Workshare Protect Server

Installation

Table of Contents

Chapter 1: Introducing Workshare Protect Server

This chapter introduces Workshare Protect Server, providing an overview of how it works as well as a summary of the key features and benefits. It includes the following sections:

- **What is Workshare Protect Server?**, page 7, introduces Protect Server.
- **Workshare Protect Server Functionality**, page 7, describes the different functionality available with Protect Server.
- **Deployment Scenarios**, page 12, describes typical deployments for Protect Server.
- **System Requirements**, page 13, describes the hardware and software specifications for Protect Server.
- **Overview of Installation**, page 15, outlines the steps required to set up and install Protect Server in your environment.

What is Workshare Protect Server?

Workshare Protect Server provides server-side metadata cleaning and document processing. Protect Server processes all emails passing through the corporate mail server, including those that originate from webmail and mobile mail clients. In corporate email scenarios, email is always routed through the corporate email server - and consequently Protect Server - ensuring complete protection. By locating this processing effort on the server, email send performance on the originating device is not impacted, and users are not affected.

Protect Server is a mail gateway that removes metadata from Microsoft Office attachments (Word, Excel and PowerPoint) as well as PDF attachments. It can also automatically convert Microsoft Office attachments to PDF. A web application - the Workshare Protect Server web console – is provided to enable administrators to configure which metadata elements to remove and view a history of what was previously removed.

Additionally, Protect Server can include the Policy Editor which provides a new policy framework to determine whether an email should be sent or bounced. It provides for control at the matter level through policies that associate email whitelists with matter-IDs.

Workshare Protect Server Functionality

Workshare Protect Server can secure attachments before they are sent by cleaning them of metadata or converting to PDF. Additionally, Protect Server can block emails and prevent them from being sent at all. An overview of the functionality is provided in the following sections.

Securing email attachments

Protect Server processes emails leaving an organization according to the profile applied to the email. This processing could be cleaning the attachments by removing metadata from them or converting the attachments to PDF, or both.

Where emails are sent to both internal and external recipients and the Workshare Protect Routing Agent is **not** installed, the internal recipient will receive the unprocessed document and the external recipient will receive a processed version. When the Protect Routing Agent **is** installed, both internal recipients and external recipients will receive a processed version.

Protect Server processes Microsoft Office and PDF attachments. The following file formats can be processed:

File format	Cleans	Converts to PDF or PDF/A
Microsoft Word 97 or later (DOC, DOT, DOCX, DOTX, DOCM, DOTM)	✓	✓
Microsoft Excel 97 or later (XLS, XLT, XLSX, XLTX)	✓	✓
Microsoft PowerPoint 97 or later (PPT, POT, PPTX, POTX)	✓	✓
RTF	✓	✓
Word 2003 XML	✓	✓
Open Document Text (both ODT 1.1 and 1.2 are cleaned, but files saved in ODT 1.1)	✓	✓
PDF	✓	✗

Protect Server processes the following types of attachments:

- Password-protected attachments (when the Workshare Protect Portal is installed).

  ***Note**: Protect Server does not process password-protected PowerPoint files.*

- The contents of archive (ZIP) attachments.
- Attachments of embedded emails.
- Attachments to meeting requests and other Microsoft Exchange-specific features, such as polls and forms.

***Note**: Protect Server does not process digitally signed documents or corrupt documents and does not check the attachments of digitally signed emails.*

Workshare Protect Routing Agent

With the installation of the Protect Routing Agent, Protect Server processes attachments of emails that are sent to both internal and external recipients. When an email has a relevant attachment and includes both external and internal recipients, the Protect Routing Agent will ensure that both the internal recipient and the external recipient receive the same processed version of the attachment.

The installation and setup of the Protect Routing Agent is described in the *Workshare Protect Routing Agent Admin Guide*.

Profiles determine cleaning and conversion

Profiles specify what metadata to remove from an email attachment and whether to convert the attachment to PDF. Every profile has an email address and this is how Protect Server determines which profile to apply to any given email. When a sender adds the email address of a profile as a recipient in an email then this profile will be used to process the email.

When a sender does not specify a profile email address in an email, the following occurs:

- If you have enabled the Active Directory cache feature, then Protect Server will look to see what AD group the sender belongs to and apply whichever profile you have defined for that group. If no profile has been defined for the group, then Protect Server will apply whichever profile you defined as the Default profile.
- If you have **not** enabled the Active Directory cache feature, then Protect Server will apply whichever profile you have defined as the Default profile.

If the sender specifies more than one profile email address in an email, then Protect Server will apply whichever profile you have defined as the Fallback profile.

Users allocated an Administrator role can create and manage multiple metadata cleaning/PDF conversion profiles. Configuring profiles is described in the *Workshare Protect Server Metadata Removal guide*.

Rule-based email blocking

Protect Server can prevent emails from being sent, based on business rules. The decision to block emails is driven by policies configured in the Protect Server Policy Editor. The Policy Editor provides for control at the matter level through policies that associate email groups with client engagements.

Policies determine access

You can set a policy that tells Protect Server to look for specific custom properties in the email attachments together with specific email addresses. If found, the email will be bounced.

The Policy Editor supports both whitelisting and blacklisting with policies that ensure access to certain information is to pre-approved recipients only as well as policies that ensure certain documents are never sent to untrustworthy recipients.

This granular approach to policies ensures confidential files pertaining to confidential matters are not accidentally sent to the wrong people.

This functionality can be enabled during or after installation. Configuring policies is described in the *Workshare Protect Server Email Data Loss Prevention guide*.

Additional functionality

Additional functionality can be configured on the Protect Server web console.

- **Clean reports for senders**

  Senders receive a clean receipt email with a Clean Report PDF attached providing details of the exact metadata cleaned from the document. The clean receipt email can also include the original email and the processed attachments. Administrators configure clean receipts on the Protect Server web console.

- **Bouncing emails**

  Protect Server can be configured to prevent emails with attachments that include comments or track changes or that cannot be processed from being delivered. There are several reasons why Protect Server may not be able to process an attachment. For example, the attachment may be corrupt or digitally signed. When Protect Server is configured this way, it bounces the email back to the sender with a non-delivery report. Administrators configure which emails to bounce on the Protect Server web console.

- **Preview functionality for senders**

  Protect Server provides previews of the cleaned/converted attachments to the sender. The sender can request a preview of what the processed attachments will look like before sending them to the recipients. This is done by sending an email to a profile email address only. Protect Server will treat such an email as a preview request and send the processed attachments back to the sender.

- **Synchronization**

  You can configure synchronization so that where any email attachment is processed by Protect Server, the original copy of the email found in the sender's "Sent Items" folder will be updated with the processed attachments. This update occurs for email destined for external recipients only as well as emails destined for both internal and external recipients.

  Additionally, to ensure that internal recipients always have access to the same version of attachments that are received by external recipients, where emails are sent internally and externally, the internal recipients can receive a clean receipt with the processed attachment included.

Web console for configuration

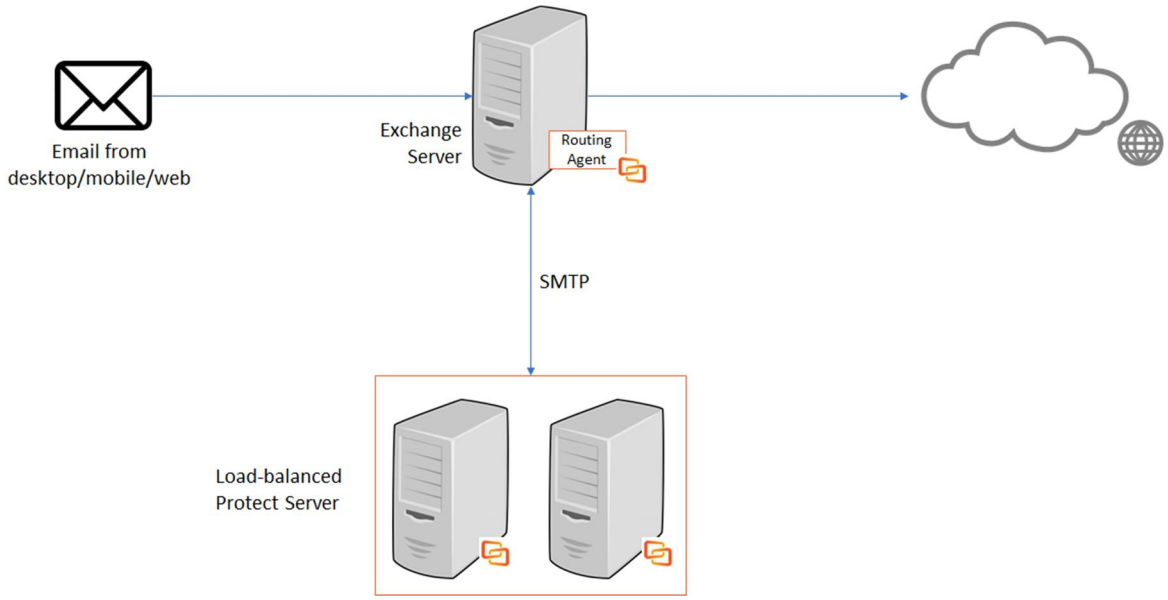
The functionality available in the Protect Server web console depends on the type of user:

- Users allocated an **Administrator** role can do the following:
  - View information about the performance and current health of Protect Server. For example, whether Protect Server services are up and running, whether the database is connected, whether the Protect Server license is expired and details of any emails queued on Protect Server.
  - Search through all emails processed by Protect Server.
  - Configure profiles.
  - Define policies (when the Policy Editor is enabled)
  - Specify Protect Server configuration settings, such as whether clean reports should be sent, how to override cleaning settings as well as configuring alert settings and email templates.
- Users allocated a **Business** role can do the following:
  - Access detailed statistics on the activities of Protect Server. For example, how many emails were processed using each profile and how many emails were processed in Microsoft Word format.
  - Search through and view emails that they themselves have sent through Protect Server. They cannot search or view emails sent by other users.
  - View profiles configured for Protect Server. They cannot create new profiles or modify or delete existing profiles.
- Users allocated a **User** role can do the following:
  - Search through and view emails that they themselves have sent through Protect Server. They cannot search or view emails sent by other users.
  - View profiles configured for Protect Server. They cannot create new profiles or modify or delete existing profiles.

***Note**: Roles are allocated during installation.*

Deployment Scenarios

Workshare Protect Server will typically be deployed as follows within an organization. This diagram shows Protect Server delivering email to a third-party gateway but Protect Server can also do final delivery.



In brief, the flow is as follows:

1. Email sent to the corporate mail server.
2. If the recipient is external to the organization, the corporate mail server relays the email to Protect Server. Protect Server removes metadata from any attachments and converts to PDF according to profile.

   ***Note**: Optionally, Protect Server can send a clean receipt to the sender of the email via the corporate mail server to confirm processing.*

3. Protect Server delivers the email to a third-party mail gateway (such as MimeCast or MessageLabs) which will deliver the email.

   ***Note**: Optionally, Protect Server can do final delivery of the email.*

System Requirements

Workshare Protect Server is designed to run on both entry level and enterprise scale servers. Recommended specifications are given below:

Hardware

CPU	64-bit architecture-based computer with Intel or AMD processor
Memory	8GB RAM (12GB RAM for Windows Server 2012)
Storage	1GB free disk space for installation
Networking	Gigabit Ethernet Controller

Supported operating systems

- Microsoft Windows Server 2016 Standard/Datacenter x64 Edition (recommended)
- Microsoft Windows Server 2012 R2 Standard/Datacenter x64 Edition

Note: *It is recommended that you upgrade the server to the latest service pack.*

Certified email systems

Protect Server is certified with Microsoft Exchange 2010, 2013 and 2016.

Prerequisites

The following software must be installed prior to the installation of Protect Server. The first three are installed automatically by running the scripts provided by Workshare, described in Configuring Prerequisites.

- Application Server and Web Server (IIS) Roles configured on Microsoft Windows Server.
- Microsoft IIS (Internet Information Services) 7.5, 8.0 or 8.5 with virtual SMTP service installed
- Microsoft Message Queue
- Microsoft SQL Server 2012, 2014 or 2016 with Full Text Search

Note*: If Protect Server is to be configured to run with a remote SQL database, ensure that both machines (Protect Server and Microsoft SQL Server) are on the same domain and that the credentials used to configure SQL are sufficient to authenticate against the domain controller.*

The following software is required but if it has not been pre-installed, it will be installed during the installation of Protect Server by the Workshare.ProtectServer.InstallWizard.exe.

- Microsoft .NET Framework 4.5.2 or higher
- Windows Visual C++ 2008 SP1 Redistributable Package (x86/x64)
- Windows Visual C++ 2005 SP1 Redistributable Package (x86/x64)
- Microsoft SQL Server Compact 4.0 (x64)
- IIS URL Rewrite Module 2

Virtual environments

Protect Server is supported in virtual environments. Workshare makes extensive use of virtual environments in the testing, development and support of Protect Server. Workshare is not aware of any issues with Protect Server running in a virtual environment.

Database implications

Assuming that no emails are stored in the database and that on average an email has one attachment, the following guidelines apply:

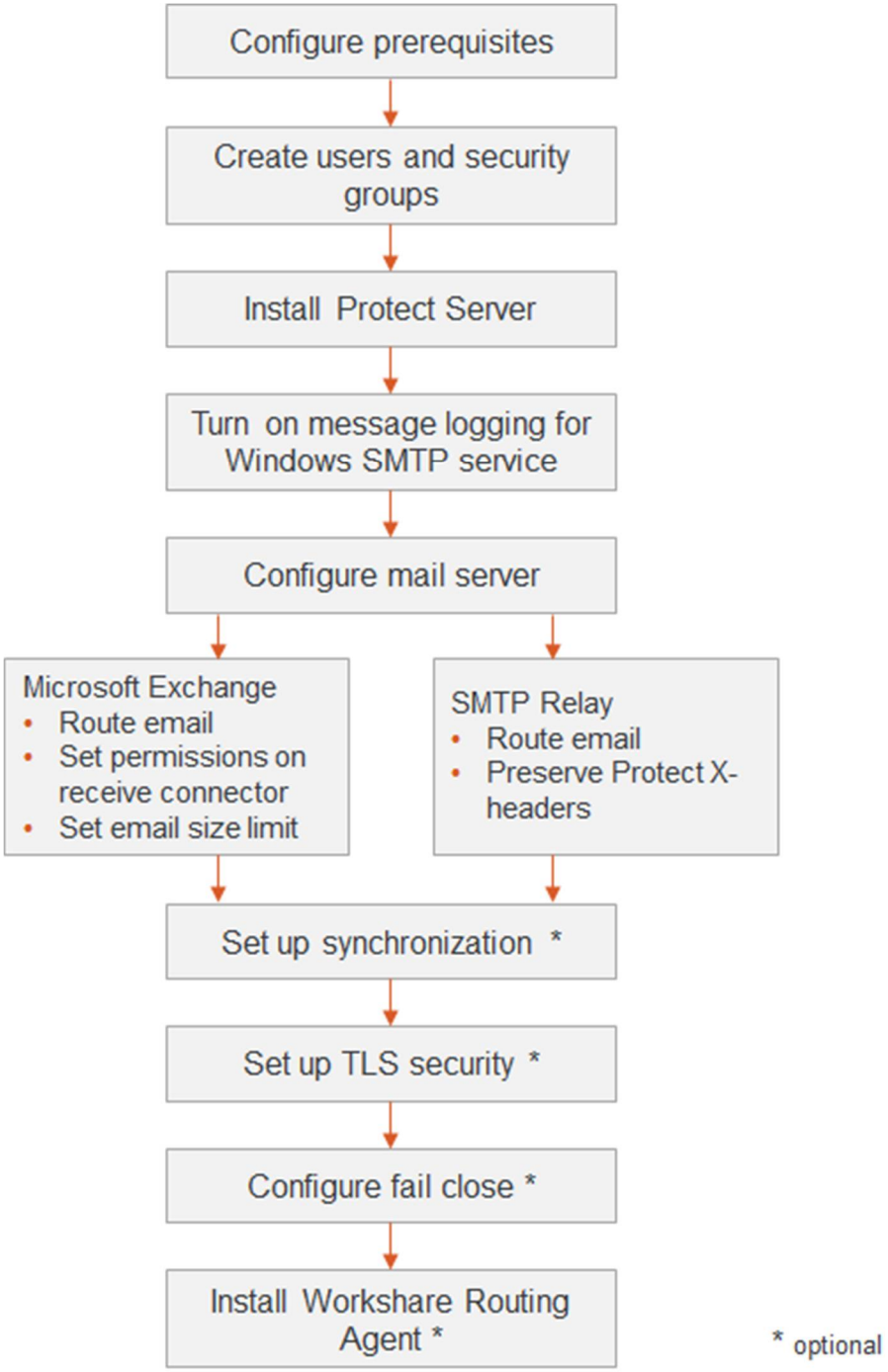
- Sending 10,000 emails a day and assuming 15% of those emails include metadata will add approximately 5.3MB of data to your database per day.
- Sending 50,000 emails a day and assuming 15% of those emails include metadata will add approximately 26.94MB of data to your database per day.
- Sending 100,000 emails a day and assuming 15% of those emails include metadata will add approximately 53.89MB of data to your database per day.
- Sending 250,000 emails a day and assuming 15% of those emails include metadata will add approximately 134.72MB of data to your database per day.

Pre-deployment checklist

Refer to Appendix D: Pre-Deployment Checklist for a pre-deployment checklist that you can complete, print out and reference during the installation.

Overview of Installation

In brief, there are the steps required to set up and install Workshare Protect Server in your environment:



Chapter 2: Setting Up

This chapter describes how to configure your system to work with Workshare Protect Server. It includes the following sections:

- **Configuring Prerequisites**, page 17, describes how Microsoft IIS and Microsoft Message Queue should be configured to work with Protect Server.
- **Creating Users and Security Groups**, page 18, describes the security roles implemented in Protect Server.

Configuring Prerequisites

This section describes how Microsoft Windows Server should be configured to work with Workshare Protect Server.

By running the scripts, described below, the following prerequisites are installed automatically:

- Application Server and Web Server (IIS) Roles configured on Microsoft Windows Server.
- Microsoft IIS (Internet Information Services) 7.5, 8.0 or 8.5 with virtual SMTP service installed
- Microsoft Message Queue

The following steps must be performed as a user with local administrator access.

Install the prerequisites as follows:

1. Select the script most appropriate to your environment.
   - For Windows 2016 – use “install-ps-prerequisites-win2016.ps1”
   - For Windows 2012 R2 – use “install-ps-prerequisites-win2012.ps1”

   These scripts can be downloaded from the Workshare knowledge base http://workshare.force.com/knowledgebase/articles/Help_Articles/Workshare-Protect-Server-3-11-Installation-Guide1
2. Copy the script to your Protect Server machine.
3. Click Start.
4. Type “command”.
5. Right-click **Command Prompt** and select **Run as administrator**.
6. Run the command below (assuming you copied the script to C:\psinstall).

```
@powershell -ExecutionPolicy Unrestricted -Command
“C:\psinstall\install-ps-prerequisites-win2012.ps1”
```

> ***Note**: The script can take some time to run.*

Runtime prerequisites

In addition, the following three redistributable packages need to be installed before installation of Protect Server:

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package ATL Security Update

  The executable file is downloaded by clicking this link: http://download.microsoft.com/download/6/B/B/6BB661D6-A8AE-4819-B79F-236472F6070C/vcredist_x86.exe
- Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package ATL Security Update

  The executable file is downloaded by clicking this link: http://download.microsoft.com/download/9/7/7/977B481A-7BA6-4E30-AC40-ED51EB2028F2/vcredist_x86.exe
- IIS URL Rewrite Module 2

  The executable file is downloaded by clicking this link: http://download.microsoft.com/download/D/D/E/DDE57C26-C62C-4C59-A1BB-31D58B36ADA2/rewrite_amd64_en-US.msi

Creating Users and Security Groups

Workshare Protect Server implements the following security roles:

- Processor role
- Business role
- Administrator role
- User role

Before starting the installation, you must prepare a list of users and security groups that will be assigned during installation. A sample procedure is shown here.

***Notes**:*
*The **Security Group Name** can be specified using the NetBIOS domain format or fully qualified name. For example, if the fully qualified domain name is "test.net" and the group is "protectserver", then the group must be specified as test\protectserver or protectserver@test.net.*

If a user changes user groups (roles), you must wait 20 minutes for IIS to recycle the app pool to clear out the caches credentials that IIS has kept.

Processor role

This role will allow the audit service to write results of the inspecting and/or cleaning of emails to the database.

It will also retrieve the latest versions of profiles that will be used to control the inspecting and/or cleaning of emails. These profiles will synchronize on a regular basis. The synchronization is every one minute or when the profile service receives an instruction from the web site to synchronize the profile cache.

If the database is local to the Protect Server installation then the Processor role can be the **Local System account**. If the database is remote then the Processor role needs to be a **Windows domain account**. This account does not need to be special, just to be able to log on to the machine where Protect Server is installed.

This user needs the 'Log on as a Service' privilege on the machine that the Protect Server Audit/Profile Services will run on. The installer will automatically assign this privilege to the user.

***Note**: It is recommended that a new user account is created for the Processor role and this user has the **password never expired** option selected and the **User must change password at next logon** option NOT selected.*

Business role

This role will allow all business users to view reports, any results details, the profile used against the results and the current profiles in use. If the user is part of the Windows domain then they will be able to view and search their own email results.

The Business role has to be assigned a **Windows domain security group**.

Administrator role

This role will allow administrators to monitor system status, add, edit or remove existing profiles as well as configure settings, such as bounce, alert and override settings. The administrator user will be able to search any email results. If the user is part of the Windows domain then they will be able to see their own email results as well.

The Administrator role has to be assigned a **Windows domain security group**.

User role

This role will allow users to view the current profiles in use. If the user is part of the Windows domain then they will be able to view and search their own email results.

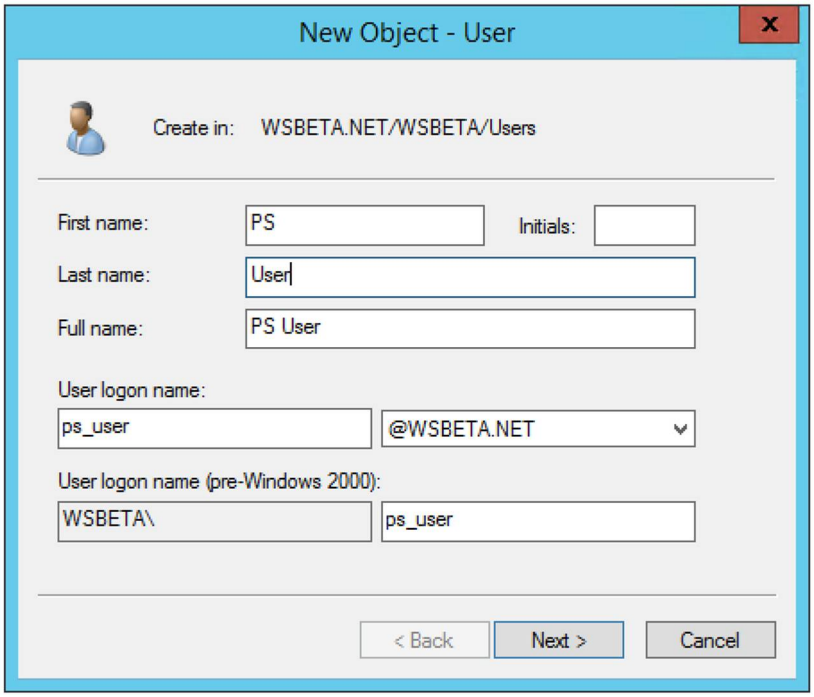
The User role has to be assigned a **Windows domain security group**.

Sample procedure

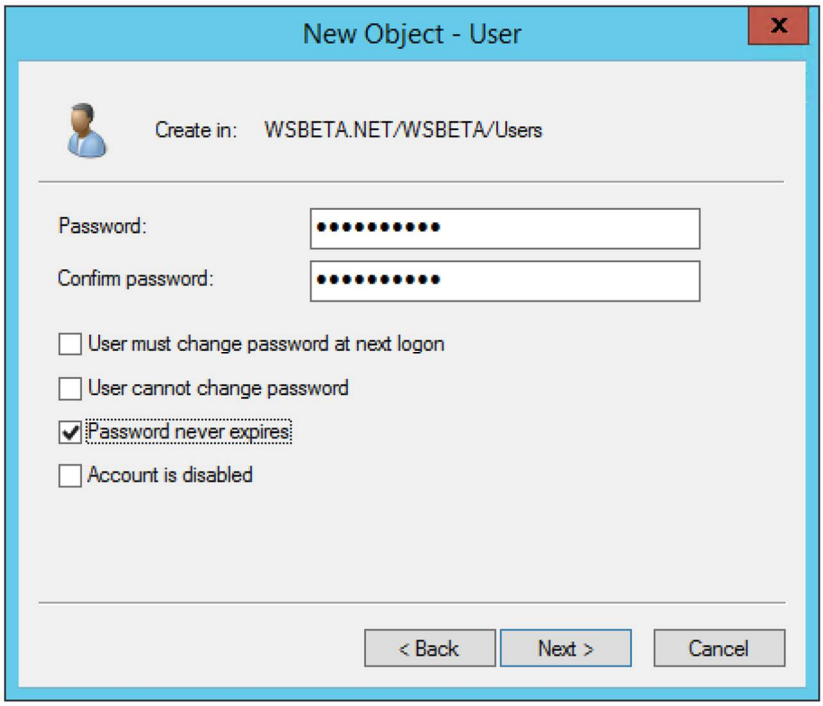
The following procedure describes how to create users, then create a security group and add the users as members. This group can then be assigned during the installation of Protect Server.

To create a user:

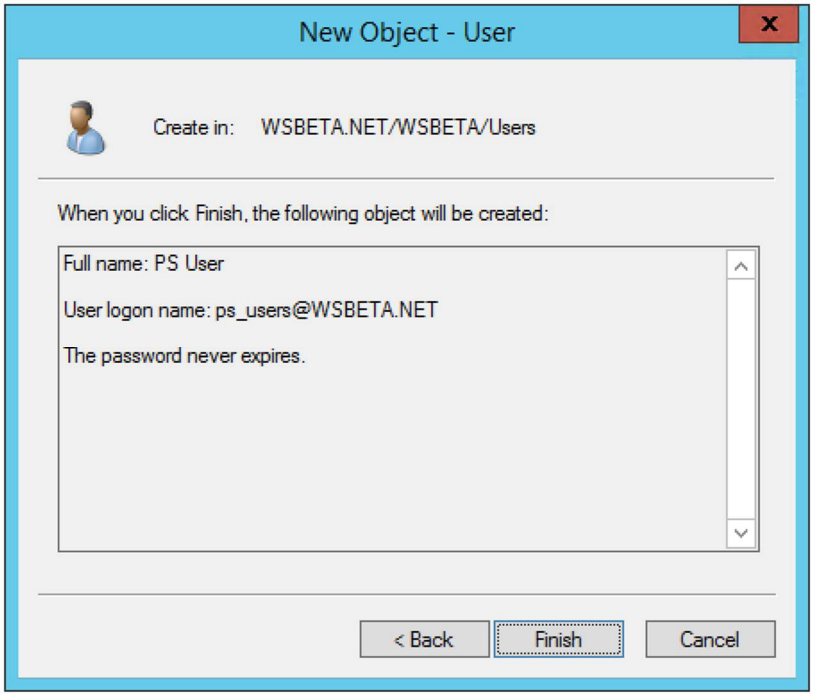
1. Open Active Directory Users & Computers.
2. Right-click the Users OU and select New and then User.



3. Enter a name for your user and a logon name. Click **Next**.



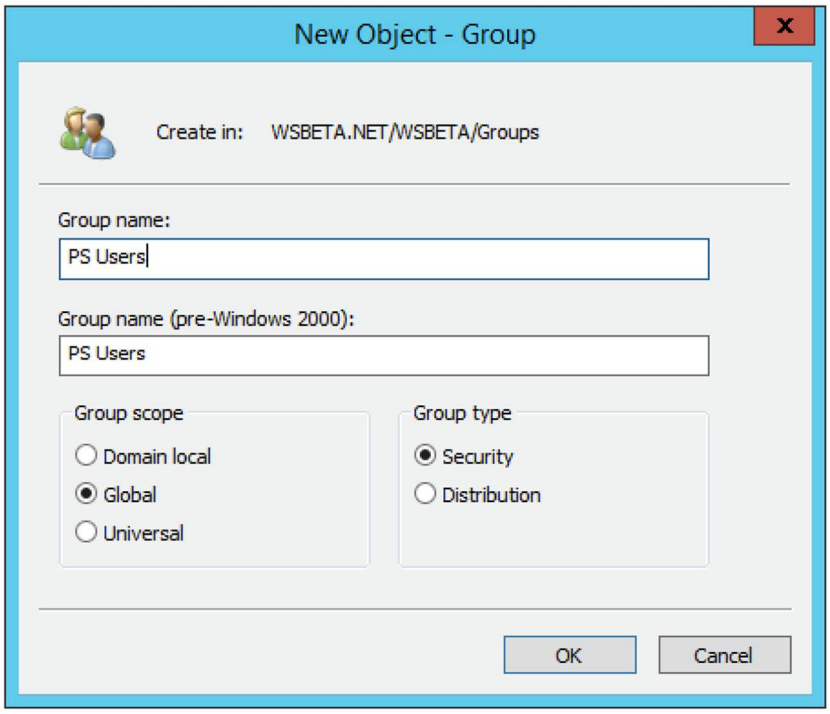
4. Enter the password for the user and select that the password never expires. Click **Next**.



5. Click **Finish**. Now create a group.

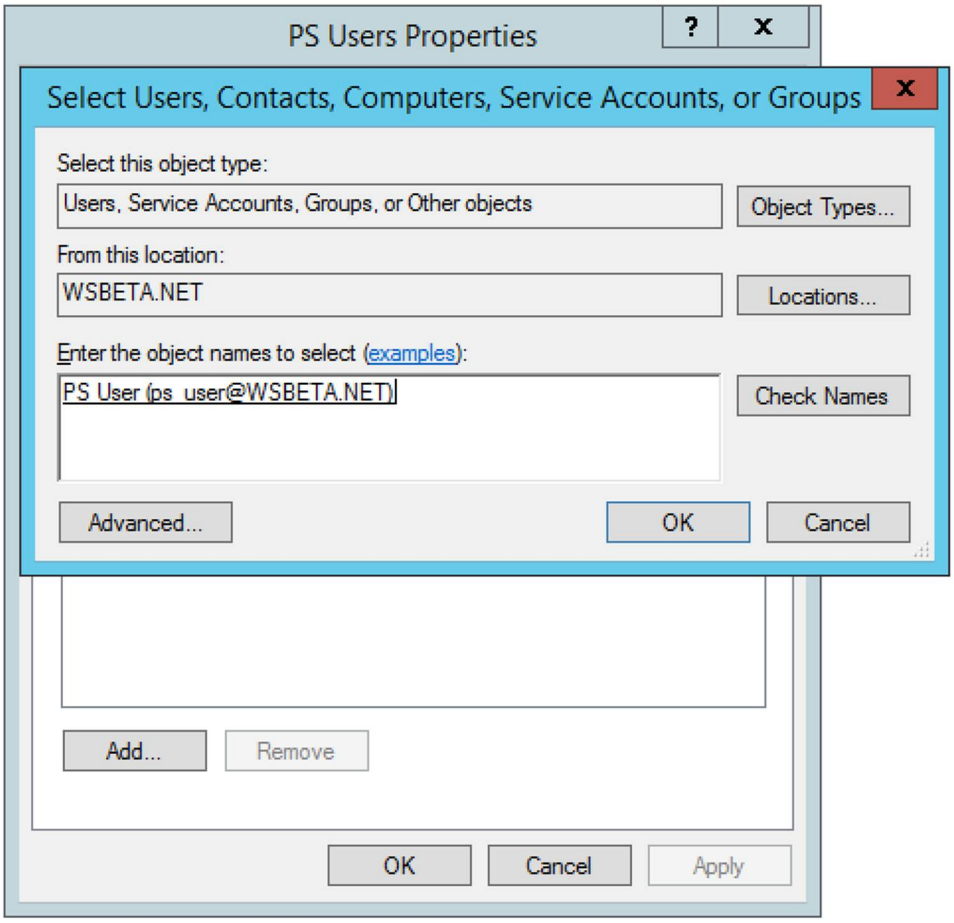
To create a group:

1. Open Active Directory Users & Computers.
2. Right-click the **Users** OU and select **New** and then **Group**.



3. Enter a name for your group, such as “PS Users” and select **Global** as the **Group scope** and **Security** as the **Group type**.
4. Click **OK**.
5. Double-click the newly created group. The group *Properties* dialog is displayed.

6. Select the **Members** tab and click **Add**.



7. Search for the users you want to be User role users and add them to the group.

Chapter 3: Installing

This chapter describes how to configure your system to work with Workshare Protect Server. It includes the following sections:

- **Installing Workshare Protect Server**, page 25, describes how to install Protect Server using the install wizard.
- **Turning on Email Message Logging**, page 50, describes how to turn on logging of messages for the Windows SMTP service.
- **Access to the Workshare Protect Server Web Console**, page 53, describes how to access the Protect Server web console where you configure what metadata should be removed from email attachments as well as other useful configuration settings, such as whether clean reports should be sent.
- **Licensing**, page 55, describes how to license Protect Server.

Installing Workshare Protect Server

This section describes how to install Workshare Protect Server in the simplest state – a final delivery “Protect Server” with SQL, SMTP and the Protect Server configured on a single machine.

In order for Protect Server to remove metadata from email attachments, your corporate mail server (or servers) should be modified to send emails to Protect Server for relay or to perform final delivery. Protect Server leverages the Windows SMTP server to process emails. The Windows SMTP server receives emails which are then processed by Protect Server. After processing by Protect Server, the Windows SMTP server will deliver the email or forward to it to the next server (relay). In both cases you need to set up Protect Server to accept incoming email from your corporate mail servers. You do this during the installation process.

The following procedure includes the Workshare Protect Portal in the installation so that Protect Server will be able to process password-protected documents. The Protect Portal provides a separate website for email senders to log in and provide passwords. You can install the portal at any time – Protect Server knows when it is installed, and when it is not. There is no configuration required on the Protect Server side.

