

Workshare Protect Server on Microsoft Azure Admin Guide

Table of Contents

Introducing Protect Server on Azure	3
Spam prevention software	3
Deployment Overview	4
Endpoints	5
Supported SQL servers	5
Deployment steps.....	5
Azure Configuration	6
Create a resource group	6
Create a network security group	6
Add new Protect Server machine.....	8
Add new remote SQL server.....	10
Protect Server Configuration.....	11
Configure Windows Server	12
Configure Workshare Protect Server	18
Step 1: Navigate to the Workshare Protect Server web console.....	18
Step 2: Configure database.....	19
Step 3: Create Protect Server database on remote SQL server	20
Step 4: Use existing Protect Server database on remote SQL server.....	22
Step 5: License Protect Server	23
Exchange Online Configuration	25
Set up the accepted domain	25
Create an Outbound Connector	26
Create an Inbound Connector.....	27
Create On Premise Relay Machine.....	28
Network Topology Recommendations	36
Protect Server fault tolerance	36
Protect Server high availability.....	36
Corresponding, but independent settings	36
DNS round robin for load balancing across outbound smart hosts	37
DNS MX priority for outbound smart host failover	37
Protect Server disaster recovery.....	37

Introducing Protect Server on Azure

Workshare Protect Server provides server-side metadata cleaning and document processing. A web application - the Workshare Protect Server web console – is provided to enable administrators to configure which metadata to remove and to enable them to view a history of what was previously removed.

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. It processes all emails passing through the corporate mail server (which is all emails), including those that originate from webmail and mobile mail clients. By locating this processing effort on the server, email send performance on the originating device is not impacted, and users are not affected.

When Protect Server is installed on Microsoft Azure - rather than on your premises – there is no user integration with Active Directory. This difference means:

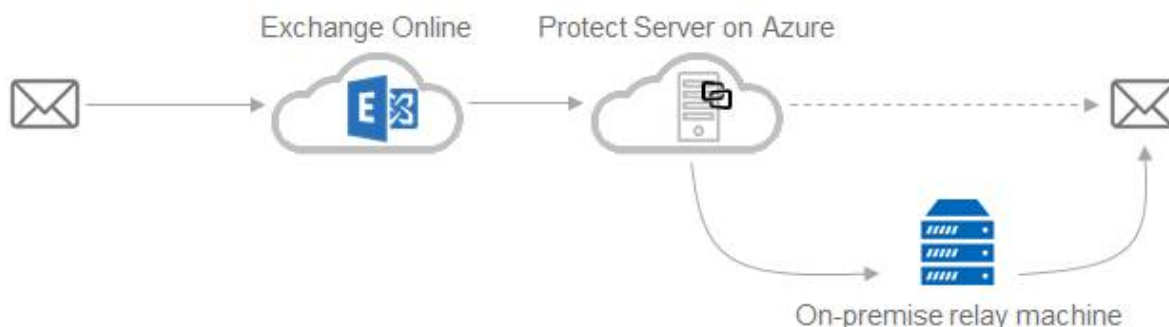
- Single web-based user logon to Workshare Protect Server web console.
- No group-based profiles to enable metadata processing per AD group.

Additionally, when Protect Server is installed on Azure, it doesn't support the processing of password-protected attachments.

Note: *Protect Server on Azure has access control functionality enabled by default.*

Spam prevention software

Maintaining Protect Server machines on Azure presents a challenge for mail delivery. Emails originating from the Azure infrastructure (or any public cloud service) are often rejected due to spam prevention software at the server level. It may be necessary to relay email via an on-premise mail server as follows:



- **For outbound email:**

Exchange Online → (TLS) → Protect Azure → (TLS) → On-premise relay → Final delivery

- **For clean summaries:**

Exchange Online → (TLS) → Protect Azure → (TLS) → On-premise relay → (TLS) → Exchange Online

Deployment Overview

This section describes the steps required to deploy a new instance of Workshare Protect Server from the Azure Marketplace. You should adapt these instructions to fit your own requirements.

The instructions in this guide will produce a machine with the following settings:

- **DNS name:** protectserversample.cloudapp.net
- **Local Administrator user name:** ProtectAdmin
- **Local Administrator password:** DontUseThisPassword
- **Machine size:** D2-V2 Standard
 - 2 vCPUs
 - 7GB RAM
 - 4 data disks
 - 4x500 max IOPS
 - 100GB local SSD
 - Load balancing
- **Machine location:** Central US/North Europe

In order to set up the mail flow correctly, you need to record the following parameters:

ID	Record	Value
A	External Protect Azure machine IP address	
B	External on-premise relay IP address	

Endpoints

These are the ports which Workshare Protect Server requires for operation and configuration.

Endpoint	Protocol	Public Port
SMTP	TCP	25
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389

Supported SQL servers

Protect Server works with Microsoft SQL Server 2012, 2014 or 2016 with Full Text Search.

Note: *The Azure SQL service is not supported.*

Deployment steps

The steps required for the deployment are as follows:

- Azure configuration
 - Create resource group
 - Create network security group
 - Add new Protect Server machine
 - Add new remote SQL server (optional)
- Protect Server configuration
 - Configure the newly created Protect Server machine
- Exchange Online configuration
 - Connect your Exchange Online instance to Protect Server

Azure Configuration

Create a resource group

This is an optional step, but it is recommended in order to keep all resources related to Protect Server together. This helps locate and modify these resources on the Azure management portal.

In the unlikely event that the resources built for the Protect Server installation need to be removed from the Azure portal, deleting the resource group ensures that there are no floating resources that will remain in the Azure management portal.

Once the resource group is created, note the name down as this will be used in the next three steps.

To create a resource group:

1. Click **Resource groups** in the Hub menu on the left. If this option is not present in the menu, you'll find it by clicking **More Services >** at the bottom of the Hub menu.
2. Click **+ Add** in the top bar under the title **Resource groups**.
3. Name your resource group and select your subscription as appropriate.
4. Select the resource group location. You are recommended to pick a geography as close to your physical office as possible, to reduce network lag time.
5. Click **Create**.

All the resources that you create in the next three steps need to be associated with this resource group.


Create a network security group

In this step, you will create an Azure network security group called "Office365NSG". This will be shared amongst all Protect Server machines. If you use a different name for the network security group, then note the new name as this will be used in the next two steps.

You must ensure the following ports are enabled in the Azure network security group:

Port	Service	Direction	IP Range
25	SMTP	Inbound	To ensure a secure Protect Server installation, the inbound addresses should be limited to those used by Exchange Online. See https://technet.microsoft.com/en-gb/library/dn163583(v=exchg.150).aspx If you're intending to route email from other on-premise installations to your Protect Server on Azure, add the IP addresses of those servers too.
80	HTTP	Inbound	This is for access to Protect Server's web console.
443	HTTPS	Inbound	This is for access to Protect Server's web console.
3389 (default)	RDP	Inbound	This is for access to the remote desktop on both Protect Server and SQL Server (if installed).

To create a network security group:

1. Click **More services >** at the bottom of the Hub menu on the left.
2. Scroll down to the **Networking** sub-section, and click **Network security groups**.
3. Click **+ Add** in the top bar under the title **Network security groups**.
4. Name your network security group ("Office365NSG" preferred) and select your subscription as appropriate.
5. Select **Use existing** and select the resource group created in the previous step.
6. Assign the location to be the same as the resource group.
7. Click **Create**.
8. Click your newly created network security group from the list shown. (Click  **Refresh** in the top bar under the title **Network security groups** if you don't see your group already.)

9. Add inbound security rules to match the list above.
 - Select **Inbound security rules** (under **Settings**) in the left menu.
 - Click **+ Add**.

The screenshot shows the 'Add inbound security rule' dialog box in the Azure portal. The dialog is titled 'Add inbound security rule' and 'H5Office365NSG'. It has a 'Basic' tab. The fields are as follows:

- Source:** Any
- Source port range:** *
- Destination:** Any
- Destination port range:** 8080
- Protocol:** Any, TCP, UDP
- Action:** Allow, Deny
- Priority:** 100
- Name:** Port_null
- Description:** (empty text area)

An 'OK' button is located at the bottom of the dialog.

Add new Protect Server machine

In this step you create your Protect Server machine.

To set up a Workshare Protect Server machine:

1. Log on to the Azure portal (<https://portal.azure.com>).
2. Click **+ NEW** in the Hub menu.
3. Click **Compute**.
4. Search for Workshare Protect Server.

