Symprex Email Signature Manager

User's Guide

Version 9.0.1.

Contents

Contents

Contents

Introduction 1

Symprex Email Signature Manager is the perfect solution for ensuring professional email communication across your organization with consistent signatures, mail format and contact information.

Benefits

Some of the most important benefits of Email Signature Manager are:

- Helps to ensure professional email communication.
- Standardized, identical and consistent email signatures for everyone.
- Correct and up-to-date contact information in emails.
- Signatures are visible to users when composing emails.
- Signatures are applied to emails sent from mobile devices.
- Helps improve professional organization image and branding.
- Minimum administration hassle for everyone.
- Emails are not re-routed from source to destination.
- Users do not have to do anything to use deployed signatures.

Features

Some of the most important features of Email Signature Manager are:

- Deploy identical signatures to Outlook, OWA and other email clients.
- Works with Android, iPhone, iPad, and Windows Mobile devices.
- Built-in disclaimer and campaign support.
- Powerful WYSIWYG template designer.
- Supports HTML, RTF and Plain Text email formats.
- HTML designer offers color-coded HTML source editing.
- Merge signatures with contact information from Active Directory.
- Merge signatures with contact information from virtually any type of database.
- Powerful test module with full preview in all formats.
- Test signatures before deployment in preview and in actual email clients.
- Flexible deployment of signatures to groups and individual users.
- Supports nested sub-groups when determining user group membership.
- Simple deployment via logon script command-line utility, Active Directory or ClickOnce installation.
- Status monitor to verify deployment status to every individual user.
- Signatures work both when on-line and off-line.

Getting Started

This introduction will take you through the system requirements, an overview of Email Signature Manager and how to either perform a first-time install of the product or upgrade an existing installation.

About Symprex

Symprex is one of the leading companies in the world for add-on solutions for Microsoft Exchange Server, Office 365 and Outlook. Please see Symprex.com for more information about Symprex and the solutions we offer.

Introduction 1

System Requirements

Email Signature Manager minimum system requirements are:

- Supported email clients:
  Microsoft Outlook 2013/2016/2019/365
  Microsoft OWA/OOTW on Exchange Online
  Microsoft OWA/OOTW on Exchange Server 2013 CU15/2016/2019
  Mobile devices on Office 365 when subscribing to the Signature Injection Service for Office 365
  Mobile devices on Exchange Server when using the Email Signature Manager Transport Agent

- Supported email servers:
  Microsoft Exchange Online
  Microsoft Exchange Server 2013 CU15/2016/2019

- Operating system software:
  Microsoft Windows 8.1/10/11
  Microsoft Windows Server 2012/2012 R2/2016/2019/2022

- Framework software:
  Email Signature Manager:
  Microsoft .NET Framework 4.5.2 or later

  Email Signature Manager Agent:
  Microsoft .NET Framework 4.5.2 or later

  Email Signature Manager Transport Agent:
  Microsoft .NET Framework 4.5.2 or later

- System hardware:
  Email Signature Manager:
  CPU and memory requirements for operating system
  200MB free hard-disk space plus 5MB per 100 users for database
  1024 x 768 screen resolution

  Email Signature Manager Agent:
  CPU and memory requirements for operating system
  2MB free hard-disk space

  Email Signature Manager Transport Agent:
  CPU and memory requirements for operating system
  40MB free hard-disk space

Introduction 1

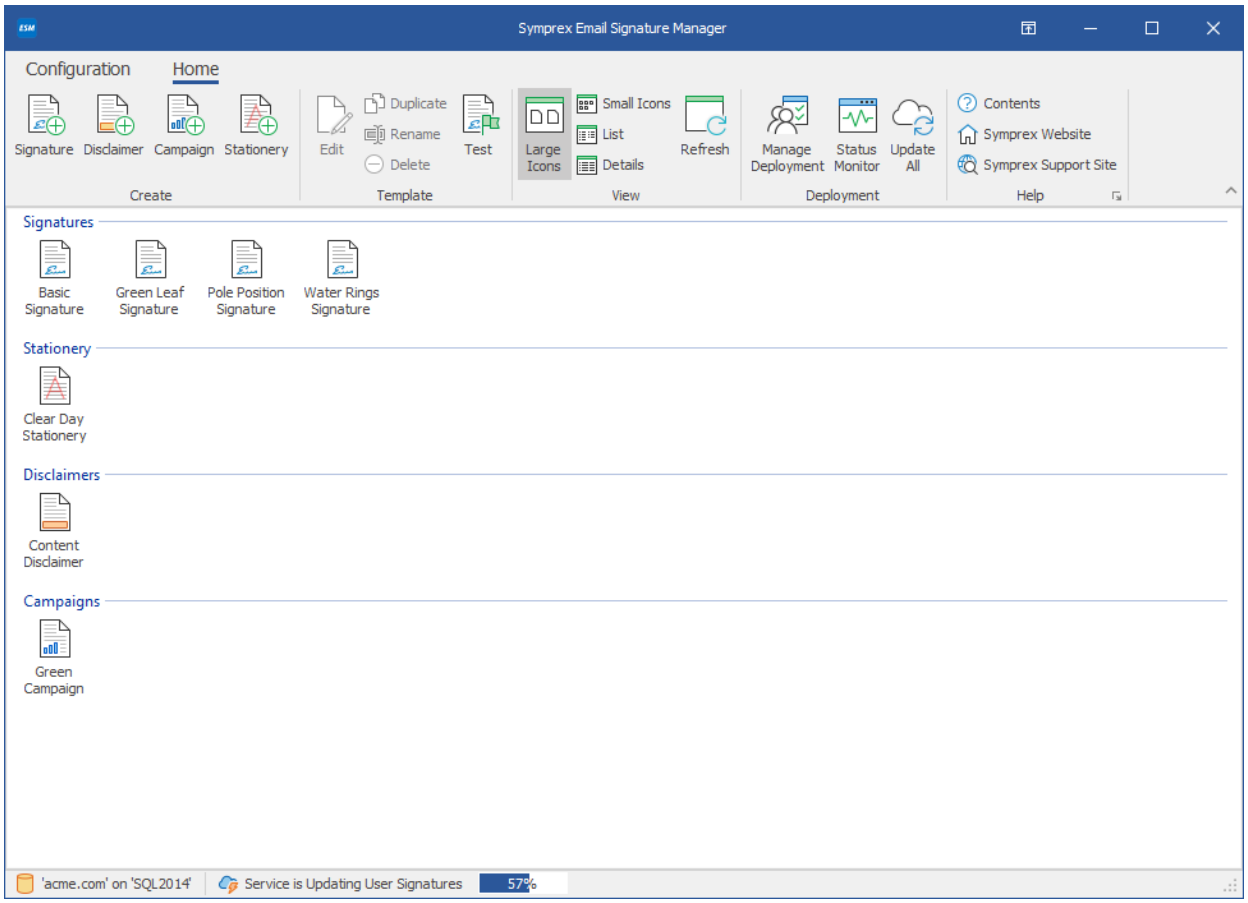
Email Signature Manager Overview

For an introduction to Email Signature Manager including solution benefits, features and how to get started, please see the general introduction.

Easy to Use

The Email Signature Manager user interface is designed in accordance with current Microsoft guidelines for Microsoft Office applications. The main application window is divided into a top ribbon for accessing all of the commands, a work area in the middle for managing and editing templates, a status bar at the bottom, and a backstage for accessing configuration and tools.

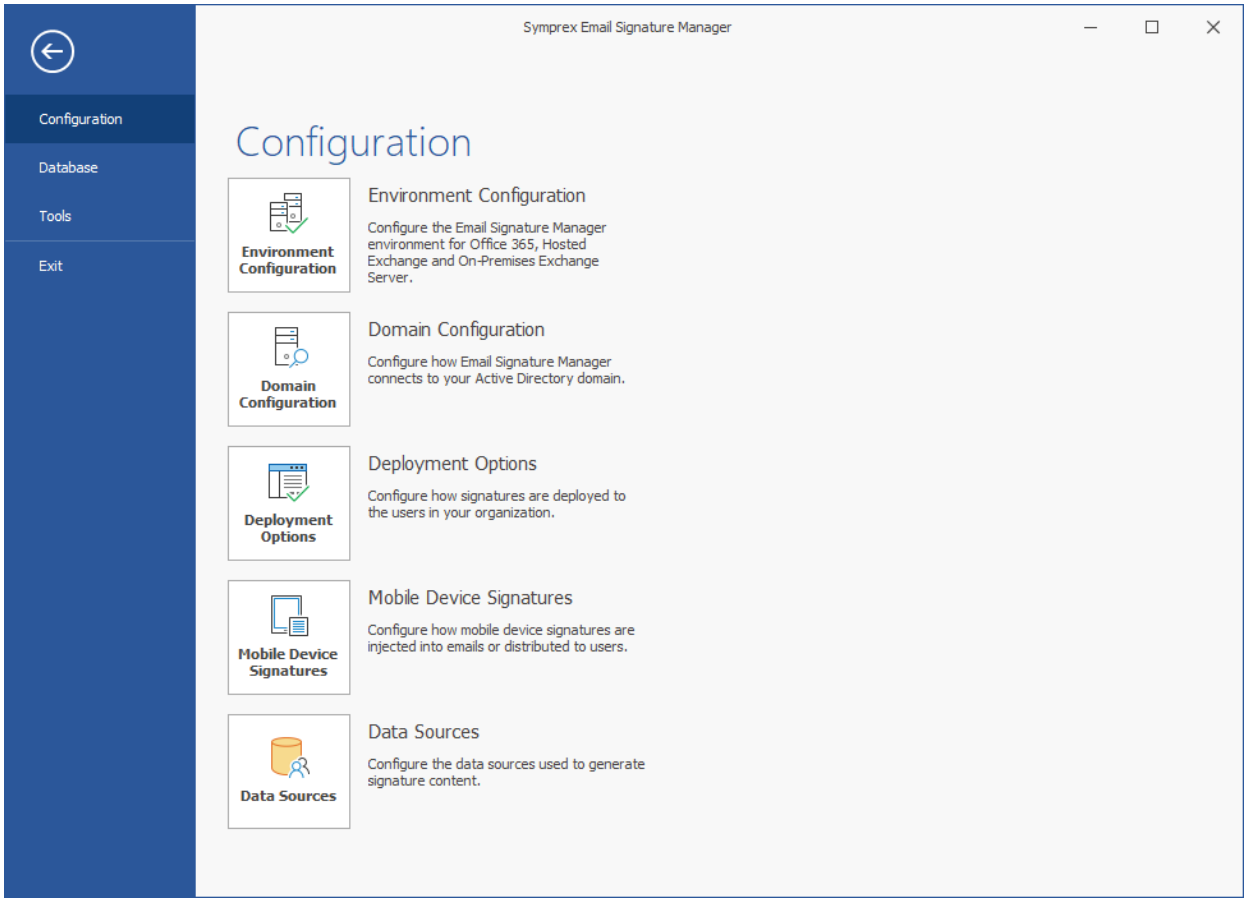
The main application is shown below with the **Home** ribbon tab selected:



The main application is shown below with the **Configuration** ribbon tab selected:

Introduction

1



With a user interface that works in the same way as current and recent versions of Microsoft Office applications, Email Signature Manager is intuitive and easy to use.

Central Management

All aspects of the Email Signature Manager solution are managed from within the graphical user interface of the main application. This is where you for example create, design and test your email signature templates, manage deployment to groups and users, and verify deployment results in the status monitor. The solution includes a service, which is responsible for generating signatures for Outlook, OWA and mobile devices by merging data from Active Directory (or custom data sources) with the signature templates including any disclaimers and campaigns.

Simple Deployment

Deployment of Outlook signatures is seamlessly performed by the Email Signature Manager Agent, a small executable that runs on each user's computer. The Agent can either be started from a network share from a logon script, or installed using for example Group Policy. Further, the Agent can be configured to update Outlook signatures at logon only, or to stay running in the background and update Outlook signatures continuously. The Agent works whether users log on to the domain or not.

The Outlook signatures are generated by the Email Signature Manager Service that is installed with Email Signature Manager. This service is also responsible for seamless deployment of OWA signatures and

generation of mobile device signatures. OWA signatures automatically work in the OWA App for mobile devices on Office 365, and signatures can be injected into emails sent from mobile devices by the optional Email Signature Manager Transport Agent when using On-Premises Exchange Server.

Powerful Built-in Template Editor

Email Signature Manager offers a powerful built-in template editor for designing and editing email signature, disclaimer and campaign templates.

A template consists of the following information:

- Basic properties, such as name, description and data source.
- HTML and Plain Text templates with dynamic fields (which are merged with the data source) and conditional statements (to control when content appears in the signature).
- Optional client settings, such as default fonts and other settings.
- Template specific properties such as start and end date for campaigns.

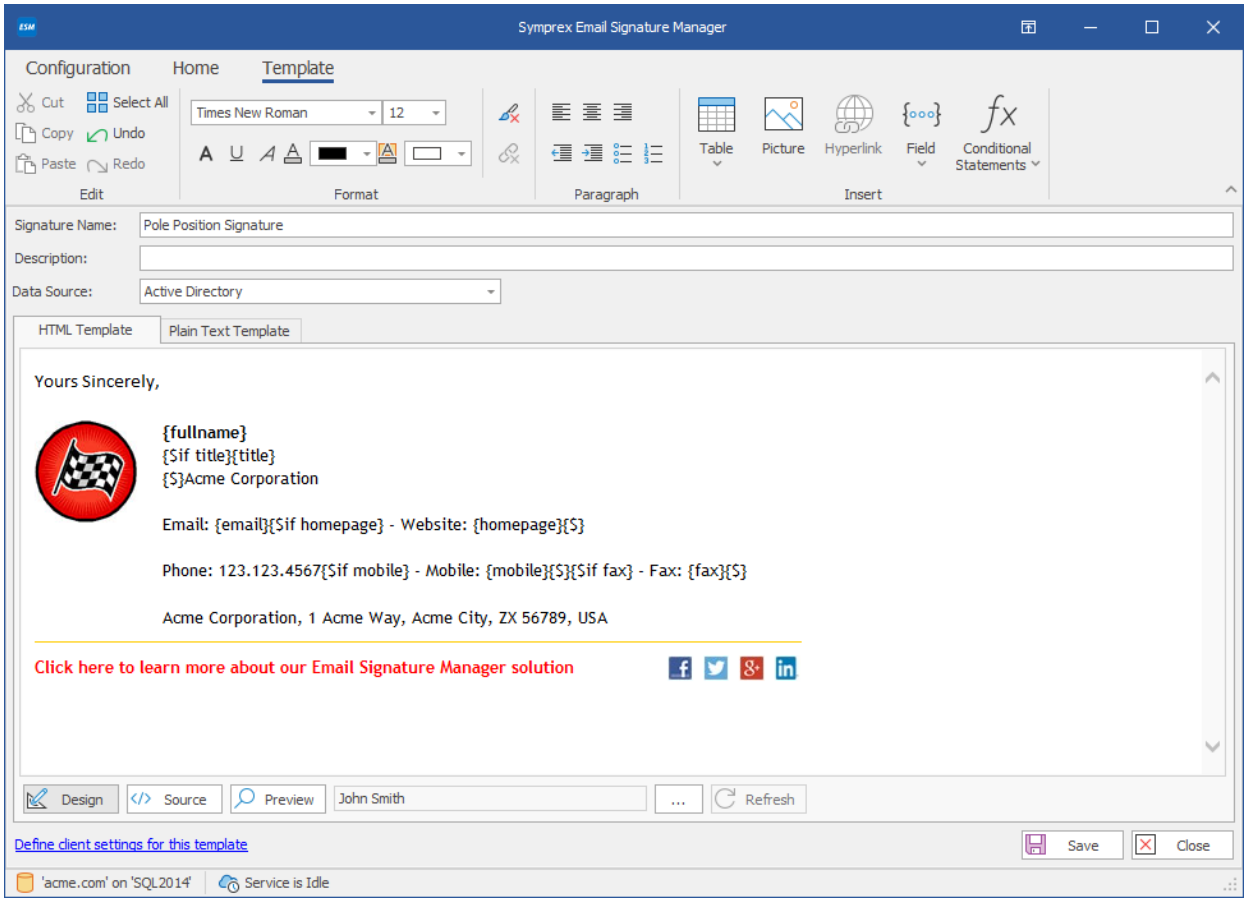
Note RTF signatures are generated automatically from HTML signatures.

When editing HTML templates the editor offers a Design, Source and Preview mode for WYSIWYG editing, HTML code editing (syntax color-coded), and previewing the template merged with user data.

The built-in template editor is shown below in **Design** mode for WYSIWYG editing:

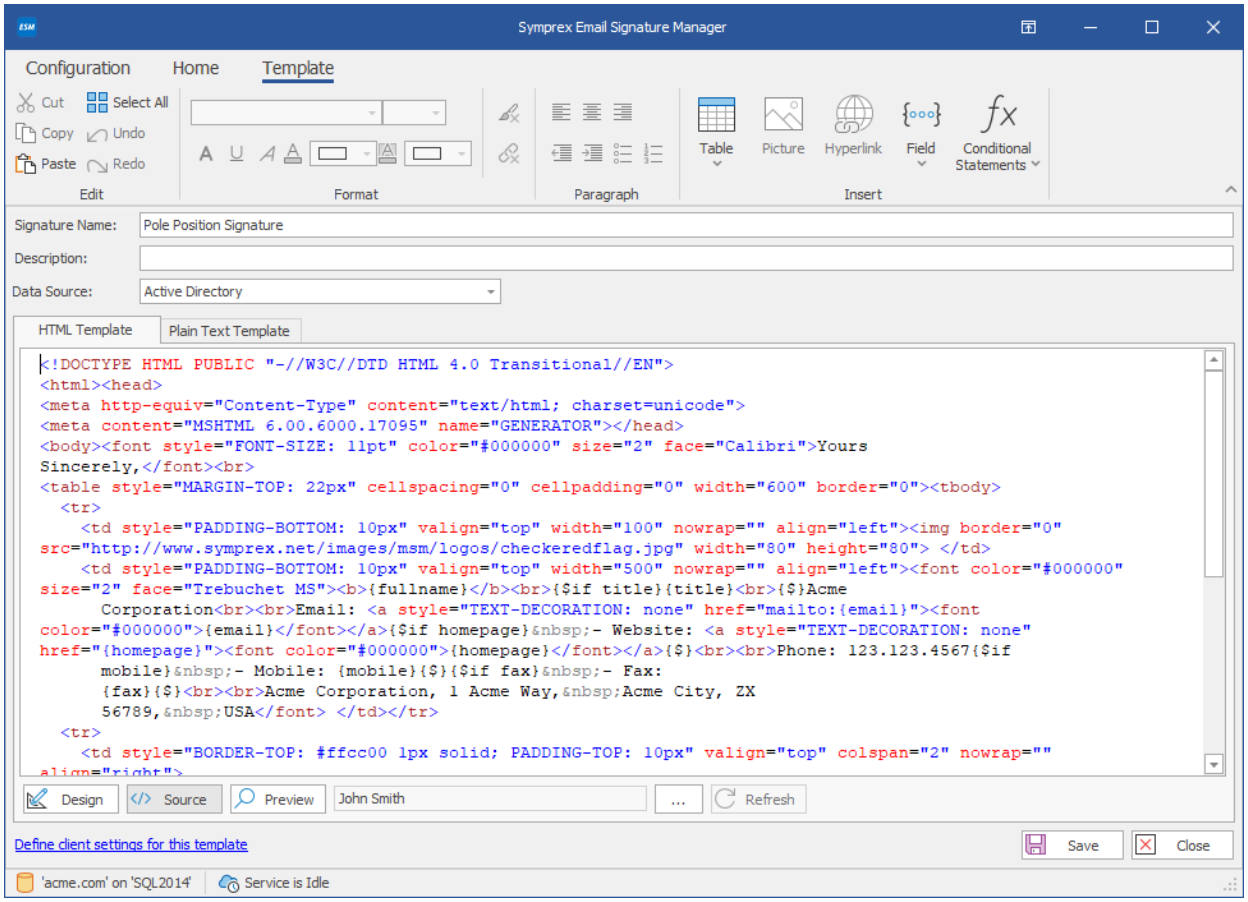
Introduction

1



The built-in template editor is shown below in **Source** mode for source editing:

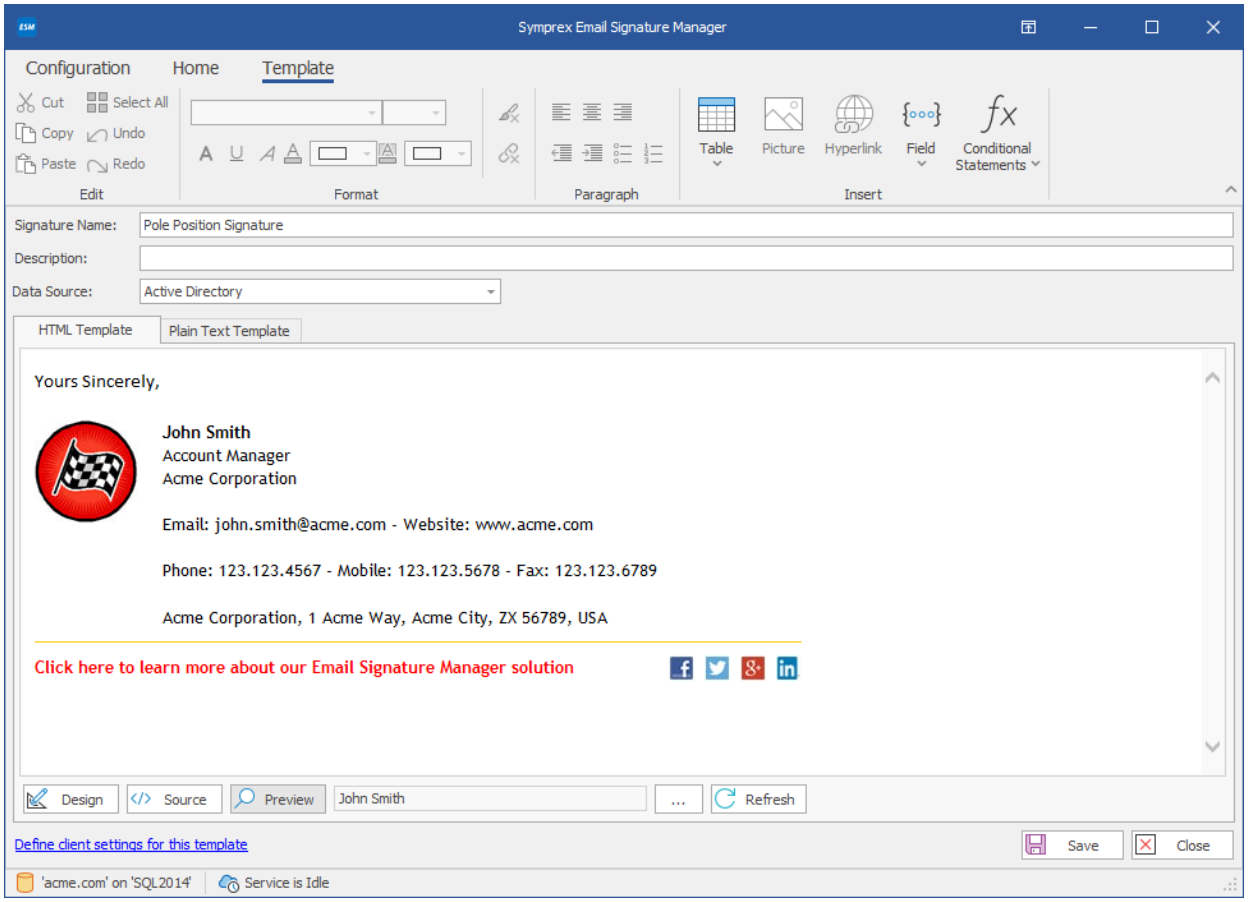
Introduction 1



The built-in template editor is shown below in **Preview** mode merging template with user data:

Introduction

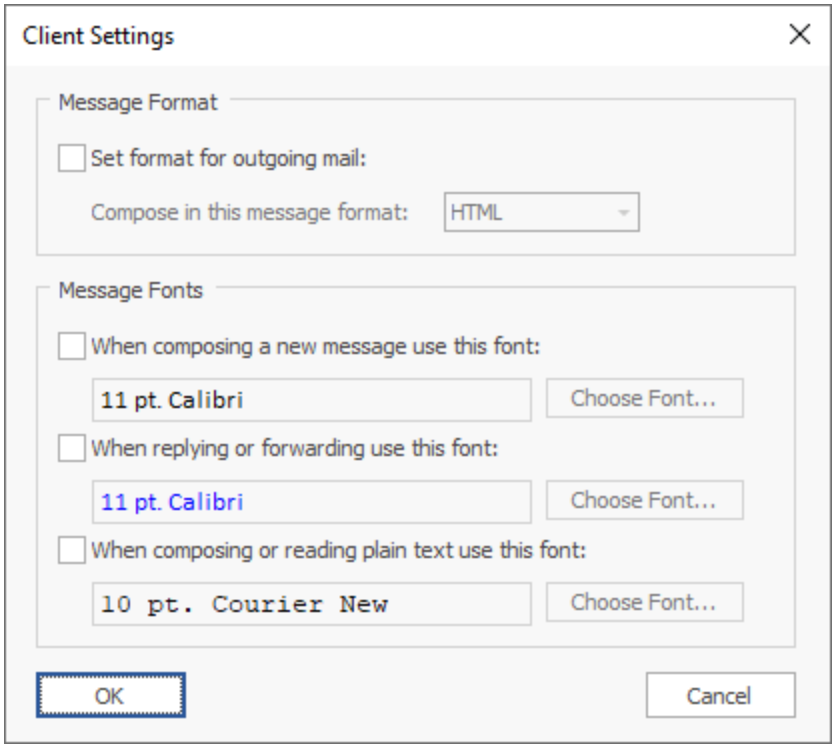
1



Client Settings

A signature template can optionally include a set of client settings to control default message format and fonts using the Client Settings dialog from within the template editor:

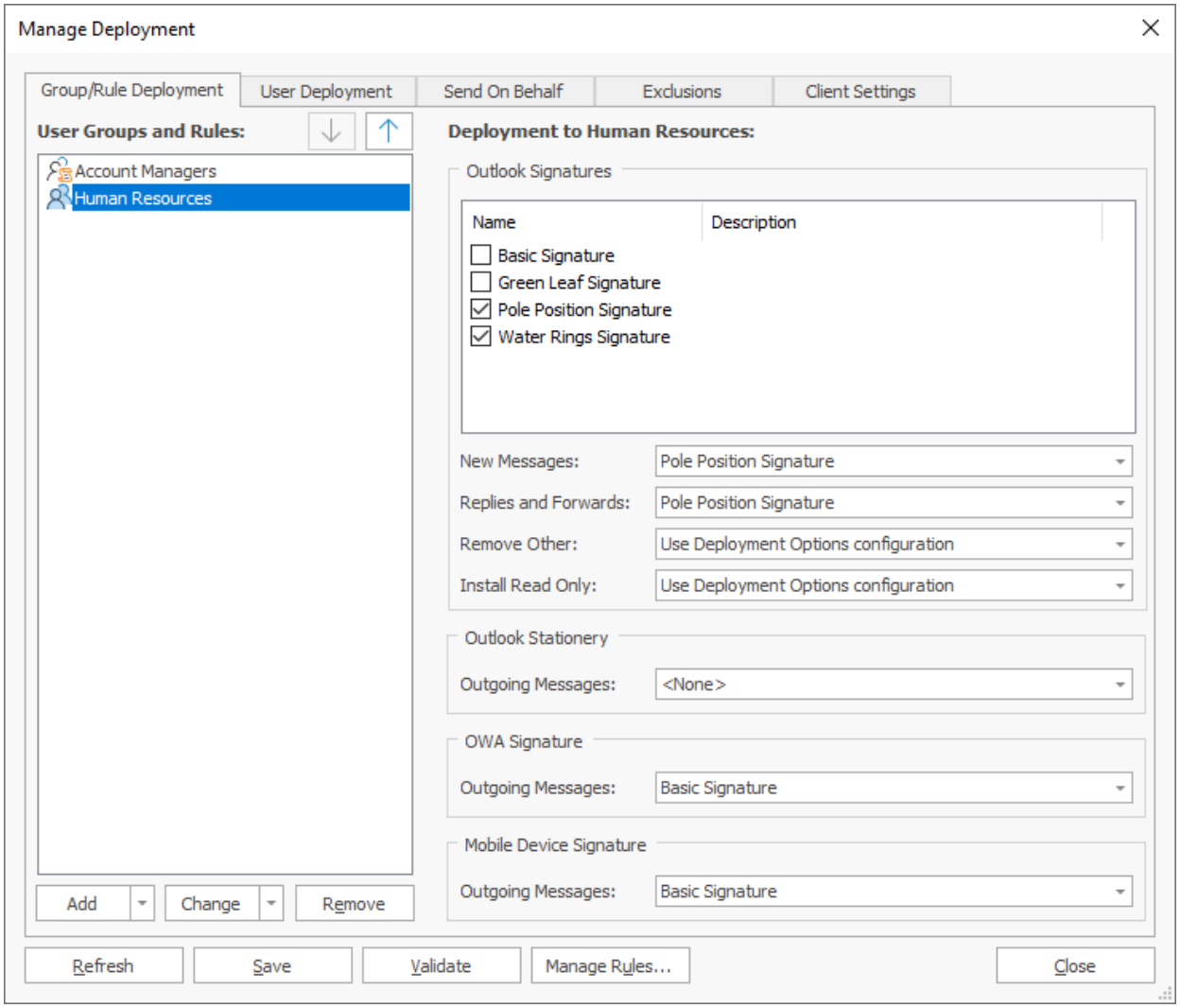
Introduction 1



Client Settings can also be defined on a global level so that they are applied automatically when any signature is installed.

Easy Deployment Configuration

Configuring how users in your organization will receive signatures is simple using the Manage Deployment dialog:

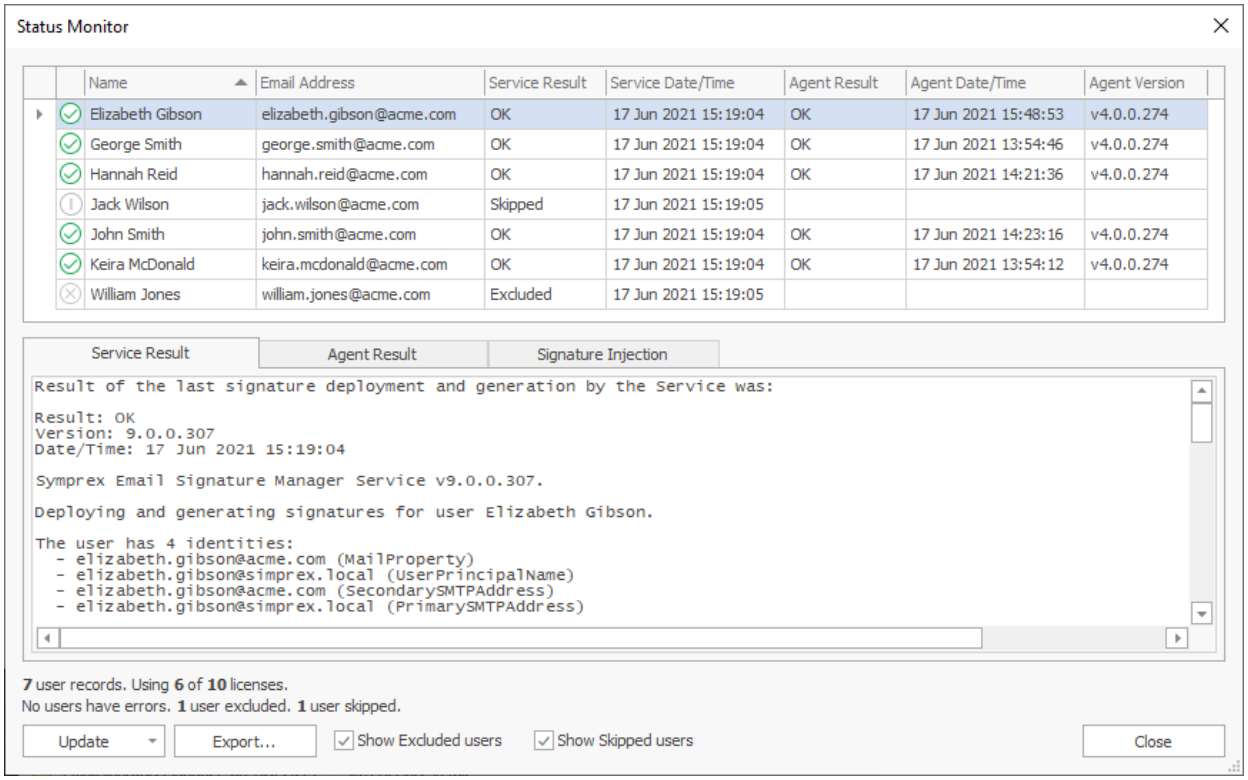


Deployment can be specified either by group membership or by individual user, and signatures can also be deployed for users who send emails on behalf of other users in your organization.

Powerful Status Monitor

Reviewing signature deployment results is easy using the Status Monitor dialog:

Introduction 1



The list of users can be sorted for example by status, name or last service our agent deployment date/time. It is also possible to jump directly to any user by searching for example by name or email address. Finally the deployment to users can be updated immediately.

How Email Signature Manager Works

Email Signature Manager comprises the following components:

- **Main Application** for managing signatures, and configuring and monitoring deployment.
- **Database** holding settings, templates, deployment configuration and status information.
- **Service** responsible for generation and deployment of user signatures.
- **Client Access Service** used by the Agent and Transport Agent to fetch signature settings from the database.
- **Agent** for updating Outlook signatures on each user's computer.
- **Transport Agent** (optional) for Exchange Server for injecting signatures into emails sent from mobile devices.

The **Database**, **Service** and **Client Access Service** are installed with the **Main Application** when performing a **Full Installation** of Email Signature Manager.

The following steps are used to deploy signatures to the users in your organization:

- Using the **Email Signature Manager Main Application**, your environment is configured. This tells Email Signature Manager how Exchange is deployed across your organization, and optionally, is used to

specify the service accounts that are used to update the mailboxes on Exchange Server and Office 365.

- Using the WYSIWYG editor, the signature templates are designed. The templates use dynamic fields and conditional statements that are evaluated during deployment to produce signatures that are specific to each user (e.g. the signature can contain for example each user's name, email address and direct dial number) but standardized across your organization.

- Once the templates are designed and tested, the main application is used to specify how signatures are deployed to the users in your organization. Deployment can be specified either by group membership or for individual users. The main application is also used to set certain deployment options that control how signatures are installed to Outlook on your users' computers.

- With signature design completed and deployment configured, the **Email Signature Manager Service** performs three core functions:

  - Generates Outlook signatures and stores them in the database, and also writes them to each user's mailbox.
  - Deploys OWA signatures to each user's mailbox.
  - Generates mobile device signatures, to be injected into emails sent from mobile devices, and stores them in the database.

- The **Email Signature Manager Agent** runs on each user's computer to fetch the pre-generated signatures and deploy them to Outlook. The Agent normally connects to the **Email Signature Manager Client Access Service** to fetch the signatures, but it can also fetch them from the user's mailbox when running off domain. The Agent can be started from a network share from a logon script, or installed using for example Group Policy. Further information about the Agent can be found in this topic and about the Client Access Service in this topic.

- If the users in your organization use their mobile devices to send emails via your On-Premises Exchange Server, the **Email Signature Manager Transport Agent** is used to inject the appropriate pre-generated signatures into those emails during delivery. The Transport Agent knows where to inject the signature based on a set of rules. Further information about the Transport Agent can be found in this topic.

Note The Email Signature Manager Transport Agent can normally only be used in conjunction with On-Premises Exchange Server, although some Hosted Exchange providers may allow the Transport Agent to be installed. The Transport Agent cannot be used with Office 365, but OWA signatures will automatically work in the OWA App for Android and iOS platforms.

Installing Email Signature Manager

Before installing Email Signature Manager, if you have not already done so, it is recommended to review how the product works, and then proceed as appropriate to:

- Perform a new installation
- Upgrade an existing installation

Introduction 1

New Installations of Email Signature Manager

Each installation of Email Signature Manager requires one instance of a **Full Installation** of the product, which comprises the following components:

- The Email Signature Manager main application.
- The Email Signature Manager Service.
- The Email Signature Manager Client Access Service.
- The Built-in Database.

For details of what each component does, please refer to the topic on how the product works.

The steps to install Email Signature Manager depend on your Exchange environment:

- On-Premises Exchange Server
- Office 365
- Office 365 and On-Premises Exchange Server
- Hosted Exchange
- Hosted Exchange and On-Premises Exchange Server
- Exchange Server without Impersonation or Other Email Platform

Installing for On-Premises Exchange Server

This topic describes the steps for installing Email Signature Manager in an organization that uses On-Premises Exchange Server:

1. Create the service account on your On-Premises Exchange Server for Email Signature Manager to use to access mailboxes in your organization.

2. Review the guidance on throttling policies for Exchange Server 2010 and higher.

3. Perform a **Full Installation** of Email Signature Manager on to a suitable Windows Server.

4. Complete the post-installation tasks to configure Email Signature Manager.

Installing for Office 365

This topic describes the steps for installing Email Signature Manager in an organization that uses Office 365:

1. Create the service account on Office 365 for Email Signature Manager to use to access mailboxes in your organization.

2. Perform a **Full Installation** of Email Signature Manager on to a suitable Windows Server.

3. Complete the post-installation tasks to configure Email Signature Manager.

Installing for Office 365 and On-Premises Exchange Server

This topic describes the steps for installing Email Signature Manager in an organization that uses a mixed Office 365 and On-Premises Exchange Server environment:

1. Create the service account on your On-Premises Exchange Server for Email Signature Manager to use to access mailboxes in your organization.
2. Review the guidance on throttling policies for Exchange Server 2010 and higher.
3. Create the service account on Office 365 for Email Signature Manager to use to access mailboxes in your organization.
4. Perform a **Full Installation** of Email Signature Manager on to a suitable Windows Server.
5. Complete the post-installation tasks to configure Email Signature Manager.

Installing for Hosted Exchange

This topic describes the steps for installing Email Signature Manager in an organization that uses Hosted (Off-Premises) Exchange:

1. Contact your Exchange hosting provider and ask them to create the service account within their Exchange platform for Email Signature Manager to use to access mailboxes in your organization.
2. Perform a **Full Installation** of Email Signature Manager on to a suitable Windows Server.
3. Complete the post-installation tasks to configure Email Signature Manager.

Installing for Hosted Exchange and On-Premises Exchange Server

This topic describes the steps for installing Email Signature Manager in an organization that uses a mixed Hosted Exchange and On-Premises Exchange Server environment:

1. Contact your Exchange hosting provider and ask them to create the service account within their Exchange platform for Email Signature Manager to use to access mailboxes in your organization.
2. Create the service account on your On-Premises Exchange Server for Email Signature Manager to use to access mailboxes in your organization.
3. Review the guidance on throttling policies for Exchange Server 2010 and higher.
4. Perform a **Full Installation** of Email Signature Manager on to a suitable Windows Server.
5. Complete the post-installation tasks to configure Email Signature Manager.

Installing without Impersonation Account

This topic describes the steps for installing Email Signature Manager without an impersonation account (for example, due to security restrictions imposed by a hosted Exchange provider):

1. Perform a **Full Installation** of Email Signature Manager on to a suitable Windows Server.

2. Complete the post-installation tasks to configure Email Signature Manager.

Note that when installing without an impersonation account, the following restrictions apply:

- OWA signatures will not be deployed.
- Automatic support for Outlook signatures for remote users will not work.

Post Installation Tasks

Having performed a **Full Installation** of Email Signature Manager, start the main application and complete Product Configuration Wizard as follows:

1. On the **Introduction** page, click the **Next** button.

2. On the **Installation Type** page, select **New Installation** and click the **Next** button.

3. On the **New Installation** page, select the **Type** and **Built-In Database** and click the **Next** button.

4. On the **Database Connection Established** page, click the **Next** button.

5. On the **Environment Configuration** page, it is recommended that you select **Configure Environment Now** to complete the configuration of Email Signature Manager for your type of Exchange environment; however, this step can be skipped and completed at a later stage. When you have selected the appropriate option, click the **Next** button.

6. If you selected the **Configure Environment Now** option, the Environment Configuration dialog will be opened. Select the appropriate option that describes your Exchange environment and enter the details of the service accounts; it is recommended to use the **Test** button to ensure that each account has been properly configured. Click the **OK** button to proceed to the final step of the wizard or the **Cancel** button to return to the **Environment Configuration** page of the wizard.

7. The **Finished** page of the wizard will report on the current configuration of the product. Click the **Finish** button to close the wizard.

After the wizard has been completed, you are ready to configure the product to deploy signatures to the users in your organization:

1. To get started, you can use one of the example signature templates that are included with the product or you can use the WYSIWYG editor to create your own.