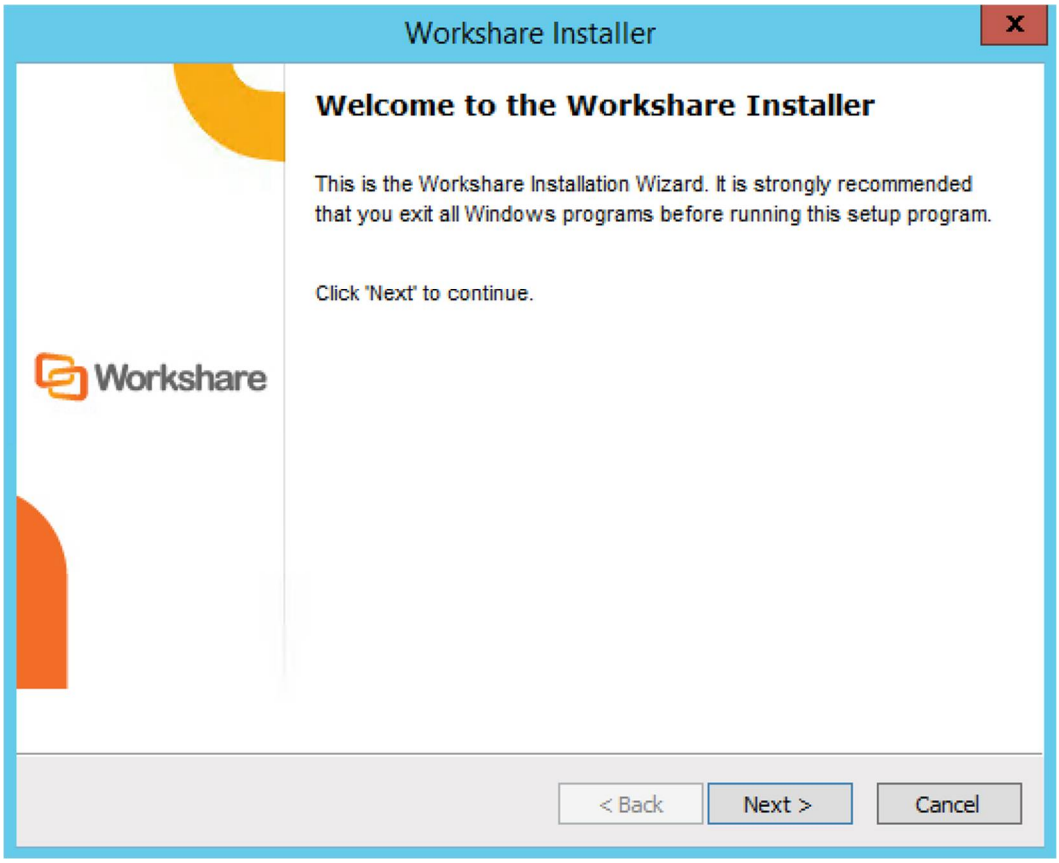
***Note**: The Protect Portal is optional. If you do not want password-protected attachments to be cleaned or converted to PDF, don’t install it. If you do install it and you would like it to be accessible to users outside your firewall, you will need to allow access to the Protect Portal through your firewall.*

The Policy Editor is an add-on to Protect Server and has a separate installation file which is installed at any time after Protect Server is installed.

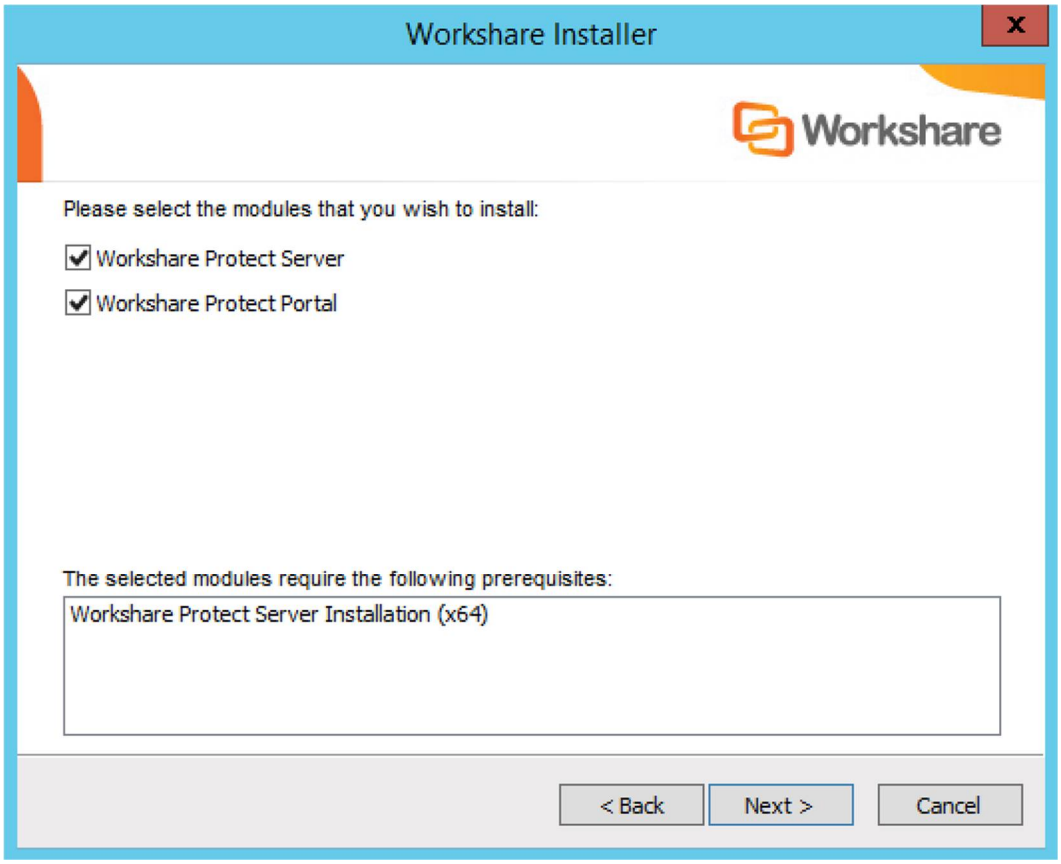
Before starting the installation, refer to Creating Users and Security Groups and prepare a list of users and security groups that will be assigned during installation.

To install Protect Server:

1. Download and run Workshare.ProtectServer.InstallWizard.exe.



2. Click **Next** to show the prerequisites that need to be installed with Protect Server and Protect Portal.

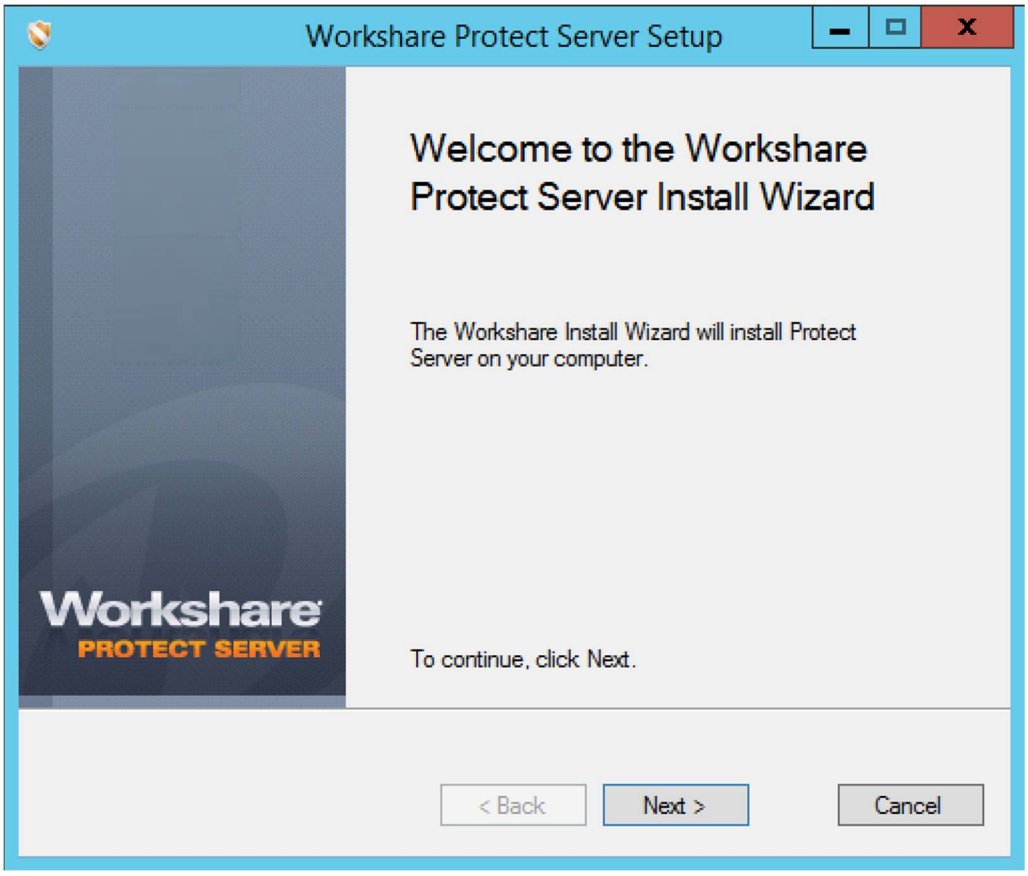


3. Ensure the **Workshare Protect Server** checkbox is selected (it should be by default). If you want Protect Server to process password-protected documents, you must also select to install the **Workshare Protect Portal**. Any required prerequisites are listed. Click **Next**.

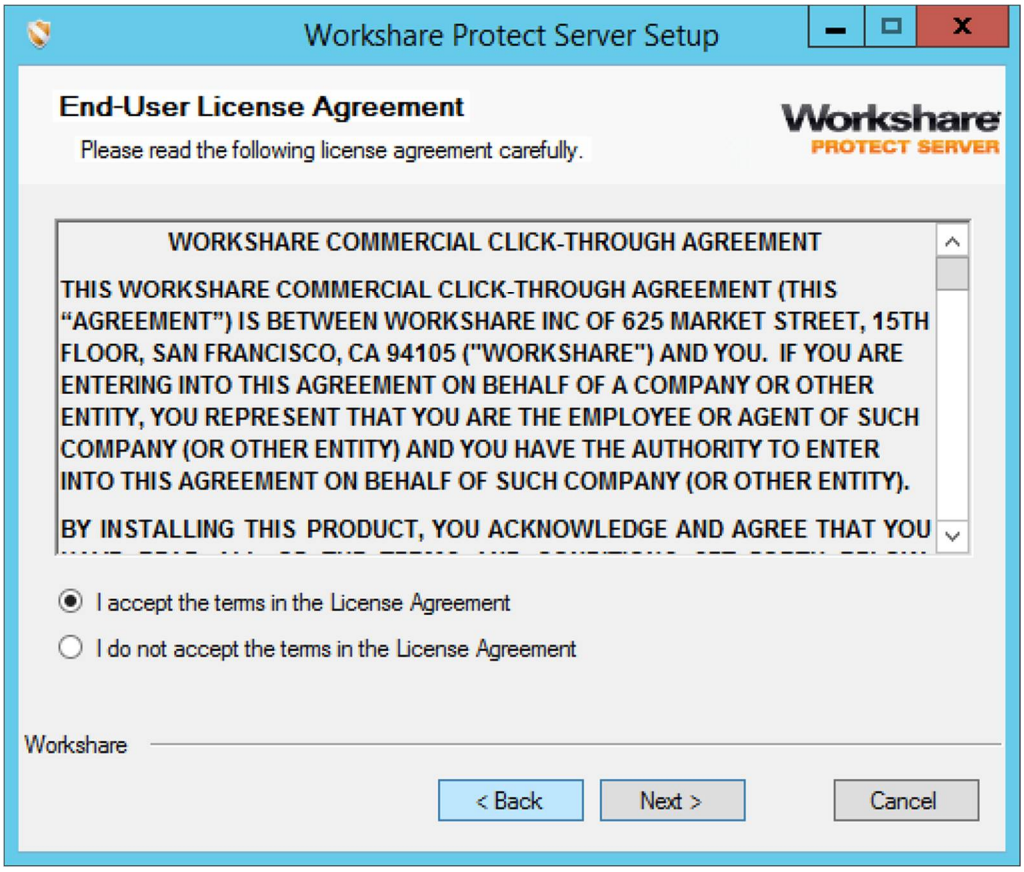
> ***Note**: The Protect Portal installation follows automatically after the Protect Server installation and is described in Installing Workshare Protect Portal.*

4. If prompted to download components from the internet, select **Yes**. The required prerequisites will be downloaded and installed.

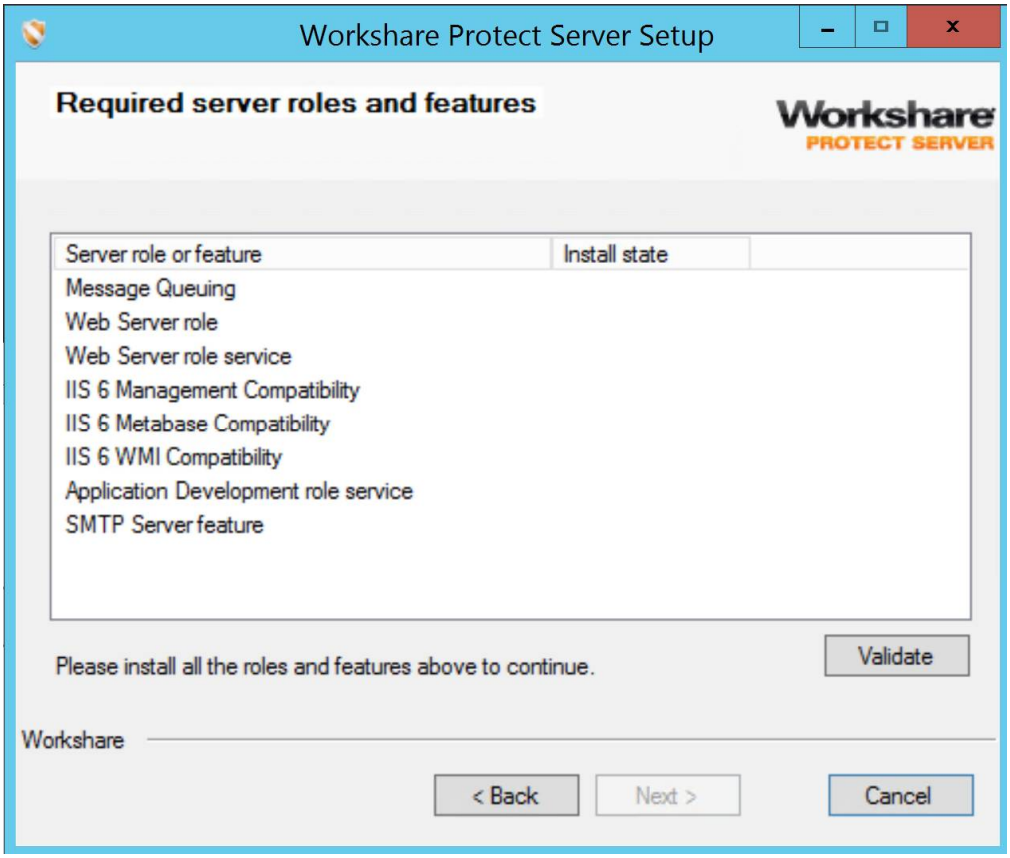
5. Once the prerequisites are installed, the Protect Server install begins and the Welcome page is displayed.



6. Click **Next**.

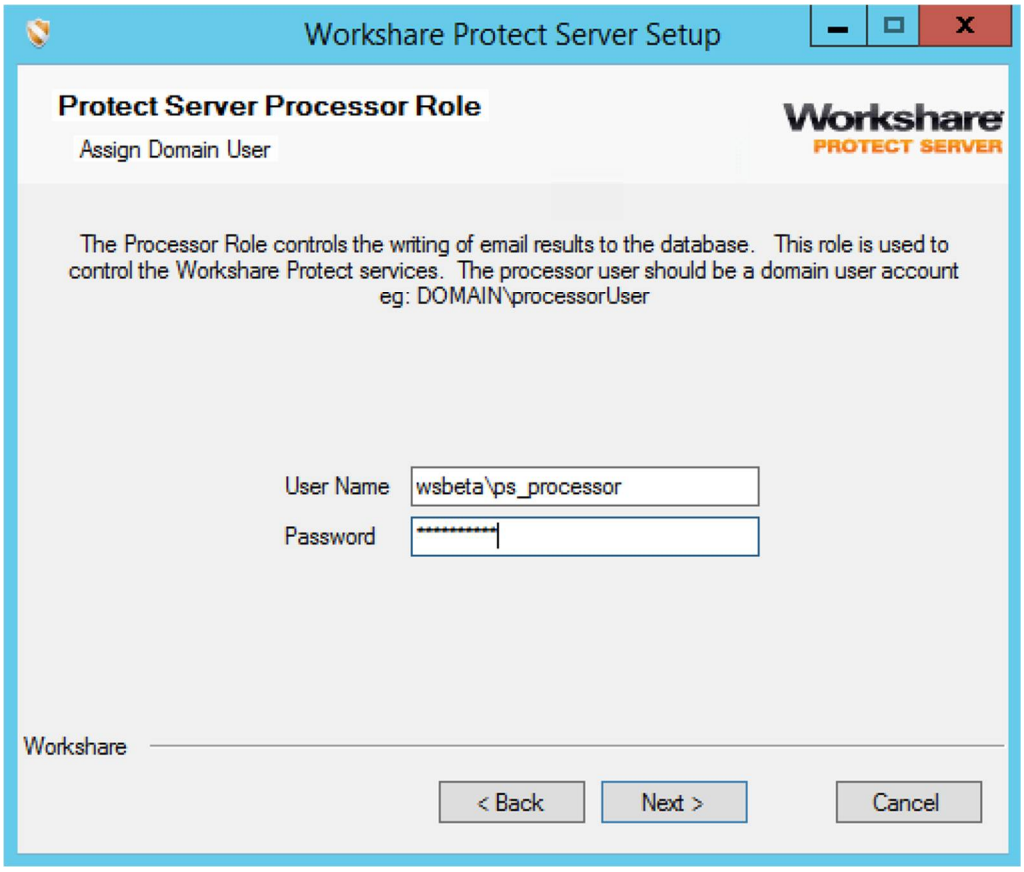

Workshare Protect Server Setup
End-User License Agreement
Please read the following license agreement carefully.
Workshare
PROTECT SERVER
WORKSHARE COMMERCIAL CLICK-THROUGH AGREEMENT
THIS WORKSHARE COMMERCIAL CLICK-THROUGH AGREEMENT (THIS "AGREEMENT") IS BETWEEN WORKSHARE INC OF 625 MARKET STREET, 15TH FLOOR, SAN FRANCISCO, CA 94105 ("WORKSHARE") AND YOU. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER ENTITY, YOU REPRESENT THAT YOU ARE THE EMPLOYEE OR AGENT OF SUCH COMPANY (OR OTHER ENTITY) AND YOU HAVE THE AUTHORITY TO ENTER INTO THIS AGREEMENT ON BEHALF OF SUCH COMPANY (OR OTHER ENTITY).
BY INSTALLING THIS PRODUCT, YOU ACKNOWLEDGE AND AGREE THAT YOU
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
Workshare
< Back
Next >
Cancel

7. Agree to the terms in the EULA and click **Next**. The Required server roles and features page is displayed.



8. Click **Validate** and wait until all features are validated.

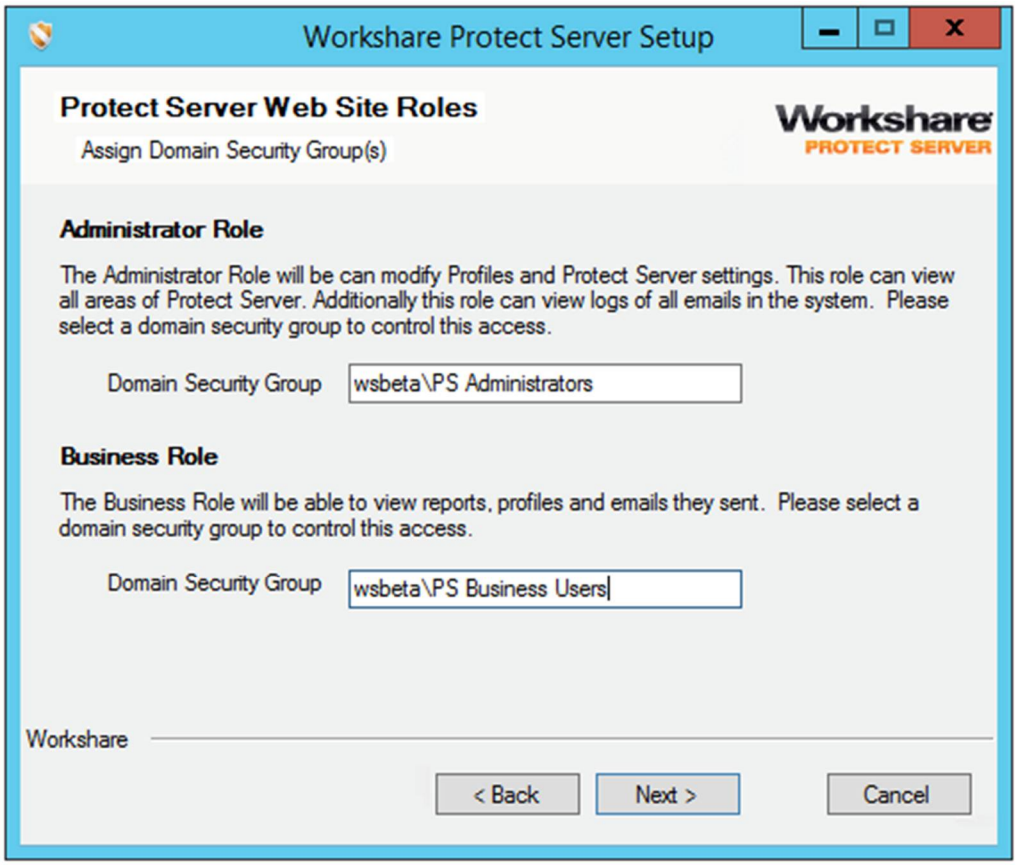
9. Click **Next**. The Protect Server Processor Role page is displayed.



10. Enter a domain user and password for this role.

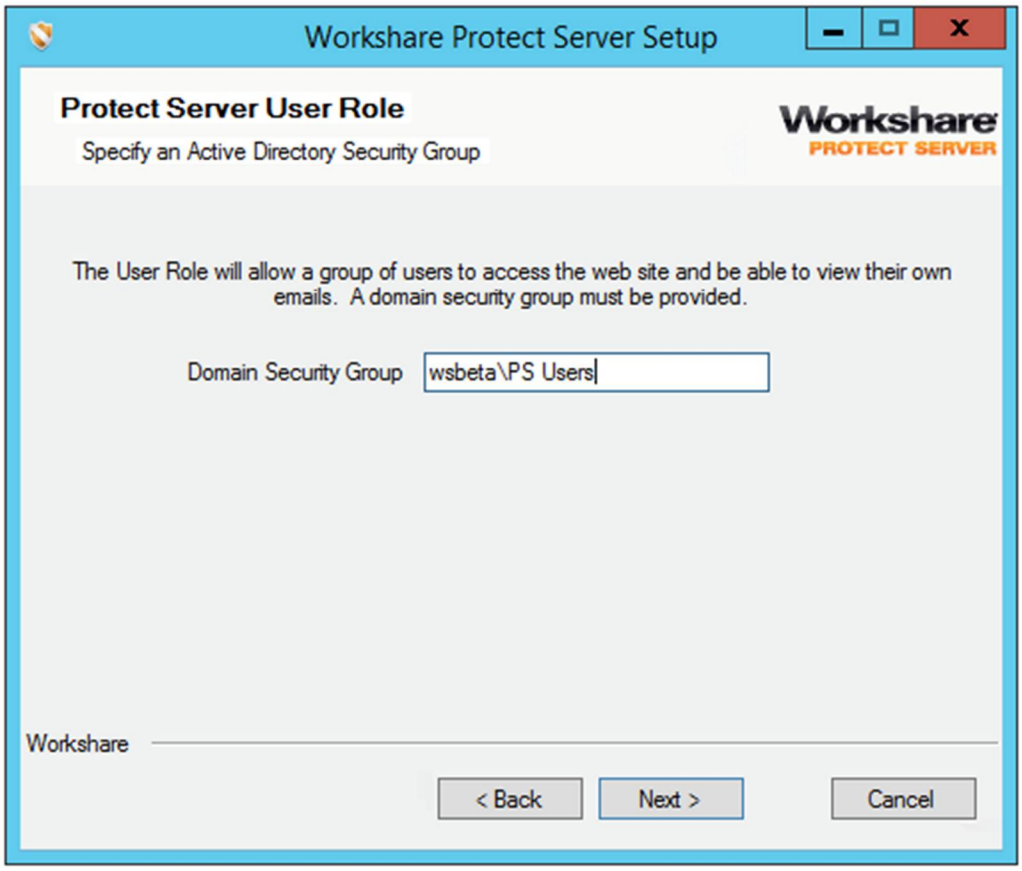
> ***Tip!*** *It is recommended that you create a new user for the Processor role as this account will have read/write access to the Protect Server database.*

11. Click **Next**. The Protect Server Web Site Roles page is displayed.



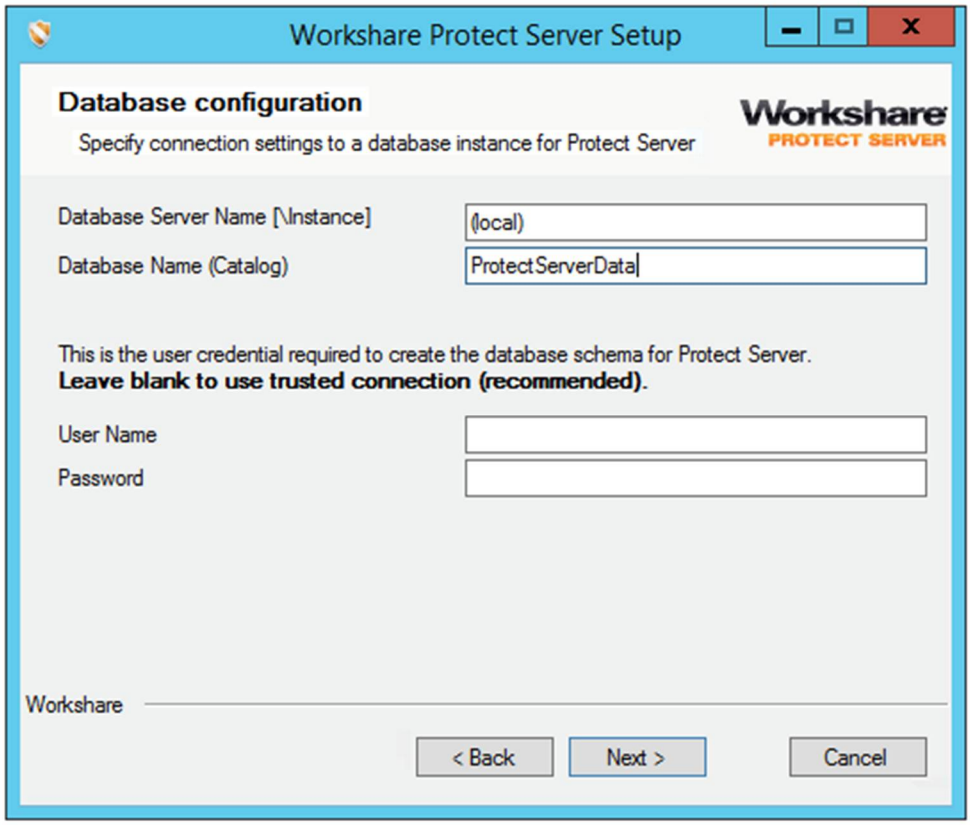
12. Specify the security group for the Administrator role and Business role. You must enter domain security groups and the domain has to be specified as well, for example, wsdemo\ProtectServerAdministrator.

13. Click **Next**. The Protect Server User Role page is displayed.



14. Specify the security group for the User role. You must enter a domain security group and the domain has to be specified as well, for example, wsdemo\ProtectServerUser.

15. Click **Next**. The Database configuration page is displayed.



16. In the **Database Server Name** field, enter the name of the SQL server. A hostname may be used or an instance name, for example (local)\SQLExpress.

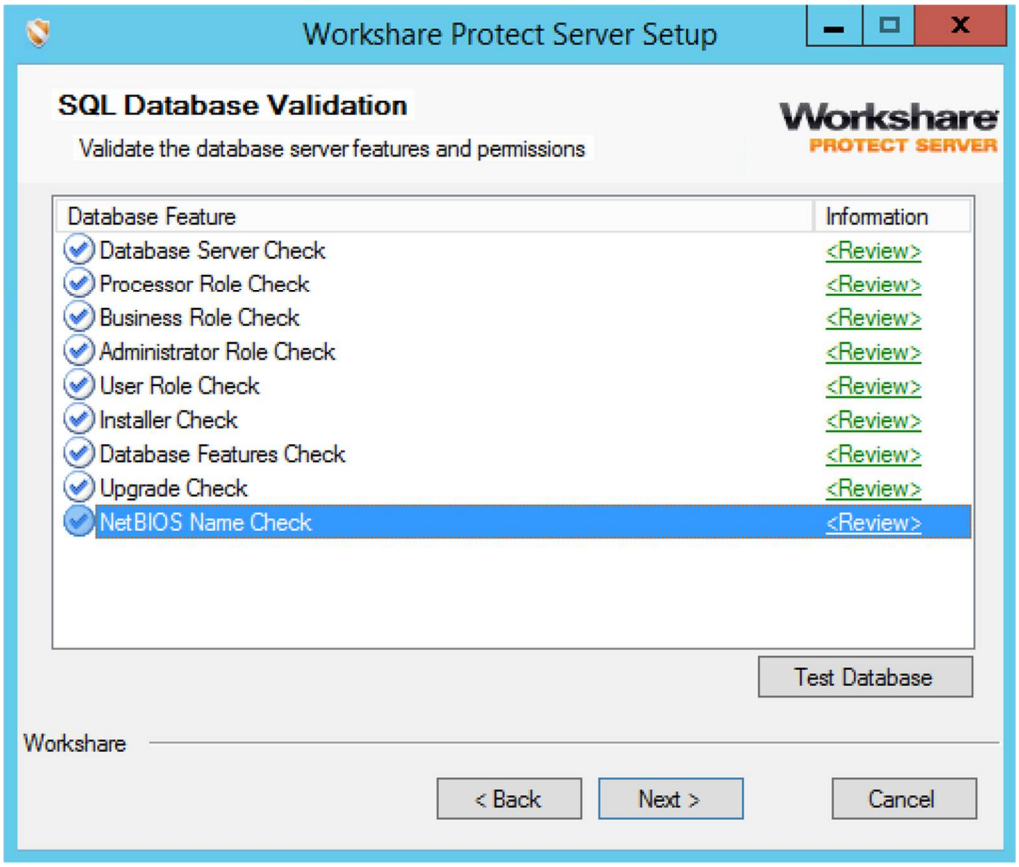
> ***Note**: If your SQL server is not using the default port (1433), please specify the port number after the name in the **Database Server Name** field using the following format: <server name>,<port number>.*

17. In the **Database Name** field, enter the name of the database to be created, for example, **ProtectServerData**. It is recommended not to mix numbers and characters in the database name.

18. In the **User Name** and **Password** fields, enter the user credentials required to access the database. It is recommended to leave these fields blank and use the trusted connection.

