WORKSHARE PROTECT SERVER 3.2

SOLUTIONS GUIDE

Workshare

Version 2.0 | March 2015

COMPANY INFORMATION

Workshare Protect Server Solutions Guide

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

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

Workshare Website: www.workshare.com

Trademarks

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

Disclaimers

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

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

Copyright

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:

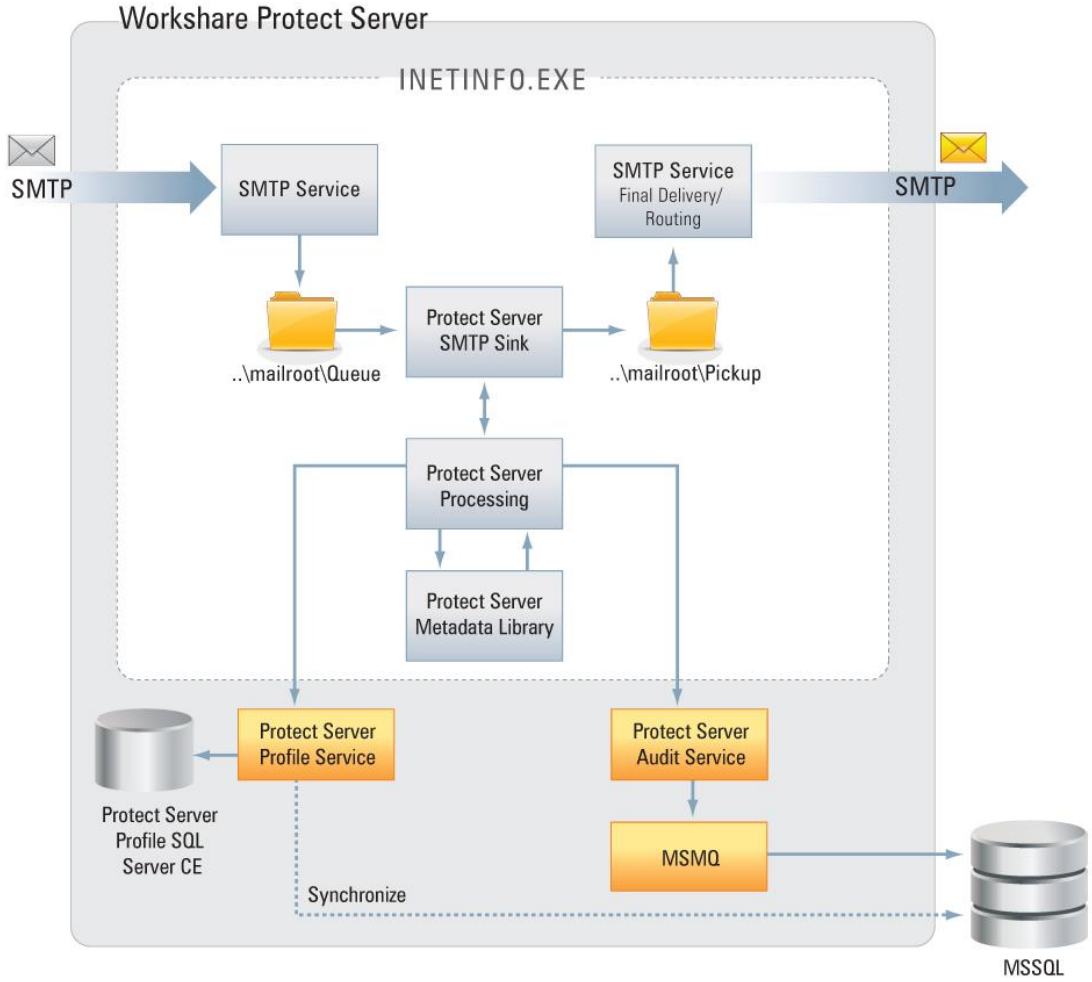
WHAT IS WORKSHARE PROTECT SERVER?

Workshare 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.

Workshare Protect Server provides server-based metadata cleaning and provides coverage for email from BlackBerry PDAs and Webmail (Outlook Web Access/Domino iNotes) as well as email from SMTP email servers (Microsoft Exchange or IBM Lotus Domino). Locating metadata cleaning on the server minimizes desktop applications and Outlook/Lotus Notes plug-ins that may impact email performance.

Email sent by any of the channels mentioned are always routed through the main Exchange/Domino server for which Workshare Protect Server acts a relay/final delivery server.

WORKSHARE PROTECT SERVER ARCHITECTURE



This diagram describes what happens to an email once it has been delivered by a corporate mail server to Workshare Protect Server.

1. The corporate mail server delivers an EML message which is received via SMTP.
2. The Microsoft SMTP Service drops email into the ..\mailroot\Queue folder located on Workshare Protect Server.
3. Workshare Protect Server SMTP Sink picks up emails from the Queue.
4. Workshare Protect Server SMTP Sink passes on the EML for processing.
5. Workshare Protect Server Processing reads the configuration file and processes the email before starting the metadata cleaning. This includes validating the attachments, unzipping, processing, override, etc.
6. Workshare Protect Server Metadata Library cleans metadata based on the configuration in the metadata.config file.
7. Workshare Protect Server Metadata Library returns emails with the clean attachments.
8. Workshare Protect Server activity is logged into MSSQL.
9. The message with the cleaned attachments is returned to the SMTP Sink.
10. The message with the cleaned attachments is then saved into the ..\mailroot\Pickup folder.
11. The message with the cleaned attachments is then sent out to a relay server or for final delivery.

FAIL CLOSE

In a production environment with two Workshare Protect Servers in operation (a primary and a backup), both Workshare Protect Servers can be configured to perform fail close. This means that if Workshare Protect Server detects an error that would affect email delivery, it automatically rejects inbound SMTP traffic so the corporate mail server will route email to the backup Workshare Protect Server. The delay to email delivery should be negligible.

In most cases, the reason for the fail close will be temporary (for example, the number of messages in the inbound queue may have passed the specified threshold) and the primary Workshare Protect Server will continue to process the backlog and then resume delivery once the queue size has dropped below the threshold value.

CHAPTER 2. WORKSHARE PROTECT SERVER DEPLOYMENTS

This chapter describes different deployments of Workshare Protect Server. It includes the following sections:

- **Information Required before Deployment**, page 9, describes the information you should gather prior to deployment of Workshare Protect Server.
- **Deployment Scenarios**, page 12, describes how to install and configure Workshare Protect Server in some typical deployment scenarios.
- **Post-Install System Tests**, page 18, describes tests to perform to verify that Workshare Protect Server is functioning correctly after installation.

INFORMATION REQUIRED BEFORE DEPLOYMENT

This section provides a reminder of the system requirements for Workshare Protect Server and then provides a checklist of the information you will need in order to install Workshare Protect Server.

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 2012 R2 Standard/Datacenter x64 Edition (recommended)
- Microsoft Windows Server 2012 Standard/Datacenter x64 Edition
- Microsoft Windows Server 2008 R2 Standard x64 Edition
- Microsoft Windows Server 2008 Standard x64 Edition

Notes:
Microsoft Windows Server 2003
Support for Windows Server 2003 (x86 and x64) has been removed from Workshare Protect Server.

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

Prerequisites

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

- Application Server and Web Server (IIS) Roles configured on Microsoft Windows Server.
- Microsoft IIS (Internet Information Services) 6.0, 7.0 or 7.5 with virtual SMTP service installed
- Microsoft Message Queue
- Microsoft SQL Server 2012-2005 SP3 with Full Text Search

***Note**: Only Microsoft SQL Server Express Advanced editions have Full Text Search while SQL Express editions do not.*

***Note**: If Workshare Protect Server is to be configured to run in with a remote SQL database, ensure that both machines (Workshare 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 Workshare Protect Server by the Workshare.ProtectServer.InstallWizard.exe.

- Microsoft .NET Framework 3.5 SP1 or higher
- Microsoft ASP.NET MVC 1.0
- Windows Installer for Server 2008 (x64/x86)
- Windows Visual C++ 2008 SP1 Redistributable Package (x86/x64)
- Windows Visual C++ 2005 SP1 Redistributable Package (x86/x64)
- Microsoft SQL Server Compact 3.5 SP2 (x86/x64)

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.

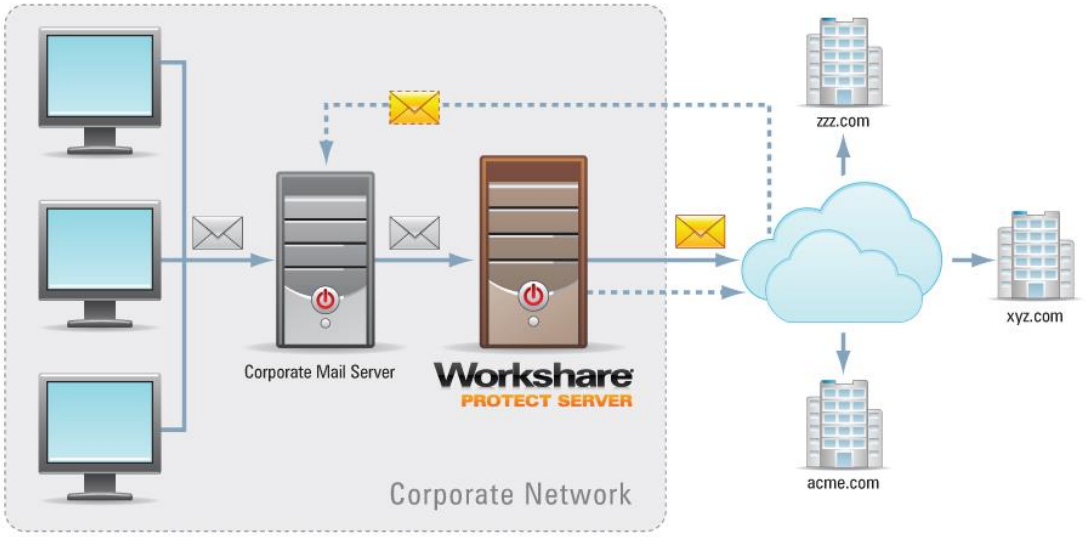
Pre-Deployment Checklist

Mail Server	
Exchange/Domino Version	*Specify version*
Service Pack or Hotfix applied	*List all SP or Hotfixes*
Exchange/Domino Addins	*List all addins installed on Exchange/Domino*
Third party mail services	
Exchange/Domino Server #1	*IP Address*
Exchange/Domino Server #2	*IP Address*
<add as necessary>	*IP Address*
Client	
Outlook/Notes 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>*

DEPLOYMENT SCENARIOS

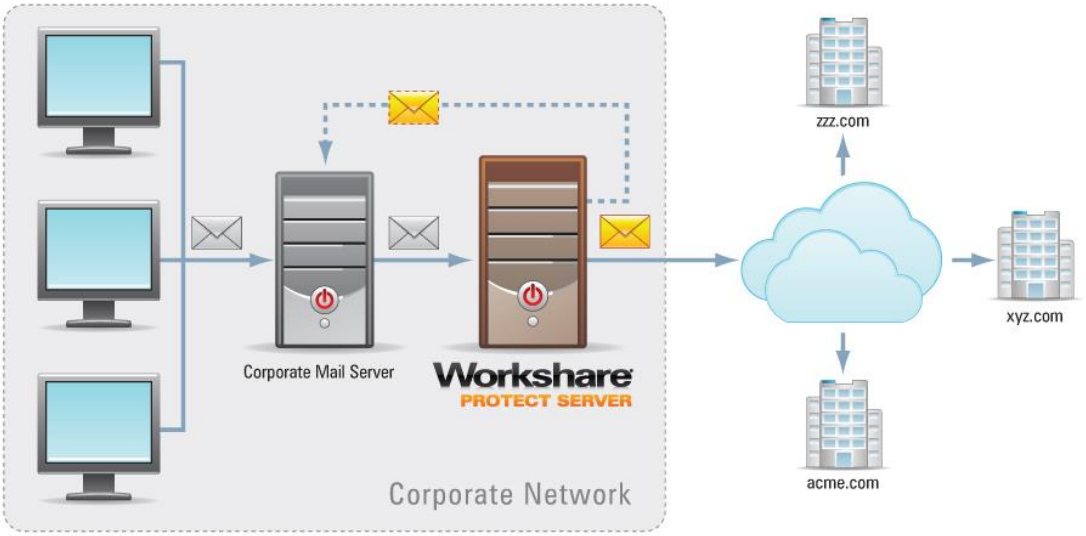
Four possible scenarios for Workshare Protect Server are detailed below

Scenario 1: One Corporate Mail Server Relays to One Workshare Protect Server



The Workshare Protect Server installer will cater for this scenario. The only additional configuration required is the modification of the corporate mail server to forward SMTP traffic through Workshare Protect Server. Consult the appropriate section of the *Workshare Protect Server Administrator Guide*.

Scenario 2: One Corporate Mail Server and One Workshare Protect Server with Cleaning Summary Emails Routed Internally



When Workshare Protect Server is configured in final delivery mode all emails are routed through the default SMTP domain and delivered through the internet. These settings can be modified in IIS Manager to suit the individual needs of a company and 3 examples are presented here:

- Route cleaning confirmation emails internally so that they are not delivered through the internet
- Route traffic to a specific domain (for example, a partner company)
- Route traffic to a mail gateway (post install steps)

***Note**: This scenario keeps clean receipt emails internal to reduce external email traffic.*

1. Run the Workshare Protect Server install in the normal manner and specify one mail server in the relevant host name field of the install.
2. Once the install has completed launch IIS Manager. (If you are using Windows 2008, you will need to launch the IIS 6.0 Manager.)
3. Expand the **Default SMTP Virtual Service** node, right-click **Domains** and select **New** and then **Domain**. The *New SMTP Domain Wizard* is displayed.
4. Select the **Remote** radio button and click Next.
5. In the **Domain Name** field, enter the domain name extension to which this connector should send email.

6. Continue in any of the following ways:

   Case 1: Route Cleaning Summary Emails Internally

   a. In the **Name** field, enter the internal domain name extension, for example ***.Workshare.com** and click **Finish**.

   b. The remote domain should be added in IIS Manager. Right-click on the domain and select **Properties**. The *[domain name] Properties* dialog is displayed.

   c. Select the **Forward all mail to smart host** radio button and enter the name of your mail server in the field. Click **OK**.

