Workshare Protect Server

Post-Install Guide

Table of Contents

About this Document 3
Understanding the Protect Server workflow 3
Updating Settings after Installation 5
Email settings 5
Database settings 6
Override Email Address 6
Manual Configuration of Security Roles 7
Users with system administrator (sysadmin) server role 7
Processor role 7
Processor role - access control lists 11
Changes to Workshare services 12
Administrator role 14
Administrator role - access control lists 15
Modifications to web.config 15
Business role 16
Business role - access control lists 17
Modifications to web.config 17
User role 18
User role - access control lists 19
Modifications to web.config 19

About this Document

This document covers changes to configuration you may want to make after installation of Workshare Protect Server.

You can find more information about installing and configuring Protect Server and the Routing Agent from these guides on our knowledge base (http://workshare.force.com/knowledgebase):

If you require further assistance, contact Workshare Support.

Understanding the Protect Server workflow

When you have Protect Server with the Protect Routing Agent installed, mail is routed from Microsoft Exchange to Protect Server if it:

- Contains one or more non-image attachment; and
- Contains one or more external recipient; and
- (configurable) Has not been previously cleaned by Workshare Protect or other cleaning product (triggered by email header)

Protect Server sends the processed mail back to Microsoft Exchange Server, then Exchange Server does the final mail routing, similar to the typical Exchange Server setup shown in Figure 1.

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

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

4. Microsoft Exchange Server will receive the mail back from Protect Server. This is allowed by a Receive Connector created during installation. The Protect Routing Agent will see that the mail came from Protect Server and allow Exchange to route the mail normally (to the mail gateway for external recipients and into the appropriate mailbox for internal recipients).