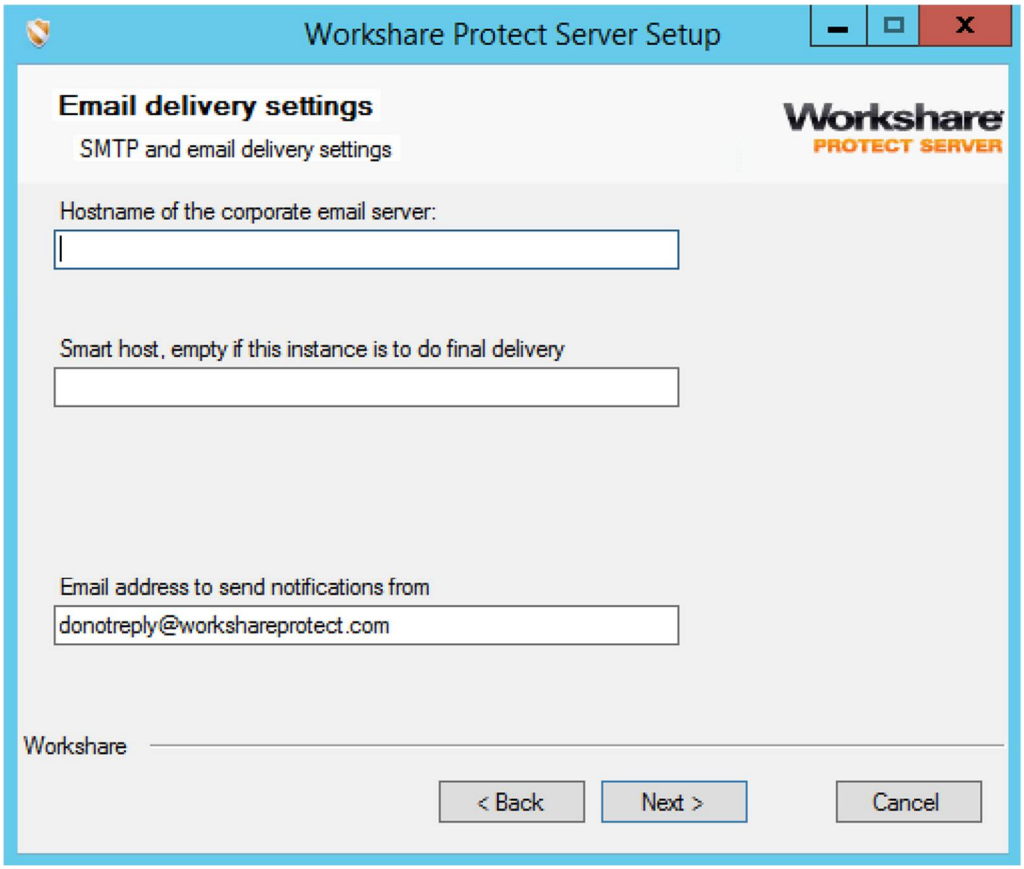
> ***Note**: It is recommended that the user installing Protect Server is not a member of any other security groups. This is because if one of the other security groups is dropped for any reason, the installer user will not be able to access the database. When the installer user attempts to access the SQL database, the SQL database will authenticate the user against all the security groups to which the user belongs. If there is even one authentication failure, then access is denied.*

19. Click **Next**. The SQL Database Validation page is displayed.
20. Click **Test Database**.



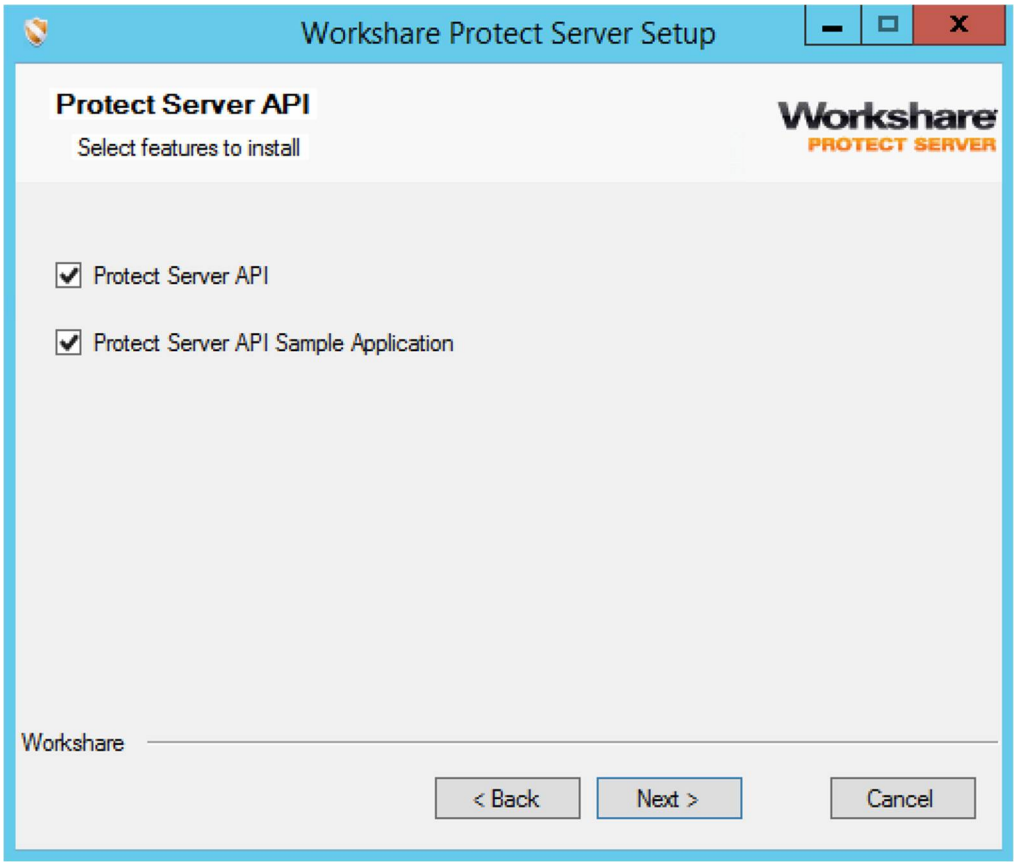
***Note**: You can click the **Review** link to get more information about any of the tests. The **Next** button is only enabled when the tests are passed.*

21. Click **Next**. The Email delivery settings page is displayed.



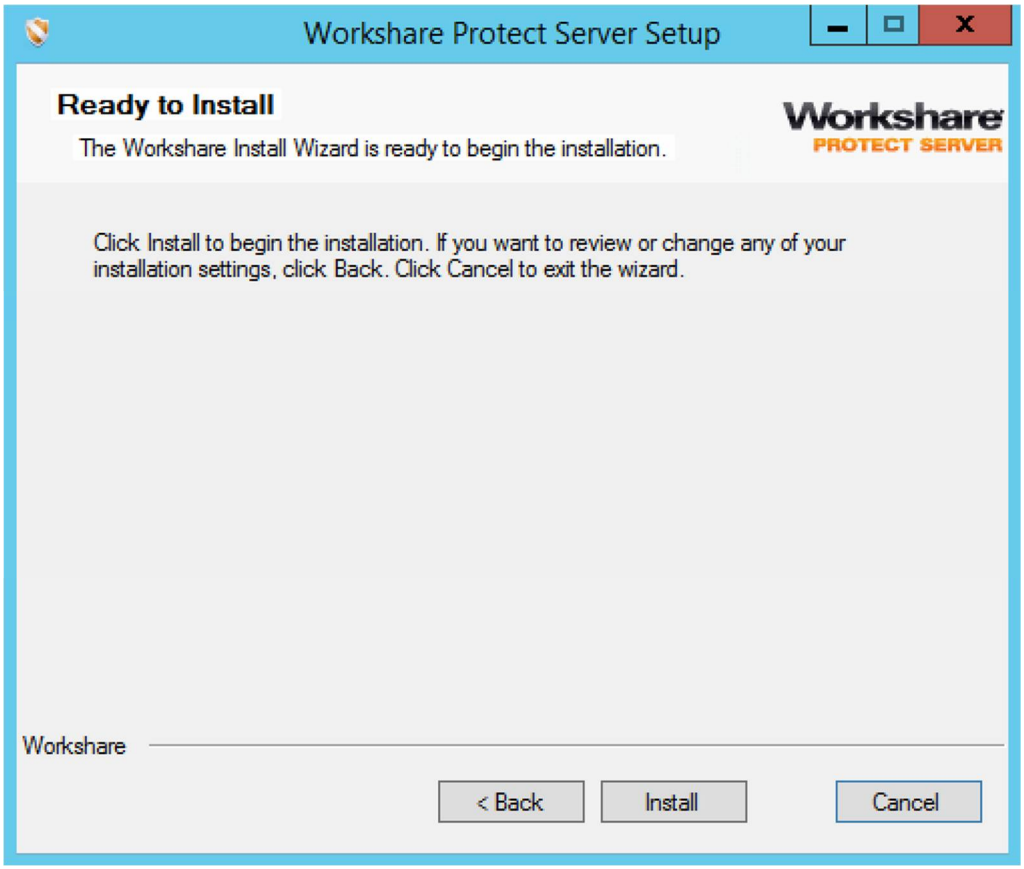
22. In the **Hostname of the corporate email server** field, enter the name of the mail server forwarding email to Protect Server. You can enter an IP address or fully qualified domain name (FQDN).
23. If required, in the **Smart host** field, enter the name of a final delivery server. Leave this field blank if Protect Server is to do final delivery.
24. In the **Email address to send notifications from** field, enter a valid email address to be used for sending out alerts and clean receipts. Ensure that your corporate email server can receive and deliver emails from this email address and will not label it as spam.

25. Click **Next**. The Protect Server API page is displayed.



26. If required, select to install the Protect Server API and sample application.

27. Click **Next**. The Ready to Install page is displayed.



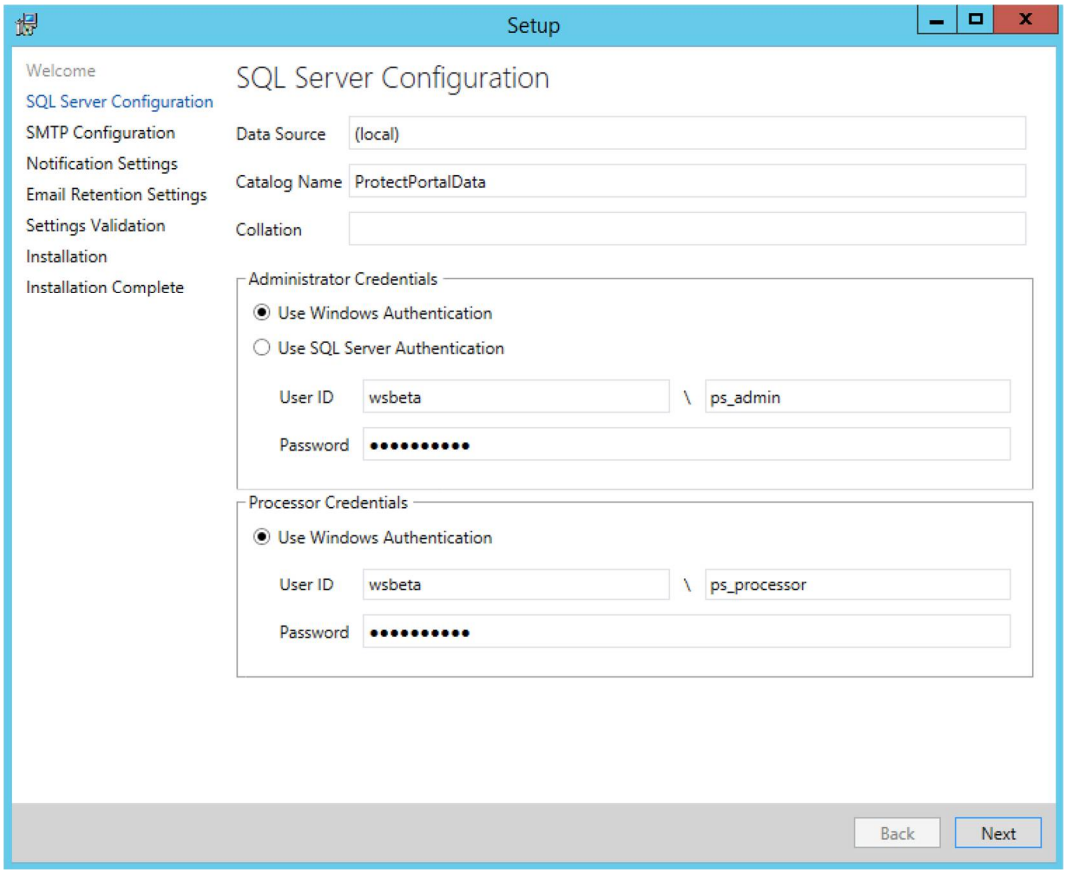
28. Click **Next**. Protect Server is installed. Once installation is complete, the Protect Portal installation begins (see following section).

Installing Workshare Protect Portal

When you select to install the Protect Portal, the installation wizard automatically begins once Protect Server is installed. Once the Installation Wizard has loaded, the welcome screen is displayed, providing an opportunity to import an answer file from a previous installation.

***Note**: If you have previously installed the Protect Portal and saved the settings in an answer file, you can browse to the saved file and re-use the settings.*

1. Click **Install**.



2. Specify your database settings here. Use “ProtectPortalData” as the catalog name. If **Collation** is left blank, the default database collation is used.

3. Enter the logon credentials for the database administrator. This user should have sysadmin rights. These credentials are used during install ony.

   If the database administrator is an SQL user:

   - Select **Use SQL Server Authentication**.
   - Enter the user name in the text box to the right of the \ symbol.
   - Enter the user password in the **Password** field.

   If the database administrator is a Windows user:

   - Select **Use Windows Authentication**.
   - Enter the domain name of the user in the text box between **User ID** and \.
   - Enter the user name in the text box to the right of the \ symbol.
   - Enter the user password in the **Password** field.

***Note**: It is necessary to enter the windows credentials even if you are currently logged in as this user.*

4. Enter the logon credentials for the processor user. For security reasons, the processor user must not be the same user as the administrator user.

   If the processor user is an SQL user:

   - Select **Use SQL Server Authentication**.
   - Enter the user name in the text box to the right of the \ symbol.
   - Enter the user password in the password field.

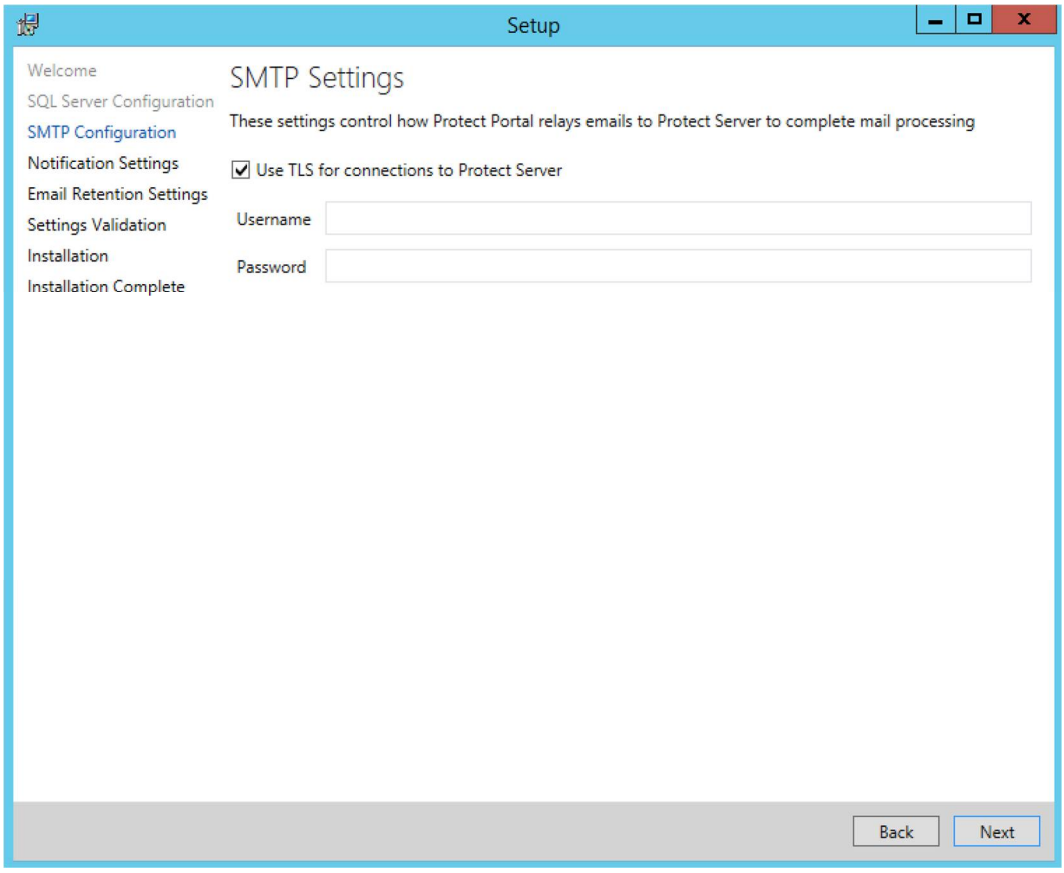
   ***Note**: If this user doesn't presently exist, the user is created and given the minimum required permissions to access the Protect Server database only.*

   If the processor user is a Windows user:

   - Select **Use Windows Authentication**.
   - Enter the domain name of the user in the text box between **User ID** and \.
   - Enter the user name in the text box to the right of the \ symbol.

   The processor user must be a pre-existing Windows user. If the user does not presently have permissions on the SQL Database, a logon will be created and the user shall be given the minimum required permissions to access the Protect Server database only.

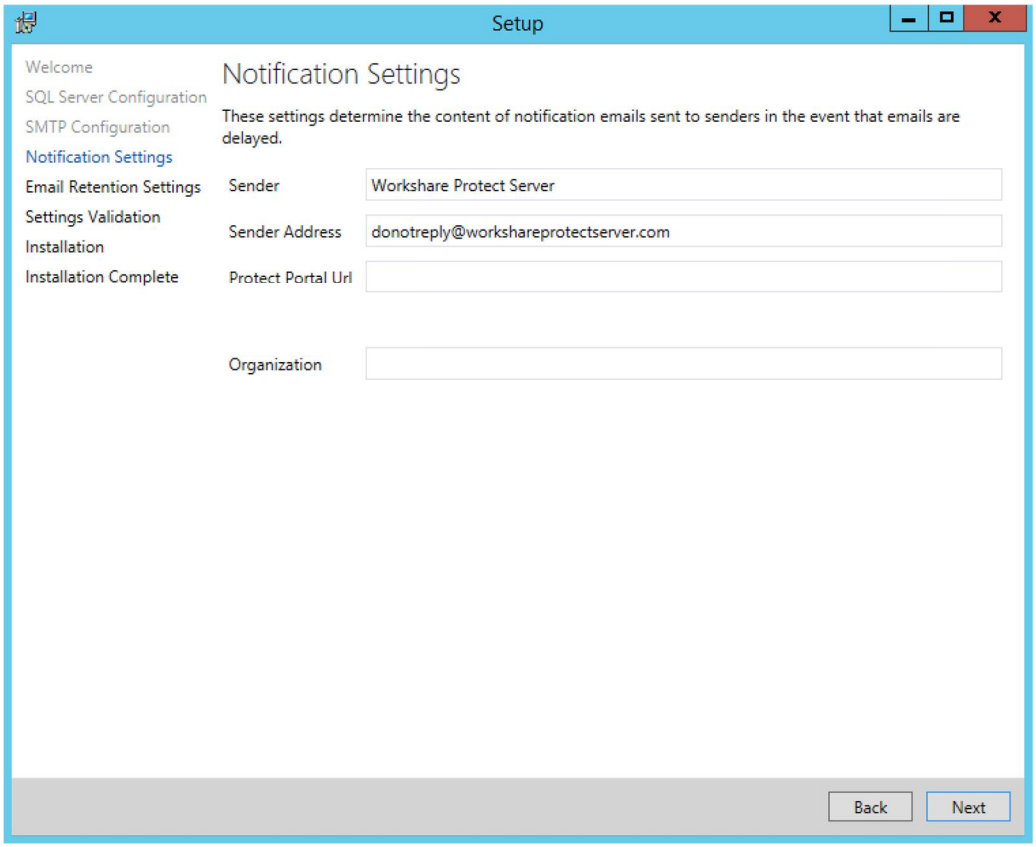
5. Click **Next**.



6. The Protect Portal uses the local SMTP server to send out notification emails and must be given any relevant authentication details.
   - If you have configured the local SMTP server to require TLS encryption, select **Use TLS for connections to Protect Server**. See Setting TLS Security for more details.
   - If you have configured a username and password for the SMTPSVC service, you may provide these here.

   The settings you have set here may be changed post installation by editing a configuration file. Refer to Protect Portal Configuration.

7. Click **Next**.



When an attachment is password-protected, the sender will receive an email notification alerting them that their email has not been sent and providing a link to a form where they can enter the password. This page is where you configure that email template.

8. In the **Sender** field, enter the display name for the sender of the notification email.
9. In the **Sender Address** field, enter the email address of the sender of the notification email.

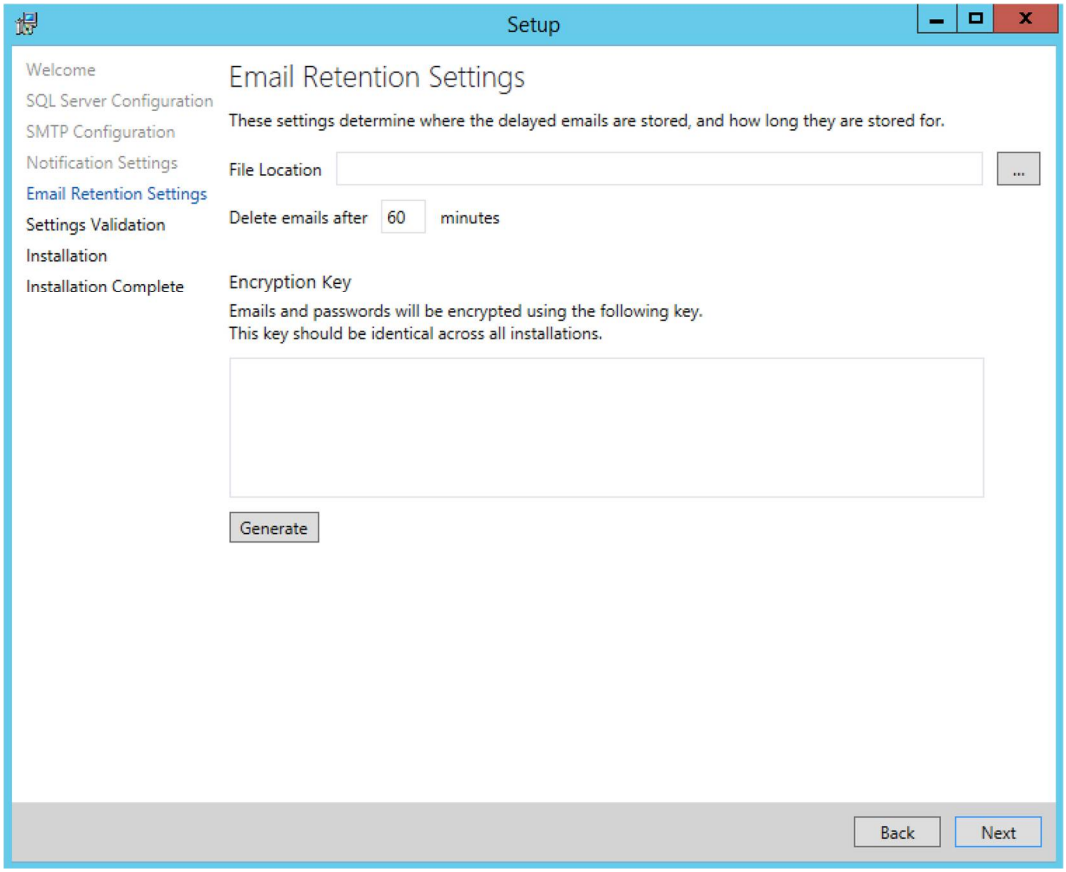
10. In the **Protect Portal Url** field, enter the URL assigned to Protect Server, if there is one. The link presented to the sender in the notification email will be [protectportalurl]/protect-portal/…

    For example, if **https://protect-server.law-firm.com** was set as the URL, the link presented to the sender will be https://protect-server.law-firm.com/protect-portal/…

> ***Notes**: Any URL specified must be https.*
>
> *If the **Protect Portal Url** field is left blank, the fully qualified domain name of the machine is used.*
>
> *To employ load balancing/high availability, administrators can set this URL to a virtual address.*

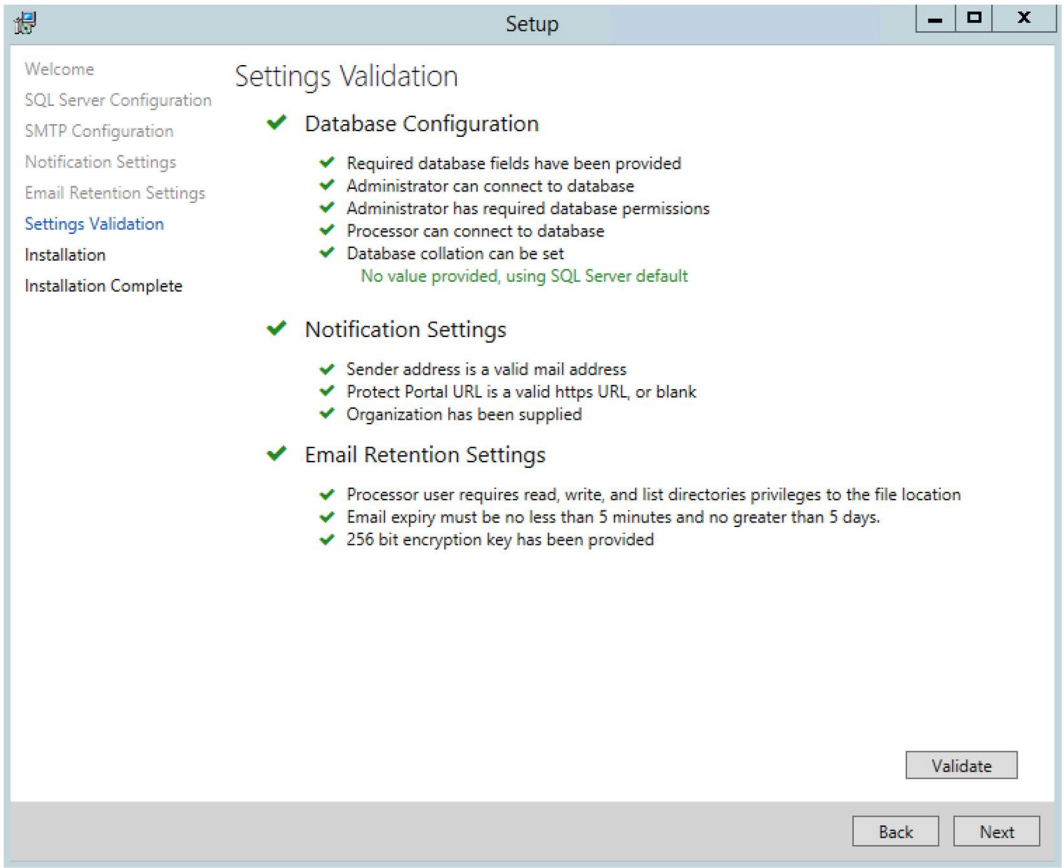
11. In the **Organization** field, specify the company name. This will be included in the form displayed to the sender, for example, "[organization] is using Workshare Protect Server to secure your emails…"

12. Click **Next**.

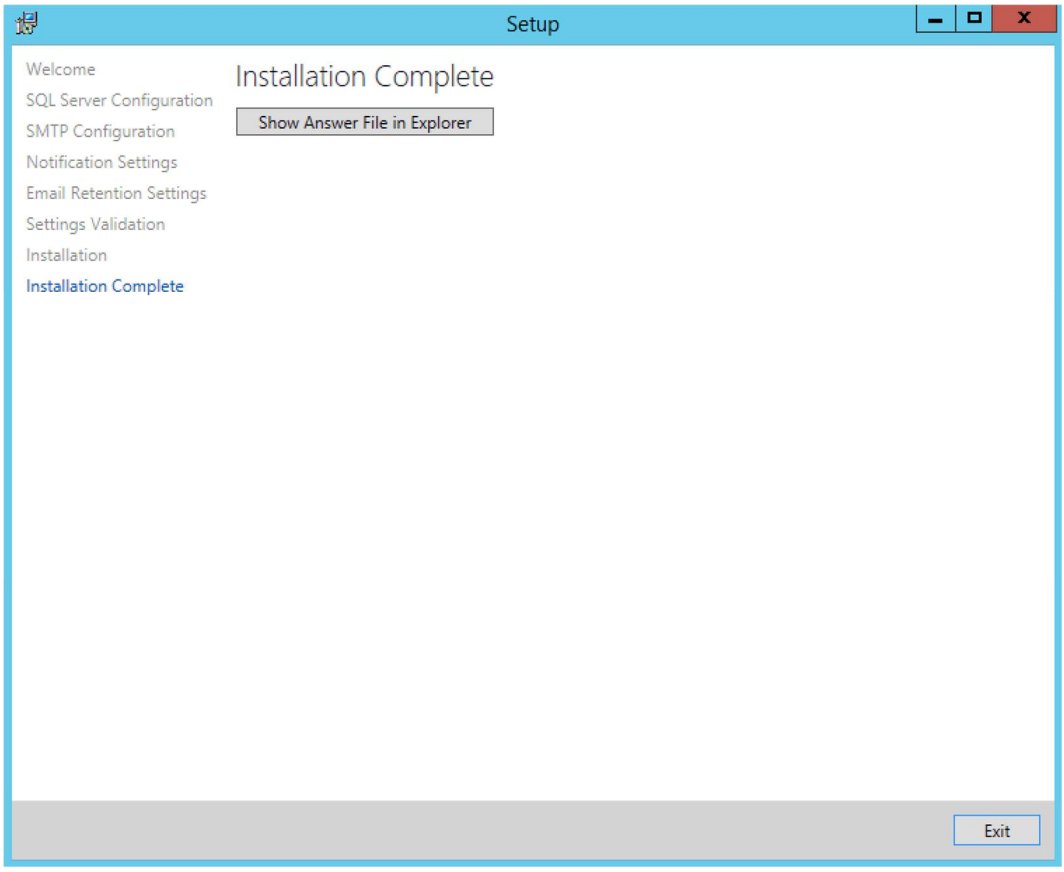


All emails awaiting input (passwords) from the senders are stored locally on Protect Server as encrypted files. The Email Retention Settings specify how and where these emails are stored.

13. In the **File Location** field, select an existing folder or create a new one to store the emails being held for processing. Each Protect Portal instance should point to the same location. A network file store is recommended.
14. By default, all files being held are deleted after 60 minutes. You can configure this as low as 5 minutes, or as high as 5 days (7,200 minutes).
15. Enter the encryption key used throughout your installation of Protect Server. The files being stored are encrypted using an encryption key and this key needs to be generated for encryption to work. For a set up with multiple Protect Servers with Protect Portal, this encryption key needs to be generated for the first installation and then re-used for all subsequent Protect Servers. If an answer file is used, then there is no additional need to remember or store this encryption key.
16. Click **Next**.
17. Click **Validate** in the Settings Validation page.



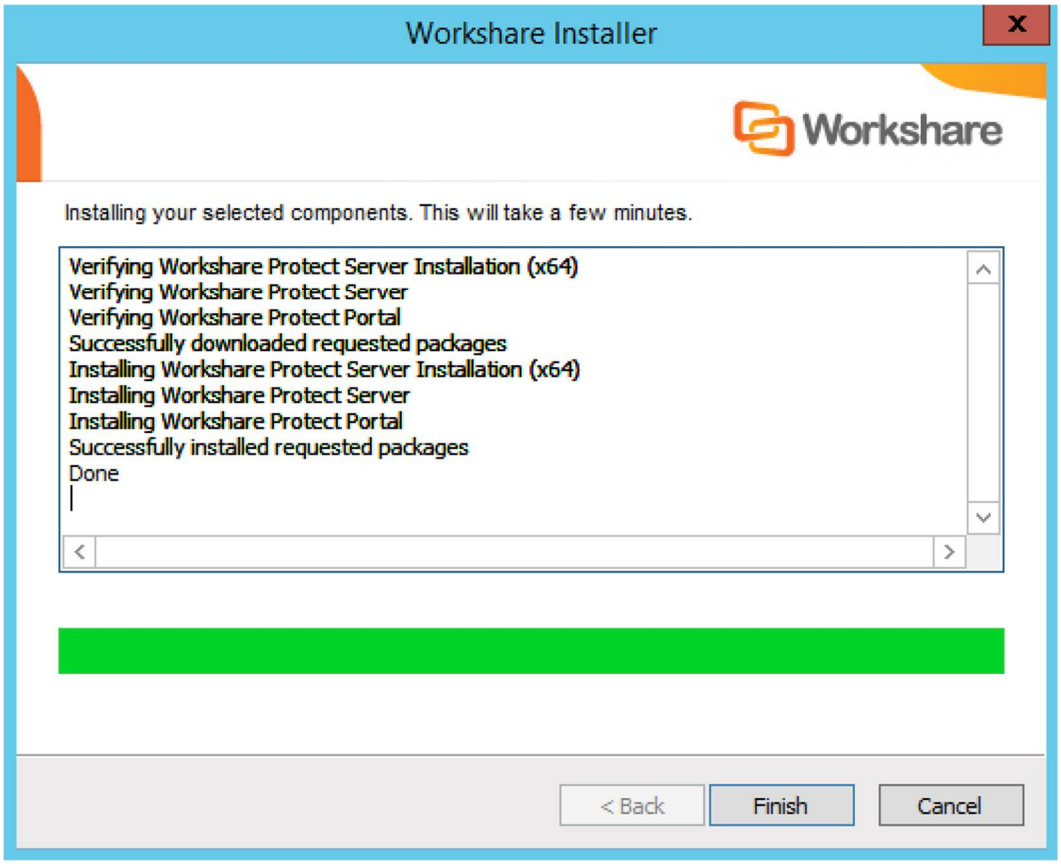
18. Once all the settings are validated, click **Next**. The Protect Portal is installed.



19. Once the installation is complete, you can display and save 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.

    In case you are setting up multiple Protect Servers, this answer file can be used during set up for subsequent installations.

20. Click **Exit**.



21. Click **Finish**.

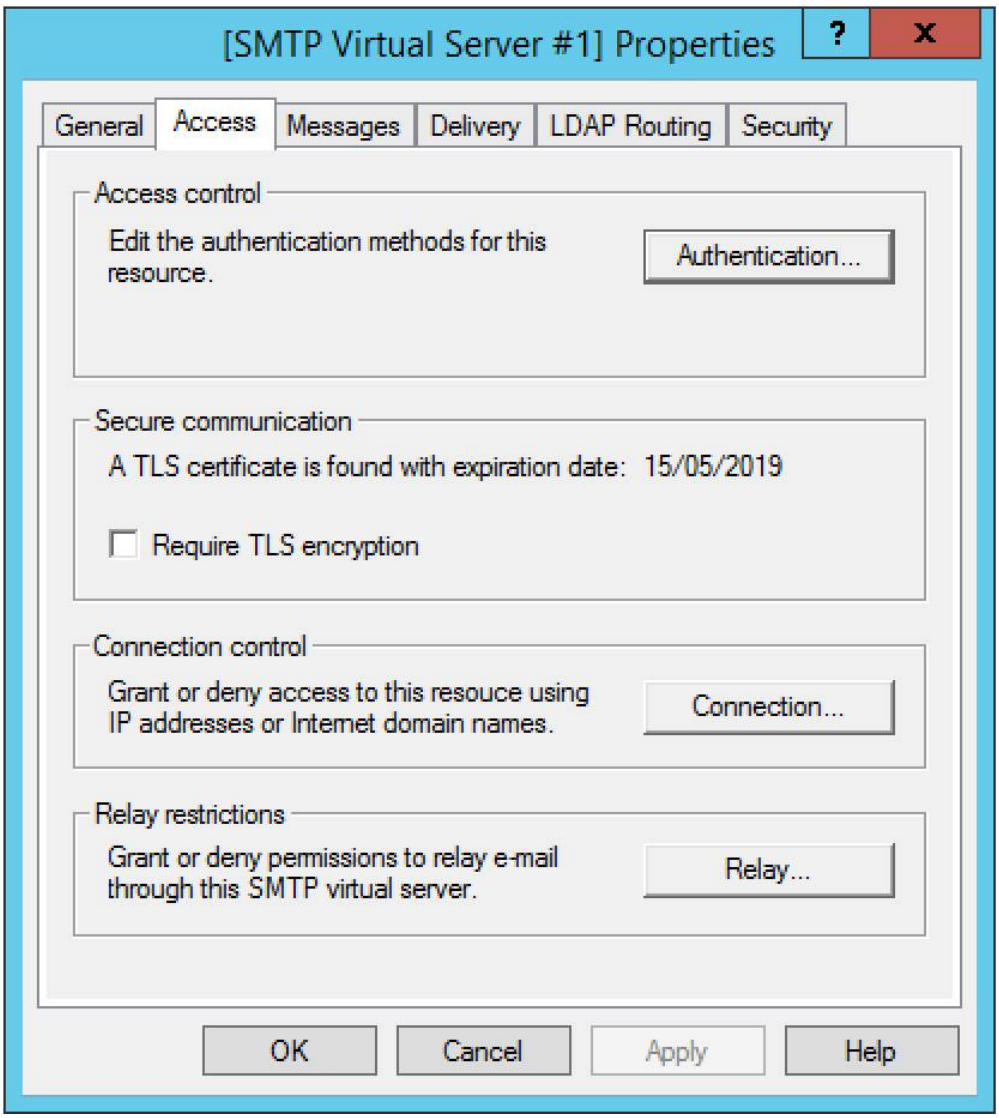
Protect Server and the Protect Portal are now installed. The Protect Server web console is now also available. See Access to the Workshare Protect Server Web Console.

Confirm IIS SMTP relay entry

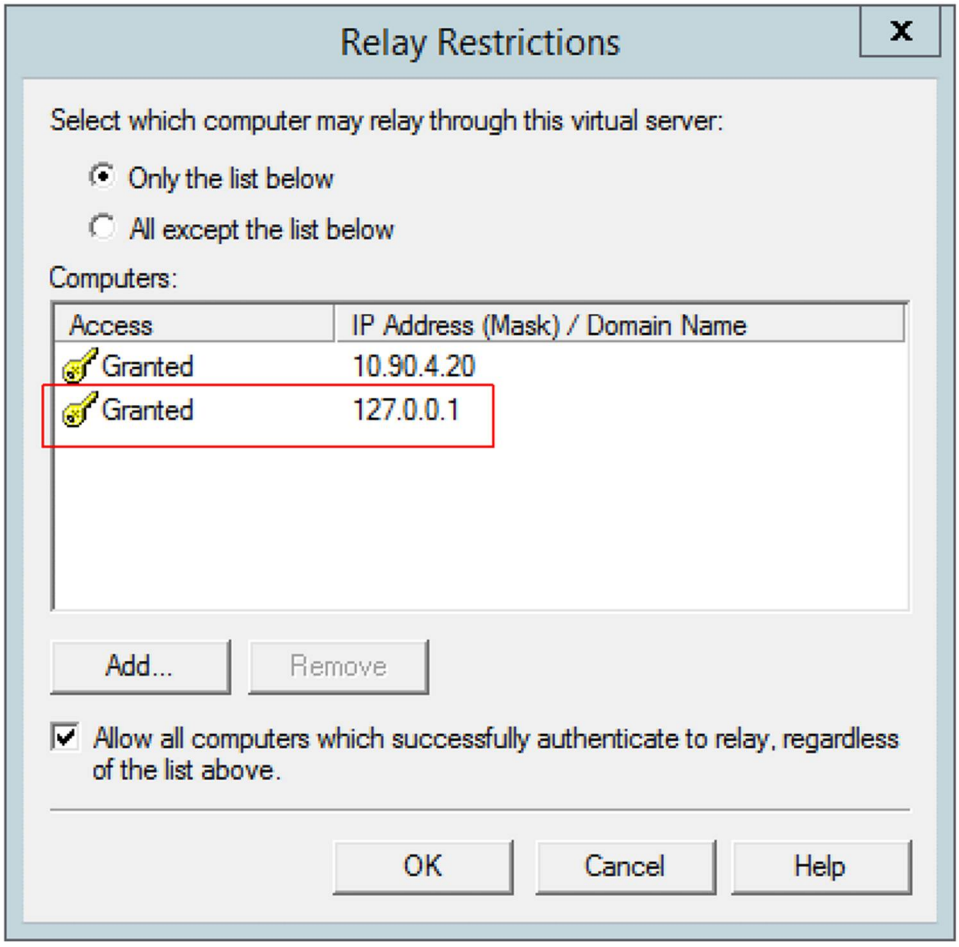
The portal installation will add 127.0.0.1 to the allowed relay server list. This allows Protect Server to relay emails to itself when dealing with password-protected emails. Confirm that 127.0.0.1 has been added.