5. Click **Workshare Protect Server (BYOL)**.
6. Click **Create** to get started.
7. In the **Create virtual machine** blade, configure the following:
 - **Basics**
 - **Name:** The name you'd like to assign to the Protect Server
 - Select the VM disk type to be **HDD**
 - **User Name:** The Admin user name for the machine
 - **Password/Confirm Password:** The Admin password for the user name above.
 - Select your subscription
 - Choose the resource group created earlier
 - Choose the location that the resource group belongs to.
 - **Size**

A D2_V2 Standard machine is recommended (at the minimum). A D2_V2 Standard machine has the following configuration set:

 - 2 vCPUs
 - 7GB of RAM
 - 4 data disks
 - 4x500 max IOPS
 - 100GB local SSD
 - Load balancing enabled
 - **Settings**
 - Select **None** for Availability Set
 - Use managed disks
 - Create a new virtual private network. Note the name of this network for when the SQL server is created.
 - Set the Public IP address to be static
 - Select the network security group created in the earlier step
 - Don't select any extensions
 - Disable Auto-shutdown
 - Enable Boot diagnostics
 - Disable Guest OS diagnostics
 - **Purchase**

Confirm your purchase with the **Purchase** button.

Azure will now provision your VM and will indicate it is complete in **Notifications** in the Hub menu.

Add new remote SQL server

You have the option to use the on-board SQL Express installation on Protect Server. This helps reduce the amount of configuration required, and saves additional servers from being built and billed to you.

However, in the case of disaster recovery friendly installations, it is recommended that you have more than one Protect Server in your mail flow. For this scenario, you would need to set up a remote SQL server.

To set up a remote SQL server:

1. Log on to the Azure portal (<https://portal.azure.com>).
2. Click **+ NEW** in the Hub menu.
3. Click **Compute**
4. Search for **SQL Server 2016 SP1 Standard on Windows Server 2016**.
5. Ensure that **Resource Manager** is selected as the deployment model, and then click **Create**.
6. In the **Create virtual machine** blade, configure the following:
 - **Basics**
 - **Name:** <Name you'd like to assign to the Protect Server>
 - Select the VM disk type to be **HDD**
 - **User Name:** <Admin user name for the machine>
 - **Password / Confirm Password:** <Admin password for the username above>
 - Select your subscription
 - Choose the resource group created earlier
 - Choose the location that the resource group belongs to
 - **Size**

We recommend a D2_V2 Standard at the minimum. A D2_V2 Standard machine has the following configuration set:

 - 2 vCPUs
 - 7 GB of RAM
 - 4 data disks
 - 4x 500 Max IOPS
 - 100 GB Local SSD
 - Load Balancing enabled

- **Settings**
 - Select **None** for Availability Set
 - Select HDD as the Disk type
 - Use managed disks
 - Select the virtual private network created during the Protect Server creation stage.
 - Leave the Public IP Address as is
 - Select the network security group created in the earlier step
 - Don't select any extensions
 - Disable Auto-shutdown
 - Enable Boot diagnostics
 - Disable Guest OS diagnostics
- **SQL Server settings**
 - Leave SQL connectivity as Private (within Virtual Network)
 - Enable SQL Authentication. Choose a username and password to use as the SQL administrator password
 - Leave Storage configuration as Not available
 - Leave Automated patching to the default value
 - Configure Automated backup to match your firm's policy
 - Leave Azure Key Vault integration as Disabled
 - Disable R Services
- **Purchase**

Confirm your purchase with the **Purchase** button.

Protect Server Configuration

This section describes how to configure Workshare Protect Server. There are two basic steps:

- Configure Windows Server
- Configure Workshare Protect Server

For information on setting the email size limit, setting up synchronization and email message logging, refer to the relevant section in the Workshare Protect Server Administrator Guide

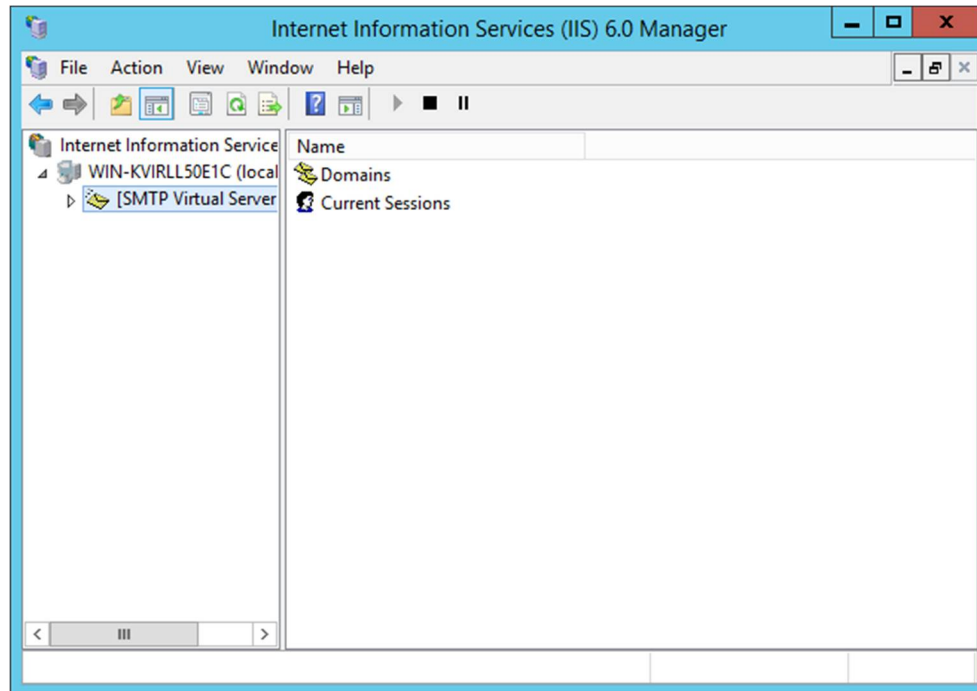
http://workshare.force.com/knowledgebase/articles/Help_Articles/Workshare-Protect-Server-3-8-Admin-Guide

Configure Windows Server

In this step, you prepare the SMTP server to receive emails from the Exchange Online server.

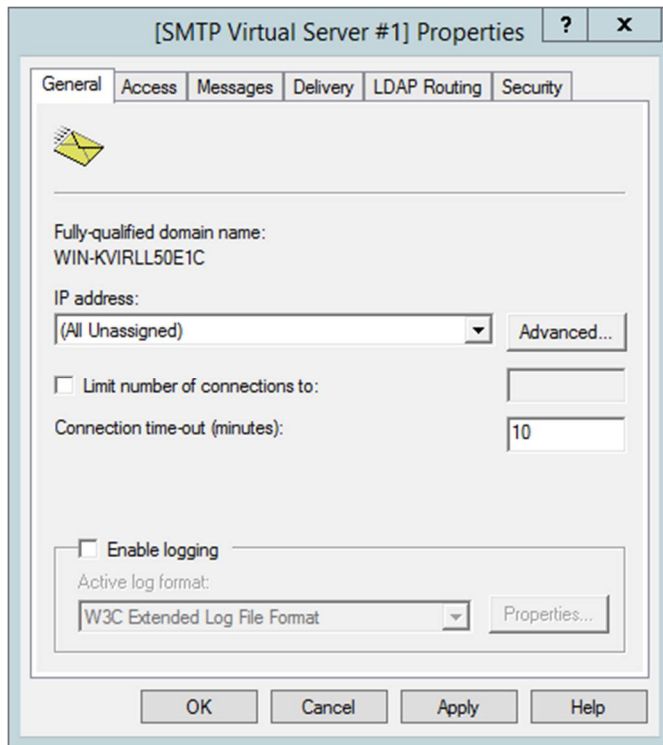
To configure Windows Server:

1. In the Start menu, type **inetmgr6**.
2. Select and run Internet Information Services (IIS) 6.0 Manager.



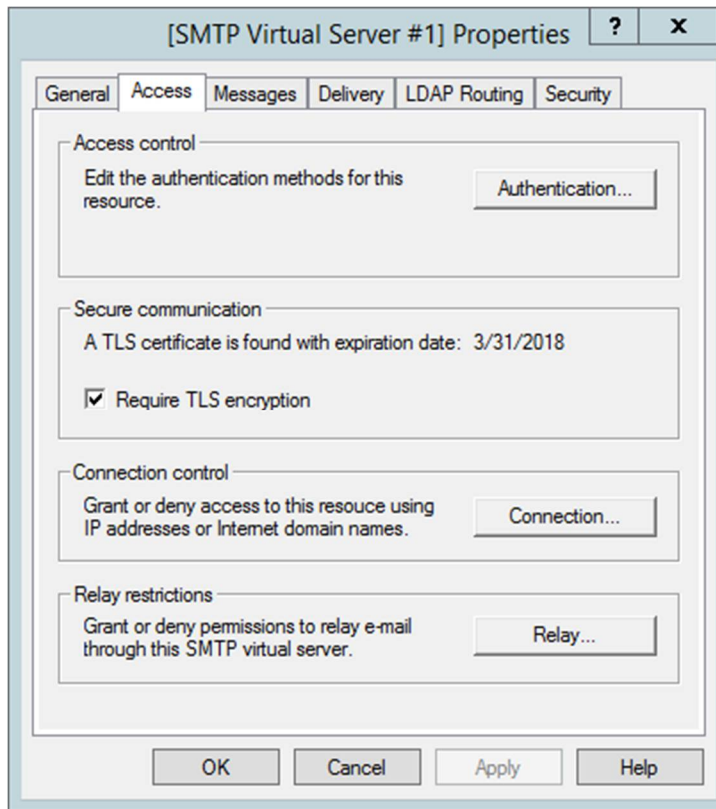
3. Select [SMTP Virtual Server #1].