2. Using the Manage Deployment dialog, specify which users will receive signatures.

3. The service now has everything that it needs to generate the signatures for Outlook and to deploy signatures to OWA, so click the **Update Now** button in the ribbon.

4. Use the Status Monitor dialog to verify that the service is working.

5. Arrange for the **Email Signature Manager Agent** to be executed on your end users' computers. There are a number of ways of achieving this; please refer to this topic.

Congratulations! You have now completed the basic configuration of the product and can start to deploy email signatures to your users.

Other post-installation tasks that you may wish to complete are:

- Optionally, migrate the database to SQL Server if you wish to use the **Email Signature Manager Transport Agent** to inject signatures into emails sent from mobile devices, or if you wish to be able to manage your Email Signature Manager installation from multiple computers.

- Optionally, install the Transport Agent to inject signatures into emails sent from mobile devices.

Upgrading Email Signature Manager

Before upgrading Email Signature Manager, it is recommended that you first read how the product works and then use the following the instructions in the appropriate topic to upgrade your installation:

- Upgrading v7.x and later
- Upgrading from v5.x or v6.x
- Upgrading from v4.x or earlier

Upgrading v7.x and Later

Upgrading an installation of v7.x or later is very simple:

1. Using the new installer, upgrade the computer where the **Full Installation** has been made (i.e. the machine where the Email Signature Manager Service is located).

2. Run Email Signature Manager in the upgraded full installation; this will upgrade the database if necessary.

3. Using the new installer, upgrade any other computers where there is a **Manager-Only** installation.

The **Email Signature Manager Agent** has its own version numbering system, and new versions of the Agent can be released independently of the main application; hence, there may not necessarily be a new version of the Agent to match a new version of the main application, and vice versa. How the Agent is upgraded will depend on how it has been deployed in your organization:

- If you are starting the Agent via a logon script from a shared folder, the new version simply needs to be copied to the folder.

- If you are using GPO, please follow the upgrade instructions in the Group Policy topic.

- If you are using ClickOnce, then the Agent can be updated using the **Check Now** button in the **Software Updates** group on the **Options** dialog.

Note It is recommended to use v4.0 or higher of the Agent with this version of Email Signature Manager.

Introduction 1

The optional **Email Signature Manager Transport Agent** is always released in step with the main application. It is not strictly necessary to upgrade the Transport Agent as all major releases are compatible with the matching major version of the main application (for example, v9.0 of the Transport Agent will be compatible with v9.1 of the main application). However, it is recommended to keep the Transport Agent up-to-date with the main application when convenient to do so. The Transport Agent is upgraded by simply running the installer for the new version. When moving to a newer major version of Email Signature Manager, the Transport Agent **must** be updated.

To complete the upgrade of the **Email Signature Manager Transport Agent**, it is necessary to restart the Exchange Transport Service, which is responsible for delivering email. It is therefore recommended that you plan to upgrade at a quiet time. The installer can automatically restart the Exchange Transport Service or you can manually restart the service.

Upgrading from v5.x and v6.x

There are a number of key changes between v5.x/v6.x and v9.x, as follows:

- The Deployment Tool (`sign.exe`) has been replaced by a new **Email Signature Manager Agent** that runs on users' computers seamlessly updating Outlook signatures at configured intervals. The new Agent gets signature settings from the Client Access Service or, in the case of remote users, from the user's mailbox using Exchange Web Services.
- The Access database (`settings.mdb`) has been replaced by a new **Built-in Database** that can scale to any number of users and which does not require sharing on a network share.
- The **Email Signature Manager Service** is now a core component of the product and is automatically installed/upgraded when installing Email Signature Manager. The new service always runs under the **Local System** account. The service account(s) for mailbox access are configured in a new **Environment Configuration** dialog.

You should upgrade from v5.x and v6.x using following these steps:

1. Determine the type of database you are presently using (open the **Settings Database** dialog) and complete the appropriate step:

   ➔ If you are using an Access database (typically, `settings.mdb`), move it from its current location (i.e. the shared folder) to a secure location and take a backup copy.
   ➔ If you are using SQL Server, take a full backup.

2. Determine how the old Deployment Tool (`sign.exe`) is currently executed by the users in your organization and complete the appropriate step:

   ➔ If you are running it from a logon script, remove the call to it from that logon script and delete `sign.exe` from your shared folder.
   ➔ If you are using GPO to deploy it using the MSI package, delete the GPO that installs it (this will ensure that it is uninstalled when your users logon to their machines).

3. If you are currently running the service in conjunction with On-Premises Exchange Server, review the permissions required by the service account according to your version of Exchange Server.

4. One server (and one server only) in your organization will need to have a **Full Installation** of the product. It is therefore recommended that you determine if the **Email Signature Manager Service** is

already installed within organization and then **either**:

➔ Perform a **Full Installation** on the server where the service is already installed; the installer will automatically upgrade both the main application and the service (i.e. there is no need to uninstall anything first), **or**
➔ Uninstall the previous version of the main application and service from the current server, and then install perform a **Full Installation** on a new server.

5. Complete the upgrade process.

Upgrading from v4.x and Earlier

There are a number of key changes between v4.x and earlier, and v9.x, as follows:

- The Deployment Tool (`sign.exe`) has been replaced by a new **Email Signature Manager Agent** that runs on users' computers seamlessly updating Outlook signatures at configured intervals. The new Agent gets signature settings from the Client Access Service or, in the case of remote users, from the user's mailbox using Exchange Web Services.
- The Access database (`settings.mdb`) has been replaced by a new **Built-in Database** that can scale to any number of users and which does not require sharing on a network share.
- A new **Email Signature Manager Service** is now responsible for generating Outlook signatures and deploying OWA signatures to users' mailboxes using EWS. In addition it also generates signatures for use by the new **Email Signature Manager Transport Agent** to inject into emails sent from mobile devices when using On-Premises Exchange Server.

You should upgrade from v4.x and earlier using following these steps:

1. Determine the type of database you are presently using (open the **Settings Database** dialog) and complete the appropriate step:

   ➔ If you are using an Access database (typically, `settings.mdb`), move it from its current location (i.e. the shared folder) to a secure location and take a backup copy.
   ➔ If you are using SQL Server, take a full backup.

2. Determine how the old Deployment Tool (`sign.exe`) is currently executed by the users in your organization and complete the appropriate step:

   ➔ If you are running it from a logon script, remove the call to it from that logon script and delete `sign.exe` from your shared folder.
   ➔ If you are using GPO to deploy it using the MSI package, delete the GPO that installs it (this will ensure that it is uninstalled when your users logon to their machines).

3. Uninstall the current version using Windows Control Panel. When prompted, you should remove the current database (make sure to backup the database first) and settings.

4. Create a service account for use with the new **Email Signature Manager Service**.

5. One server (and one server only) in your organization will need to have a **Full Installation** of the product.

6. Complete the upgrade process.

Completing the Upgrade

Having performed a Full Installation of Email Signature Manager, start the main application and complete Product Configuration Wizard as follows:

1. On the **Introduction** page, click the **Next** button.

2. On the **Installation Type** page, select **Existing Installation** and click the **Next** button.

3. On the **Existing Installation** page, choose either to import your old settings database or upgrade your existing SQL Server database as appropriate, and click the **Next** button.

   ➔ If you are importing an Access database, then select it on the **Import Access Database** page and click the **Next** button.
   ➔ If you are upgrading an existing SQL Server database, enter the details on the **Upgrade SQL Server Database** page and click the **Next** button (note SQL Server Authentication is required; please read the **Dedicated Login** section in this topic for more information).

4. On the **Database Connection Established** page, click the **Next** button.

5. On the **Environment Configuration** page, it is recommended that you select **Configure Environment Now** to complete the configuration of Email Signature Manager for your type of Exchange environment; however, this step can be skipped and completed at a later stage. When you have selected the appropriate option, click the **Next** button.

6. If you selected the **Configure Environment Now** option, the Environment Configuration dialog will be opened and where possible, the wizard will have migrated any previous configuration. If necessary, select the appropriate option that describes your Exchange environment and enter the details of the service account(s) as required; it is recommended to use the **Test** button to ensure that each account has been properly configured. Click the **OK** button to proceed to the final step of the wizard or the **Cancel** button to return to the **Environment Configuration** page of the wizard.

7. The **Finished** page of the wizard will report on the current configuration of the product. Click the **Finish** button to close the wizard.

8. If you are using **Email Signature Manager Transport Agent**, upgrade each server where it is installed.

Note If you are using v5.x of the Transport Agent, the installers for 2007/10 and 2013 have been unified into a single installer that supports all Exchange Server versions. In addition, the Exchange Transport Service must be restarted to complete the upgrade; the installer can do this automatically or you can manually restart the service.

After the wizard has been completed, your existing signatures and deployment configuration should now be available and if the Exchange environment has been configured, the **Email Signature Manager Service** will start to deploy and generate signatures. You can now complete the upgrade using the following steps:

1. Use the Status Monitor dialog to verify that the service is working.

2. Arrange for the new **Email Signature Manager Agent** to be executed on your end users' computers. There are a number of ways of achieving this; please refer to this topic.

Congratulations! You have now completed the upgrade of the product and the users in your organization should have signatures deployed just as they did with your previous version.

Other post-installation tasks that you may wish to complete are:

- The **Email Signature Manager Transport Agent** can be used to inject signatures into email sent from mobile devices when using On-Premises Exchange Server; please refer to this topic.

- From v7.0 upwards, it is not possible to share the Built-in Database. Therefore, if you wish to manage the database from multiple computers, you need to migrate to SQL Server if you are presently using the built-in (Access) database, and then you can perform a **Manager Only** installation of the product on the appropriate computers; please refer to this topic for more information.

Service Accounts

In order for the Email Signature Manager Service to be able to write Outlook signatures and deploy OWA signatures to user mailboxes, using Exchange Web Services (EWS), it is necessary to create an appropriate service account on Exchange Server. The details of this account (or accounts if you have a hybrid environment) are then entered in the Environment Configuration dialog.

- If you are using On-Premises Exchange Server, create an account using Active Directory User and Computers on a domain controller and then assign it the appropriate rights depending on the version of Exchange Server you are using:

  ➔ On Exchange Server 2016 and 2019.
  ➔ On Exchange Server 2013.

  In addition, please read this topic on Exchange Server Throttling Policies.

- If you are using Hosted Exchange, you will need to contact your hosting provider and ask them to create an account with the appropriate permissions.

- If you are using Office 365, please read this topic to create the account through the administration portal.

Note If you have selected the **Exchange without Impersonation Account** option in the **Environment Configuration** dialog, then you do not need to create any service accounts. However, selecting this option, OWA signatures will not be deployed, and automatic support for Outlook signatures for remote users will not work.

Permissions for the Service Account on Exchange Server 2016 and 2019

Permissions requirements for the service account on Exchange Server 2016 and 2019 are:

- **Application Impersonation**

To assign the service account the required Exchange Server permissions, follow these steps:

1. Open the **Exchange Management Shell** and connect to Exchange Server.
2. Type the following line, and then press **ENTER**:

   ```
   New-ManagementRoleAssignment -Role ApplicationImpersonation -User <Account>
   ```

   where <*Account*> is the name of the service account to which the required role will be assigned.

Permissions for the Service Account on Exchange Server 2013

Permissions requirements for the service account on Exchange Server 2013 are:

- **Application Impersonation**

To assign the service account the required Exchange Server permissions, follow these steps:

1. Open the **Exchange Management Shell** and connect to Exchange Server.
2. Type the following line, and then press **ENTER**:

   ```
   New-ManagementRoleAssignment -Role ApplicationImpersonation -User <Account>
   ```

   where <*Account*> is the name of the service account to which the required role will be assigned.

Note In v5.x of Email Signature Manager the required permissions were:

- **Receive-As**

These permissions can be removed from the service account.

Exchange Server Client Throttling Policies

In order for the Email Signature Manager Service to function correctly on Exchange Server 2010 and higher, it is necessary to disable client throttling for the service account. This can be accomplished as follows:

1. Open the **Exchange Management Shell** and connect to Exchange Server.
2. Type the following command:

   ```
   New-ThrottlingPolicy <Policy>
   ```

   where `<Policy>` is a suitable, unique name for the policy (for example, `ESMServiceAccountPolicy`)

3. On **Exchange Server 2010 (SP3 and higher)**, type the following command:

   ```
   Set-ThrottlingPolicy <Policy> -EWSFastSearchTimeoutInSeconds $null -EWSFindCountLimit
   $null -EWSMaxConcurrency $null -EWSMaxSubscriptions $null -EWSPercentTimeInAD $null -
   ```

```
EWSPercentTimeInCAS $null -EWSPercentTimeInMailboxRPC $null
```

4. On **Exchange Server 2013**, **Exchange Server 2016** and **Exchange Server 2019**, type the following command:

```
Set-ThrottlingPolicy <Policy> -EwsCutoffBalance Unlimited -EwsMaxBurst Unlimited -
EwsMaxConcurrency Unlimited -EwsMaxSubscriptions Unlimited -EwsRechargeRate Unlimited
-IsServiceAccount:$true
```

5. Type the following command:

```
Set-ThrottlingPolicyAssociation -ThrottlingPolicy <Policy> -Identity <Account>
```

   where `<Policy>` is the name of the policy and `<Account>` is the name of the service account to which the policy will be assigned.

Note Changes to client throttling policies will not be applied immediately on your Exchange Server; please allow some time for the changes to become effective.

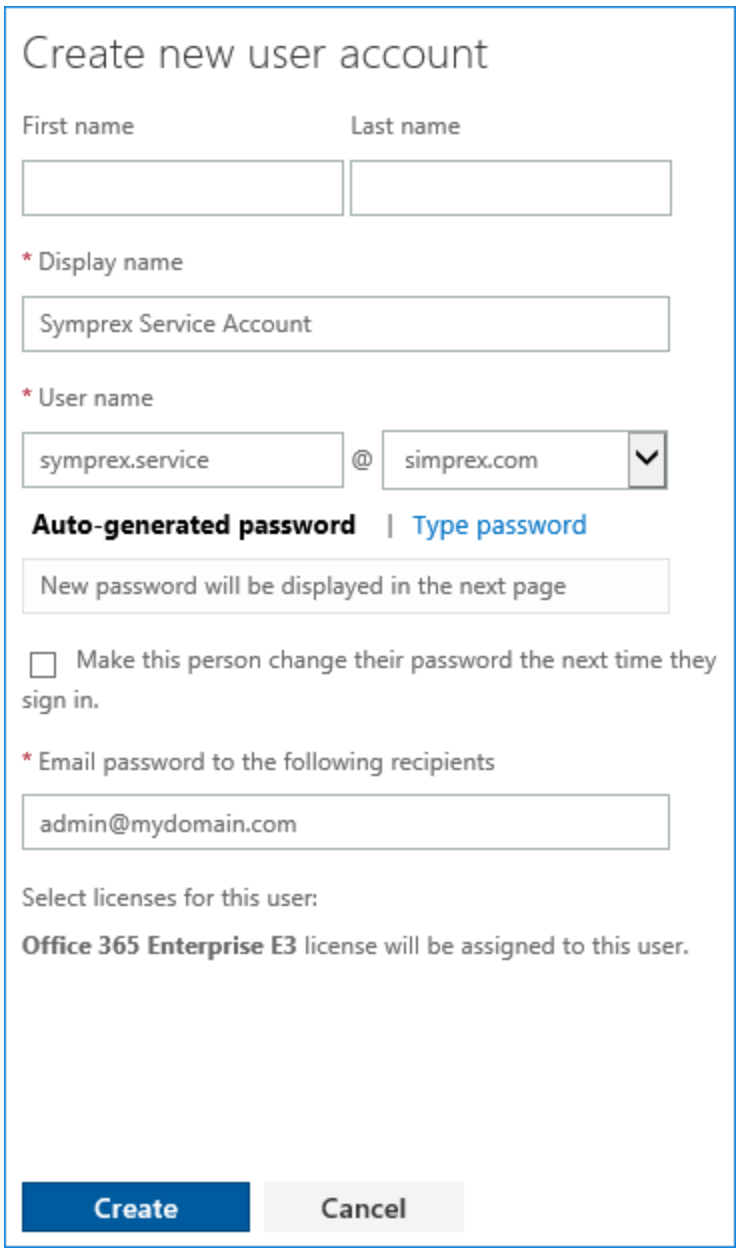
Creating the Service Account on Office 365

When deploying signatures to Office 365, Email Signature Manager requires a service account assigned to the *Application Impersonation* role. This account can be created using the Office 365 administration portal as follows:

1. Log on to Office 365 as an administrative account.

2. Select **Active Users** in the **USERS** node of the tree on the left side of the page, and then click the add symbol (+) on the **Active Users** list page to add a new user.

3. In the **Create new user account** popup, enter a suitable **Display Name** and **User Name**, configure the password according to your password policy, and ensure that the **Make this person change their password the next time they sign in option** is not checked. Here is an example:



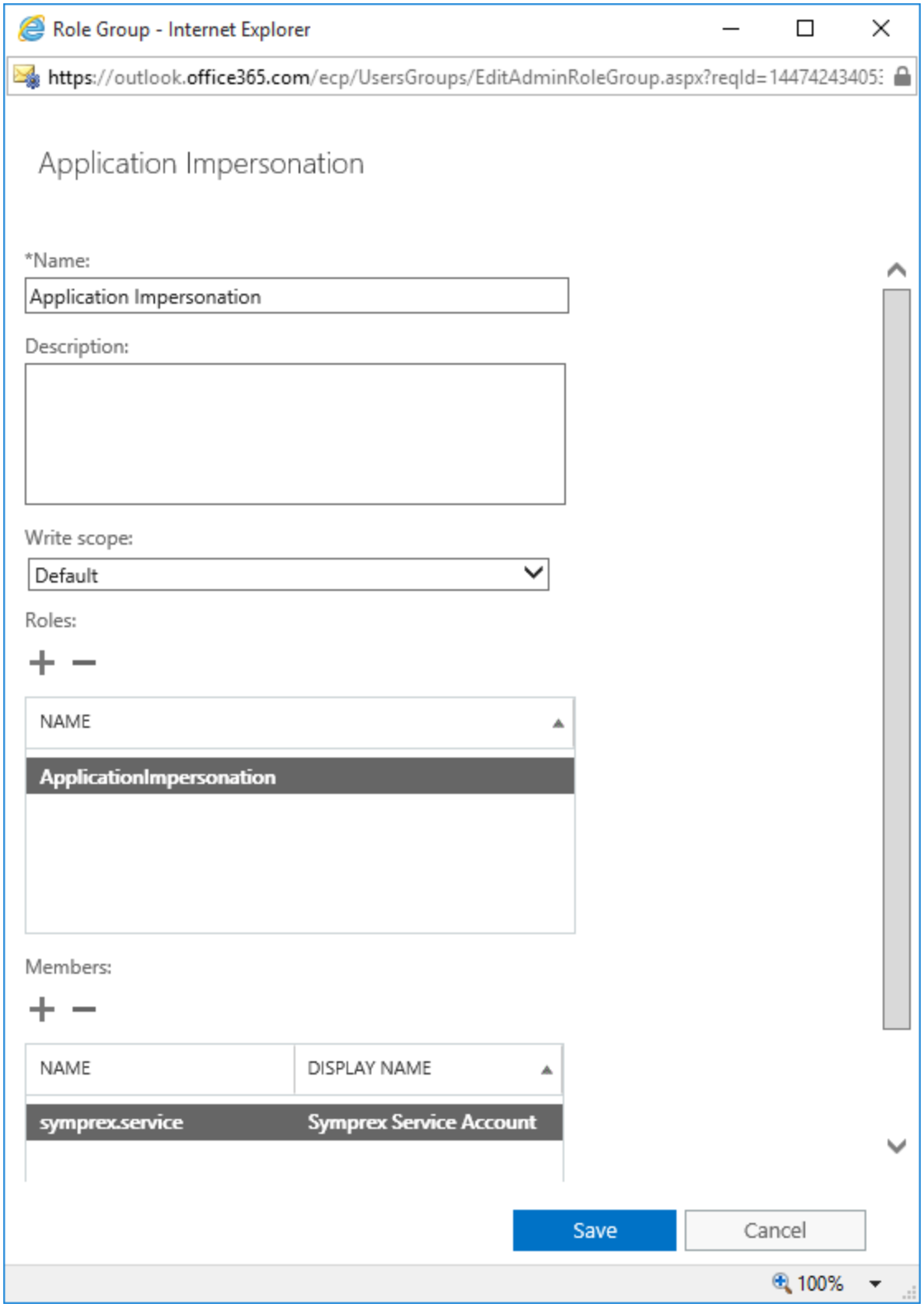
Click the **Create** button to create the account. If you have auto-generated the password, make a note of it.

4. Click **Exchange** in the **ADMIN** node of the tree on the left side of the page; this will open the **Exchange admin center** in a new window.

5. In the **Exchange admin center**, click **permissions** on the left side of the window.

6. Select the **Application Impersonation** role and click the edit symbol ( ).

7. In the **Members** list, click the add symbol (+) and from the **Select Members** windows, add the account created in step 3 and click the **OK** button. The Members list should now contain the service account; for example:



8. Click the **Save** button; the service account has now been assigned to the *Application Impersonation* role.

Direct Database Mode

Email Signature Manager can work in **Direct Database Mode**, in which the **Email Signature Manager Agent** connects directly to the Email Signature Manager database. In this mode the service will not write Outlook settings and signatures to each mailbox, and the Agent will fetch the same information directly from the database.

Examples of when direct database mode may be useful are:

- You want the Agent to work directly with the database in the same way as in Email Signature Manager version 4.x, 5.x and 6.x.
- Due to specific environment restrictions the Agent is unable to connect to mailboxes.

There are certain limitations to using direct database mode:

- The Email Signature Manager database must be hosted on SQL Server.
- Off-premises users may not be able to make direct connections to the database or VPN may be required.

These are the steps to take if you want to use direct database mode:

1. If you are currently using the built-in database, migrate it to SQL Server.

2. Within the main application, open the **Deployment Options** dialog and on the Advanced page, select the **Direct Database Mode** option.

3. Click the **Save Configuration File** button to save a configuration file that configures the Agent to connect to the SQL Server database.

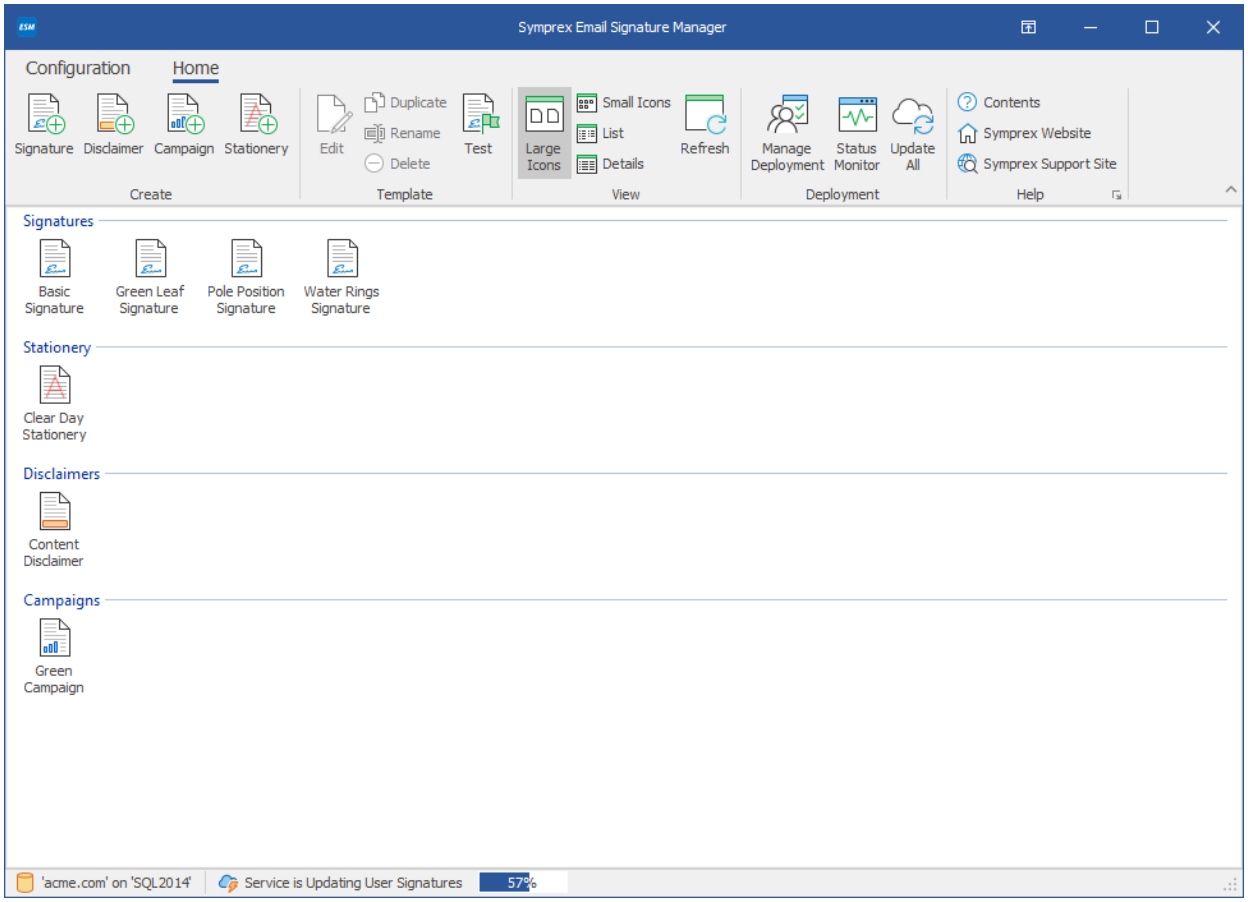
Note When using Group Policy, the configuration file is copied by the MSI package at installation time. Hence, any existing installations will not have the configuration file copied. It is therefore recommended to create a new GPO to install the latest version of the Agent, which will upgrade any existing installations and install the file.

Tutorial 2

Email Signature Manager is started by clicking its icon in the program group. When first started, an evaluation license will be automatically granted that will allow you to evaluate the software for a limited number of users for a limited amount of time. Once you have purchased an appropriate license, you will need to apply it to fully enable the application and remove the evaluation restrictions; please refer to the chapter on licensing for further information.

Main Application Window

The main application window has several areas, as shown below:



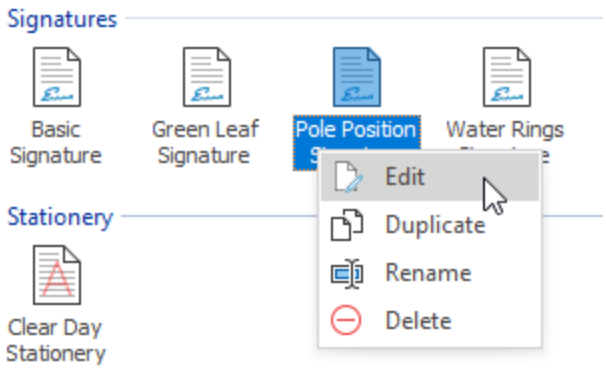
The ribbon at the top of the window provides access to all of the functions in the application. The ribbon can be collapsed by clicking the arrow in the top right-corner to provide more space for the main content of the window. The buttons in the ribbon will be available according to the current selection in the main window. The settings database to which the application is connected is displayed in the status bar at the bottom of the window, together with the current status of the service (only displayed on the machine where the full installation has been performed). Further details and options for the application can be found by clicking the **Configuration** ribbon tab, which opens the Configuration page by default.

The main area of the window displays the template browser, which displays the templates defined in the database. The list can be viewed in one of four modes; click the appropriate button in the **View** group in

the **Home** ribbon to change the view. To create a new template, click the appropriate button in the **Create** group in the **Home** ribbon. With an existing template selected, you can:

- Click the **Edit** button in the **Template** group in the ribbon to edit the selected template (this can also be accomplished by double-clicking the template), or
- Click the **Rename** button in the **Template** group in the ribbon to rename the selected template, or
- Click the **Delete** button in the **Template** group in the ribbon to *permanently* delete the selected template, or
- Click the **Duplicate** button in the **Template** group in the ribbon to create an identical duplicate the selected template.

Note The commands are also available in the context menu, which is opened by right-clicking on the appropriate template as illustrated below:



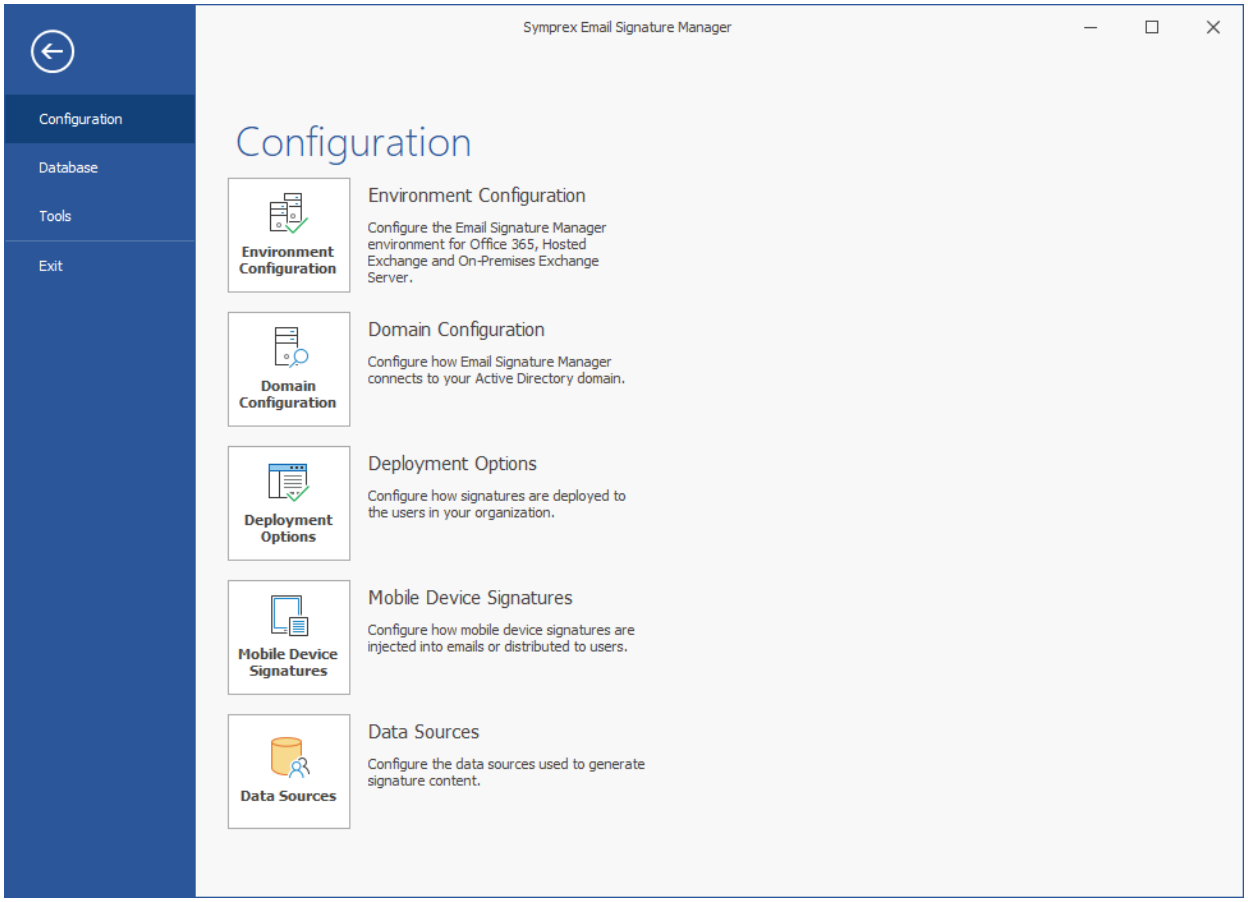
Please see this topic for further information about creating and editing templates. Once you have created your templates, they can be tested by clicking the **Test** button in the **Template** group in the **Home** ribbon to open the Test Signatures dialog.

The deployment of your templates is managed using the tools in the **Deployment** group in the ribbon:

- The **Manage Deployment** button will open the Manage Deployment dialog, which is used to configure which users in your organization receive which signatures.
- The **Status Monitor** button will open the Status Monitor dialog, which is used to monitor the deployment of signatures to the users in your organization.
- The **Update All** button (only available in the Full Installation of the product) will send a command to the Email Signature Manager Service to update the signatures for all users; more information about what the service does can be found in this topic.

Configuration Page

The Configuration page is displayed by clicking the **Configuration** ribbon in the main application window and selecting the **Configuration** page:

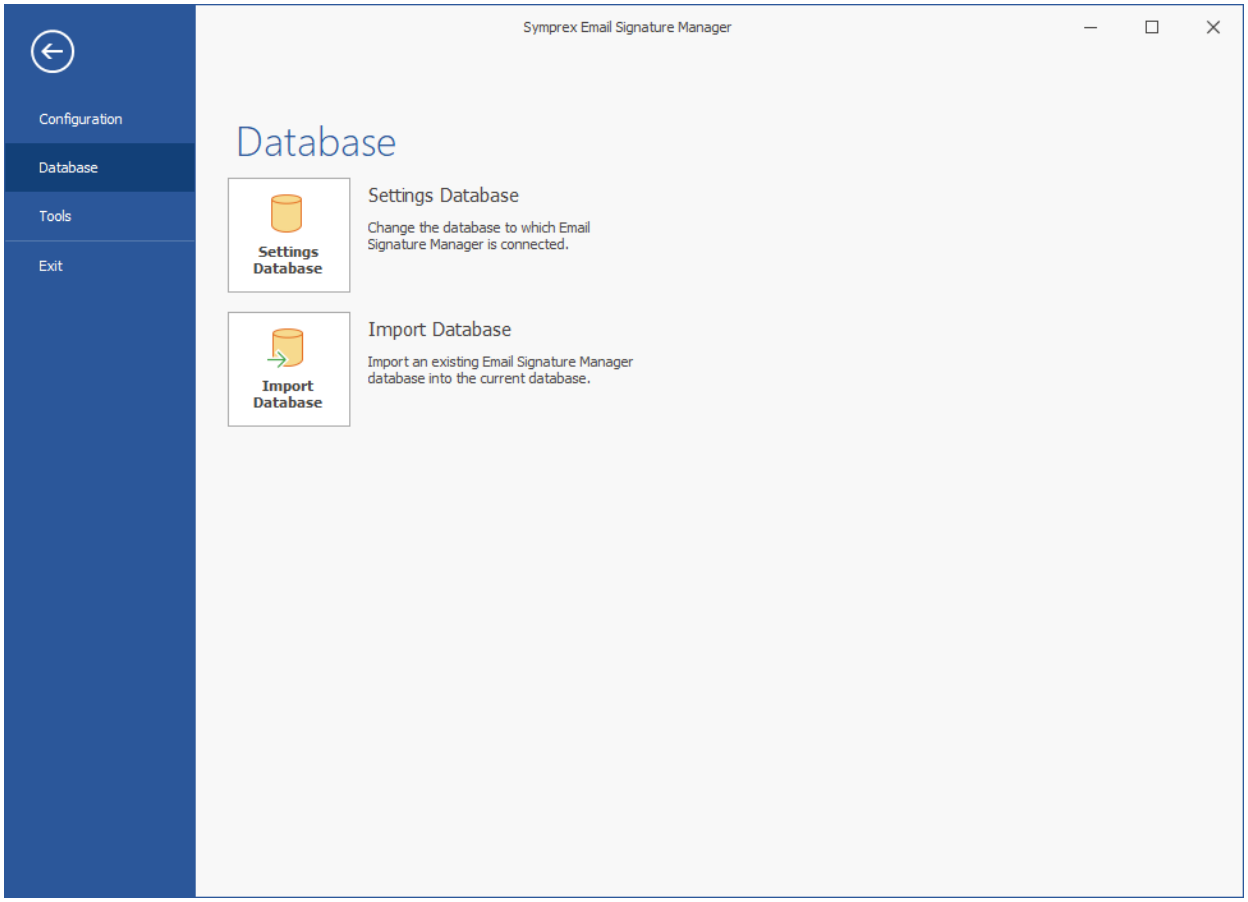


The buttons on this page perform the following actions:

- **Environment Configuration**: Opens the Environment Configuration dialog, which is used to configure the Email Signature Manager environment.
- **Domain Configuration**: Opens the Domain Configuration dialog, which configures how Email Signature Manager connects to Active Directory.
- **Deployment Options**: Opens the Deployment Options dialog, which configures the top-level settings that determine how signatures are deployed to users in your organization.
- **Mobile Device Signatures**: Opens the Mobile Device Signatures dialog, which configures how the signatures for the mobile devices in your organization are handled.
- **Data Sources**: Opens the Data Sources dialog, which configures the custom data sources used to generate signature content.

Database Page

The Database page is displayed by clicking the **Configuration** the ribbon in the main application window and selecting the **Database** page:

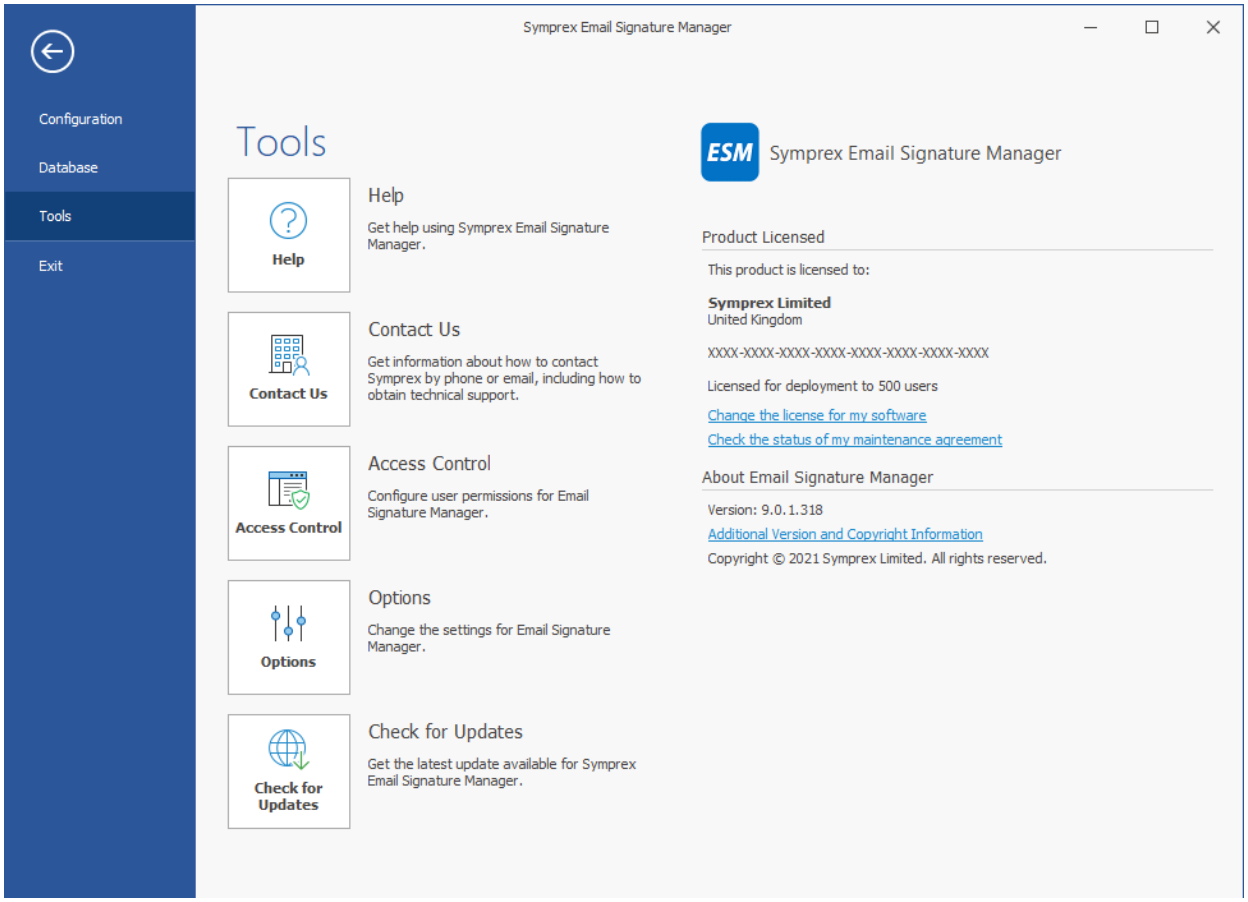


The buttons on this page perform the following actions:

- **Settings Database**: Opens the Settings Database dialog, which determines the database to which Email Signature Manager is connected.
- **Import Database**: Opens the Import Database dialog, which imports data from an existing database to the current database.