   Case 2: Route Cleaned Messages to a Partner Company

   a. In the **Name** field, enter the third party (partner company) domain name extension, for example ***.microsoft.com** and click **Finish**.

   b. The remote domain should be added in IIS Manager. Right-click on the domain and select **Properties**. The *[domain name] Properties* dialog is displayed.

   c. Select the **Forward all mail to smart host** radio button and enter the name of the third party (partner company) mail server in the field. Click **OK**.

7. Restart the Default SMTP Virtual Service.

Scenario 3: One Corporate Mail Server and Two Workshare Protect Servers (MX Record Example) Performing Final Delivery

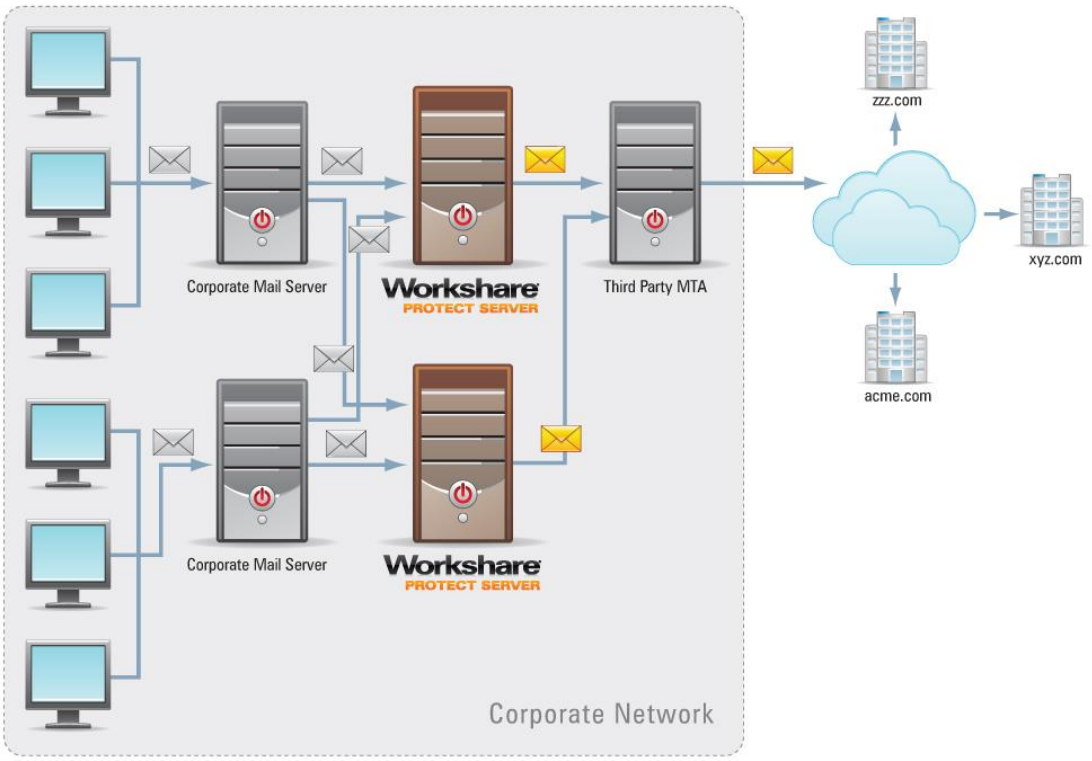
This scenario requires the creation of a sub domain inside the corporate domain prior to installation. Install both Workshare Protect Servers in your main domain; for each Workshare Protect Server specify the hostname of the corporate mail server in the **Hostname of the corporate email server** field during installation.

Configure the corporate mail server with a send connector to route all outbound traffic to the sub domain.

Add two MX records to the sub domain and for each specify an “A” record with the IP address of a Workshare Protect Server. The MX records may be assigned a priority which determines the order in which they are tried by the sending server:

- If different weights are specified in the MX records for the Workshare Protect Servers, the lowest weight record will be used. In the event of a failure in the primary Workshare Protect Server, the sending mail server would fail over to the secondary mail server.
- If the two MX records are assigned equal priorities, the sending mail server will randomly determine which Workshare Protect Server to use and, effectively, load balance the two Workshare Protect Servers.

Scenario 4: Two Corporate Mail Servers and Two Workshare Protect Servers



***Note**: To reduce the complexity of this diagram, the routing of cleaning summary emails was omitted.*

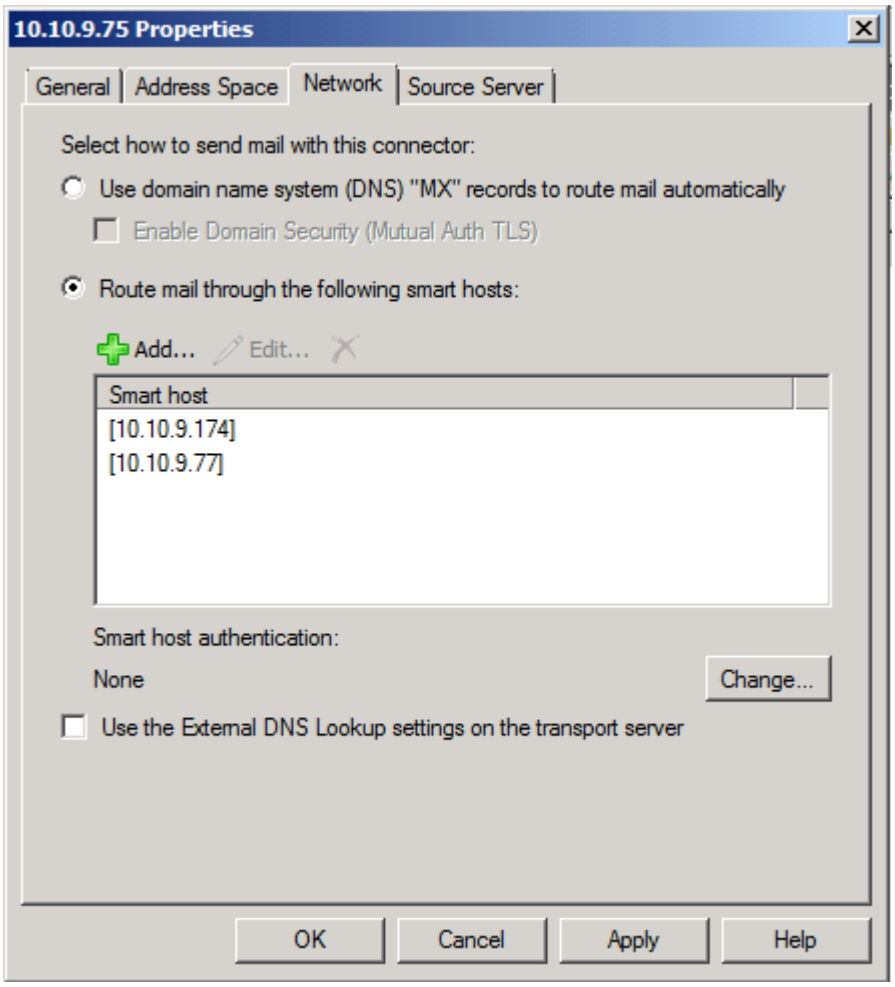
During installation of each Workshare Protect Server specify the IP address of the mail gateway and specify the IP address of one corporate mail server.

Use the steps from example 2 to add the additional corporate mail server to each Workshare Protect Server.

1. Run the Protect Server install in the normal manner and specify one mail server in the relevant host name field of the install.
2. Once the install has completed, launch IIS Manager. (If you are using Windows 2008, you will need to launch the IIS 6.0 Manager.)
3. Right-click **Default SMTP Virtual Service** and select **Properties**. The *SMTP Server Properties* dialog is displayed.
4. Select the **Access** tab and click **Relay**. The *Relay Restrictions* dialog is displayed showing the IP address of the configured corporate mail server.
5. Click **Add** and enter the IP address of the second corporate mail server in the **IP Address** field.

6. Click **OK**. The IP address of the second mail server should be added to the list in the *Relay Restrictions* dialog.
7. Click **OK** in the *Relay Restrictions* dialog and click **OK** again in the *SMTP Server Properties* dialog.
8. Restart the **Default SMTP Virtual Service**.

To accomplish fault tolerance and load balancing on Microsoft Exchange (2007 in this example), specify the IP address of both Workshare Protect Servers in the send connector, as follows:



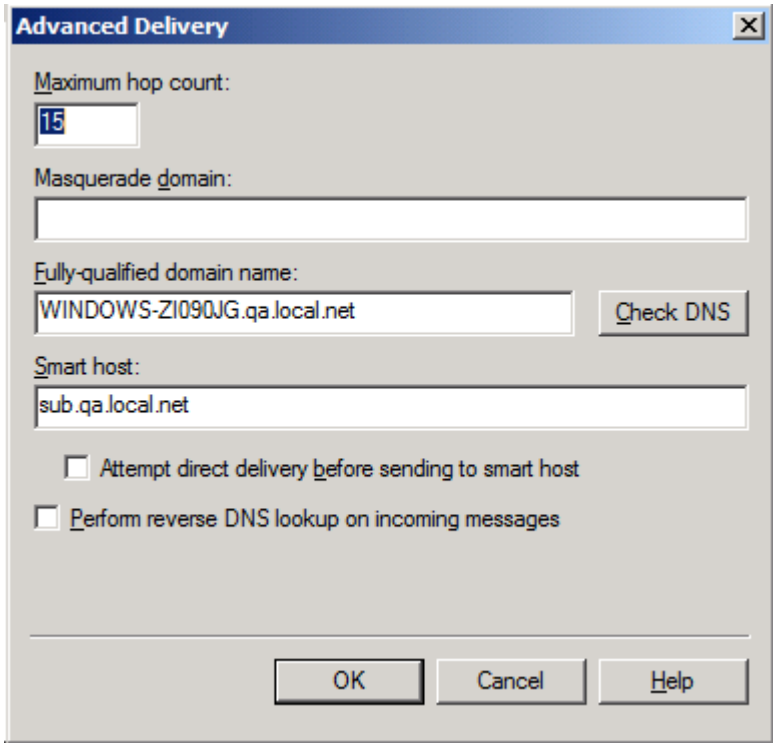
Scenario 5: Two Workshare Protect Servers Forwarding Email to Two or More Failover Final Delivery Servers

This scenario requires the creation of a sub-domain inside the corporate domain prior to installation. The sub-domain should contain 2 (or more) MX records corresponding to each of the final delivery mail servers. Each MX record must have an associated “A” record that identifies the IP address of the server.

If different weights are specified in the MX records for the Workshare Protect Servers, the lowest weight record will be used. In the event of a failure in the primary Workshare Protect Server, the sending mail server would failover to the secondary mail server.

If the two MX records are assigned equal priorities, the sending mail server will randomly determine which Workshare Protect Server to use and, effectively, load balance the two Workshare Protect Servers.

1. Install both Workshare Protect Servers in your main domain. For each Workshare Protect Server specify the hostname of the corporate mail server in the **Hostname of the corporate email server** field during installation.
2. Configure each Workshare Protect Server virtual SMTP service to forward email to a smart host for delivery and specify the sub-domain.
3. Run the Workshare Protect Server install in the normal manner and specify one mail server in the relevant host name field of the install.
4. Once the install has completed, launch IIS Manager. (If you are using Windows 2008, you will need to launch the IIS 6.0 Manager.)
5. Right-click **Default SMTP Virtual Service** and select **Properties**. The *SMTP Server Properties* dialog is displayed.
6. Select the **Delivery** tab and click **Advanced**. The *Advanced Delivery* dialog is displayed.



7. In the **Smart host** field enter the sub-domain and select **OK**
8. Click **OK** in the *SMTP Server Properties* dialog.
9. Restart the SMTP virtual service.

POST INSTALL SYSTEM TESTS

The following tests enable you to verify that Workshare Protect Server is functioning correctly after installation. These tests are not appropriate for testing a hosted Workshare Protect Server. It is intended that each test be run sequentially since the tests require that the previous test was successful to correctly verify that Workshare Protect Server is functioning correctly.

Test 1: Workshare Protect Server Web Page

Verify that the Workshare Protect Server web console is accessible after installation. Use Microsoft Internet Explorer 8 for this test.

Action	Expected Result	Possible Failure	Troubleshooting
On Workshare Protect Server launch Internet Explorer 8 and enter http://localhost/protect.	"Windows Security" authentication dialog displayed	Error 404 Web Page not Found	Is the IIS Service running on the Workshare Protect Server? Enter "IISRESET" in the *Run* dialog to restart IIS services. Is ASP.NET v2.0.50727 "Allowed"? Launch "Internet Information Services Manager" and select "Web Service Extension".
Enter a valid username and password and click Log On. The credentials used to log on are members of the "Administrators" group specified during installation. See the Workshare Protect Server Administration Guide for more information.	Workshare Protect Server "Message Logs" screen displayed with 0 entries	Blank "Windows Security" authentication dialog displayed	Re-enter valid username/password credentials – ensure that the user name is entered in the netbiosdomain\ username format.
		"500 – Internet server error" warning displayed	Verify that Workshare Protect Server can connect to the domain controller.
In the Messages tab, select the Search button.	Workshare Protect Server Message Logs screen displayed with 0 entries	"500 – Internet server error" warning displayed	Verify that Workshare Protect Server can access the SQL server and that the SQL server is running.

Action	Expected Result	Possible Failure	Troubleshooting
Select the Status tab.	All status indicators green	License status indicator red	Ensure that Workshare Protect Server is licensed. See the Workshare Protect Server Administration Guide for more information.
		Database status indicator red	Ensure that the SQL server is running and can be accessed by Workshare Protect Server.
		Mail Server status indicators grey	The SMTP performance counters will function after Workshare Protect Server is rebooted. It is necessary also to set the SMTP service to start automatically (in Windows Services Manager).
		Protect Server Profile Windows Service status indicator red	Ensure that the Profile service is running and the SQL server can be contacted.
		Simple Mail Transfer Protocol (SMTP) Windows Service status indicator red	Ensure the SMTP service is running.
From a remote computer launch Internet Explorer 8 and enter the URL for Workshare Protect Server: http://servername/protect.	"Windows Security" authentication dialog displayed	Error 404 Web Page not Found	Verify that the URL for Workshare Protect Server is correctly entered in IE8.
Enter a valid username and password and click Log On.	Workshare Protect Server "Message Logs" screen displayed with 0 entries	Blank "Windows Security" authentication dialog displayed	Re-enter valid username/password credentials

Test 2: Mail Server Connectivity

The following tests enable you to verify that mail is correctly sent from the corporate mail server to Workshare Protect Server.