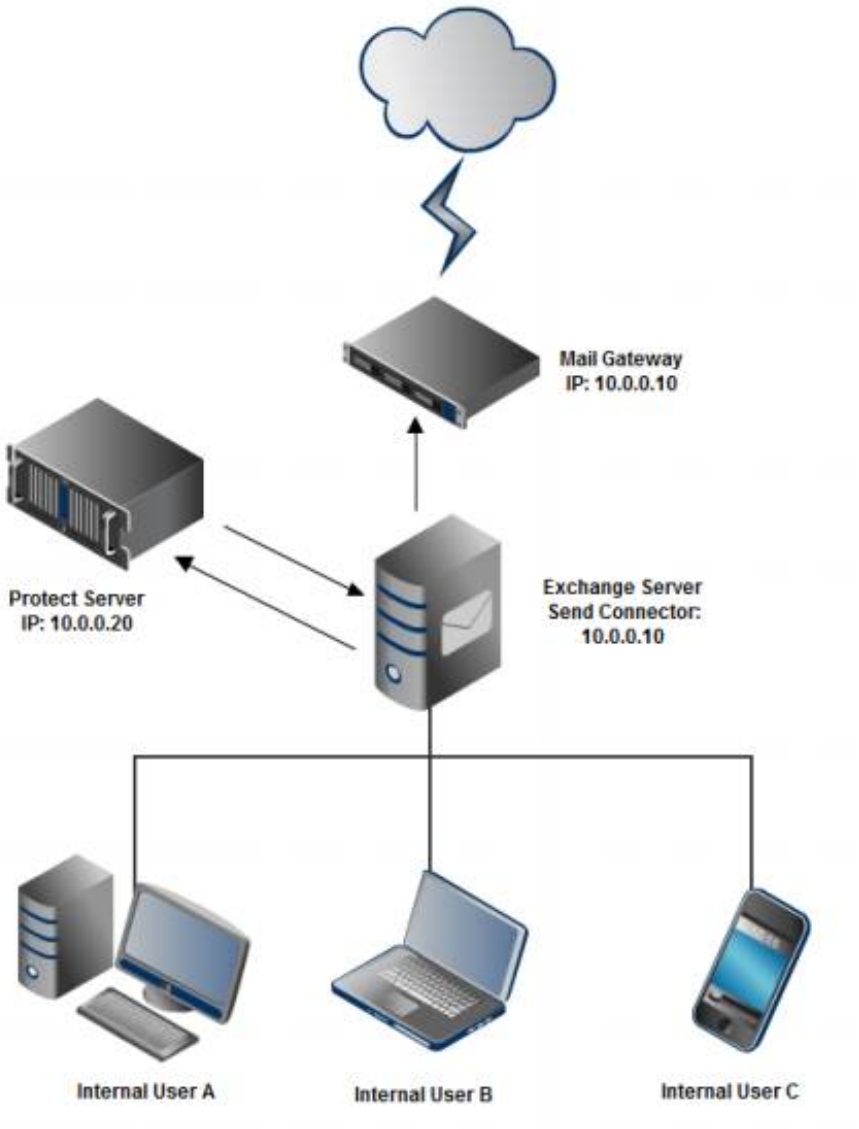


Figure 1: *Typical mail flow through Workshare Protect Server*

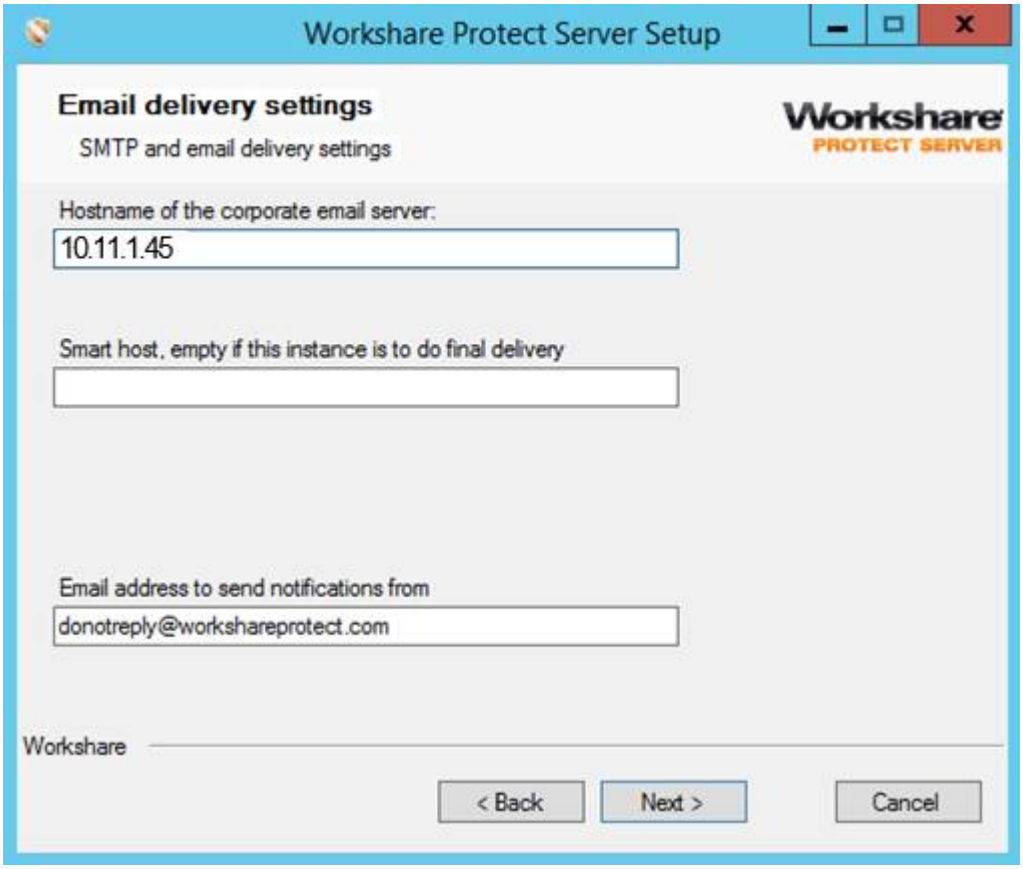
This custom routing is performed by the Protect Routing Agent (a transport agent) on Microsoft Exchange Server. The configuration prevents a mail loop by ensuring that mail coming back from Protect Server does not get re-routed back to Protect Server.

Updating Settings after Installation

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

Email settings

The email delivery settings (shown below) specified during installation 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 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 Protect Server web console and select **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 notification emails are delivered. This email address is the “sender” of clean receipt emails and “Clean Failed - Email 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 during installation on the Database configuration page), it is recommended that you delete the specified database and re-run the Protect Server installation.

Override Email Address

A user can use an override address to bypass cleaning by Workshare Protect Server. For information on how to configure a cleaning override address, refer to the *Workshare Protect Server Installation guide*. If a real email address is used 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 or converted and the override address is removed. The email then continues its journey to recipients. However, when emails include a digital signature, Protect Server does not remove the override address and therefore the actual email will also be delivered to the override address.