To check the relay server list:

1. Open IIS Manager.
2. Right click the SMTP Virtual Server you want to check the relay entry for and select **Properties**.
3. Select the **Access** tab.



4. Click **Relay**.



5. If 127.0.0.X does not appear in the list, click **Add** to add it.

Configuring multiple Workshare Protect Server connections to a single database

In order to have multiple Protect Servers pointing to the same SQL server, run the installation on each server that will host Protect Server. Select the same settings each time. The installation will not update the database server unless there were any changes to the security roles.

Shutting down Workshare Protect Server

Protect Server may be started and shut down in the standard way (provided the services are configured correctly) in Windows Services, as follows:

Required Services	Service (recommended “startup type”)
Workshare Protect Server Active Directory Cache Service	Required - Automatic (Delayed Start)
Workshare Protect Server License Service	Required - Automatic (Delayed Start)
Workshare Protect Server Audit Service	Required - Automatic (Delayed Start)
Workshare Protect Server Health Service	Required - Automatic (Delayed Start)
Workshare Protect Server Profile Service	Required - Automatic (Delayed Start)
Workshare Protect Server Mail Updater Service	Required - Automatic (Delayed Start)
IIS Admin Service	Required (Automatic)
Simple Mail Transfer Protocol (SMTP)	Required (Automatic)
SQL Server (MSSQLSERVER)	Required (Automatic)
SQL Full-text Filter Daemon Launcher (MSSQLSERVER)*	Required (Automatic)

***Note**: *The Full Text search functionality of Workshare Protect Server requires that the SQL Full-text Filter Daemon Launcher (MSSQLSERVER) service is running. This is disabled by default.*

***Note:** After install, the Workshare services all have a startup type of **Automatic** but after a reboot the startup type becomes **Automatic (Delayed Start)**.*

Uninstalling Workshare Protect Server

The uninstalling of Protect Server will not automatically remove the SQL database so data is still available.

When uninstalling Protect Server, ensure you complete the following steps:

- Drop the Protect Server database.
- Delete the Profiles and ADCache folders which can be found in “C:\Users\<processor role>\AppData\Local\Workshare\Protect Server\[version].
- Drop the Protect Server User Group login.
- Drop the SMTP login if it is the hidden machine account. (This is when Protect Server is installed on a different server then SQL.)

- Change SMTP login default database to master if user is NT AUTHORITY\SYSTEM. (This is when Protect Server is installed on the same server as SQL.)

These steps must be completed otherwise any follow on installations may fail. The main reason is that the default database assigned no longer exists.

***Note**: The installer user should NOT belong to the Protect Server User security group. The reason is that if the installer user is not explicitly added to the SQL database, but uses one of the security groups for example Administrators, and the Protect Server User security group is Domain Users (not recommended). Then when the installer logs in they are authenticated against both groups to make sure they are allowed access. If the database that the Domain Users has set as default is dropped then when the installer user logs in, it will fail, because the Domain Users default database no longer exists, even if the Administrators does. A security failure will always trump a success. The installer user may still be able to connect if the default database is explicitly set in the connection.*

Upgrading Workshare Protect Server

The latest version of Protect Server supports upgrades from previous versions back to Protect Server 3.6. The upgrade process is automatic and running the new Protect Server installation file will automatically uninstall the previous installation before running the new Protect Server installer. The uninstall will preserve the Protect Server database and once the new Protect Server installer runs it will upgrade the existing database preserving all data therein. The following steps should be taken prior to the upgrade process.

Step 1: Backup the existing Workshare Protect Server database

It is recommended that you perform the backup at the latest possible time before the upgrade procedure.

Step 2: Ensure install user requirements

For the upgrade/install, the install user will need to be logged into the Protect Server machine as a DOMAIN user who:

- Is a local administrator on the machine (in order to execute the installation itself)
- Is a user on the MSSQL server hosting the Protect Server database with the sysadmin role

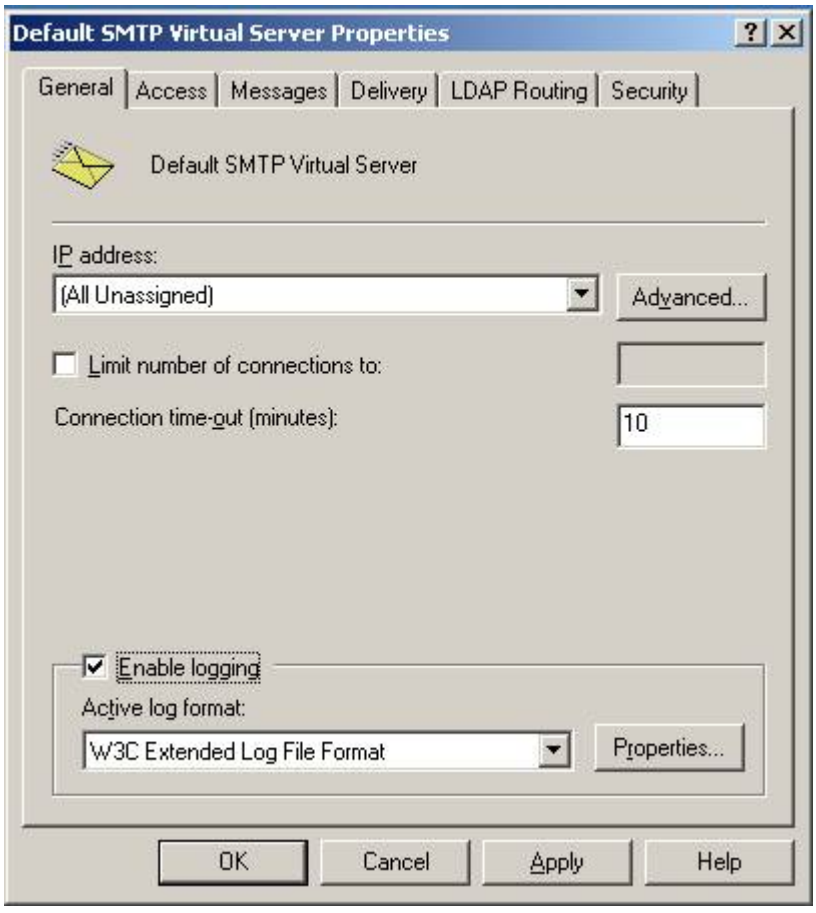
The version of Protect Portal included in the 3.11 release has been upgraded to 4.1. It is recommended that when upgrading to 3.11, the Protect Portal is also upgraded to 4.1.

Turning on Email Message Logging

In order to properly diagnose errors with messages processed by Workshare Protect Server, logging of messages must be turned on for the Windows SMTP service. This serves the same purpose as the Message Tracking feature of Microsoft Exchange and allows you to track the processing of a message with greater granularity.

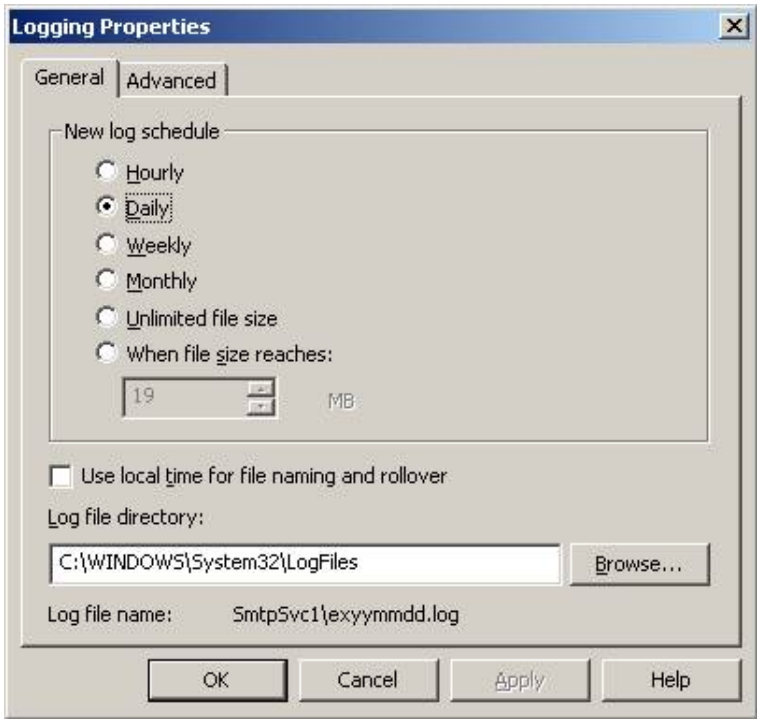
To enable the access log for a Windows SMTP Virtual Server

1. Open IIS Manager.
2. Right click the SMTP Virtual Server you want to enable an access log for and select **Properties**.

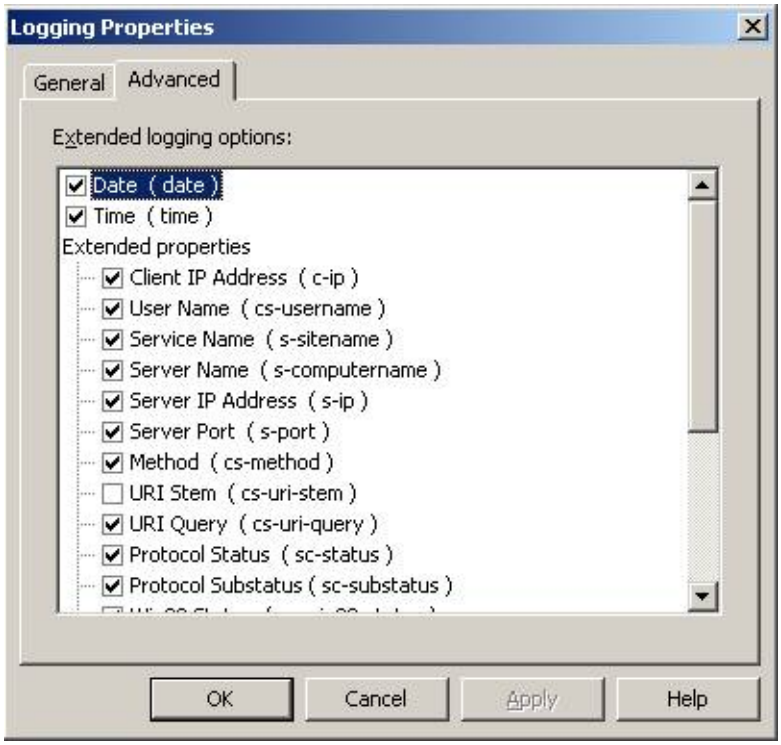


3. Check the **Enable logging** checkbox, and make sure **W3C Extended Log File Format** is selected from the **Active log format** dropdown list.

4. Click the **Properties** button.

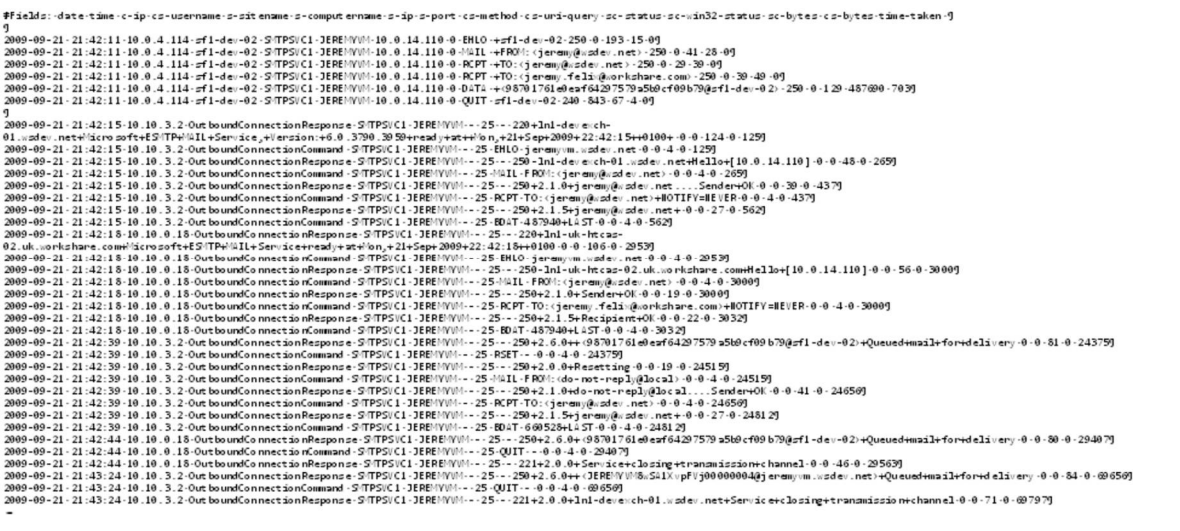


5. Select an appropriate log schedule.
6. Select the **Advanced** tab.



7. Make sure the following checkboxes are selected:
   - Date
   - Time
   - Client IP Address
   - User Name
   - Service Name
   - Server Name
   - Server IP Address
   - Server Port
   - Method
   - URI Query
   - Protocol Status
   - Protocol Substatus
   - Win32 Status
   - Bytes Sent
   - Bytes Received
   - Time Taken
8. Click **OK** and then **OK** again to save the settings.

The output of the log file will be in the C:\WINDOWS\system32\LogFiles\SMTPSVC* folder, and will look like the following:



The log entries above are for a single mail passing through the product. The first 6 entries indicate the reception of the email from the mail server or client mailer, and list the MAIL FROM and RCPT TO commands. The following entries indicate the delivery of the mail to the downstream mail server (in this case, final delivery was performed, so there are entries for submission to both the wsdev.net and workshare.com mail servers).

Accessing the Workshare Protect Server Web Console

Using the Workshare Protect Server web console, you configure what metadata should be removed from email attachments as well as other useful configuration settings, such as licensing and whether clean reports should be sent. The Protect Server web console supports the following browsers:

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome

To access the Protect Server web console:

1. Open a web browser and enter http://[URL to Protect Server] in the address bar. During installation, the Protect Server URL is automatically generated in the format http://localhost/Protect. The login page is displayed.

> ***Note**: You can change the Protect Server URL using IIS.*

2. Enter your login credentials and click **OK**. The **Messages** page of the Workshare Protect Server web console is displayed.

Overview of console tabs

The availability of tabs in the Protect Server web console depends on the type of user accessing the console. During installation, Active Directory user groups are assigned to the Protect Server roles and tab access in the Protect Server web console is determined according to the role you have. The Protect Server roles are as follows:

- Administrator role users can access all tabs of the Protect Server web console except for the **Reports** tab, so they can configure profiles and other Protect Server settings, view system status information and search through all emails sent through Protect Server.
- Business role users can access all tabs of the Protect Server web console except for the **Status** and **Settings** tabs, so they can search through emails that they themselves have sent through Protect Server, view statistics about the metadata cleaned by Protect Server and view profiles configured on Protect Server. They cannot search or view emails sent by other users and they cannot create new profiles or modify or delete existing profiles.
- User role users can only access the **Messages** and **Profiles** tabs of the Protect Server web console, so they can search through and view emails that they themselves have sent through Protect Server and view profiles configured on Protect Server. They cannot search or view emails sent by other users and they cannot create new profiles or modify or delete existing profiles.

Status tab

Administrator role users can view the **Status** tab. This tab provides information about the performance and current health of Protect Server. For example, the **Status** tab shows whether Protect Server services are up and running, whether the database is connected, whether the Protect Server license is expired and details of any emails queued on Protect Server.

Reports tab

Business role users can view the **Reports** tab. This tab provides more detailed statistics on the activities of Protect Server. For example, how many emails were processed using each profile and how many emails were processed in Microsoft Word format.

Messages tab

All role users can view the **Messages** tab. However, the functionality differs, as follows:

- Administrator role users can search through all emails sent through Protect Server.
- Business and User role users can only search through and view emails that they themselves have sent through Protect Server. They cannot search or view emails sent by other users.

Profiles tab

All role users can view the view the **Profiles** tab. This tab provides access to the profiles configured on Protect Server. Administrator role users can add new profiles and edit or delete existing profiles, however Business and User role users can only view existing profiles.

Settings tab

Administrator role users can view the **Settings** tab. This tab provides access to Protect Server configuration settings such as whether clean reports should be sent, how to override cleaning settings as well as configuring alert settings and email templates. It also provides access to the Policy Editor.

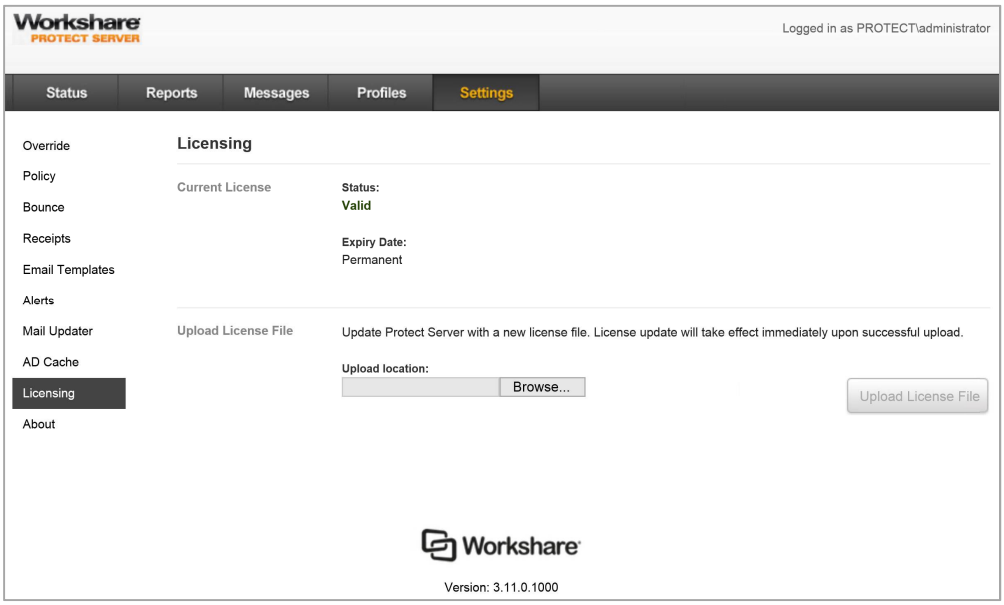
Licensing

After install, you must license Workshare Protect Server. Until you enter a valid license, Protect Server will not clean any emails - they will simply be forwarded to your configured smart host or delivered to the recipients.

Licensing is done using a .lic file.

To license Protect Server:

1. Log into the Protect Server web console (as an Administrator role user).
2. Select **Settings**.
3. Select **Licensing**. The status of your current license is displayed in the **Current License** field.



4. Click **Browse** and browse to the location of your saved license file.
5. Click **Open**.
6. Click **Upload License File**. The file is uploaded, a message is displayed across the top of the screen and the status changed accordingly.

Renewing a license

When you renew your Protect Server license, you will need to upload a new license file via the Protect Server web console in order to reflect the new subscription period. If the existing license expires and a new license file is not uploaded then emails will either pass through unprocessed or bounce back to the sender according to the Fail Close and Bounce Functionality. If you have not received an updated license file and need one, please contact the Workshare support team.

To renew your Protect Server license:

1. Log into the Protect Server web console (as an Administrator role user).
2. Select **Settings** and then **Licensing**.
3. Click **Browse** and browse to the location of your saved new license file.
4. Click **Open**.
5. Click **Upload License File**. The new file is uploaded.

Chapter 4: Configuring the Mail Server

This chapter describes how to configure your system to work with Workshare Protect Server. It includes the following sections:

- **Configuring your Corporate Mail Server**, page 58, describes how to configure your Microsoft Exchange server to route mail through Protect Server.
- **Additional Administrative Tasks**, page 86, describes other configuration tasks you may need to complete, such as configuring the Windows SMTP Service maximum message size.

Configuring your Corporate Mail Server

After installing Workshare Protect Server, you must configure your corporate mail server to relay mail to Protect Server. You must also allow Protect Server to send emails back through your email server. This section describes how to configure Microsoft Exchange.

Protect Server has been certified against Microsoft Exchange 2010 SP3 to Microsoft Exchange 2013 SP1 as well as Microsoft Exchange 2016 (RTM and CU4).

You should not configure an intermediate SMTP relay between Microsoft Exchange server and Protect Server.

Microsoft Exchange 2016

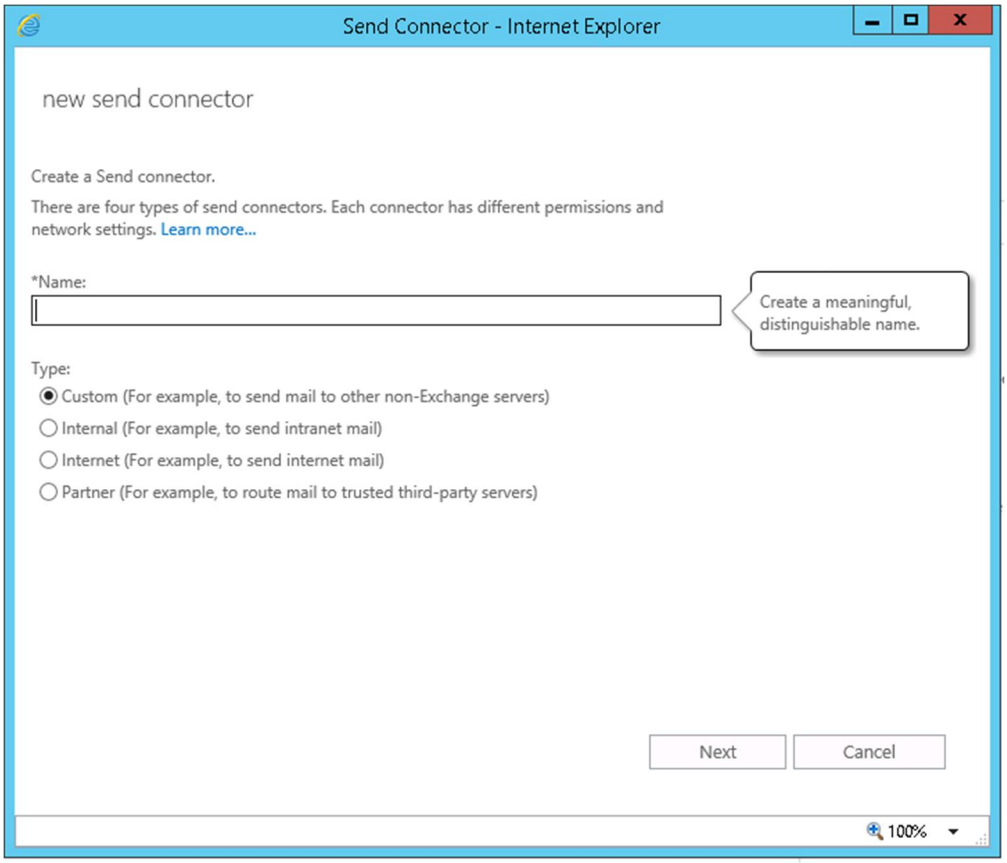
The following procedure uses Microsoft Exchange 2016.

***Note**: A sample procedure using Microsoft Exchange 2010 SP3 is also provided.*

To configure Microsoft Exchange 2016:

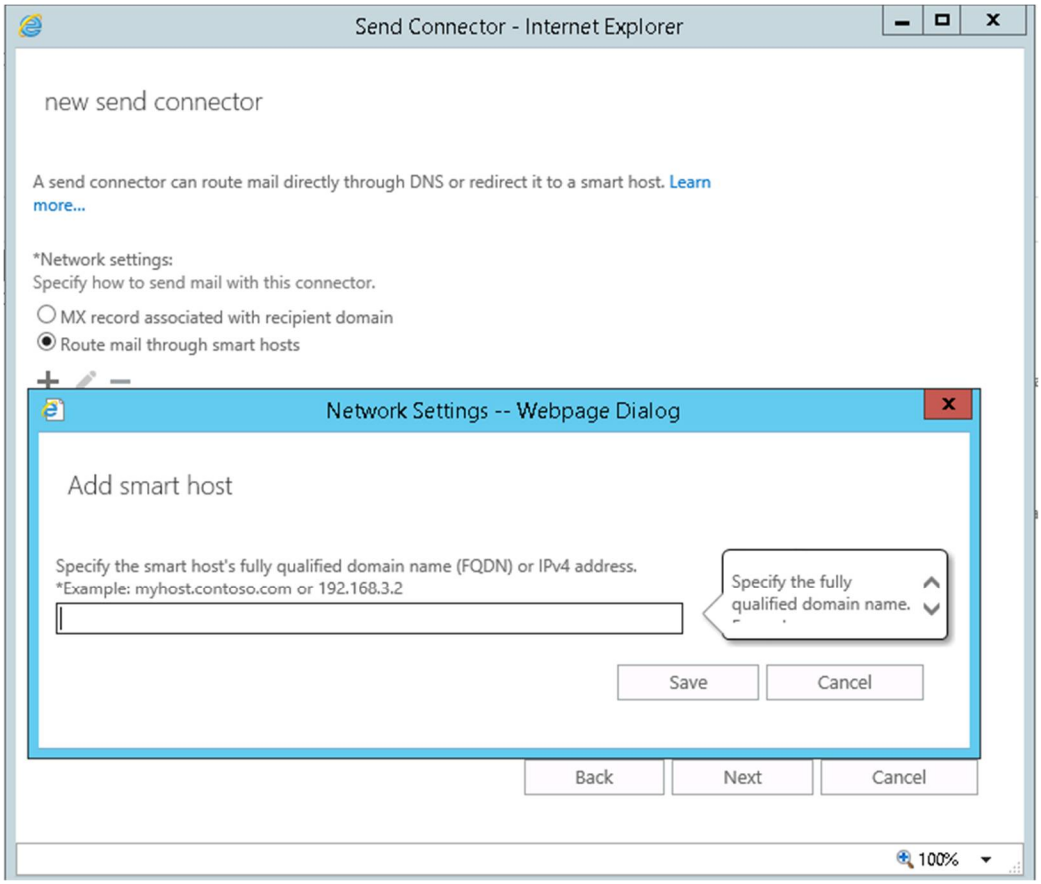
1. Log in to the Exchange admin center at https://localhost/ecp.
2. In the left panel, select **Mail Flow**.
3. Select **Send Connectors** across the top.

4. Click the add + button.



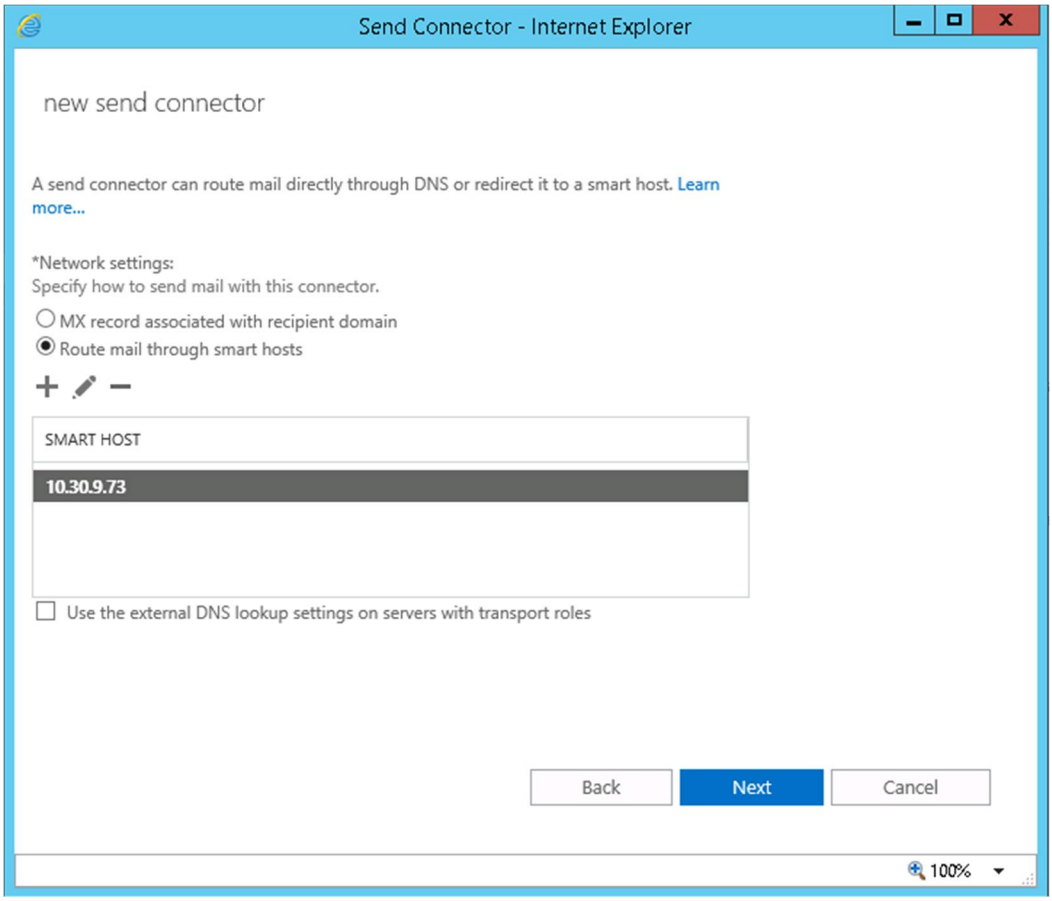
5. In the **Name** field, enter a name for the connector, for example, ProtectServer.
6. Leave the type as **Custom**.
7. Click **Next**.

8. Select the **Route mail through the smart hosts** radio button and click the add button.

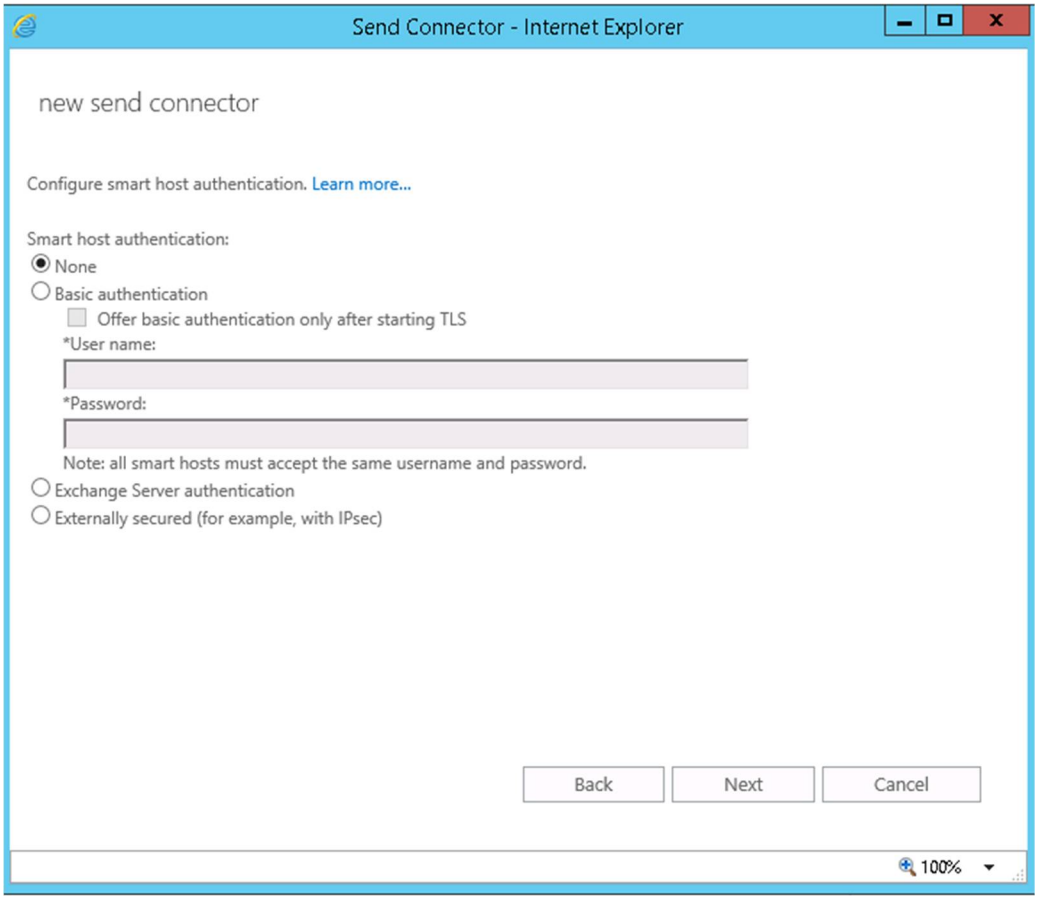


9. Enter the IP address or fully qualified domain name of Protect Server.

10. Click **Save**. The smart host is added to the list.



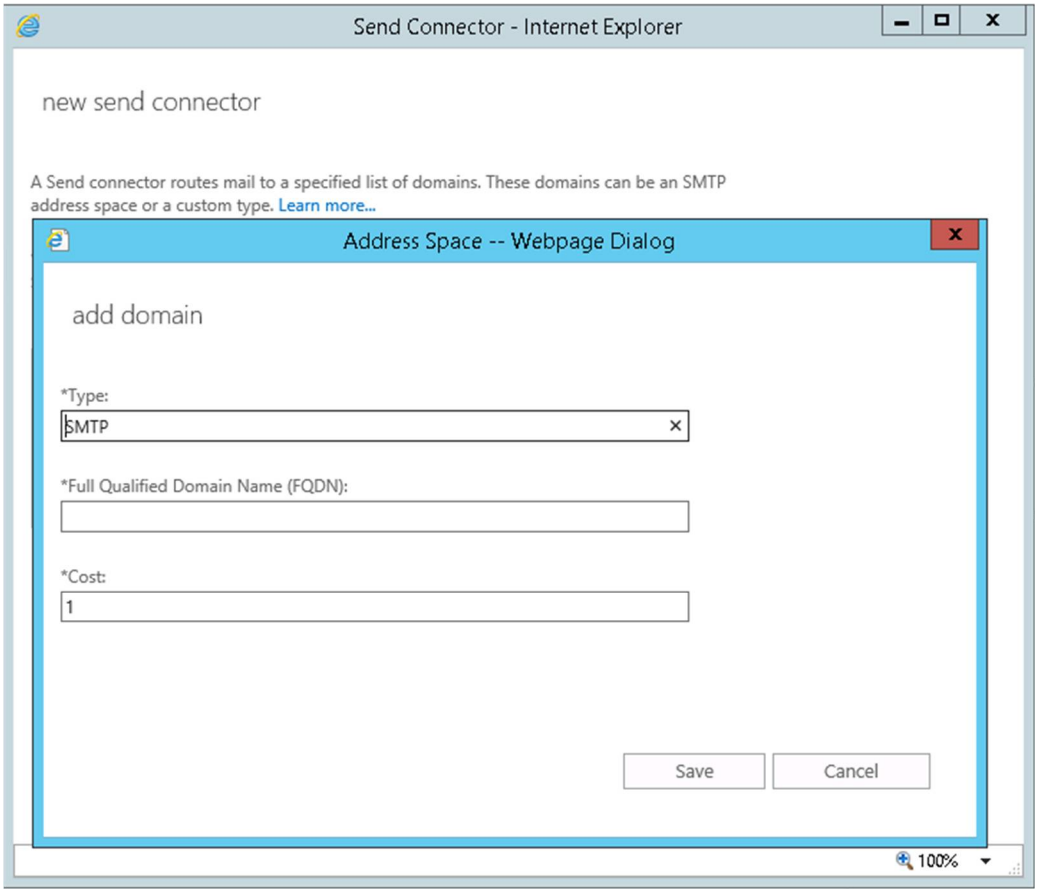
11. Click **Next**.