Action	Expected Result	Possible Failure	Troubleshooting
Using a test account on the corporate mail server send a test email without attachment to an external recipient	Email delivered to external recipient and cleaning summary sent to sender (if configured)	Email not received by external recipient	Verify that the IP/FQDN of Workshare Protect Server is specified in the configuration of the corporate mail server
		"The message could not be sent because one of the recipients was rejected by the server…."	Verify that the virtual SMTP service on Workshare Protect Server has the IP address for the corporate mail server configured in the "Relay" section.
		Email not delivered to intended recipient. Non delivery report with: "The message could not be sent because one of the recipients was rejected by the server…"	Verify that the virtual SMTP service on Workshare Protect Server has the IP address for the test machine configured in the Relay section.
		Email not delivered to intended recipient. Non delivery report with: "The connection to the server has failed" error.	Verify that the virtual SMTP service is in the running state on Workshare Protect Server.
		Email not delivered to intended recipient.	If Workshare Protect Server is performing final delivery, verify that the email is not in the spam folder on the recipients email system.
Using a test account on the corporate mail server send a test email with supported attachment to an external recipient	Email delivered to external recipient with cleaned attachment	Email not received by external recipient	Consult Workshare Support.
		Email received but attachment not present	Consult Workshare Support.
		Email not delivered to intended recipient. Non delivery report with: "The message could not be sent because the size exceeded the servers limit...".	Verify that the file sent was less than the "message size" limit in the virtual SMTP server.

Action	Expected Result	Possible Failure	Troubleshooting
		The email is bounced back to sender with a warning: “Attachment is corrupt”.	Workshare Protect Server cannot process the attachment. Repair the document as necessary and re-send the email.
		The email is bounced back to sender with a warning: “Attachment is digitally signed and cannot be opened”.	Workshare Protect Server cannot process digitally signed attachments without invalidating the certificate. Re-send a copy of this attachment without a signature.
		The email is bounced back to sender with a warning: “The email is digitally signed”.	Workshare Protect Server cannot process digitally signed emails without invalidating the certificate. Re-send the email without the digital signature.
		The email is bounced back to sender with a warning: “Attachment is in legacy format such as Office 95”.	Workshare Protect Server does not support documents created by versions of Office before Office 97. Please save the attachment using Office 97 or later and se-send the attachment.
		The email is bounced back to sender with a warning: “Attachment is password-protected or encrypted”.	Workshare Protect Server cannot remove password protection from attachments. Remove the encryption and re-send the attachment.
		The email is bounced back to sender with a warning: “Errors occurred while processing attachment”.	Consult Workshare Support.

Test 3: Cleaning Functionality

The following tests enable you to verify that file attachments are cleaned and that the cleaning summary notification is delivered.

Action	Expected Result	Possible Failure	Troubleshooting
Send an email with supported attachment to a valid external email address	Email with supported attachment delivered to external recipient and attachment cleaned according to metadata cleaning settings. Message log and dashboard updated.	Attachment not cleaned	Verify that Workshare Protect Server is licensed (consult the Workshare Protect Server Administration Guide).
		Attachment not cleaned	Verify that the cleaning override address was not used.
		Attachment not cleaned	If Workshare Protect client is used, verify that Workshare Protect Server is configured to clean messages handled by Workshare Protect client.
		Attachment not cleaned	Verify that the “Metadata Removal” settings or the particular file type are configured in the Profiles page of the Workshare Protect Server web console.
		Attachment not cleaned	Verify that the attachment is a supported file type (consult the Workshare Protect Server Administration Guide).
		Attachment not cleaned	Verify that the attachment or email is not signed or otherwise protected
		Cleaning Summary email not received	Verify that a From email address is configured in the “Email Communication” section of the “Cleaning Settings” page of the Workshare Protect Server web console.
		Cleaning Summary email not received	Verify the cleaning summary email is not in your spam folder.
		Cleaning Summary email not received	Verify that “send Clean Receipt” is selected in the “Cleaned Receipt” sections of the “Cleaning Settings” page of the Workshare Protect Server web console.
		Incorrect cleaning	Verify Workshare Protect Server cleaning settings. Consult the Workshare Protect Server Administration Guide for details on expected outcomes from cleaning.

Test 4: Protect Server Reporting and Search

The following tests will verify that Workshare Protect Server is correctly configured to produce audit logs and reports.

Action	Expected Result	Possible Failure	Troubleshooting
From a remote computer launch Internet Explorer 8 and enter the URL for Workshare Protect Server: http://servername/protect.	"Windows Security" authentication dialog displayed	Error 404 Web Page not Found	Verify that the URL for Workshare Protect Server is correctly entered in IE8.
Enter a valid username and password for a member of the "business users" group	Workshare Protect Server "Message Logs" screen displayed with 0 entries	Blank "Windows Security" authentication dialog displayed	Re-enter valid username/ password credentials
Select the Reports tab	Reports page opened with "Profile Usage" statistics displayed	Reports tab not displayed	Ensure that the logged in user is a member of the "business user" role. See the Workshare Protect Server Administration Guide for more information.
		No Profile Usage data displayed	Select the "Past Week"/"Past Month" hyperlinks to ensure that all data is displayed.
Select the "Metadata" link	Summary information displayed for all attachments cleaned	No metadata summary data displayed	Select the "Past Week"/"Past Month" hyperlinks to ensure that all data is displayed.
Select the "File Formats" link	Summary information displayed for all file types cleaned by Workshare Protect Server	No file format information data displayed	Select the "Past Week"/"Past Month" hyperlinks to ensure that all data is displayed.

Action	Expected Result	Possible Failure	Troubleshooting
Close and re-open IE8. Navigate to the Workshare Protect Server web page and when logging on, use a user account that is a member of the Administrators security group	Workshare Protect Server "Message Logs" screen displayed with a number of entries	-	-
Enter a word or phrase in the search field and click "Search"	A list of all the messages that contain the specified word or phrase should be returned	No search data returned	Re-try the test with a different search term (ensure that the search string exists in the cleaned email messages).

CHAPTER 3. WORKSHARE PROTECT SERVER AND CLIENT

This chapter describes the interaction between Workshare Protect Server and client. It includes the following sections:

- **Skip Cleaning on Workshare Protect Server**, page 25, describes how to configure Workshare Protect Server to skip cleaning of emails that have been processed by Workshare Protect client.
- **Skip Cleaning on Workshare Protect Client**, page 26, describes how to configure Workshare Protect client to not check email for metadata.
- **User Interaction with Workshare Protect Server**, page 27, describes how a desktop user may interact with Workshare Protect Server.

SKIP CLEANING ON WORKSHARE PROTECT SERVER

It is possible to have Workshare Protect Server cleaning all emails passing through your corporate network and also to have Workshare Protect client cleaning emails from individual machines within your corporation. To avoid duplication of cleaning, you can configure Workshare Protect Server to skip cleaning of emails that have been processed by the Workshare Protect client. This means that if you have the Workshare Protect client installed on your desktop and the client is checking your emails for metadata, then your emails will not be cleaned again by Workshare Protect Server.

To configure Workshare Protect Server to skip cleaning:

1. Log into the Workshare Protect Server web console.
2. Select **Settings**.
3. Select **Override**.
4. In the **Protect Client Message Processing** area, select **Skip cleaning on messages processed by Workshare Protect Client**: Workshare Protect Server will not clean emails that have already been cleaned by the Workshare Protect client.
5. Click **Save Changes**. The settings are saved and a message is displayed across the top of the screen.

If you do not configured Workshare Protect Server in this way, then Workshare Protect Server will clean all emails even those that have already been cleaned by the Workshare Protect client.

Payne Metadata Assistant

Where you work with Payne Metadata Assistant, you can configure Workshare Protect Server to skip cleaning of emails that have been processed by Payne Metadata Assistant. This means that if you have Payne Metadata Assistant installed on your desktop checking your emails for metadata, then your emails will not be cleaned again by Workshare Protect Server. However, Workshare Protect Server can still offer cleaning of emails sent from mobile devices.

SKIP CLEANING ON WORKSHARE PROTECT CLIENT

You can also configure Workshare Protect client to skip cleaning if you have Workshare Protect Server cleaning all emails passing through your network.

To configure Workshare Protect client to skip cleaning:

1. Access the Workshare Policy Configuration Manager.
2. Select the Internal Policy category.
3. Make sure the **Ignore all Protect policies on internal email** parameter is selected (this parameter is selected by default). Workshare Protect client will not check the content and attachments of emails sent internally for metadata.
4. Select the External Policy category.
5. Make sure the **Ignore all Protect policies on external email** parameter is selected (this parameter is NOT selected by default). Workshare Protect client will not check the content and attachments of emails sent externally for metadata.
6. Click **OK**.

It is recommended not to remove or uninstall Workshare Protect Client. There is further functionality available with Workshare Protect client aside from metadata cleaning, such as PDF creation, checking open documents for metadata, manual redaction and document classification.

USER INTERACTION WITH WORKSHARE PROTECT SERVER

There is essentially no interaction with Workshare Protect Server for the normal desktop user. In effect, a user will not always know that all emails sent are cleaned by Workshare Protect Server. The following areas are where a user may interact with Workshare Protect Server:

- **Profiles**: Workshare Protect Server processes emails according to profiles. A profile is a collection of metadata and PDF conversion settings – a set of instructions to Workshare Protect Server as to 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 Workshare Protect Server determines which profile to apply to any given email. The user can add the email address of a profile as a recipient in an email and Workshare Protect Server will apply this profile when processing the email. If no profile email address is specified then Workshare Protect Server will apply whichever profile the administrator has defined as the Default profile. If more than one profile email address is specified then Workshare Protect Server will apply whichever profile the administrator has defined as the Fallback profile.
- **Cleaning Override Address**: When a cleaning override email address has been configured, the user can use this address to bypass cleaning/conversion on Workshare Protect Server. In order to send an email which will not be cleaned/converted by Workshare Protect Server, the user must enter this override email address in the any of the recipient fields of an email (**To** or **Cc**).

  ***Note**: The cleaning override email address will always take precedence over any profile email address. So when the cleaning override email address is specified, even if a profile email address is also specified, Workshare Protect Server will always skip processing.*

- **Previewing Processed Email Attachments**: Workshare Protect Server can provide a preview of what attachments will look like once processed (cleaned or converted). In order to request a preview of what the processed attachments will look like before sending them to recipients, users must send the email to a profile email address only. Workshare Protect Server will treat such an email as a preview request and send the processed attachments back to you.
- **Cleaning Receipts**: When Workshare Protect Server has been configured to send clean receipts, the user will receive a clean receipt email with an attached Clean Report PDF each time a sent email is processed. The clean receipt email provides a summary of the processing performed and the metadata removed from each attachment whereas the Clean Report provides the details of the actual content of the metadata removed. The clean receipt email may also include a copy of the processed email as an attachment.

- **Bounced Emails**: When Workshare Protect Server has been configured to prevent emails with attachments that include comments or track changes or that cannot be processed from being delivered, it bounces the email back to users with a non-delivery email. There are several reasons why Workshare Protect Server may not be able to process an attachment (for example, corrupt attachment, digitally signed attachment) and the reason is outlined in the non-delivery email. The non-delivery email will recommend a course of action for the user and the original email may also be attached. When users receive a non-delivery email with notifications that Workshare Protect Server has found comments or track changes in the attachments or cannot process attachments, they can choose to resend the email from their Sent folder with the override email address as well as the original recipients – this bypasses Workshare Protect Server processing – or create a new email with updated attachments and send.

***Note**: For information on how to configure any of the above functionality, refer to the Workshare Protect Server Administrator Guide.*

Users can also use the Workshare Protect Server web console to view and search through emails they have sent through Workshare Protect Server and also view profiles. Additionally, Business Role users can view reports about Workshare Protect Server activity.

Appendix A. CREATING SMTP ACCOUNT FOR TESTING PROTECT SERVER

This appendix describes the configuration of Microsoft Outlook (2007) to send email directly to Workshare Protect Server for testing purposes.

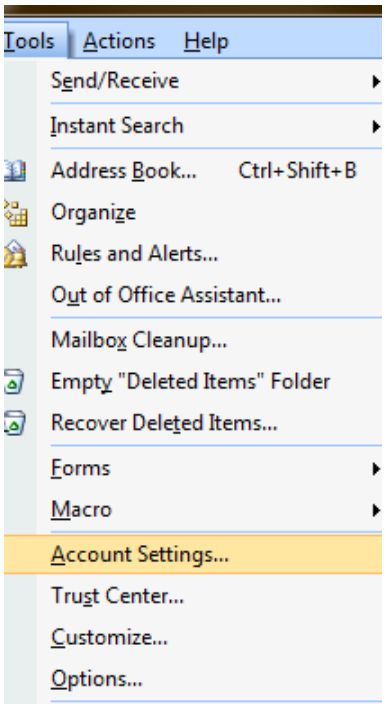
CREATING SMTP ACCOUNT

For each user that will be testing Workshare Protect Server, the administrator will have to setup a test email account that will allow the tester to receive email from the Exchange server and then to deliver any outbound emails to Workshare Protect Server.