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" (the override address).

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

Manual Configuration of Security Roles

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

- Administrator role
- Business role
- User role

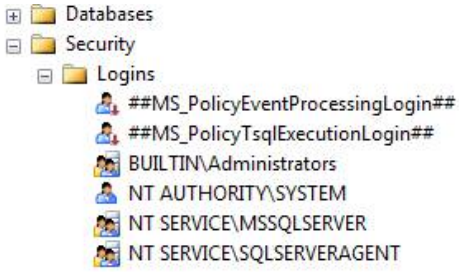
This is due to a design decision by Microsoft and the IS_ROLEMEMBER function. The user will be internally mapped as the dbo (database owner) to all databases. See this feedback note: http://connect.microsoft.com/SQLServer/feedback/details/345809/is-member-function-does-not-work-as-expected. If you try 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 map explicitly 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 Protect Server processing engine. The role is installed locally to the Windows services called Workshare Audit Service and Workshare Profile Service.

To add a new login to the database:

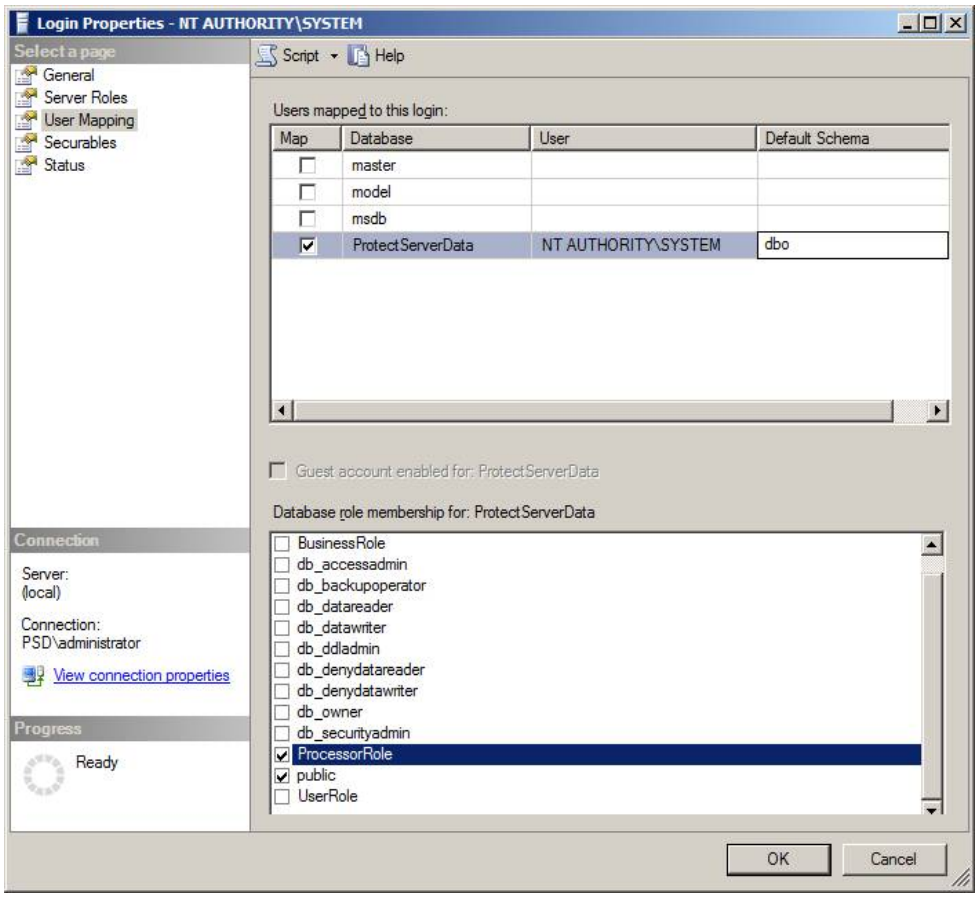
1. Launch Microsoft SQL Server Management Studio (SSMS) and log in with sysadmin server role.
2. Expand the **Security**/**Logins** nodes.



The login you add to the database server will depend on whether you are going to use the Local System account to run the Windows services or a dedicated domain account.