12. By default, Workshare Protect Server does not use authentication so there is no need to change the settings. However, if you set up authentication of Protect Server, you will need to configure authentication settings.

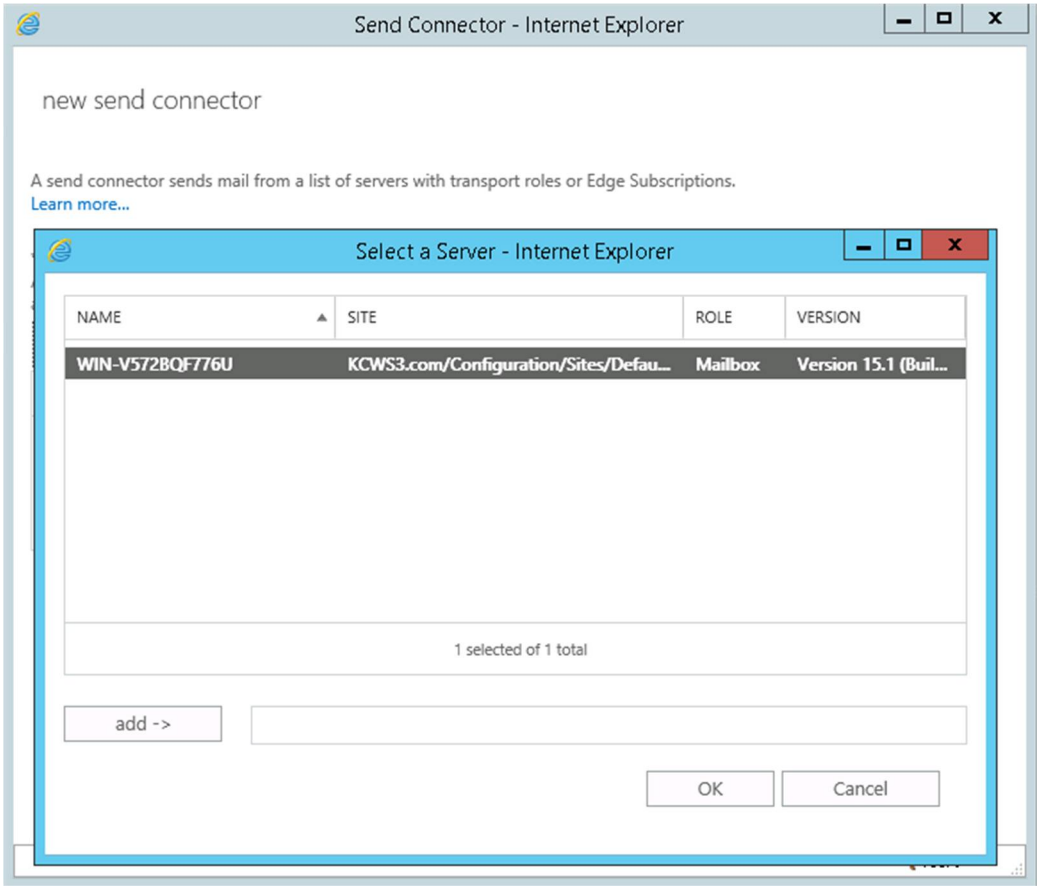
13. Click **Next**.

14. Click the add button.



15. In the address field, enter * so that all addresses are routed through Protect Server.

16. Click **Save** and click **Next**.



17. Select the server and click **OK**.

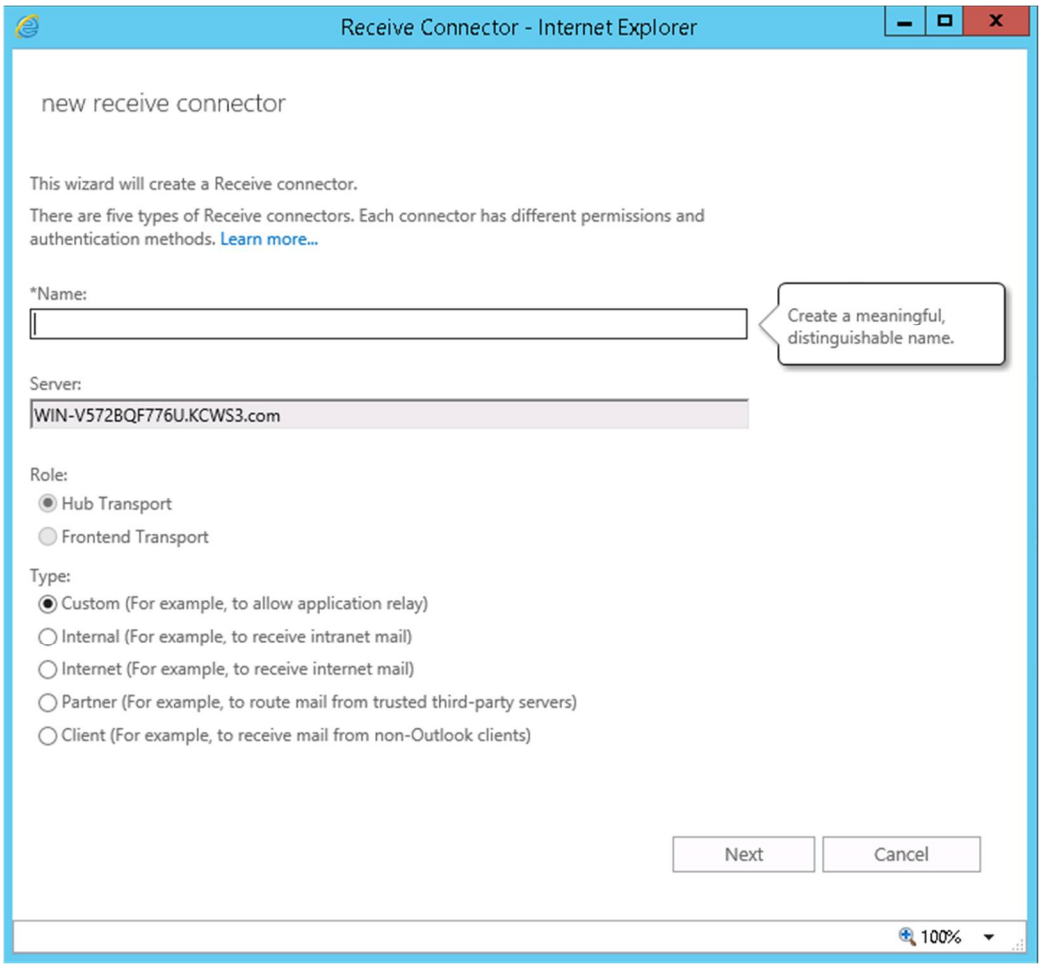
18. Click **Finish**. A new send connector is created and a confirmation message is displayed. All mail from this Microsoft Exchange server will now be routed through Protect Server.

Setting Permissions on Receive Connector – Exchange 2016

In order to allow Protect Server to send emails back through Microsoft Exchange, you must create a new receive connector for Protect Server and specify access permissions.

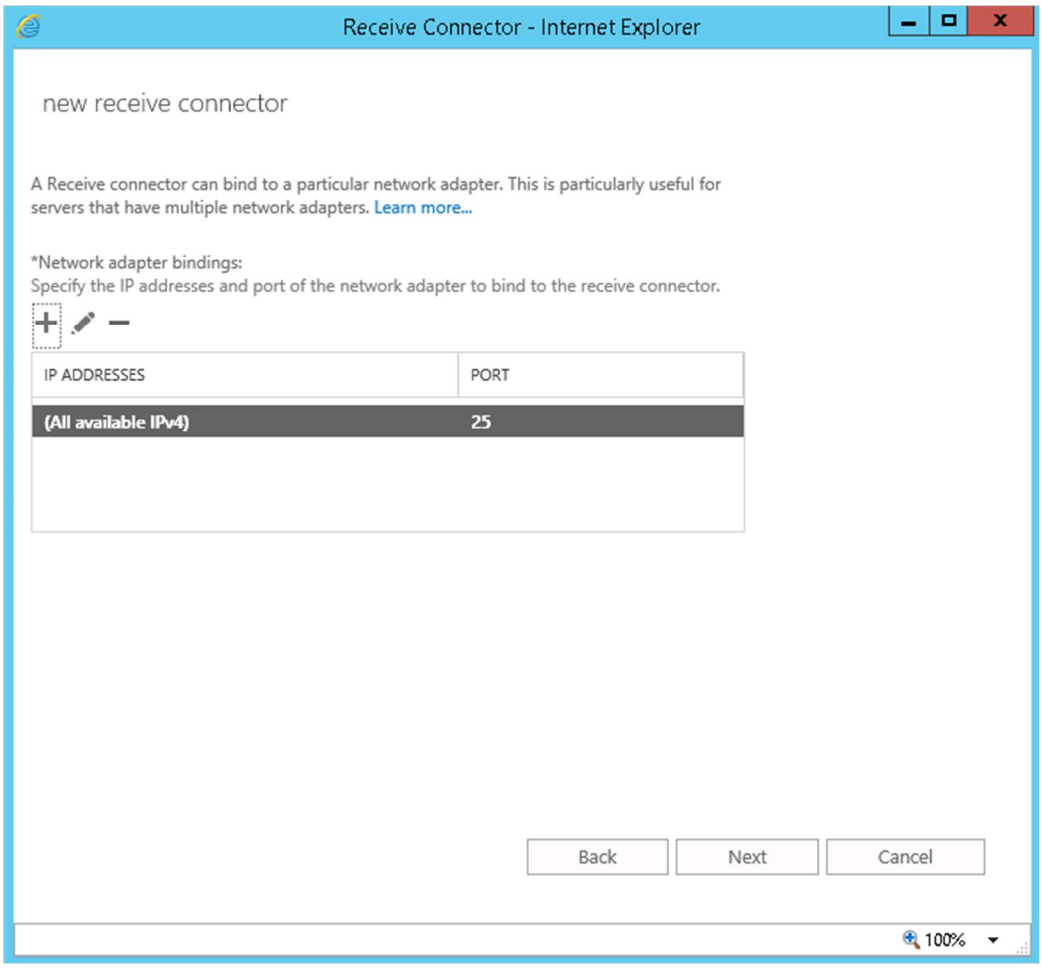
To set permissions:

1. Log in to the Exchange admin center at https://localhost/ecp.
2. In the left panel, select **Mail Flow**.
3. Select **Receive Connectors** across the top.
4. Click the add + button.



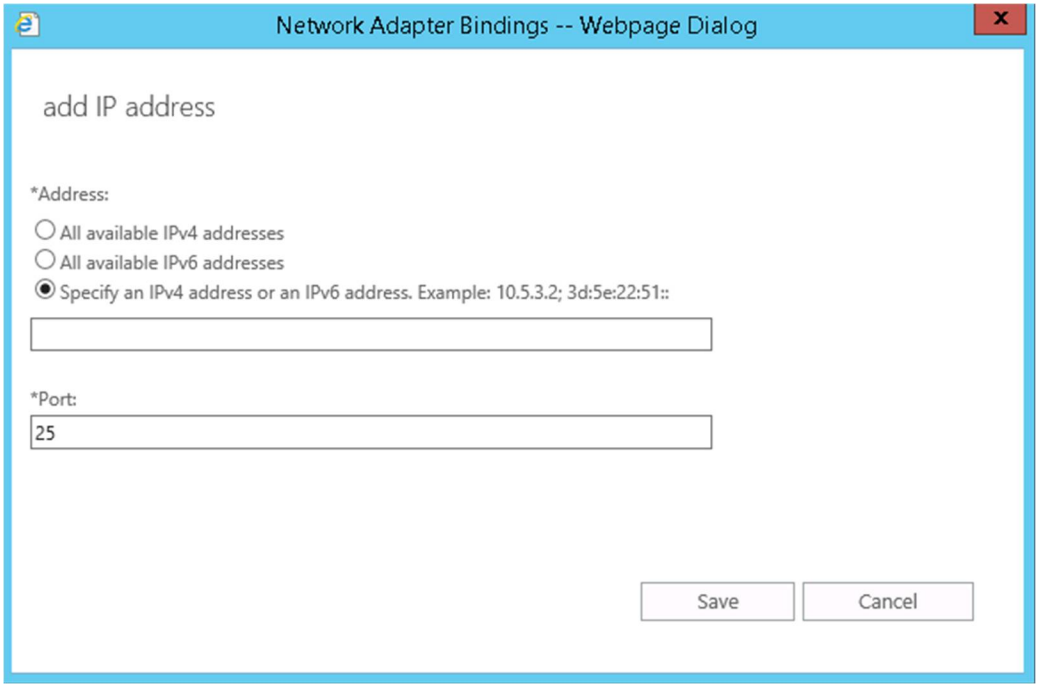
5. In the **Name** field, enter a name for the connector.
6. Leave the role as **Hub Transport** and the type as **Custom**.

7. Click **Next**.



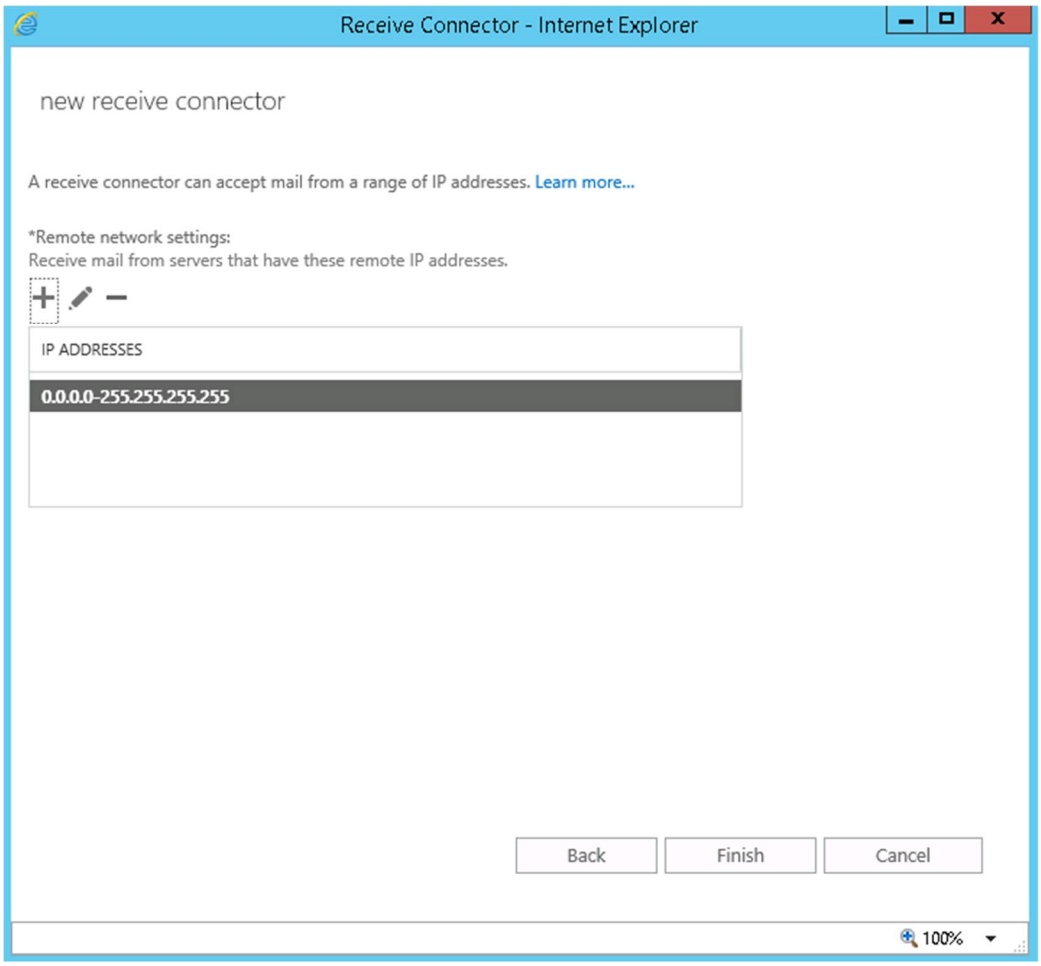
8. Select any existing entries in the table and click the delete button.

9. Click the add button.

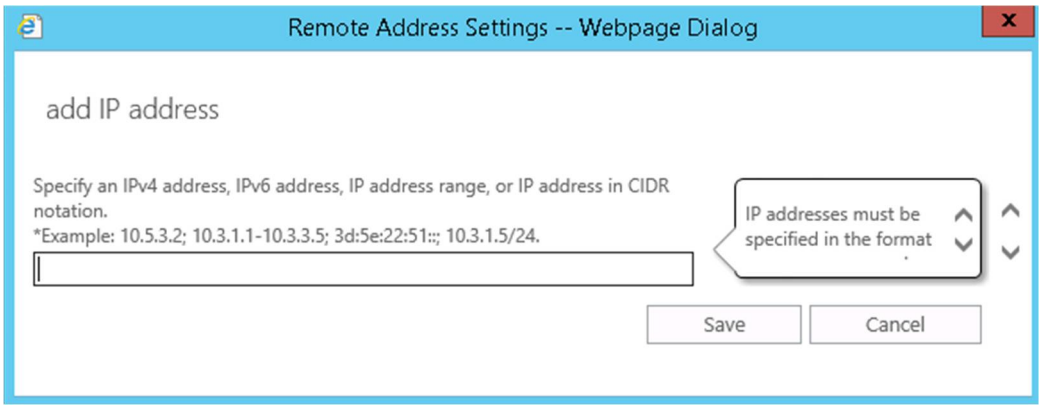


10. Enter the IP address of Protect Server.
11. Click **Save**.

12. Click **Next**.

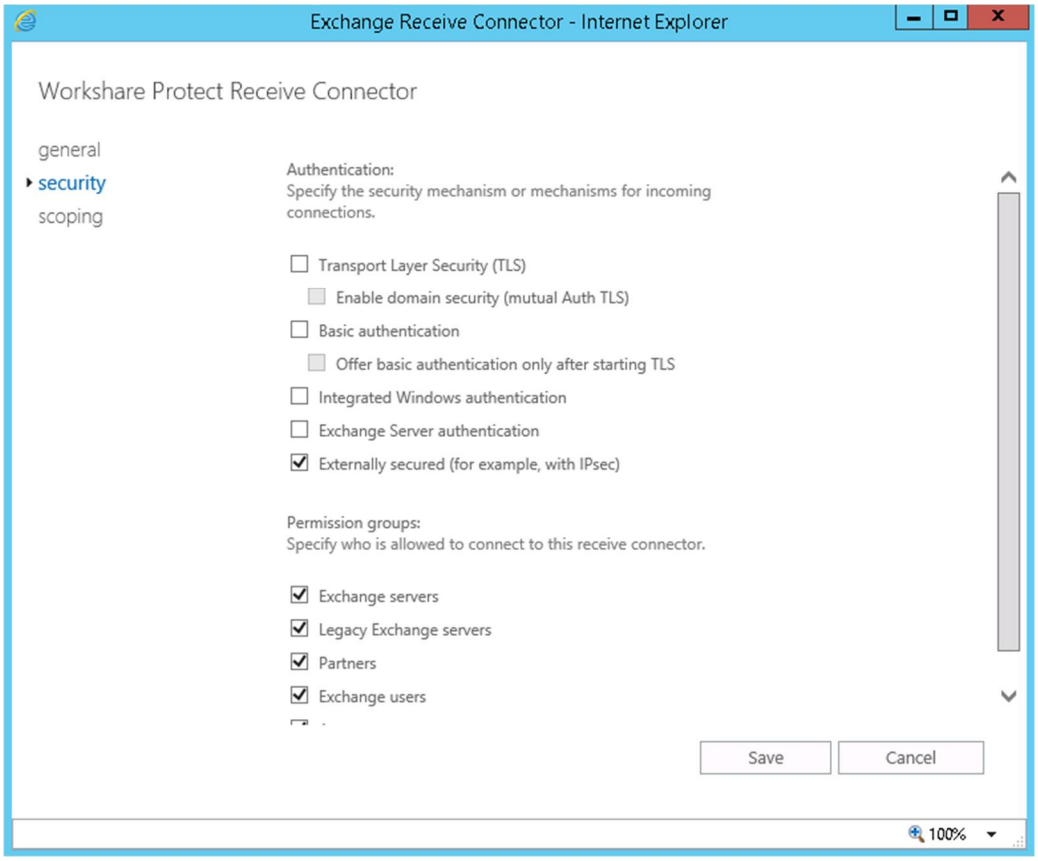


13. Select any existing entries in the table and click the delete button.
14. Click the add button.



15. Enter the IP address of Protect Server.
16. Click **Save**.

17. Click **Finish**.
18. In the list of receive connectors, double-click the new receive connector you have just created.
19. Select **Security** on the left.



20. Make sure the **Anonymous users** checkbox in the **Permissions groups** area is selected.
21. Click **Save**.

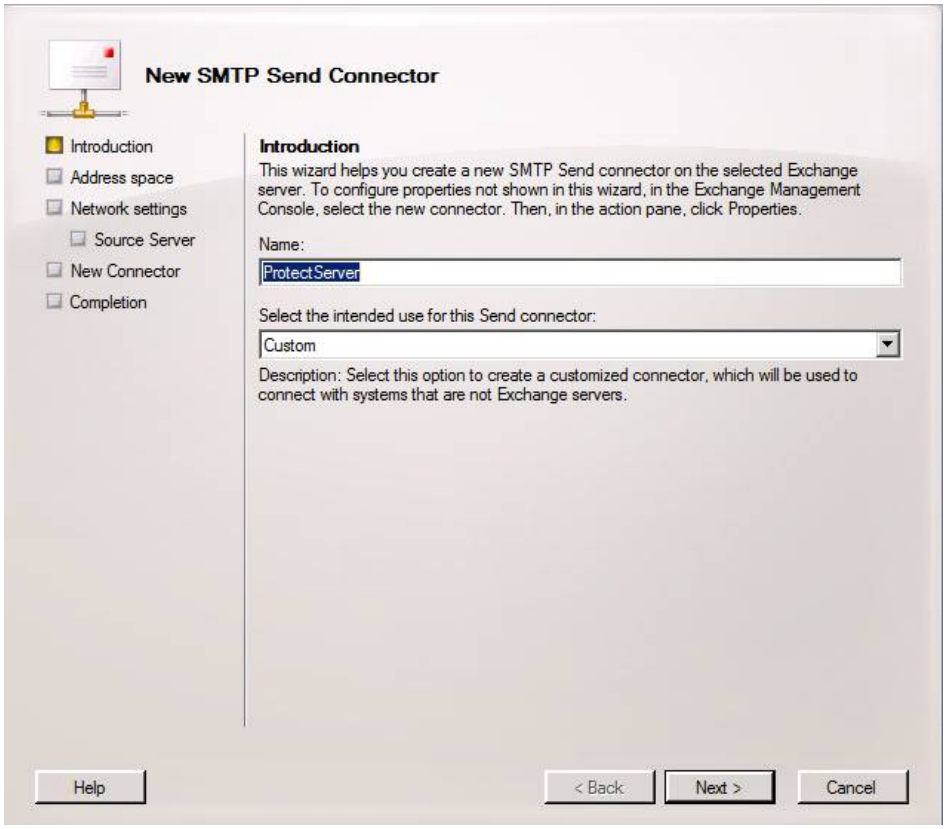
Microsoft Exchange 2010

The following procedure shows how to configure Microsoft Exchange 2010 SP3 to route mail through Protect Server.

To configure Microsoft Exchange:

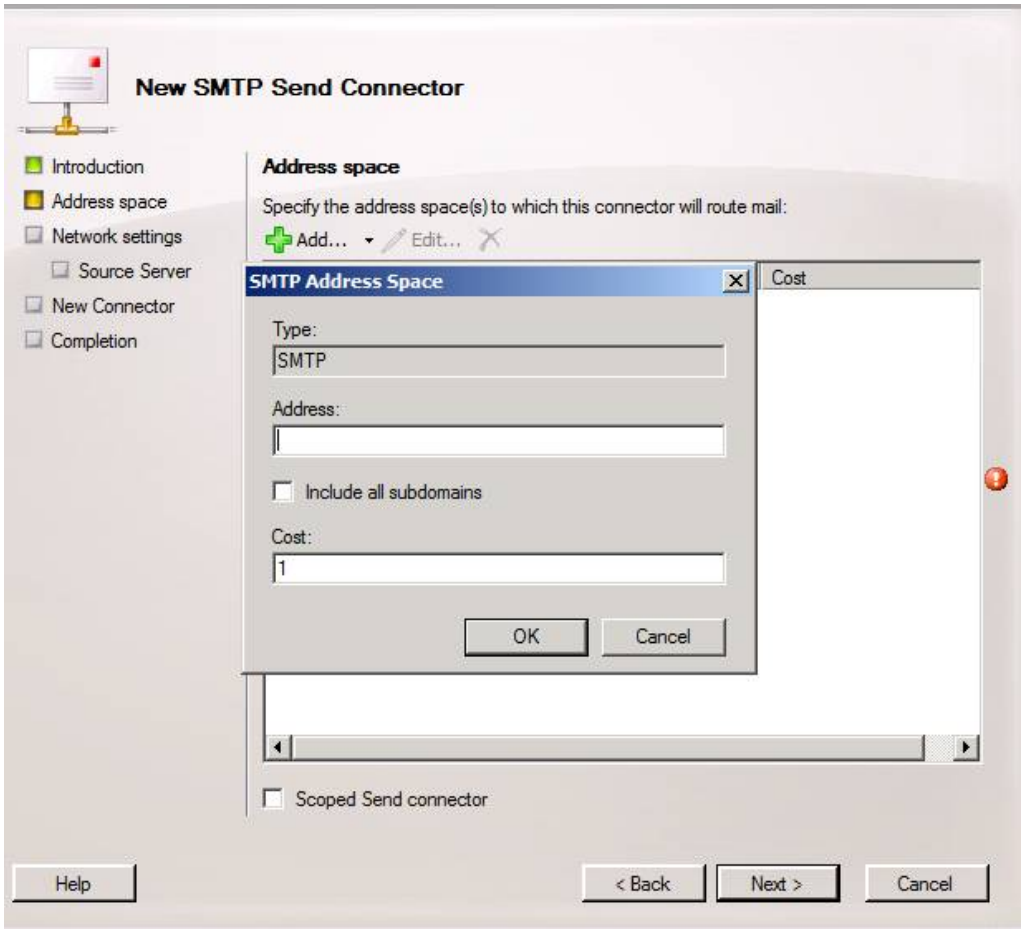
1. Launch the Exchange Management Console.
2. In the left panel, select **Organization Configuration** and then **Hub Transport**.
3. Select the **Send Connectors** tab.

4. In the Actions panel on the right, click **New Send Connector**. The New SMTP Send Connector is launched with the Introduction page displayed.



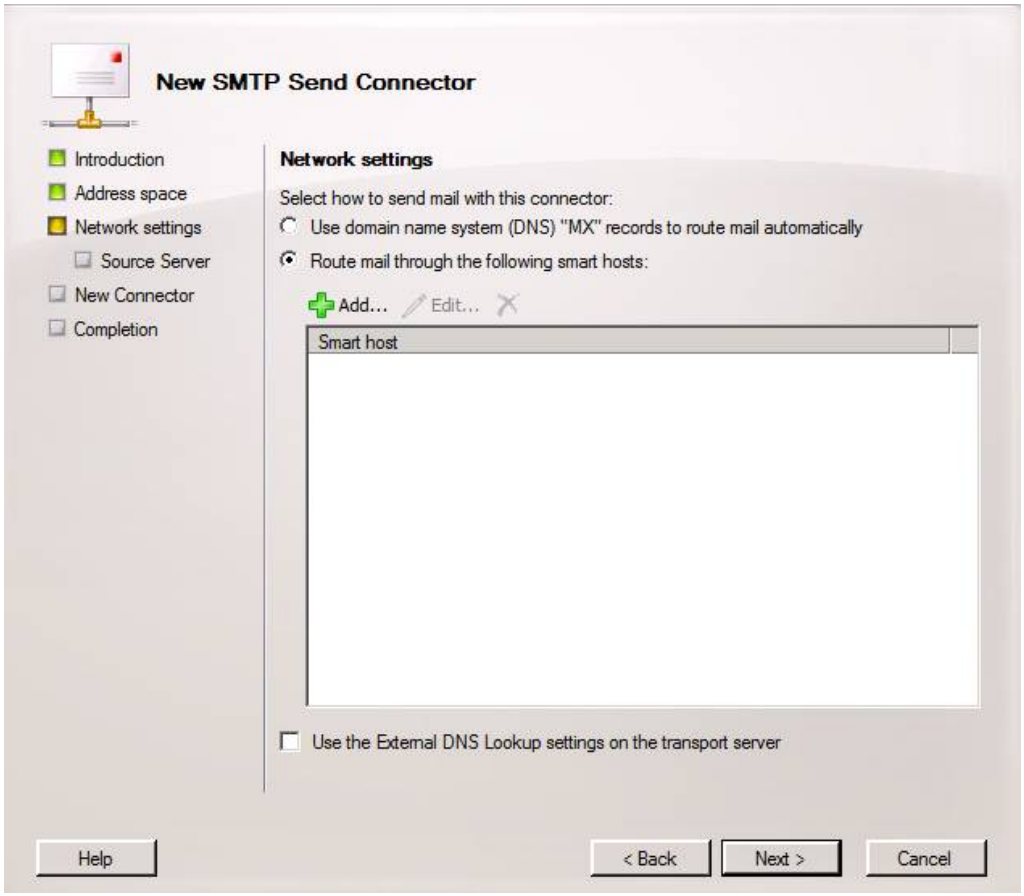
5. In the **Name** field, enter a name for the connector, for example, ProtectServer.
6. Click **Next**. The Address space page is displayed.

7. Click **Add**. The *SMTP Address Space* dialog is displayed.

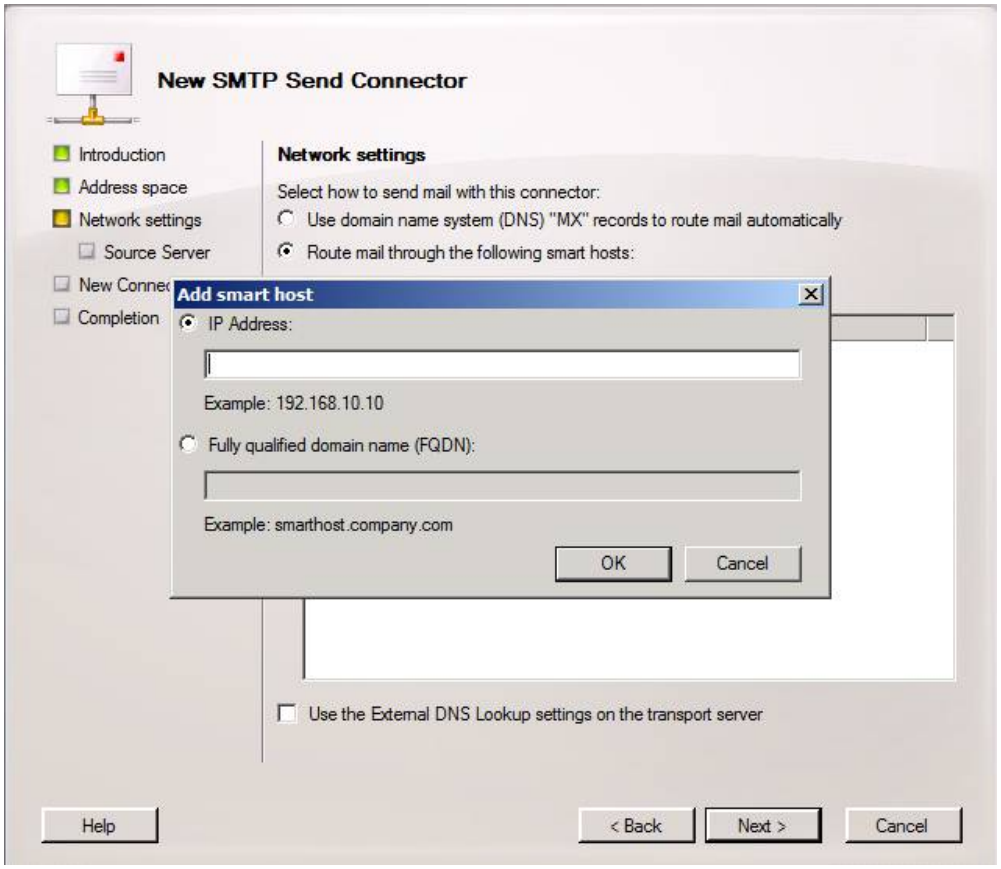


8. In the Address field, enter * so that all addresses are routed through Protect Server.

9. Click **OK** and click **Next**. The Network settings page is displayed.

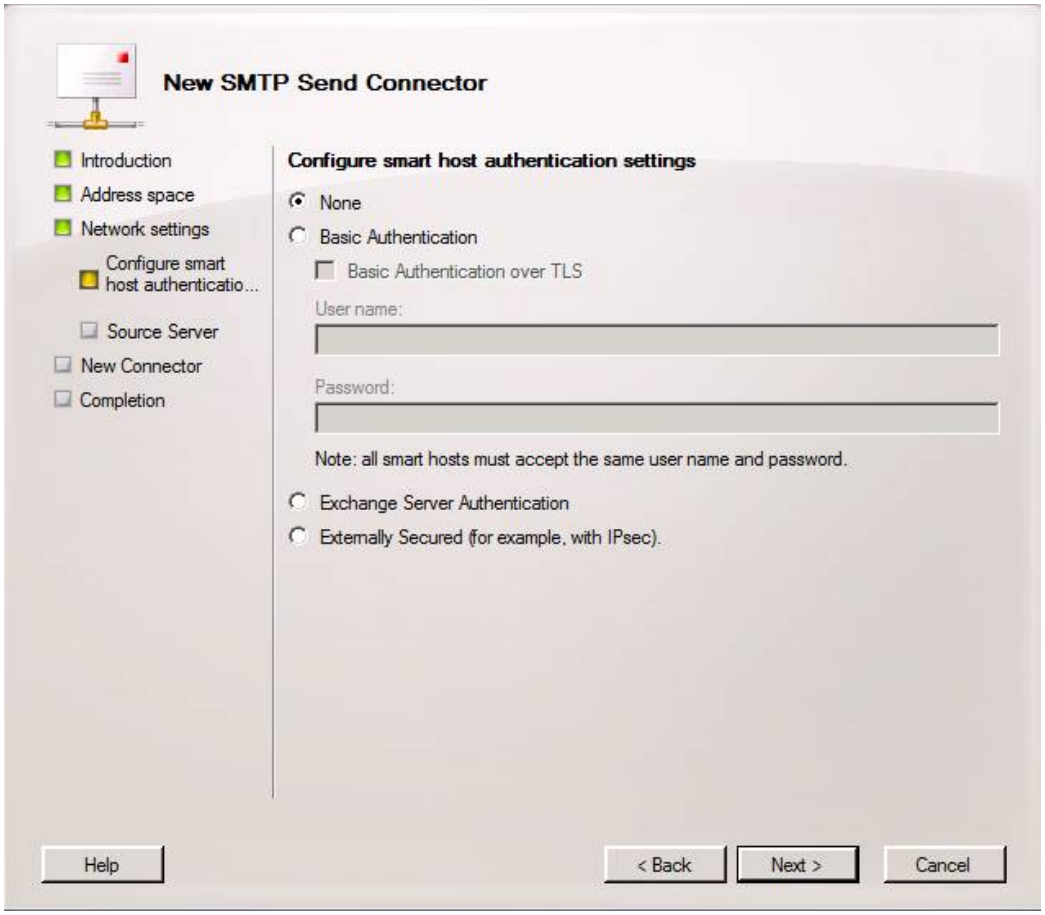


10. Select the **Route mail through the following smart hosts** radio button and click **Add**. The *Add smart host* dialog is displayed.