Tools Page

The Tools page is displayed by clicking the **Configuration** ribbon in the main application window and selecting the **Tools** page:



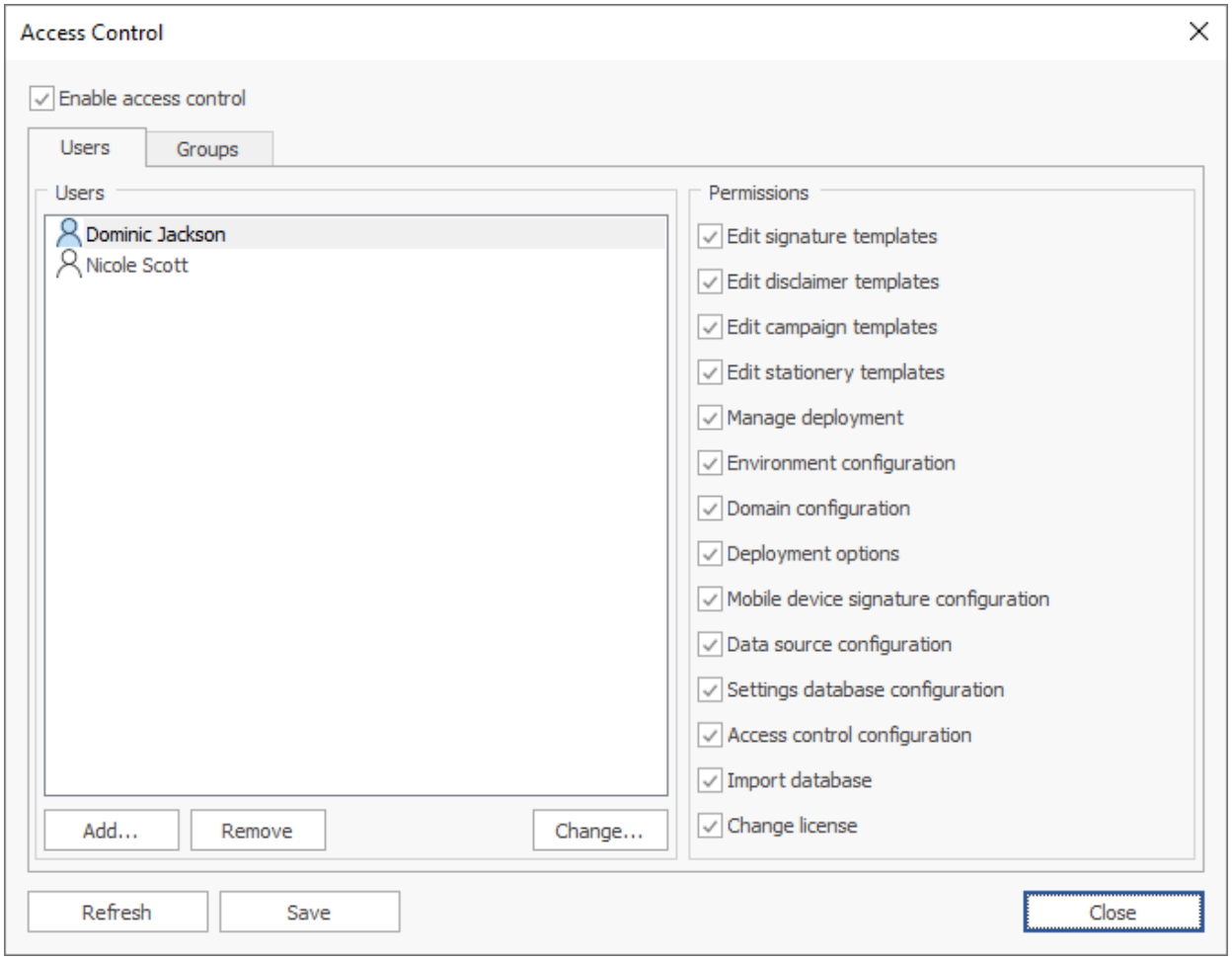
The buttons on this page perform the following actions to assist you with using Email Signature Manager:

Help: Opens the Email Signature Manager User's Guide.
Contact Us: Opens the Support Centre on the Symprex website.
Access Control: Opens the Access Control dialog to configure user permissions for using the software.
Options: Opens the Options dialog to configure application settings.
Check for Updates: Checks for updates to Email Signature Manager.

The right side of the page displays information about your license and product specific details for Email Signature Manager such as the version number. This information can be useful if you need to contact Symprex for technical assistance.

Access Control

The Access Control dialog is opened by clicking the **Options** button on the Tools page in the Configuration backstage of the main application window:



The Access Control dialog is used to specify the permissions that the users in your organization have when using Email Signature Manager. To enable access control, select the **Enable access control** option at the top of the dialog. If access control is disabled, all users can perform all actions. Once access control is enabled, permissions to use the various functions of the application can be specified either individually per user or by group membership.

Note Users that are members of the **Domain Admins** group always have full access and can perform all actions.

The permissions applied to a user are calculated in the following order of precedence:

- Permissions granted to an individual user on the **Users** page.
- Permissions granted through membership of a group specified on the **Groups** page where a user will take the permissions of the first group of which the user is a member.
- Default permissions.

The default permissions are:

- Start the application and browse templates.
- Open the Status Monitor dialog.

The permissions that can be assigned are:

- **Edit signature templates**: Allows a user to create or edit a signature template.
- **Edit disclaimer templates**: Allows a user to create or edit a disclaimer template.
- **Edit campaign templates**: Allows a user to create or edit a campaign template.
- **Edit stationery templates**: Allows a user to create or edit a stationery template.
- **Manage deployment**: Allows a user to open the Manage Deployment dialog.
- **Environment configuration**: Allows a user to open the Environment Configuration dialog.
- **Domain configuration**: Allows a user to open the Domain Configuration dialog.
- **Deployment options**: Allows a user to open the Deployment Options dialog.
- **Mobile device signature configuration**: Allows a user to open the Mobile Device Signatures dialog.
- **Data source configuration**: Allows a user to open the Data Sources dialog.
- **Settings database configuration**: Allows a user to open the Settings Database dialog.
- **Access control configuration**: Allows a user to open this dialog.
- **Import database**: Allows a user to open the Import Database dialog.
- **Change license**: Allows a user to change the application license.

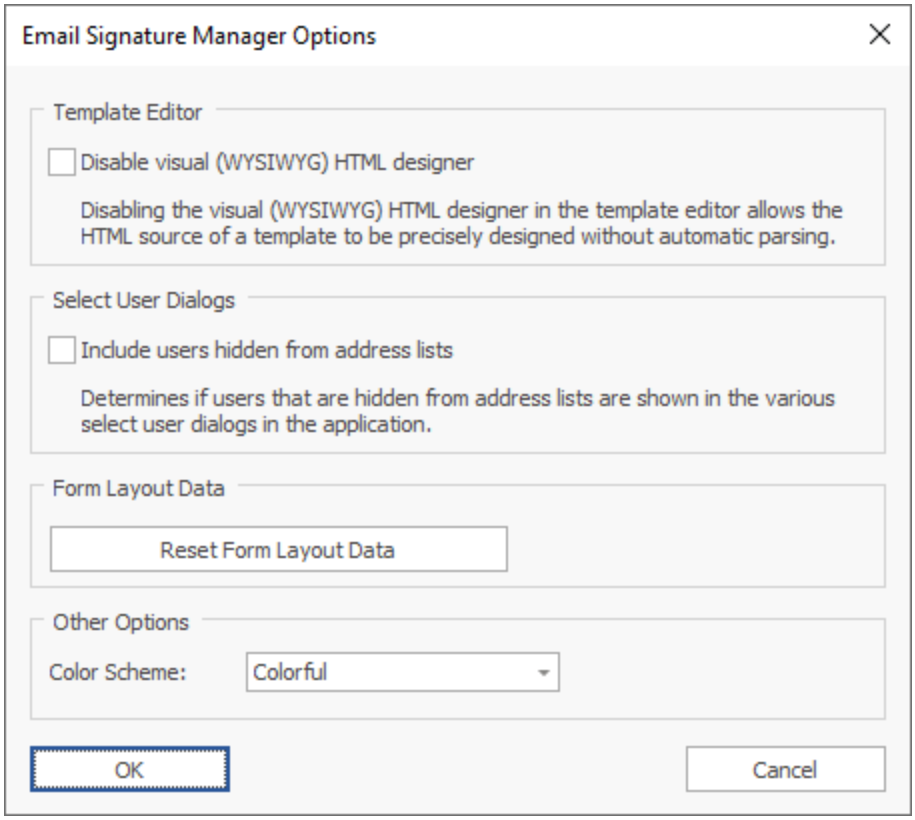
Both the **Users** and **Groups** page work in an identical manner. The left side of each page lists the objects to which permissions have been granted. Selecting an object from the list will display the assigned permissions on the right side of the page, and the rights can be assigned as required. To add a new object, click the **Add...** button. This will open a dialog to allow one or more objects to be selected from the domain. The selected object can be removed by clicking the **Remove** button or changed to another object, preserving the assigned permissions, clicking the **Change...** button. In addition, the order of groups can be altered by selecting a group and clicking the up or down arrow to move that group up or down within the list.

To refresh the access control configuration from the database, click the **Refresh** button.

When the access control has been configured as required, click the **Save** button to save your changes. Click the **Close** button to close the dialog; if you have made any changes, you will be prompted to save before the dialog is closed.

Options Dialog

The Email Signature Manager Options dialog is opened by clicking the **Options** button on the Tools page in the Configuration backstage of the main application window:



The following settings can be modified:

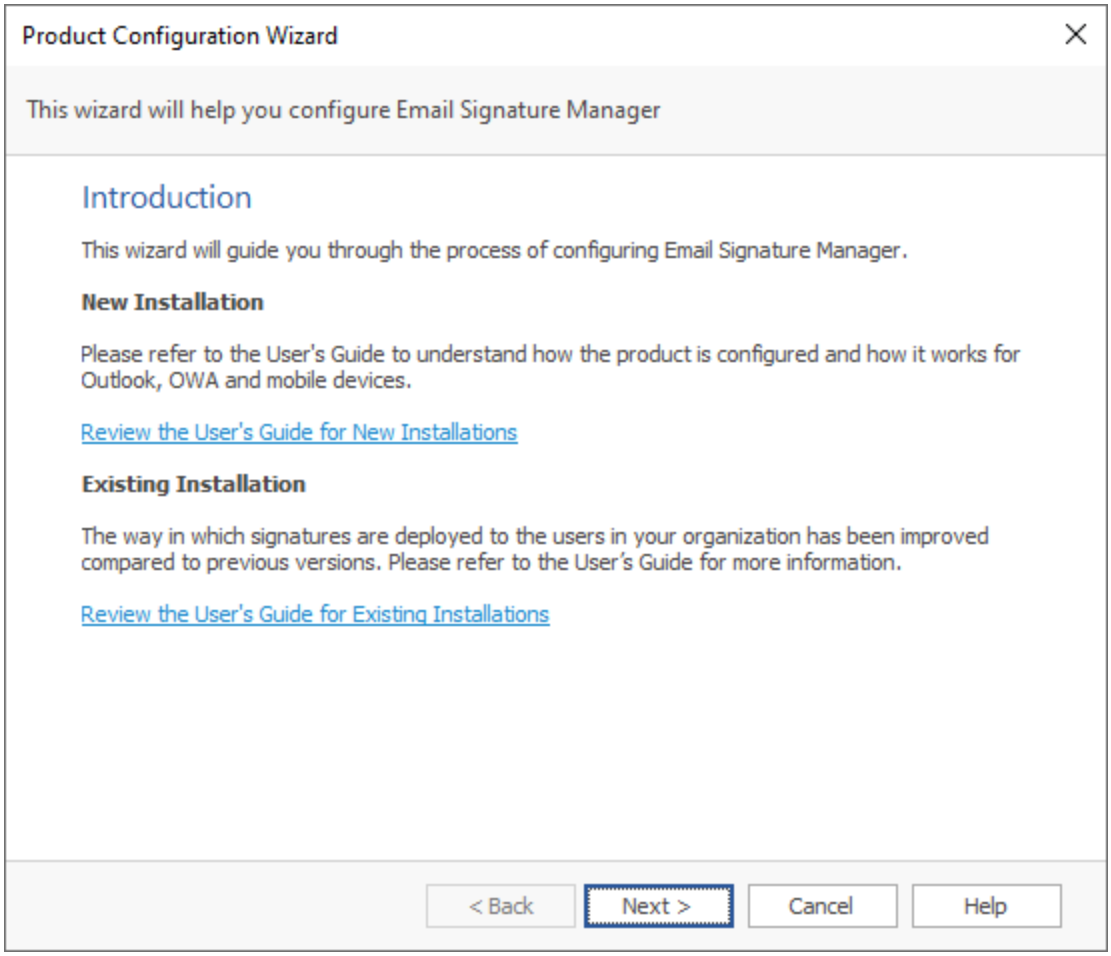
Disable visual (WYSIWYG) HTML designer: Disables the visual HTML designer when editing templates and forces the use of the Source view in the template editor. This option is useful if full control over the HTML of your templates is required, as it prevents the visual editor from parsing and modifying the HTML automatically.
Include users hidden from address lists: Various dialogs in the application require a user to be selected from Active Directory (for example, the Test Signatures dialog). By default, these Select User dialogs will exclude users hidden from address lists. This option can be enabled to include users that are hidden from address lists. Note that this will include various Exchange system mailboxes.
Form Layout Data: Clicking the **Reset Form Layout Data** button will reset the size and position of all windows within the application to their defaults.
Color Scheme: Allows you to choose the color scheme for the main application window.

To accept the changes you have made, click the **OK** button. Otherwise, click the **Cancel** button to close the dialog.

Product Configuration Wizard

The Product Configuration Wizard appears automatically when the application is started but has not previously been configured.

The first page displayed is the Introduction page:

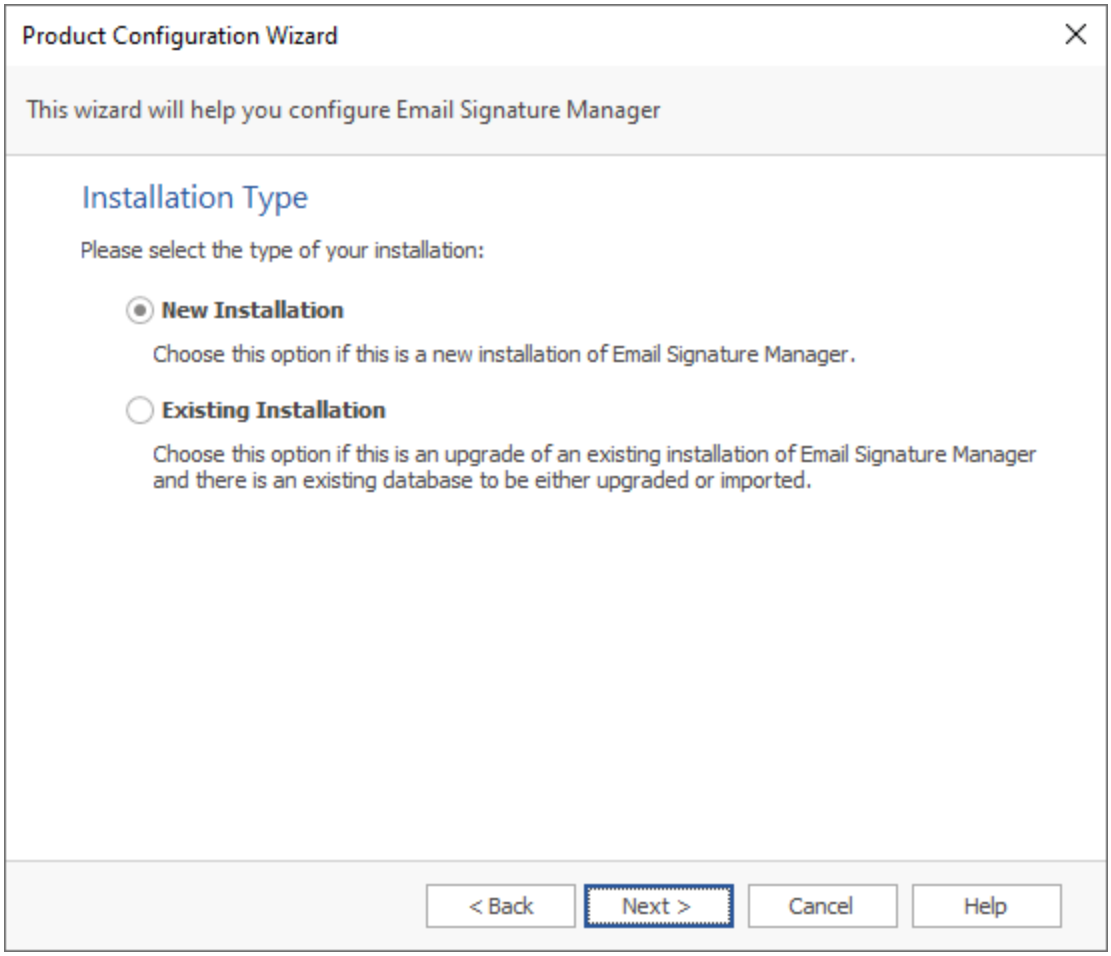


Please ensure that you have read the relevant topic in this User's Guide depending on whether this is a new installation or an existing installation of Email Signature Manager, and then click the **Next** button to proceed to the Installation Type page.

Note If you cancel the wizard at this stage, the application will not be usable and the main application window will be mainly disabled. If you close and later restart the application, you will be presented with the wizard again.

Installation Type

The Installation Type page in the Product Configuration Wizard is the next page after the Introduction page:

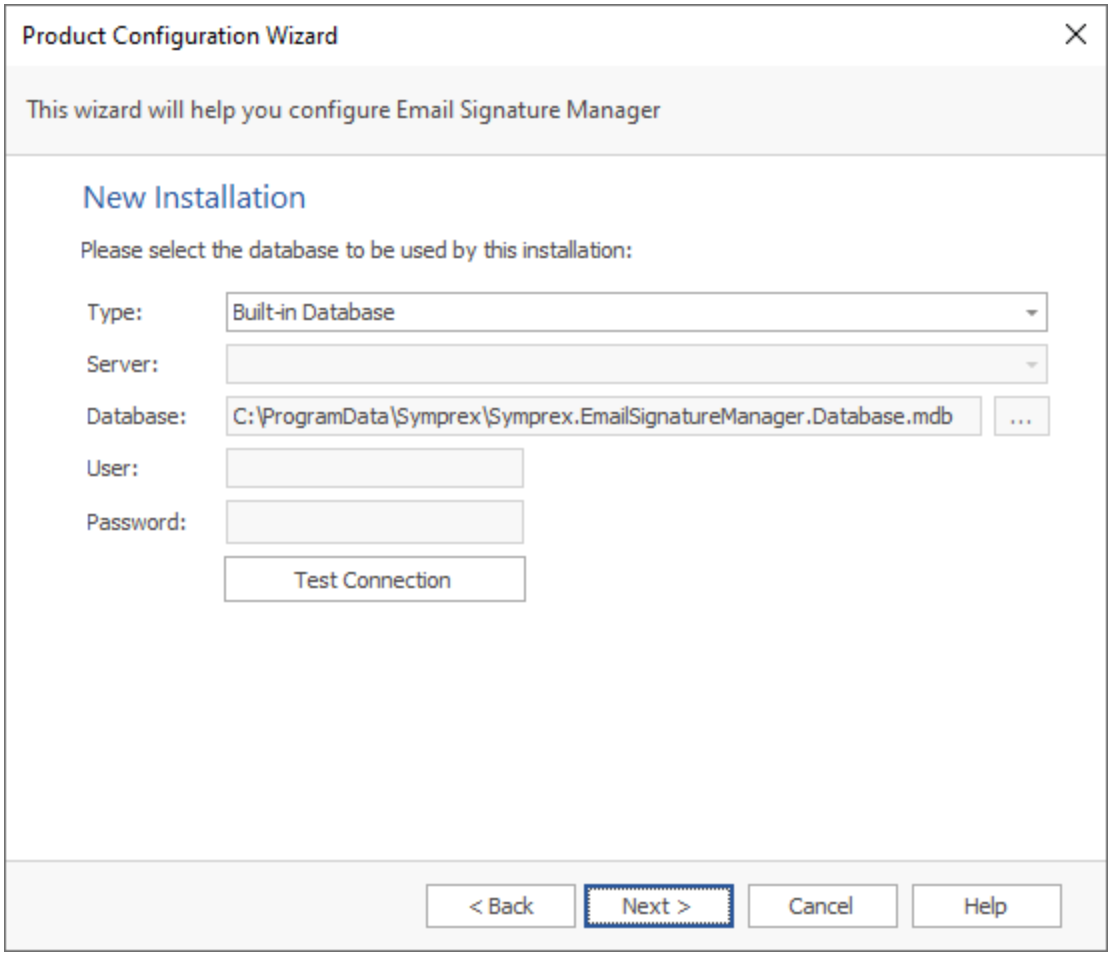


Select the appropriate option depending on whether this is a new installation or an existing installation, and click the **Next** button to proceed to either the New Installation page or Existing Installation page.

Note If you cancel the wizard at this stage, the application will not be usable and the main application window will be mainly disabled. If you close and later restart the application, you will be presented with the wizard again.

New Installation

The New Installation page in the Product Configuration Wizard is the next page after the Installation Type page when the **New Installation** option has been selected:



You can select whether to connect to the Built-in Database (recommended for new users of the product) or a SQL Server database (if one has been created following the guide for using SQL Server):

- When connecting to the Built-in Database, there are no other settings that need to be entered.
- When connecting to SQL Server, you must enter the credentials (user name and password) for the dedicated SQL login to be used by the application.

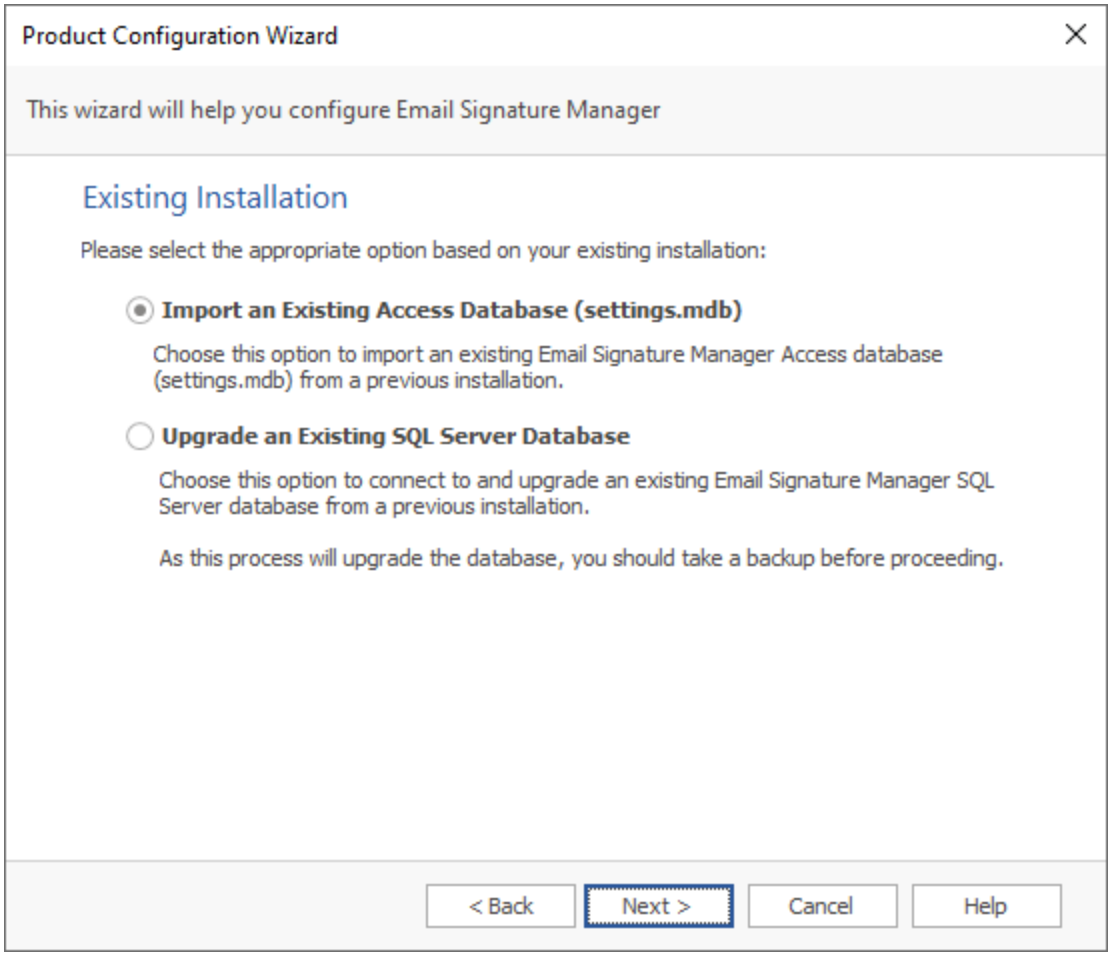
To verify you have entered the details of the database correctly, click the **Test Connection** button. This will open a connection to the database using the specified settings, read the current version, and show the result in a message box.

To connect to the database, click the **Next** button and, if the connection is successfully established, the wizard will proceed to the Database Connection Established page.

Note If you cancel the wizard at this stage, the application will not be usable and the main application window will be mainly disabled. If you close and later restart the application, you will be presented with the wizard again.

Existing Installation

The Existing Installation page in the Product Configuration Wizard is the next page after the Installation Type page when the **Existing Installation** option has been selected:



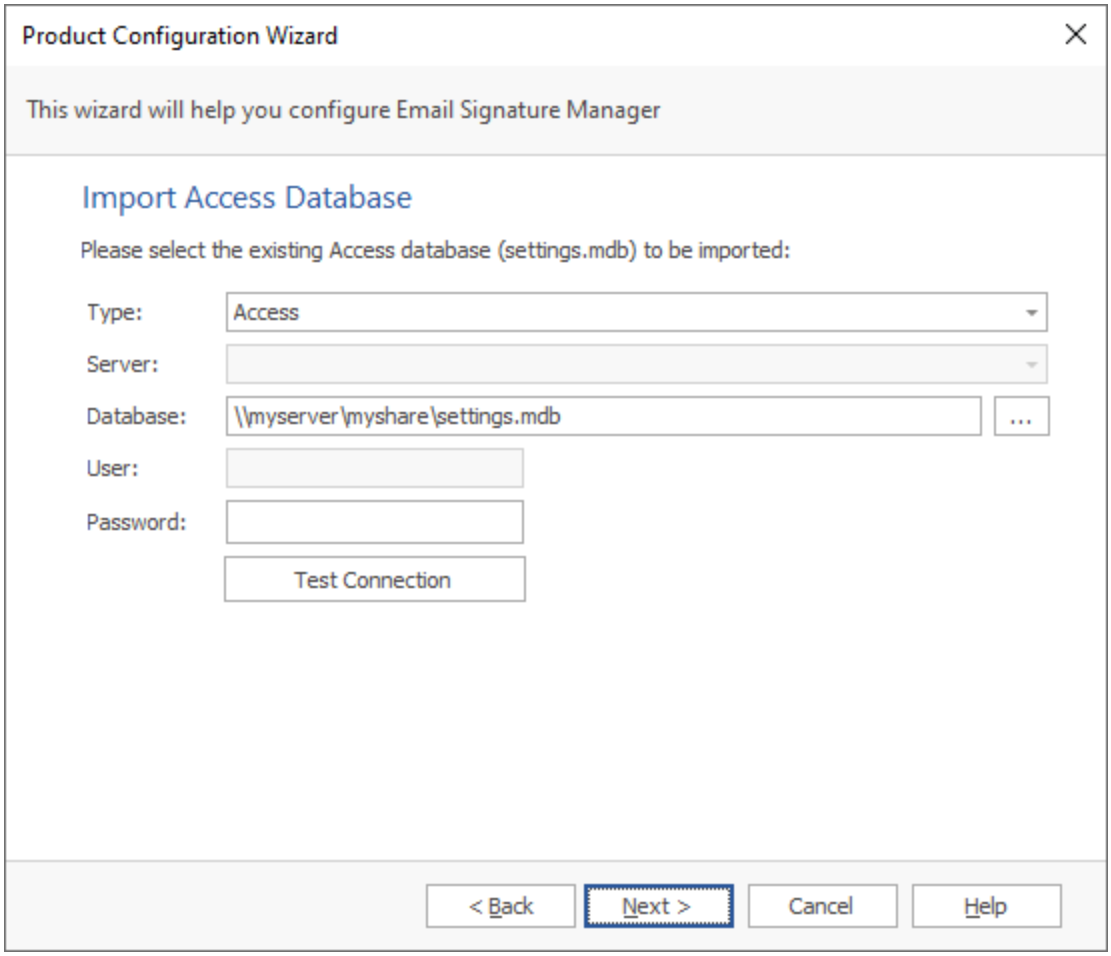
You should select the appropriate option depending on your current installation:

- If you have been using an Access database (`settings.mdb`) in a shared folder, select the **Import an Existing Access Database** option, and click the **Next** button to proceed to the Import Existing Database page.
- If you have been using SQL Server, select the **Upgrade an Existing SQL Server Database** option, and click the **Next** button to proceed to the Upgrade Existing Database page.

Note If you cancel the wizard at this stage, the application will not be usable and the main application window will be mainly disabled. If you close and later restart the application, you will be presented with the wizard again.

Import Database

The Import Database page in the Product Configuration Wizard is the next page after the Existing Installation page when the **Import an Existing Access Database** option has been selected:



This page of the wizard will import an Access database (`settings.mdb`) that was previously located in a shared folder.

Note The selected database will be imported to the Built-in Database. This will overwrite any current data in the Built-in Database.

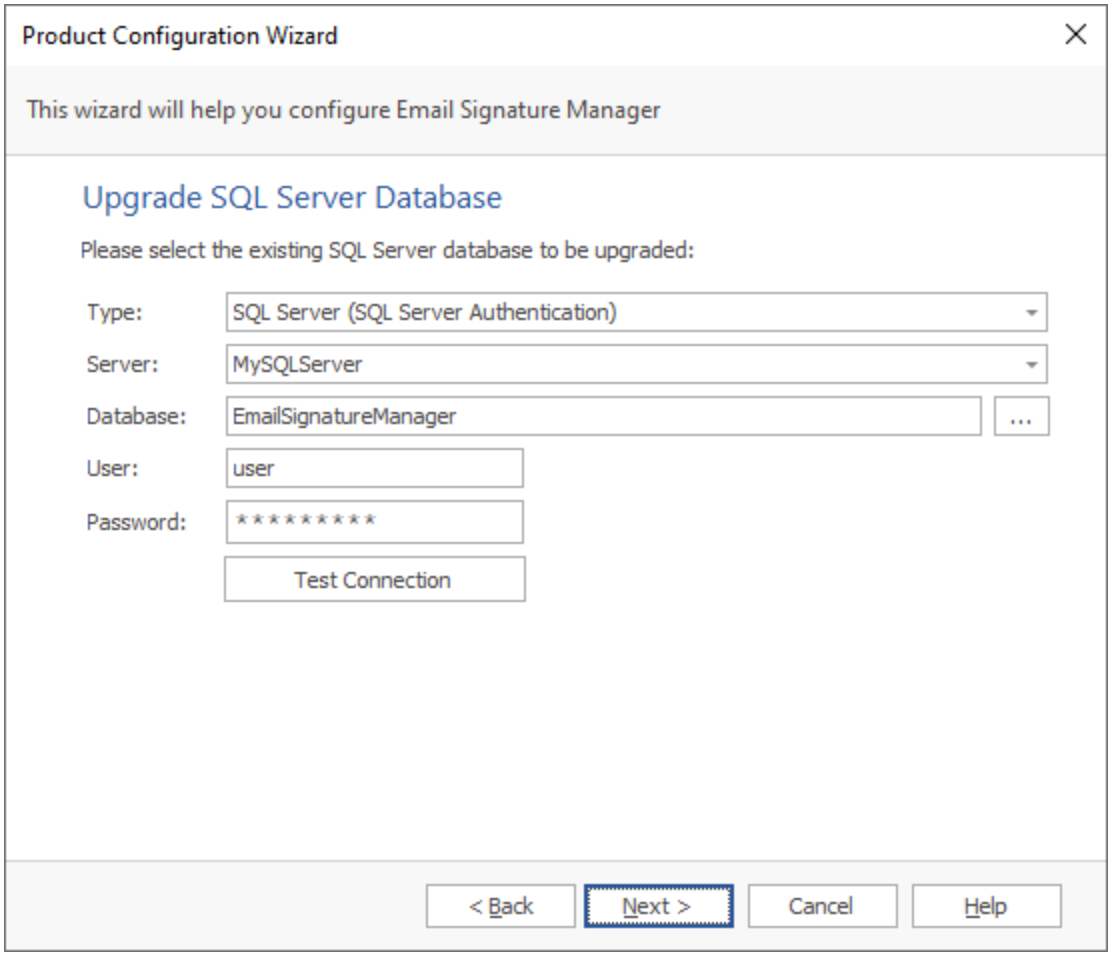
In the Database field, enter the full path to the database or click the ellipses ("...") button to locate the database. If necessary, enter the password for the database.

To proceed with the import, click the **Next** button. If the import completes successfully, the wizard will progress to the Database Connection Established page.

Note If you cancel the wizard at this stage, the application will not be usable and the main application window will be mainly disabled. If you close and later restart the application, you will be presented with the wizard again.

Upgrade Database

The Upgrade Database page in the Product Configuration Wizard is the next page after the Existing Installation page when the **Upgrade an Existing SQL Server Database** option has been selected:



This page of the wizard will upgrade an existing SQL Server database.

Important The specified account must have `db_owner` rights in order to update the database schema. Please refer to this topic for more information.

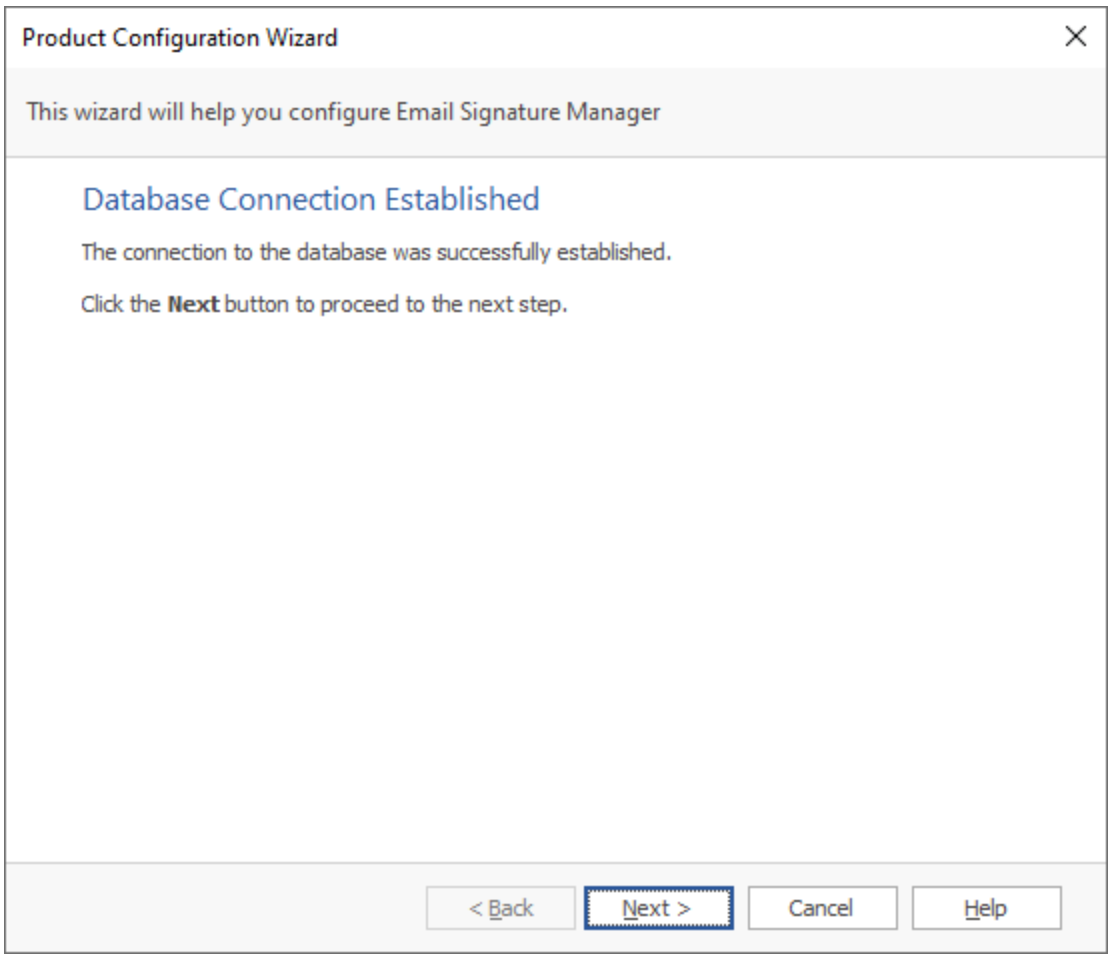
In the Server field, enter the name of the server where the database is located or drop down the list and select the appropriate server. In the Database field, enter the name of the database or click the ellipses ("...") button to select a database from the specified server. Finally, enter the credentials of the dedicated SQL login for the application.

To proceed with the upgrade, Click the **Next** button. If the upgrade completes successfully, the wizard will progress to the Database Connection Established page.

Note If you cancel the wizard at this stage, the application will not be usable and the main application window will be mainly disabled. If you close and later restart the application, you will be presented with the wizard again.

Database Connection Established

The Database Connection Established page in the Product Configuration Wizard is the next page after the connection to the Email Signature Manager database has been successfully established:



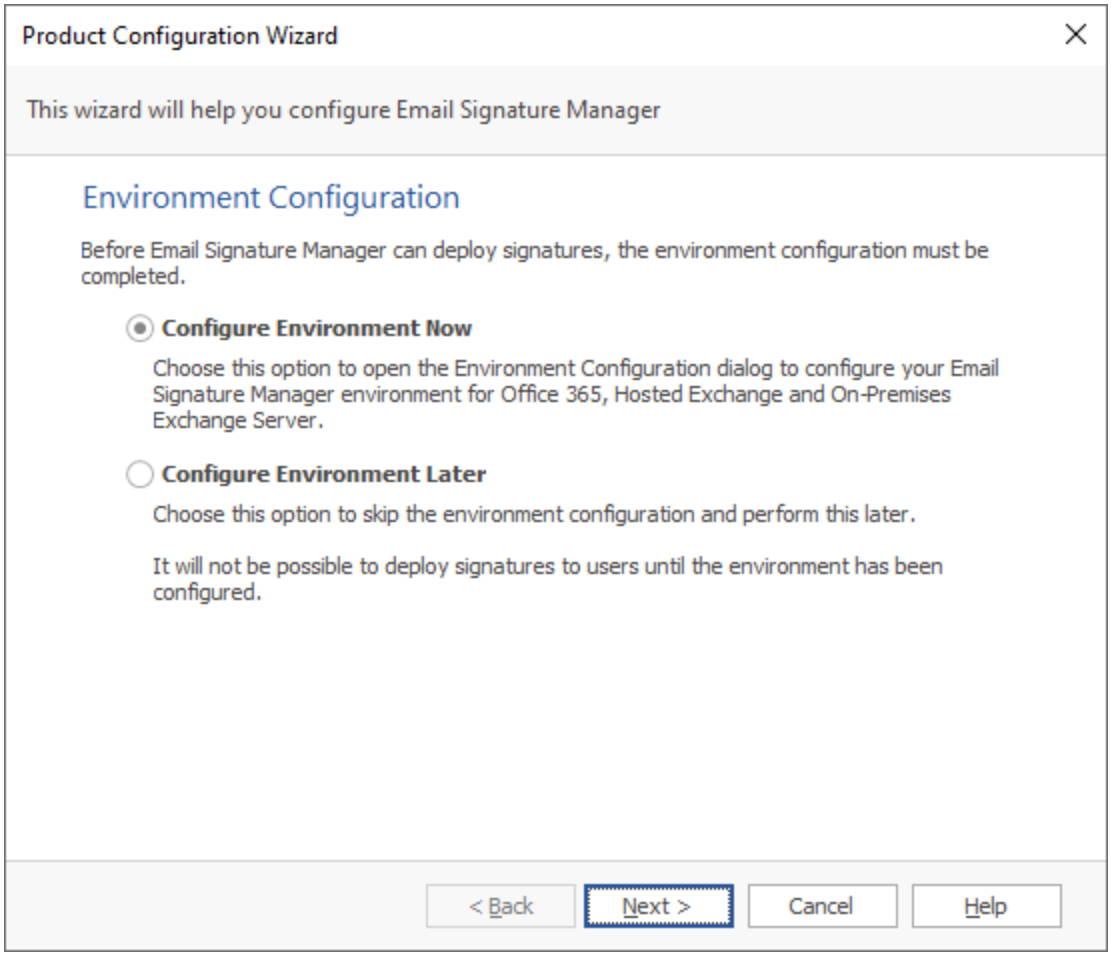
The exact content of this page will depend on whether this is a new installation of Email Signature Manager or if an existing installation has been upgraded.

Click the **Next** button to proceed to the Environment Configuration page.