- **Local System account and local database**

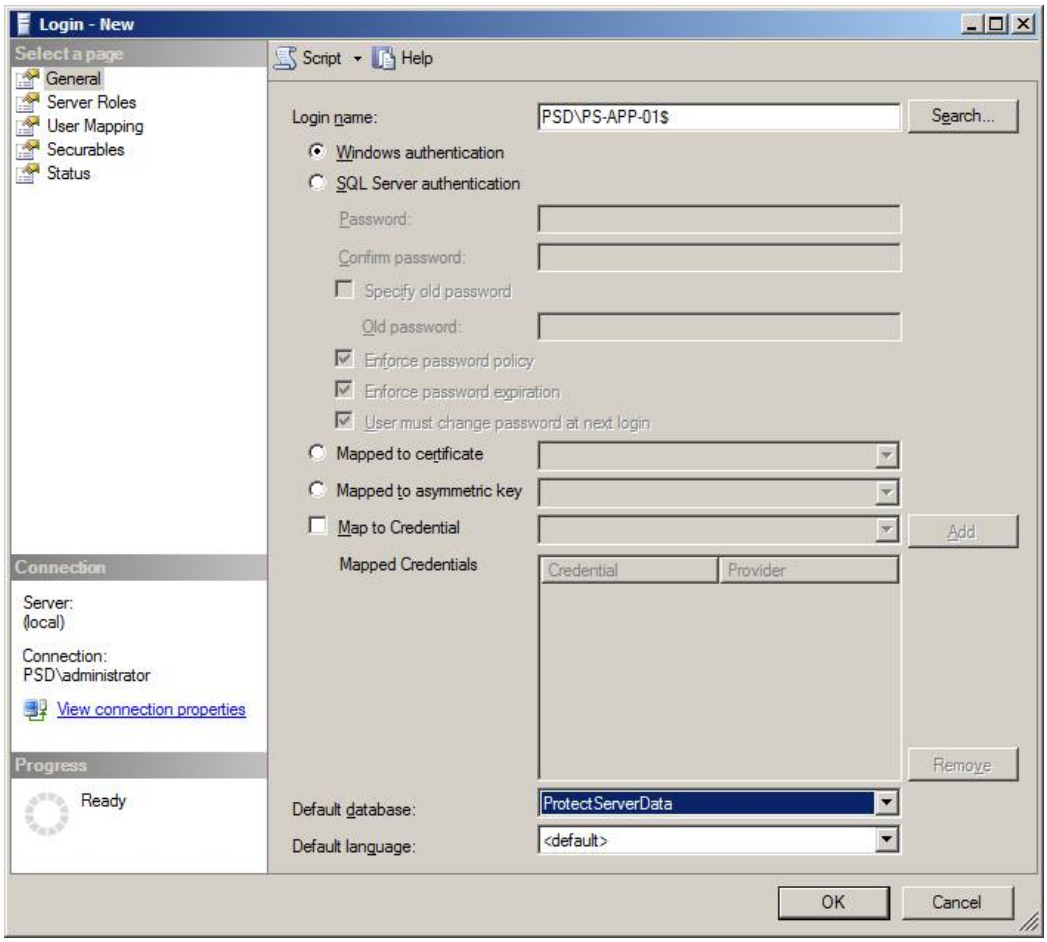
  If using the Local System account and the database is local, then you may already have the account added (NT AUTHORITY\SYSTEM). If so, just right-click this user, select **User Mapping** and select the Protect Server database. Assign the user the database role **ProcessorRole** and set the default schema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