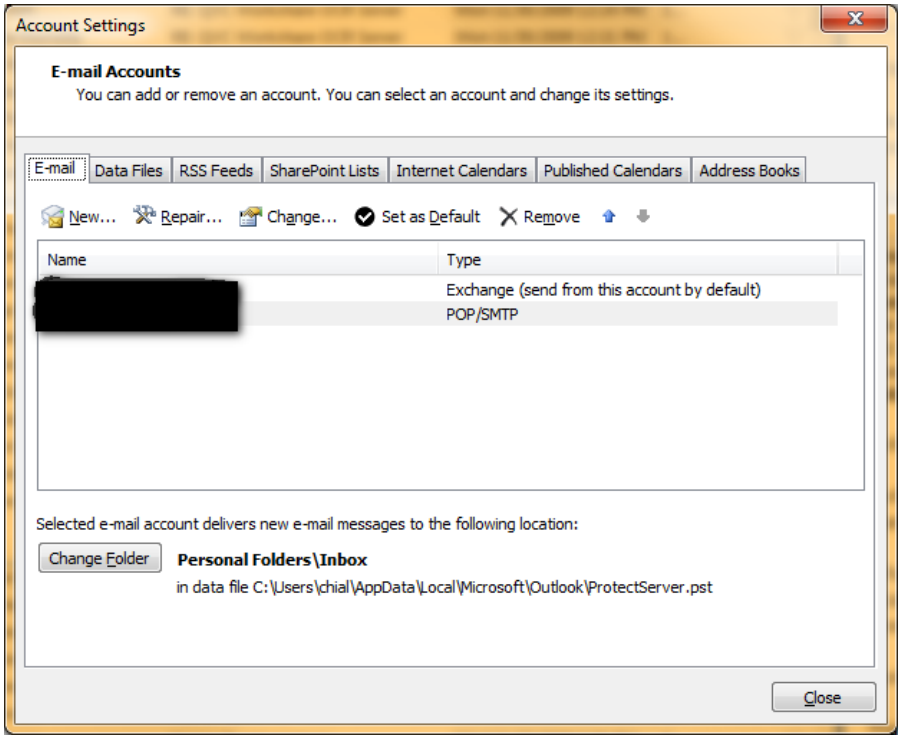
In addition, Workshare Protect Server must be configured to allow relay access to each user that will be testing Workshare Protect Server.

To configure Outlook to send email directly to Workshare Protect Server for testing purposes:

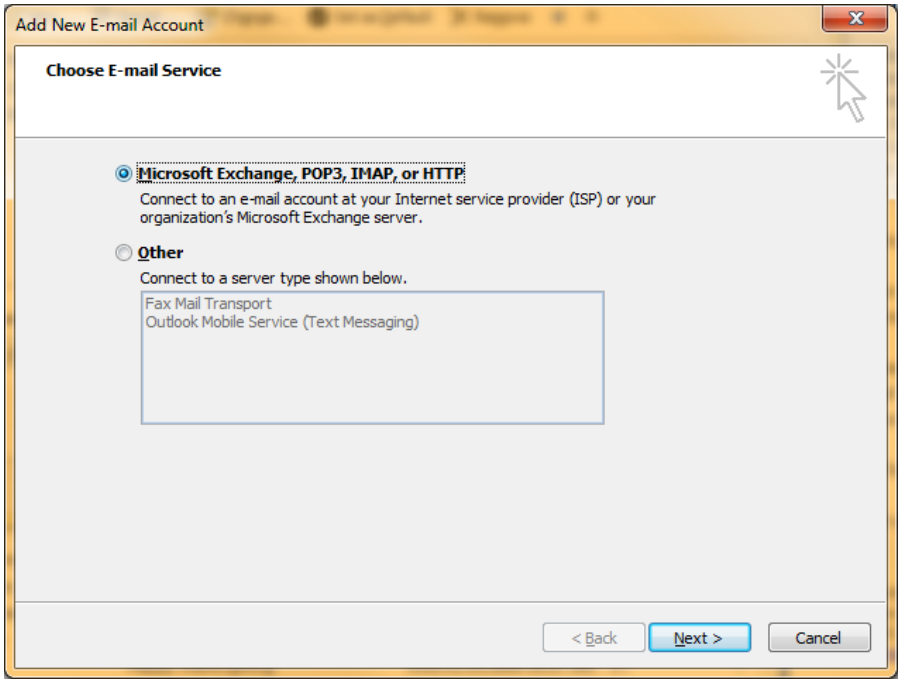
1. Open Outlook.
2. From the *Tools* menu, select **Account Settings**.



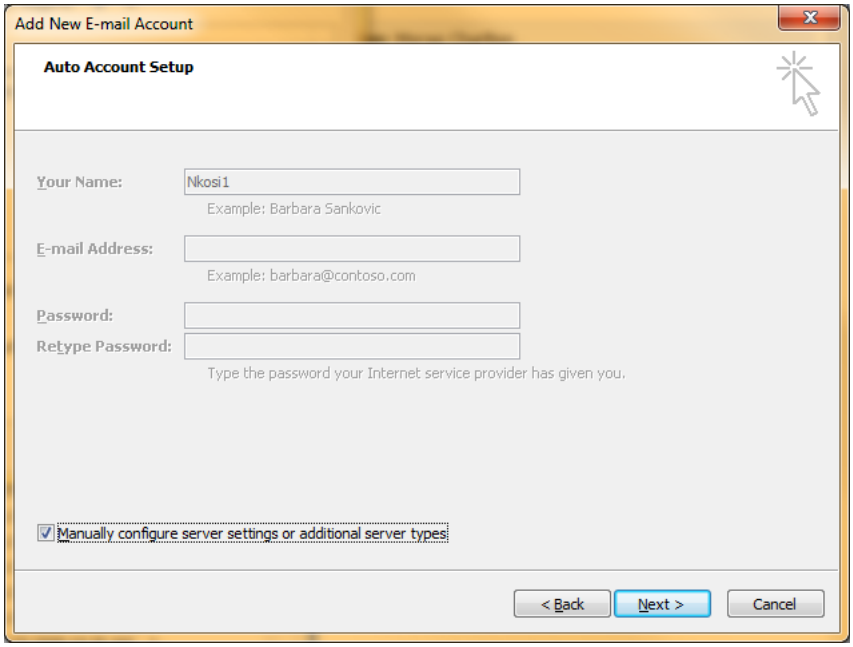
3. Select the **Email** tab.



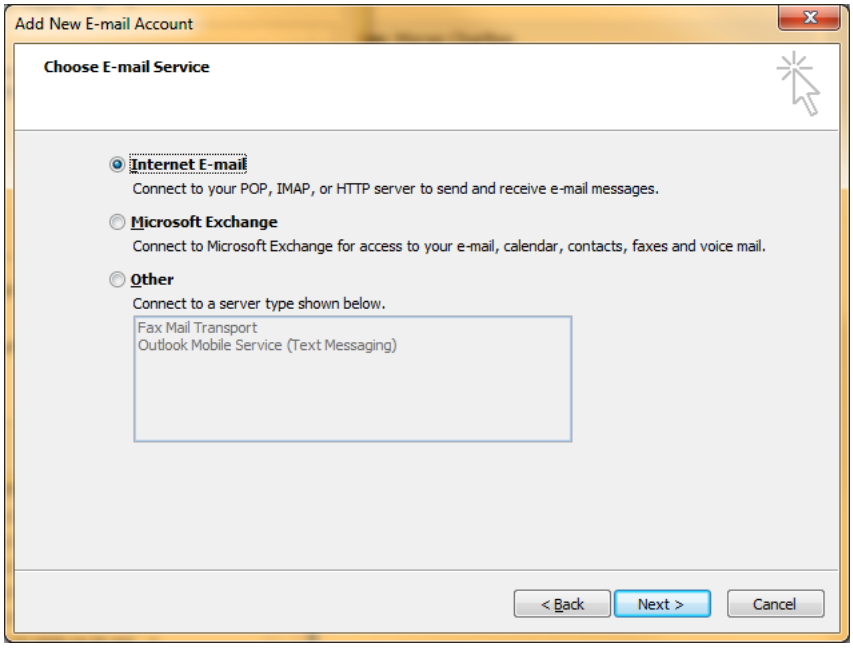
4. Click **New**.



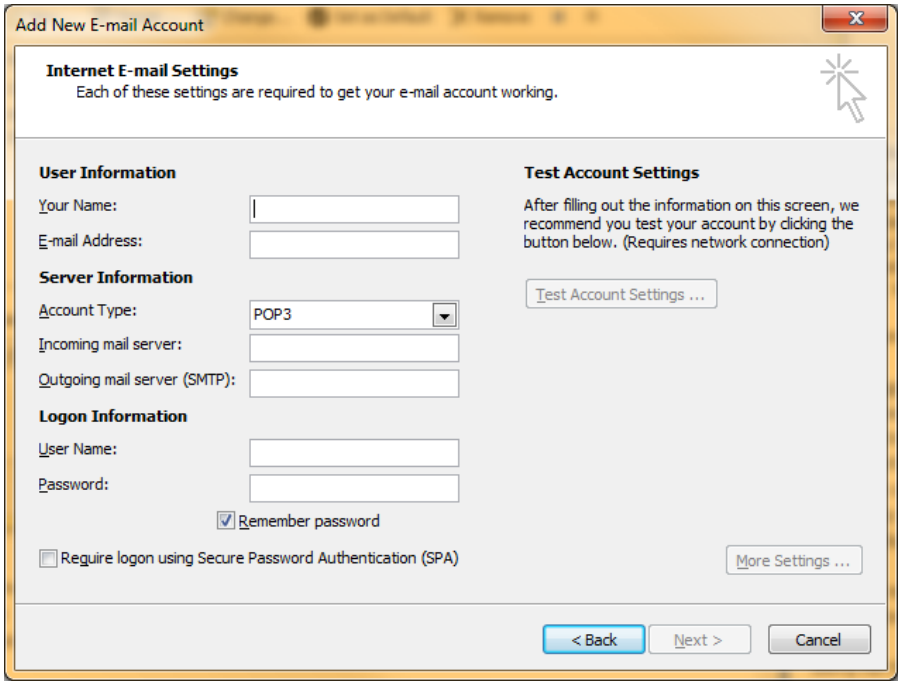
5. Select Microsoft Exchange,POP3,IMAP, or HTTP and click Next.



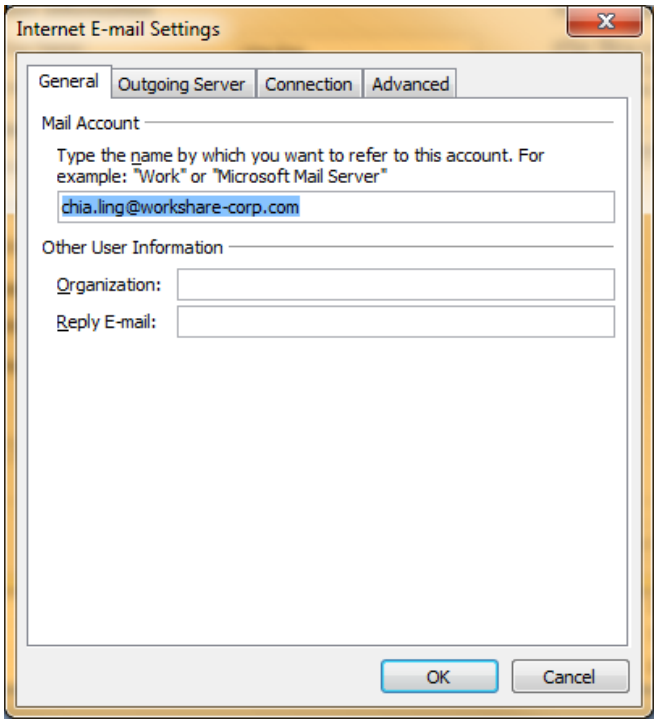
6. Select the **Manually configure server settings or additional server types** checkbox and click **Next**.



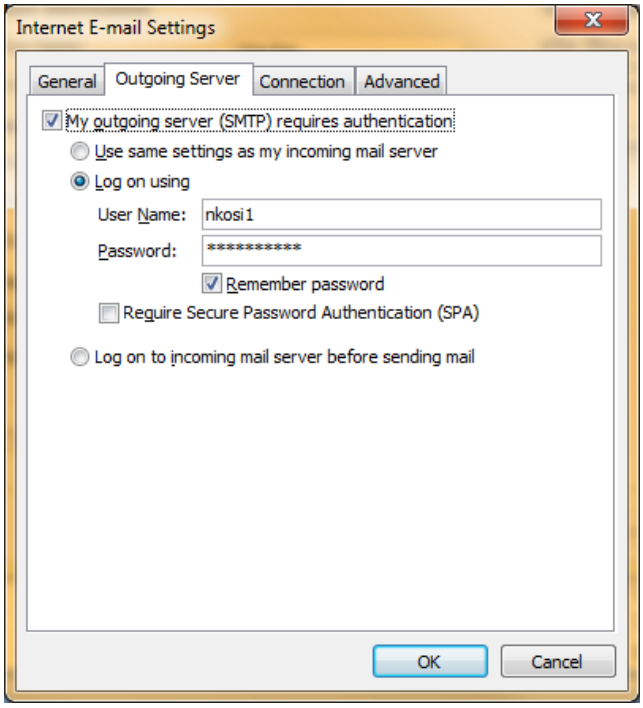
7. Select **Internet E-mail** and click **Next**.



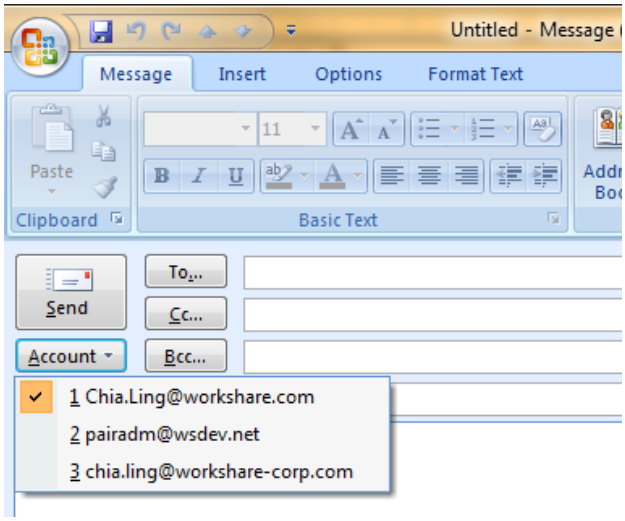
8. Enter the email user information, specifying the production Exchange server as the **Incoming mail server** and Workshare Protect Server as the **Outgoing mail server**. You will also need to enter the logon credentials for Workshare Protect Server to ensure emails can be sent from this account to Workshare Protect Server. You can specify the Workshare Protect Server logon credentials by clicking **More Settings**.



