

WORKSHARE PROTECT SERVER 3.2

ROUTING AGENT ADMIN GUIDE



COMPANY INFORMATION

Workshare Protect Server Routing Agent Admin Guide

Workshare Ltd. (UK)
20 Fashion Street
London
E1 6PX
UK

Workshare Inc. (USA)
625 Market Street, 15th Floor
San Francisco
CA 94105
USA

Workshare Website: www.workshare.com

Trademarks

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.

Disclaimers

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.

Copyright

© 2015. Workshare Ltd. All rights reserved. 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.

Sold under a license for U.S. Patent Nos. 7,895,276 and 8,060,575 and 8,977,697.

TABLE OF CONTENTS

Overview	4
Mail Flow	5
Installation	8
Prerequisites	8
Preparation	9
Installation Steps	9
Manual Installation for a Single Exchange Server	9
Manual Installation for Multiple Exchange Servers	11
Upgrades	11
Diagnostics/Maintenance	11
Enabling/Disabling	11
Logging	11
Performance Counters	12
Configuration Options	12
Restrict Routing Agent to Specified Users	12
Whitelist Autonomy iManage EMM Email Addresses	13
Support Exchange Server Journaling	14

OVERVIEW

Workshare Protect Server enables organizations to define and enforce security policies preventing harmful metadata from leaking to the outside world. Workshare Protect Server is designed to work well with all mail servers, including Microsoft Exchange environments, without the need to install additional components on the mail servers themselves.

Workshare Protect Routing Agent is an optional lightweight add-on to Microsoft Exchange Server 2007/2010/2013 that extends this core functionality. This add-on is useful for organizations that want to ensure that internal recipients as well as the sender always have access to the same version of attachments that are received by external recipients.

The Workshare Protect Server Routing Agent provides the following function:

- For all emails sent from within the organization containing both internal and external recipients and at least one attachment, the add-on will direct them to Workshare Protect Server before they are delivered to any recipients. This ensures that both internal and external recipients receive the same versions of attachments.

Workshare Protect Routing Agent is installed on Microsoft Exchange 2007/2010/2013 servers with the Hub Transport role. It is a simple transport agent designed to do as little work as possible; its only role is to change routing and direct mail to and from Workshare Protect Server.

MAIL FLOW

In normal Microsoft Exchange environments, servers are configured to deliver mail destined to external recipients to a mail gateway (see Figure 1 below), or in rare cases to perform final delivery based on DNS lookups.