4. Click **Action > Properties**.

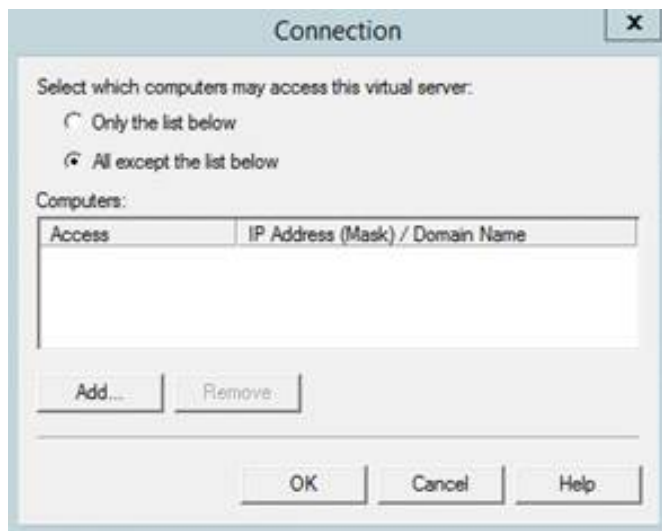


Note: In the **General** tab, you can enable logging for the SMTP connection.

5. Select the **Access** tab.



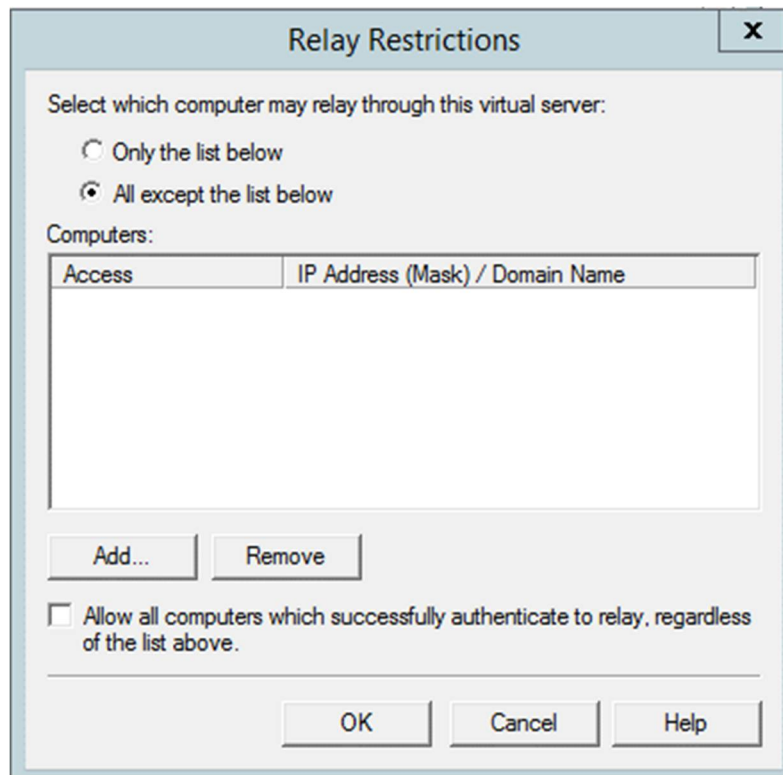
6. Ensure **Require TLS encryption** is selected. This ensures that SMTP traffic to Workshare Protect Server is encrypted.
7. Click **Connection...**



8. Select **All except the list below**.

Note: You have already limited access at the network security group level in Azure.

9. Click **OK**.
10. In the **Access** tab, click **Relay...**



11. Select **All except the list below**.

Note: You have already limited access at the network security group level in Azure.

12. Click **OK**.

13. Select the **Messages** tab.

The screenshot shows the 'Messages' tab of the '[SMTP Virtual Server #1] Properties' dialog box. The 'Messages' tab is selected, and the 'General' tab is also visible. The 'Messages' tab contains the following settings:

- Specify the following messaging information.**
- ☒ Limit message size to (KB): 2048
- ☒ Limit session size to (KB): 10240
- ☒ Limit number of messages per connection to: 20
- ☒ Limit number of recipients per message to: 100
- Send copy of Non-Delivery Report to: (empty text box)
- Badmail directory: C:\inetpub\mailroot\Badmail (with a 'Browse...' button)

At the bottom of the dialog box are the buttons: OK, Cancel, Apply, and Help.

14. In this tab, you can set the maximum message size. Refer to the Workshare Protect Server Administrator Guide for more information.

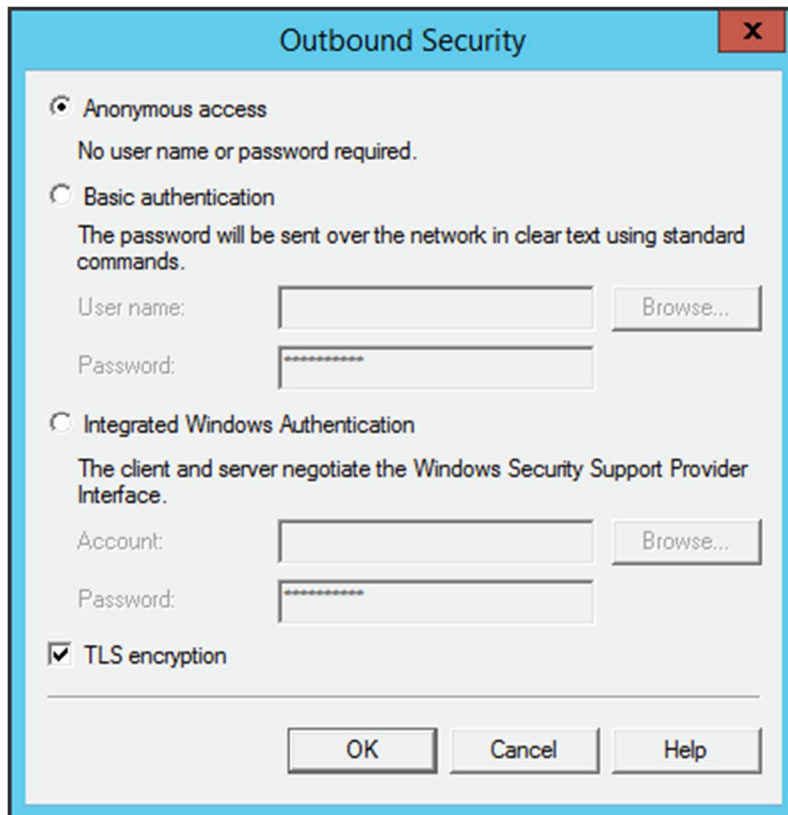
15. Select the **Delivery** tab.

The screenshot shows the 'Delivery' tab of the '[SMTP Virtual Server #1] Properties' dialog box. The 'Delivery' tab is selected, and the 'Messages' tab is also visible. The 'Delivery' tab contains the following settings:

- Outbound**
- First retry interval (minutes): 15
- Second retry interval (minutes): 30
- Third retry interval (minutes): 60
- Subsequent retry interval (minutes): 240
- Delay notification: 12 Hours (with a dropdown arrow)
- Expiration timeout: 2 Days (with a dropdown arrow)
- Local**
- Delay notification: 12 Hours (with a dropdown arrow)
- Expiration timeout: 2 Days (with a dropdown arrow)

At the bottom of the dialog box are the buttons: OK, Cancel, Apply, and Help. There are also three buttons at the bottom of the 'Delivery' tab: Outbound Security..., Outbound connections..., and Advanced...