9. Select the **Outgoing Server** tab.



10. Select the **My outgoing server (SMTP) requires authentication** checkbox.
11. Select **Log on using** and enter the logon credentials of the administrator used to setup Workshare Protect Server.
12. Click **OK** to finish this configuration.
13. Click on **Test Account Settings** to ensure that you can receive and send emails.
14. When sending an email, you will have to select **New** and then change the **Account** you will be sending it out from, as follows:



Appendix B. ADVANCED CONFIGURATION FOR WORKSHARE PROTECT SERVER EMAIL SECURITY

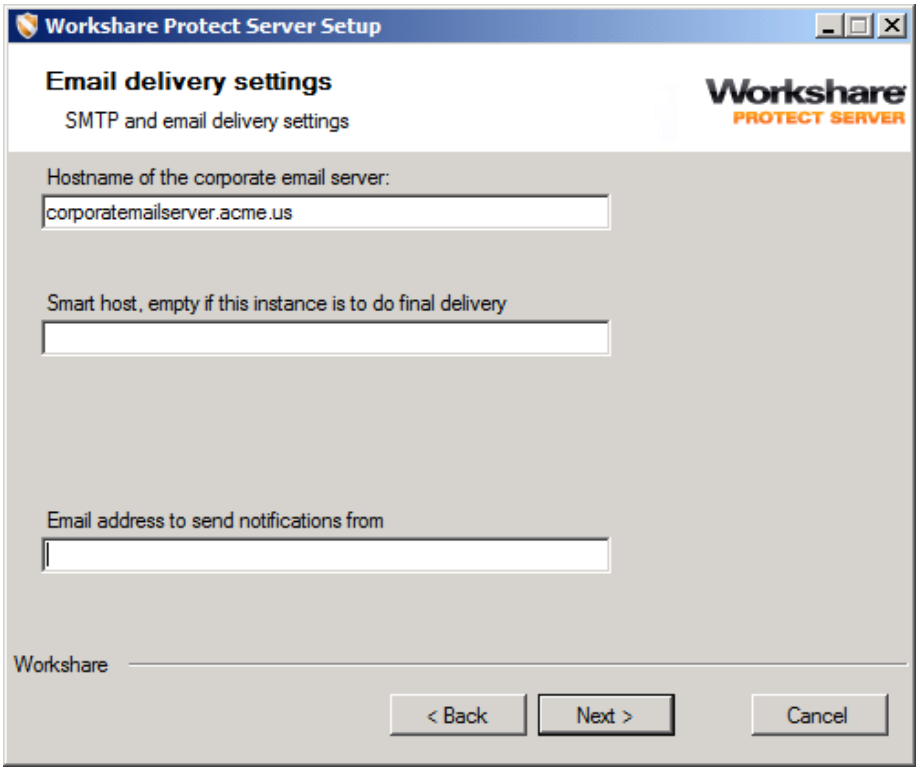
INTRODUCTION

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.

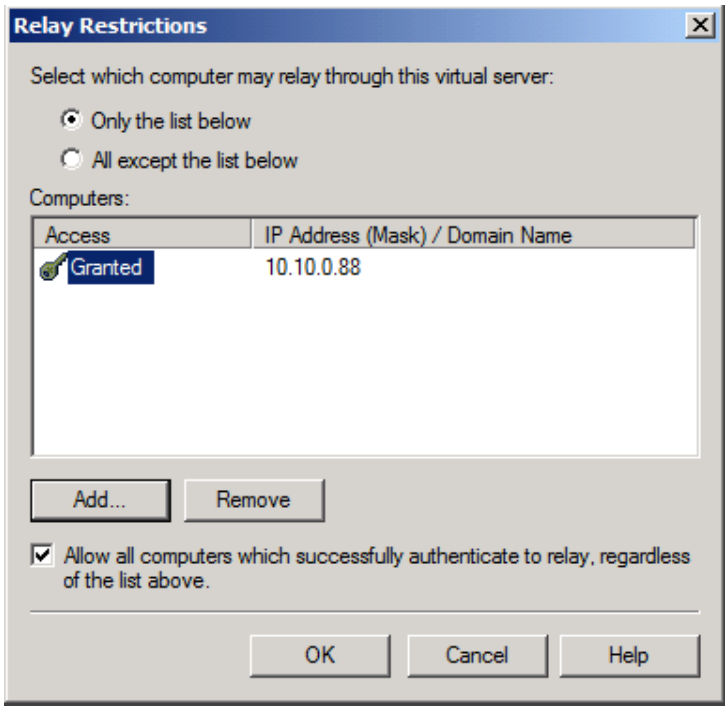
It is assumed in this appendix that Workshare Protect Server is being deployed in a corporate environment with correctly configured security and firewalls; only computers within the firewall would be able to access Workshare Protect Server. An internal user could make use of an incorrectly configured instance of Workshare 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.

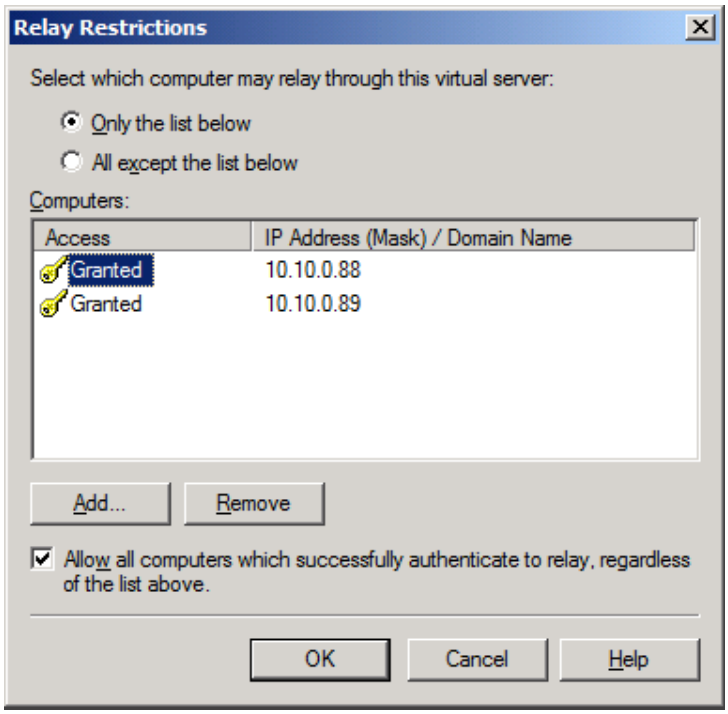


The IP address/computer name entered in the **Hostname of the corporate email server** field during installation is added to the granted list in the Microsoft SMTP service as the only computer able to relay.



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".

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

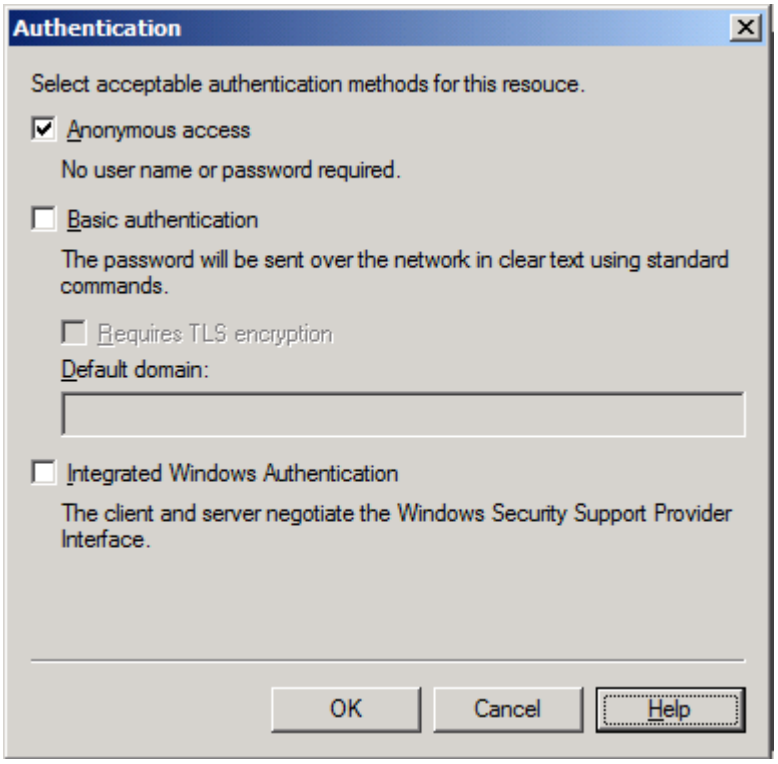


WORKSHARE PROTECT SERVER SMTP AUTHENTICATION

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

Anonymous Access

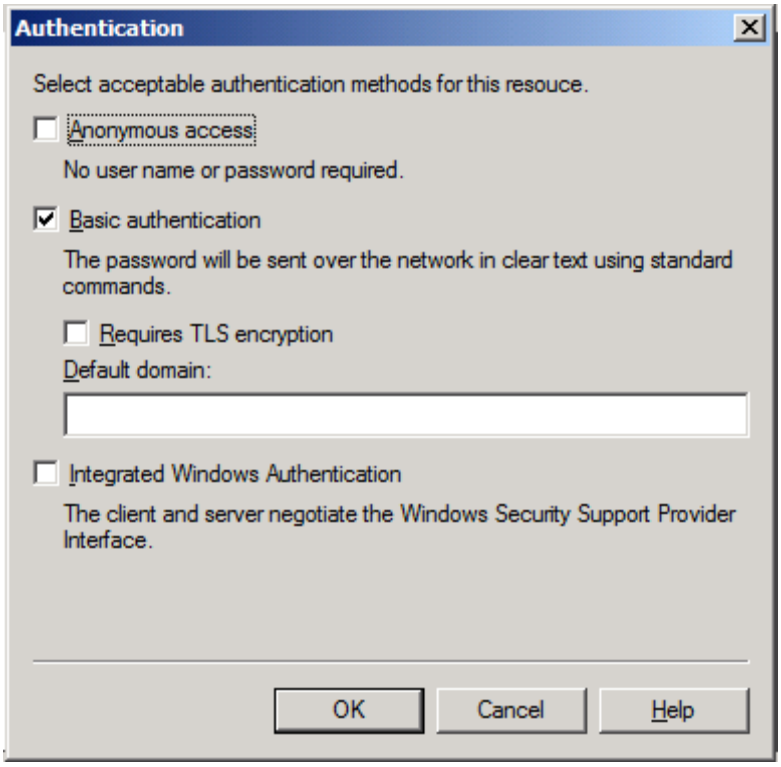
By default Workshare Protect Server is installed with **Anonymous access** – no user name or password is required to access the SMTP service.



All email servers support this configuration. With this configuration selected, security of Workshare 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 35), then the security of Workshare 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 2003/2007/2010 and IBM Lotus Domino 8 and above.

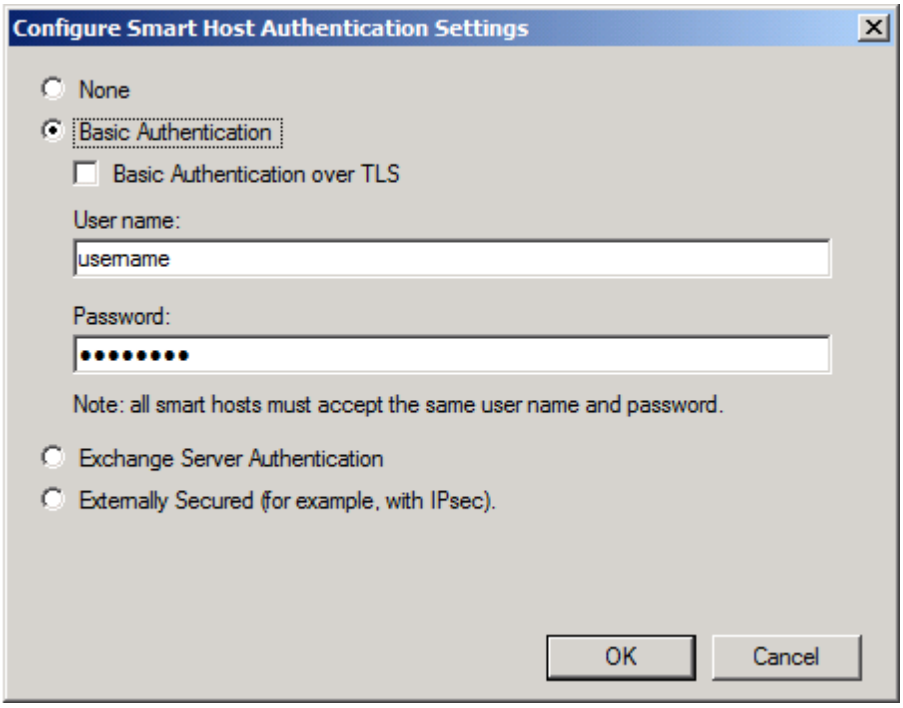
Workshare Protect Server Configuration

To enable basic authentication, in the *Authentication* dialog (page 36) 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 2007 Configuration