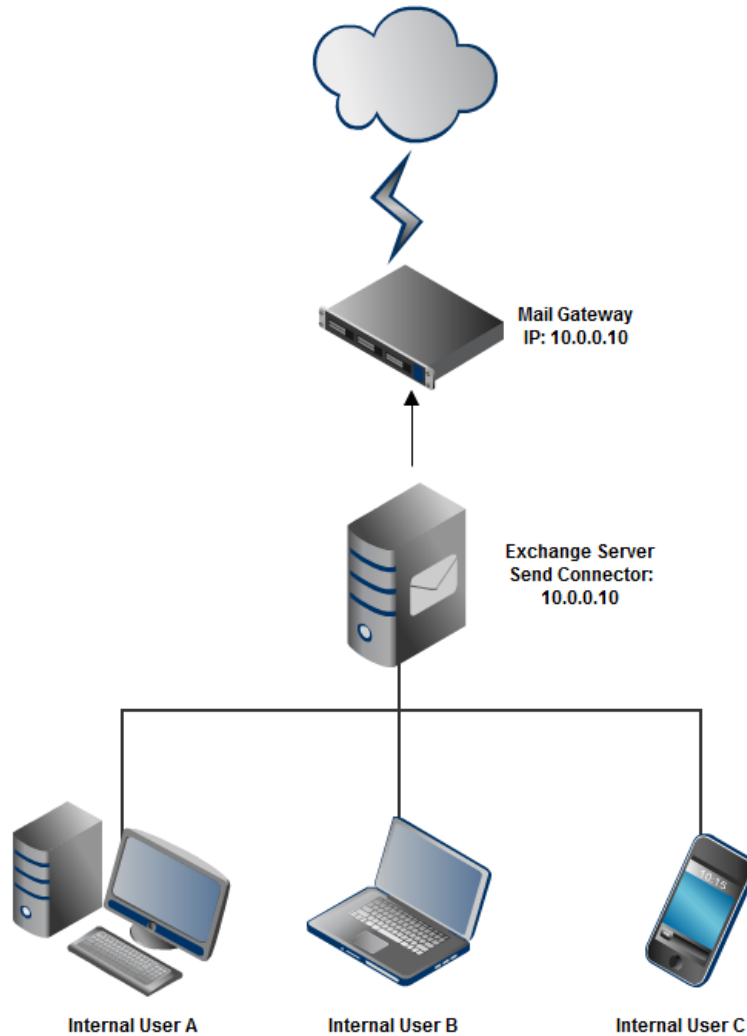


Figure 1: Typical Microsoft Exchange setup – Microsoft Exchange Server has a Send Connector configured to send outgoing mail to the Mail Gateway at 10.0.0.10.

When Workshare Protect Server is installed within an organization, typically it will be placed between the mail server(s) and the mail gateway as an MTA (see Figure 2 below). This allows Workshare Protect Server to enforce the metadata policies of the organization on all outgoing mail.

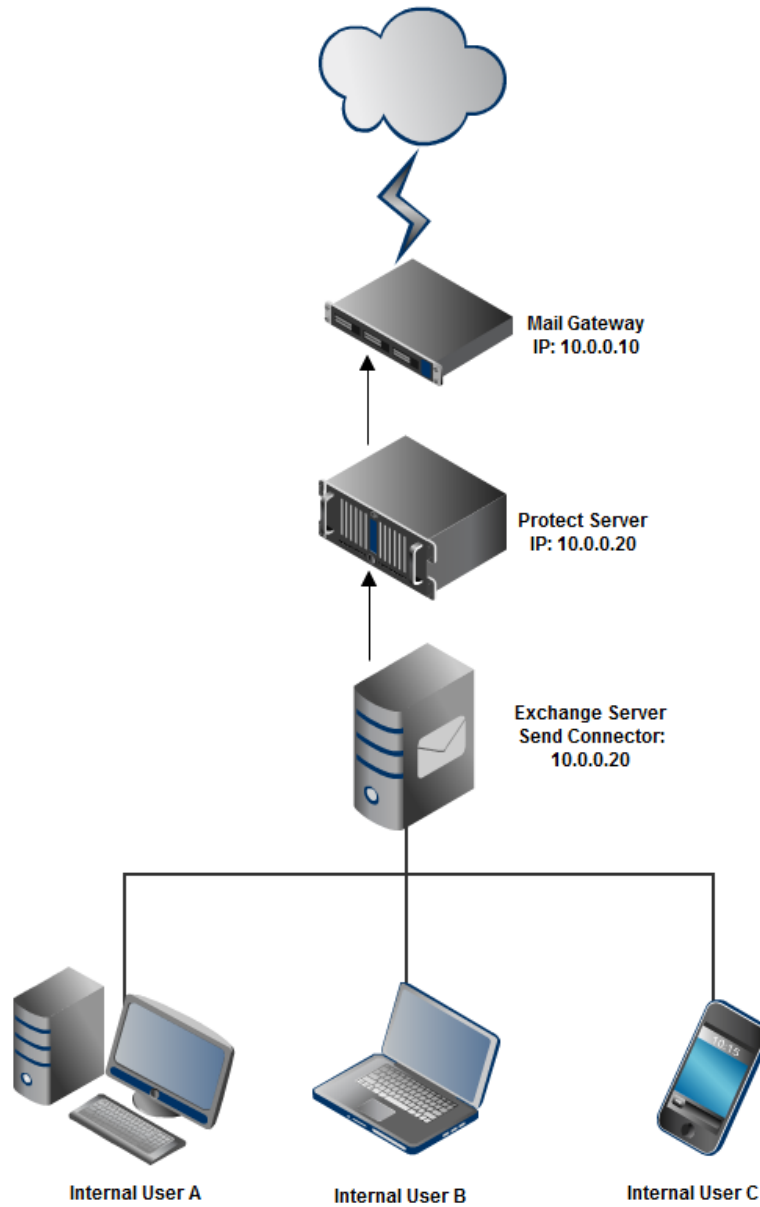


Figure 2: Typical Microsoft Exchange-Workshare Protect Server setup – Microsoft Exchange Server’s external Send Connector is now configured to send outgoing mail to the Workshare Protect Server at 10.0.0.20. Workshare Protect Server will send all traffic to the original Mail Gateway at 10.0.0.10.