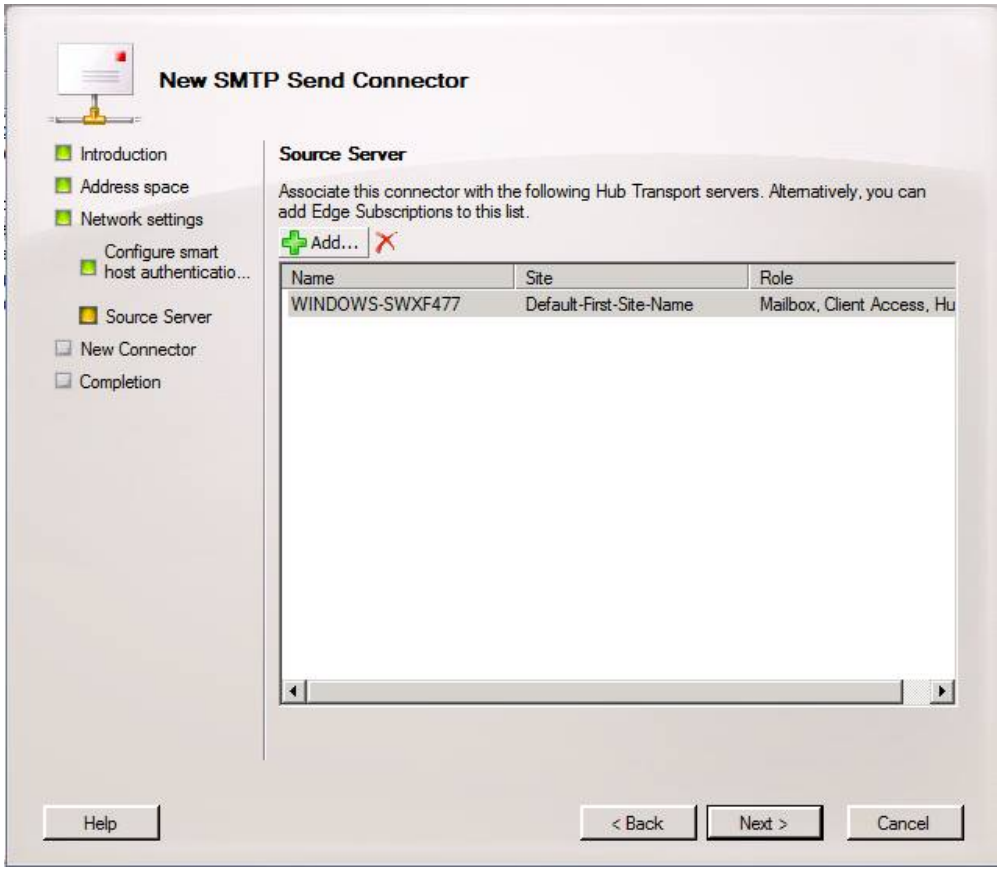


11. Select the **IP Address** radio button and enter the IP address of Protect Server.

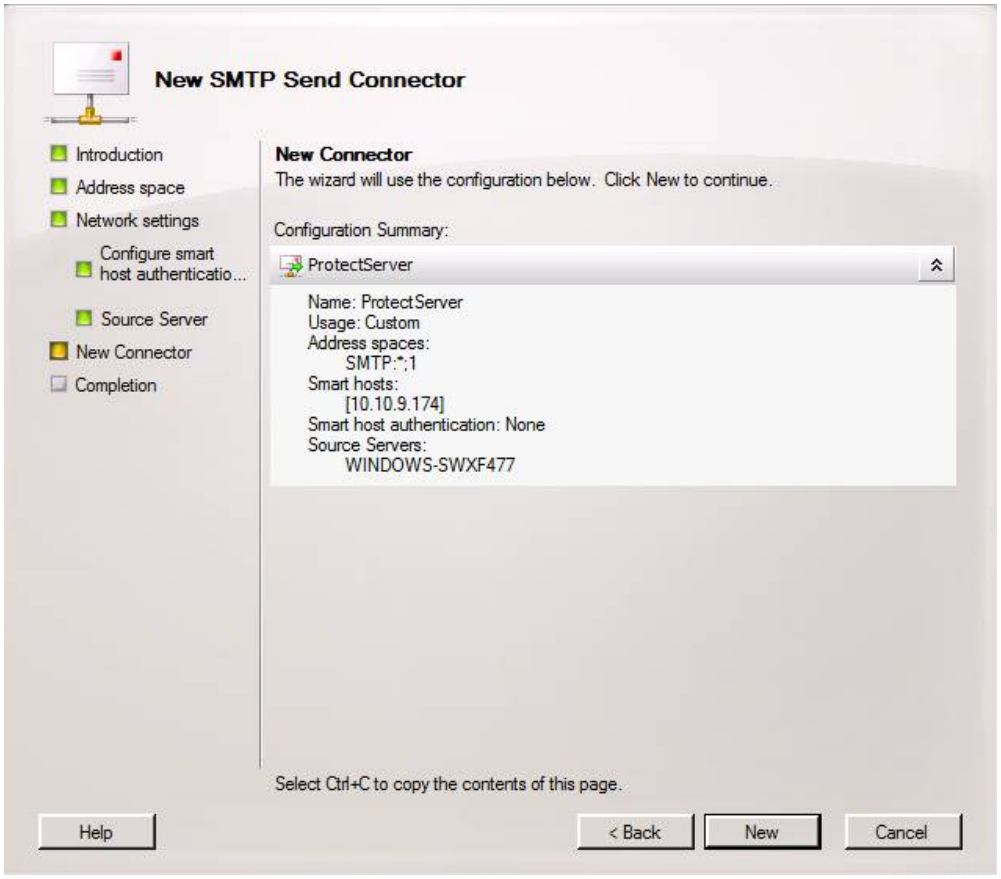
12. Click **OK** and click **Next**. The Configure smart host authentication settings page is displayed.



13. By default, Protect Server does not use authentication so there is no need to change the settings. However, if you set up authentication of Protect Server, you will need to configure authentication settings. Click **Next**. The Source Server page is displayed.



14. Leave the default settings and click **Next**. A summary of your settings is displayed.



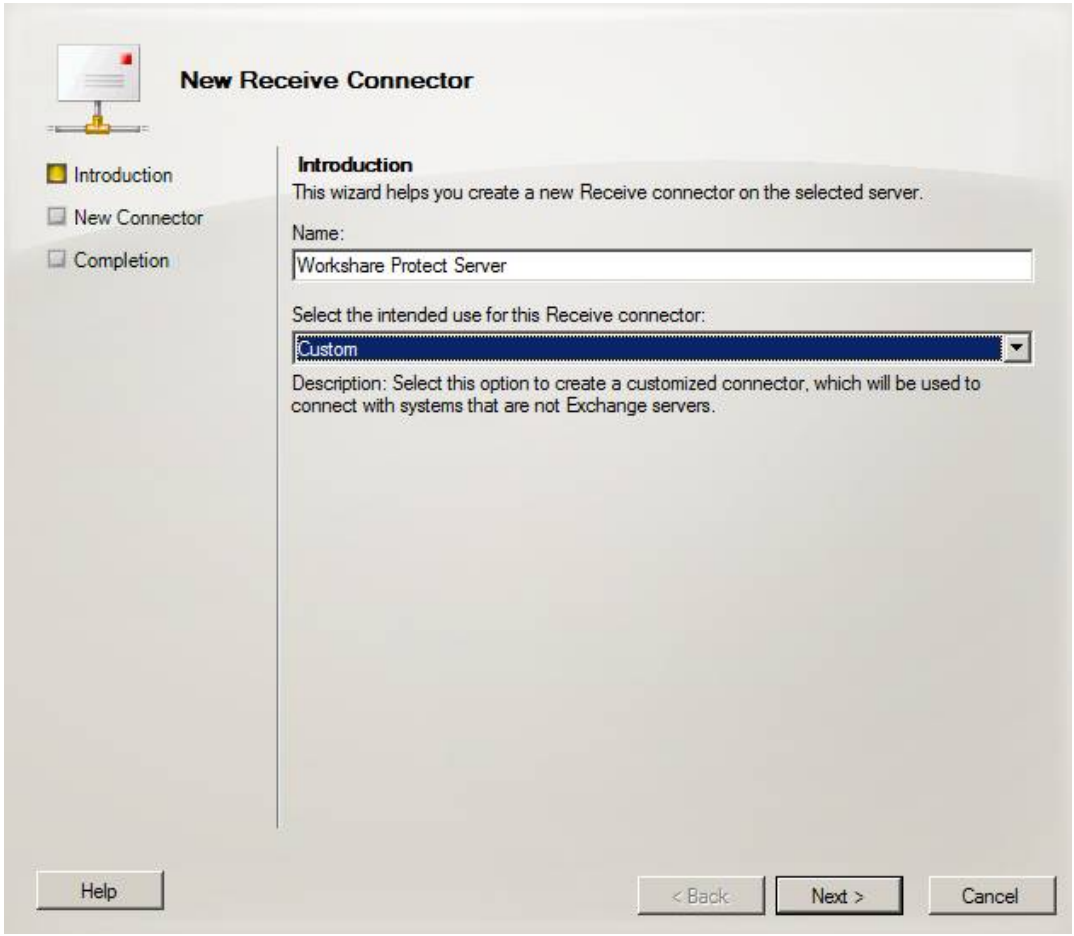
15. Click **New**. A new Send Connector is created and a confirmation message is displayed.
16. Click **Finish**. The new Send Connector is displayed in the **Send Connectors** tab. All mail from this Microsoft Exchange server will now be routed through Protect Server.

Setting Permissions on Receive Connector – Exchange 2010

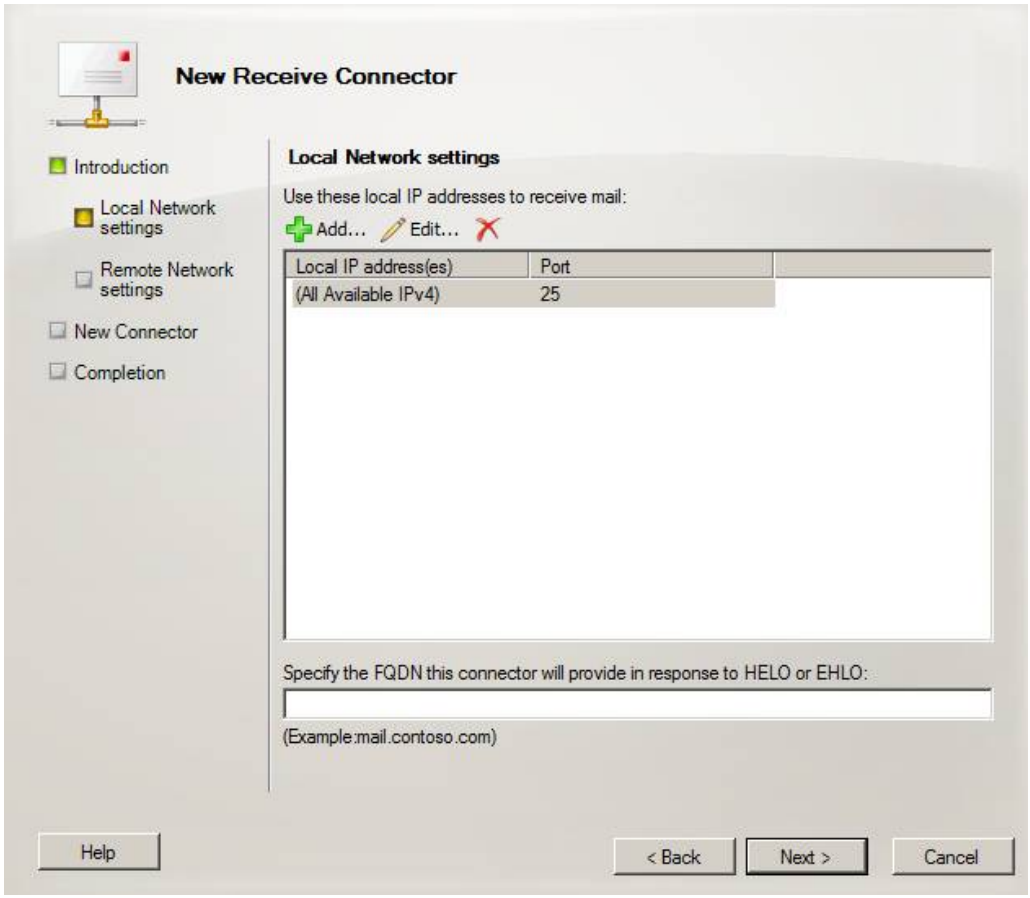
In order to allow Protect Server to send emails back through Microsoft Exchange, you must create a new receive connector for Protect Server and specify access permissions.

To set permissions:

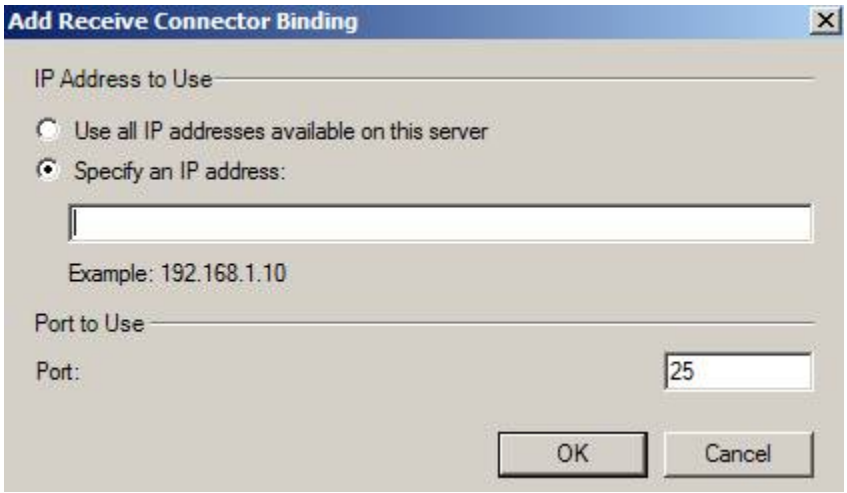
1. Launch the Exchange Management Console.
2. In the left panel, select **Server Configuration** and then **Hub Transport**.
3. Right-click in the **Receive Connectors** tab and select **New Receive Connector**.
4. Enter a name for the connector.



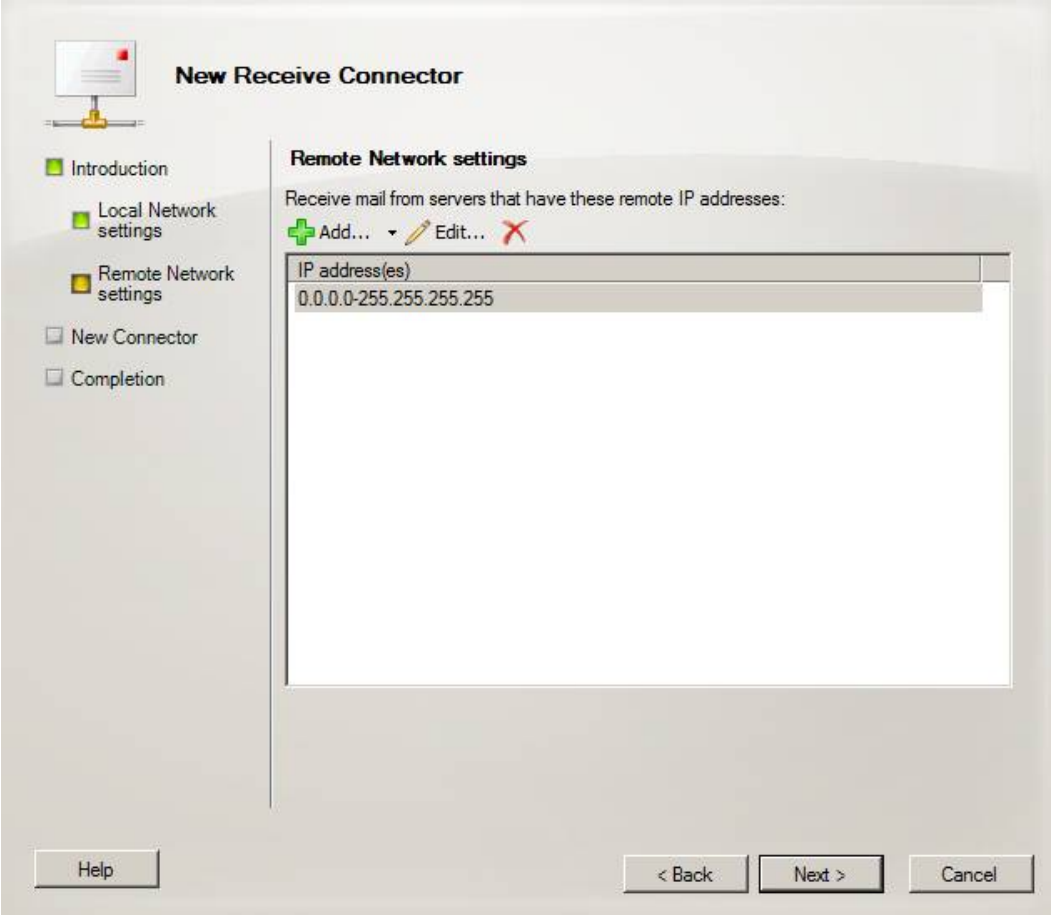
5. Click **Next**.



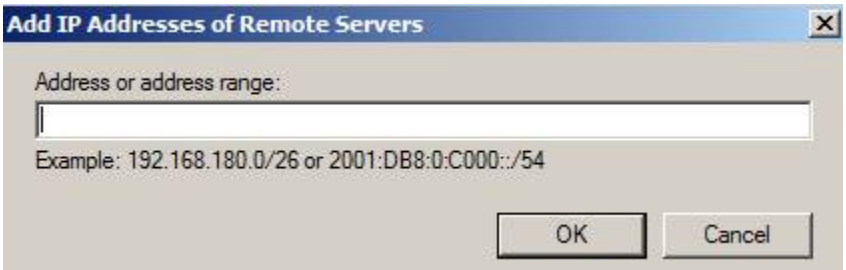
6. Select any existing entries in the table and click the delete button.
7. Click **Add**.



8. Enter the IP address of Protect Server.
9. Click **OK**.
10. Click **Next**.

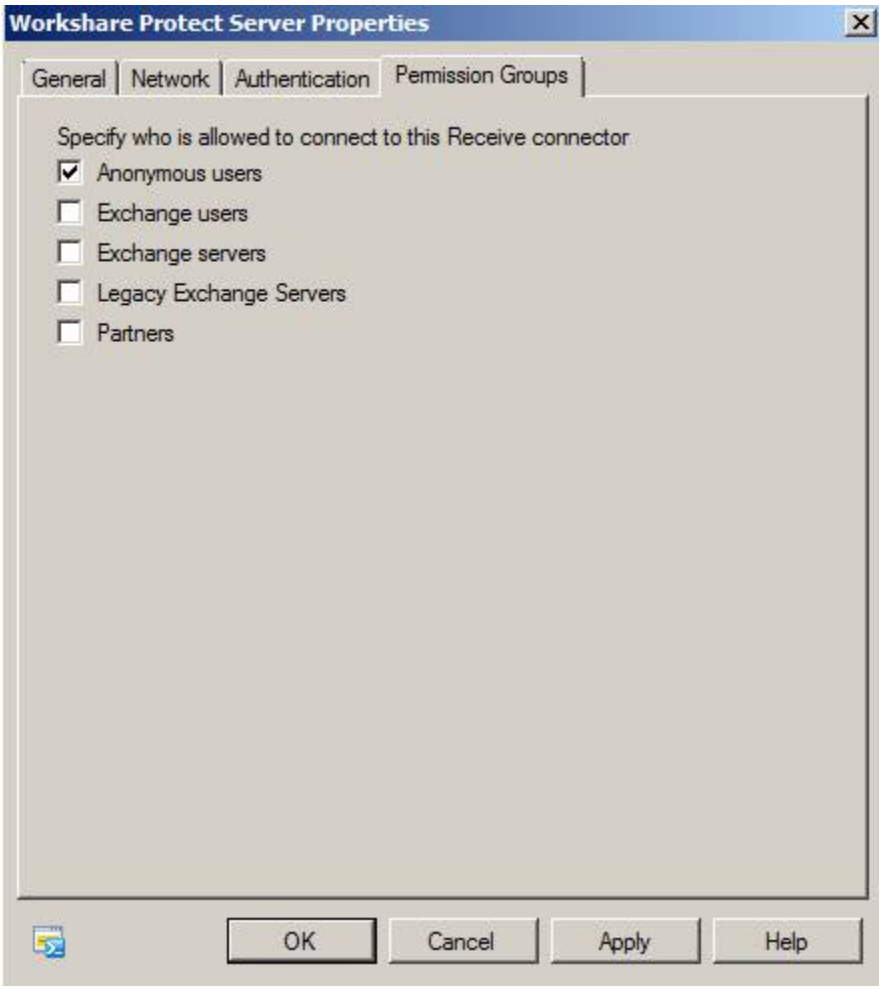


11. Select any existing entries in the table and click the delete button.
12. Click **Add**.



13. Enter the IP address of Protect Server.
14. Click **OK**.
15. Click **Next**.

16. Click **New**.
17. Click **Finish**.
18. In the **Receive Connectors** tab, right-click the new receive connector you have just created and select **Properties**.
19. Select the **Permission Groups** tab.
20. Select the **Anonymous users** checkbox.



21. Click **OK**.

Setting the Email Size Limit

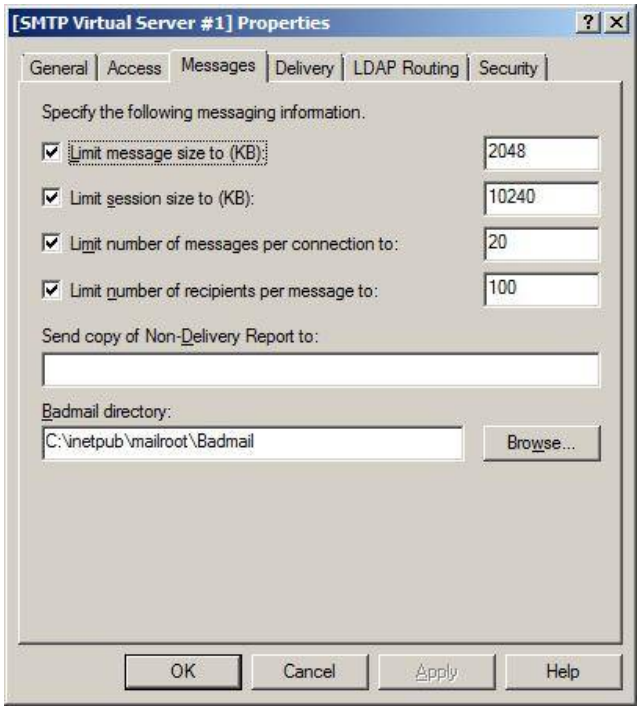
All external mail, whether it comes from a protected sender or not, will be routed through Protect Server. To prevent large emails from bouncing, you'll need to ensure the size limit is the same in these places:

- Protect Server SMTP service
- Exchange Hub Transport
- Exchange Web Services

Protect Server SMTP Service

For each Protect Server:

1. Open Internet Information Services (IIS) Manager.
2. Right-click **SMTP Server** and select **Properties**. The SMTP Server Properties dialog is displayed.
3. Select the **Messages** tab.
4. In the **Limit message size to (KB):** field, enter the maximum message size. Workshare recommends you set this value to be about 33% larger than what is set on your corporate email system. This is to account for the difference in email size between MAPI and MIME.

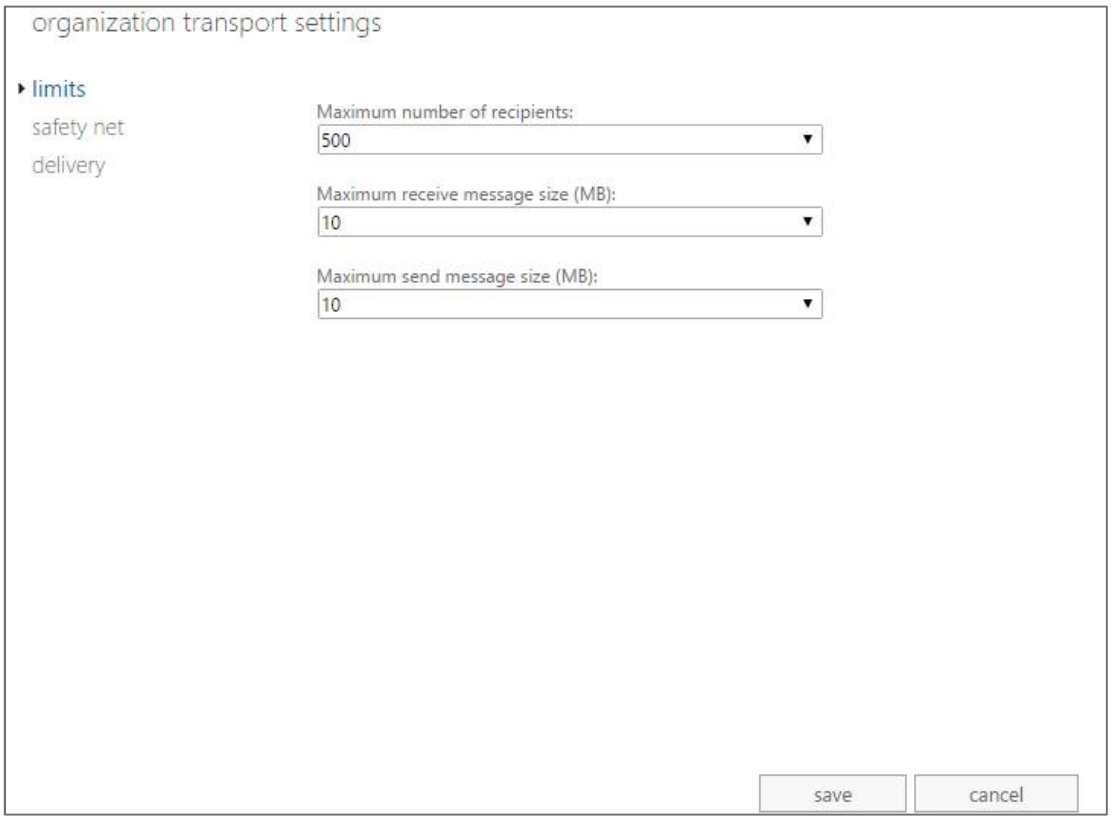


5. In the **Limit session size to (KB):** field, enter the maximum session size.

Exchange Hub Transport

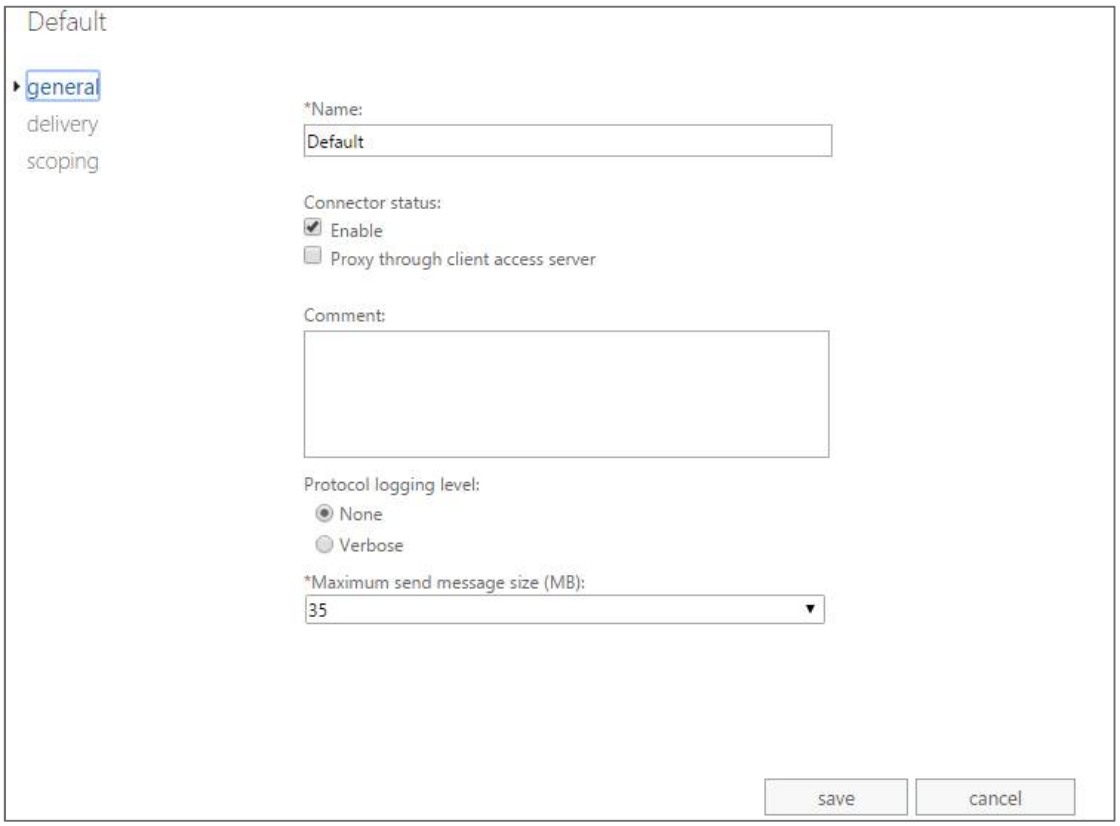
If you're using Exchange 2016/2013, for each Hub Transport:

1. Log in to the Exchange admin center at https://localhost/ecp.
2. In the left panel, select **Mail Flow**.
3. Select **Send Connectors** across the top.
4. Click the **more** icon and select **Organizational transport settings**.



5. Set the **Maximum send message size (MB)** for the organization and click **save**.

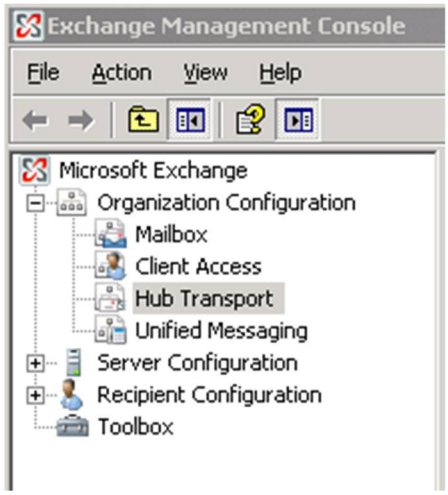
6. In the list of send connectors, double-click each relevant send connector and set the **Maximum send message size (MB)**.



For more information about the Hub Transport in Exchange 2016/2013, see Microsoft's support site: https://technet.microsoft.com/en-us/library/bb124345%28v=exchg.150%29.aspx

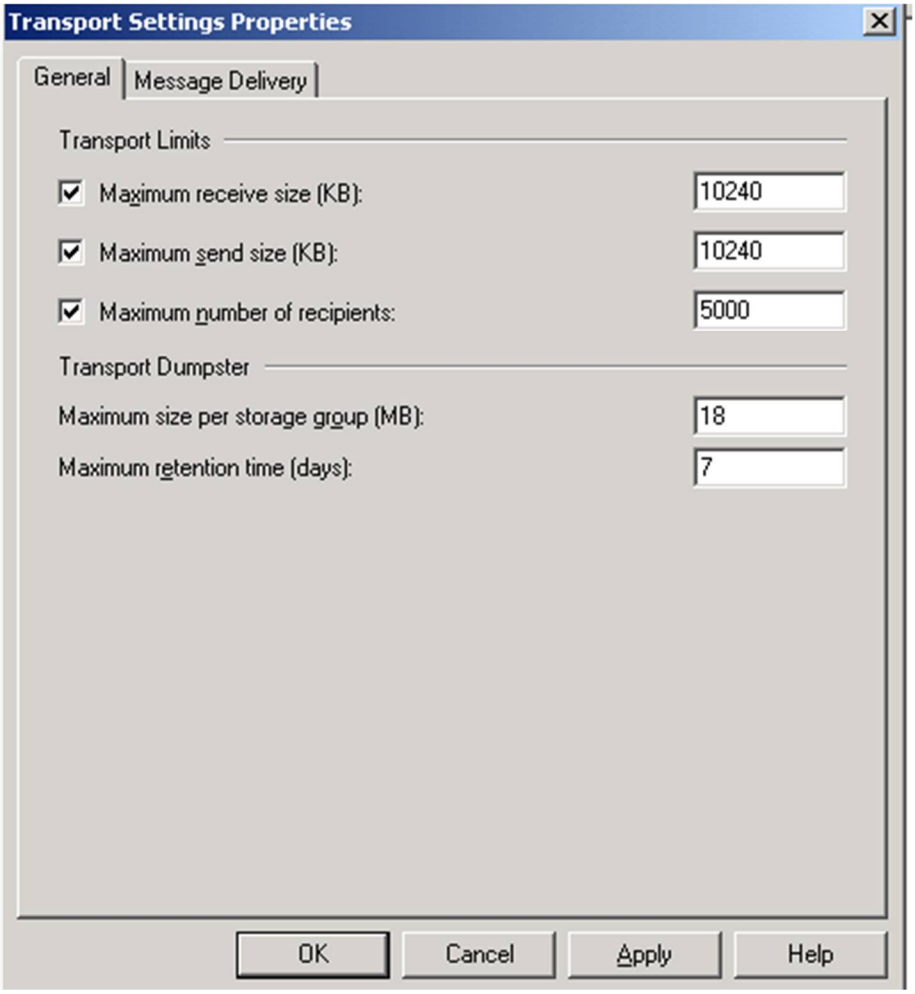
If you're using Exchange 2010, for each Hub Transport:

1. Open the Exchange Management Console.
2. Expand **Organization Configuration**.
3. Click **Hub Transport**.



4. Select the **Global Settings** tab.
5. Double-click **Transport Settings**. The *Transport Setting Properties* dialog is displayed.