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

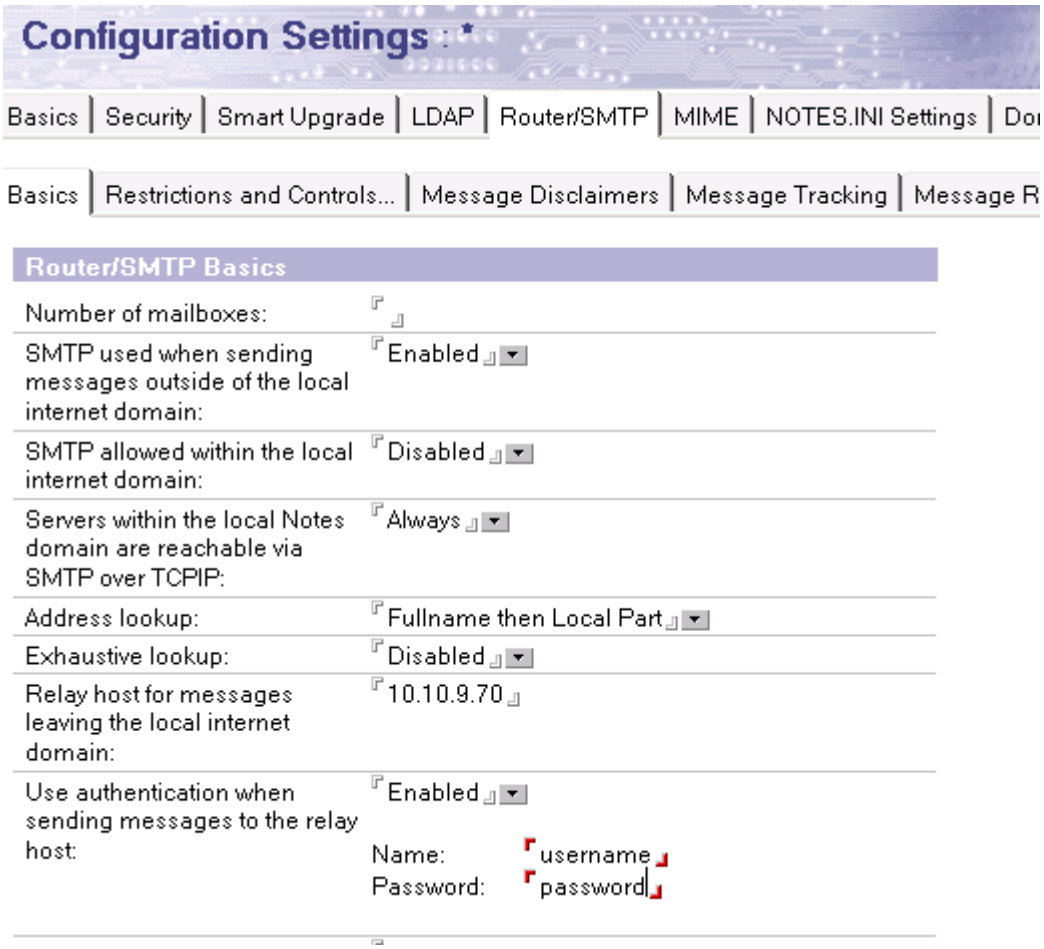
View the properties of the send connector configured to route email to Workshare Protect Server and select the **Network** tab. Select **[Change...]** to display the *Configure Smart Host Authentication Settings* dialog.



IBM Lotus Domino 8 Configuration

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

Edit the configuration settings document for all servers on your domino domain and select the **Router/SMTP** tab.



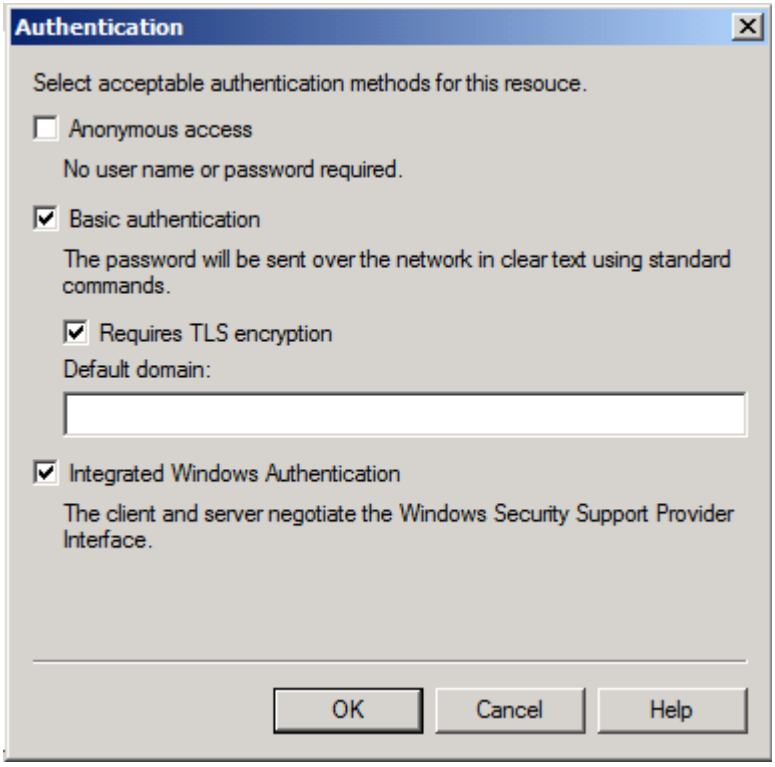
Enable the **Use authentication when sending messages to the relay host** option and enter the user name and password. Save and close the configuration document.

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 Workshare Protect Server. TLS security is supported by Microsoft Exchange 2003/2007/2010 only.

Workshare Protect Server Configuration

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

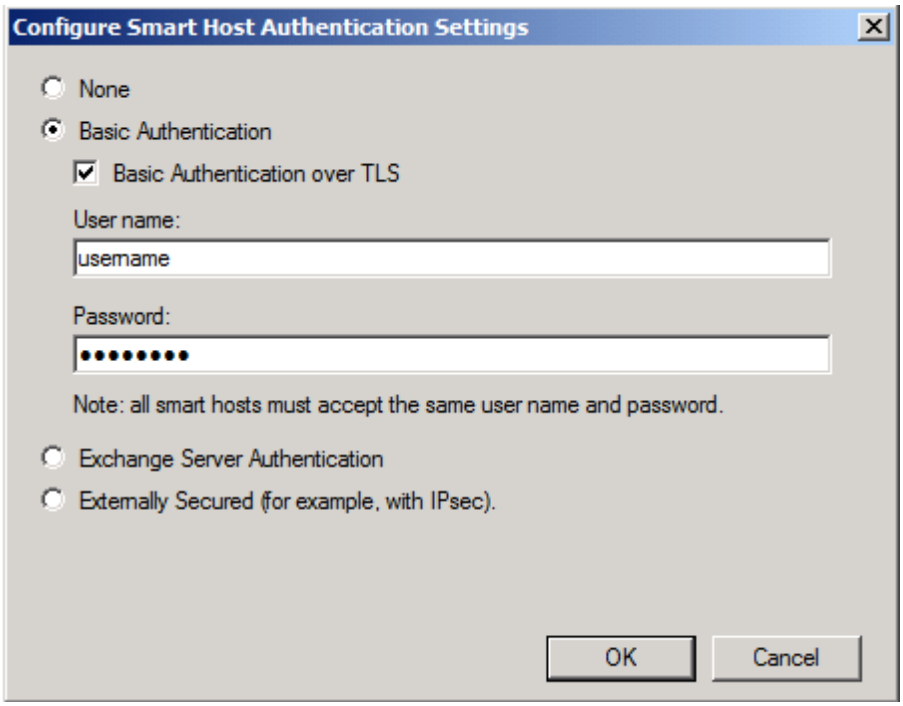


This configuration will require a X.509 certificate for Workshare Protect Server from a 3rd party certificate vendor. A self-signed certificate may be created for testing purposes using the selfssl.exe v 1.0 tool which is available in the IIS 6.0 resource kit (http://support.microsoft.com/kb/840671#11).

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.



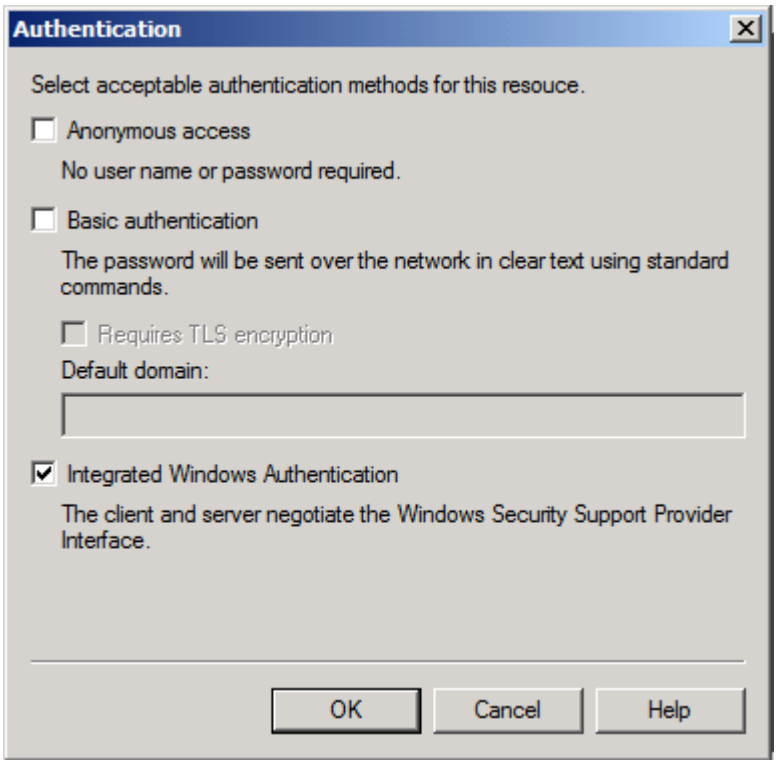
Select the **Basic Authentication over TLS** checkbox.

Integrated Windows Authentication

Microsoft SMTP Service supports Integrated Windows Authentication to control access to Workshare Protect Server. NTLM/Kerberos is used to authenticate computers sending mail to Workshare Protect Server. Please note that both computers must be in the same domain. Send connectors in Microsoft Exchange 2007 do not support Integrated Windows Authentication (http://support.microsoft.com/kb/931742/en-us).

Workshare Protect Server Configuration

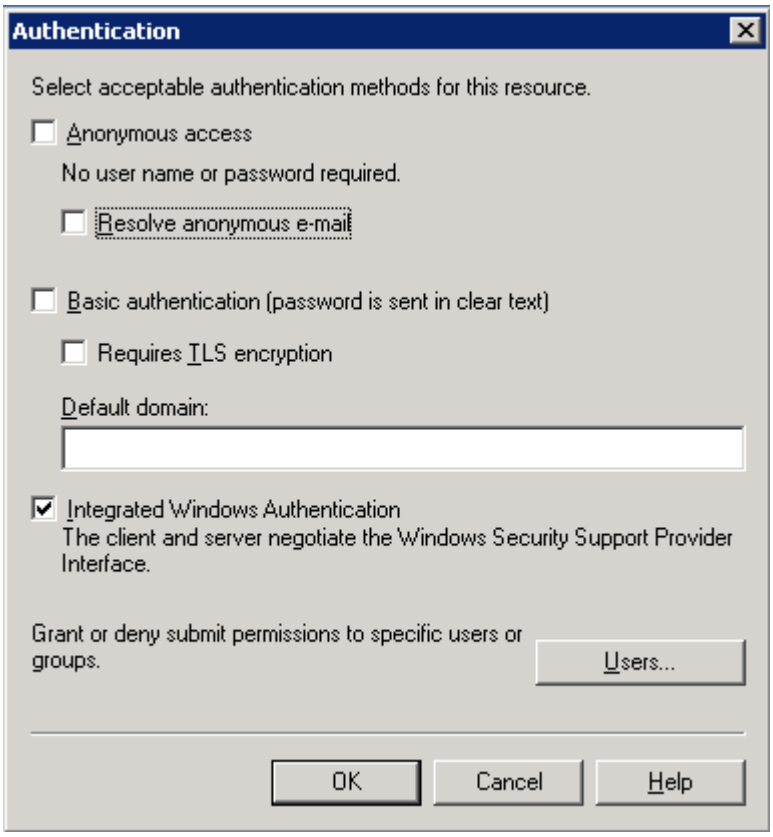
To enable Integrated Windows Authentication, in the *Authentication* dialog (page 36) deselect the **Anonymous access** checkbox and select the **Integrated Windows Authentication** checkbox.



Microsoft Exchange 2003 Configuration

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

Launch the Exchange Management console and open the **Administrative Groups** node. Select the relevant administration group for your organization and expand the **Servers** node, then the **Protocols** node and then the **SMTP** node. Right-click the SMTP node, select **Default SMTP Virtual Server** and select **Properties** from the Action menu. From the **Access** tab, select **Authentication**.



Select the **Integrated Windows Authentication** checkbox and save the changes. Changes made in this dialog will affect all email sent by the Exchange server so ensure that the existing settings are not altered.

Appendix C. TROUBLESHOOTING

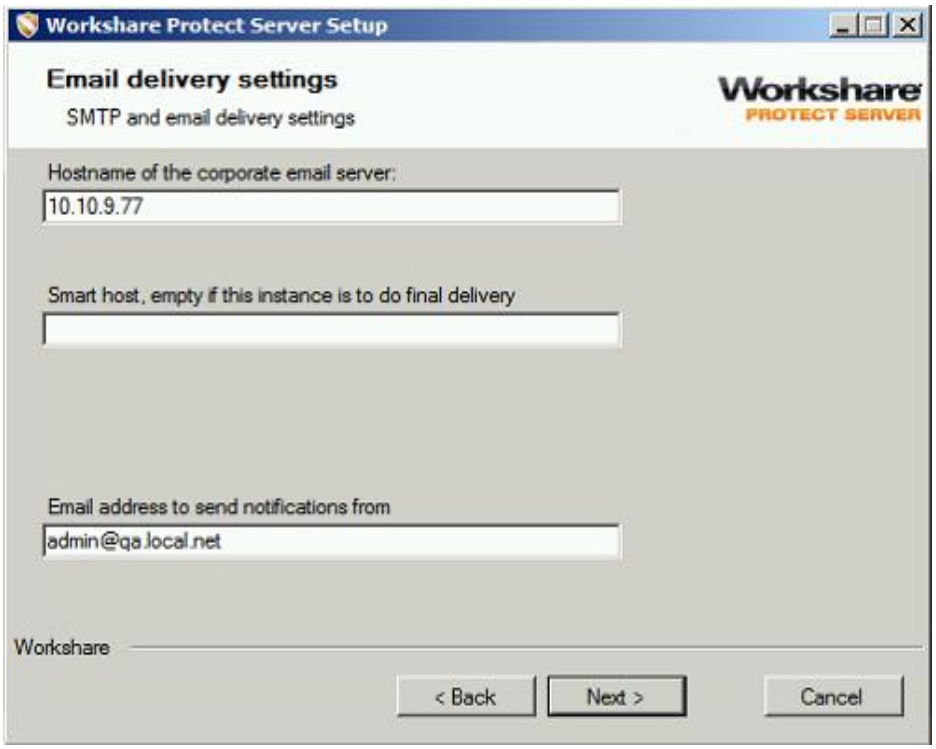
This appendix provides answers to common questions that may arise when using Workshare Protect Server.