- **Local System account and remote database**

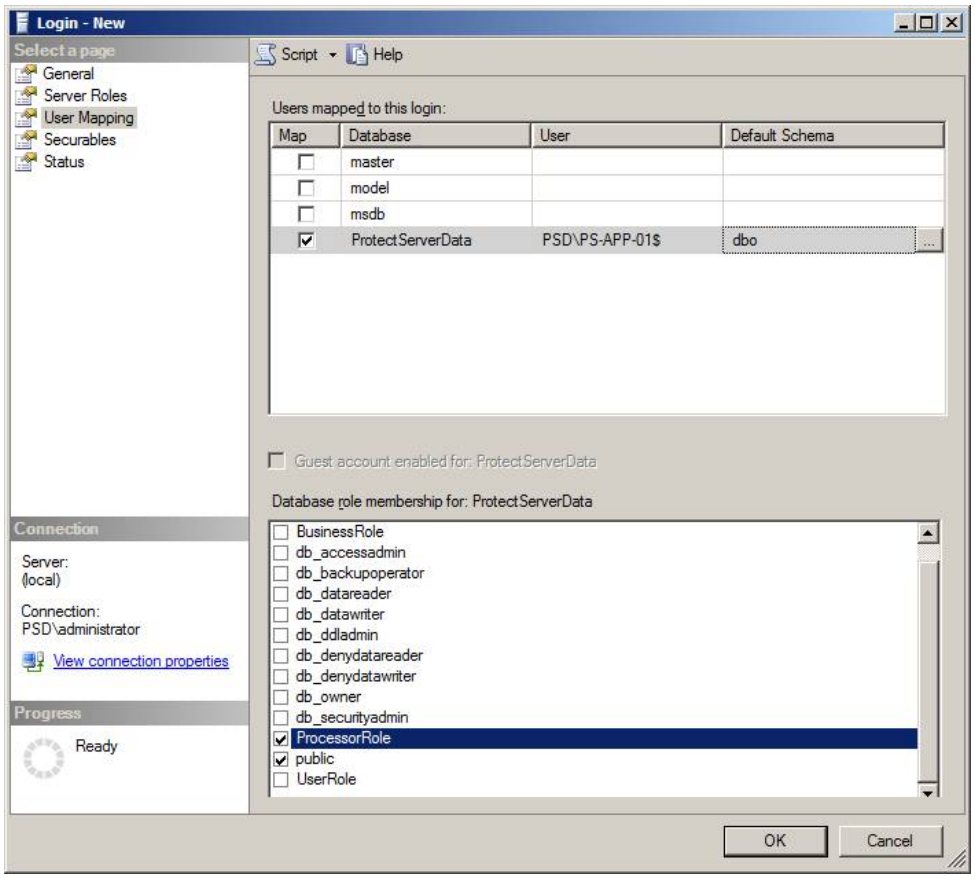
  If using the Local System account and the database is remote, then you will probably need to add this account to the database. **This is not recommended as it relies on kerberos security and Service Principal Names (SPN) being setup correctly to work.**

  - Right-click the **Logins** node and select **New Login**.



  - For the **Login name** you have to manually type in the hidden machine account name. This name is made up 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 registered in a domain called PSD, the login name will be PSD\PS-APP-01$.
  - Set the **Default database** to the Protect Server database.

- Select **User Mapping**.



- Select the Protect Server database. Assign the user the database role **ProcessorRole** and set the default schema to **dbo**.

- **Domain account**

  If using a domain account, then follow the steps described for a Local System account with a remote database and replace the machine domain account with the user domain account.

Processor role - 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.

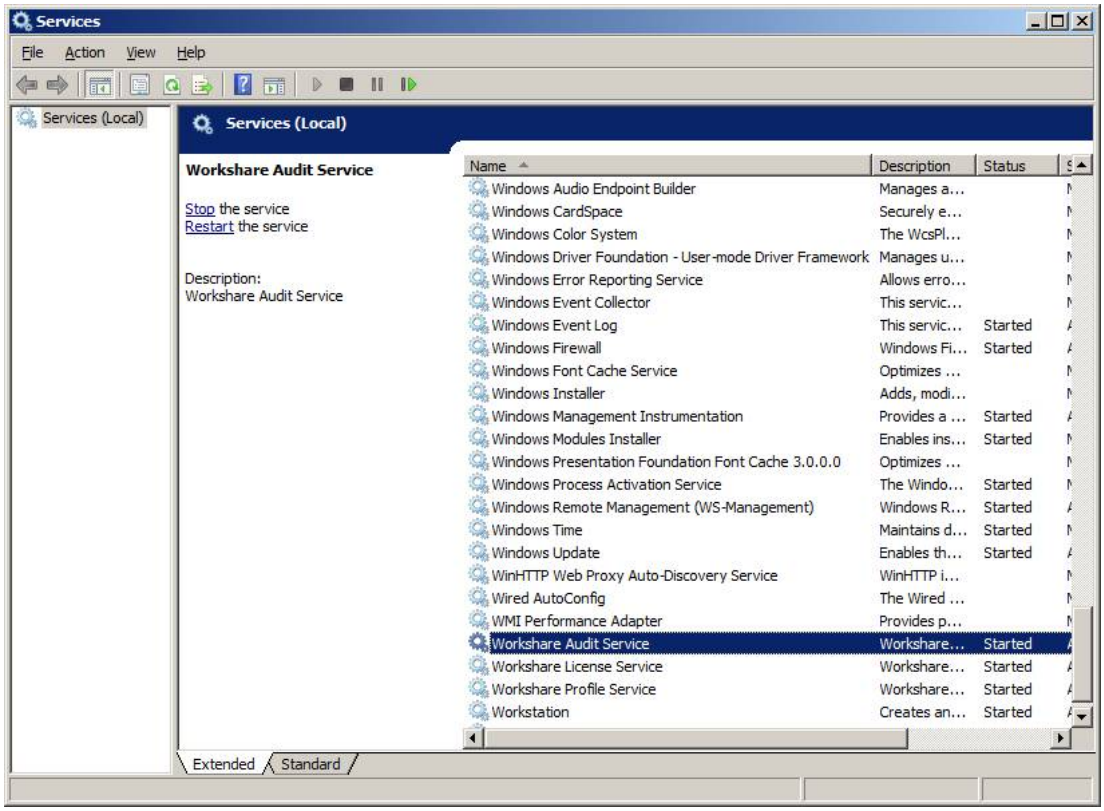
Location	File	Permissions required
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Db.config	Read
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Logging.config	Full Control
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Metadata.config	Read
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Unity.config	Read
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Results		Full Control
C:\Program Files\Workshare\Protect Server\Smtp Server		Full Control