The mail flow changes when the Workshare Protect Server Routing Agent is installed. In this scenario, Workshare Protect Server is no longer situated between Microsoft Exchange Server and the mail gateway. Instead, mail containing one or more attachments and one or more external recipients is routed to Workshare Protect Server. Workshare Protect Server is configured to send traffic back to Microsoft Exchange Server after it has processed the mail. Microsoft Exchange Server then does the final routing of the mail, similar to the typical Microsoft Exchange Server setup of Figure 1. This custom routing is performed by the Workshare Protect Routing Agent (a transport agent) on Microsoft Exchange Server and it also ensures that mail coming back from Workshare Protect Server does not get re-routed back to Workshare Protect Server causing a mail loop.

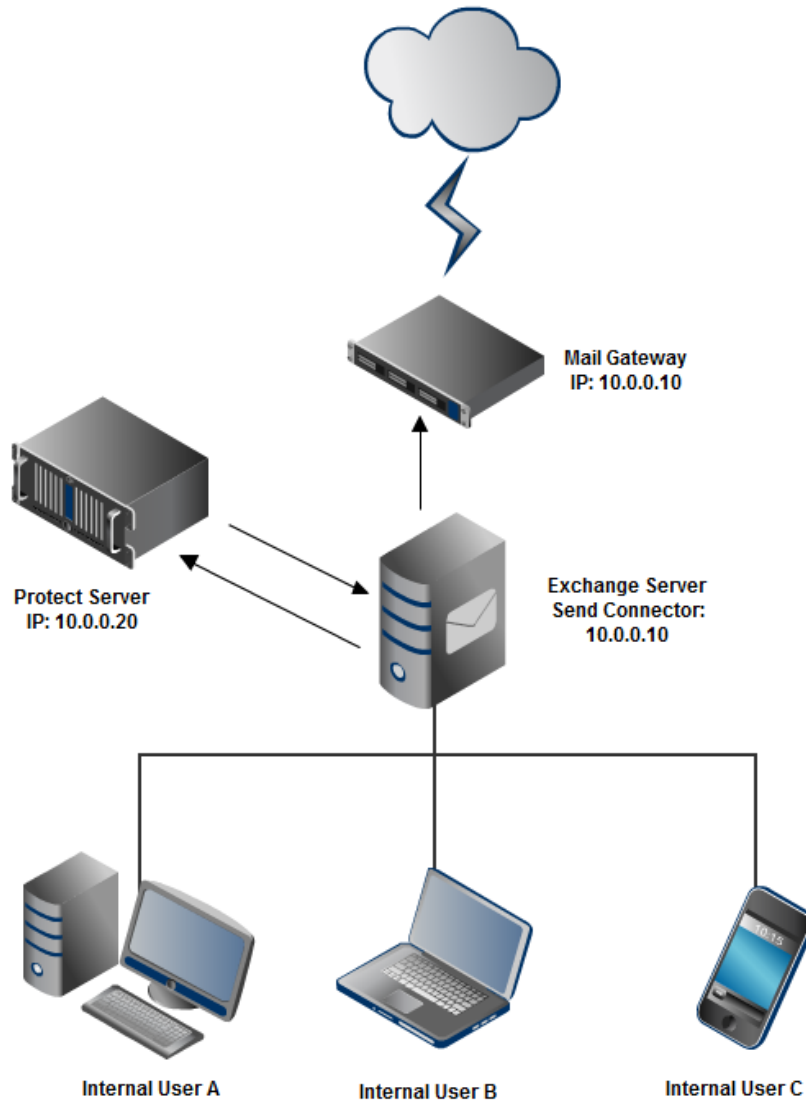


Figure 3: Workshare Protect Routing Agent setup – Microsoft Exchange Server’s external Send Connector is configured once again to send outgoing mail to the Mail Gateway at 10.0.0.10 (same as Figure 1). The Workshare Protect Routing Agent on Microsoft Exchange Server will direct mail with attachment(s) and external recipient(s) to Workshare Protect Server at 10.0.0.20 by using a special Send Connector created during the installation of the Workshare Protect Routing Agent (network name: workshareprotectserver.com) that points to Workshare Protect Server at 10.0.0.20. Workshare Protect Server’s smart host is configured to point back to Microsoft Exchange Server where normal routing of the mail continues.

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

1. Mail sent by an internal user reaches the Microsoft Exchange hub transport server with the Workshare Protect Routing Agent installed.
2. Before Microsoft Exchange Server delivers the mail, it gets processed by the Workshare Protect Routing Agent. If the mail includes external recipients and one or more attachments, the transport agent will set routing on the mail to a special Send Connector, workshareprotectserver.com, that was created during the installation process and points to Workshare Protect Server as its smart host. The transport agent also adds a MIME header to the mail to avoid a mail loop.
3. Workshare Protect Server will receive, inspect and possibly clean or convert the email attachment(s). It will then send the mail back to Microsoft Exchange Server. Workshare Protect Server will need to be configured to route all traffic back to Microsoft Exchange Server by setting its SMTP Server smart host to Microsoft Exchange Server on all domains in IIS 6 Manager.
4. Microsoft Exchange Server will receive the mail back from Workshare Protect Server. This is allowed by a Receive Connector created during installation. The Workshare Protect Routing Agent will see that the mail came from Workshare Protect Server and allow Microsoft Exchange to route the mail normally (to the mail gateway for external recipients and into the appropriate mailbox for internal recipients).