Note If you cancel the wizard at this stage, the database will remain connected and the application will be usable. However, the Email Signature Manager Service will not be able to update user signatures until the environment configuration has been completed.

Environment Configuration

The Environment Configuration page in the Product Configuration Wizard is the next page after the Database Connection Established page:



In order for the Email Signature Manager Service to update user signatures, it is necessary to complete the environment configuration.

On this page, there are two options:

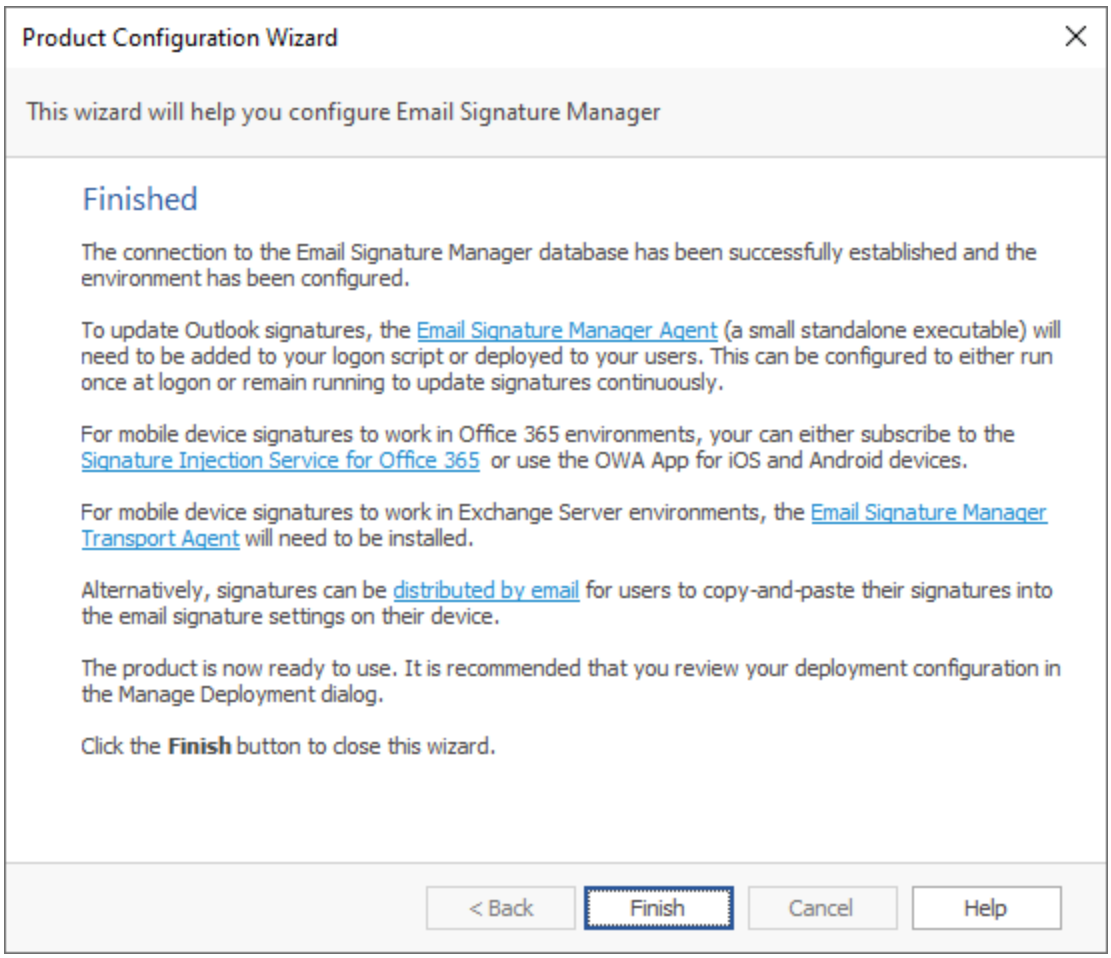
- **Configure Environment Now**: Select this option to proceed with environment configuration immediately (recommended). You will need the details of the relevant service accounts. Clicking the **Next** button with this option selected will open the Environment Configuration dialog. If the environment configuration is completed successfully, the wizard will then proceed to the Finished page.

- **Configure Environment Later**: Select this option to complete the wizard without completing environment configuration. Clicking the **Next** button with this option selected will cause the wizard to proceed to the Finished page.

Note If you cancel the wizard at this stage, the database will remain connected and the application will be usable. However, the Email Signature Manager Service will not be able to update user signatures until environment configuration has been completed.

Finished

The Finished page in the Product Configuration Wizard is the next page after the Environment Configuration page:



The content of this final page will depend on the content of the database to which the application has been connected.

The suggested next steps are as follows:

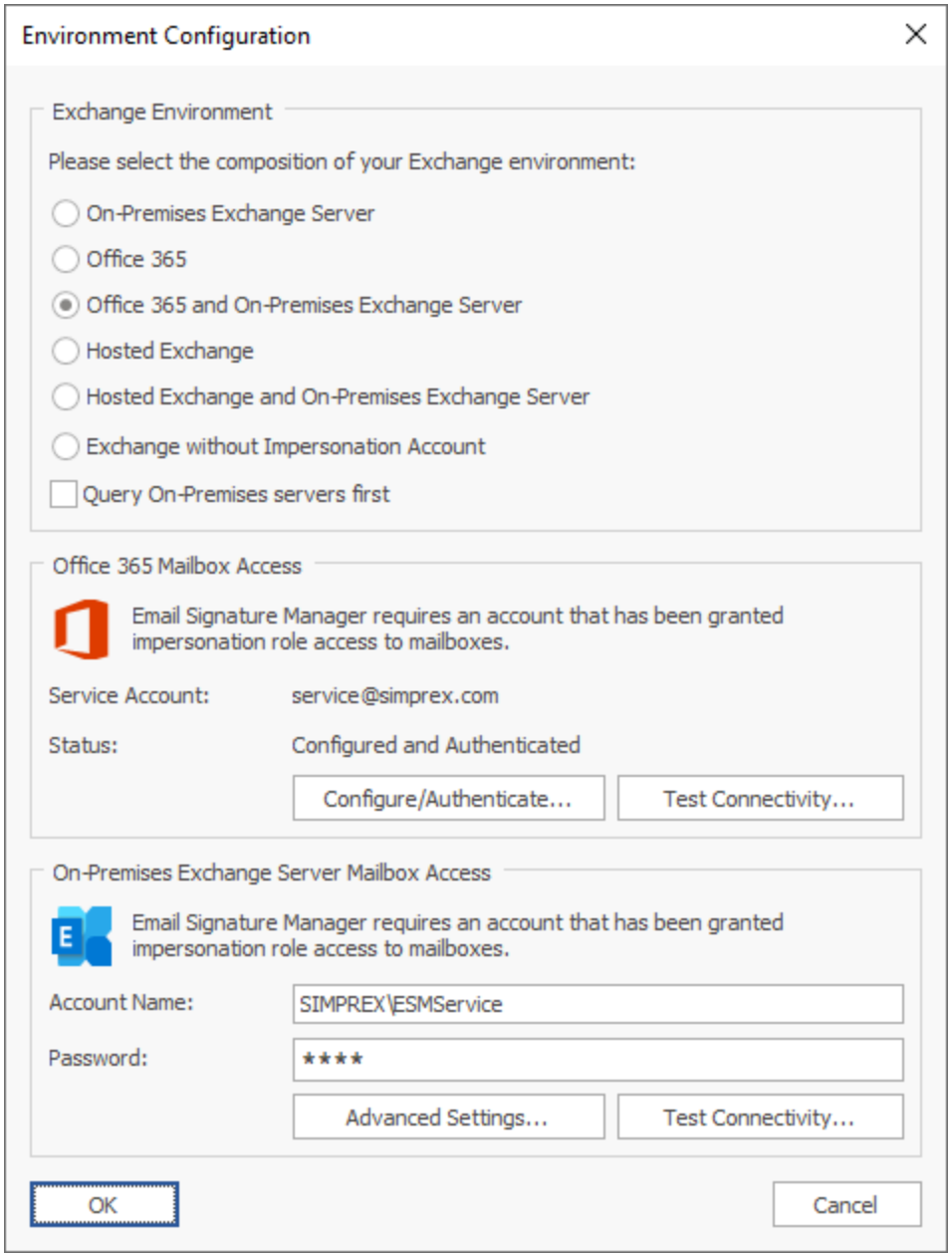
- If not already completed, complete the environment configuration.
- Design your own templates using our guide or use the sample templates supplied with Email Signature Manager.
- Configure the deployment of signatures to your users.
- Verify that the Email Signature Manager Service is updating user signatures in the Status Monitor.
- Arrange for the Email Signature Manager Agent to be executed on your end users' computers.

- For signatures on mobile devices, you can either:
  - Install the Email Signature Manager Transport Agent to inject signatures into emails sent through On-Premises Exchange Server.
  - Subscribe to the Signature Injection Service for Office 365 to inject signatures into emails sent through Office 365.
  - Distribute signatures by email.

Click the **Finish** button to proceed to the close the wizard.

Environment Configuration

The Environment Configuration dialog is opened by clicking the **Environment Configuration** button on the Configuration page in the Configuration backstage of the main application window:



The Environment Configuration dialog is used to tell Email Signature Manager how your Exchange environment is configured and the service accounts to use to access mailboxes.

The following environments are supported:

- On-Premises Exchange Server
- Office 365
- Office 365 and On-Premises Exchange Server
- Hosted Exchange
- Hosted Exchange and On-Premises Exchange Server
- Exchange without Impersonation Account

Depending on the selected environment, you will be required to enter the details of the service account that has been created and assigned the Application Impersonation role within each platform supported by that environment. For example, if you have selected an environment with On-Premises Exchange Server, then you will need to enter the details of the service account that has been created within your On-Premises Exchange Server platform.

Each environment supports for the following options:

On-Premises Exchange Server: Advanced Settings and Test Connectivity.
Office 365: Configure Modern Authentication and Test Connectivity.
Hosted Exchange: Advanced Settings and Test Connectivity.

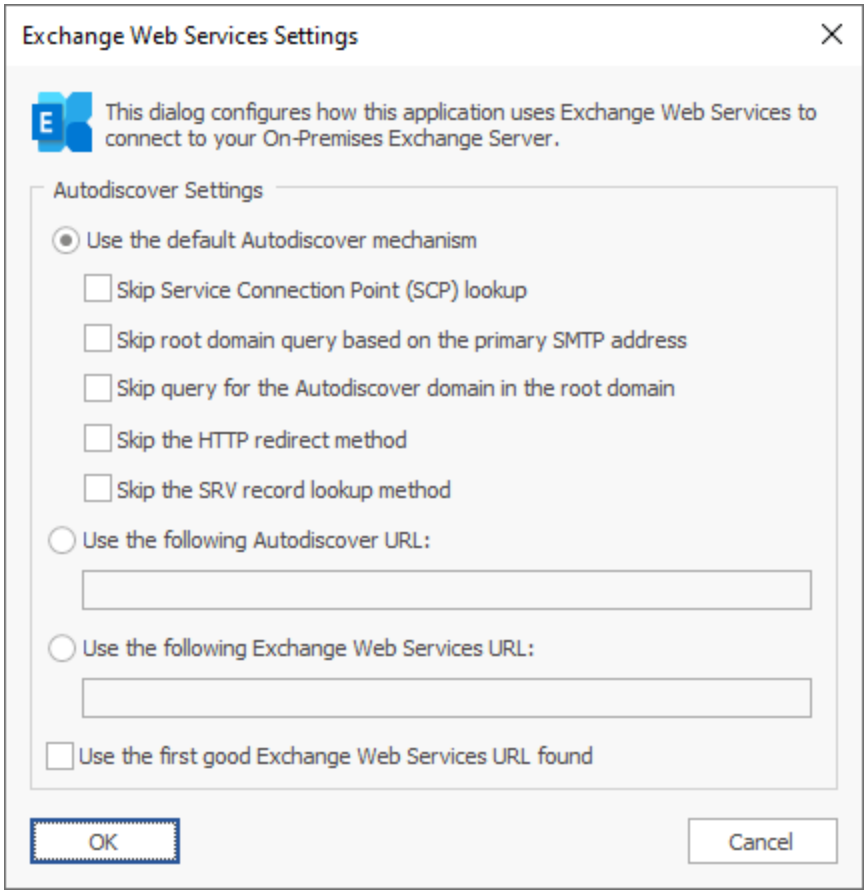
Note that if you select the **Exchange without Impersonation Account** option, then no other configuration is required, but the following restrictions apply:

- OWA signatures will not be deployed.
- Automatic support for Outlook signatures for remote users will not work.

When the environment has been configured as required, click the **OK** button to save your changes and close the dialog. Alternatively, click the **Cancel** button to close the dialog without saving any changes.

On-Premises Settings

The On-Premises Exchange Web Services Settings dialog is opened by clicking the **Advanced Settings...** button in the On-Premises Exchange Server Mailbox Access group in the Environment Configuration dialog:



Note In normal conditions, the connection to Exchange Web Services will be configured automatically using the Autodiscover mechanism built into Exchange Server. It should only be necessary to change these advanced settings if specific problems are being encountered that prevent Autodiscover from working correctly, or if performance problems are being encountered.

The following **Autodiscover Settings** can be configured:

Setting	Description
Use the default Autodiscover mechanism	Specifies that the default Autodiscover mechanism should be used. *This is the default setting.*
Use the following Autodiscover URL	Specifies that the Autodiscover mechanism should use the specified Autodiscover service URL directly.
Use the following Exchange Web Services URL	Disables the Autodiscover mechanism, forcing the connection to Exchange Web Services to use the specified fixed Exchange Web Services URL for all users.
Use the first good Exchange Web Services URL found	When using the default Autodiscover mechanism, this setting stipulates that once the first good Exchange Web Services URL has been discovered (from a Service Connection Point), the mechanism should stop and use that URL alone (rather than continuing and querying further Service Connection Points). This can be useful if you have a number of Autodiscover servers (i.e. a number of Service Connection Points), some of which are not currently available.

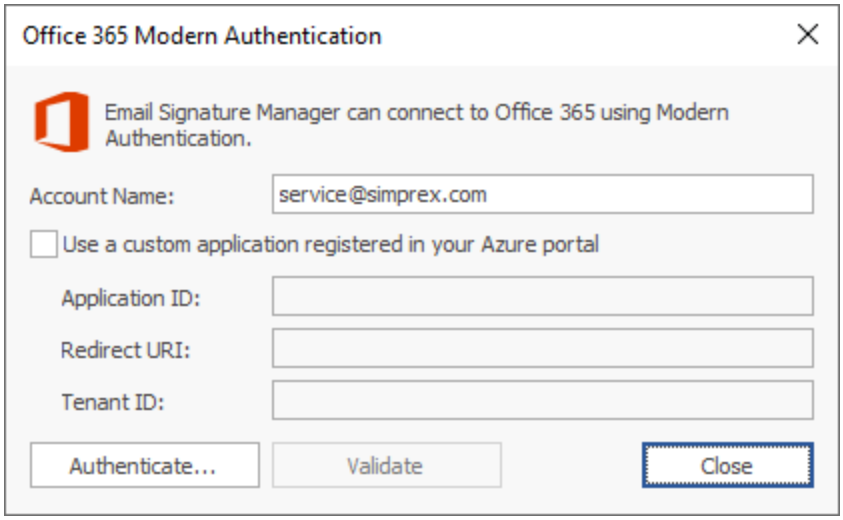
The following settings are applicable when the **Use the default Autodiscover mechanism** option is selected:

Setting	Description
Skip Service Connection Point (SCP) lookup	Specifies that the Autodiscover mechanism will not query Active Directory for Service Connection Points (SCPs).
Skip root domain query based on the primary SMTP address	Specifies that the Autodiscover mechanism will not query for an Autodiscover service at the URL based on the *root domain* found in the primary SMTP email address for a user. The URL format is `https://<smtp-address-domain>/autodiscover/autodiscover.xml`, so for a user with the email address `user@contoso.com`, this would resolve to `https://contoso.com/autodiscover/autodiscover.xml`.
Skip query for the Autodiscover domain in the root domain	Specifies that the Autodiscover mechanism will not query for an Autodiscover service at the URL based on the *Autodiscover sub-domain of the root domain* found in the primary SMTP email address for a user. The URL format is `https://autodiscover.<smtp-address-domain>/autodiscover/autodiscover.xml`, so for a user with the email address `user@contoso.com`, this would resolve to `https://autodiscover.contoso.com/autodiscover/autodiscover.xml`.
Skip the HTTP redirect method	Specifies that the Autodiscover mechanism will not query for an HTTP redirect on the *Autodiscover sub-domain of the root domain* found in the primary SMTP email address for a user. The URL format is `https://autodiscover.<smtp-address-domain>/autodiscover/autodiscover.xml`, so for a user with the email address `user@contoso.com`, this redirect query would be made against `https://autodiscover.contoso.com/autodiscover/autodiscover.xml`.
Skip the SRV record lookup method	Specifies that the Autodiscover mechanism will not query for SRV DNS records (which point to the Autodiscover service) for the domain found in the primary SMTP email address for a user.

When the settings have been configured as required, click the **OK** button save your changes and close the dialog. Alternatively, click the **Cancel** button to close the dialog without saving any changes.

Office 365 Modern Authentication

The Office 365 Modern Authentication dialog is opened by clicking the **Configure...** button in the Office 365 Mailbox Access group in the Environment Configuration dialog:



Modern Authentication provides a secure mechanism for connecting to Office 365, including support for Multi-Factor Authentication (MFA), and this process requires Email Signature Manager to be registered as an application in Azure. Symprex provides a default application registration to authenticate users in your tenant but this does *not* provide Symprex any access to your mailboxes in your Exchange Online platform. If you wish to register your own custom application, please go to https://www.symprex.com/support/docs for documentation how to configure this in your Azure portal.

To configure Modern Authentication, follow these steps:

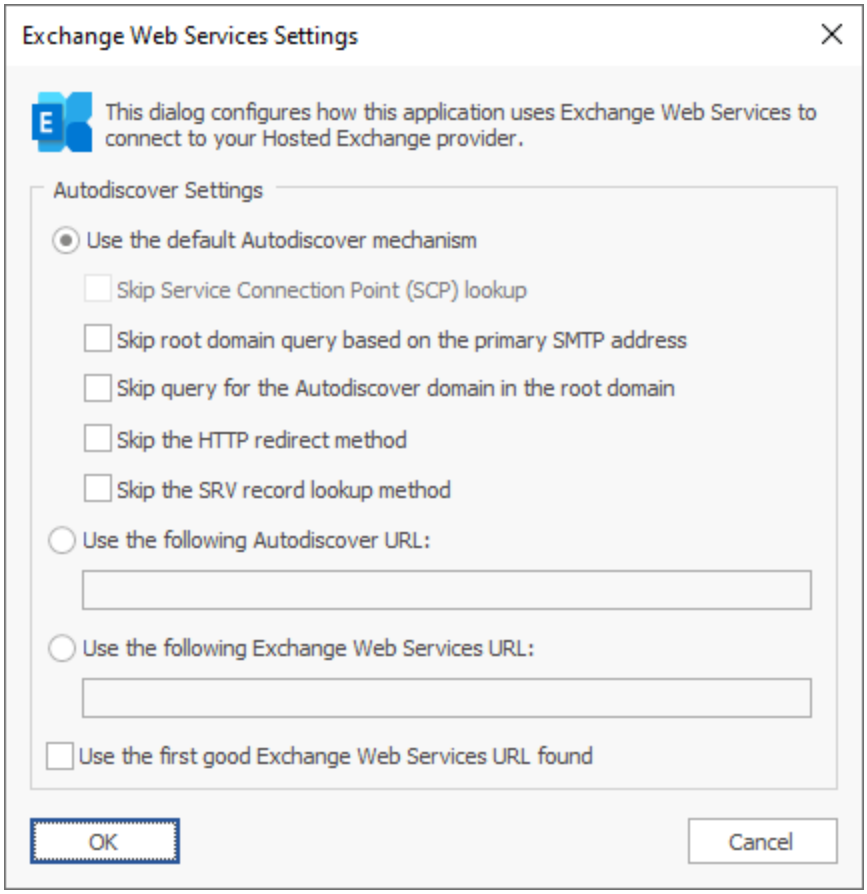
1. Enter the name of the service account in the **Account Name** box.
2. If you wish to use a custom application in your Azure portal, select the **Use a custom application registered in your Azure portal** option, and enter the **Application ID**, **Redirect URI** and **Tenant ID**.
3. Click the **Authenticate...** button; this will initiate authentication using the specified account and either the default Symprex application or your own custom application.

Once authentication has been completed, the **Validate** button can be used to verify that the persisted token cache, used to authenticate the service account, is valid.

When authentication has been configured as required, click the **Close** button to close the dialog.

Hosted Settings

The Hosted Exchange Web Services Settings dialog is opened by clicking the **Advanced Settings...** button in the Hosted Exchange Mailbox Access group in the Environment Configuration dialog:



Note In normal conditions, the connection to Exchange Web Services will be configured automatically using the Autodiscover mechanism built into Exchange Server. It should only be necessary to change these advanced settings if specific problems are being encountered that prevent Autodiscover from working correctly, or if performance problems are being encountered.

The following **Autodiscover Settings** can be configured:

Setting	Description
Use the default Autodiscover mechanism	Specifies that the default Autodiscover mechanism should be used. *This is the default setting.*
Use the following Autodiscover URL	Specifies that the Autodiscover mechanism should use the specified Autodiscover service URL directly.
Use the following Exchange Web Services URL	Disables the Autodiscover mechanism, forcing the connection to Exchange Web Services to use the specified fixed Exchange Web Services URL for all users.
Use the first good Exchange Web Services URL found	When using the default Autodiscover mechanism, this setting stipulates that once the first good Exchange Web Services URL has been discovered (from a Service Connection Point), the mechanism should stop and use that URL alone (rather than continuing and querying further Service Connection Points). This can be useful if you have a number of Autodiscover servers (i.e. a number of Service Connection Points), some of which are not currently available.
Query Outlook provider settings first	When using the Autodiscover mechanism, each Autodiscover service (i.e. each Service Connection Point) is queried using the standard Autodiscover protocol. If this fails, the service is queried for the settings to be used by Outlook (which uses a different protocol). In some environments, the standard Autodiscover protocol is not available on any server, so it is beneficial (from a performance standpoint) to query for the Outlook provider settings first.

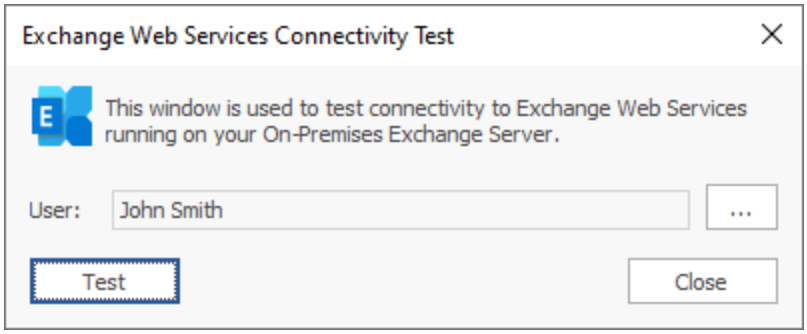
The following settings are applicable when the **Use the default Autodiscover mechanism** option is selected:

Setting	Description
Skip Service Connection Point (SCP) lookup	*Not applicable to Hosted Exchange environments.*
Skip root domain query based on the primary SMTP address	Specifies that the Autodiscover mechanism will not query for an Autodiscover service at the URL based on the *root domain* found in the primary SMTP email address for a user. The URL format is `https://<smtp-address-domain>/autodiscover/autodiscover.xml`, so for a user with the email address `user@contoso.com`, this would resolve to `https://contoso.com/autodiscover/autodiscover.xml`.
Skip query for the Autodiscover domain in the root domain	Specifies that the Autodiscover mechanism will not query for an Autodiscover service at the URL based on the *Autodiscover sub-domain of the root domain* found in the primary SMTP email address for a user. The URL format is `https://autodiscover.<smtp-address-domain>/autodiscover/autodiscover.xml`, so for a user with the email address `user@contoso.com`, this would resolve to `https://autodiscover.contoso.com/autodiscover/autodiscover.xml`.
Skip the HTTP redirect method	Specifies that the Autodiscover mechanism will not query for an HTTP redirect on the *Autodiscover sub-domain of the root domain* found in the primary SMTP email address for a user. The URL format is `https://autodiscover.<smtp-address-domain>/autodiscover/autodiscover.xml`, so for a user with the email address `user@contoso.com`, this redirect query would be made against `https://autodiscover.contoso.com/autodiscover/autodiscover.xml`.

When the settings have been configured as required, click the **OK** button save your changes and close the dialog. Alternatively, click the **Cancel** button to close the dialog without saving any changes.

EWS Connectivity Test

The Exchange Web Services Connectivity Test dialog is opened by clicking the **Test Connectivity...** button in the relevant group on the Environment Configuration dialog:



This dialog is used to test connectivity to your organization's Exchange Web Services platform. This is helpful to test that the deployment of signatures will work as expected using the account specified on the Environment Configuration dialog.

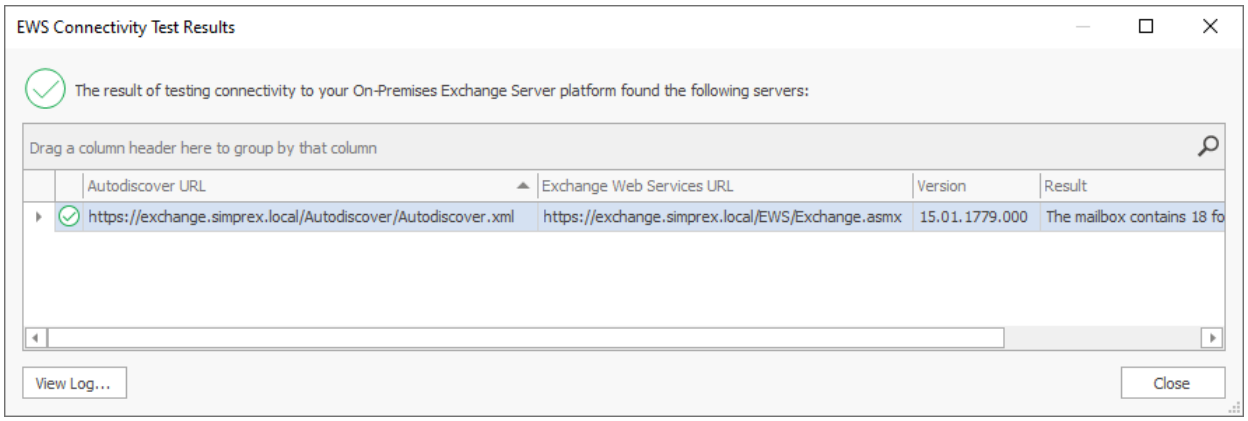
By default, the current Windows user is selected for the test. To choose a different user against which to test, click the ellipses button ("...") next to the user.

When ready, click the **Test** button. If the tests complete successfully, you will be presented with a confirmation message, giving the choice to open the detailed results dialog. It the tests fail, the results dialog will open automatically.

Once testing has been completed, click the **Close** button to close the dialog.

EWS Connectivity Test Results

The Exchange Web Services Connectivity Test Results dialog is opened after completing a connectivity test using the EWS Connectivity Test dialog:



The information message at the top of the window will give a summary of the overall result of the test. Contained within the grid are all of the Exchange Web Services servers that were found during the testing process. The information that is displayed is as follows:

- **Autodiscover URL**: This is the URL of the autodiscover service that was queried to locate the Exchange Web Services URL. The autodiscover URL can be found in a number of ways depending on the precise configuration of the platform being tested; for example, when testing On-Premises Exchange Server, autodiscover URLs can be determined by querying Active Directory for Service Connection Points.
- **Exchange Web Services URL**: This is the URL of the tested Exchange Web Services server.
- **Version**: This is the best-match version of the tested Exchange Web Services platform. The version number reported can vary depend on the precise configuration of your environment; for example, the mailbox version (as returned from the autodiscover service) may not match precisely the version of Exchange Server.
- **Result:** This details the information that was read from the specified mailbox to test connectivity.

If a server reports an error, double-click it to open a dialog that will display detailed information about what happened and why the test failed. The test process also maintains a detailed log of what happened; to view this log, click the **View Log...** button.

When ready, click the **Close** button to close the dialog.

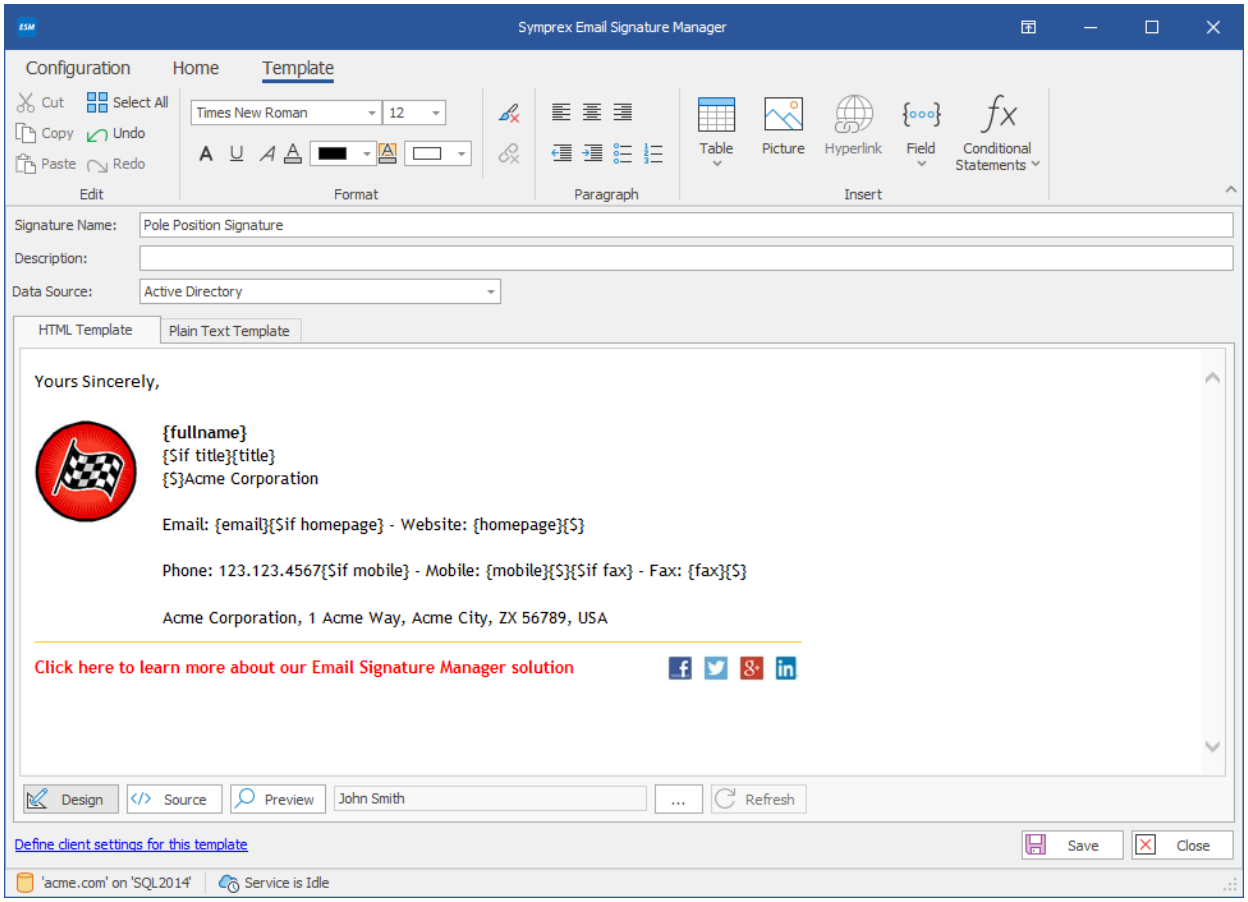
Creating and Editing Templates

Signatures can help to make your emails look professional, convey your brand, and to identify who you are. Signatures configured for deployment to Microsoft Outlook, OWA and mobile devices are automatically added to the end of new emails you compose. By designing and deploying signatures from a central point, you can achieve a consistent appearance for all emails from your organization. Email Signature Manager offers four different types of templates to accomplish this:

Icon	Type	Description
	Signature	Signatures normally include graphics such as a logo to convey corporate identity and branding, and include fields to merge contact information from Active Directory or another data source. Disclaimers and campaigns can be appended to any signature.
	Disclaimer	Disclaimers are normally of a legal nature and will be appended to designated signatures. Separating disclaimers from signatures makes it easy to maintain the same disclaimer on many different signatures.
	Campaign	Campaigns are normally used to include graphics or text, for example news or sales promotions, and will be appended to designated signatures. Campaigns can be scheduled to run within a certain time frame.
	Stationery	Stationery can be used to set background images. Note that stationery only works in Outlook and only when creating new email in HTML format.

Templates are created and managed from the main application window.

When designing a template, the main application window displays the Template ribbon and the template editor:



The Template ribbon offers various commands whilst designing your templates:

- The Edit group contains the standard commands for working with the clipboard and content of the template.
- The Format group contains commands to adjust the formatting of the text (HTML templates only).
- The Paragraph group contains commands to adjust the style of the text (HTML templates only).
- The Insert group contains commands to insert Hyperlinks, Pictures, Tables, Fields and Conditional Statements.

All templates share two common properties:

- The name of the template, used to uniquely identify each template.
- A description of the template, which is an optional field describing the template.

Depending on the type of the template, other properties are also available. These are discussed in the separate topics for each template type.

All templates in Email Signature Manager have two principal components:

- The HTML Template, which defines the content appended to HTML emails.
- The Plain Text Template, which defines the content appended to plain text emails.

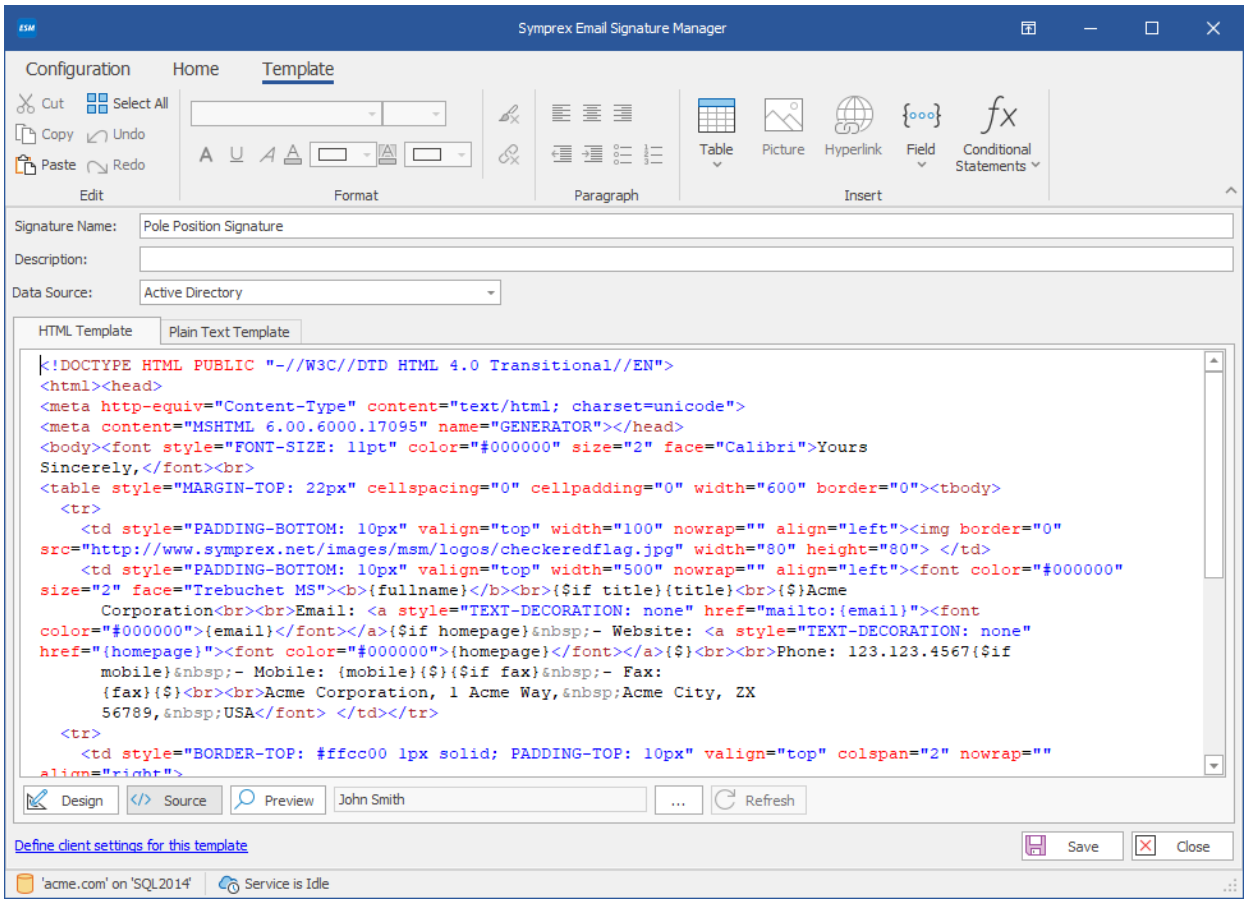
Note RTF signatures are generated automatically from HTML signatures.

Each component can contain fields (identified by { } braces), which are dynamically replaced by the appropriate user data from the selected data source when the template is deployed to each user. This means that templates are dynamic and their content can be tailored to suit your organization. Prior to deployment, you can test how your templates will appear for any user in your organization using the Test Signatures dialog.

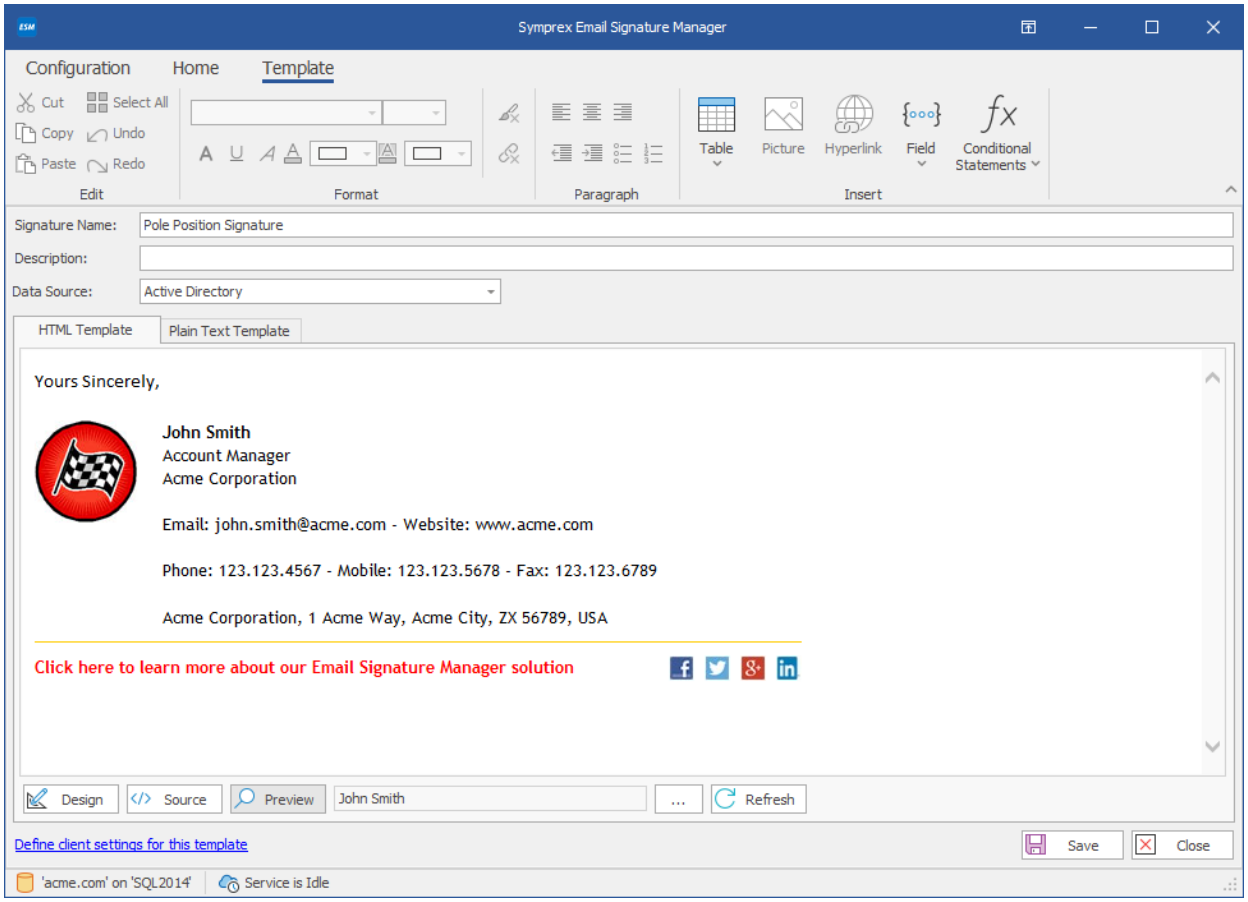
Please refer to the working with fields topic for detailed information on how to use fields in your templates.