Changes to Workshare services

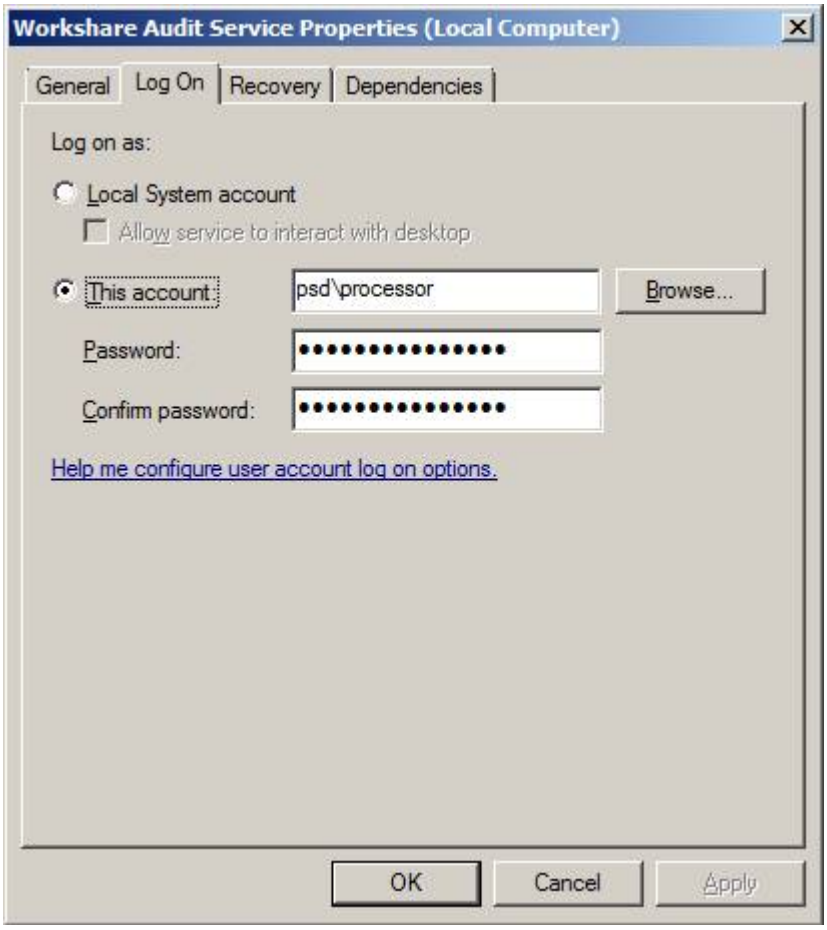
Once the access control lists are set up on the database, you can change the login details for the Workshare services - Workshare Audit Service and Workshare Profile Service.