UPDATING SETTINGS AFTER INSTALLATION

Settings and properties specified during installation may be modified after installation without running the installer again.

Email Settings

The settings specified on the Email delivery settings page can be modified using IIS Manager and the Workshare Protect Server web console.



To make changes to the Hostname of the corporate email server:

1. Start Internet Information Services (IIS) Manager, right-click **SMTP Virtual Server** and select **Properties**.
2. Select the **Access** tab and click **Relay**. The Relay Restrictions dialog is displayed showing the IP address of the configured corporate mail server.

3. Remove the listed IP address and click **Add** to specify different details for your corporate mail server.
4. Click **OK** and click **OK** in the *Relay Restrictions* dialog.

To make changes to the Smart host:

1. Start Internet Information Services (IIS) Manager, right-click **SMTP Virtual Server** and select **Properties**.
2. Select the **Delivery** tab and click **Advanced**. The *Advanced Delivery* dialog is displayed showing the IP address of the next mail gateway configured.
3. In the **Smart host** field, modify the address of the next mail gateway as required and click **OK**. If Workshare Protect Server is at the end of the chain before the email goes to the internet, then leave this field blank.

To make changes to the email address to send notifications from:

1. Log into the Workshare Protect Server web console and select **Cleaning Settings**.
2. Select **Alerts**.
3. In the **Email Address** field of **the Email communication** area, you can see the email address entered during installation to ensure clean notification emails are delivered. This email address is the "sender" of clean report emails and Clean Failed Message Sent emails. You can edit the email address and also enter a display name for this email address if required.
4. Click **Save Changes**.

***Note**: This setting is saved and stored in a web.config file.*

Database Settings

If you need to make changes to the database settings (specified on the Database configuration page), it is recommended that you delete the specified database and re-run the Workshare Protect Server installation.

OVERRIDE EMAIL ADDRESS

If you use a real email address as the override address, it may receive a lot of emails.

In usual circumstances, once Workshare Protect Server has detected the override address in an email, the attachments of the email are not cleaned and the override address is removed. However, when emails include a digital signature, Workshare Protect Server does not remove the override address and therefore the actual email will also be delivered to the override address.

***Note**: A user can use the override address to bypass cleaning on Workshare Protect Server. For information on how to configure a cleaning override address, refer to the Workshare Protect Server Administrator Guide.*

In such circumstances, you may want to drop all the emails that the override address receives without even viewing them. To do so, you need to send it to a “black hole”. This uses a feature of Microsoft Exchange where any email that is sent to a distribution group is no longer stored on the server once it has been delivered to the group, even if the group has no members.

To set up a black hole:

1. Create a mail-enabled distribution group called "black hole" but do not add any members to it.
2. Right-click the new distribution group and select **Properties**.
3. In the **E-Mail Addresses** tab, add the email address that you want to "black hole" (for example, the override address).

Any email sent to that address will simply disappear - never to be seen again.

MANUAL CONFIGURATION OF SECURITY

This section describes how to manually configure or change individual Workshare Protect Server Security Role settings.

Users with System Administrator (sysadmin) Server Role

If a user either has sysadmin privilege explicitly set or inherits sysadmin privilege from a group login, then this user has to be explicitly mapped to one of the following database roles:

- AdministratorRole
- BusinessRole
- UserRole

This is due to a design decision by Microsoft and the IS_ROLEMEMBER function. The user will be internally mapped as the dbo (database owner) to all databases. See this feedback note: http://connect.microsoft.com/SQLServer/feedback/details/345809/is-member-function-does-not-work-as-expected. If you try to map the dbo login to the above roles then you will receive the error “cannot use the special principal 'dbo'“. The workaround is to explicitly map the individual users to the roles required.

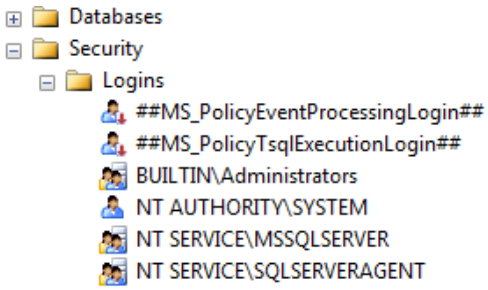
Processor Role

This role controls the writing of email results to the database and the retrieval of profiles for the Workshare Protect Server processing engine installed locally to the Windows services called Workshare Audit Service and Workshare Profile Service.

Adding a New Login to the Database

To add a new login to the database:

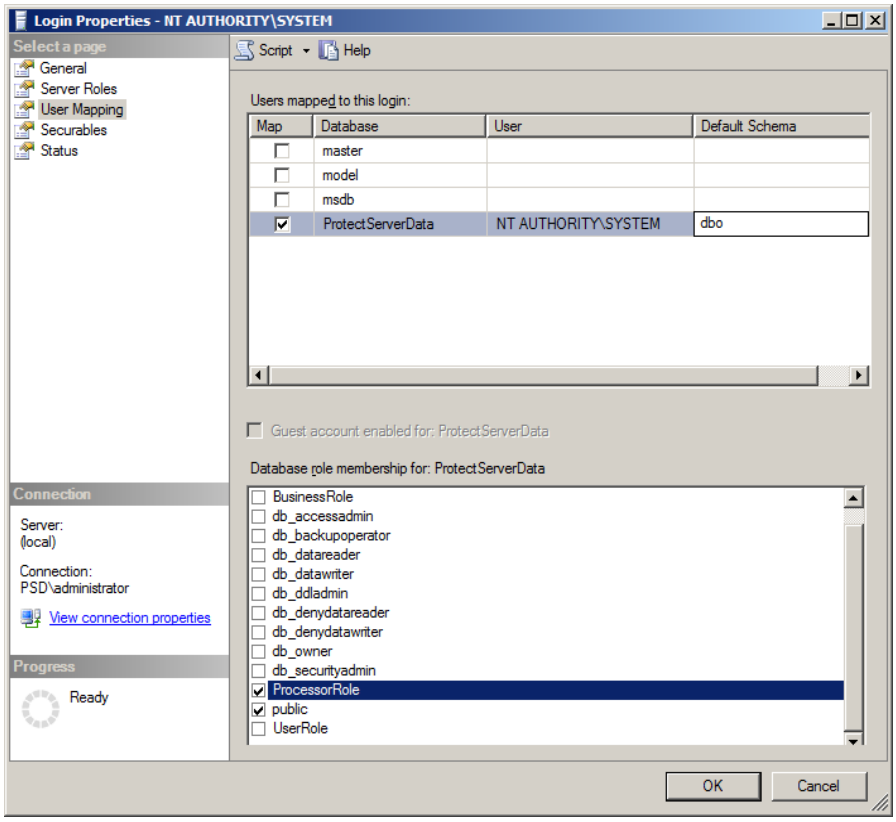
1. Launch Microsoft SQL Server Management Studio (SSMS) and login with sysadmin server role.
2. Expand the **Security/Logins** nodes.



3. Depending if you are going to be using the Local System account to run the Windows services or a dedicated domain account will make a difference to the login added to the database server.

Local System Account and Local Database

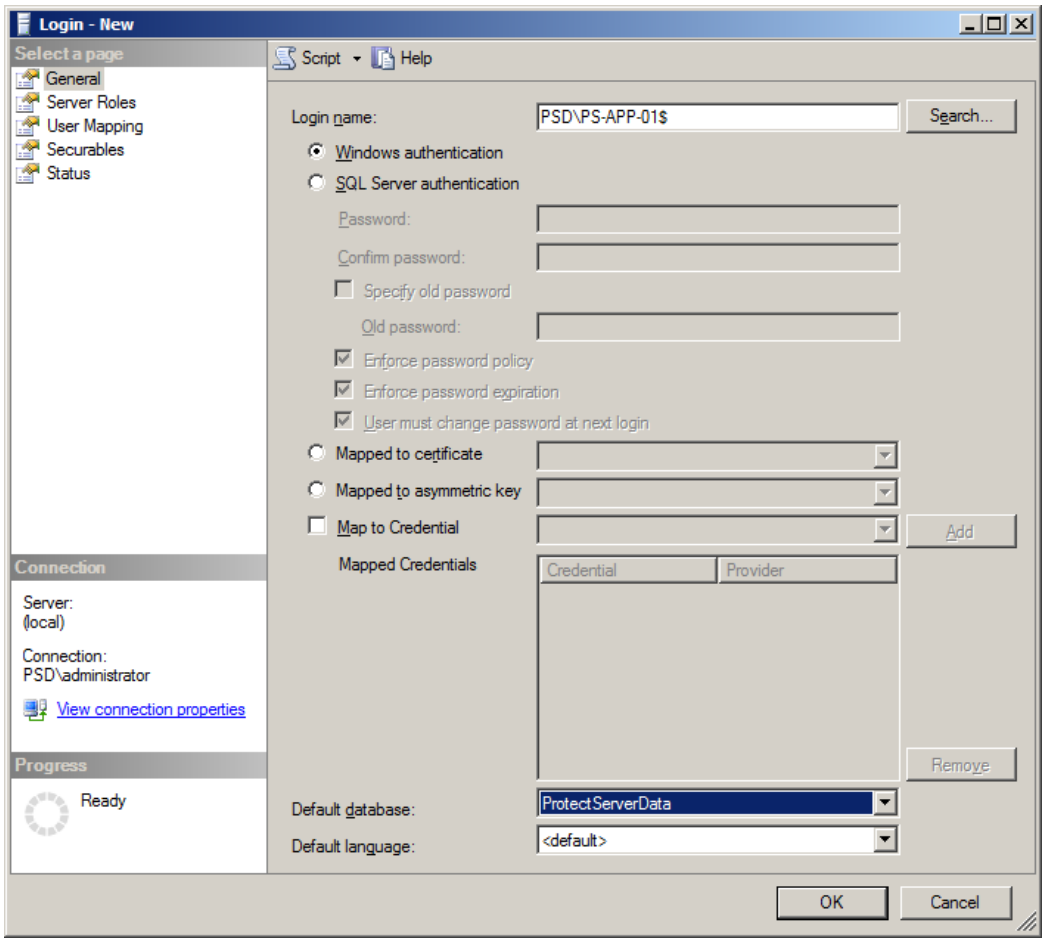
If Local System account and the database is local, then you may already have the account added (NT AUTHORITY\SYSTEM). In which case just right-click this user and select **User Mapping** and select the Workshare Protect Server Database. Assign the user the database role **ProcessorRole** and set the default Schema to **dbo**.



Local System Account and Remote Database

If Local System account and the database is remote, then you will probably need to add this account to the database. **This is not recommended as it relies on kerberos security and Service Principal Names (SPN) being setup correctly to work.**

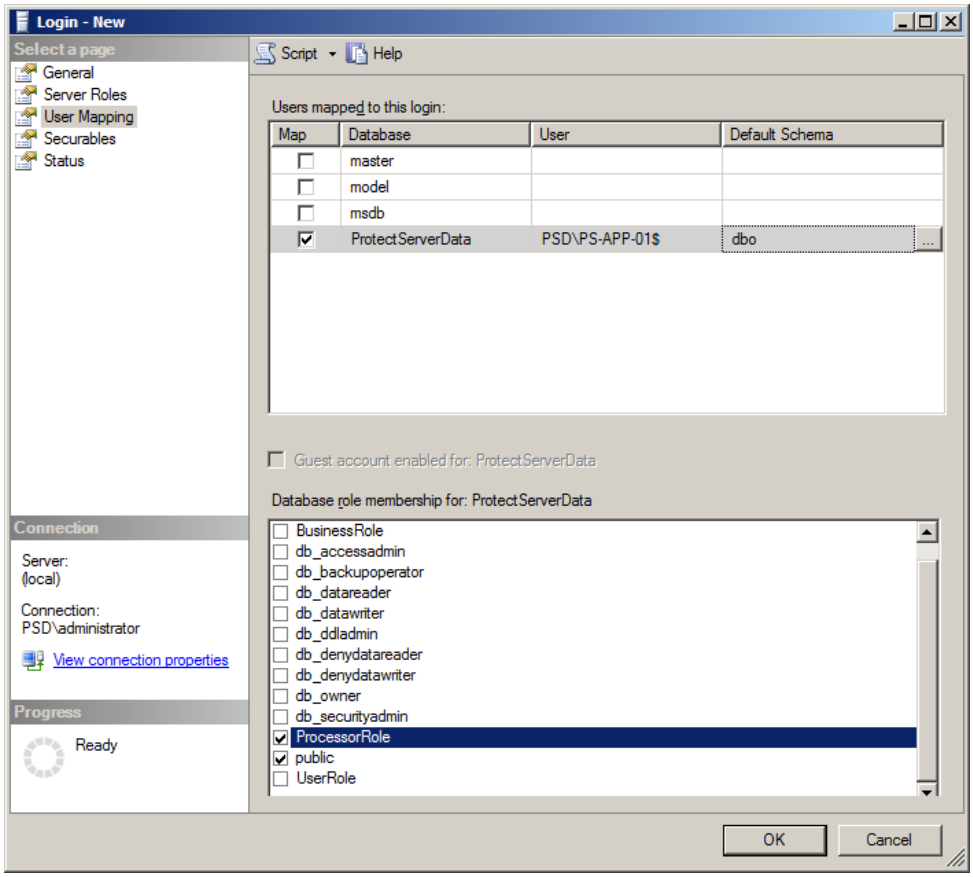
1. Right click the **Login** node and select **New Login**.



2. For the **Login name** you have to manually type in the hidden machine account name. This name is made of the domain name that the machine is part of and the machine name with a $ symbol at the end. For example, for a machine called PS-APP-01 which is registered in a domain called PSD, the login name will be PSD\PS-APP-01$.

3. Set the **Default database** to the Workshare Protect Server Database.

4. Click **User Mapping**.



5. Select the Workshare Protect Server Database.
6. Assign the user the database role **ProcessorRole** and set the default Schema to **dbo**.