Please also refer to the conditional statements topic for information about how to use conditional statements to for example avoid labels followed by empty fields.

All templates are designed in a WYSIWYG editor, however, for the HTML template, the source can also be modified directly by clicking the **Source** button:



While designing your template, you can, at any time, preview how it will look when merged with user data by clicking the **Preview** button:



The user for which the preview will be generated can be selected by clicking the ellipses ("...") button and the preview can be refreshed by clicking the **Refresh** button.

When you have finished designing your template, you can:

- Click the **Save** button to save the changes to your template.
- Click the **Close** button to close the template and return to the template browser; you will be prompted to save if you have made any changes.

It is recommended that you read the section of design guidance before authoring your templates to ensure you achieve the best results.

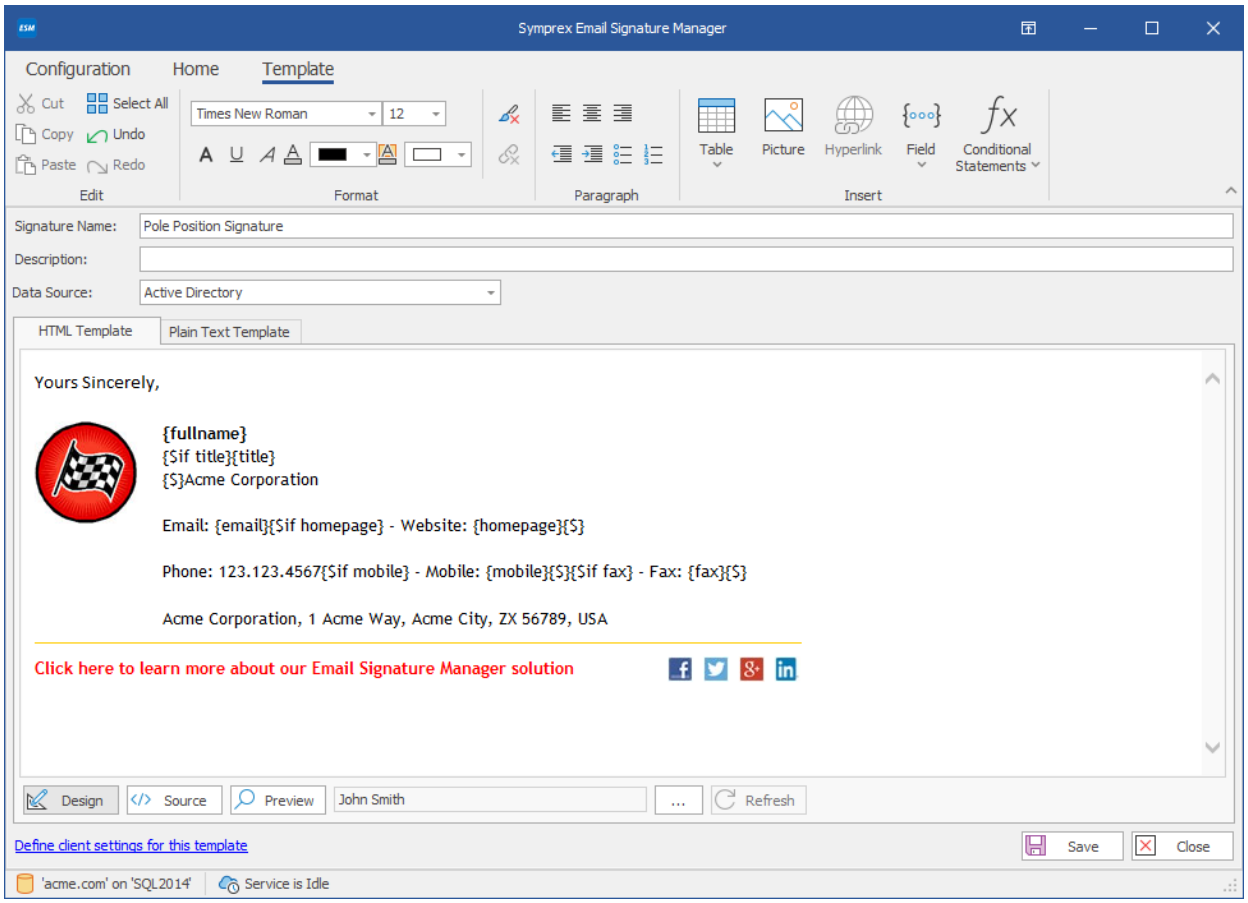
Signatures

A signature is the basic template used to sign your emails. The design of each signature should generally contain information about the author of the email and the organization. Legal information can be appended to signatures using disclaimers and news and marketing information can be appended using campaigns.

- To create a new signature, click the **Signature** button in the **Create** group in the **Home** ribbon on the main application window.
- To edit an existing signature, you can either:

- Select the signature in the template browser on the main application window and click the **Edit** button in the **Template** group of the **Home** ribbon, or
- Double-click the signature in the template browser, or
- Right-click the signature in the template browser and select **Edit** from the context menu.

When you create or edit a signature, the template editor will be opened:



Signatures can have the following properties configured:

- **Name**: The unique name of the signature (mandatory).
- **Description**: A description of the signature.
- **Data Source**: The data source from which the user data will be merged for the signature. By default, this will be Active Directory but can be set to any custom data source.

Client Settings for the template can be defined by clicking the **Define client settings for this template** link.

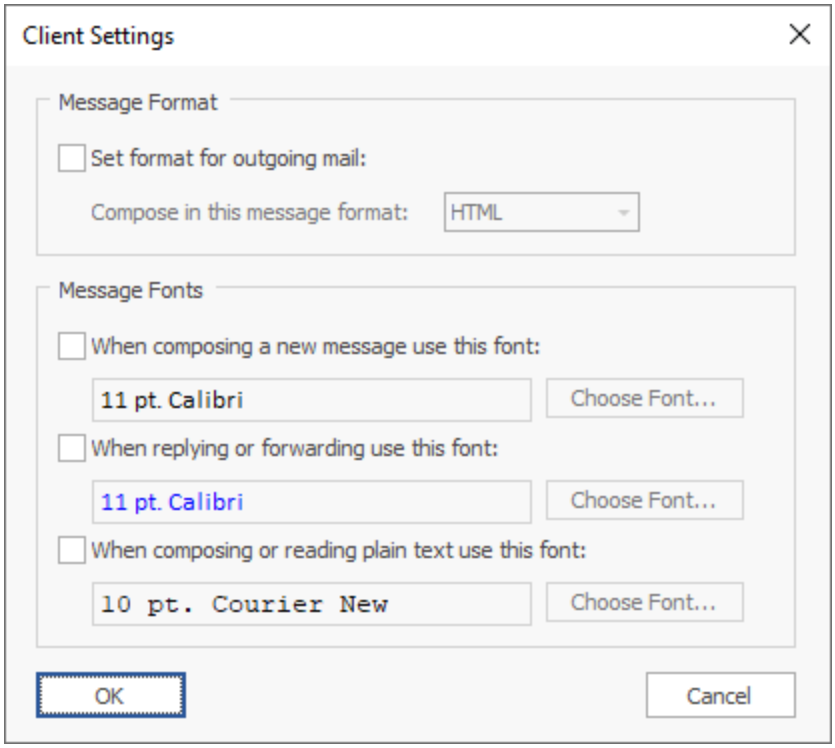
Note The client settings defined for the template will be applied when the signature is installed as the default signature for new emails for a user *unless* global client settings take precedence. Please review the section on deployment for further details.

- To save the changes and continue editing the signature, click the **Save** button.

- To close the editor and return to the template browser, click the **Close** button; you will be prompted to save if you have made any changes.

Client Settings

The Client Settings dialog is opened by clicking the **Define client settings for this template** link when editing a signature template.



Client settings are used to configure email preferences for writing emails in Microsoft Outlook.

Note Global client settings can also be specified in the Manage Deployment dialog which, depending on how they are configured, can override the settings defined in a template.

The following settings can be configured for the message format:

- **Set format for outgoing mail**: Specifies the format to be used for writing outgoing email. This can be either HTML, Rich Text or Plain Text.

The following settings can be configured for the message font:

- **Compose font**: Specifies the font and color that will be used when a user creates a new email.
- **Reply/Forward font**: Specifies the font and color that will be used when a user replies to or forwards an email.
- **Plain Text font**: Specifies the font that will be used to compose emails in plain text format.

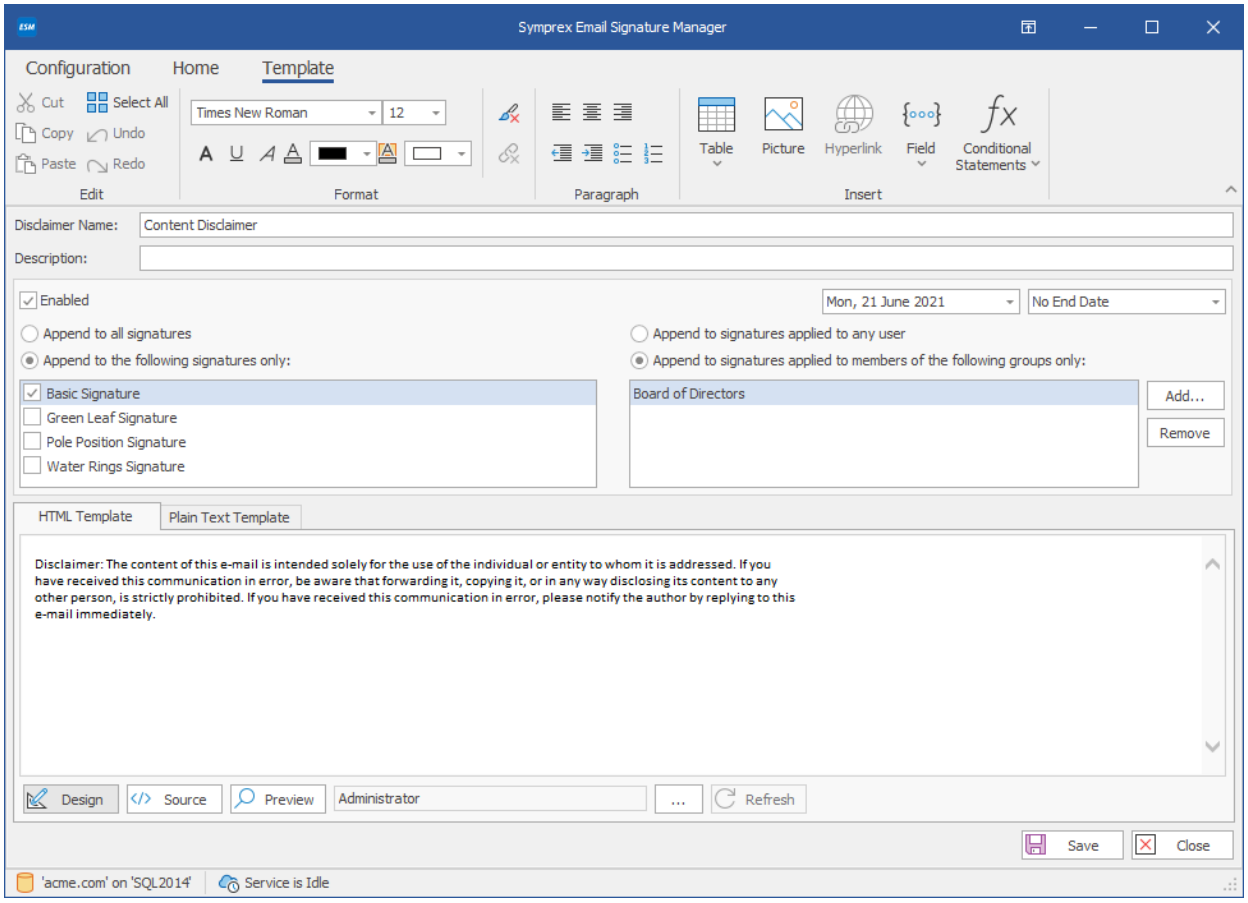
To accept the changes you have made, click the **OK** button. Otherwise, click the **Cancel** button to close the dialog.

Disclaimers

Disclaimers are generally used to add legal information to the end of the designated signatures; for example, this can be to give details of your organization's email policy.

- To create a new disclaimer, click the **Disclaimer** button in the **Create** group in the **Home** ribbon on the main application window.
- To edit an existing disclaimer, you can either:
  - Select the disclaimer in the template browser on the main application window and click the **Edit** button in the **Template** group of the **Home** ribbon, or
  - Double-click the disclaimer in the template browser, or
  - Right-click the disclaimer in the template browser and select **Edit** from the context menu.

When you create or edit a disclaimer, the template editor will be opened:



Disclaimers can have the following properties configured:

- **Name**: The unique name of the disclaimer (mandatory).
- **Description**: A description of the disclaimer.
- **Enabled**: Determines if the disclaimer is currently enabled. When enabled, the disclaimer is appended to the designated signatures.

- **Start Date**: Optionally specifies the date from which the disclaimer will be appended to the designated signatures.
- **End Date:** Optionally specifies the date until which the disclaimer will be appended to the designated signatures.
- **Append to all signatures:** When selected, specifies that the disclaimer is appended to all signatures.
- **Append to the following signatures**: When selected, the disclaimer is only appended to the signatures selected in the list.
- **Append to signatures applied to any user**: When selected, specifies that the disclaimer is appended to signatures for any user.
- **Append to signatures applied to members of the following groups only**: When selected, specifies that the disclaimer is appended to signatures for only members of the specified group or groups.

Note The fields in the disclaimer will be merged using the data source from the parent signature at the point of deployment.

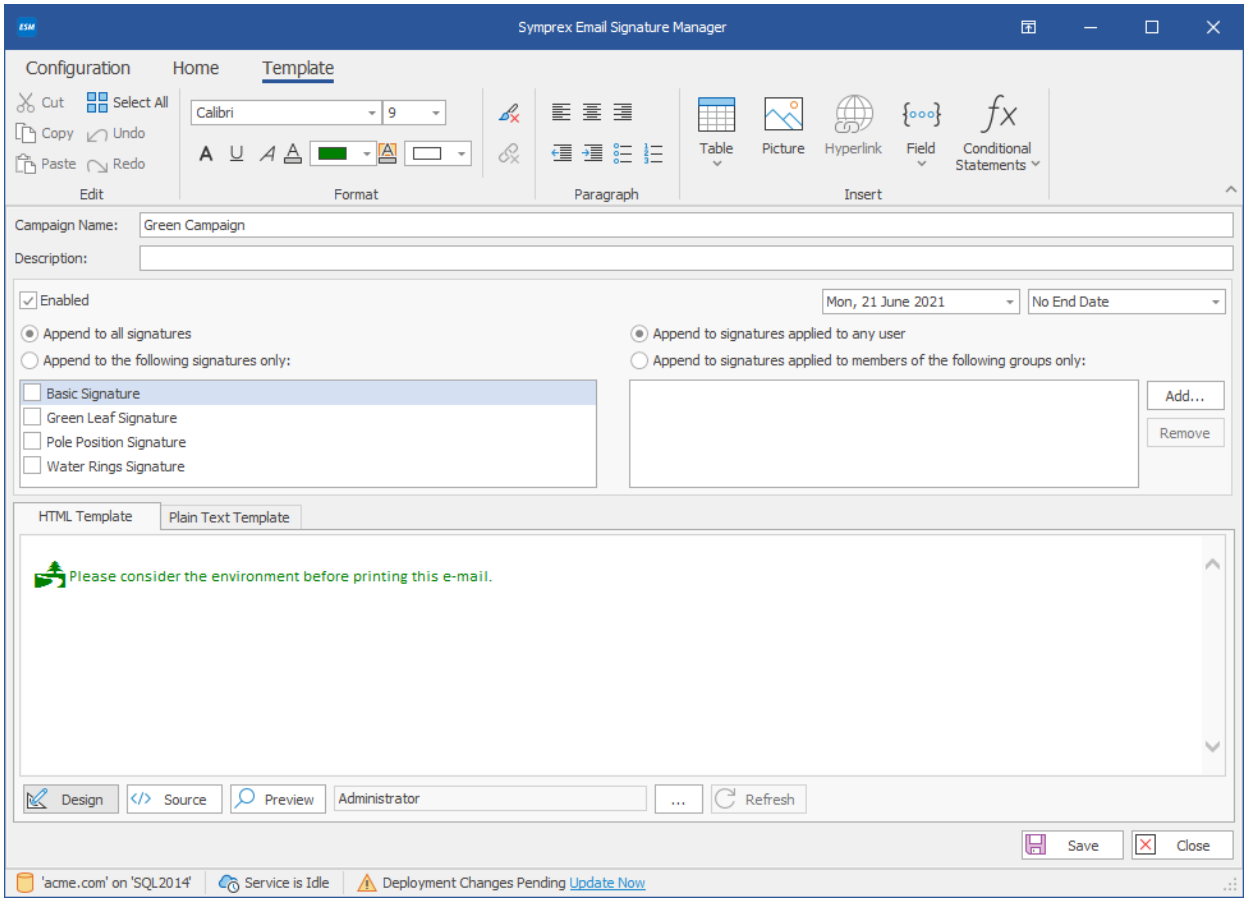
- To save the changes and continue editing the disclaimer, click the **Save** button.
- To close the editor and return to the template browser, click the **Close** button; you will be prompted to save if you have made any changes.

Campaigns

Campaigns are generally used to add news and marketing information to the end of the designated signatures; for example, to tell recipients of emails from your organization about a forthcoming promotion.

- To create a new campaign, click the **Campaign** button in the **Create** group in the **Home** ribbon on the main application window.
- To edit an existing campaign, you can either:
  - Select the campaign in the template browser on the main application window and click the **Edit** button in the **Template** group of the **Home** ribbon, or
  - Double-click the campaign in the template browser, or
  - Right-click the campaign in the template browser and select **Edit** from the context menu.

When you create or edit a campaign, the template editor will be opened:



Campaigns can have the following properties configured:

- **Name**: The unique name of the campaign (mandatory).
- **Description**: A description of the campaign.
- **Enabled**: Determines if the campaign is currently enabled. When enabled, the campaign is appended to the designated signatures.
- **Start Date**: Optionally specifies the date from which the campaign will be appended to the designated signatures.
- **End Date:** Optionally specifies the date until which the campaign will be appended to the designated signatures.
- **Append to all signatures:** When selected, specifies that the campaign is appended to *all* signatures.
- **Append to the following signatures**: When selected, the campaign is only appended to the signatures selected in the list.
- **Append to signatures applied to any user**: When selected, specifies that the campaign is appended to signatures for any user.
- **Append to signatures applied to members of the following groups only**: When selected, specifies that the campaign is appended to signatures for only members of the specified group or groups.

Note The fields in the campaign will be merged using the data source from the parent signature at the point of deployment.

- To save the changes and continue editing the campaign, click the **Save** button.

- To close the editor and return to the template browser, click the **Close** button; you will be prompted to save if you have made any changes.

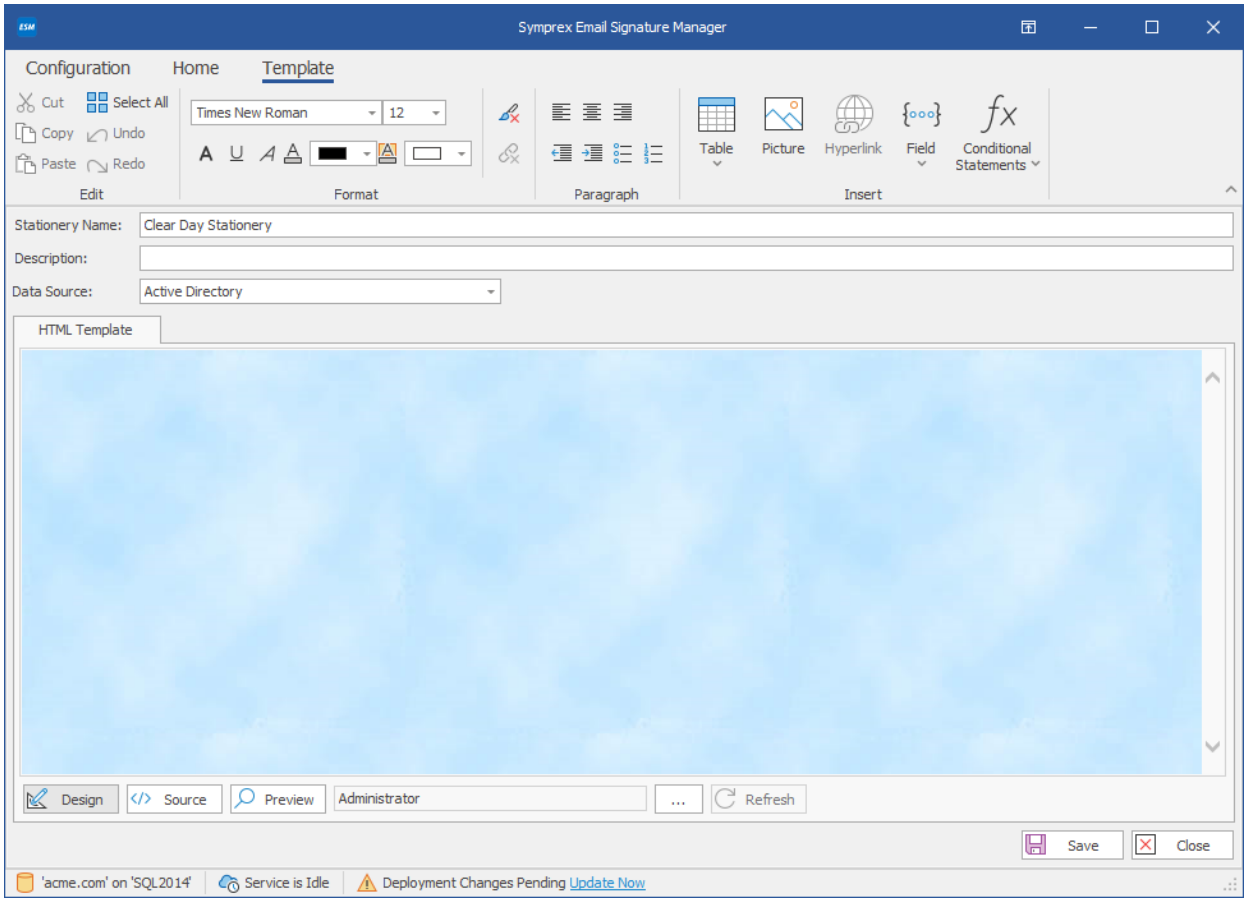
Stationery

Stationery can be used to set background images for HTML messages authored in Microsoft Outlook.

To create new stationery, click the **Stationery** button in the **Create** group in the **Home** ribbon on the main application window.

- To edit existing stationery, you can either:
  - Select the stationery in the template browser on the main application window and click the **Edit** button in the **Template** group of the **Home** ribbon, or
  - Double-click the stationery in the template browser, or
  - Right-click the stationery in the template browser and select **Edit** from the context menu.

When you create or edit stationery, the template editor will be opened:



Stationery can have the following properties configured:

- **Name**: The unique name of the stationery (mandatory).
- **Description**: A description of the stationery.

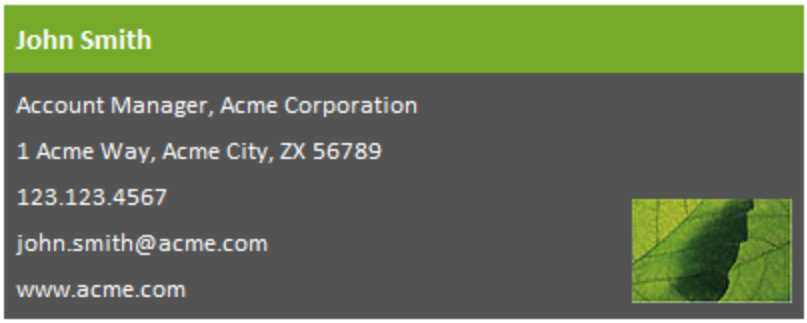
Note Stationery can only be applied to HTML messages authored in Microsoft Outlook. Hence, the Plain Text Template tabs are not available for stationery.

- To save the changes and continue editing the stationery, click the **Save** button.
- To close the editor and return to the template browser, click the **Close** button; you will prompted if changes have been made.

Dynamic Fields

Dynamic Fields is a very powerful feature in Email Signature Manager. Each component (HTML, Rich Text and Plain Text) of a template is essentially the final content that will be deployed but instead of actual user information, field markers (dynamic fields) are inserted where the real user information will be inserted (or *merged*). This is illustrated in the simple signature below:

In this example, most of the content will be populated dynamically at the point of deployment. For example, the `{fullname}` field will be replaced by the user's full name from the data source for the template (the data source is normally Active Directory but custom data sources can be configured). The deployed signature would appear something like the following example:



This examples demonstrates basic use of simple fields in signatures; a full list of the available fields is listed in the appendix.

Formatting a Field Value in Upper, Lower or Title Case

Field values can be formatted to be in upper, lower or title case as follows:

- **Upper Case**: Add the `:U` suffix to the field name, for example `{fullname:U}`
- **Lower Case**: Add the `:L` suffix to the field name, for example `{fullname:L}`
- **Title Case**: Add the `:T` suffix to the field name, for example `{fullname:T}`

Disabling Encoding of Field Values

When a field value is inserted into a signature, it is encoded to HTML to ensure it appears correctly. However, this may not be the desirable behaviour if the field contains HTML that should be used directly in the signature *without* being encoded. To disable encoding of field values, add the `:N` suffix; for example `{description:N}`.

Use any Active Directory Property Value

The pre-defined fields available in Email Signature Manager are the most commonly used fields for signatures. However, it is possible to obtain the value of *any* Active Directory property by using the following syntax:

```
{#propertyname}
```

where `propertyname` is the name of the property. If the property has multiple values, a specific value can be obtained using the following syntax:

```
{#propertyname(index)}
```

where `(index)` is the is 1-based index of the value to be used. A list of some Active Directory fields that can be useful in signatures can be found here.

Replacing Field Values

Field values has been replaced with alternative values from a specified list using a replacement function. There are four such functions, with two distinct modes. The replacement function is specified after the field name as follows:

```
{fieldname:function("","","")}
```

where:

- `fieldname` is the name of the field whose value is to be replace.
- `function` is the appropriate replacement function, as set out below.
- the comma-separated list of match and replacement values; each value must be specified in quotes.

Match Value and Replacement Value Specified in Pairs

In this mode, the replacement function accepts a list of pairs of values; the first value is the value to be matched and the second value is the replacement value:

```
"<Match One>","<Replacement One>","<Match Two>","<Replace Two>",...,"<Match N>","<Replace N>"
```

When the function is applied, all instances of each match value found in the field is replaced with the associated value. There are two version of this function:

Function	Description
r	Perform replacement using a case insensitive comparison according to the paired list of match values and associated replacement values.
rc	Perform replacement using a case sensitive comparison according to the paired list of match values and associated replacement values.

Example One: Ensure that departments are given consistent names in your signatures:

```
{department:r("hr","Human Resources","finance","Finance Department")}
```

This would perform a case insensitive comparison, replacing "hr" with "Human Resources" and "finance" with "Finance Department".

Example Two: Ensure consistent formatting of phone numbers:

```
{phone:r(" ","-")}
```

This would replace all spaces in the telephone number with a hyphen, for example "901 555 1234" would become "901-555-1234".

Multiple Match Values with a Single Replacement Value

In this mode, the replacement function accepts a list of values where the last value is the replacement value and all preceding values are the match values:

```
"<Match One>","<Match Two>",...,"<Match N>","<Replace>"
```

When the function is applied, all instances of each match value found in the field is replaced with the last value in the list. There are two version of this function:

Function	Description
rl	Perform replacement using a case insensitive comparison according to the list of match values and using the last value for the replacement.
rlc	Perform replacement using a case sensitive comparison according to the list of match values and using the last value for the replacement.

Example One: Ensure that a consistent phone number is used for certain numbers (such as converting geographic numbers to non-geographic free-phone numbers):

```
{phone:rl("01234 123456","01234 654321","0800 123 4567")}
```

This would replace telephone numbers "01234 123456" and "01234 654321" with 0800 123 4567.

Example Two: Ensure consistent formatting of phone numbers:

```
{phone:rl("-","  "," ")}
```

This would replace all double spaces and hyphens in the telephone number would be replaced by a single space, for example "901-555 1234" would become "901 555 1234".

Wildcards

All of the replace functions support the use of wildcards in the match values. The following characters can be used:

- `*` : zero for more alpha-numeric characters
- `?` : any single character
- `#` : any single digit

Important: When wildcards are used, the match is performed against *whole* field value and the associated replacement value replaces the *whole* field value.

Example One: Ensure that a consistent phone number is used for all numbers:

```
{phone:r("01234 *","0800 123 4567")}
```

This would replace any telephone numbers starting "01234 " with "0800 123 4567".

Limiting Replacement to the First Match

It is possible to replace just the first match found at the the start or end of a field value using the hat (^) character.

Example: Ensure that telephone numbers start with the country dialing code:

```
{phone:r("0^","+44 0")}
```

This would cause any telephone numbers starting "0" with to be updated to start "+44 ", for example "01234 123456" would become "+44 1234 123456".

Escaping Characters

In order to use special characters in the value list, they should be escaped as follows:

- Quotation mark: `\"`
- Left angle-bracket: `\[`
- Right angle-bracket: `\]`
- Backslash: `\\`
- Hat: `\^` (only applicable at the end of a match value)

Conditional Statements

Conditional Statements is a very powerful feature in Email Signature Manager. They allow you to include or exclude part of a template based on whether or not there is data in a specific field. A common use of this feature is to avoid labels in front of empty fields.

If Conditional Statement

The `$if` conditional statement allows you to specify that the enclosed block of content should only be included if the specific field contains data.

The syntax for the `$if` conditional statement is:

```
{$if field}content to include when field contains data{$}
```

Example:

```
{$if mobile}Mobile: {mobile}{$}
```

Ifno Conditional Statement

The `$ifno` conditional statement allows you to specify that the enclosed block of content should only be included if the specific field contains no data or is null.

The syntax for the `$ifno` conditional statement is:

```
{$ifno field}content to include when field contains no data{$}
```

Example:

```
{$ifno mobile}Mobile: N/A{$}
```

Else Conditional Statement

The `$if` and `$ifno` statements can be combined with the `$else` statement to test for the inverse condition. This simplifies conditional statements as there is no need to define both `$if` and `$ifno` statements to test for a field value containing data or being empty.

The syntax for the `$else` conditional statement is:

```
{$if field}content to include when field contains data{$else}content to include when field contains
```

Example:

```
Mobile: {$if mobile}{mobile}{else}N/A{$}
```

Testing if Field Is Equal To a Specific Value

The `$if` statement can be used to test if a field value is equal to a specific value by using the `=` operator and using the following syntax:

```
{$if field="value"}content to include when field is equal to the specified value{$}
```

Example:

```
Country: {$if countrycode="GB"}Great Britain{$else}Somewhere else{$}
```

The comparison is case insensitive.

Testing if Field Is Not Equal To a Specific Value

The `$if` statement can be used to test if a field value is not equal to a specific value by using the `<>` operator and using the following syntax:

```
{$if field<>"value"}content to include when field is not equal to the specified value{$}
```

Example:

```
Country: {$if countrycode<>"US"}Not the United States{$else}The United States{$}
```

The comparison is case insensitive.

Testing if Field Is Like a Specific Value

The `$if` statement can be used to test if a field value is like a specific value by using the `%` operator and using the following syntax:

```
{$if field%"value"}content to include when field is like the specified value{$}
```

The tested value can include the following wildcards:

- `*` matches zero or more characters.
- `?` matches any single character.
- `#` matches any single digit.

Example:

```
Area Code: {$if phone%"0208*"}Outer London{$else}Somewhere else{$}
```

The comparison is case insensitive.

AND and OR Operators

Conditional statements support multiple comparisons in a single statement using the logical AND (`$and`) and OR (`$or`) operators, which combine the logical result from each comparison in the order in which they appear in the statement (i.e. the operators are evaluated from left to right with no precedence). For the AND operator to give a logical result of TRUE, both comparisons must give a logical result of TRUE. For the OR operator to give a logical result of TRUE, only one of the comparisons need give a result of TRUE. The syntax for using the operators is as follows:

```
{$if conditionOne $and conditionTwo $and conditionThree...}content to include when all of the condit
{$if conditionOne $or conditionTwo $or conditionThree...}content to include when one of the conditio
```

Examples:

```
{$if firstname $and lastname}{firstname} {lastname}{$else}{fullname}{$}
{$if firstname="John" $and lastname="Smith"}John Smith{$else}Not John Smith{$}
{$if firstname<>"John" $or lastname<>"Smith"}Not John Smith{$else}John Smith{$}
```

Additional Notes on Conditional Statements

When the "Remove trailing spaces from field values" option is enabled (configured through the Deployment Options dialog), any trailing spaces in field values will be removed before evaluating conditional statements. Field values that only contain one or more spaces will be trimmed to an empty value; this is desirable as such fields would generally be considered empty in relation to signatures.

When using conditional statements in HTML templates care needs to be taken to ensure that the correct HTML tags are either included or excluded in the conditional statement. This can be verified by checking the Source for the template in the template browser.

Avoiding Blank Lines

To avoid a blank line when a conditional statement that evaluates to false includes a whole full line, include the line break within the conditional statement. For example this template would result in a blank line between name and phone in signatures for users that do not have a mobile number:

```
{fullname}
{$if mobile}Mobile: {mobile}{$}
Phone: {phone}
```

To avoid the potentially empty line, the signature should be rewritten like this:

```
{fullname}
{$if mobile}Mobile: {mobile}
{$}Phone: {phone}
```

Note In HTML templates, you may need to either include or exclude line break tags (i.e. `<br>`) *inside* the end of the conditional statement to achieve the desired effect. When using paragraph tags (i.e. `<p>...</p>`), ensure that the tags will not become unbalanced by getting excluded by the conditional statement.

Template Design Guidance

To ensure that your signatures appear as expected when applied to emails, please read the following sections providing guidance on various aspects of template design.

Styling Templates

Use Only Inline CSS

When authoring templates in HTML, it is important to avoid using internal or external CSS style sheets, but to only use inline CSS to apply styles within the template content. This is because when templates are deployed to Outlook and OWA, or injected into emails by the Transport Agent, it is not possible to merge any CSS style sheet that may be present in an email with those in the template. This is also true when campaigns and disclaimers are appended to signatures.

In short, all styles within your HTML templates should be applied inline, for example:

```
<SPAN STYLE="font-family: arial; font-size: 10pt; color: black">Your text here</SPAN>
```

The best method to produce a clean template is to first complete the content of the template without any styles, and then apply the styles (such as bold, italic etc.) to the content as required. It is also recommended to avoid pasting into the HTML WYSIWYG editor from word processors, such as Microsoft Word, which may include a large amount of Word specific HTML tags and content, which can lead to formatting problems.

HTML and CSS Support in Outlook

Microsoft Outlook uses the HTML parsing and rendering engine from Microsoft Word to display HTML message bodies. The same HTML and CSS support available in Word is available in Outlook.

To learn about support for the HTML and CSS specifications provided by Word and Outlook please refer to the following Microsoft articles:

- Word 2007 HTML and CSS Rendering Capabilities in Outlook 2007 (Part 1 of 2)
- Word 2007 HTML and CSS Rendering Capabilities in Outlook 2007 (Part 2 of 2)

These articles provides reference documentation related to supported and unsupported HTML elements, attributes, and CSS properties.

Note that while the articles date back to 2006 and were written for Word 2007 and Outlook 2007, **the content remains valid for Office 2010, 2013, 2016, 2019 and 365**, and therefore remains valuable reference documentation when designing email signatures for the Outlook client.

More Information

Please refer to our Knowledge Base for more information on signature design.

Including Graphics

Email Signature Manager supports including images in signatures, such as logos, banners, social media icons, employee pictures and so on.

For best results:

- The best image formats for emails signatures are JPG and GIF.

- Use images that are the size they need to be in the HTML signatures.
- Ensure the `width` and `height` attributes on the HTML `img` tags are set correctly.
- Ideally ensure the `alt` attribute on the HTML `img` tags is set to an alternate text.
- Keep images on a web server and reference in HTML signatures using image URLs.
- Smaller image file sizes are better.

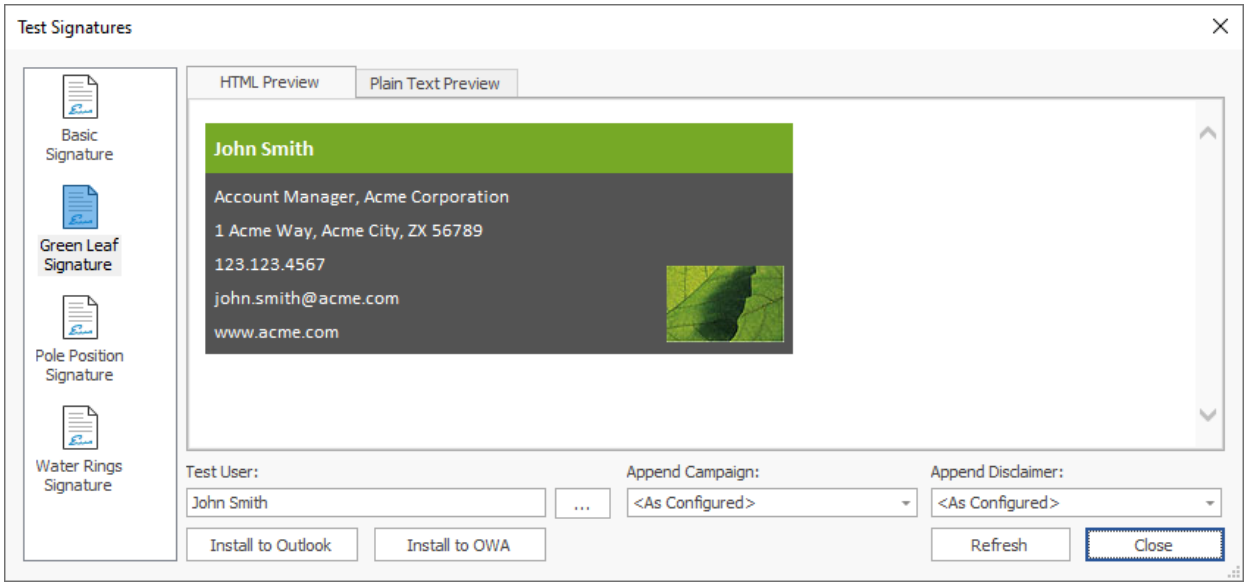
It is also worth noting the following:

- When sending email from Outlook, images can be linked or embedded (this is controlled in the Deployment Options dialog).
- When sending email from OWA and mobile devices, images are always linked.
- Microsoft email clients and most other email clients do not support animations.

Please refer to our Knowledge Base for more information on signature design.

Test Signatures

The Test Signatures dialog is opened by clicking the **Test** button in the **Templates** group in the **Home** ribbon on the main application window:



This dialog allows you to test how your signatures will look when deployed to your users, and can also install the signature preview directly to Outlook, OWA and Office 365.

- To preview a signature, select it from the list on the left side of the dialog (the preview automatically updates when a new signature is selected).
- The preview will be populated using the data source defined for the signature; see creating and editing signatures for details on how to change the data source.
- The preview will be populated using the data for the selected user. Click the ellipses ("...") button next to **Test User** to select a different user from Active Directory, and then click the **Refresh** button to see how the signature will be generated for that user.

- Alternatively, you can enter the account name for a user in the **Test User** box and click the **Refresh** button; the specified user will be loaded from Active Directory and the signature preview generated. The user can be specified using either the plain account name (e.g. "john.smith"), the DOMAIN\Account format (e.g. "MYDOMAIN\john.smith") or the account@domain format (e.g. "john.smith@mydomain.com").
- By default, the configured campaign(s) will be appended to the signature preview (see creating and editing campaigns for further details). To see how a specific campaign will look, select it from the **Append Campaign** list and click the **Refresh** button.
- By default, the configured disclaimer(s) will be appended to the signature preview (see creating and editing disclaimers for further details). To see how a specific disclaimer will look, select it from the **Append Disclaimer** list and click the **Refresh** button.

The current preview (i.e. the exact contents of the previewed signature, as currently displayed in the dialog) can be installed to a number of the supported platforms *for the currently logged on user* to see how it will look.