INSTALLATION

Prerequisites

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

- Workshare Protect Server, reachable from but not installed on the Microsoft Exchange Server
- 64-bit Microsoft Windows Server 2008, 2008 R2, 2012 or 2012 R2
- Microsoft Exchange 2007 SP3 to Microsoft Exchange 2013 SP1
- Hub Transport role
- Microsoft Exchange Management Shell
- CAS role installed or server with CAS role accessible
- IIS Windows Authentication Role service (needed for Updater Service to authenticate with EWS)
- Microsoft .NET Framework 3.5

Note: *The account used to install the Workshare Protect Routing Agent must have administrative rights in the top level domain to create the necessary email account.*

Preparation

Microsoft Exchange Server and Workshare Protect Server need to be configured to direct mail traffic correctly. See *Mail Flow*, page 4, for an overview of the mail flow in this scenario.

First of all, if Workshare Protect Server is already installed similarly to Figure 2 (page 6), with Workshare Protect Server between Microsoft Exchange Server and the mail gateway, **any Send Connector(s) pointing to Workshare Protect Server need to be removed/reconfigured to point to the mail gateway** (similar to Figure 1, page 5). The add-on installer needs to create a new special Send Connector pointing to Workshare Protect Server.

Secondly, **Workshare Protect Server's virtual SMTP Server instance needs to be configured with Microsoft Exchange Server as the only smart host for all mail domains**. This is required so Microsoft Exchange can synchronize processed emails to internal recipients and sender's Sent Items folders (see Figure 3, page 8).

Installation Steps

Installation is by PowerShell script. The installer performs the following steps internally:

- Adds and enables the transport agent "Workshare Protect Routing Agent".
- Adds Send Connector "Workshare Protect Send Connector" that points to Workshare Protect Server. **It has a special address space "workshareprotectserver.com", which is only used internally by the transport agent. Do not change the value of this address space.** Also note that if you change the IP address of Workshare Protect Server, you must update the smart host of this Send Connector.
- Adds Receive Connector "Workshare Protect Receive Connector" that allows Workshare Protect Server's IP the rights to relay mail back into Microsoft Exchange Server. By default, this Receive Connector allows anonymous access from the one IP address. Modify this if you want to change security options. As with the Send Connector, you must update the allowed IP address if the Workshare Protect Server IP address changes.
- Adds a system account with a mailbox used for updating Sent Items called protectpluginuser. This system account is set up with impersonation rights so the Protect Exchange Updater Service can access and update internal user mailboxes to update Sent Items.