16. Click **Outbound Security...**

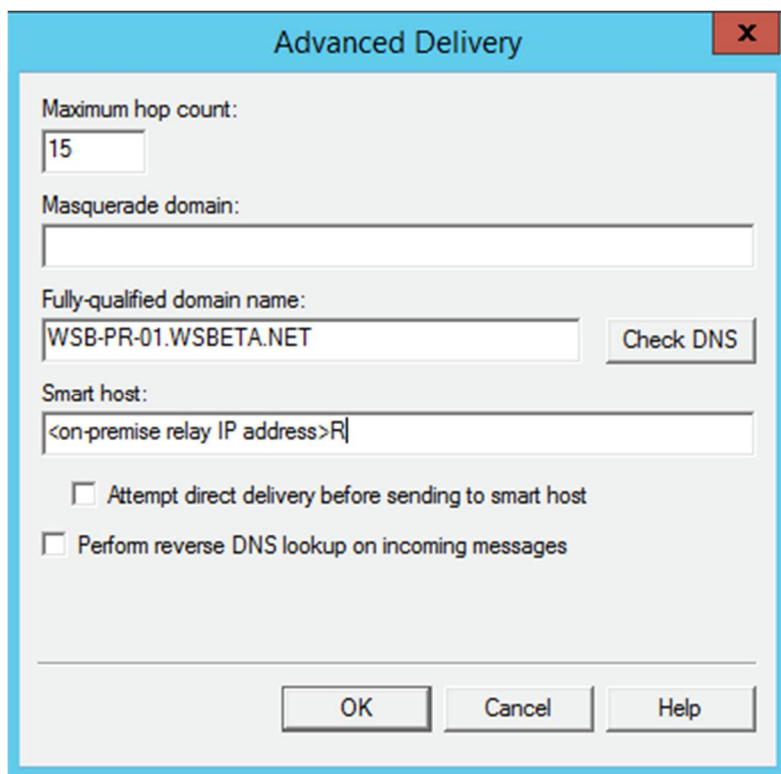


17. Select **Anonymous access**.

18. Ensure **TLS encryption** is selected. This ensures that outbound SMTP traffic from Workshare Protect Server is encrypted. Other upstream authentication settings can also be set here.

19. Click **OK**.

20. In the **Delivery** tab, click **Advanced...**

The image shows a Windows dialog box titled "Advanced Delivery" with a blue header bar and a red close button in the top right corner. The dialog contains several input fields and checkboxes. The "Maximum hop count:" field has a text box with the value "15". The "Masquerade domain:" field is an empty text box. The "Fully-qualified domain name:" field has a text box containing "WSB-PR-01.WSBETA.NET" and a "Check DNS" button to its right. The "Smart host:" field has a text box containing "<on-premise relay IP address>R". Below these fields are two checkboxes: "Attempt direct delivery before sending to smart host" and "Perform reverse DNS lookup on incoming messages", both of which are currently unchecked. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

21. Fill in the **Smart host** to "External On Prem Relay IP address" (B, page 4).
22. Click **OK**.
23. Click **OK** to accept changes and close the [SMTP Virtual Sever #1] Properties window.
24. Close Internet information Services (IIS) 6.0 Manager.

Configure Workshare Protect Server

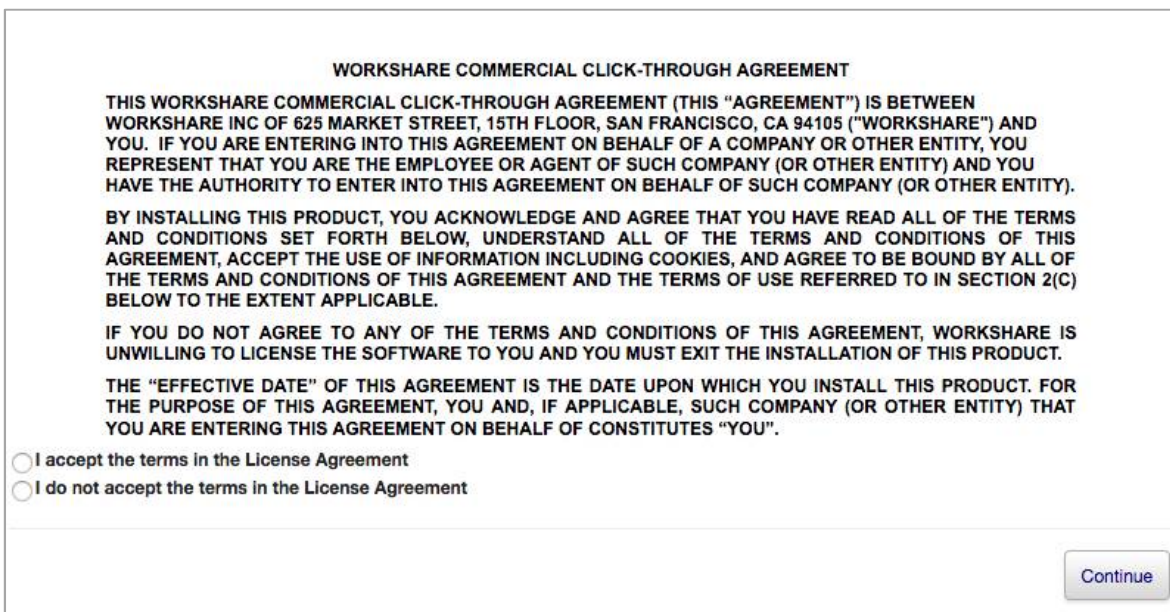
Step 1: Navigate to the Workshare Protect Server web console

Browse to the Workshare Protect Server web console at <https://<IP address>/protect>.

Note: The IP address is the public IP address for the Protect Server virtual machine.

Your browser will advise you that the machine is using a self-signed certificate for HTTPS communication. This is to be expected and you should proceed anyway. You may replace the self-signed certificate with your own.

The Workshare Protect Server Configuration Wizard is launched in your browser and the first page is the End User License Agreement.



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 HAVE READ ALL OF THE TERMS AND CONDITIONS SET FORTH BELOW, UNDERSTAND ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, ACCEPT THE USE OF INFORMATION INCLUDING COOKIES, AND AGREE TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THE TERMS OF USE REFERRED TO IN SECTION 2(C) BELOW TO THE EXTENT APPLICABLE.

IF YOU DO NOT AGREE TO ANY OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, WORKSHARE IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND YOU MUST EXIT THE INSTALLATION OF THIS PRODUCT.

THE "EFFECTIVE DATE" OF THIS AGREEMENT IS THE DATE UPON WHICH YOU INSTALL THIS PRODUCT. FOR THE PURPOSE OF THIS AGREEMENT, YOU AND, IF APPLICABLE, SUCH COMPANY (OR OTHER ENTITY) THAT YOU ARE ENTERING THIS AGREEMENT ON BEHALF OF CONSTITUTES "YOU".

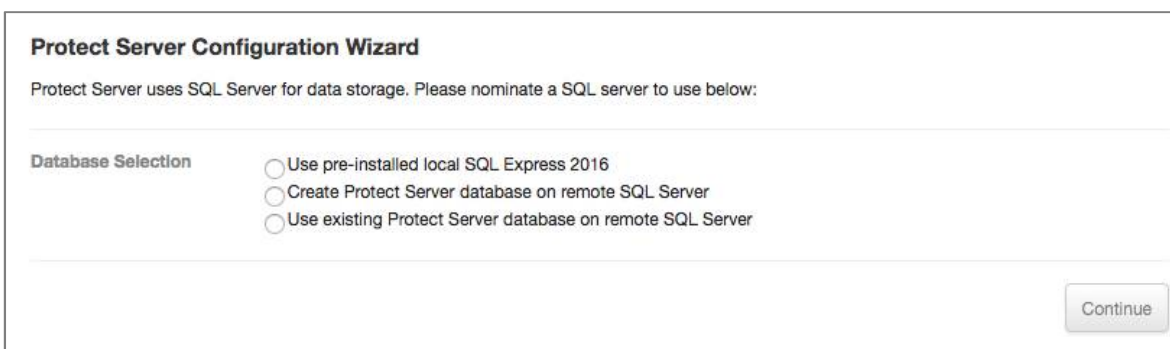
☐ I accept the terms in the License Agreement
☐ I do not accept the terms in the License Agreement

[Continue](#)

You must accept these conditions to proceed. Then click **Continue**.

Step 2: Configure database

The database configuration screen is where you configure which SQL server instance is used for data storage.



Protect Server Configuration Wizard

Protect Server uses SQL Server for data storage. Please nominate a SQL server to use below:

Database Selection

☐ Use pre-installed local SQL Express 2016
☐ Create Protect Server database on remote SQL Server
☐ Use existing Protect Server database on remote SQL Server

[Continue](#)

There are three options:

- **Use pre-installed local SQL Express 2016:** Workshare Protect Server comes with a local instance of SQL Express 2016. If this option is selected, data will be stored on this local database. However, other machines will not be able to access Workshare Protect Server data without further configuration. Any administrator of the local machine can administer this instance of SQL Express. There is no additional database configuration required for this option. Click **Continue** and go to step 5.

- **Create Protect Server database on remote SQL Server:** Workshare Protect Server is able to connect to a remote SQL server. This option should be used for the first installation of a series of Workshare Protect Server machines. Additional database configuration is required for this option. Go to step 3.
- **Use existing Protect Server database on remote SQL Server:** This option should be used if there is a pre-existing Workshare Protect Server database on a remote server and you want to share audit logs and metadata processing rules across multiple Workshare Protect Servers. Additional database configuration is required for this option. Go to step 4.