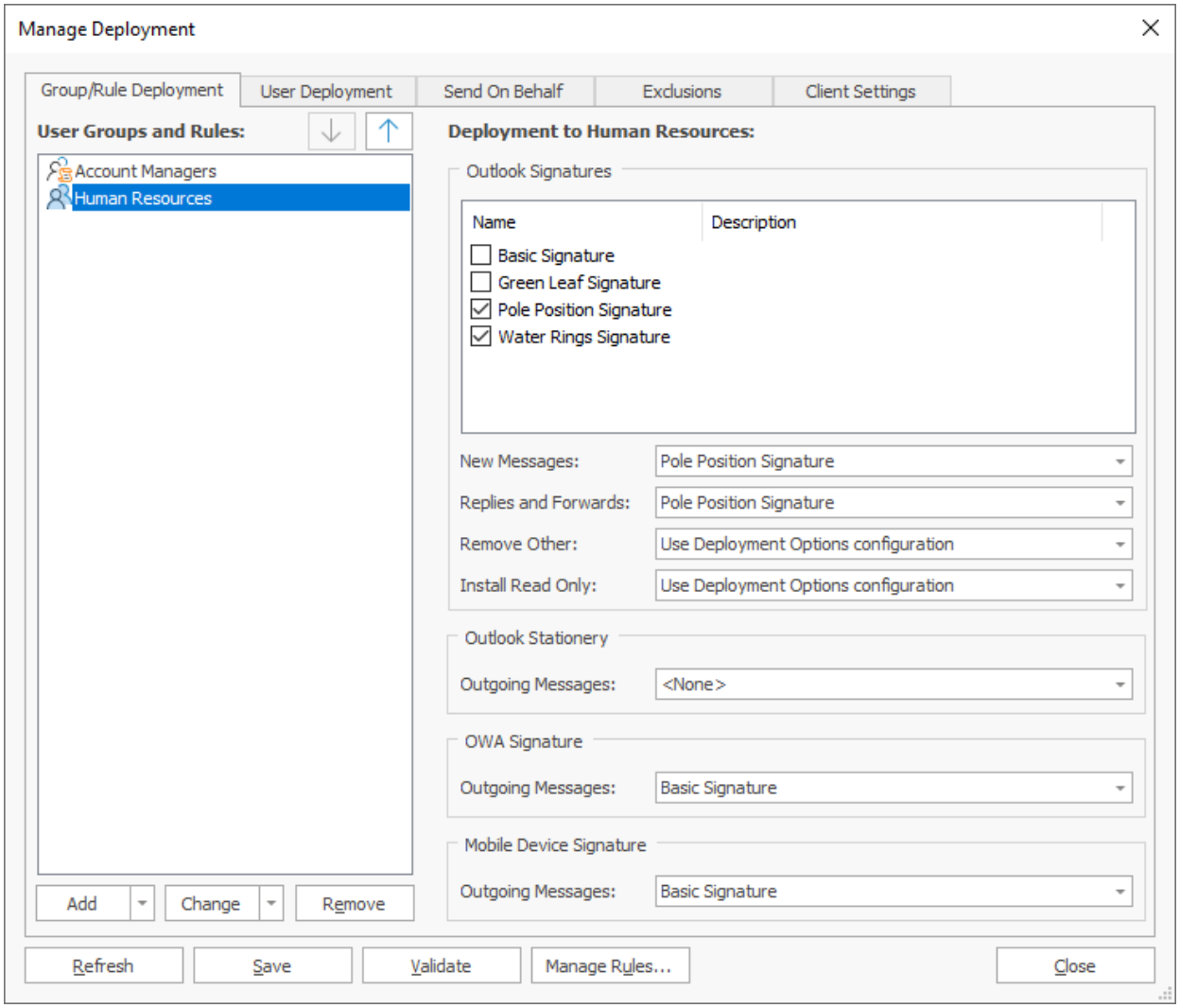
- To install to Outlook, click the **Install to Outlook** button. You will be prompted to confirm this action before the preview is deployed to Outlook as the default signature for new and reply/forwarded emails. Any client settings defined in the signature will also be applied and the deployment will use the settings configured in the Deployment Options dialog.
- To install to OWA on the local domain, click the **Install to OWA** button. You will be prompted to confirm this action before the preview is deployed as the default OWA signature. The deployment will use the settings configured in the Environment Configuration dialog and the *currently logged on user* must have a discoverable mailbox for the deployment to succeed.
- To install to Office 365, click the **Install to Office 365** button. You will be prompted to confirm this action before the preview is deployed to Office 365. This option is not available unless deployment to Office 365 has been configured using the Environment Configuration dialog and the *currently logged on user* must have an Office 365 hosted email account for the deployment to succeed.

Note Closing the dialog will not undo any test deployment of the previewed signature.

Once testing has been completed, click the **Close** button to close the dialog.

Manage Deployment

The Manage Deployment dialog is opened by clicking the **Manage Deployment** button in the **Deployment** group in the **Home** ribbon on the main application window:



Deployment of signatures to the users in your organization can be configured either by group membership (i.e. users will receive the signatures for the group to which they belong), rule-based membership (i.e. users will receive the signatures from a rule if they are included by that rule) or individually (i.e. per-user). The **Group/Rule Deployment** page manages the Active Directory groups and rules for which deployment has been configured, and the **User Deployment** page manages the individual Active Directory users for which deployment has been configured.

Important If deployment for a user has been specified both by group/rule membership and individually, then the individual deployment settings will take precedence.

Important If deployment for a user has been specified by membership of more than one group or rule, the deployment settings from the first group/rule (of which the user is a member) in the list will take precedence. The groups/rules can be ordered using the up and down arrows to set the desired precedence.

The **Group/Rule Deployment** page work as follows:

- The list of **Groups** and **Rules** is displayed on the left of the page; selecting a group or rule will display the deployment settings on the right of the page.
- To add a new group or rule, click the drop-down arrow on the **Add** button and select either **Group...** to add a domain group or **Rule...** to add a rule; you will be presented with a new dialog to select the group from Active Directory or the rule from the defined rules.
- To change the selected group or rule whilst preserving its deployment configuration, click the drop-down arrow on the **Change** button and select the appropriate option. The first option will allow the selected object to be changed for an object of the same type (for example, changing a domain group to another group), and the second option will allow the selected object to be changed for an object of the opposite type (for example, changing a domain group to a rule). In addition, when a rule is selected, click the **Edit Rule...** option to open the Manage Rule dialog for that rule.
- To remove the selected group or rule, click the **Remove** button.
- The selected group or rule can be moved up or down using the arrow buttons at the top of the list. The order of the groups/rules controls the precedence that will be used when determining deployment settings based on group membership.

The **User Deployment** page works as follows:

- The list of users is displayed on the left of the page; selecting a user will display their deployment settings on the right of the page.
- To add a new user, click the **Add...** button; you will be presented with a new dialog to select the user from Active Directory.
- To change the selected user whilst preserving their deployment configuration, click the **Change...** button; you will be presented with a new dialog to select the user to replace the selected user.
- To remove the selected user, click the **Remove** button.

With an object selected (group, rule or user), the following options are available to specify how signatures are deployed to that object:

- **Outlook Signatures**: Select the signatures that you wish to be installed to Microsoft Outlook for the group/rule/user. The selected signatures will then be available for the user to choose within Outlook for signing emails.
- **Outlook Signatures - New Messages**: Select the signature that will be set as the default signature for signing new emails. The default can be set to none by selecting "<None>" or it can be left unchanged by selecting "<Do Not Change>".
- **Outlook Signatures - Replies and Forwards**: Select the signature that will be set as the default signature for replying and forwarding emails. The default can be set to none by selecting "<None>" or it can be left unchanged by selecting "<Do Not Change>".
- **Outlook Signatures - Remove Other**: Select if any other signatures than specifically deployed (this includes any signatures that users have defined themselves) must be removed from Outlook. The default is to use the global **Remove all signatures other than those specifically deployed** setting specified in the Deployment Options dialog.
- **Outlook Signatures - Install Read Only**: Select the appropriate option for installing signatures read-only. The default is to use the global **Make signatures read only** and **Only overwrite user changes if template or user data changes** settings specified in the Deployment Options dialog.
- **Outlook Stationery - Outgoing Messages**: Select the stationery that will be set as the default stationery for outgoing messages. The stationery can be set to none by selecting "<None>" or it can be left unchanged by selecting "<Do Not Change>".

- **OWA Signature - Outgoing Messages**: Select the signature that will be set as the default signature for outgoing messages authored in OWA (Outlook Web Access/Outlook Web App/Outlook on the Web). The signature can be set to none by selecting "<None>" or it can be left unchanged by selecting "<Do Not Change>".
- **Mobile Device Signature - Outgoing Messages**: Select the signature that will be set as the default signature for outgoing messages on mobile devices. The signature can be set to none by selecting "<None>" or it can be left unchanged by selecting "<Do Not Change>".

The Mobile Device Signature is used as follows:

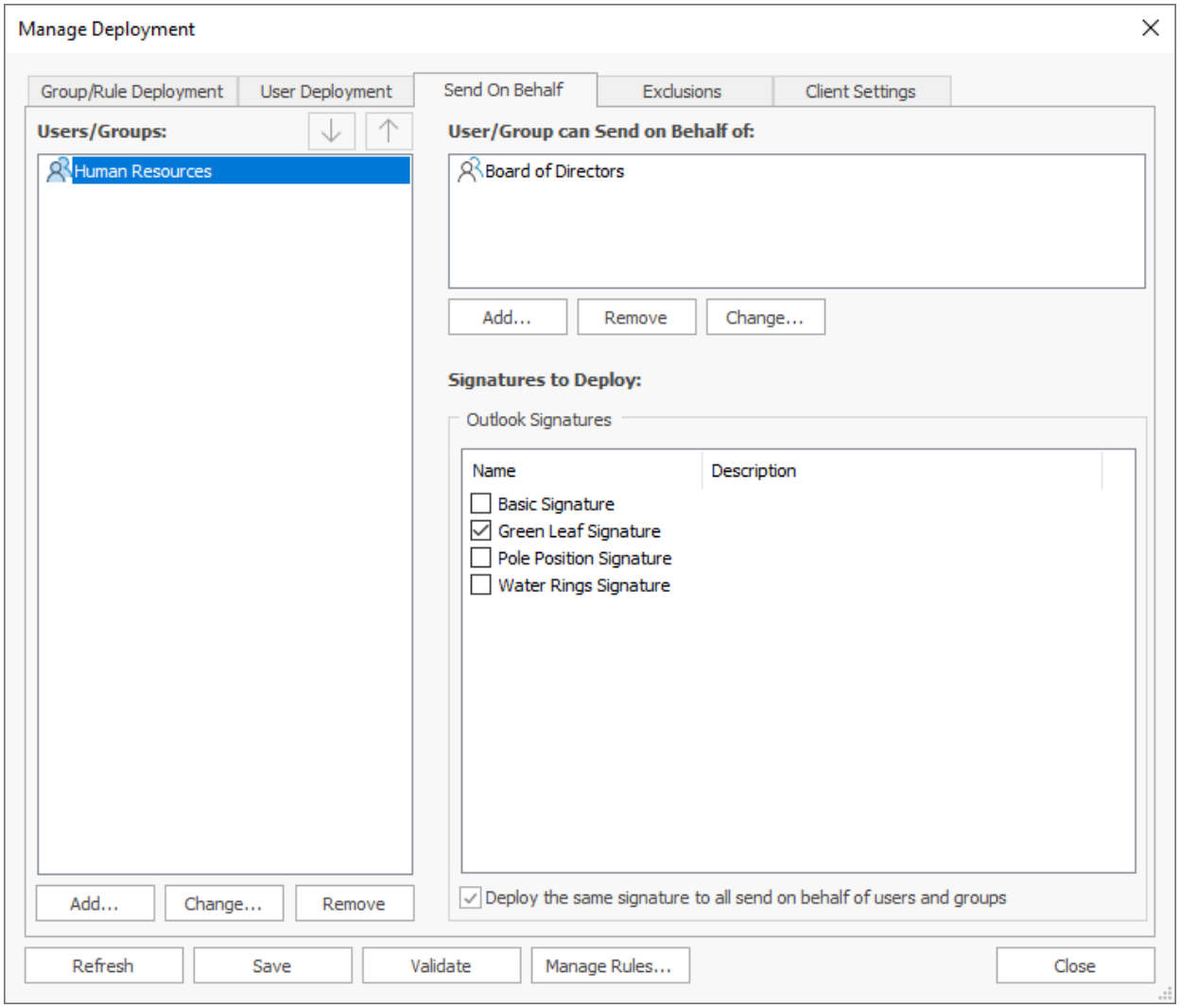
- Specifies the signature that is injected by the Transport Agent when emails are delivered through On-Premises Exchange Server.
- Specifies the signature that is emailed to the users in your organization when Send Signatures is enabled in the Mobile Device Signatures dialog.
- Specifies the signature that is injected by the Signature Injection Service for Office 365.

To refresh the deployment configuration from the database, click the **Refresh** button. To ensure that deployment is valid, click the **Validate** button. This will start a process that verifies each group, rule and user can be loaded from Active Directory, and updates as appropriate. If a certain object cannot be found, the icon for that object is updated to show that it is no longer valid. If this happens, either remove the object or replace it with a new object. To manage the rules that can be used to configure deployment, click the **Manage Rules...** button to open the Manage Rules dialog.

When the deployment has been configured as required, click the **Save** button to save your changes. Click the **Close** button to close the dialog; if you have made any changes, you will be prompted to save before the dialog is closed.

Send On Behalf

Send On Behalf settings are used to deploy additional Outlook signatures to users who send emails on behalf of other users within your organization:



The users who will receive send on behalf signatures during deployment are shown in the Users/Groups list on the left-hand side of the tab; users can be specified either individually or by group membership. The list can be modified using the buttons beneath it:

- To add a new user or group, click the **Add...** button; you will be presented with a new dialog to select the appropriate object from Active Directory.
- To remove the selected user or group, click the **Remove** button.
- To change the selected user or group whilst preserving the send on behalf configuration, click the **Change...** button; you will be presented with a new dialog to select the replacement object from Active Directory.
- The selected user or group can be moved up or down using the arrow buttons at the top of the list. The order (of the users and groups) controls the precedence that will be used when determining the send-on-behalf signatures received by each user.

The right-hand side of the tab is used to configure the send on behalf signatures that each user and group will receive. The Send on Behalf of list defines the users and groups for which signatures will be deployed to the selected object. The list can be modified using the buttons beneath it:

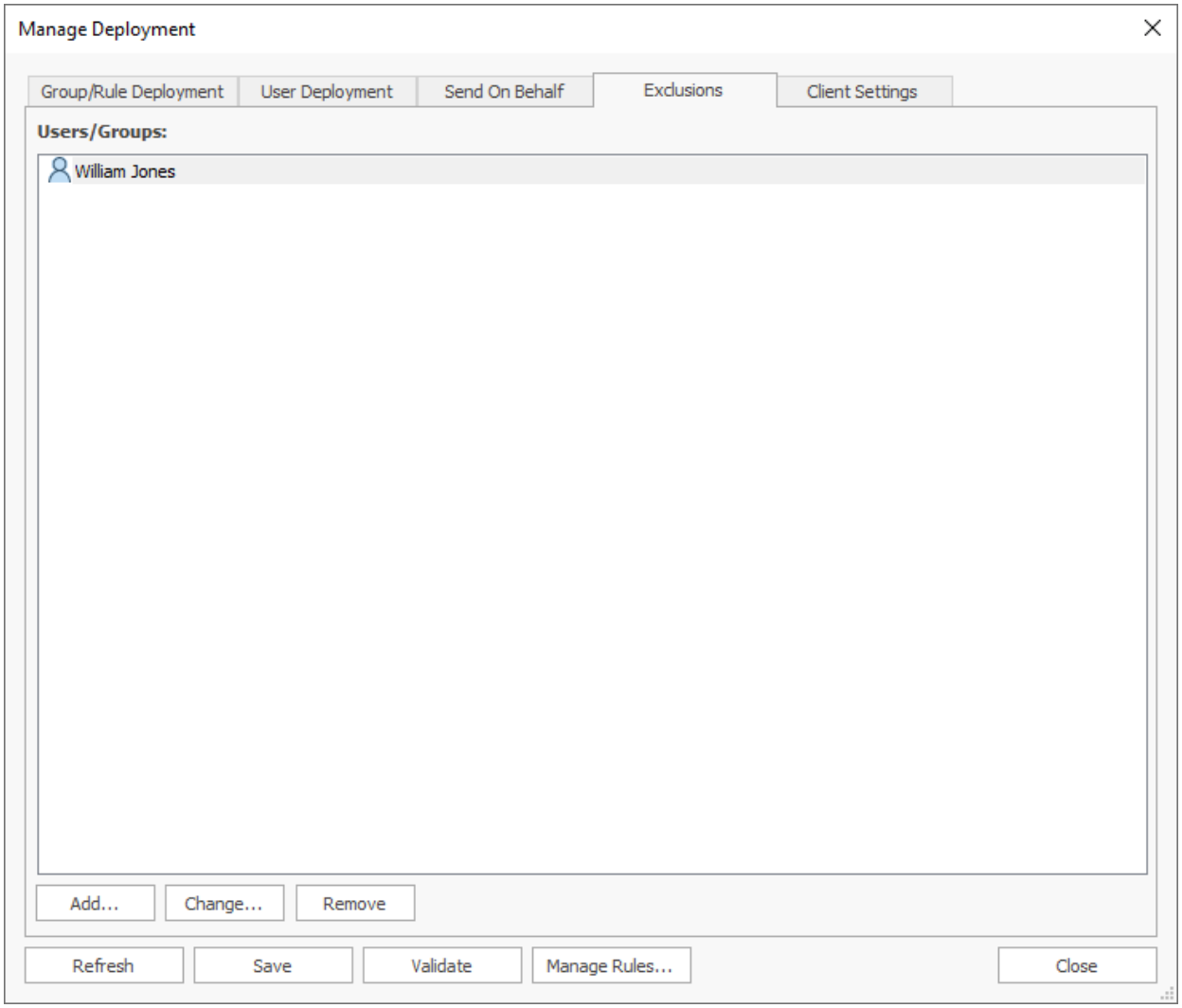
- To add a new send on behalf of user or group, click the **Add...** button; you will be presented with a new dialog to select the appropriate object from Active Directory.
- To remove the selected send on behalf of user or group, click the **Remove** button.
- To change the selected send on behalf of user or group whilst preserving the signature configuration, click the **Change...** button; you will be presented with a new dialog to select the replacement object from Active Directory

The Signatures to Deploy list defines which signatures will be deployed for the selected send on behalf of user or group; simply check each signature that should be deployed. The signatures can be specified either separately for each send on behalf of user and group, or can be specified for *all* of the send on behalf of users and groups (for the user or group selected in the left-hand list) by selecting the **Deploy the same signature to all send on behalf users** option.

For example, the configuration shown above defines that all users in the *Human Resources* group will have the *Green Leaf Signature* deployed with the details for all members of the *Board of Directors* group.

Exclusions

Exclusions are used to specify users who should not receive signatures:



When a user is excluded from deployment, the following actions are taken:

- Outlook signatures deployed using Email Signature Manager will be removed.
- OWA signature deployed using Email Signature Manager will be removed.
- Signatures for injection by the Email Signature Manager Transport Agent for Exchange will not be generated.

The Exclusions page works as follows:

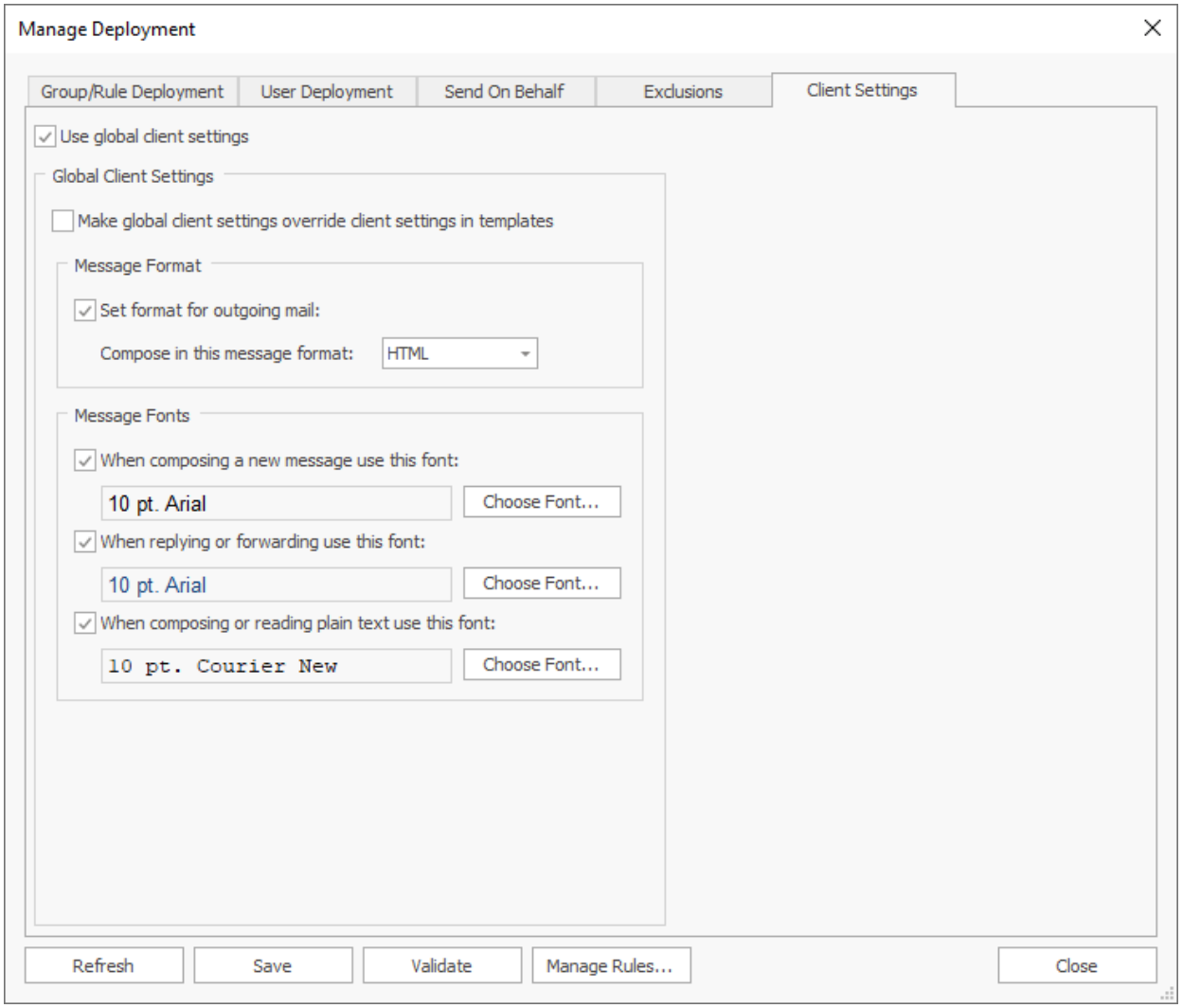
- The list of excluded users and groups is displayed in the main part of the page.
- To refresh the list of excluded users and groups, click the **Refresh** button.
- To add a new user or group, click the **Add...** button; you will be presented with a new dialog to select the group or user to be added from Active Directory.

- To remove the selected user or group, click the **Remove** button.
- To change the selected user or group, click the **Change...** button; you will be presented with a new dialog to select the group or user to replace the selected object.

Excluded users are reported in the Status Monitor dialog.

Global Client Settings

Global client settings are used to configure email preferences for all of the users in your organization when writing emails in Microsoft Outlook:



Select the **Enable global client settings** option to configure the client settings that will be applied to all users when templates are deployed.

If you wish to apply the global settings *ignoring* any settings made in your templates, select the **Make global client settings override client settings in templates** option. When this setting is not selected,

any settings found in your templates will be applied, and when no template settings are found, the global settings will be applied.

The following settings can be configured for the message format:

- **Set format for outgoing mail**: Specifies the format to be used for writing outgoing email. This can be either HTML, Rich Text or Plain Text.

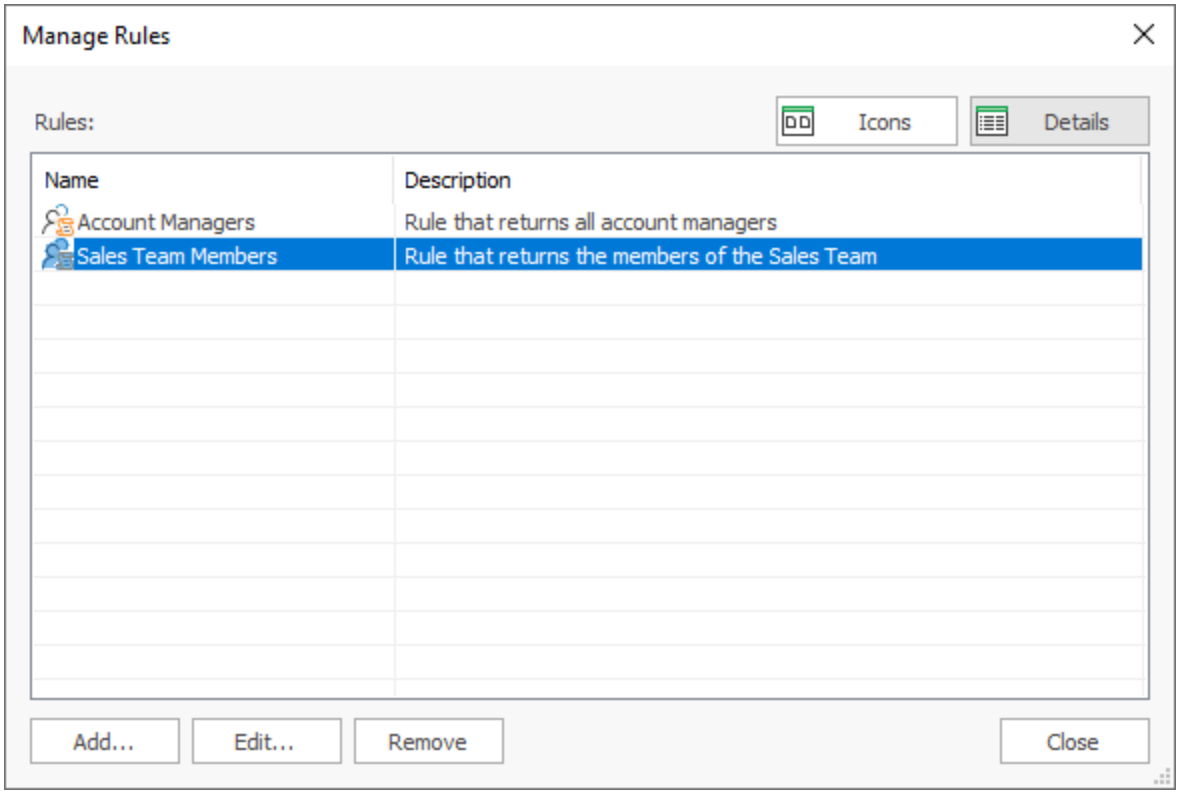
The following settings can be configured for the message font:

- **Compose font**: Specifies the font and color that will be used when a user creates a new email.
- **Reply/Forward font**: Specifies the font and color that will be used when a user replies to or forwards an email.
- **Plain Text font**: Specifies the font that will be used to compose emails in plain text format.

The global client settings will be applied to each user when signatures are being deployed to the user.

Manage Rules

The Manage Rules dialog is opened by clicking the **Rules...** button in the Manage Deployment dialog:



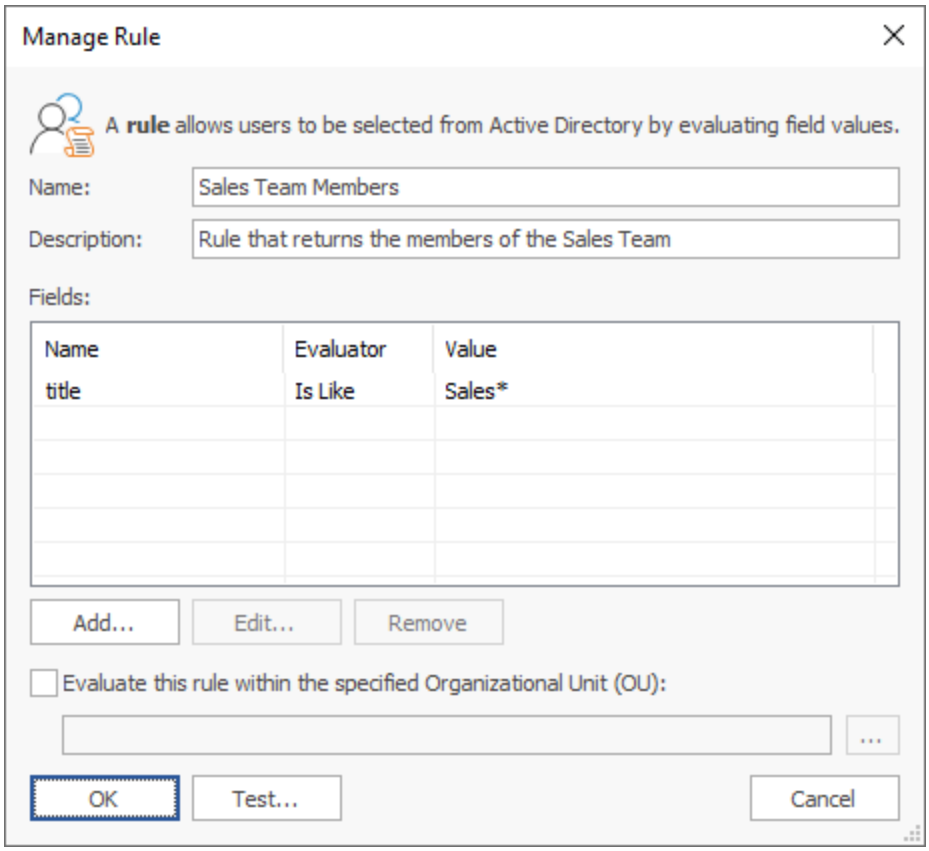
A rule in Email Signature Manager specifies a group of users to be selected from the domain by matching attribute values. Signatures and settings can then be applied using the rule as though it were a domain group.

The dialog shows the list of defined rules, and the view can be altered between **Icons** and **Details** using the buttons above the list. To create a new rule, click the **Add...** button to open the Manage Rule dialog, or to edit an existing rule, select it and click the **Edit...** button. To remove a rule, select it and click the **Remove** button. Note it is not possible to remove rules that are in use in the deployment configuration.

When the rules have been configured as required, click the **Close** button to close the dialog.

Manage Rule

The Manage Rule dialog is used to create or modify a rule for selecting users from the domain to be used as part of the deployment configuration. It is opened using either the **Add...** or **Edit...** button on the Manage Rules dialog.



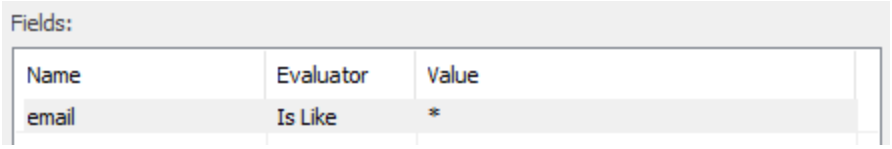
A rule is used to select users from the domain by matching specified attribute values.

Each rule has the following properties that can be modified:

Name	Description
Name	The name of the rule.
Description	A description of the rule.
Fields	The list of fields to be matched when evaluating a user. To add a new rule, click the **Add...** button. To edit a rule, select it and click the **Edit...** button. To remove rule, select it and click the **Remove** button.
Evaluate this rule within the specified Organizational Unit	Specifies if the rule should be evaluated against the users in the specified Organizational Unit (OU), rather than against all users in the domain (according to the current domain configuration).

Creating a new field or editing an existing field will open the Field Definition dialog. The results of evaluating the fields are logically combined using the AND operator i.e. all of the field definitions must match in order for a user to be included by the rule. To test that the rule is returning the expected users, click the **Test...** button to open the test dialog that will list the members returned by the rule.

It is possible to define a rule without any fields. This can be useful to return all users within a specific Organizational Unit (OU). If this approach is adopted, it is recommended that a single field matching on all email addresses is defined to ensure that only mail-enabled users are returned. This field would be configured as follows:



Once the rule has been configured, click the **OK** button to apply the changes and close the dialog, or click the **Cancel** button to close the dialog without saving changes.

Field Definition

The Field Definition dialog is used to create or modify a field within a rule for selecting users from the domain. It is opened using either the **Add...** or **Edit...** button on the Manage Rule dialog.

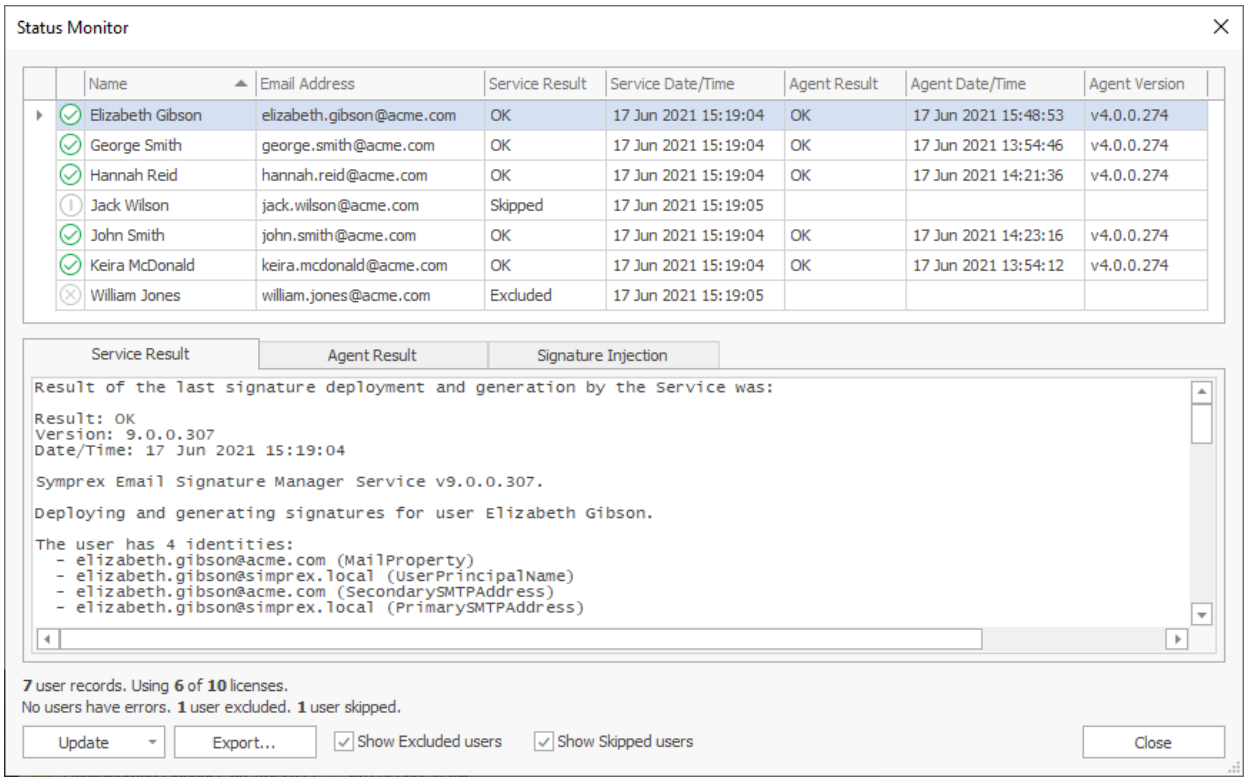
Each field definition has the following properties that can be modified:

Name	Description
Name	The name of the field or attribute to be evaluated. Select from the predefined list of the most commonly used fields, or enter the name of any Active Directory attribute.
Evaluator	The evaluator to be used when evaluating the value of the field.
Value	The value to be used when evaluating the field. The **Is Like** and **Is Not Like** evaluators support the wildcard (*) character.

Once the field has been configured, click the **OK** button to apply the changes and close the dialog, or click the **Cancel** button to close the dialog without saving changes.

Status Monitor

The Status Monitor dialog is opened by clicking the **Status Monitor** button in the **Deployment** group in the **Home** ribbon on the main application window:



Whenever a user is processed by the Email Signature Manager Service, or signatures are installed by the Email Signature Manager Agent, the results are written to the Status Monitor; this allows deployment to be monitored and verified remotely. The top of the dialog lists all of the users (with their email addresses) that have been processed by the service, together with the Service result and (where applicable) and the Agent result. The result can be one of the following:

- **OK**: Indicates that the Service successfully processed the user or the Agent successfully installed signatures.
- **Error**: Indicates that an error occurred during the processing or installation.
- **Skipped**: Indicates the user was not processed due to their configuration (for example, their account was disabled).
- **Excluded**: Indicates that the user was excluded from deployment (in the Manage Deployment dialog).
- **License Exceeded**: Indicates that the limit of users licensed has been exceeded.
- **Invalid License**: Indicates that the license for the application is invalid or missing.

Selecting a user from the list will show the detailed logs for that user the last time deployment was performed. There are a number of logs available, depending on your installation:

- **Service Result**: This log records the work that has been done processing the user by the Email Signature Manager Service.
- **Agent Result**: This log records the result of installing signatures by the Email Signature Manager Agent.
- **Signature Injection**: This log records the last signature injection performed by the Email Signature Manager Transport Agent. In order to log signature injection, it must be enabled on the Advanced page of the Deployment Options dialog.

Note For further information about the deployment methods available, please review the chapter on deployment.

The **Update** drop-down menu has the following commands:

- **Update All**: sends a command to the Email Signature Manager Service to generate and deploy signatures for all users (this is the same as clicking the **Update All** button in the **Deployment** group of the ribbon). Once the update has completed, the grid will be automatically refreshed.
- **Update Selected:** sends a command to the Service to generate and deploy signatures for the currently user. Once the update is complete, the row for the user will be refreshed.
- **Refresh Grid:** refreshes the grid with the latest deployment information from the database.

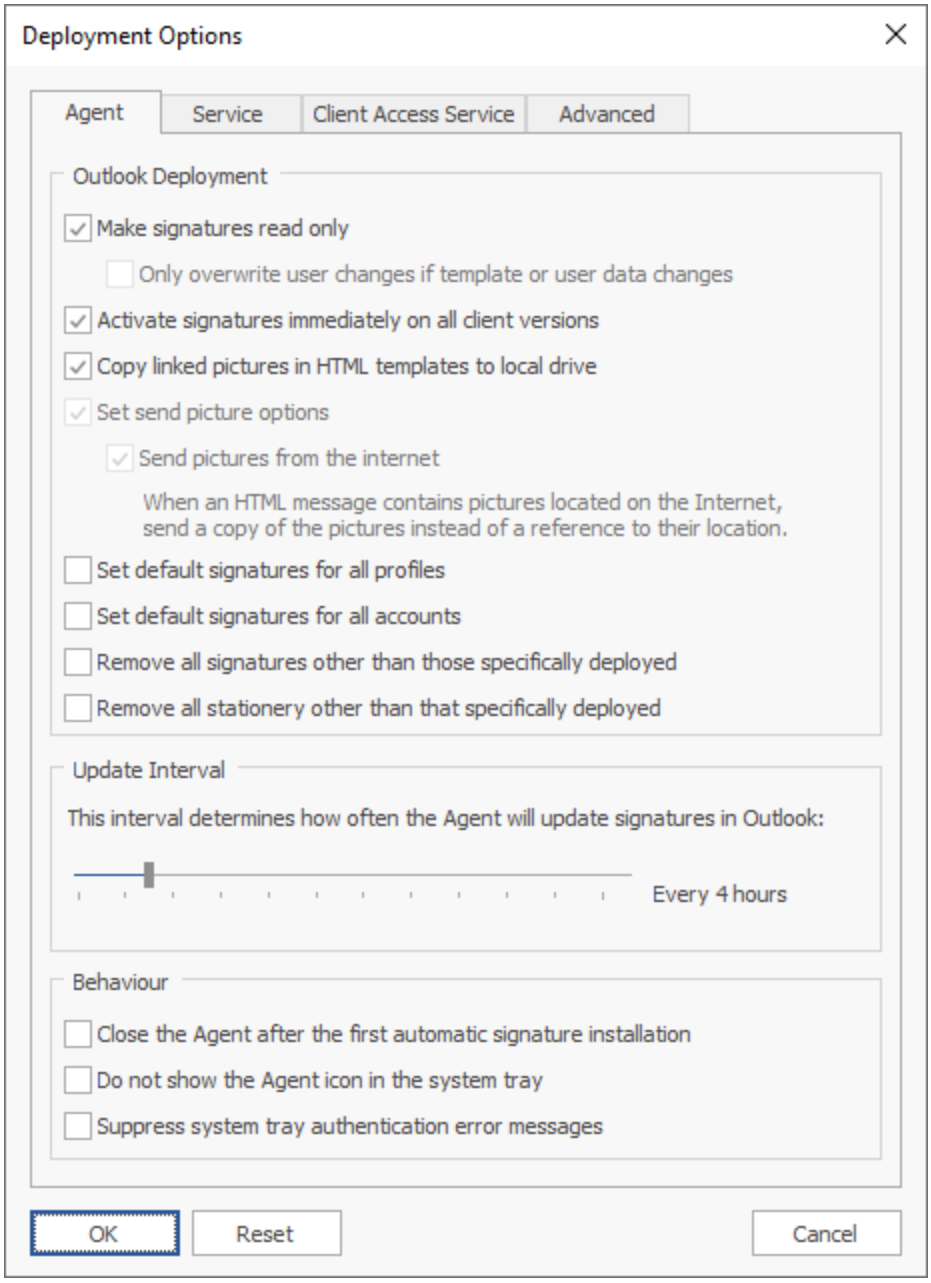
Users who were excluded can be shown or hidden by changing the **Show Excluded users** option, and users who were skipped can be shown or hidden by changing the **Show Skipped users** option as required; after changing these options, use the **Refresh Grid** button to refresh the list of users.