6. In the **Maximum send size** field, enter a number the same size or smaller than the one you set for the SMTP server's message size. We recommend this value to be about 33% smaller than the SMTP's server message size.



For more information about the Hub Transport in Exchange 2010, see Microsoft's support site: http://technet.microsoft.com/en-gb/library/bb676532(v=exchg.141).aspx

Exchange Web Services

You only need to modify this if you're using the synchronization feature.

1. On your CAS server, go to C:\Program Files\Microsoft\Exchange Server\ClientAccess\exchweb\ews.
2. Open web.config with a text editor (e.g. Notepad).
3. Change the value of maxrequestlength to reflect the message size you want in kilobytes.
4. Save the file.
5. Go to C:\Program Files\Microsoft\Exchange Server\ClientAccess\owa.
6. Repeat steps 2-4 to change the maxrequestlength.
7. Once both files have been edited, open a command prompt and run the commands below. You'll need to replace [size in Bytes!] with the actual number of bytes based on the settings you chose for the web.config files.

```
cd \Windows\System32\inetsrv

appcmd set config "Default Web Site/ews" -section:requestFiltering
-requestLimits.maxAllowedContentLength:[size in Bytes!]

appcmd set config "Default Web Site/owa" -section:requestFiltering
-requestLimits.maxAllowedContentLength:[size in Bytes!]

iisreset
```

Additional Administrative Tasks

This section describes other configuration tasks you may need to complete. These are not mandatory tasks – it depends on your system configuration.

Setting up synchronization

If you want to use the synchronization functionality provided by Workshare Protect Server where the Sent Items folder is updated with the processed attachments, you need to set up a user with special impersonation rights.

In order to create an impersonation user, run the script **InstallProtectImpersonator User.ps1** in the Exchange PowerShell console. This script can be downloaded from the following link on the Workshare Knowledge Base.

http://workshare.force.com/knowledgebase/articles/Text_Article/Create-an-impersonation-user/

Download the .ps1 file and run `/InstallProtectImpersonatorUser.ps1 -Domain <domain> -Username <logonname> -Password <password>`

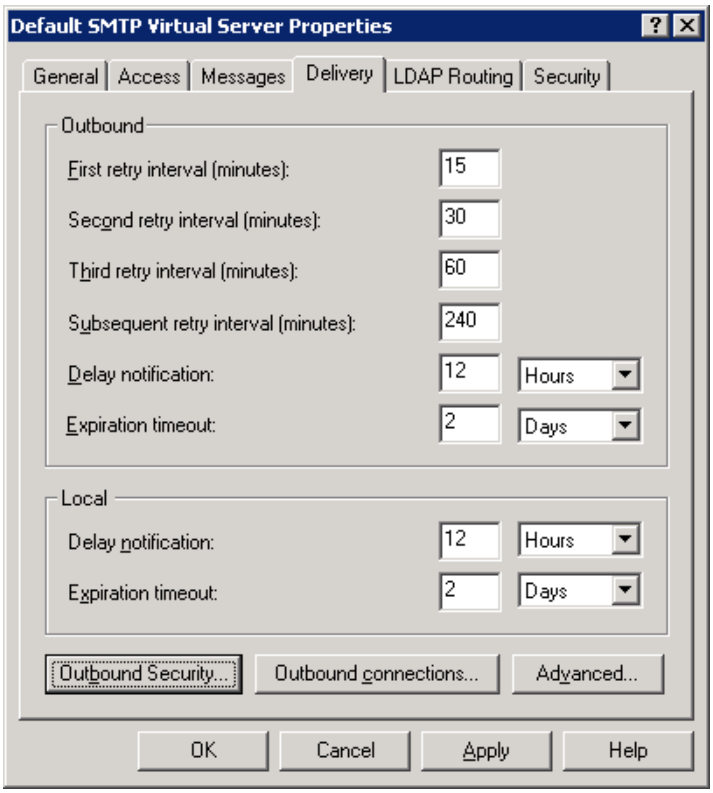
This will create an impersonation user account for Exchange environments with the name "Workshare Protect Exchange User".

Setting TLS security

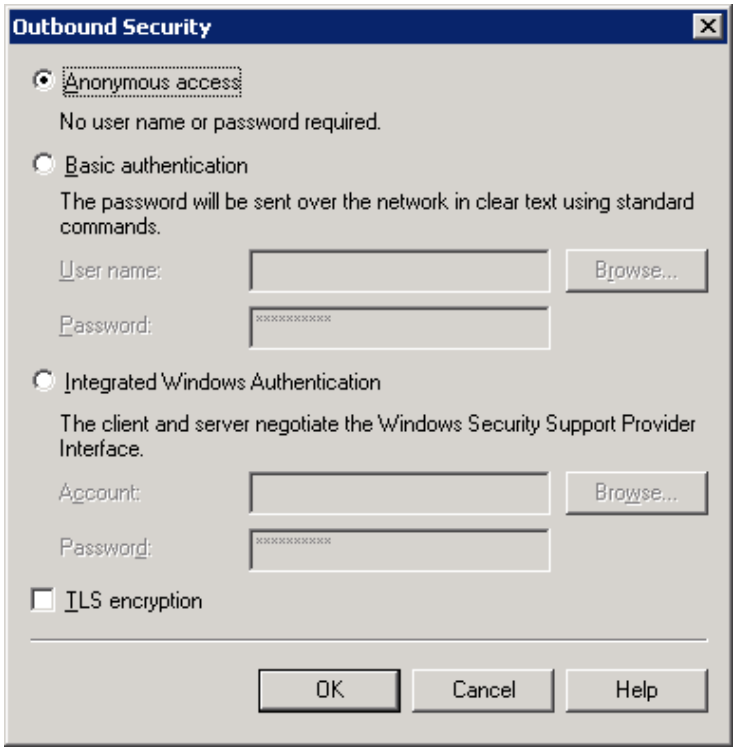
In cases where Protect Server acts as a relay server (rather than a final delivery server) and your final delivery server requires TLS encryption, use the following procedure to set TLS encryption for outbound SMTP traffic from Protect Server.

To set the TLS security for outbound traffic from Protect Server:

1. In Internet Information Services 6.0 Manager, right click **SMTP Server** and select **Properties**. The *SMTP Server Properties* dialog is displayed.
2. Select the **Delivery** tab.



3. Click **Outbound Security**.



4. Select **Basic authentication** and enter your user name and password for access to your mail gateway.
5. Select the **TLS encryption** checkbox.
6. Click **OK** and click **OK** again.

Auditing changes to Workshare Protect Server configuration

If you want to monitor configuration changes on Protect Server and to view who made any changes in the Event Viewer, you must edit the following elements in the logging.config file:

```
<add switchValue="Off" name="audit">
```

```
<allEvents switchValue="Off" name="All Events">
```

Change “Off” to “All”.

By default, the logging.config file is located on Protect Server at C:\Program Data\Workshare\Protect Server\3.11.0.0\Configuration

Configuring fail close

Protect Server will reject inbound SMTP traffic (fail close) in the event of a system or software failure or if one of the key performance indicators exceeds the specified threshold value. In the event of a failure in Protect Server, remedial action from a system administrator will usually be required to resolve the problem. If the threshold for any of the key performance indicators is exceeded, Protect Server will resume normal operation once the key performance indicators have dropped below the configured threshold.

Enabling and disabling fail close

Fail close is enabled by default and controlled from the metadata.config file (C:\Users\All Users\Workshare\Protect Server\[version]\Configuration\metadata.config). The following default threshold settings are specified and they can be adjusted as required.

Option name in metadata.config	Value	Notes
IncomingQueueMessageThreshold	10000	Fail close triggered if more than 10000 emails exist in incoming SMTP queue
IncomingQueueDiskThreshold	1073741824	Fail close triggered if free disk space falls below 1GB
DeliveryQueueMessageThreshold	10000	Fail close triggered if more than 10000 emails exist in outgoing SMTP queue
DeliveryQueueDiskThreshold	1073741824	Fail close triggered if free disk space falls below 1GB
TemporaryFolderDiskThreshold	0	Fail close triggered if free disk space falls below 0GB

To disable fail close set all the following options in the metadata.config file to “false”. Optionally a subset of the key performance indicators can be monitored.

```
<FailClosedOnLicenseProblem>false</FailClosedOnLicenseProblem>

<FailClosedOnDatabaseError>false</FailClosedOnDatabaseError>

<FailClosedBelowIncomingQueueMessageThreshold>false</FailClosedBelowIncom
ingQueueMessageThreshold>

<FailClosedBelowDeliveryQueueMessageThreshold>false</FailClosedBelowDeliv
eryQueueMessageThreshold>

<FailClosedBelowDiskThreshold>false</FailClosedBelowDiskThreshold>
```

Fail close cannot be disabled in the event of a system/software failure. The Workshare Protect Health Service is responsible for monitoring the status of Protect Server and any of the following failures will result in fail close being triggered:

- Failure of the Windows Service “Workshare Protect Service License Service”
- Failure of the Windows Service “Workshare Protect Server Health Service”
- Failure of the Windows Service “Workshare Protect Profile Service”

***Note**: In the event of an SQL connection issue when fail close is enabled, it is likely that the automatic email alert will not be generated.*

Fail close and bounce functionality

- If the Protect Server bounce functionality is enabled and fail close is enabled, any email routed to the Protect Server in a fail close state will be automatically rejected and routed by the corporate mail server to the configured backup server. No bounce email will be triggered.
- If the Protect Server bounce functionality is enabled and fail close is disabled, any email routed to the Protect Server in a fail close state will be bounced back to the sender.

  ***Warning!** This may lead to significant load on the corporate mail server.*

- If the Protect Server bounce functionality is disabled and fail close is disabled, any email routed to the Protect Server in a fail close state will pass through unprocessed.

Chapter 5: Configuring Workshare Protect Server

This chapter describes how to specify configuration settings such as whether clean reports should be sent, how to override cleaning settings as well as configuring alert settings and email templates. This configuration is performed from the Workshare Protect Server web console. This chapter includes the following sections:

***Note**: For a description on how to configure profiles for removing metadata from attachments, refer to the Workshare Protect Server Metadata Removal guide. For a description on how to configure policies for blocking email, refer to the Workshare Protect Server Email Data Loss Prevention guide.*

- **Overriding Cleaning Settings**, page 92, describes how to configure Protect Server to skip cleaning of a particular email and also to skip cleaning of emails that have been processed by the Workshare Protect client.
- **Configuring Bounce Settings**, page 94, describes how to configure Protect Server to bounce emails that cannot be processed.
- **Configuring Cleaning Reports and Email Storage**, page 97, describes how to configure Protect Server to send reports to senders when their email is cleaned.
- **Configuring Email Templates**, page 98, describes how to configure the templates for system email messages sent when an email has been cleaned or if there has been a failure to clean an email.
- **Configuring Alert Settings**, page 100, describes how to configure email addresses to enable Protect Server to send notification emails, e.g. clean reports.
- **Configuring Sync Settings**, page 101, describes how to configure synchronization so that for any email attachment that is processed by Protect Server, the original copy of the email found in the sender's "Sent Items" folder will be updated with the processed attachments.
- **Configuring Active Directory Cache Settings**, page 102, describes how to configure Protect Server to work with Active Directory groups.

This functionality is available for Administrator role users only.

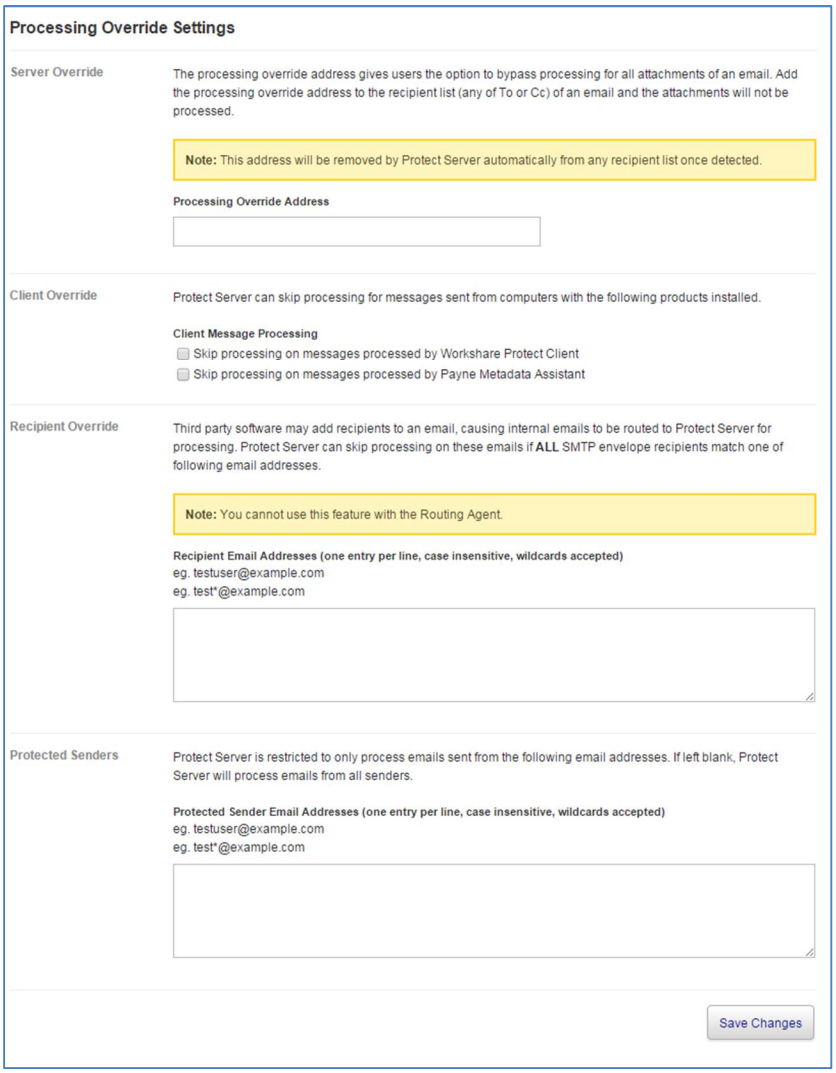
***Note**: The user experience of the Protect Server configuration options pages is improved if javascript is enabled in your browser.*

Overriding Cleaning Settings

Workshare Protect Server can be configured to skip cleaning of a particular email and also to skip cleaning of emails that have been processed by the Workshare Protect client or by Payne Metadata Assistant.

To override cleaning settings:

1. Log into the Protect Server web console as an Administrator role user and select **Settings**.
2. Select **Override**.



3. In the **Processing Override Address** field, enter an email address that can be used to bypass the cleaning action on the server. The sender can add this email address to the recipient list (**To** or **Cc** fields) of an email and the attachments will not be cleaned.

> ***Note**: This address can be fictional or real. If real, then you will need to monitor the email account.*

Once Protect Server has detected the override address in an email, the attachments of the email are not cleaned and the override address is removed.

> ***Note**: When emails include a digital signature, Protect Server does not remove the override address.*

4. In the **Client Message Processing** area, select how to handle emails sent from computers with the Workshare Protect client or Payne Metadata Assistant installed:
   - **Skip processing on messages processed by Workshare Protect Client**: Protect Server will not clean emails that have already been cleaned by the Protect client.
   - **Skip processing on messages processed by Payne Metadata Assistant**: Protect Server will not clean emails that have already been cleaned by Payne Metadata Assistant.
5. When EMM routes filed internal-only emails through Protect Server, Protect Server processes them. To prevent this, you can use either the Workshare Protect Routing Agent or “Recipient Override”. To use recipient override, in the **Recipient Override** area, add the EMM email address pattern that will trigger Protect Server to skip processing.

> ***Note:** It is not recommended to use **Recipient Override** and the Protect Routing Agent together.*

6. The **Protected Senders** area is for testing purposes only. You can enter an email address or address pattern and Protect Server will ONLY process emails from that specified email address.
7. Click **Save Changes**. The settings are saved and a message is displayed across the top of the screen.

Configuring Bounce Settings

Workshare Protect Server can be configured to bounce emails in the following circumstances:

- Emails with attachments that include comments or track changes: When attachments contain comments or track changes, Protect Server can bounce the email back to the sender with a non-delivery report. This is to encourage users to carefully consider files with comments or track changes before sending them externally. Once a sender receives such an email back, they may decide to send it again specifying a clean profile or they may decide that the track changes or comments should remain and specify the override profile.
- Emails with attachments that cannot be processed: When Protect Server cannot process an attachment, it can bounce the email back to the sender with a non-delivery report. There are several reasons why Protect Server may not be able to process an attachment. For example, the attachment may be corrupt or digitally signed.

You can configure the content of the non-delivery report that Protect Server sends according to the reason for non-delivery.

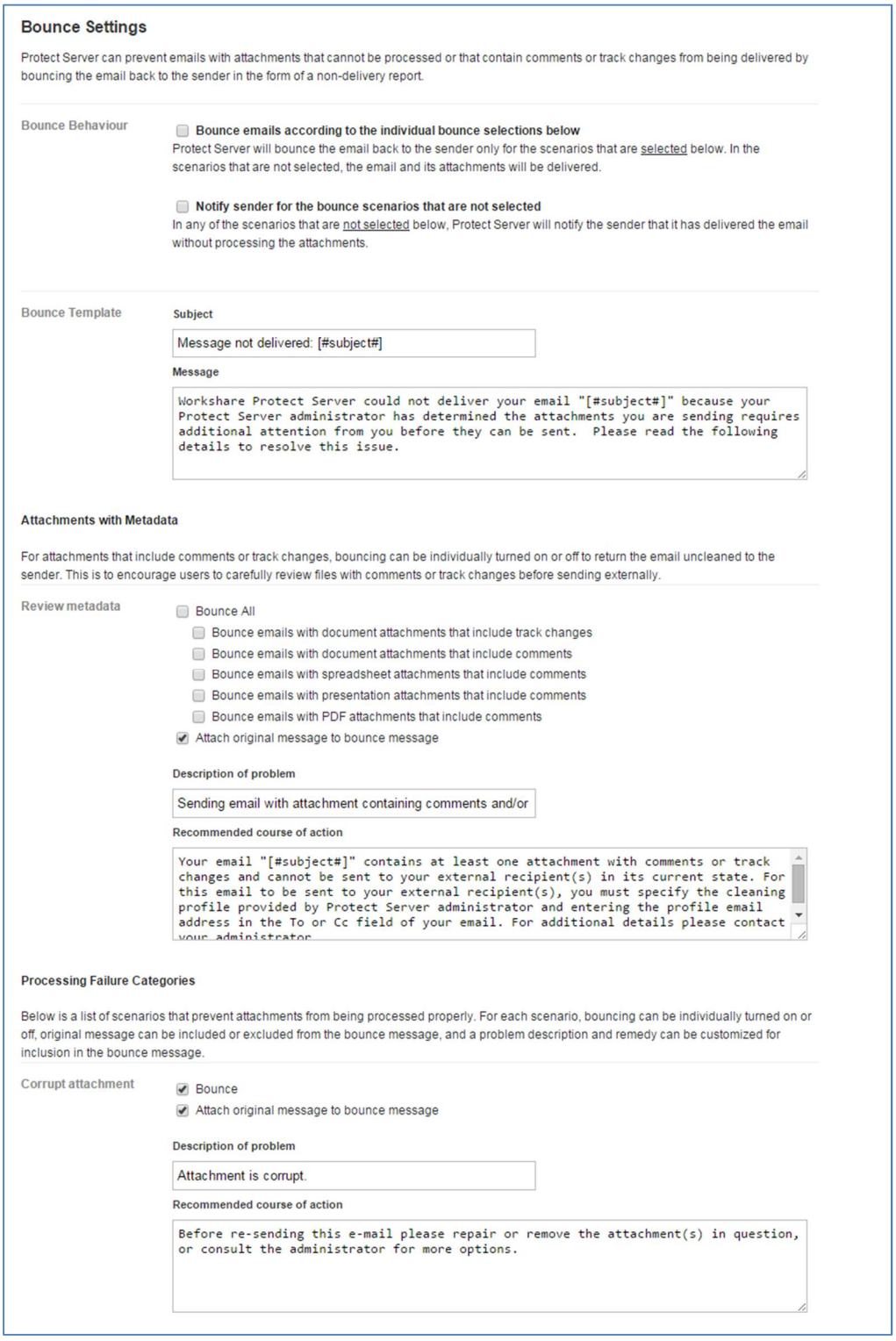
***Note**: To enable non-delivery reports to be sent to senders, ensure that a valid email address is specified in Configuring Alert Settings.*

When bounce has not been configured, emails with attachments that include comments or track changes or emails with attachments that cannot be processed will be sent without processing. You can select to notify the sender in these circumstances.

To configure bounce settings:

1. Log into the Protect Server web console as an Administrator role user and select **Settings**.

2. Select **Bounce**.



3. Select the **Bounce emails according to the individual bounce selections below** checkbox to enable Protect Server to stop delivery of emails that include attachments with comments/track changes or that it cannot clean/convert according to your selections in this page.
4. Select the **Notify sender for the bounce scenarios that are not selected** checkbox to enable Protect Server to send notifications to senders when bounce is not selected and emails that include attachments with comments/track changes or that it cannot clean/convert have been delivered.
5. In the **Subject** field, edit the text that will appear in the Subject line of the non-delivery email. This is the email sent to the sender informing them that their email has not been sent.
6. In the **Message** field, edit the text that will appear in the non-delivery email. This should explain to the sender that their email has not been sent.
7. In the **Attachments with Metadata** area, select whether Protect Server should bounce emails with attachments that include comments or track changes. Select the **Bounce All** checkbox to bounce emails with any attachment containing comments or track changes or select individual file types.
8. In the **Description of problem** field, edit the brief description if required.
9. In the **Recommended course of action** field, edit the description of what the sender could do to remedy the problem so that their email may be resent and successfully processed by Protect Server.
10. In the **Processing Failure Categories** area, you can configure how Protect Server deals with the following specific types of attachments/emails that it cannot process:
    - Corrupt attachment
    - Digitally signed attachment
    - Digitally signed email
    - Document format not supported
    - Password protected or encrypted attachment

> ***Note**: If The Workshare Protect Portal is installed, then password-protected Word, Excel, PDF and zip files can be processed by Protect Server. However, password-protected PowerPoint files cannot be processed.*

    - Processing error, for example, when emails are stuck in a queue awaiting final delivery

    For each type of attachment/email, configure the following as required:

Bounce	Select to enable Protect Server to bounce emails with attachments of this type.
Attach original message to bounce message	Select and Protect Server will include the original email when sending the non-delivery email to the sender.

Description of problem	Edit the brief description of the problem.
Recommended course of action	Edit the description of what the sender could do to remedy the problem so that their email may be resent and successfully processed by Protect Server.

> ***Note**: Remember that for any scenarios you don't select, the email will be delivered. You can notify the user of this by selecting the **Notify sender for the bounce scenarios that are not selected** checkbox.*

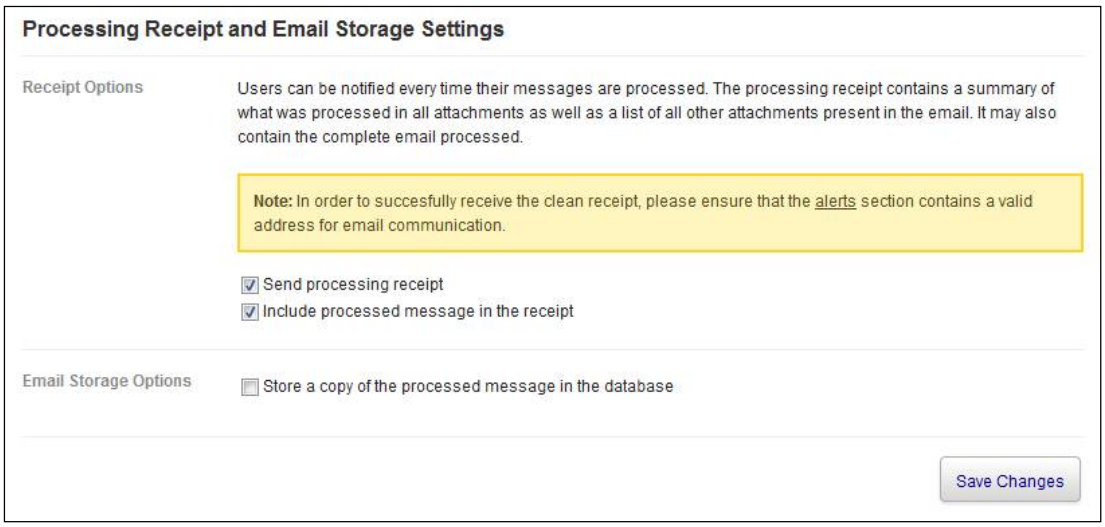
11. Click **Save Changes**. The settings are saved and a message is displayed across the top of the screen.

Configuring Cleaning Reports and Email Storage

Workshare Protect Server can be configured to send reports to senders each time one of their emails is processed. The report (or processing receipt) details the metadata that was removed from each attachment and whether attachments were converted to PDF. The processing receipt can also be accompanied by a copy of the processed message. In addition, you can configure Protect Server to store all processed emails in the database.

To configure processing receipts and email storage:

1. Log into the Protect Server web console as an Administrator role user and select **Settings**.
2. Select **Receipts**.



3. Select the **Send processing receipt** checkbox to enable processing receipts to be sent to senders each time an email they send is processed by Protect Server. To enable processing receipts to be sent to senders, ensure that a valid email address is specified in Configuring Alert Settings.
4. Select the **Include processed message in the receipt** checkbox to enable copies of the processed email and its attachments to be sent to senders with the processing receipt. To enable copies of emails and their attachments to be sent to senders, ensure that a valid email address is specified in Configuring Alert Settings.

> ***Note**: If neither checkbox is selected, no email is sent to senders notifying them that their emails have been processed.*

5. Select the **Store a copy of the processed message in the database** checkbox to enable copies of the processed email and its attachments to be saved in the database.
6. Click **Save Changes**. The settings are saved and a message is displayed across the top of the screen.

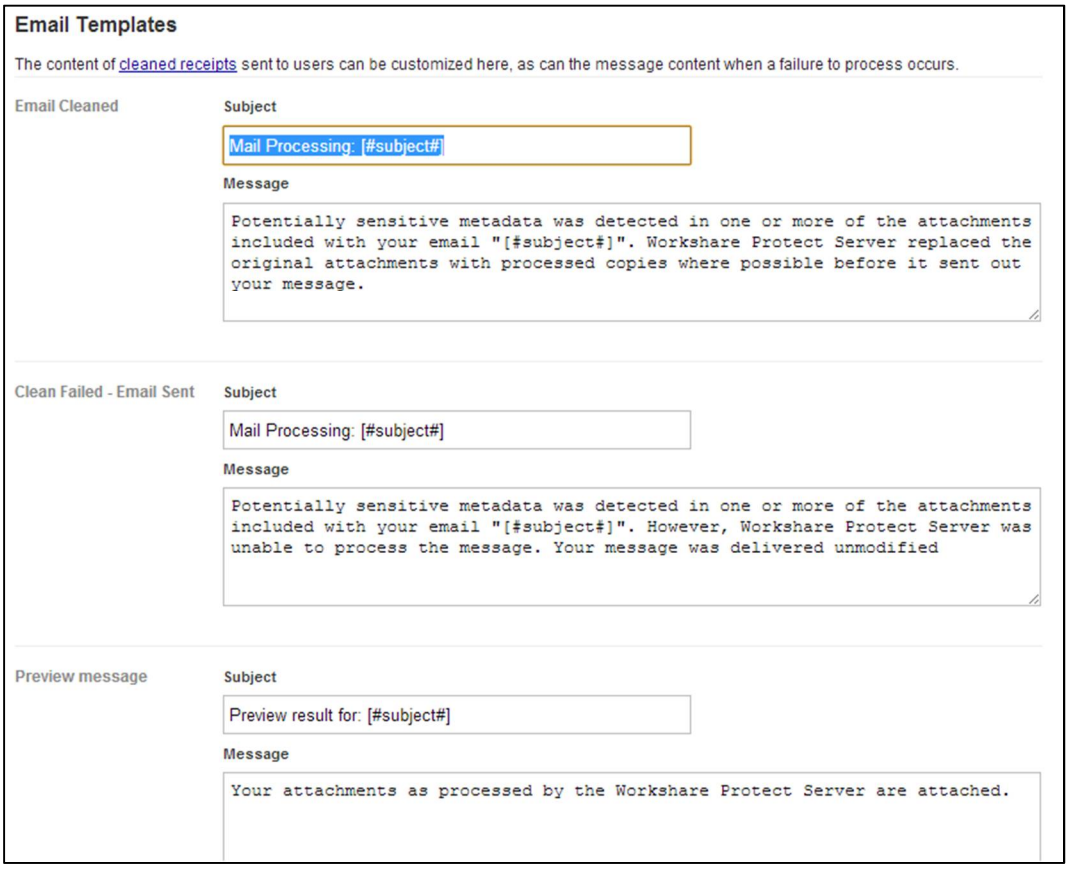
Configuring Email Templates

You can configure the templates for system email messages sent when an email has been cleaned or if there has been a failure to clean an email or when a preview request is sent.

To configure email templates:

1. Log into the Workshare Protect Server web console as an Administrator role user and select **Settings**.

2. Select **Email Templates**.



3. Edit the **Email Cleaned** template as required. The Email Cleaned email is sent when metadata is detected and cleaned from attachments. To enable clean reports to be sent to senders each time an email they send is cleaned by Workshare Protect Server, ensure that the **Send processing receipt** checkbox is selected in the Receipts settings (described in Configuring Cleaning Reports and Email Storage).

4. Edit the **Clean Failed - Email Sent** template as required. The Clean Failed - Email Sent email is sent when metadata is detected but Protect Server is unable to clean the attachment and the email is sent uncleaned.

> ***Note**: Customize each template as required. You can include the following variables in the messages: **[#subject#]** = Original Subject, **[#recipients#]** = Original Recipients, **[#date#]** = Date/Time Sent*

5. Edit the **Preview message** template as required. The Preview message email is sent when the sender has requested a preview of what the processed attachments will look like before sending them to recipients. This is done by sending an email to a profile email address only. Protect Server will treat such an email as a preview request and send the processed attachments back to the sender with a **Preview message** email.

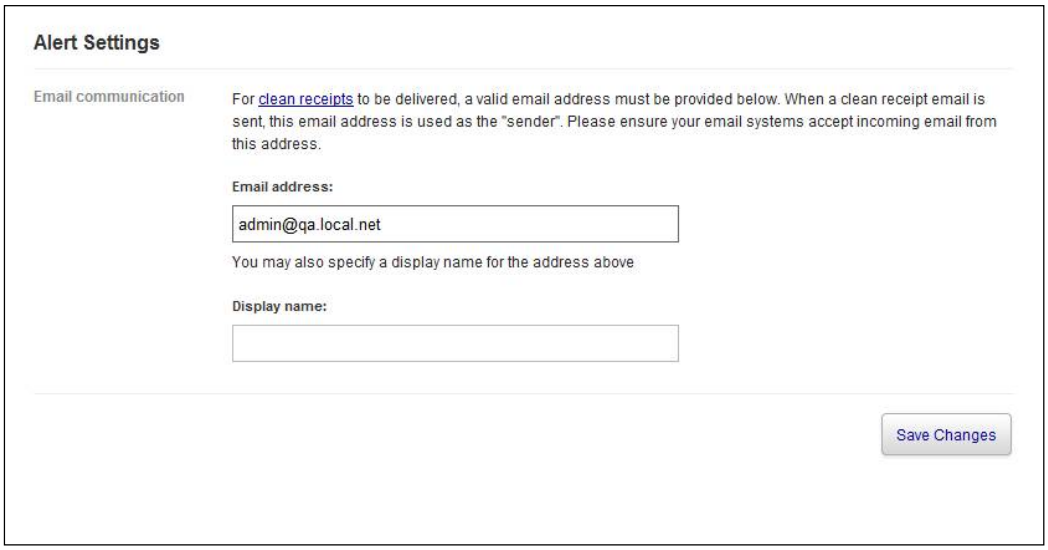
6. Click **Save Changes**. The settings are saved and a message is displayed across the top of the screen.

Configuring Alert Settings

A valid email address and display name must be specified in **Alert Settings** in order for Workshare Protect Server to send emails to senders, such as clean reports, copies of emails and their attachments, copies of processed emails, non-delivery reports and preview emails.

To configure alert settings:

1. Log into the Protect Server web console, as an Administrator role user, and select **Settings**.
2. Select **Alerts**.



3. In the **Email address** field, enter a valid email address to ensure clean notification emails are delivered. This email address is the “sender” of clean receipt emails and other notification emails.
4. In the **Display name** field, enter a display name for this email address.
5. Click **Save Changes**. The settings are saved and a message is displayed across the top of the screen.

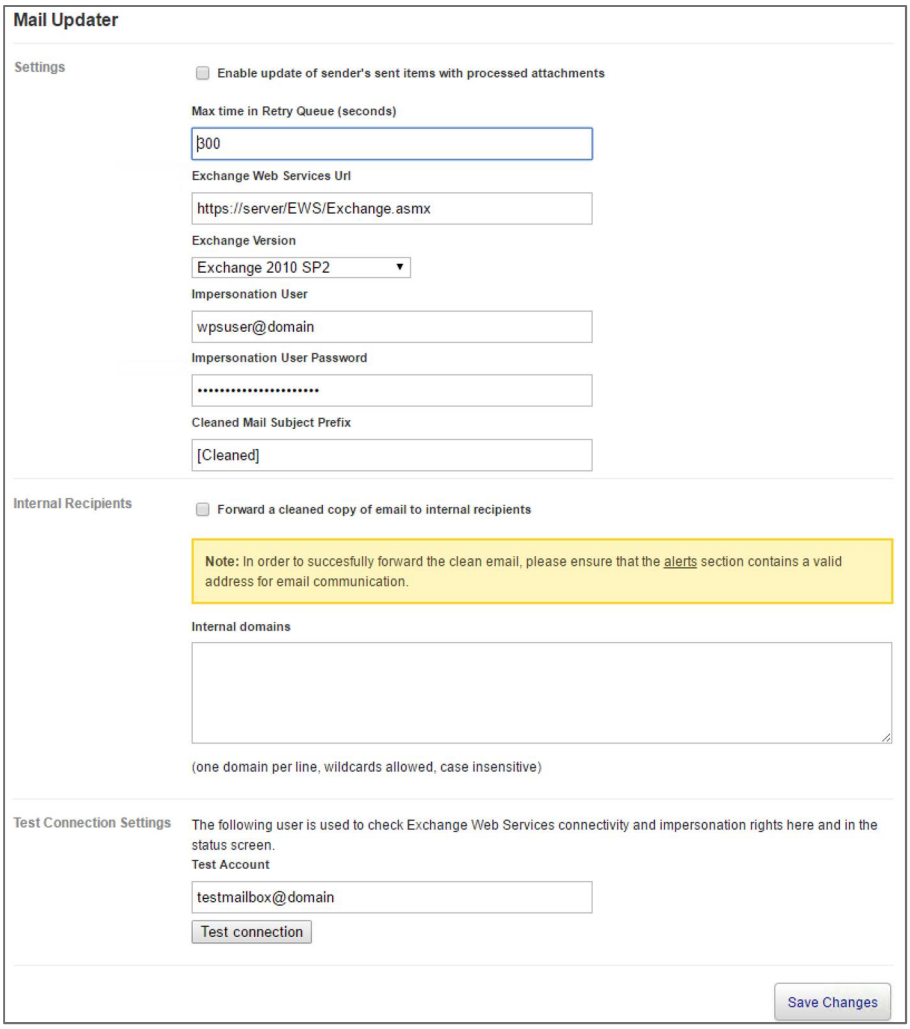
Configuring Sync Settings

The Mail Updater settings enable you to configure synchronization in the following ways:

- When email attachments are processed by Workshare Protect Server, the original copy of the email found in the sender's "Sent Items" folder will be updated with the processed attachments.
- To ensure that internal recipients always have access to the same version of attachments that are received by external recipients, where emails are sent internally and externally, the internal recipients will receive a clean receipt with the processed attachment included.