Step 3: Create Protect Server database on remote SQL server

When you select to create the Workshare Protect Server database on a remote SQL server, the following fields are displayed:

Protect Server Configuration Wizard
Protect Server uses SQL Server for data storage. Please nominate a SQL server to use below:

Database Selection

☐ Use pre-installed local SQL Express 2016
☒ Create Protect Server database on remote SQL Server
☐ Use existing Protect Server database on remote SQL Server

Create Database

SQL Server Name
Prerequisite: SQL Server 2008 R2-2016 SP1 with Full Text Search enabled. Azure SQL is not supported.

Database Name

Installer User
Requires: SQL Authentication
Required role: sysadmin OR dbcreator & securityadmin & serveradmin

Installer User Password

Processor User
This user shall be created if it does not already exist.

Processor User Password

Confirm Processor User Password

Create Database

Complete the settings as follows:

SQL Server Name	<p>This is the DNS host name or IP address for the SQL Server. Valid examples for the server name are listed below:</p> <p>IP Address: 172.16.0.32</p> <p>IP Address with port 1433: 172.16.0.32, 1433</p> <p>DNS Hostname: mssql.cloudapp.net</p> <p>DNS Hostname with port 1433: mssql.cloudapp.net, 1433</p> <p>Forced TCP protocol, DNS host name with port 1433: tcp:mssql.cloudapp.net, 1433</p> <p>If you added a new remote SQL server, use the private IP address of that server.</p>
Database Name	This is the name of the database to create for Workshare Protect Server.
Installer User Installer User Password	These are the credentials to use to create the database. This user must have either the sysadmin role or all of the following roles: dbcreator, securityadmin, serveradmin. These details are not stored on Workshare Protect Server.
Processor User Processor User Password Confirm Processor User Password	This is the user used by Workshare Protect Server to access the Workshare Protect Server database that was created. If this user does not exist, it will be created. These user details are stored on Protect Server.

Click **Create Database**. Depending on the configuration of SQL Server, database creation can take up to 10 minutes. Once complete, go to Step 5.

Step 4: Use existing Protect Server database on remote SQL server

When you select to use an existing Workshare Protect Server database on a remote SQL server, the following fields are displayed:

Protect Server Configuration Wizard

Protect Server uses SQL Server for data storage. Please nominate a SQL server to use below:

Database Selection

☐ Use pre-installed local SQL Express 2016
 ☐ Create Protect Server database on remote SQL Server
 ☒ Use existing Protect Server database on remote SQL Server

Existing Database

SQL Server Name

Database Name

Processor User

Processor User Password

Connect to Database

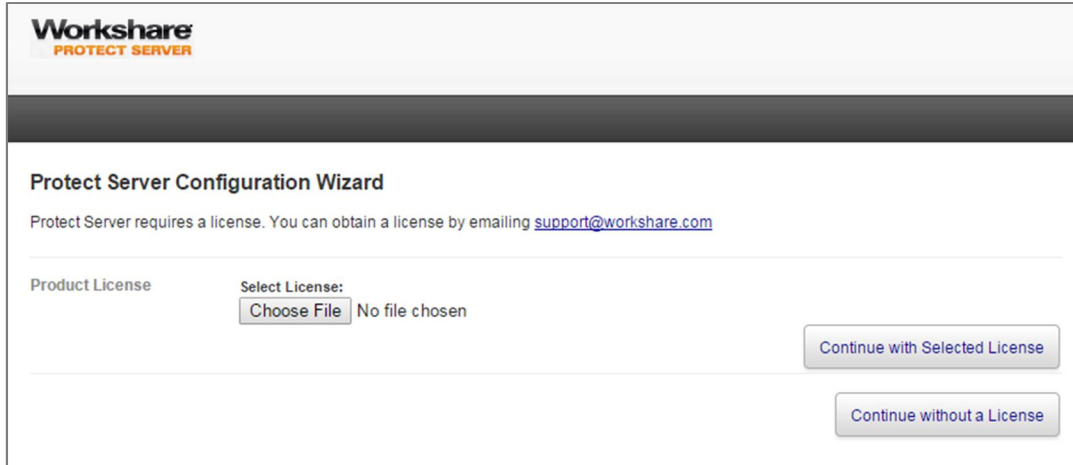
Complete the settings as follows:

SQL Server Name	<p>This is the DNS host name or IP address for the SQL Server. The SQL Server must have a version between 2012 - 2016, and have the Full Text search feature. The Azure SQL service is not supported. Valid examples for the server name are listed below:</p> <p>IP Address: 172.16.0.32</p> <p>IP Address with port 1433: 172.16.0.32, 1433</p> <p>DNS Hostname: mssql.cloudapp.net</p> <p>DNS Hostname with port 1433: mssql.cloudapp.net, 1433</p> <p>Forced TCP protocol, DNS host name with port 1433: tcp:mssql.cloudapp.net, 1433</p>
Database Name	This is the name of the database to create for Workshare Protect Server.
Processor User Processor User Password	This is the user used by Workshare Protect Server to access the Workshare Protect Server database that was created. If this user does not exist, it will be created. These user details are stored on Protect Server.

Click **Connect to Database** and go to Step 5.

Step 5: License Protect Server

Finally, if you are using the BYOL (bring-your-own-license) version of Workshare Protect Server, you will see the license page.



The screenshot shows the 'Protect Server Configuration Wizard' interface. At the top left is the 'Workshare PROTECT SERVER' logo. Below the header, the title 'Protect Server Configuration Wizard' is displayed. A message states: 'Protect Server requires a license. You can obtain a license by emailing support@workshare.com'. Under the 'Product License' section, there is a 'Select License:' label. Below this label is a 'Choose File' button and the text 'No file chosen'. To the right of these elements are two buttons: 'Continue with Selected License' and 'Continue without a License'.

Click **Choose File** and upload your license, or continue unlicensed. Workshare Protect Server will not process mail if it is unlicensed. However, you can review or update your license in the Settings pages of the Workshare Protect Server web console, so if you don't have your license yet, you can still continue and configure Workshare Protect Server.

All menus for the web console are now displayed.

The screenshot shows the Workshare Protect Server web console interface. At the top, the logo "Workshare PROTECT SERVER" is on the left, and "Logged in as admin" is on the right. Below the logo is a navigation bar with tabs: Status (selected), Reports, Messages, Profiles, and Settings. The main content area is titled "System Status" and lists several categories with their respective status indicators (green circles with checkmarks) and values:

- Mail Server**
 - SMTP Queue Directory: 0
 - Badmailed Messages (Bad Pickup File): 0
 - Badmailed Messages (General Failure): 0
 - Badmailed Messages (Hop Count Exceeded): 0
 - Badmailed Messages (NDR of DSN): 0
 - Badmailed Messages (No Recipients): 0
 - Remote Queue Length: 0
 - Remote Retry Queue Length: 0
 - Event Message Queue: Private\$Protect Server Results
 - SMTP Sinks
 - Simple Mail Transfer Protocol (SMTP) Windows Service
 - Free Diskspace (System Temp): 111.08 GB
 - Free Diskspace (Queue): 111.09 GB
 - Free Diskspace (Pickup): 111.09 GB
 - Free Diskspace (Drop): 111.09 GB
- Licensing**
 - License
 - WPSLicenseService Windows Service
- Auditing**
 - Database
 - Event Message Queue Size: 0
 - Event Message Queue: Private\$Protect Server Results
 - WPSAuditService Windows Service
 - Message Queuing Windows Service
- Profile**
 - Active Profiles: 1
 - Profile Changed: none
 - Profile Synchronization: 4/1/2015 2:22:06 PM
 - WSPProfileService Windows Service
- Mail Updater**
 - Mail Updater Message Queue: Private\$Protect Server Mail Updater Queue
 - Mail Updater Message Queue Size: 0
 - Rapid Retry Message Queue Size: 0
 - Mail Updater Retry Queue: Private\$Protect Server Mail Updater Retry Queue
 - Mail Updater Retry Queue Size: 0
 - Exchange Web Services Connectivity: none
 - WPSMailUpdaterService Windows Service

At the bottom of the Mail Updater section, there is a yellow box containing the text: "1. Mail Updater is not enabled".

The functionality of the web console is the same as for an on premise Workshare Protect Server and is described in full in the Workshare Protect Server Administrator Guide http://workshare.force.com/knowledgebase/articles/Help_Articles/Workshare-Protect-Server-3-8-Admin-Guide.

The only differences are:

- No Active Directory groups in Profiles
- No AD Cache settings
- New Credentials settings

You can use the Credentials settings to change your login to Workshare Protect Server.