Manual Installation for a Single Exchange Server

To deploy the Workshare Protect Server Routing Agent in an environment with a single Exchange server:

1. Extract **WorkshareProtectRoutingAgent-3.1.0.XXX.zip** (where XXX is the version number).
2. Launch Exchange Management Shell.

3. In the console, type:

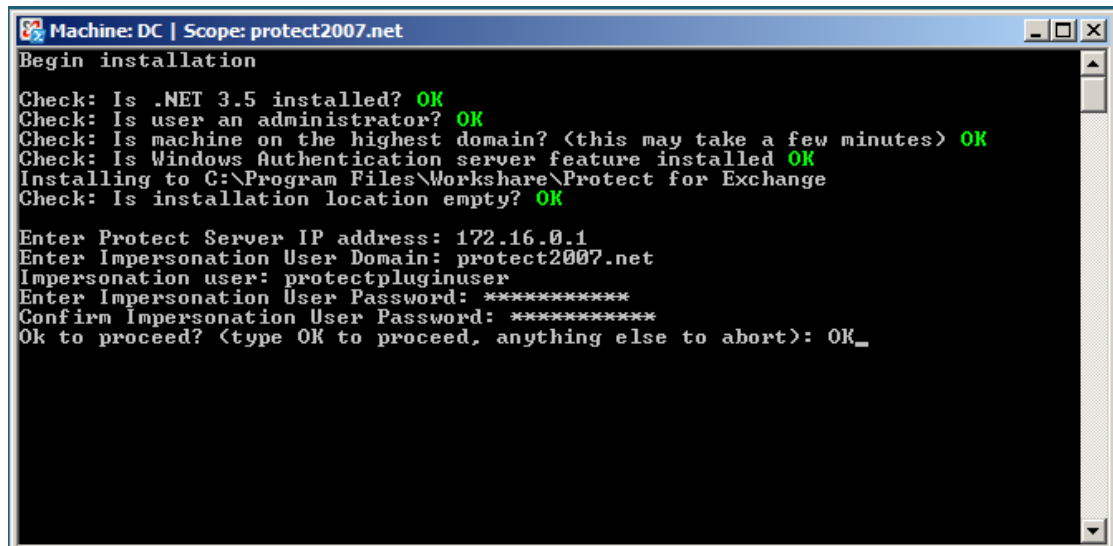
```
cd "<path to your extraction directory>\scripts"
```

4. In the console, type:

```
.\setup.ps1
```

5. Follow prompted instructions and enter the following information:

- Workshare Protect Server IP address
- Impersonation user domain
- Impersonation user
- Impersonation user password



```
Machine: DC | Scope: protect2007.net
Begin installation
Check: Is .NET 3.5 installed? OK
Check: Is user an administrator? OK
Check: Is machine on the highest domain? (this may take a few minutes) OK
Check: Is Windows Authentication server feature installed OK
Installing to C:\Program Files\Workshare\Protect for Exchange
Check: Is installation location empty? OK
Enter Protect Server IP address: 172.16.0.1
Enter Impersonation User Domain: protect2007.net
Impersonation user: protectpluginuser
Enter Impersonation User Password: *****
Confirm Impersonation User Password: *****
Ok to proceed? (type OK to proceed, anything else to abort): OK_
```

Note: If there are multiple mailbox databases, you will be prompted to select which one will host the impersonation user.

To uninstall the Workshare Protect Server Routing agent:

1. Launch Exchange Management Shell.

2. In the console, type:

```
cd "C:\Program Files\Workshare\Protect for Exchange\scripts"
```

3. In the console, type:

```
.\uninstall.ps1
```

4. Close Exchange Management Shell.

5. Delete the contents of C:\Program Files\Workshare\Protect for Exchange".

Manual Installation for Multiple Exchange Servers

It is necessary to deploy the Workshare Protect Server Routing Agent to every Microsoft Exchange server in the organization.

