like to assure users of their continued best efforts in supplying the most effective help material possible.

The authors/publishers, however, make no warranty of any kind, expressed or implied, with regard to Workshare programs or help material associated with them, including this guide. The authors/publishers shall not be liable in the event of incidental or consequential damages in connection with, or arising out of, the programs or associated help instructions.

For details of Workshare patents, see [www.workshare.com/patents](http://www.workshare.com/patents)

#### **Revisions**

Published for Workshare Protect Routing Agent 4.0: 5/10/17

Revised for Workshare Protect Routing Agent 4.1: 16/11/17

Revised for Workshare Protect Routing Agent 4.2: 25/4/18

Revised for Workshare Protect Routing Agent 4.2.1: 6/7/19

Workshare Ltd., 20 Fashion Street, London E1 6PX [www.workshare.com](http://www.workshare.com)