The screenshot shows the Workshare Protect Server web interface. At the top, the logo 'Workshare PROTECT SERVER' is on the left, and 'Logged in as admin' is on the right. Below the header is a navigation bar with tabs: Status, Reports, Messages, Profiles, and Settings (which is highlighted). The main content area is titled 'Administrator Credentials'. On the left, there is a sidebar menu with links: Override, Bounce, Receipts, Email Templates, Alerts, Mail Updater, Credentials, Licensing, and About. The main content area contains the text 'The following credentials are used to secure access to Protect Server.' followed by a section titled 'User Credentials'. This section has four input fields: 'User Name' (containing 'admin'), 'Password', 'Confirm', and an empty field. At the bottom right of the form is a 'Save Changes' button.

Exchange Online Configuration

This section describes the setup process on your instance on Exchange 365 to send emails to Protect Server, and to receive clean receipts from Protect Server.

Set up the accepted domain

As Protect Server alters the contents of your email, any DKIM signatures generated will be immediately invalidated and will trigger suspicion on whether your email has been tampered with. To avoid this scenario, ensure that DKIM for your domain is disabled.

To disable the DKIM setting for your domain:

1. Log in to your Office configuration portal (<https://portal.office.com/>).
2. Click **Admin**.
3. In the menu on the left, select **Admin Centers** and then **Exchange**.
4. In the menu on the left, select **protection**.
5. Select the dkim tab and ensure that DKIM signatures are disabled for the domain.

For further information, see: [https://technet.microsoft.com/en-gb/library/mt695945\(v=exchg.150\).aspx#DKIMMultiDomain](https://technet.microsoft.com/en-gb/library/mt695945(v=exchg.150).aspx#DKIMMultiDomain)

Create an Outbound Connector

In order for email to be sent from Exchange Online to Protect Server, an outbound connector needs to be created.

To create an outbound connector:

1. Log in to your Office configuration portal (<https://portal.office.com/>).
2. Click **Admin**.
3. In the menu on the left, select **Admin Centers** and then **Exchange**.
4. In the menu on the left, select **mail flow**.
5. Select the connectors tab.
6. Click **+** to create a new connector.
7. In the **From** field, select **Office 365** and in the **To** field, select **Partner organization**.



The image shows a screenshot of the configuration interface for creating an outbound connector. It features two dropdown menus. The first dropdown, labeled 'From:', has 'Office 365' selected. The second dropdown, labeled 'To:', has 'Partner organization' selected. Both dropdowns have a small downward-pointing arrow on the right side of the selection box.

8. Click **Next**.
9. Enter an appropriate name and description.
10. Ensure that the **Turn it on** checkbox is not selected. The Protect Server is not ready to accept email just yet.
11. Click **Next**.
12. Select **Only when email messages are sent to these domains** and click **+** to add a new domain.
13. Set the new domain to '*' to capture all email sent.
14. Click **OK** and click **Next**.
15. Select **Route email through these smart hosts** and click **+** to add a smart host.
16. Add the External Protect Azure Machine IP addresses (A, page 4).
17. Click **Save** and click **Next**.

18. Select **Always use Transport Layer Security (TLS) to secure the connection** and select the sub-option **Any digital certificate, including self-signed certificates**.
19. Click **Next**.
20. Click **Save** to save your configuration and create your connector.
21. Enable the connector (click **Turn it on** under **Status**) when the all the steps after this are complete to start email flow through Protect Server.

Create an Inbound Connector

In order for clean receipts to be sent from Protect Server back to the email sender, an inbound connector needs to be created.

To create an inbound connector:

1. Log in to your Office configuration portal (<https://portal.office.com/>).
2. Click **Admin**.
3. In the menu on the left, select **Admin Centers** and then **Exchange**.
4. In the menu on the left, select **mail flow**.
5. Select the connectors tab.
6. Click **+** to create a new connector.
7. In the **From** field, select **Partner organization** and in the **To** field, select **Office 365**.
8. Click **Next**.
9. Enter an appropriate name and description.
10. Ensure that the **Turn it on** checkbox is selected.
11. Click **Next**.
12. Select **use the sender's IP address**.
13. Click **Next**.
14. Click **+** to add the sender IP address range. Enter the External on-premise relay IP address (B, page 4).
15. Click **OK** and click **Next**.
16. Select **Reject email messages if they aren't sent over TLS** and deselect the **And require that...** sub-option.
17. Click **Next**.
18. Click **Save** to save your configuration and create your connector.

Create On Premise Relay Machine

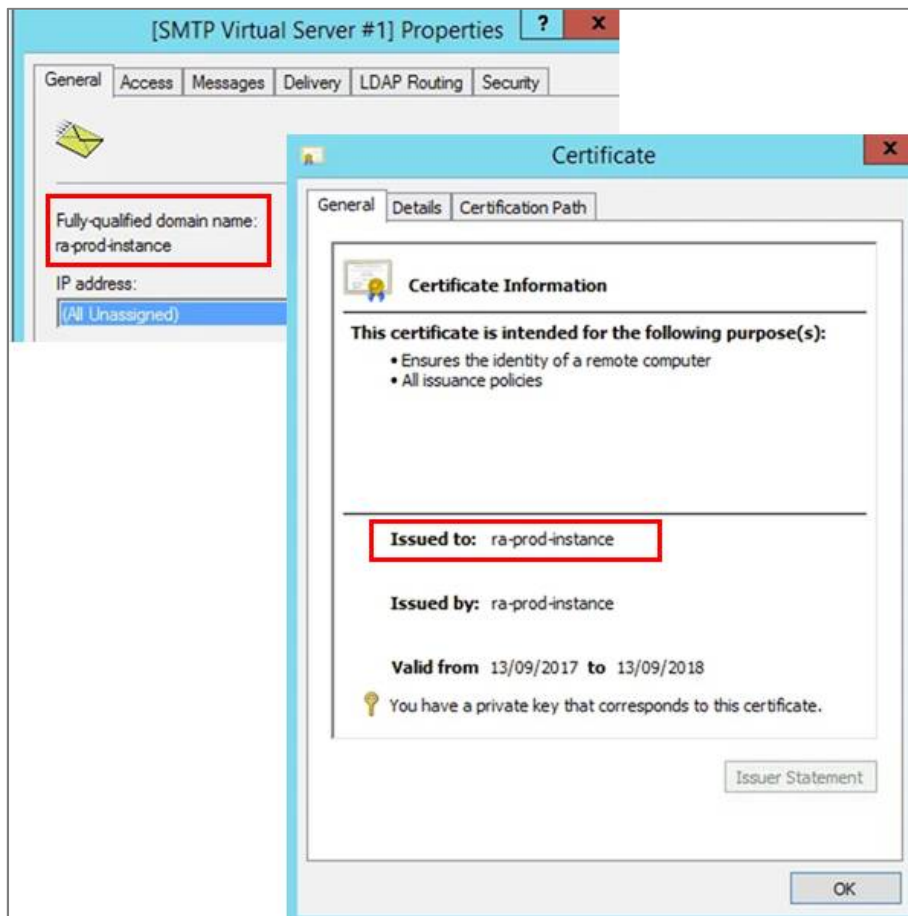
All services that run on popular cloud infrastructure (Microsoft Azure, Amazon S3, etc.) cannot send email out from that instance. This is due to the fact that these resources have been used to send spam email in the past. As a result, all email sent out from Azure compute resources will be marked as spam due to the originating IP address. There are three possible workarounds to this at the moment:

- **Relay email to a downstream process:** All email being sent out of Protect Server could be routed through a downstream email processing engine (e.g., Mimecast).
- **Relay email to a third-party cloud email solution:** All email being sent out of Protect Server could be routed through a third party email relay service (e.g., SendGrid) or an online instance of a server running an email forwarding service such as Postfix.
- **Relay email through a standalone on-premise email forwarder.** All email being sent out of Protect Server could be routed through an on-premise relay server. This helps ensure that the final relay for the email is held within the organization.

To create an on-premise email relay:

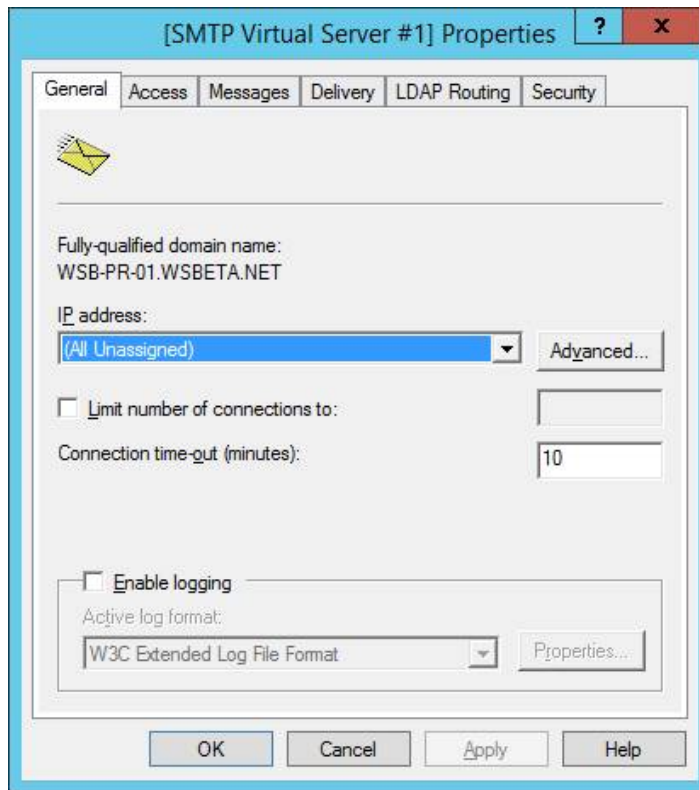
1. Install SMTP server windows feature.
2. Create a self-signed certificate for the relay machine. The easiest way to do this is here: [https://technet.microsoft.com/en-us/library/cc753127\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc753127(v=ws.10).aspx)

Note: The certificate must be issued to the hostname of the SMTP server. Notice how "ra-prod-instance" is the **Fully-qualified domain name** of the SMTP server in the example below and the certificate is issued to "ra-prod-instance".