Complete the first deployment using the steps described in *Manual Installation for a Single Exchange Server*. On the second and subsequent deployments, the only variation in the process is that the installer will detect that the impersonation user account exists on the domain and will prompt for confirmation of the password.

Upgrades

Upgrades from previous versions of the Workshare Protect Routing Agent are not supported and you must first uninstall the previous version.

Note: Ensure that the “Protect Plugin User” is removed by the uninstall before installing the latest version of the Workshare Protect Server Routing Agent.

DIAGNOSTICS/MAINTENANCE

Enabling/Disabling

The Workshare Protect Server 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 this transport agent will return the Microsoft Exchange mail flow from a scenario similar to Figure 3 (page 8) to Figure 1 (page 5), bypassing Workshare Protect Server and performing normal routing on all mail.

The easiest way to enable and disable the transport 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 Workshare Protect Server or troubleshooting mail flow problems for example.

Logging

By default, the Workshare Protect Server Routing Agent outputs useful diagnostic information to avoid using the DebugView program. The level of logging and logging destinations can be changed in the configuration files for the routing agent. See *Configuration Options*, page 11, for more details.

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 Protect Server Transport 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

CONFIGURATION OPTIONS

Configuration of the Workshare Protect Server Transport Agent is via the configuration file: Workshare.ProtectServer.Exchange.exe.config located by default at C:\Program Files\Workshare\Protect for Exchange. To apply changes, restart MExchangeTransport service.

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:

Enter a comma or semi-colon delimited list of the senders' email addresses in the routing agent configuration file: Workshare.ProtectServer.Exchange.dll.config (C:\Program Files\Workshare\Protect for Exchange).

At node: `TestSenderEmailList`

Example:

```
<setting name="TestSenderEmailList" serializeAs="String">
  <value>sfstest1@wsdev.net;sfstest3@wsdev.net;scott.more@workshare.com</value>
</setting>
```

Only email with attachment(s) from the three specified senders will be processed by the Workshare Protect Server Routing Agent.

Whitelist Autonomy iManage EMM Email Addresses

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

To whitelist email addresses:

Enter the domain part of the email address used by the EMM module to indicate that a message should be filed in the routing agent configuration file: 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 Workshare Protect Server for cleaning.

Note: It is possible that custom Exchange transport rules can interfere with the Autonomy iManage EMM whitelist feature with the end result that emails destined for the Autonomy iManage EMM module are unprocessed even though all other recipients receive a processed copy of the email.

For example, the Workshare Protect Server Routing Agent is registered as a custom routing agent as part of the installation. By default the Workshare transport agent is deployed as the lowest priority transport agent. This means that, in a default configuration of Microsoft Exchange, the Exchange transport agent is executed before the Workshare transport agent when the Exchange server receives an email.

The purpose of the Exchange transport agent is to perform custom routing of email based on Exchange transport rules and it is possible that these rules may route email that meet the criteria of the rule before they can be routed by the Workshare transport agent.

An example would be if a custom transport rule was written to route email to an Autonomy iManage EMM server; any email that matched the rule criteria would be sent directly to the EMM server. Email that did not meet the criteria may then be routed by the Workshare transport agent (provided they meet the criteria of the Workshare transport agent). The result is that an unprocessed copy of the message is saved to Autonomy iManage EMM while the recipients of the email receive a processed version.

Send Connectors are the suggested resolution for the routing of email if this scenario is indicated.

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 3 settings in the routing agent configuration file: Workshare.ProtectServer.Exchange.dll.config (C:\Program Files\Workshare\Protect for Exchange). All are set to “True” by default and should not be modified.

- **AvoidDuplicateJournals** – Boolean (True/False). When set to True, the Workshare Protect Routing Agent ensures that only post-cleaned messages are added to Exchange journaling, avoiding journaling of both the pre- and post-cleaned messages. This feature has no effect on journaling of traffic that is not cleaned by Workshare Protect Server.
- **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="AvoidDuplicateJournals" serializeAs="String">
  <value>True</value>
</setting>
<setting name="AvoidCleanReportJournals" serializeAs="String">
  <value>True</value>
</setting>
<setting name="AvoidBifurcatedJournals" serializeAs="String">
  <value>True</value>
</setting>
```