Note A user is excluded through the **Exclusions** tab on the Manage Deployment dialog. A user is skipped if they are configured in the Manage Deployment dialog but have not received any signatures.

To close the dialog, click the **Close** button.

Deployment Options

The Deployment Options dialog is opened by clicking the **Deployment Options** button on the Configuration page in the Configuration backstage of the main application window:



This dialog is used to configure system-wide settings used when deploying signatures to the users in your organization.

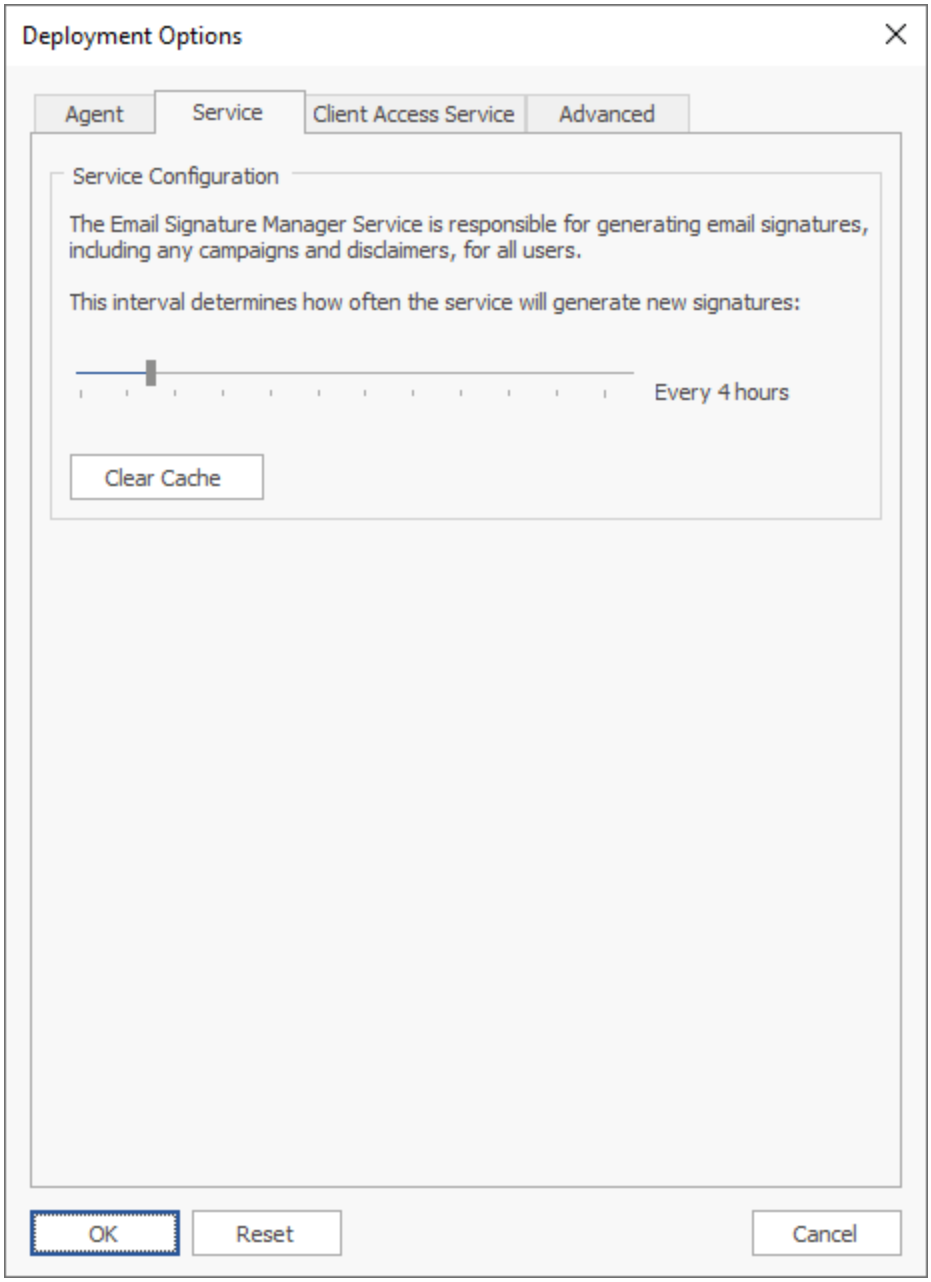
By default, the dialog is opened on the Agent page, which is used to configure the settings specific to deploying signatures to Microsoft Outlook. The following settings can be configured:

Setting	Description
Make signatures read only	Specifies that when the signatures are installed to Microsoft Outlook, they are marked as read-only. Enabling this option will make signatures read-only in the Signatures dialog in Outlook; this means that the actual signatures cannot be changed or removed.
Only overwrite user changes if template or user data changes	Specifies that only signatures that have been altered server-side (due to a change in their design or a change in the user's account information) will be written to disk, preserving any changes that the user makes locally to their signatures.
Activate signatures immediately on all client versions	Specifies that when signatures are deployed on a computer where Microsoft Outlook is already running, that the changes made will be activated immediately in Outlook without needing to restart.
Copy linked images in HTML templates to local drive	Specifies that linked images in HTML templates should be copied to the local drive on deployment. For example, if a template references an image on either a network drive (using a UNC path, such as `src="\\server\path\image.jpg"`) or located on the Internet (such as `src="http:\\www.mywebsite.com\image.jpg"`), that the image will be copied to the local drive and the local signature updated accordingly. Enabling this option ensures that images are correctly included when offline and composing email in Microsoft Outlook.
Send pictures options	When checked, will apply the Send pictures from the internet option when signatures are deployed by the Email Signature Manager Agent.
Send pictures from the Internet	When Outlook sends a message, this option determines if pictures located on the Internet are sent as a reference (i.e. the URL for the image is preserved in the email) or embedded as inline images. This option is not configurable in Microsoft Outlook 2007 and later and hence, Email Signature Manager is an ideal way to configure this setting for your users.
Set default signatures for all profiles	Specifies that the default signatures (for new and reply/forward emails) will be set on all mail profiles, not just the default profile.
Set default signatures for all accounts	Specifies that the default signatures (for new and reply/forward emails) will be set on all accounts, not just the default account (the default account in profile is the first Exchange account).
Remove all signatures other than those specifically deployed	Specifies that any signatures not specifically deployed using Email Signature Manager will be deleted; this includes any signatures that the users have defined themselves.
Remove all stationery other than that specifically deployed	Specifies that any stationery not specifically deployed using Email Signature Manager will be deleted; this includes any stationery that the users have defined themselves.
Update Interval	Specifies how often the Email Signature Manager Agent will update signatures in Outlook.
Close the Agent after the first automatic signature installation	Specifies that each time the Agent is executed, it will automatically close once signatures have been updated. This is the behaviour of the deployment tool (sign.exe) from previous versions of Email Signature Manager.
Do not show the Agent icon in the system tray	Specifies that the icon for the Agent is not displayed in the system tray. When this option is enabled, it is not possible for end users to close the Agent without using Windows Task Manager.
Suppress system tray authentication error	Specifies that the Agent will not show the popup notification in the system tray if an authentication error occurs when communicating with Exchange Web

When the settings have been configured as required, click the **OK** button save your changes and close the dialog. Alternatively, click the **Reset** button to return all settings to their defaults or click the **Cancel** button to close the dialog without saving any changes.

Service Page

The Service page on the Deployment Options dialog is used to configure the Email Signature Manager Service:



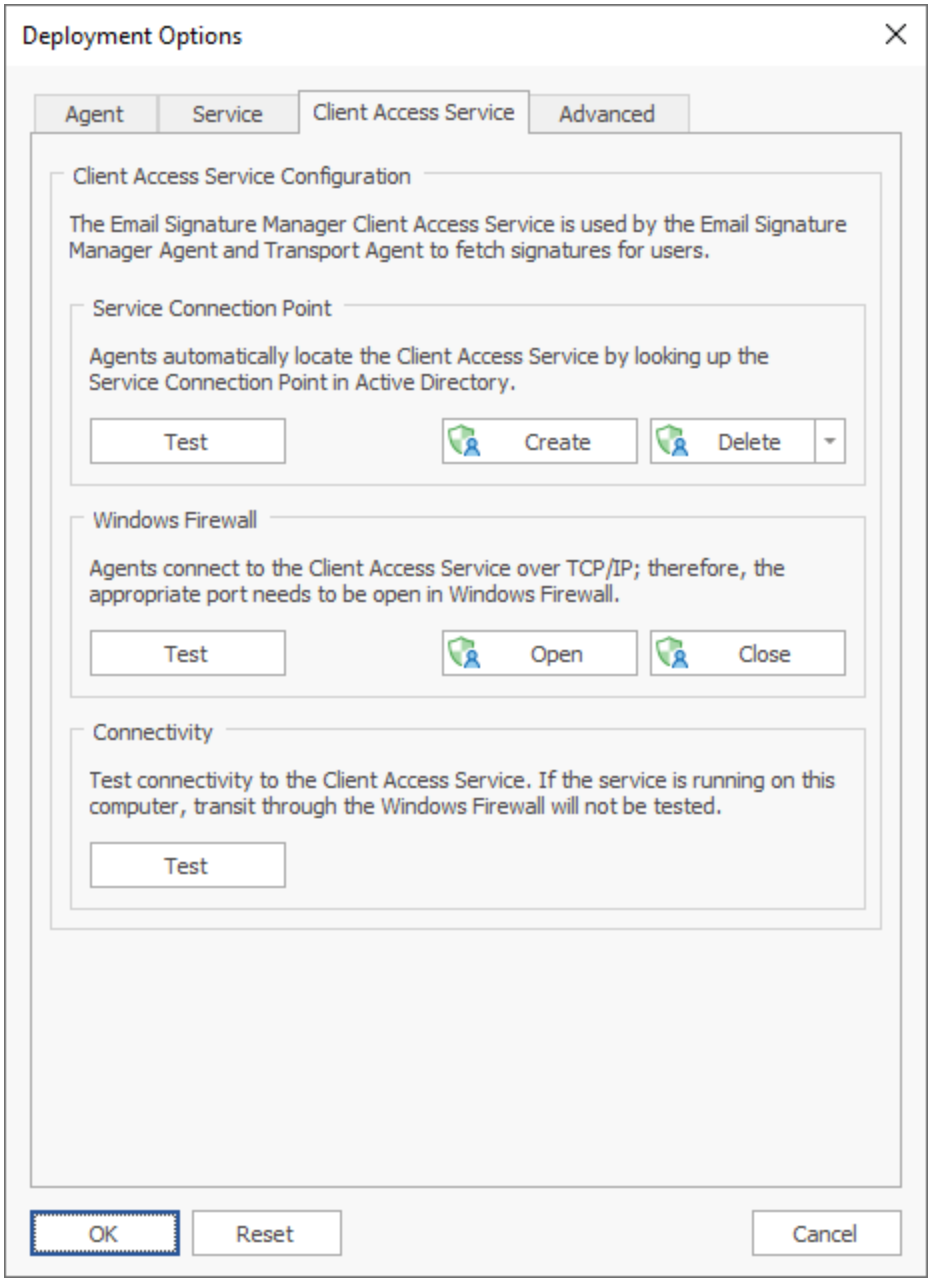
The following settings can be configured:

Setting	Description
Interval	Specifies how often the service will update signatures for the users in your organization.

When the Email Signature Manager Service updates user signatures, it uses Exchange Web Services (EWS). For efficiency, the EWS servers located during the Autodiscover process are cached in the database. In normal circumstances, this cached data will remain valid but if any problems are experienced, the service will automatically clear the cached data and repeat the Autodiscover process. However, in some rare circumstances, it may be necessary to manually clear the cached data for all users to force the Autodiscover process to be repeated and all signature settings to be written to the user mailboxes. To clear the EWS cache, click the **Clear Cache** button. The Service must be stopped in order to clear the cache.

Client Access Service

The Client Access Service page on the Deployment Options dialog is used to configure the Email Signature Manager Client Access Service:



The Client Access Service (CAS) itself has no direct configuration available. However, this page can be used to ensure that the server has been correctly configured for connections to be made to the CAS.

The **Service Connection Point** group manages the Service Connection Point (SCP) in Active Directory, which the Agent uses to locate the CAS automatically. To test that the SCP is present, click the **Test** button in this group. This will query Active Directory for all known SCPs (there should only be one) and display the results. If the SCP is missing, click the **Create** button (only available on the server where the CAS is installed) to create (or update) it in Active Directory. Alternatively, the SCP can be removed from Active Directory by clicking the **Delete** button. If multiple (redundant) SCPs are present in the domain, click the drop-down arrow on the **Delete** button and select the **All Service Connection Points in this Domain**

option. This will delete all of the SCPs for the Client Access Service in your domain (the SCP for the local machine should then be recreated using the Create button).

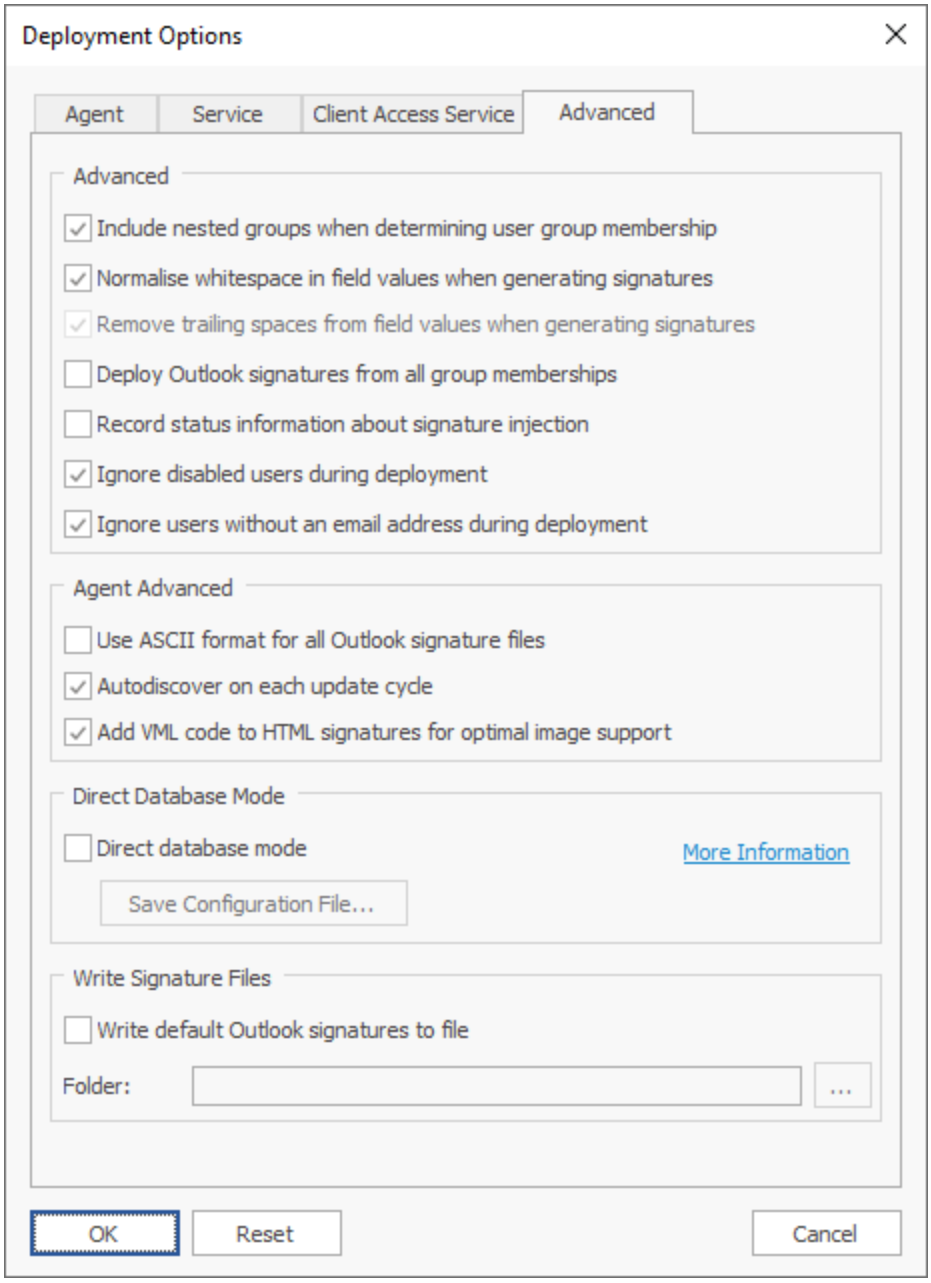
The **Windows Firewall** group manages the TCP/IP port (5757 by default) that needs to be open in Windows Firewall to allow inbound connections to the CAS. To test that the port is open, click the **Test** button in this group. This will query Windows Firewall and display the results. If required, click the **Open** button (only available on the server where the CAS is installed) to create a new rule Windows Firewall to open the port. Alternatively, the port can be closed by clicking the **Close** button.

The **Connectivity** group contains just a single button to test connectivity to the CAS. Clicking the **Test** button will run a test to lookup the SCP in Active Directory and then connect to the CAS at the location it specifies. If the connection is successfully established, the version of the CAS is queried and reported.

Note If the connectivity test is performed from the server where the CAS is installed, transit through the Windows Firewall will not be tested (as the connection will be made locally on the server).

Advanced Page

The Advanced page on the Deployment Options dialog is used to configure common deployment settings:



The following settings can be configured:

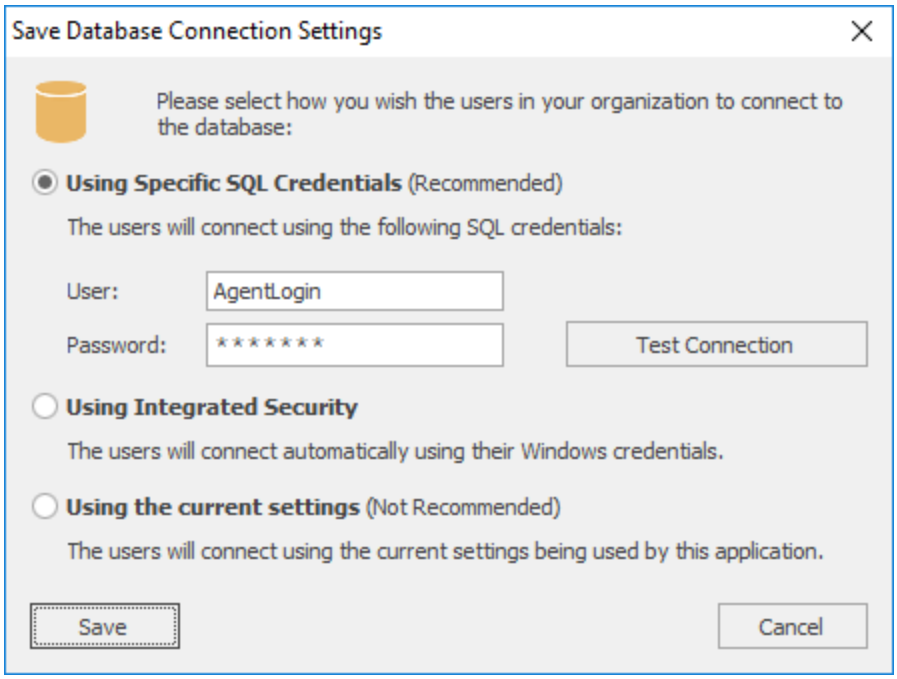
Setting	Description
Include nested groups when determining user group membership	Specifies that nested sub-groups should be included when determining user group membership during deployment of signatures.
Normalise whitespace in field values when generating signatures	Specifies that all whitespace in field values (newlines, tabs and spaces) are normalised to single spaces between words, and all leading and trailing whitespace removed; for example, " A Field Value " would become "A Field Value". This setting can be used to ensure that conditional statements in templates are evaluated correctly and the field values are formatted consistently. For further information, see the chapter on working with fields.
Remove trailing spaces from field values when generating signatures	Specifies that trailing spaces should be removed from field values when generating signatures; field values containing only spaces will be trimmed to empty values. For further information, see the chapter on working with fields.
Deploy Outlook signatures from all group memberships	Specifies that the Outlook signatures will be installed from *all* groups to which a user belongs. The main configuration (default signatures, OWA signature and mobile device signature) is determined either from the user's individual deployment configuration or from the deployment configuration for the first group to which the user belongs in the prioritized order.
Record status information about signature injection	Specifies that additional information is recorded to the Deployment Status log when signatures are injected into emails (by the Email Signature Manager Transport Agent). It is recommended that this option is not enabled unless specific logging information about the Transport Agent is required.
Ignore disabled users during deployment	Specifies that users whose account is disabled are ignored during deployment i.e. there will not be a record for them in the Status Monitor dialog.
Ignore users without an email address during deployment	Specifies that users who do not have an email address are ignored during deployment i.e. there will not be a record for them in the Status Monitor dialog.
Use ASCII format for all Outlook signature files	Specifies that the Email Signature Manager Agent should write all Outlook signature files in ASCII format, rather than Unicode, when appropriate (this will affect how HTML and plain-text signature files are written). It should not normally be necessary to use this option. If it is enabled, it is important to note that any non-ASCII characters present in the signature will be converted to question marks in the signature file.
Autodiscover on each update cycle	Specifies that the Email Signature Manager Agent should use Autodiscover on each update cycle, discarding the details of any previously discovered service for acquiring signature settings. This setting can be useful in environments where the users of the Agent move between being connected to your organization's Local Area Network (and hence, able to connect to the Client Access Service to download signature settings) and being off-premises with only an Internet connection (and hence, only able to connect to their mailbox using Exchange Web Services).
Add VML code to HTML signatures for optimal image support	Specifies that when the Email Signature Manager Agent installs HTML signatures, it should add Vector Markup Language (VML) code for optimal image support for Windows display scaling, and compatibility with encrypted and signed emails.
Direct Database Mode	Enables direct database mode (when available). For further information, see the chapter on direct database mode.
Write Signature Files	When enabled, the service will write files for the default new and reply/forward signatures in HTML and plain-text format to the specified folder. The files are written for each email address for each user defined for

Save Database Connection Settings

This topic only applies when you use Email Signature Manager in direct database mode.

When using Email Signature Manager in direct database mode, the **Email Signature Manager Agent** connects directly to the database.

The Save Database Connection Settings dialog is used to save a configuration file that configures the Agent to connect directly to the database as well as the credentials to use. The database must be a SQL Server database. The dialog is opened by clicking the **Save Configuration File** button on the **Advanced** page of the Deployment Options dialog.



When saving the configuration file, you need to decide how the Agent will connect to the database and then select the appropriate option:

- **Using Specific SQL Credentials**: This is the recommended option. To use SQL Credentials, create a new SQL login following the instructions in this topic. and then enter the user name and password for that login. To verify you have entered the correct credentials, click the **Test Connection** button. Using this approach will mean that all instances of the Agent (whether on- or off-premises) will connect with the same login.

- **Using Integrated Security**: This approach can be used when all users logon to your Active Directory domain. You will need to create a SQL Login for the appropriate domain users and/or groups. The basic principle of how to do this is outlined in this topic, which describes how to create a login for use by a domain user when running the main application in Manager Only mode.

- **Using the current settings**: This approach is not recommended, because it will mean that the Agent will connect with the same login as the main application and that login will have been granted ownership

rights on the Email Signature Manager database. However, this does provide a quick way to get the Agent working in direct database mode.

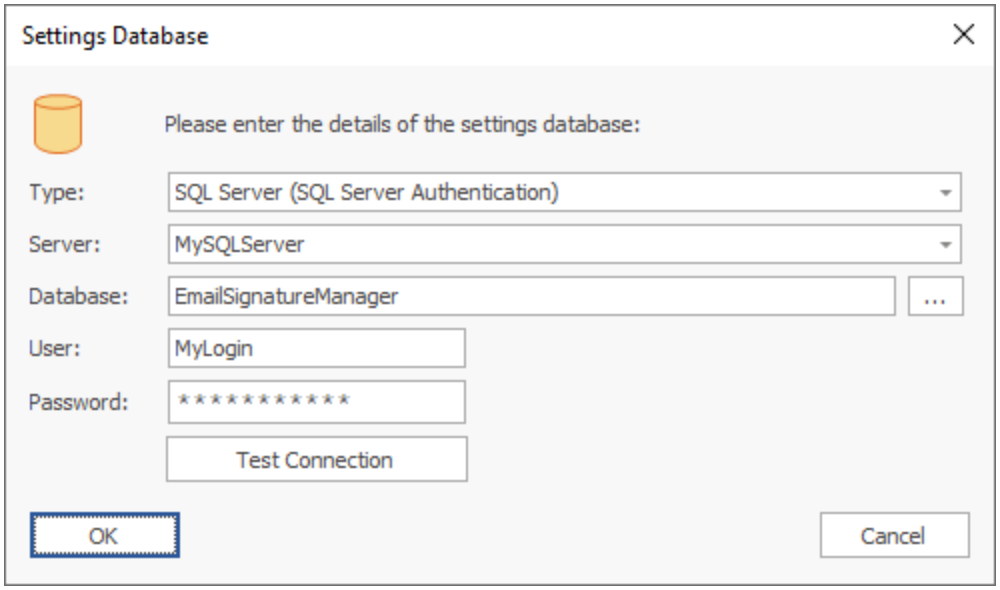
Once the appropriate option has been selected, click the **Save** button to save the configuration file; the file **must** be named `agent.ini` and should be saved in one of the following locations:

- If you are using GPO to deploy the Agent, save the file in the same folder as the MSI package; when it is installed, the package will automatically copy the file.
- If you are using a shared folder, save the file in the shared folder next to the `SignAgent.exe` executable.

Once the file has been saved, the dialog will be closed. To close the dialog without saving the file, click the **Cancel** button.

Settings Database

The Settings Database dialog is opened by clicking the **Settings Database** button on the Database page in the Configuration backstage of the main application window:



The Settings Database dialog is used to connect the application to the database storing your templates and deployment configuration. When the dialog is first opened, the settings for connecting to the current database are displayed. If required, select the type of the database in the **Type** drop-down and then configure the following settings:

- **Server**: When connecting to Microsoft SQL Server, enter the name of the server where the database is located, or select from the drop-down list of available servers.
- **Database**: Specifies the actual database for the settings database:
  - When connecting to the Built-in Database, this will be fixed to the location of the database.
  - When connecting to a Microsoft SQL Server database, enter the name of the database or select it by clicking the ellipses ("...") button.

- **User**: When connecting to Microsoft SQL Server, enter the name of the dedicated login to connect to the database.
- **Password**: When connecting to Microsoft SQL Server, enter the password for the dedicated login to connect to the database.

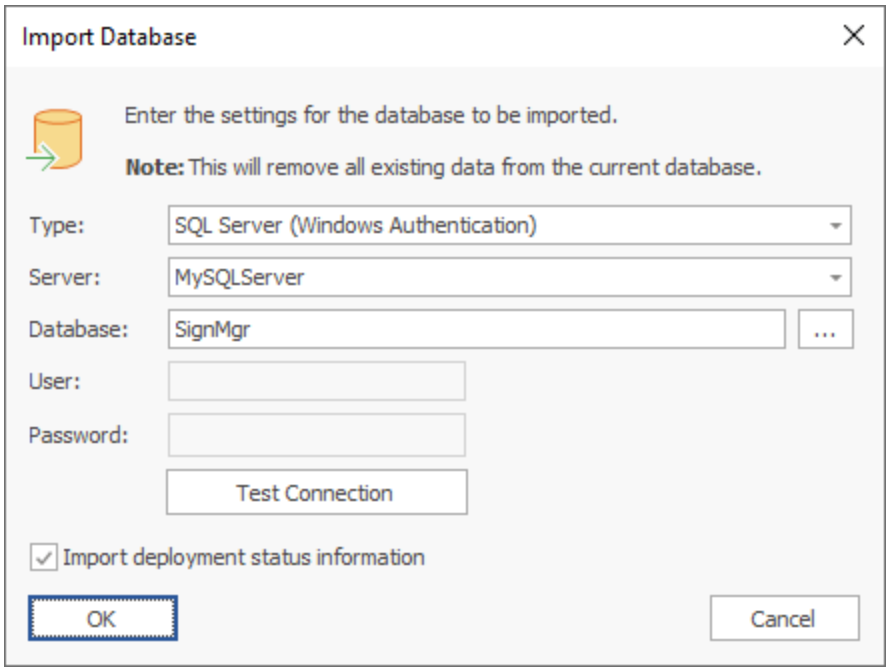
To verify that you have entered the details of the database correctly, click the **Test Connection** button. This will open a connection to the database using the settings specified and read the current version, with the result being displayed in a message box. The **Repair & Compact** button is available with the Built-in Database to reclaim unused allocated space.

When the configuration for connecting to the new settings database has been completed, click the **OK** button. The current database (if there is one open) will be closed and the specified database opened. To close the dialog without making any changes, click the **Cancel** button.

Note The current settings database is displayed in the status bar at the bottom of the main application window.

Import Database

The Import Database dialog is opened by clicking the **Import Database** button on the Database page in the Configuration backstage of the main application window:



Importing an existing database is normally used as part of migrating from using the Built-in Database included with Email Signature Manager to using Microsoft SQL Server. Full details about how to configure a SQL Server database for use with Email Signature Manager can be found in a separate chapter.

Note All existing data in the current database will be deleted during the import process. It is therefore important that you verify that you are connected to the correct target database before performing the import. You can verify the current database by opening the Settings Database dialog.

Select the type of the source database in the **Type** drop-down and then configure the following settings:

- **Server**: When connecting to Microsoft SQL Server, enter the name of the server where the database is located, or select from the drop-down list of available servers.
- **Database**: Specifies the actual database from which the data will be imported:
  - When connecting to a Microsoft Access database, enter the full path to the database or select it by clicking the ellipses ("...") button.
  - When connecting to a Microsoft SQL Server database, enter the name of the database or select it by clicking the ellipses ("...") button.
- **User**: When connecting to Microsoft SQL Server using SQL Security, enter the login to connect to the server.
- **Password**: When connecting to either a password-protected Microsoft Access database or Microsoft SQL Server using SQL Security, enter the password.

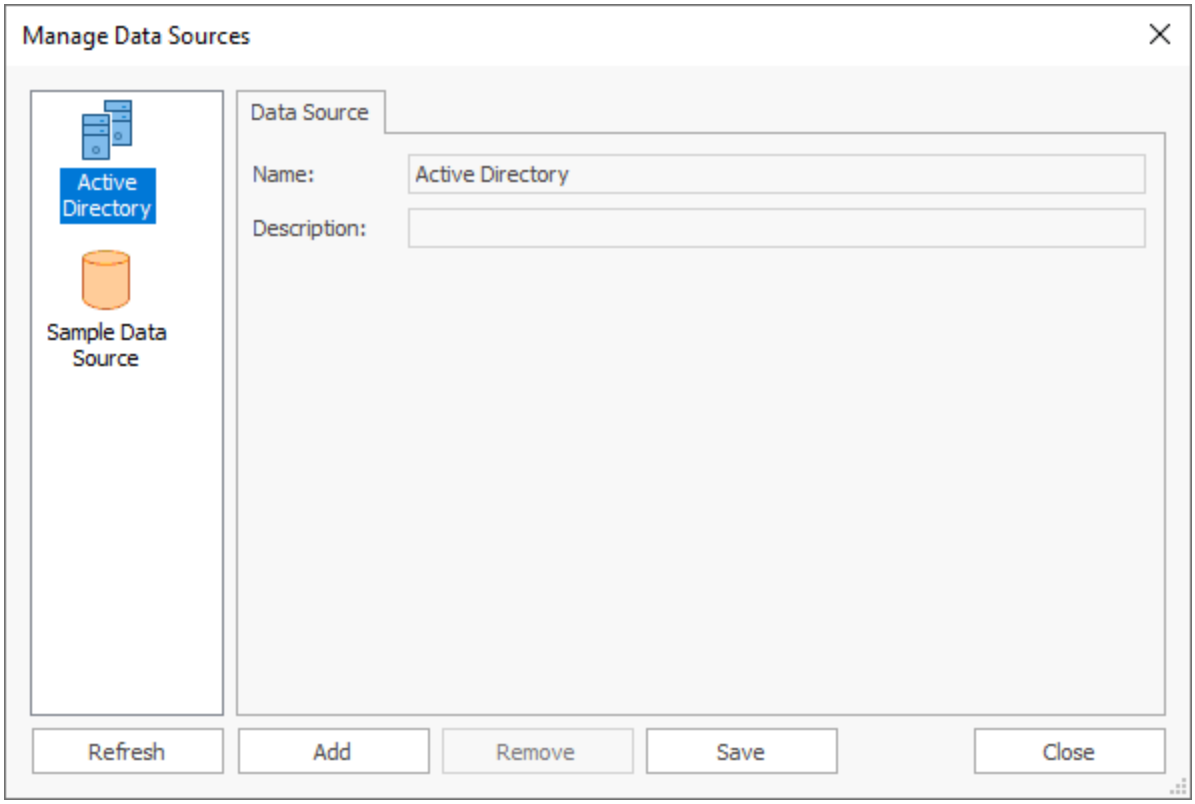
Note The Built-in Database that is included with Email Signature Manager is in Microsoft Access format and can be found in the **Program Data** folder; the default location is `C:\ProgramData\Symprex\Symprex.EmailSignatureManager.Database.mdb`.

To verify that you have entered the details of the source database correctly, click the **Test Connection** button; this will open a connection to the database using the settings specified and read the current version, with the result being displayed in a message box.

When the configuration for connecting to the source database has been completed, click the **OK** button. You will be prompted to confirm the import before the process is started. To close the dialog without importing any data, click the **Cancel** button.

Manage Data Sources

The Manage Data Sources dialog is opened by clicking the **Data Sources** button on the Configuration page in the Configuration backstage of the main application window:



A data source is used to supply information when a signature is being deployed to a user; specifically, it is used to fetch the data used to populate the fields in the signature. The default data source available for all signatures is Active Directory, where the fields in the signatures are mapped to properties on the user's Active Directory object. However, it is possible to populate signatures using the data held in a custom database; this is a custom data source.

The current data sources defined in the database are displayed in a list on the left of the dialog. Selecting any data source will display the details of that data source in the main part of the window. All data sources have the following common properties:

- **Name**: Specifies the unique name of the data source (mandatory).
- **Description**: An optional property describing the data source.
- **Data Source** Page: Specifies how to connect to the source database.
- **Data Query** Page: Specifies the SQL query to select data from the source database.
- **Data Mappings** Page: Specifies the mappings between the database and template fields.

The list of data sources can be refreshed by clicking the **Refresh** button. To create a new data source, click the **Add** button or to remove the current data source, click the **Remove** button. When the data sources have been configured as required, click the **Save** button to save your changes. Click the **Close** button to close the dialog; if you have made any changes, you will be prompted to save before the dialog is closed.

More detailed information about working with custom data sources can be found in the Configure a Custom Data Source chapter.

Configure a Custom Data Source

This topic explains how to create or edit a custom data source for use with your templates.

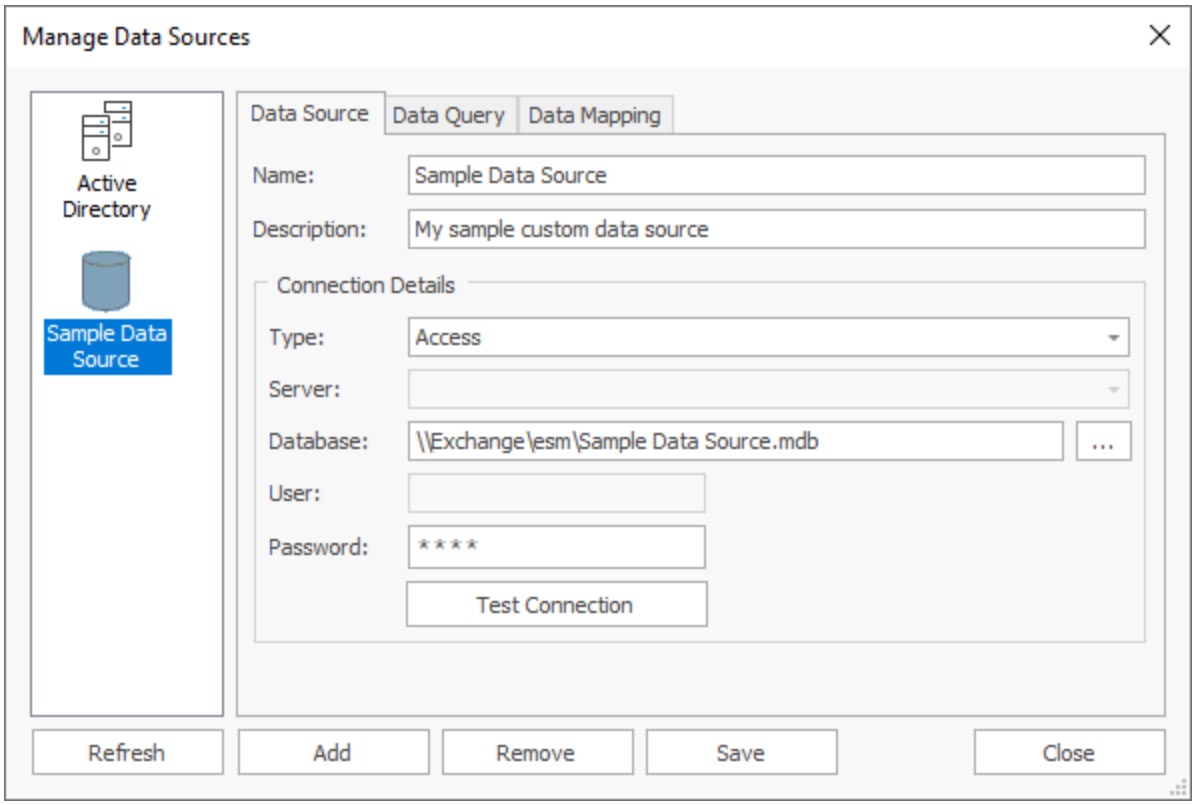
Create the Data Source

Custom data sources are managed using the Manage Data Sources dialog.

- To create a new data source, click the **Add** button on the dialog.
- To edit an existing data source, select it from the list on the left side of the dialog.

Configure the Data Source

The first part of the configuration is to specify the database from which the user data will be fetched using the **Data Source** page:



Select the type of the source database in the **Type** drop-down and then configure the following settings:

- **Server**: When connecting to Microsoft SQL Server, enter the name of the server where the database is located, or select from the drop-down list of available servers. When connecting to Oracle, specify the name of the server where the database is hosted, using a colon to specify a custom port if required.
- **Database**: Specifies the actual database from which the data will be imported:
  - When connecting to a Microsoft Access database, enter the full path to the database or select it by clicking the ellipses ("...") button.

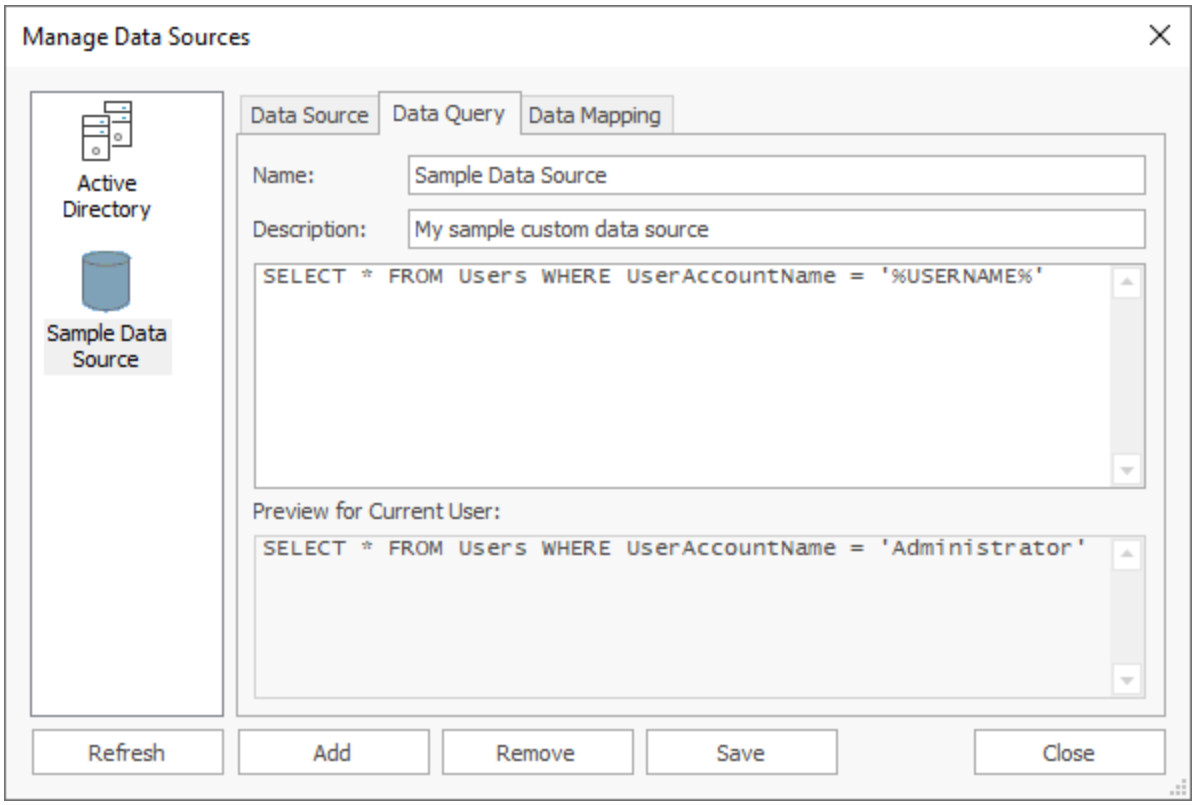
- When connecting to a Microsoft SQL Server database, enter the name of the database or select it by clicking the ellipses ("...") button.
- When connecting to an Oracle database, enter the name of the database.