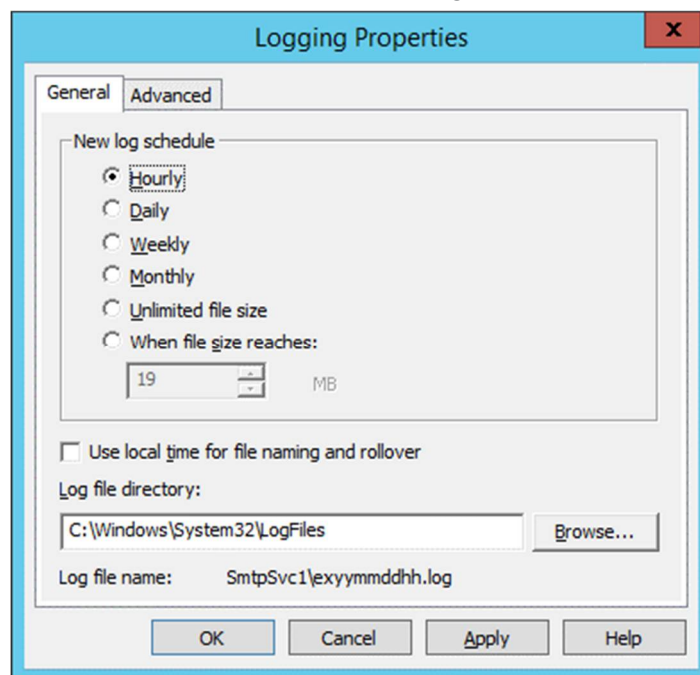


3. Start inetmgr6.

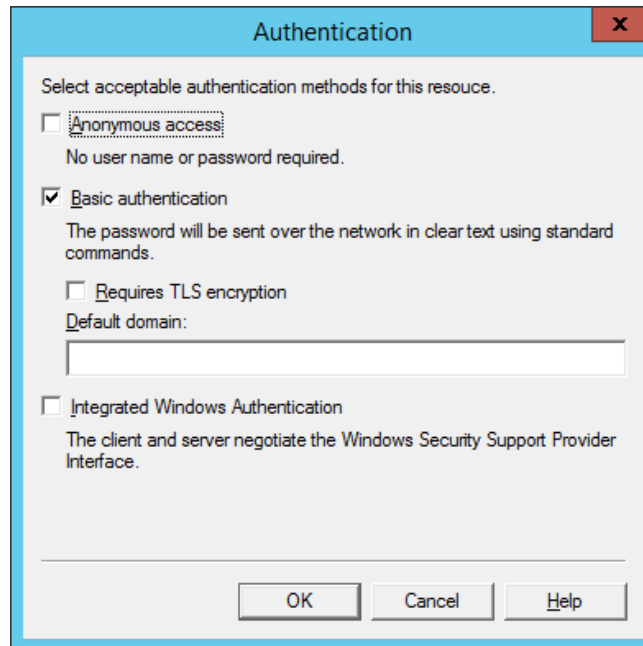
4. Select [SMTP Virtual Server #1] and click **Properties**.



5. Enable logging:
- In the General tab, select **Enable logging**.
 - Click **Properties** and set a new log schedule to **Hourly**.



- Select the Advanced tab and select all **Extended logging options**.
 - Click **OK**.
6. Configure inbound access configuration:
- Select the Access tab and click **Authentication**.



The Authentication dialog box has a title bar with 'Authentication' and a close button. The main area contains the text 'Select acceptable authentication methods for this resource.' followed by three options: 'Anonymous access' (unchecked), 'Basic authentication' (checked), and 'Integrated Windows Authentication' (unchecked). Below 'Basic authentication' is a checkbox for 'Requires TLS encryption' (unchecked) and a text field for 'Default domain:'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Select acceptable authentication methods for this resource.

☐ Anonymous access
No user name or password required.

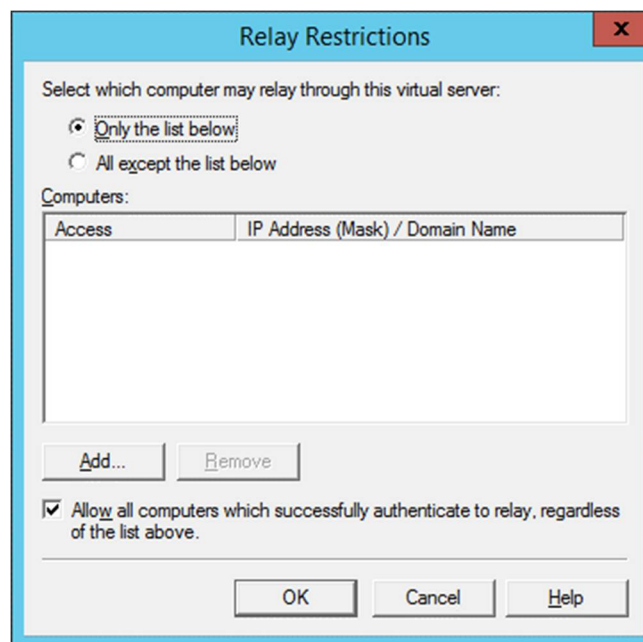
☒ Basic authentication
The password will be sent over the network in clear text using standard commands.

☐ Requires TLS encryption
Default domain:

☐ Integrated Windows Authentication
The client and server negotiate the Windows Security Support Provider Interface.

OK Cancel Help

- Ensure only **Basic authentication** is selected.
- Click **OK**.
- Back in the Access tab, click **Relay**.
- Select **Only the list below** may relay through this server.



The Relay Restrictions dialog box has a title bar with 'Relay Restrictions' and a close button. The main area contains the text 'Select which computer may relay through this virtual server:' followed by two radio buttons: 'Only the list below' (selected) and 'All except the list below'. Below is a section labeled 'Computers:' with a table with two columns: 'Access' and 'IP Address (Mask) / Domain Name'. At the bottom are 'Add...' and 'Remove' buttons, followed by a checkbox for 'Allow all computers which successfully authenticate to relay, regardless of the list above.' and 'OK', 'Cancel', and 'Help' buttons.

Select which computer may relay through this virtual server:

☒ Only the list below
☐ All except the list below

Computers:

Access	IP Address (Mask) / Domain Name
--------	---------------------------------

Add... Remove

☒ Allow all computers which successfully authenticate to relay, regardless of the list above.

OK Cancel Help

- Click **Add** and add the External Protect Azure Machine IP addresses (A, page 4) here.
 - Click **OK**.
 - Back in the Access tab, click **Connection**.
 - Select **Only the list below** may access this server.
 - Click **Add** and add the External Protect Azure Machine IP addresses (A, page 4) here.
 - Click **OK**
7. Configure message size limits:
- Select the Messages tab.
 - Ensure all limits are disabled (deselected).

The screenshot shows the 'Messages' tab of the '[SMTP Virtual Server #1] Properties' dialog box. The 'Messages' tab is selected, and the 'General' tab is also visible. The 'Messages' tab contains the following settings:

- ☐ Limit message size to (KB): 2048
- ☐ Limit session size to (KB): 10240
- ☐ Limit number of messages per connection to: 20
- ☐ Limit number of recipients per message to: 100

Below these settings, there is a text box for 'Send copy of Non-Delivery Report to:' which is currently empty. Below that is a 'Badmail directory:' section with a text box containing 'C:\inetpub\mailroot\Badmail' and a 'Browse...' button.

At the bottom of the dialog box are four buttons: 'OK', 'Cancel', 'Apply', and 'Help'.