To configure mail updater settings:

1. Log into the Protect Server web console as an Administrator role user and select **Settings**.
2. Select **Mail Updater**.



3. Complete the fields as follows:

Enable update of sender's sent items with processed attachments	Select to enable Protect Server to synchronize emails in the Sent folder with the processed attachments actually sent.
Max time in Retry Queue (seconds)	Where synchronization initially fails, specify the maximum amount of time before Protect Server will stop attempting to synchronize.
Exchange Web Services Url	Enter the URL of Exchange Web Services.
Exchange Version	Select your Exchange version.
Impersonation User	The logon name of the impersonation user (described in Setting up synchronization).
Impersonation User Password	The logon password of the impersonation user.
Cleaned Mail Subject Prefix	The prefix to add to an email in the Sent items folder once it has been synchronized.

4. If you want internal recipients to receive a clean receipt with the processed attachment included, select the **Forward a cleaned copy of email to internal recipients** checkbox and you MUST then specify the internal domain (domains) in the **Internal domains** area. To enable processing receipts to be sent to senders, ensure that a valid email address is specified in Configuring Alert Settings.
5. Enter a test email address in the **Test Account** field to check if the specified impersonation user can actually impersonate a user.
6. Click **Test connection**. If the specified impersonation user is successful, a confirmation message is displayed.
7. Click **Save Changes**.

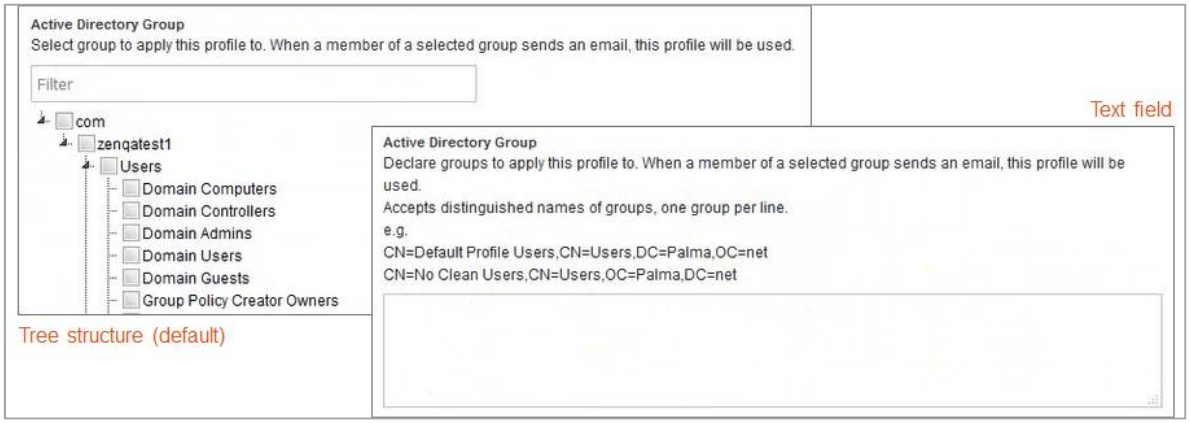
Configuring Active Directory Cache Settings

In order for Workshare Protect Server to identify which Active Directory groups senders belong to, and then apply the profile which has been defined for that group, you must specify the **Active Directory Cache** settings. Protect Server can then regularly scan your Active Directory and cache the domain structure locally.

When an AD group is added to a profile, Protect Server will periodically cache only the users of the added profile group. It will not cache groups that are members of the added profile group.

When selecting an Active Directory group to assign to a profile, you can select a group from a tree structure (default) or simply enter a group name into a text field. The default way to select Active Directory groups using a tree is a user friendly approach but, if the tree is complex, it can take a long time to download the tree into the UI.

The alternative is to use “Simple AD Cache” mode, so you get a text field where you can manually specify the distinguished name for the Active Directory group.

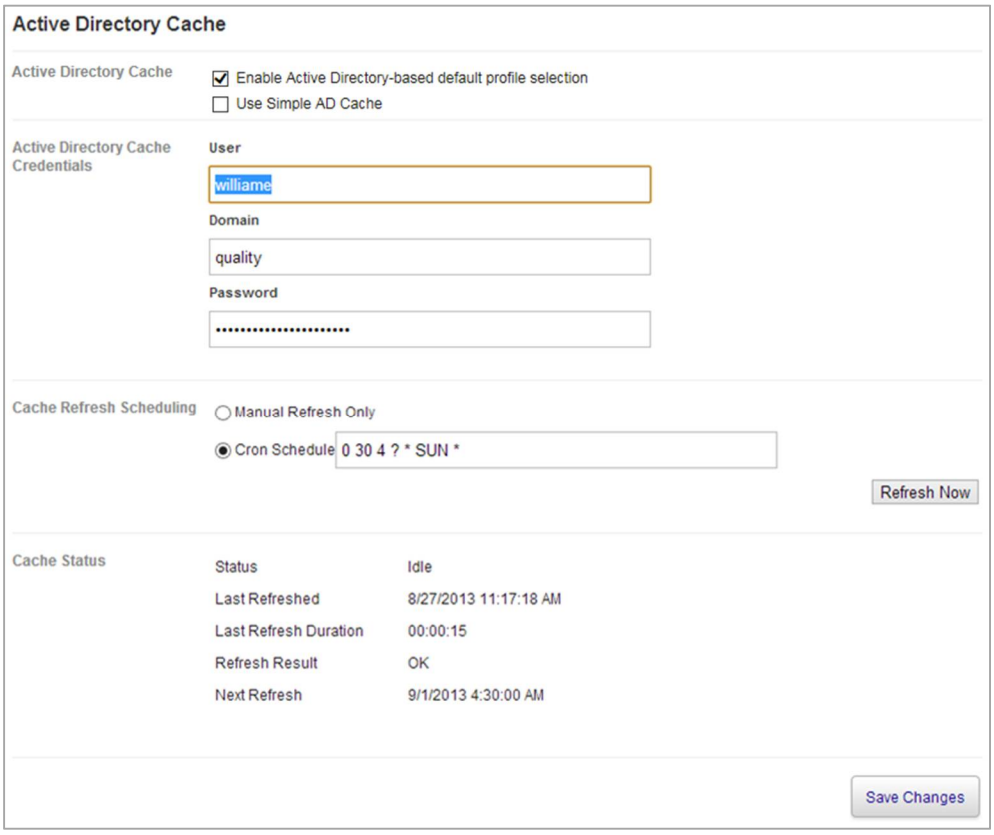


***Note**: In “Simple AD Cache” mode, Protect Server doesn’t retrieve a list of groups in the organisation. This means if the last AD cache refresh was performed with “Simple AD Cache” enabled, but you then disable it and expect a tree structure, the tree may be empty. This is because there will not be any groups to present in the tree until the next AD cache refresh is performed with “Simple AD Cache” disabled.*

To configure Active Directory cache settings:

1. Log into the Protect Server web console as an Administrator role user and select **Settings**.

2. Select **AD Cache**.



3. Select the **Enable Active Directory-based default profile selection** checkbox to enable AD group selection when creating profiles.
4. Select the **Use Simple AD Cache** checkbox if you want to specify your AD group for a profile by name using a text box rather than selecting from a tree structure.
5. Enter the credentials of a domain user to enable Protect Server to have read access to the domain controller's global catalog.
6. Click **Save Changes**.
7. Select the **Manual Refresh Only** radio button and click **Refresh Now**. Protect Server checks Active Directory for groups and caches them locally to disk.
8. In order to set up an automatic refresh of the Active Directory groups, select the **Cron Schedule** radio button and specify a Cron expression. For example, **0 30 4 ? * SUN *** means that Protect Server checks Active Directory for groups every Sunday at 4.30am.

> ***Note**: For further explanation of Cron schedule syntax, you can refer to http://www.quartz-scheduler.net/documentation/quartz-2.x/tutorial/crontriggers.html.*

9. Click **Save Changes**. The settings are saved and a message is displayed across the top of the screen.

Protect Portal Configuration

The Workshare Protect Portal can be configured by modifying properties in the web.config file (C:\Program Files\Workshare\ProtectPortal\Web\web.config).

The following table describes the properties that may be changed.

Property	Description
NotificationSender	Sender's display name for notifications sent by Protect Portal.
NotificationSenderAddress	Sender's email address for notifications sent by Protect Portal.
ExpiryMinutes	Expiry time of links sent by Protect Portal. After this time, emails are deleted. Senders must resend their email.
DatabaseExpiryDays	Number of days to retain email metadata. (This is used to inform senders about the state of their email after their links have expired.)
BaseUrl	URL to use in notification links. Leave blank to use the fully qualified domain name of this machine.
SmtpSsl	Used to configure TLS connections to Protect Server. True/False.
SmtpHost	Hostname of Protect Server machine.
SmtpPort	Port of Protect Server machine.
SmtpUser	SMTP user for Protect Server SMTP service.
SmtpPassword	SMTP password for Protect Server SMTP service.
FileStorageLocation	File path to store delayed emails.
ServerUuid	Internal use only. Do not modify.
TempStorePassphrase	Passphrase for temporary password data.
TempStoreExpiryMinutes	Expiry time for temporary password.
ProtectApiBaseUrl	URL to Protect Server. This is used to store passwords temporarily. Data is sent and stored encrypted.
Organization	The name of your organization to reference within notification emails.
DemoMode	Internal use only. Do not modify.

Appendix A. System Status

This appendix provides information on monitoring the system status of Workshare Protect Server.

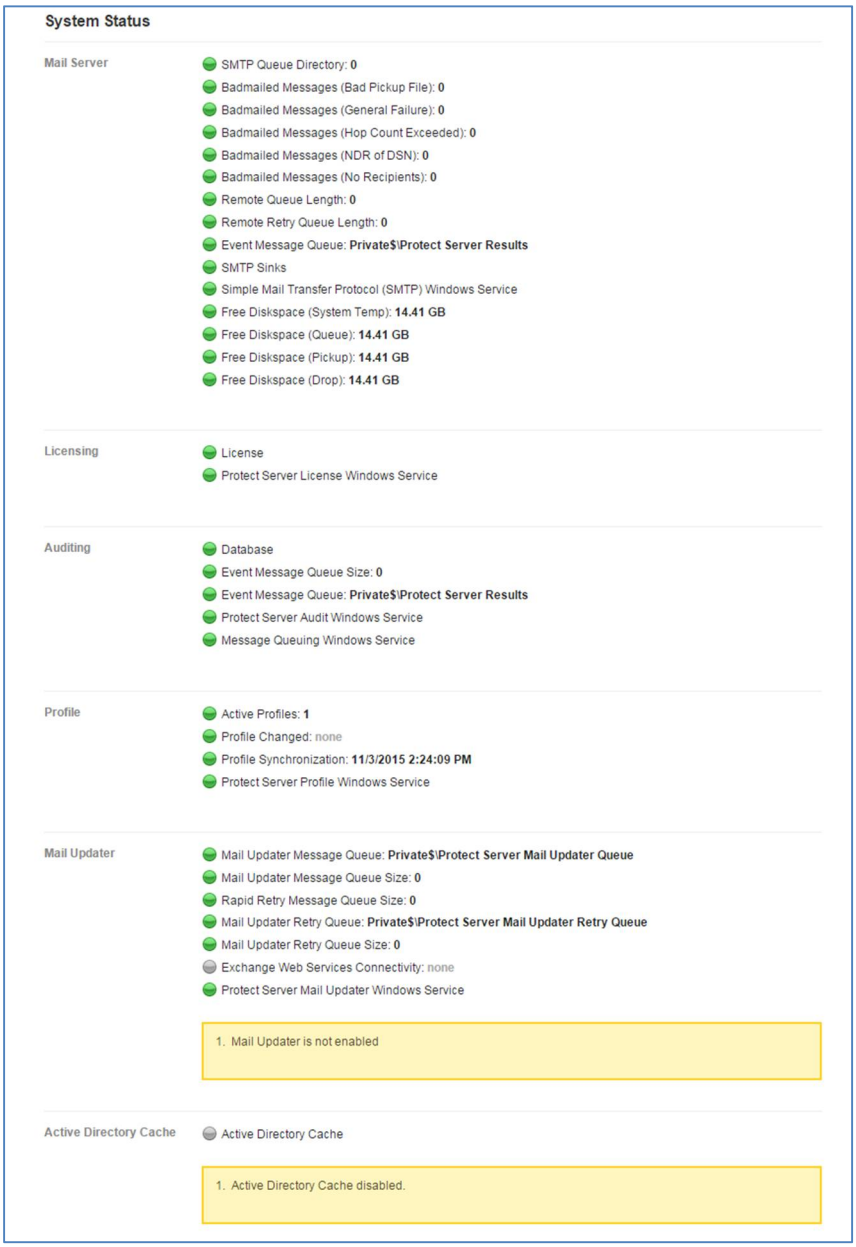
This functionality is available for Administrator role users only.

Monitoring Status

The performance and current health of Workshare Protect Server is shown in the **Status** tab of the Protect Server web console. For example, the **Status** tab shows whether Protect Server services are up and running, whether the database is connected, whether the Protect Server license is expired and details of any emails queued on Protect Server.

To monitor system status:

1. Log into the Protect Server web console (as an Administrator role user).
2. Select **Status**.



The following information is shown:

Area	Item	Description
Mail Server	**SMTP Queue Directory**	The count of how many SMTP messages are currently being processed by the SMTP service. The status indicator will show gray in the event of a failure in the performance counters.
	Badmailed Messages (Bad Pickup File)	The count of how many messages could not be delivered due to an incorrect format.
	Badmailed Messages (General Failure)	The count of how many messages could not be delivered due to an unspecified general error.
	Badmailed Messages (Hop Count Exceeded)	The count of how many messages could not be delivered due to incorrect message routing.
	Badmailed Messages (NDR of DSN)	The count of how many messages could not be delivered due to an NDR returned.
	Badmailed Messages (No Recipients)	The count of how many messages could not be delivered because no recipients were given.
	Remote Queue Length	The count of how many messages are waiting first attempt at delivery.
	Remote Retry Queue Length	The count of how many messages are waiting additional delivery attempts after the initial one failed.
	Event Message Queue	The state of the queue where processing results are stored. If this is red then the mail server has issues writing the processing results to this queue.
	SMTP Sinks	Whether the Protect Server functionality is correctly registered with the Windows SMTP server instances.
	Simple Mail Transfer Protocol (SMTP) Windows Service	Whether the SMTP service is up and running. If the status indicator is red, a warning message is displayed instructing you to restart the service.
	Free Diskspace (System Temp)	The amount of free disk space on the volume where the system temp folder is located.
	Free Diskspace (Queue)	The amount of free disk space on the volume where the SMTP server queue folder is located.

Area	Item	Description
	Free Diskspace (Pickup)	The amount of free disk space on the volume where the SMTP server pickup folder is located.
	Free Diskspace (Drop)	The amount of free disk space on the volume where the SMTP server drop folder is located.
Licensing	**License**	Whether Protect Server is licensed.
	Protect Server License Windows Service	Whether the license service is up and running. If the status indicator is red, a warning message is displayed instructing you to restart the service.
Auditing	**Database**	Whether Protect Server is connected to the database. If the status indicator is yellow, there are problems with the connection which are explained in a message box with advice on how to proceed.
	Event Message Queue Size	The count of how many message clean results are waiting to be uploaded to the database storage.
	Event Message Queue	The state of the queue where processing results are stored. If this is red then the Protect Server audit service has problems accessing the queue.
	Protect Server Audit Windows Service	Whether the audit service is up and running. If the status indicator is red, a warning message is displayed instructing you to restart the service.
	Message Queuing Windows Service	Whether the MSMQ service is up and running. If the status indicator is red, a warning message is displayed instructing you to restart the service.
Profile	**Active Profiles**	The number of profiles active in the system.
	Profile Changed	The last time a profile was changed.
	Profile Synchronization	The last time the profiles were copied to the local machine where Protect Server resides.
	Protect Server Profile Windows Service	Whether the profile service is up and running. If the status indicator is red, a warning message is displayed instructing you to restart the service.

Area	Item	Description
Active Directory Cache	**Active Directory Cache**	Whether the Active Directory cache service is up and running. If the status indicator is red, a warning message is displayed instructing you to restart the service.
Mail Updater	**Mail Updater Message Queue**	The state of the queue where emails wait to be synchronized.
	Mail Updater Message Queue Size	The count of the emails in the queue waiting to be synchronized.
	Mail Updater Retry Queue	The state of the queue where emails wait to be synchronized after initial synchronization failed.
	Mail Updater Retry Queue Size	The count of the emails in the queue where emails wait to be synchronized after initial synchronization failed.
	Rapid Retry Message Queue Size	The count of the emails in the rapid retry queue.
	Exchange Web Services Connectivity	Whether the impersonation user has rights to access other users' mailboxes.
	WPSMailUpdaterService Windows Service	Whether the mail updater service is up and running. If the status indicator is red, a warning message is displayed instructing you to restart the service.

In a healthy environment, all status indicators should be green. Where there is a red indicator, you may need to intervene.

The timeout of the five Workshare Windows services (Protect Server Profile Service, Protect Server License Service, Protect Server Health Service, Protect Server Audit Service and the Protect Server Active Directory Cache Service) is set to 30 seconds. If the machine hosting Protect Server is restarted and the services do not start within the 30 second timeout period, it will be necessary to start them manually.

Appendix B. X-Header Information

This appendix provides information on x-header information Workshare Protect Server inserts into emails.

Information Inserted

The following table describes the x-header information Workshare Protect Server inserts into emails

Xheader	Synopsis	Possible values	Presence in outbound email	Note
x-wsps-cleaned	Indicates this email was cleaned by Protect Server. Injected into every email processed by Protect Server.	Revision number of Protect Server, for example: x-wsps-cleaned: 3.6.0.155	Yes	
x-wsps-routedby	Indicates this email was rerouted through the Workshare Protect Routing Agent. Injected into every email routed by the Protect Routing Agent. Is also used by Protect Server to determine if a clean report should be generated in scenarios where TNEF formatted emails are being sent by Microsoft Exchange.	Version number of Exchange, for example: x-wsps-routedby: Exchange 8.38.	Yes	
x-wsps-cleanreport	Indicates this email is a clean report generated by Protect Server after cleaning an email. Injected into every clean report email.	Revision number of Protect Server, for example: x-wsps-cleaned: 3.6.0.155	No (clean reports are only sent to the original sender)	

Xheader	Synopsis	Possible values	Presence in outbound email	Note
X-Wsps-Bounce	Indicates this email was bounced back for violating any of the Bounce rules setup on Protect Server.	Revision number of Protect Server, for example: x-wsps-cleaned: 3.6.0.155	No (bounced emails are returned to sender)	
X-WorkshareProtect-DSP	Indicates this email was processed by the Workshare Protect Server client.	MD5 hash of subject and sender address	Yes	If email is routed through Protect Server then this header is removed by Protect Server.
x-ms-exchange-organization-processed-by-journaling	Used to mark an email as exempt from journaling to avoid duplicates. Injected into clean report emails if option AvoidCleanReportJournals is set to true. Injected into bifurcated emails if option AvoidBifurcatedJournals is set to true. Injected into bifurcated emails if option AvoidDuplicateJournals is set to true.	Version number of Exchange, for example: x-wsps-routedby: Exchange 8.38.	Yes	Only available with the Protect Routing Agent 2.2 and above.
x-wsps-InternalCleanReceipt	Indicates this email is a clean receipt generated by Protect Server sent to an internal user.		No (clean receipts are only sent to internal users)	

Appendix C. Advanced Configuration for Workshare Protect Server Email Security

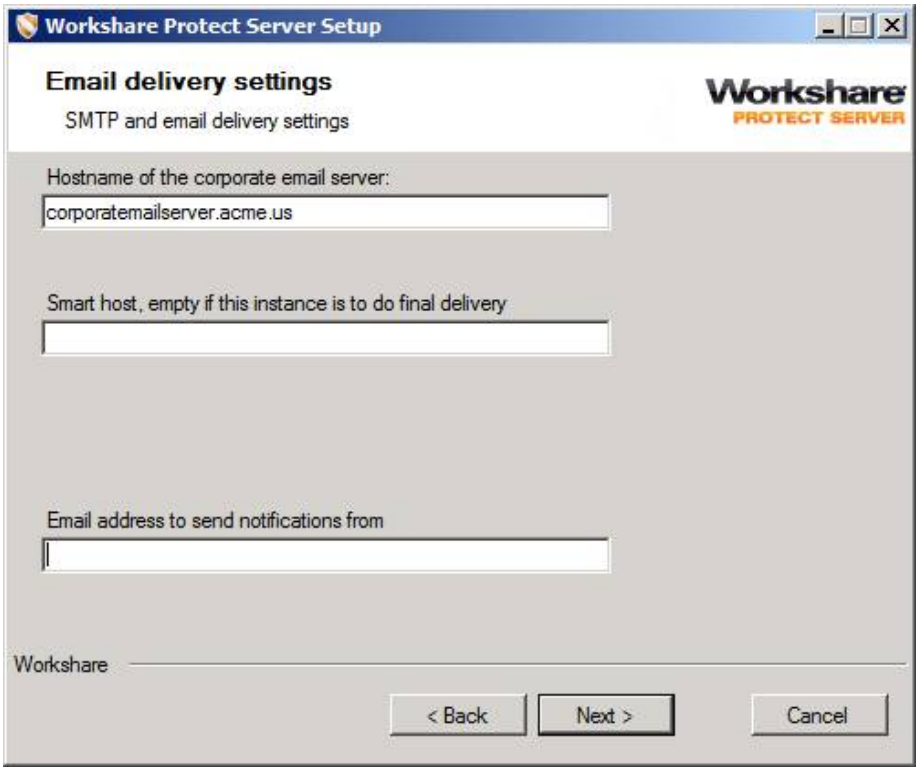
Introduction

The default installation of Workshare Protect Server is secure; consult this appendix to ensure that subsequent changes to the default configuration do not compromise security.

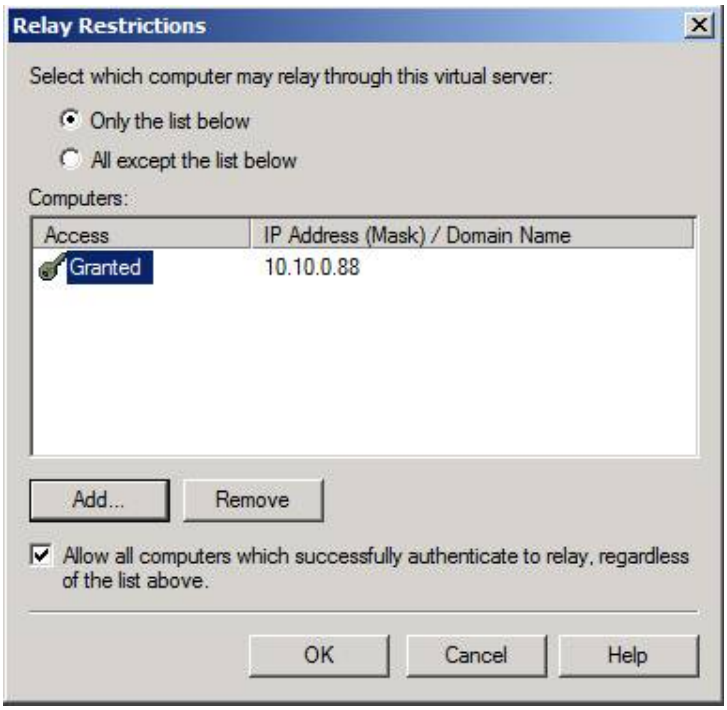
It is assumed in this appendix that Protect Server is being deployed in a corporate environment with correctly configured security and firewalls; only computers within the firewall would be able to access Protect Server. An internal user could make use of an incorrectly configured instance of Protect Server as a spam relay or allow a denial of service attack that may interrupt email delivery.

Default Installation

The default installation of Workshare Protect Server will create an SMTP relay that may only be accessed by a single computer.



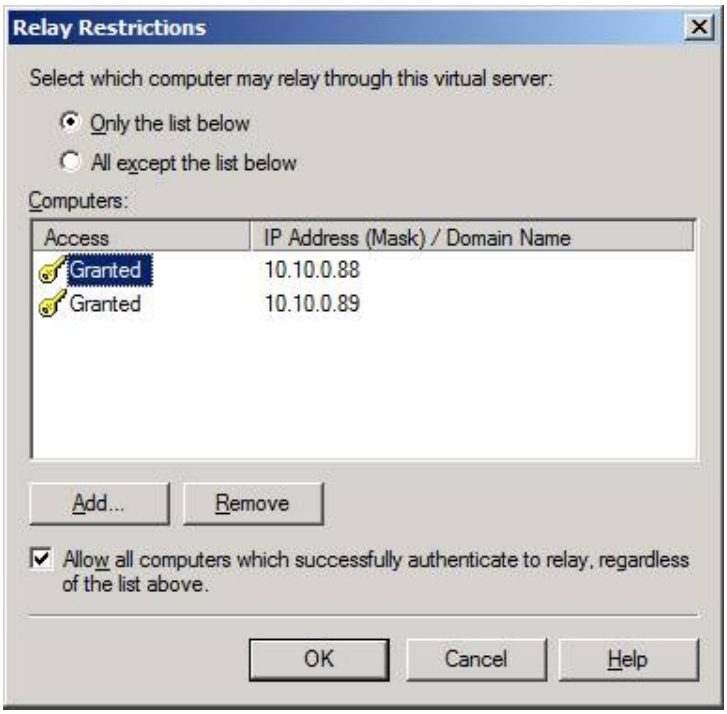
The IP address/computer name entered in the **Hostname of the corporate email server** field during installation is added to the granted list in the Microsoft SMTP service as the only computer able to relay.



Attempts to access the SMTP relay from other machines will result in a failure “Could not open a connection to the host, on port 25: Connect failed”.

***Note**: 127.0.0.1 must be added to this list if Protect Portal is installed*

Other computers can be added to this list to cater for environments with multiple mail servers.



Workshare Protect Server SMTP Authentication

The Microsoft Virtual SMTP service also provides authentication methods to verify connections to Workshare Protect Server. The configuration set on Protect Server must be supported by the email server.

Anonymous access

By default Protect Server is installed with **Anonymous access** – no user name or password is required to access the SMTP service.

All email servers support this configuration. With this configuration selected, security of Protect Server is provided only by the access control list for the SMTP relay.

Basic authentication

Basic authentication may be selected to help secure the SMTP server.

In this configuration a user name and password is transmitted, encoded in base 64, to the SMTP server before an email is submitted. This authentication method is vulnerable to "packet sniffing" attacks – the user name and password are not encrypted. If **the Allow all computers which successfully authenticate to relay, regardless of the list above** option is selected in the *Relay Restrictions* dialog (page 116), then the security of Protect Server could be compromised and the machine could be used as a spam relay or subject to a denial of service attack. Basic authentication is supported by Microsoft Exchange 2010/2013/2016.

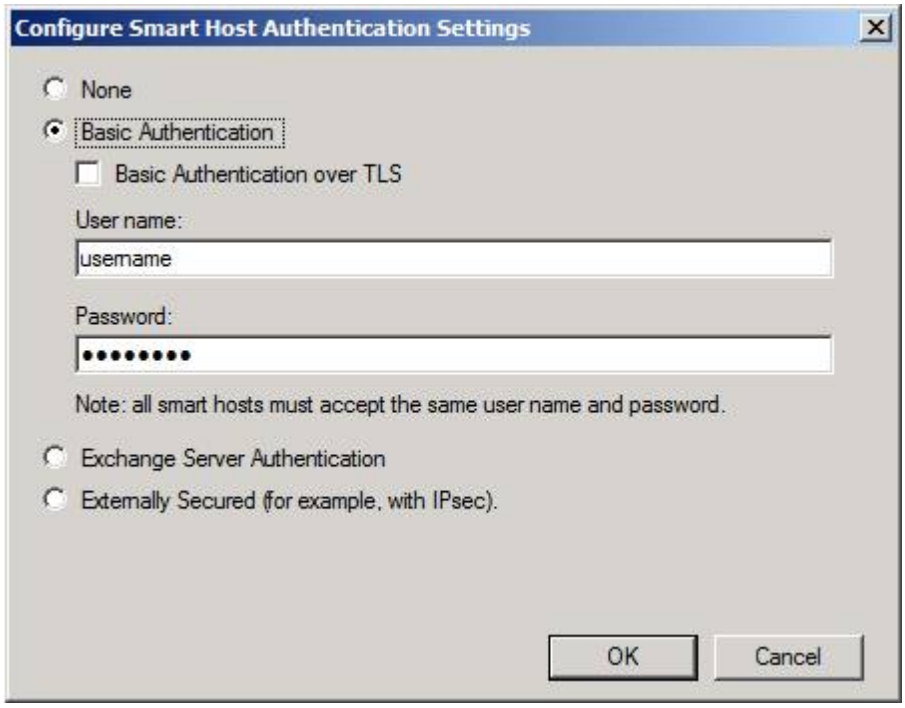
Workshare Protect Server configuration

To enable basic authentication, in the *Authentication* dialog (page 118) deselect the **Anonymous access** checkbox and select the **Basic authentication** checkbox. Optionally, enter a domain name in the **Default domain** field – members of this domain will be able to authenticate to the SMTP service and send email. If no domain is specified then the default domain is the computer name.

Microsoft Exchange 2010 configuration

To configure the email server to provide authentication to the SMTP server make the following changes:

View the properties of the send connector configured to route email to Protect Server and select the **Network** tab. Select **[Change...]** to display the *Configure Smart Host Authentication Settings* dialog.



Basic authentication with transport layer security

The use of TLS encrypts the credentials and message as it is relayed from the corporate email server to Protect Server.

Workshare Protect Server configuration

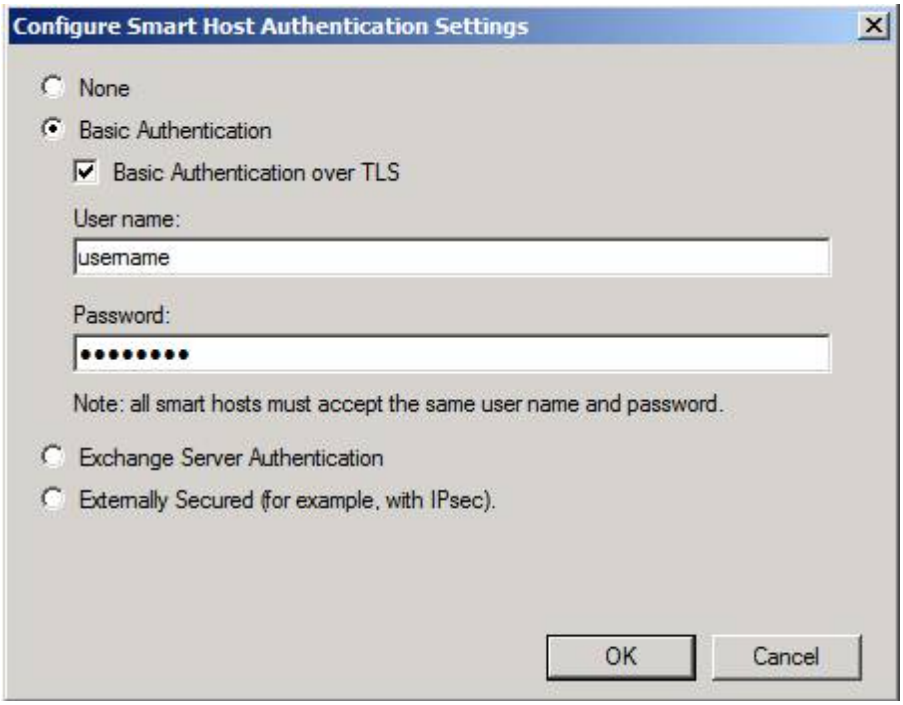
To encrypt the user name and password select the **Requires TLS encryption** checkbox in the *Authentication* dialog.

This configuration will require a X.509 certificate for Protect Server from a 3rd party certificate vendor. A self-signed certificate may be created for testing purposes using the selfssl.exe v 1.0 tool which is available in the IIS 6.0 resource kit (https://support.microsoft.com/kb/840671#11).

Microsoft Exchange configuration

To configure the email server to provide authentication to the SMTP server make the following changes.

Configure the send connector on Exchange Server for **Basic Authentication** and specify the user name and password.



Select the **Basic Authentication over TLS** checkbox.

Integrated Windows Authentication

Microsoft SMTP Service supports Integrated Windows Authentication to control access to Protect Server. NTLM/Kerberos is used to authenticate computers sending mail to Protect Server. Please note that both computers must be in the same domain.

Workshare Protect Server Configuration

To enable Integrated Windows Authentication, in the *Authentication* dialog (page 118) deselect the **Anonymous access** checkbox and select the **Integrated Windows Authentication** checkbox.

Appendix D. Pre-Deployment Checklist

This appendix provides a pre-deployment checklist that you can complete, print out and reference during the installation.

Pre-Deployment Checklist

Mail Server	
Exchange version	*Specify version*
Service Pack or Hotfix applied	*List all SP or hotfixes*
Exchange Addins	*List all addins installed on Exchange*
Third party mail services	
Exchange Server #1	*IP address*
Exchange Server #2	*IP address*
<add as necessary>	*IP address*
Client	
Outlook Client	*Specify versions used*
Service Pack or hotfix applied	*List all SP installed or hotfixes applied*
Gateways	
SMTP Gateway #1	*IP address*
SMTP Gateway #2	*IP address*
<add as necessary>	*IP address*
Blackberry Enterprise Server	*Yes/No*
MSSQL	
MSSQL Version	*Specify version*
Service Pack or Hotfix applied	*List all SP or hotfixes*
Full-Text Search installed	*Yes/No*
Remote/Local install	*Remote/local*
MSSQL Server Name	*hostname*
MSSQL Instance	*optional*

Catalog Name	*default: ProtectServerData*
DB User Name	*Use trusted connection*
Group Name	*<localmachine\Group name>*

Revisions
Published for Workshare Protect Server 3.10: 29/06/18
Published for Workshare Protect Server 3.11: 24/08/18

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

Workshare Ltd., 20 Fashion Street, London E1 6PX www.workshare.com