To change login for services:

1. Launch Services.msc module.



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



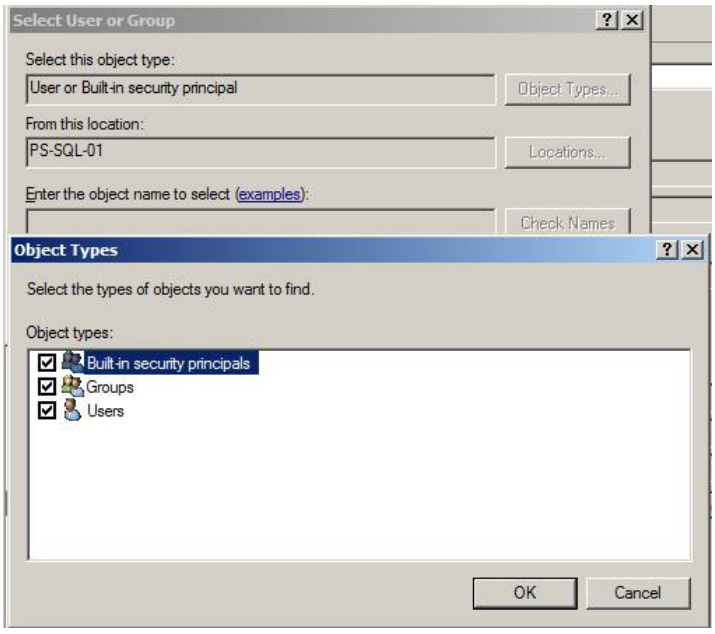
3. If the user is a Local System account, then select the **Local System account** radio button. If the user is a domain account, then select the **This account** radio button.
4. For a domain account, fill in the details of the account.
5. Click **OK**. If the domain account has never been used as a service account then you will receive a dialog stating that this account has been given 'Log On As Service' privilege when you click **OK**.
6. These settings do not take effect until the service is restarted. Click on the restart button on the top toolbar  .
7. Repeat steps 1 to 6 for Workshare Profile Service.

Administrator role

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

To add a new login to the database:

1. Launch Microsoft SQL Server Management Studio (SSMS) and log in with sysadmin server role.
2. Expand the **Security**/**Logins** nodes. This role can only be a security group.
3. If using the Local System 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 **Logins** 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 Protect Server database.
   - Select **User Mapping** and select the Protect Server database.
   - Assign the user the database role **AdministratorRole** and set the default schema to **dbo**.

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

Administrator role - 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\3.11.0.0\Configuration	Db.config	Full Control
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Logging.config	Full Control
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Metadata.config	Full Control
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Unity.config	Full Control
<InstalledLocation>Workshare\Protect Server\Dashboard\App_Data\Charts		Full Control

Modifications to web.config

Once the access control lists are set up on the database, you can modify the Administrator role in the web.config file. 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.

Modify the following elements:

- **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 the 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 the 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 Protect Server.

To add a new login to the database:

1. Launch Microsoft SQL Server Management Studio (SSMS) and log in with sysadmin server role.
2. Expand the **Security**/**Logins** nodes. This role can only be a security group.
3. If using the Local System 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 **Logins** 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 Protect Server database.
   - Select **User Mapping** and select the Protect Server database.
   - Assign the user the database role **BusinessRole** and set the default schema to **dbo**.

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

Business role - 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\3.11.0.0\Configuration	Db.config	Read
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Logging.config	Full Control
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Metadata.config	Read
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Unity.config	Read
<InstalledLocation>Workshare\Protect Server\Dashboard\App_Data\Charts		Full Control

Modifications to web.config

Once the access control lists are set up on the database, you can modify the Business role in the web.config file. 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.

Modify the following elements:

- **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 the 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 the 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 Protect Server.

To add a new login to the database:

1. Launch Microsoft SQL Server Management Studio (SSMS) and log in with sysadmin server role.
2. Expand the **Security**/**Logins** nodes. This role can only be a security group.
3. If using the 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 **Logins** 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 Protect Server database.
   - Select **User Mapping** and select the Protect Server database.
   - Assign the user the database role **UserRole** and set the default schema to **dbo**.

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

User role - 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\3.11.0.0\Configuration	Db.config	Read
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Logging.config	Read
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Metadata.config	Read
C:\ProgramData\Workshare\Protect Server\3.11.0.0\Configuration	Unity.config	Read
<InstalledLocation>Workshare\Protect Server\Dashboard\App_Data\Charts		Full Control

Modifications to web.config

Once the access control lists are set up on the database, you can modify the User role in the web.config file. 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.

Modify the following element:

- **ApplicationSettings element**

  This element is located in the Configuration element near the bottom of the file. There are three setting elements contained inside the 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.

You don’t need to update the Authorization element as all domain users are authenticated against this by default, and therefore allowed in.

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

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

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