8. Configure outbound delivery:

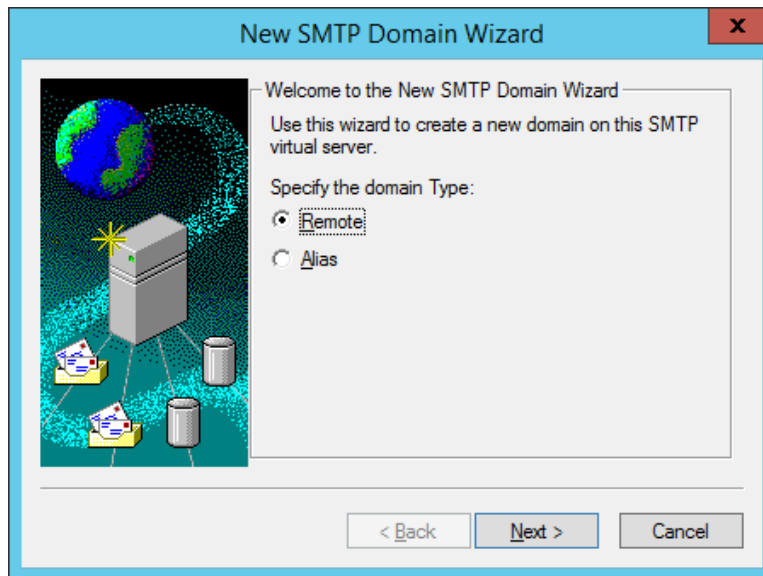
- Select the Delivery tab.

The screenshot shows the 'Delivery' tab of the '[SMTP Virtual Server #1] Properties' dialog box. It contains two sections: 'Outbound' and 'Local'. The 'Outbound' section has fields for 'First retry interval (minutes):' (15), 'Second retry interval (minutes):' (30), 'Third retry interval (minutes):' (60), 'Subsequent retry interval (minutes):' (240), 'Delay notification:' (12 Hours), and 'Expiration timeout:' (2 Days). The 'Local' section has fields for 'Delay notification:' (12 Hours) and 'Expiration timeout:' (2 Days). At the bottom, there are buttons for 'Outbound Security...', 'Outbound connections...', and 'Advanced...'. The 'Outbound Security...' button is highlighted with a dashed border.

- Click **Outbound Security**.
- Select **Anonymous access** and deselect **TLS encryption**.
- Click **OK**.
- Back in the Delivery tab, select **Advanced**.

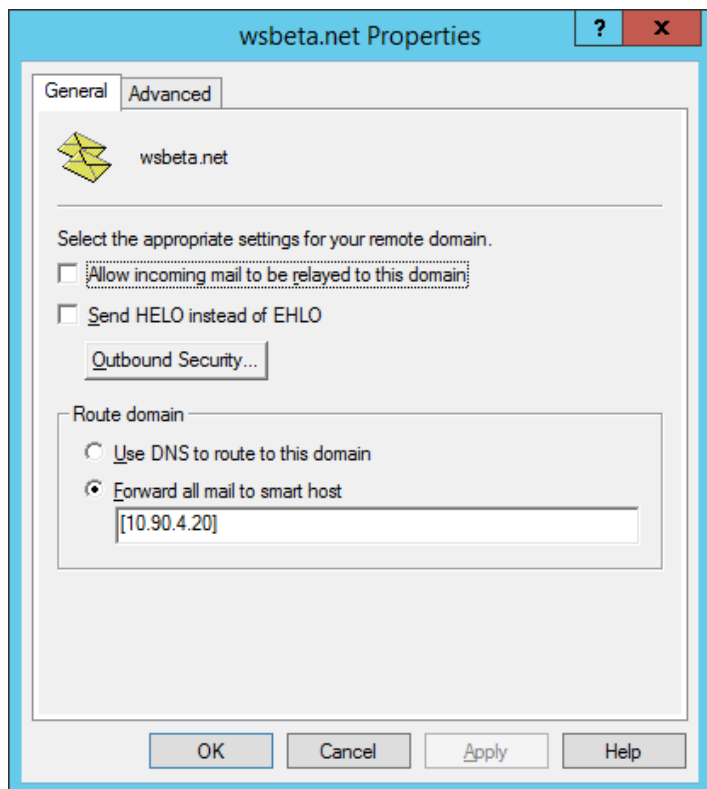
The screenshot shows the 'Advanced Delivery' dialog box. It contains the following fields and options: 'Maximum hop count:' (15), 'Masquerade domain:' (empty), 'Fully-qualified domain name:' (WSB-PR-01.WSBETA.NET) with a 'Check DNS' button, 'Smart host:' (empty), and two checkboxes: 'Attempt direct delivery before sending to smart host' (unchecked) and 'Perform reverse DNS lookup on incoming messages' (unchecked). At the bottom, there are buttons for 'OK', 'Cancel', and 'Help'.

- Ensure the **Smart host** field is left empty.
 - Click **OK**.
9. Click **OK** in the Properties dialog.
10. Create a new domain:
- Under [SMTP Virtual Server #1], right-click **Domains** and select **New** then **Domain**.



- Select **Remote** as the domain Type.
- Click **Next**.
- Enter the domain name of Exchange Online as the domain Name, for example, "protectdemo-dev.net".
- Click **Finish**. The new domain is displayed in the list of domains on the right.

11. Right-click the new domain and select **Properties**.



12. In the General tab, click **Outbound Security**.

13. Select **Anonymous access** and **TLS encryption**.

Exchange Online may reject clean receipts as spam email.

To work around this issue:

- Ensure that your domain has an SPF record allowing your on-premise relay machine to relay email for your domain.
- Ensure that your IP provider sets a reverse DNS record for your relay machine that points to your domain.

For example, where ps-relay.protectedemo-dev.net maps to 123.456.123.456, get your IP provider to map 123.456.123.456 to ps-relay.protectedemo-dev.net.

You may need to create a mailbox for the Protect Server "alert" address. For example, create the mailbox donotreply@protectedemo-dev.net (where protectedemo-dev.net is your domain name) and set the Protect Server alert email address to this mailbox. Then delist "donotreply@protectedemo-dev.net" for your relay IP address via <https://sender.office.com>.

Network Topology Recommendations

This section provides information on high availability and fault tolerance and will guide you when deciding on configuring the network topology for multiple Workshare Protect Servers.

Protect Server fault tolerance

The following features provide fault tolerance for Protect Server:

- Settings are stored locally and are machine-independent.
- Metadata profiles are stored on SQL database. However, they are also cached on machine to protect against connection failure with SQL server.
- Message-auditing functions are queued on a transactional MSMQ queue. A connection failure with SQL server will mean messages will not be written until the connection is restored.
- Protect Server will not accept mail if mission critical services are non-operational. Exchange will use a different Protect Server for delivery (if available) OR emails will queue at Exchange and will not be lost.

Protect Server high availability

Exchange allows multiple Protect Server machines to be listed as the smart host to a send connector. This allows multiple Protect Server machines to provide high availability and load-balancing. In this configuration, the following considerations should be made:

Corresponding, but independent settings

The following settings are not shared between Protect Server instances; although they often have the same values across Protect Server instances, they must be maintained separately on each instance:

- Windows SMTP Server settings
- Dashboard Settings. These may be cloned between machines by manually replacing the contents of the following files:
 - C:\ProgramData\Workshare\Protect Server\3.5.1.0\Configuration\metadata.config
 - C:\ProgramData\Workshare\Protect Server\3.5.1.0\Configuration\updater.config
- License Files

DNS round robin for load balancing across outbound smart hosts

Windows SMTP Server only supports a single outbound smart host. To achieve load-balancing across multiple smart hosts, it is recommended that a DNS Round Robin system be configured. The outbound smart host setting on Windows SMTP server can then be pointed at a virtual DNS entry, which will rotate between nominated smart hosts.

DNS MX priority for outbound smart host failover

Alternatively, DNS can be configured to allow Windows SMTP Server to fail-over to alternative smart hosts. To achieve this, configure a virtual DNS domain with MX records for each smart host. Ensure that the fail-over MX record has a numerically higher preference value.

Protect Server disaster recovery

It is recommended that the following items are backed up:

- SQL Database – at minimum, back up [Config.Profiles] to maintain operational continuity
- C:\ProgramData\Workshare\Protect Server\3.5.1.0\Configuration\metadata.config
- C:\ProgramData\Workshare\Protect Server\3.5.1.0\Configuration\updater.config

A Protect Server machine may be restored by:

1. Creating a new Azure instance of Protect Server.
2. Replacing the contents of the following files from backup:
 - C:\ProgramData\Workshare\Protect Server\3.5.1.0\Configuration\metadata.config
 - C:\ProgramData\Workshare\Protect Server\3.5.1.0\Configuration\updater.config
3. Run Protect Server Configuration Wizard, and use the same Remote SQL Server instance.



Workshare Ltd.

© 2017. Workshare Ltd. All rights reserved.

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

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.

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.

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

Revisions

Published for Workshare Protect Server 3.9: 31/10/17

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