Domain Account

If domain account then follow the steps in the *Local System Account and Remote Database* section and replace the machine domain account with the user domain account.

Access Control Lists

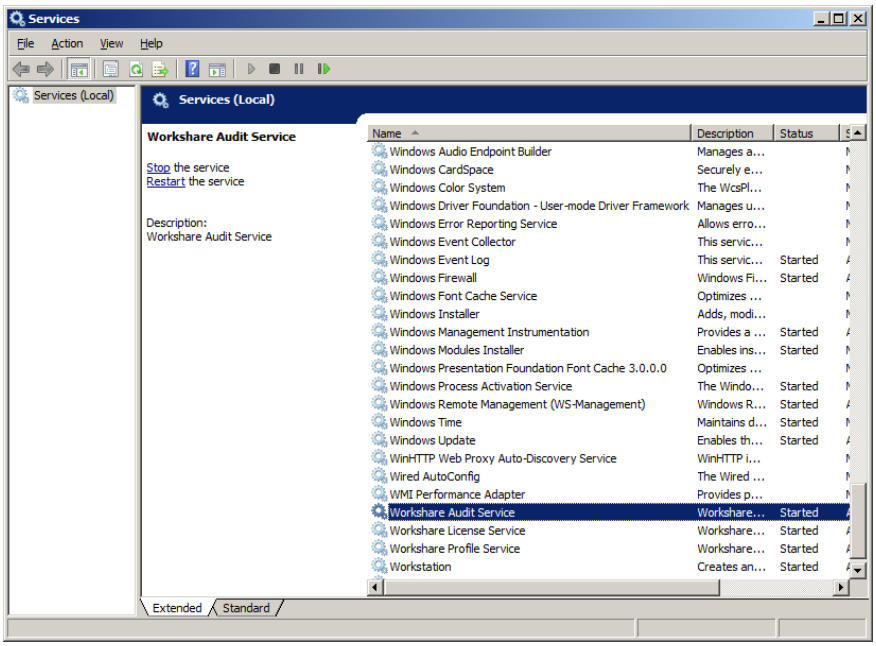
Once the account is set up on the database then the Access Control Lists for specific folders and files need to be modified. The following table highlights the changes. If the File cell is blank then give the permission to the folder.

Location	File	Permissions Required
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Db.config	Read
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Logging.config	Full Control
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Metadata.config	Read
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Unity.config	Read
C:\ProgramData\Workshare\Protect Server\2.2.0.0\InstallProfiles	Profiles.sdf	Full Control
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Results		Full Control
C:\Program Files\Workshare\Protect Server\Smtp Server		Full Control

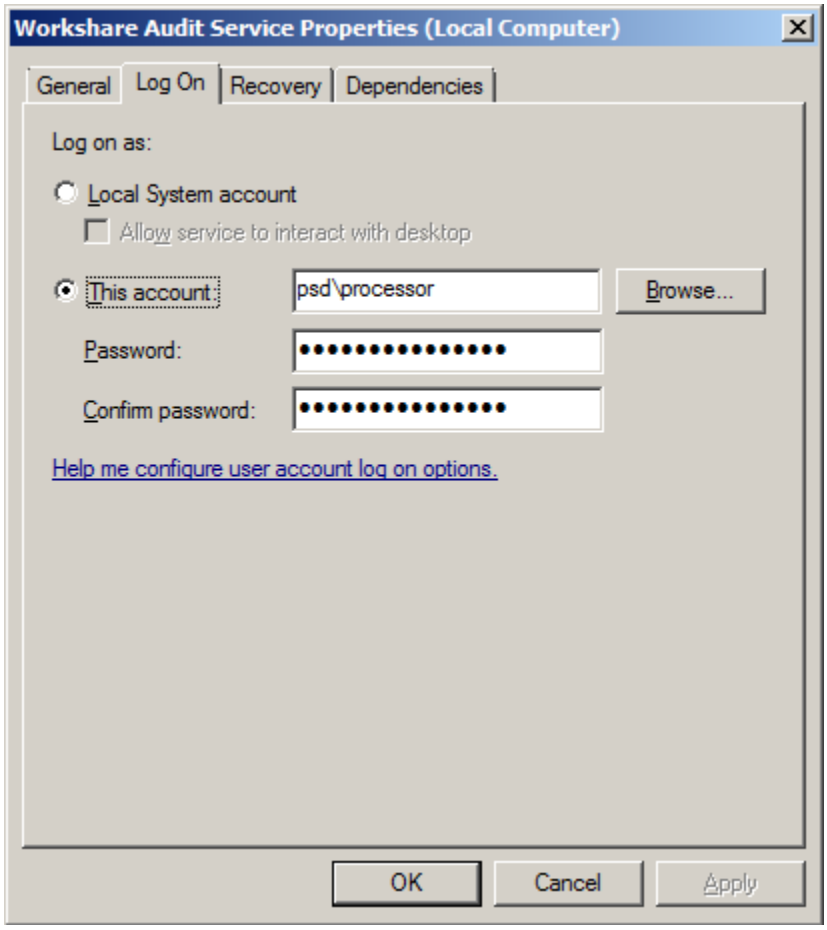
Workshare Services Changes

Once the Access Control Lists are setup on the database you will change login details for the services called Workshare Audit Service and Workshare Profile Service.

1. Launch Services.msc module.



2. Right-click Workshare Audit Service, select **Properties** and select the **Log On** tab.



3. If the user is the Local System then select the **Local System account** radio button. If the user is a domain account then select the **This account** radio button and fill in the details of the account. If the domain account has never been used as a service account then you will receive a dialog stating that this account has been given 'Log On As Service' privilege when you click **OK**.
4. These settings do not take effect until the service is restarted. Click on the restart button on the top toolbar  .
5. Repeat steps 1 to 5 for Workshare Profile Service.

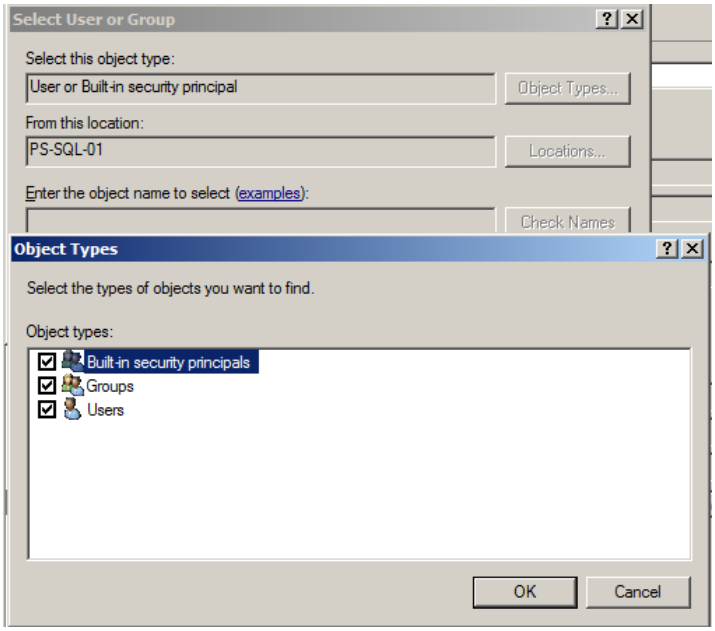
Administrator Role

This role controls the configuration of settings and profiles for Workshare Protect Server.

Adding a New Login to the Database

To add a new login to the database:

1. Launch Microsoft SQL Server Management Studio (SSMS) and login with sysadmin server role.
2. Expand the **Security/Logins** nodes. This role can only be a security group.
3. If Local Security account and the database is local, then you can add domain users to this security group if required. To add the local security group to the database:
   - Right-click the **Login** node and select **New Login**.
   - For the **Login name** you either browse to the local computer and select the account (when browsing ensure you select **Groups** in the *Object Types* dialog) or you can enter the security group name and machine name. For example, if there is a local security group called PSAdmins on machine PS-APP-01, then the login name will be PS-APP-01\PSAdmins.



- Set the default database to the Workshare Protect Server Database.
- Click **User Mapping** and select the Workshare Protect Server Database.
- Assign the user the database role **AdministratorRole** and set the default Schema to **dbo**.

***Note**: If domain security account then following the above steps and replace the local security group account with the domain security group account.*

Access Control Lists

Once the security group is set up on the database then the Access Control Lists for specific folders and files need to be modified. The following table highlights the changes. If the File cell is blank then give the permission to the folder.

Location	File	Permissions Required
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Db.config	Full Control
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Logging.config	Full Control
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Metadata.config	Full Control
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Unity.config	Full Control
<InstalledLocation>Workshare\Protect Server\Dashboard\App_Data\Charts		Full Control

Modifications to Web.config

The web.config can be found in <installed location>\Workshare\Protect Server\Dashboard. To edit this file, launch notepad.exe (or another text editor of your choice) as administrator. A Standard user, even with administrator privileges, cannot edit this file directly. This is a feature of the UAC.

Authorization Element

This element is located in Configuration\System.web\ element. There is an allow element contained inside the Authorization element. The roles attribute is a comma separated list of groups allowed to access the web site.

```
<authorization>
<allow roles="psadmins,psusers" />
<deny users="?" />
</authorization>
```

Replace the existing Administrator Role with new Role name. Do not add the domain or machine name to the role.

applicationSettings Element

This element is located in the Configuration element near the bottom of the file. There are three setting elements contained inside Workshare.ProtectServer.WebApplication.Properties.Settings element. You will need to modify the AdministratorRole element and update the value element.

```
<setting name="AdministratorRole" serializeAs="String">
<value>psd\psadmins</value>
</setting>
```

Make sure the domain or machine name is part of the value.

Business Role

This role allows the viewing of all emails results and profiles in Workshare Protect Server.

Adding a New Login to the Database

To add a new login to the database:

1. Launch Microsoft SQL Server Management Studio (SSMS) and login with sysadmin server role.
2. Expand the **Security/Logins** nodes. This role can only be a security group.
3. If Local Security account and the database is local, then you can add domain users to this security group if required. To add the local security group to the database:
   - Right-click the **Login** node and select **New Login**.
   - For the **Login name** you either browse to the local computer and select the account (when browsing ensure you select **Groups** in the *Object Types* dialog) or you can enter the security group name and machine name. For example, if there is a local security group called PSUsers on machine PS-APP-01, then the login name will be PS-APP-01\PSUsers.
   - Set the default database to the Workshare Protect Server Database.
   - Click **User Mapping** and select the Workshare Protect Server Database.
   - Assign the user the database role **BusinessRole** and set the default Schema to **dbo**.

***Note**: If domain security account then following the above steps and replace the local security group account with the domain security group account.*

Access Control Lists

Once the security group is set up on the database then the Access Control Lists for specific folders and files need to be modified. The following table highlights the changes. If the File cell is blank then give the permission to the folder.

Location	File	Permissions Required
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Db.config	Read

C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Logging.config	Full Control
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Metadata.config	Read
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Unity.config	Read
<InstalledLocation>Workshare\Protect Server\Dashboard\ App_Data\Charts		Full Control

Modifications to Web.config

The web.config can be found in <installedlocation>\Workshare\Protect Server\Dashboard. To edit this file, launch notepad.exe (or another text editor of your choice) as administrator. A Standard user, even with administrator privileges, cannot edit this file directly. This is a feature of the UAC.

Authorization Element

This element is located in Configuration\System.web\ element. There is an allow element contained inside the Authorization element. The roles attribute is a comma separated list of groups allowed to access the web site.

```
<authorization>
<allow roles="psadmins,psusers" />
<deny users="?" />
</authorization>
```

Replace the existing Business Role with new Role name. Do not add the domain or machine name to the role.

applicationSettings Element

This element is located in Configuration element near the botton of the file. There are three setting elements contained inside Workshare.ProtectServer.WebApplication.Properties.Settings element. You will need to modify the BusinessRole element and update the value element.

```
<setting name="BusinessRole" serializeAs="String">
<value>psd\psusers</value>
</setting>
```

Make sure the domain or machine name is part of the value.

User Role

This role allows the viewing of only your own email results and profiles in Workshare Protect Server.

Adding a New Login to the Database

To add a new login to the database:

1. Launch Microsoft SQL Server Management Studio (SSMS) and login with sysadmin server role.
2. Expand the **Security**/**Logins** nodes. This role can only be a security group.
3. If Local Security account and the database is local, then you can add domain users to this security group if required. To add the local security group to the database:
   - Right-click the **Login** node and select **New Login**.
   - For the **Login name** you either browse to the local computer and select the account (when browsing ensure you select **Groups** in the *Object Types* dialog) or you can enter the security group name and machine name. For example, if there is a local security group called Users on machine PS-APP-01, then the login name will be PS-APP-01\Users.
   - Set the default database to the Workshare Protect Server Database.
   - Click **User Mapping** and select the Workshare Protect Server Database.
   - Assign the user the database role **UserRole** and set the default Schema to **dbo**.

***Note**: If domain security account then following the above steps and replace the local security group account with the domain security group account.*

Access Control Lists

Once the security group is set up on the database then the Access Control Lists for specific folders and files need to be modified. The following table highlights the changes. If the File cell is blank then give the permission to the folder.

Location	File	Permissions Required
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Db.config	Read
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Logging.config	Read
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Metadata.config	Read
C:\ProgramData\Workshare\Protect Server\2.2.0.0\Configuration	Unity.config	Read
<InstalledLocation>Workshare\Protect Server\Dashboard\ App_Data\Charts		Full Control

Modifications to Web.config

The web.config can be found in <installedlocation>\Workshare\Protect Server\Dashboard. To edit this file, launch notepad.exe (or another text editor of your choice) as administrator. A Standard user, even with administrator privileges, cannot edit this file directly. This is a feature of the UAC.

You do not need to update the Authorization element as all domain users are authenticated against this web by default and allowed in.

applicationSettings Element

This element is located in Configuration element near the bottom of the file. There are three setting elements contained inside Workshare.ProtectServer.WebApplication.Properties.Settings element. You will need to modify the UserRoleName element and update the value element.

```
<setting name=" UserRoleName" serializeAs="String">
<value>psd\domain users</value>
</setting>
```

Make sure the domain or machine name is part of the value.