- **User**: When connecting to Microsoft SQL Server using SQL Security or Oracle, enter the login to connect to the server.
- **Password**: When connecting to either a password-protected Microsoft Access database, Microsoft SQL Server using SQL Security, or Oracle, enter the password.

To verify that you have entered the details of the database correctly, click the **Test Connection** button; this will open a connection to the database using settings specified (although no data will be read at this point).

Specify the Data Query

The second part of the configuration is to specify the query that will be used to fetch the user data from the database using the **Data Query** page:



The query needs to be specified such that it will return a single row of data for the user to which a signature is being deployed. To accomplish this, the `WHERE` clause of the query can be customised using the following tokens:

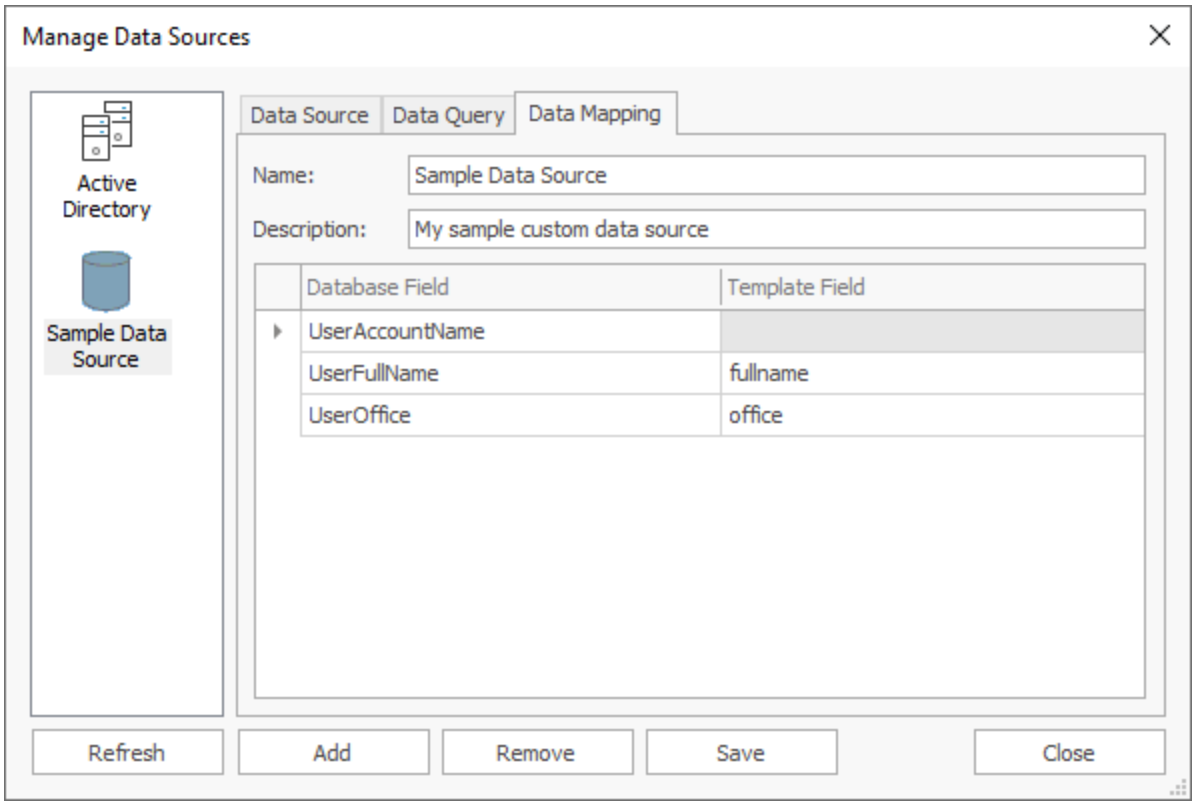
Field Name	Description
`%USEREMAIL%`	This token is replaced by the user's Active Directory email address.

%USERNAME%	This token is replaced by the user's Active Directory account name.
%USERDOMAIN%	This token is replaced by the NETBIOS name for the user's domain.
%USERDNSDOMAIN%	This token is replaced by the full DNS name for the user's domain.

Generally speaking, the source table for the query should contain a primary key that can be mapped to one (or more) of these tokens. In the example above, the `UserAccountName` field in the database is the primary key field in the table and is used to match against the user's Active Directory account name. The **Preview for Current User** box is updated from the specified query using the account details for the current user, which can be used to verify that the query is generated as expected.

Specify the Data Mappings

The third part of the configuration is to specify the mappings between the fields returned by the query and the fields in the signature using the **Data Mapping** page:



When the *Data Mapping* page is selected, a connection to the database specified on the *Data Source* page will be established and the query specified on the *Data Query* page will be executed to determine the fields available; these fields are displayed in the **Database Field** column of the grid. For each database field that should be mapped, select the field in the **Template Field** of the grid.

In the example above:

- The `UserFullName` database field has been mapped to the `fullname` template field; when the signature is deployed, any instances of the `{fullname}` field will be replaced by the value of the `UserFullName` field from the database.
- The `UserOffice` database field has been mapped to the `office` template field; when the signature is deployed, any instances of the `{office}` field will be replaced by the value of the `UserOffice` field from the database.

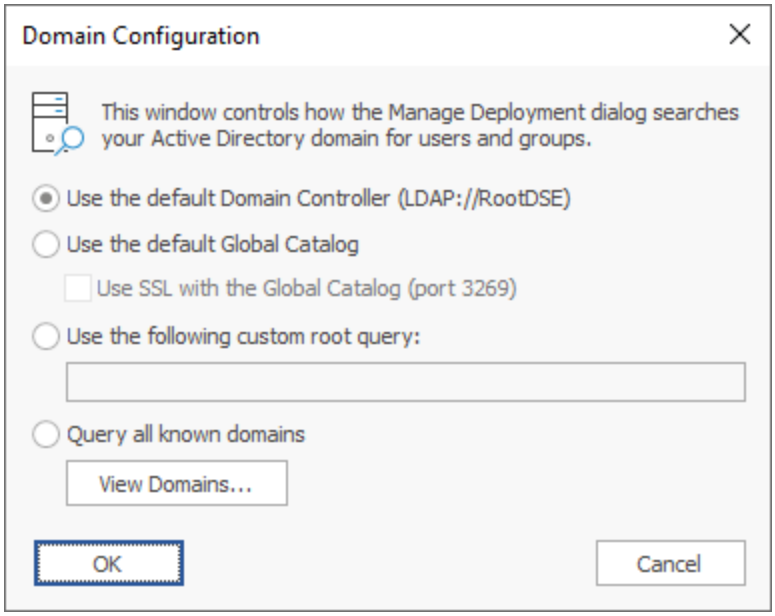
Configuration Completed

The configuration of the data source is now completed; click the **Save** button to save the changes. You can now select the data source as the source for any signature and verify that it is fetching the correct data for any user by using the Test Signatures dialog.

Note If the query fails to return a record when the signature is generated, the signature will be populated using the data from Active Directory.

Domain Configuration

The Domain Configuration dialog is opened by clicking the **Domain Configuration** button on the Configuration page in the Configuration backstage of the main application window:



This dialog configures how the Manage Deployment dialog will search your Active Directory domain for users and groups:

- **Use the default Domain Controller**: This is the default option and will use an LDAP query to find the users and groups in just your local domain.
- **Use the default Global Catalog**: This option will query the Global Catalog server for your local domain, and will find users and groups from all domains that replicate to the Global Catalog. If necessary, select

the **Use SSL with the the Global Catalog** option to make the query use secured communications on port 3269 of your Global Catalog server.
- **Use the following custom root query:** This option allows you to provide a custom query to find users and groups from any domain or domain controller for which you have trust relationship (for example, `"LDAP://DC=mydomain,DC=com"`).
- **Query all known domains**: This option will attempt to locate users and groups in all domains known to the current domain. The list of domains is determined by examining the current forest and any trust relationships that exist. To see the list of known domains that will be searched when this option is selected, click the **View Domains...** button.

When the configuration for the domain has been completed, click the **OK** button. Alternatively, click the **Cancel** button to close the dialog without saving any changes.

Mobile Device Signatures

The Mobile Device Signatures dialog is opened by clicking the **Mobile Device Signatures** button on the Configuration page in the Configuration backstage of the main application window.

This dialog controls how the signatures for mobile devices are managed in your organization. There are two approaches available:

- Injection into emails sent from mobile devices as they are delivered through Exchange Server and Office 365.
- Distribution of mobile signatures to the users in your organization by email.

The signature that is either injected or sent via email is specified using the **Mobile Device Signature** setting on the Manage Deployment dialog.

Inject Signatures

Signature injection works by using a set of rules to identify where in an email the mobile device signature should be inserted. The text specified by the rule is replaced by the pre-generated signature content, resulting in the signature being injected into the email. Signatures can be injected into emails sent through On-Premises Exchange Server using the Email Signature Manager Transport Agent and through Office 365 using our cloud-based Signature Injection Service for 365 (if your license is enabled to use it).

To enable signature injection, on the **Inject Signatures** tab, select the **Inject signatures into emails sent from mobile devices using rules** option, which will have the following effect:

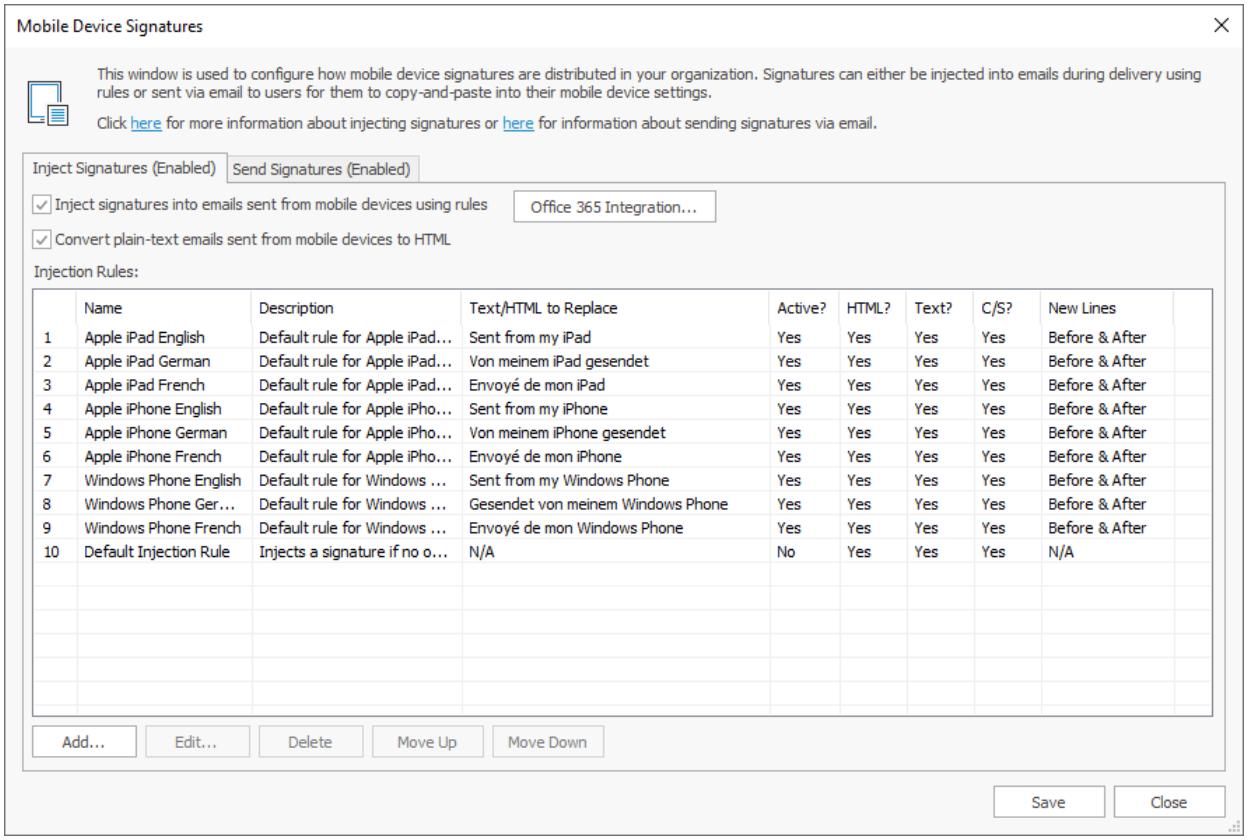
- When using Exchange Server, the Transport Agent will inject the pre-generated signatures by the Email Signature Manager Service.
- When using Office 365, the Signature Injection Service for Office 365 will inject the pre-generated signatures uploaded by the Email Signature Manager Service to the cloud.

To check if your license is enabled for the Signature Injection Service for Office 365, and configure your Office 365 tenant to use it, click the **Office 365 Integration...** button to open the Office 365 Integration dialog. This button is only available when Office 365 is configured in the Environment Configuration dialog.

By default, most mobile devices send new emails in plain-text format. Selecting the **Convert plain-text emails sent from mobile devices to HTML** option will cause the plain-text emails to be converted into HTML format and and the HTML signature to be injected.

Note When a plain-text email is converted to HTML, the rules applicable to HTML format emails will be applied, not those applicable to only plain-text emails. Further, an email is only converted if a plain-text rule matches.

The **Injection Rules** are used to define how signatures are injected and the order in which they are evaluated:



The following actions can be performed:

- To create a new rule, click the **Add...** button, which opens the Manage Signature Injection Rule dialog.
- To edit an existing rule, select it in the grid and click the **Edit...** button, which opens the Manage Signature Injection Rule dialog.
- To delete an existing rule, select it in the grid and click the **Delete** button; you will be prompted to confirm this action before the rule is deleted.
- To move a rule higher in the list (so it is evaluated earlier), select it in the grid and click the **Move Up** button.
- To move a rule lower in the list (so it is evaluated later), select it in the grid and click the **Move Down** button.

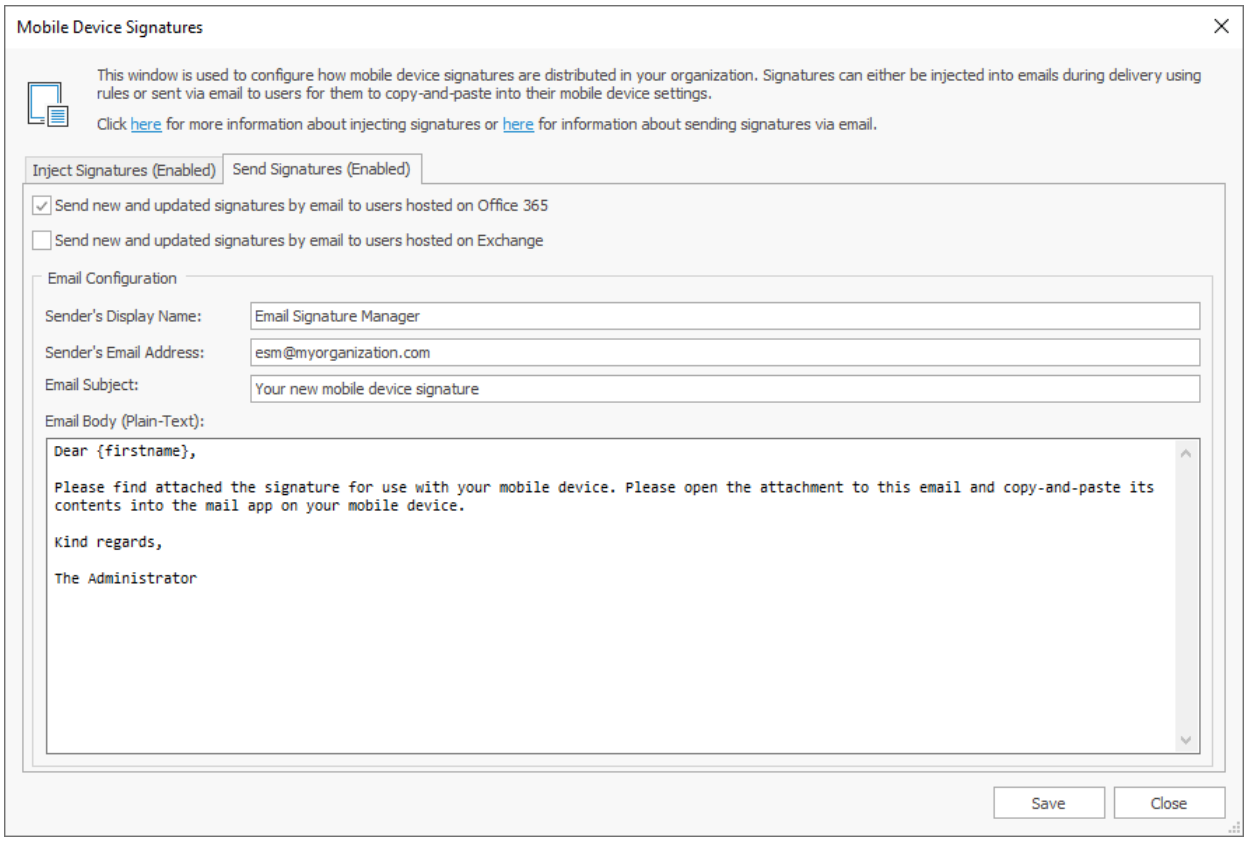
Send Signatures

Email Signature Manager can be configured to send mobile device signature via email to the users in your organization. When users receive the email, they can open the signature attachment and copy and paste the signature into their mail app. This feature is primarily intended for when there is no possibility to use the signature injection features.

To enable distribution by email:

- Select the **Send new and updated signatures by email to users hosted on Office 365** option to send mobile device signatures via email to users who have their mailbox hosted on Office 365.
- Select the **Send new and updated signatures by email to users hosted on Exchange** option to send mobile device signatures via email to users who have their mailbox hosted on Exchange Server.

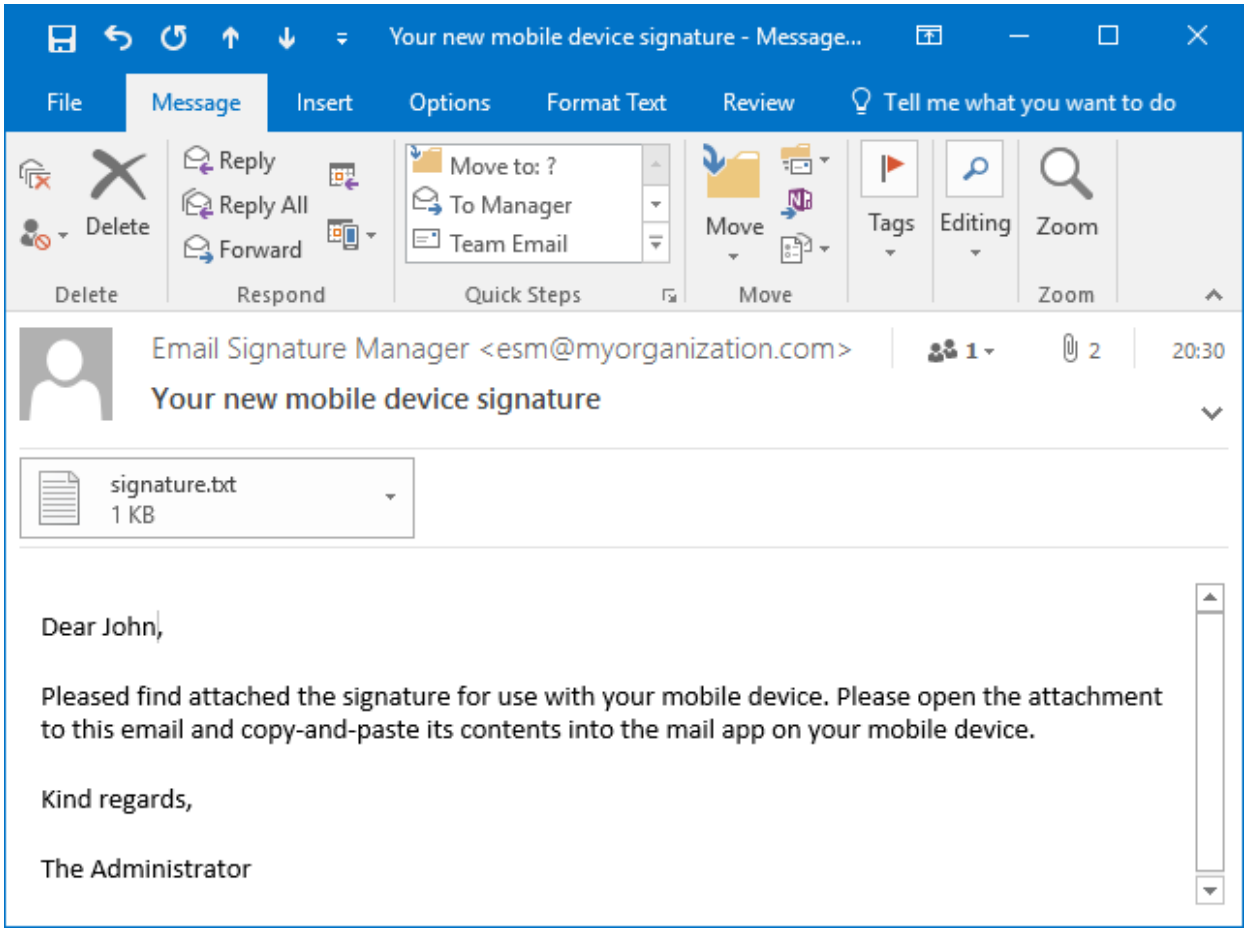
The email that is sent to each user is configured in **Email Configuration**:



The email has the following properties:

Name	Description
Sender's Display Name	The display name for the sender of the email sent to each user.
Sender's Email Address	The email address for the sender of the email sent to each user.
Email Subject	The subject for the email sent to each user.
Email Body (Plain-Text)	The plain-text body of the email; the body is parsed in the same way as signatures and you can therefore make use of the same fields (refer to this appendix for details).

From the configuration shown above, the following email would be delivered to the appropriate users in your organization:

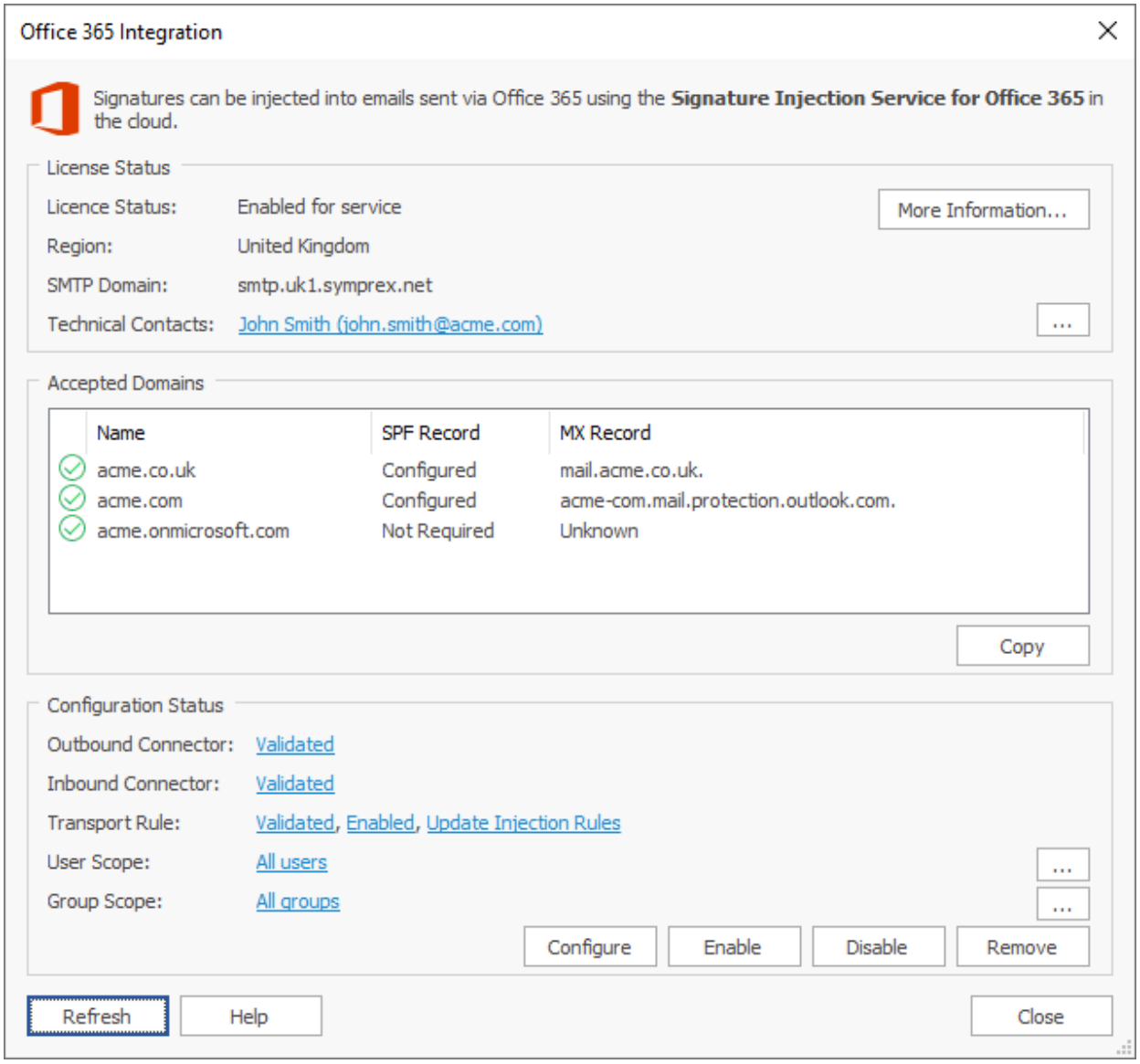


For more information about distributing signatures via email, please refer to this topic.

When the configuration has been completed as required, click the **Save** button to save your changes. Click the **Close** button to close the dialog; if you have made any changes, you will be prompted to save before the dialog is closed.

Office 365 Integration

The Office 365 Integration dialog is opened by clicking the **Office 365 Integration...** button in the Mobile Device Signatures dialog:



Note An overview of the Signature Injection Service for Office 365 can be found in this topic.

When the dialog is opened, the **License Status** frame shows if your license is enabled for use with the Signature Injection Service for Office 365. If it is, the same frame also shows the associated region of service, the SMTP domain your emails will be routed through for signature injection, and any technical contacts in your organization you have listed for Symprex to contact in the event of any technical issues with the service. You can manage this list in the Technical Contacts dialog.

If your license is enabled for use with the service, an authentication dialog will appear, requesting credentials of an administrative account, to log on to Exchange Online to query the details of your tenant.

Note If your administrative account is setup for multi-factor authentication (MFA), the Exchange Online Remote PowerShell Module must be installed, more information on which can be found in this topic.

When successfully logged on to your Office 365 tenant, the **Accepted Domains** and **Configuration Status** frames show your tenant configuration as described below.

The **Accepted Domains** frame shows a list of the accepted domains configured in your Office 365 tenant with the following information:

- **Name**: The accepted domain name.
- **SPF Record**: The state of the SPF TXT record for the domain, determining if (where required) the record includes spf.symprex.net; see below for more information.
- **MX Record**: The primary MX record for the domain.

Important Before configuring your Office 365 tenant to integrate with the Signature Injection Service for Office 365, you **must** configure the SPF record for each of your accepted domains (except the default `onmicrosoft.com` domain) to include spf.symprex.net by adding `include:spf.symprex.net`, as shown in this example:

```
v=spf1 include:spf.protection.outlook.com include:spf.symprex.net -all
```

Any incorrectly configured domains will be clearly highlighted.

You can use the **Copy** button to copy the details of your accepted domains to the clipboard, if you would like a copy of this information.

The **Configuration Status** frame shows the configuration of your Office 365 tenant for use with the Signature Injection Service for Office 365:

- **Outbound Connector**: The *Outbound Connector* sends email from your Office 365 tenant to the Symprex cloud for signature injection. The Outbound Connector must be correctly configured and match the settings in your license.
- **Inbound Connector**: The *Inbound Connector* receives email back from the Symprex cloud servers after signatures have been injected and continues the delivery process. The Inbound Connector must be correctly configured.
- **Transport Rule**: The *Transport Rule* is used to forward email to the Outbound Connector for signature injection. The Transport Rule must be correctly configured and can optionally be scoped to only forward email from specific users and/or groups. The rule is automatically scoped against the Signature Injection Rules defined on the Mobile Device Signatures dialog, so only emails matching those rules are forwarded to the Symprex cloud for signature injection; if the rule is not up to date against the injection rules, click the Update Injection Rules link to update it. The rule is also automatically scoped against the Accepted Domains *excluding* any "OnMicrosoft.com" domains; if the rule is not up to date against the accepted domains, click the Update Domain Scope link to update it
- **User Scope**: The *User Scope* allows you to scope the Transport Rule to only apply to specific users.
- **Group Scope**: The *Group Scope* allows you to scope the Transport Rule to only apply to email sent from members of specific groups.

The configuration can be updated using the buttons at the bottom of the frame:

- The **Configure** button will configure your Office 365 tenant for use with the Signature Injection Service for Office 365, including creating the Outbound Connector, Inbound Connector, and Transport Rule. This option will replace any existing configuration listed but any user, group and domain scope will be preserved.
- The **Enable** button will enable the Transport Rule, causing email to be forwarded to the Outbound Connector.
- The **Disable** button will disable the Transport Rule, which will stop email from being forwarded to the Outbound Connector and hence stop all signature injection.
- The **Remove** button will completely remove the configuration from your Office 365 tenant, which will stop all signature injection.

To refresh the dialog, click the **Refresh** button and when ready, click the **Close** button to close it.

Installing Exchange Online Remote PowerShell Module

For Email Signature Manager to be able to logon to Exchange Online, the Exchange Online PowerShell v2 module must be installed. Details about this module can be found on the Microsoft website:

https://docs.microsoft.com/en-us/powershell/exchange/exchange-online-powershell-v2

To install the module, please perform the following steps:

1. Start **Windows PowerShell** (32-bit operating systems) or **Windows PowerShell x86** (64-bit operating systems) with administrative privileges.

2. Execute the following command:

```
Install-Module -Name ExchangeOnlineManagement -Force
```

Note Installing the module may fail with the following error message:

"Unable to download the list of available providers. Check your internet connection."

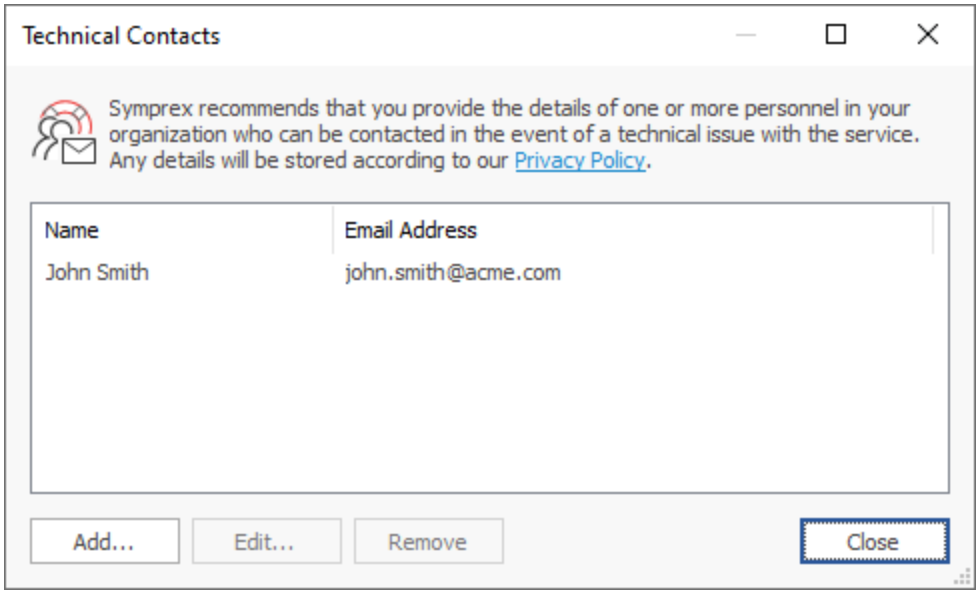
If this happens, run the following command to enable TLS1.2 and later:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12 +
[Net.SecurityProtocolType]::Tls13
```

It should now be possible to install the module.

Technical Contacts

The Technical Contacts dialog is opened by clicking the **Technical Contacts** link in the Office 365 Integration dialog:



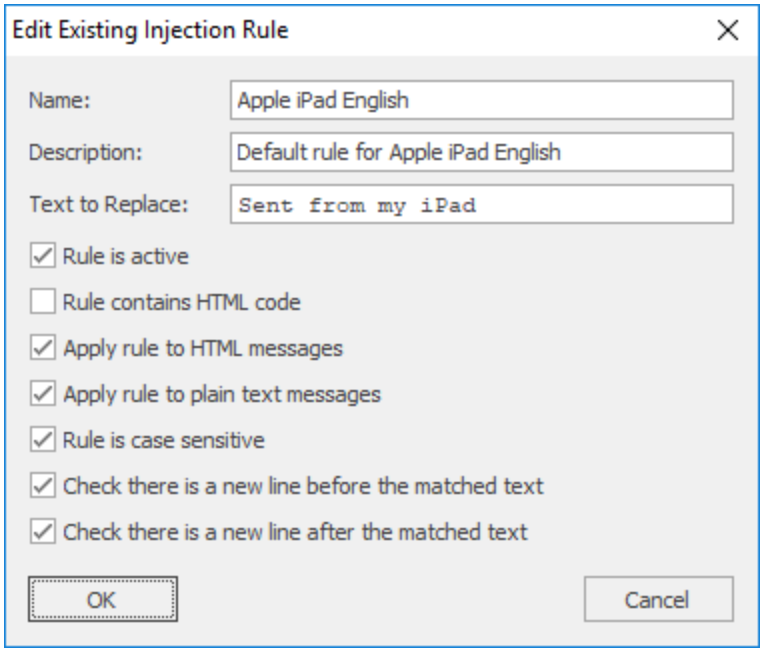
Symprex recommends that you provide the details of at least one member of your organization who can be contacted if there is a technical issue with the service. You can manage the list of such personnel using this dialog. To add a new contact, click the **Add...** button. To edit an existing contact, select the contact and click the **Edit...** button, or to remove the contact, click the **Remove** button.

Your list of technical contacts is uploaded to the Signature Injection Service for Office 365 by the Email Signature Manager Service. The details you provide will be stored according to our Privacy Policy.

When you have completed the changes to the list, click the **Close** button to close the dialog.

Manage Signature Injection Rule

The Manage Signature Injection Rule dialog is used to create or modify a rule for injecting a mobile device signature into an email. It is opened using either the **Add...** or **Edit...** button on the Mobile Device Signatures dialog.



Each Signature Injection Rule has the following properties that can be modified:

Name	Description
Name	The name of the rule.
Description	A description of the rule.
Text to Replace	The text (or HTML for direct replacement rules) in the email to be replaced by the signature.
Rule is active	Specifies if the rule is active; only active rules are applied when processing emails.
Rule contains HTML code	Specifies that the rule contains HTML code. When this option is selected, the specified HTML to replace must match *precisely* for the replacement to occur (the *Rule is case sensitive option* is respected). Using this option allows default signatures, such as those that contain a hyperlink, to be replaced.
Apply rule to HTML messages	Specifies if the rule is applied to emails formatted in HTML.
Apply rule to plain text messages	Specifies if the rule is applied to plain text emails.
Rule is case sensitive	Specifies that the match on Text to Replace is case sensitive.
Check if there is a new line before the matched text	Specifies that new line must be present before the Text to Replace for it to be considered a match; if no new line is found then the text will not be replaced.
Check if there is a new line after the matched text	Specifies that new line must be present after the Text to Replace for it to be considered a match; if no new line is found then the text will not be replaced.

Once the rule has been configured, click the **OK** button to apply the changes and close the dialog, or click the **Cancel** button to close the dialog without saving changes.

Deployment 3

Deployment of signatures to your users occurs as follows:

- Signatures are updated in Outlook by the **Email Signature Manager Agent**.
- Signatures are deployed to OWA by the **Email Signature Manager Service**.
- Signatures are injected into emails sent from mobile devices by the **Email Signature Manager Transport Agent**.

The service is also responsible for:

- Writing Outlook signatures and settings to mailboxes for use by the Email Signature Manager Agent.
- Generating signatures into the database for use by the Email Signature Manager Transport Agent.

The service is an integral part of Email Signature Manager and is installed with the Full Installation of the product.

Having completed installation or upgrade, the following additional tasks need to be completed:

- Arrange for the Email Signature Manager Agent to be executed on your end users' computers.
- If you are using On-Premises Exchange Server or Hosted Exchange, the Email Signature Manager Transport Agent needs to be installed.

Note The Email Signature Manager Transport Agent is not available for Office 365 and some Hosted Exchange providers may not support it.

The Email Signature Manager Client Access Service

The **Email Signature Manager Client Access Service** (CAS) provides a simple, configuration-free method for the Email Signature Manager Agent and Email Signature Manager Transport Agent to fetch signature settings. It is installed and started automatically with a Full Installation of Email Signature Manager. During installation, the following actions are performed:

- A **Service Connection Point** (SCP) is created in Active Directory and is used by the Agent and Transport Agent to automatically find the URL for the CAS.
- Port 5757 is opened in **Windows Firewall** to allow inbound TCP/IP connections to connect to the CAS.

The SCP and Windows Firewall rule can be managed using the Client Access Service tab on the Deployment Options dialog.

The Agent v1.2 and higher will automatically use the Client Access Server if it finds the SCP in Active Directory.

Using the Email Signature Manager Agent

Signatures are installed to Outlook by the **Email Signature Manager Agent**. The Agent connects to the Email Signature Manager Client Access Service to fetch the user's signatures and settings, updates Outlook, and sends back the deployment results to the server; those results can then be viewed in the Status Monitor dialog. If the Agent cannot connect to the Client Access Service (for example, because the

Agent is running off-domain), it reads the signatures and settings from the user's mailbox using Exchange Web Services (EWS). In this case, the Agent uses autodiscover to find the server hosting the user's mailbox, reads the signatures and settings written to the user's mailbox by the Email Signature Manager Service, updates Outlook, and writes the deployment log back the user's mailbox; the log is subsequently read by the Email Signature Manager Service and made available in the Status Monitor.

The interval at which the Agent checks for new signatures, and other Agent configuration, can be controlled through the Agent tab on the Deployment Options dialog.

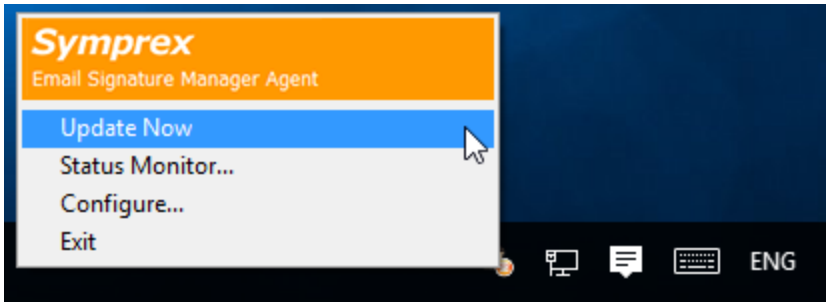
Starting the Agent on an End User's Computer

There are three ways in which the Agent can be started on an end user's computer:

- Started at logon using a script.
- Installed via Group Policy.
- Installed via ClickOnce technology.

When the Agent is running an icon appears in the Windows system tray:

The Agent menu is available by right-clicking the Agent icon in the Windows system tray:

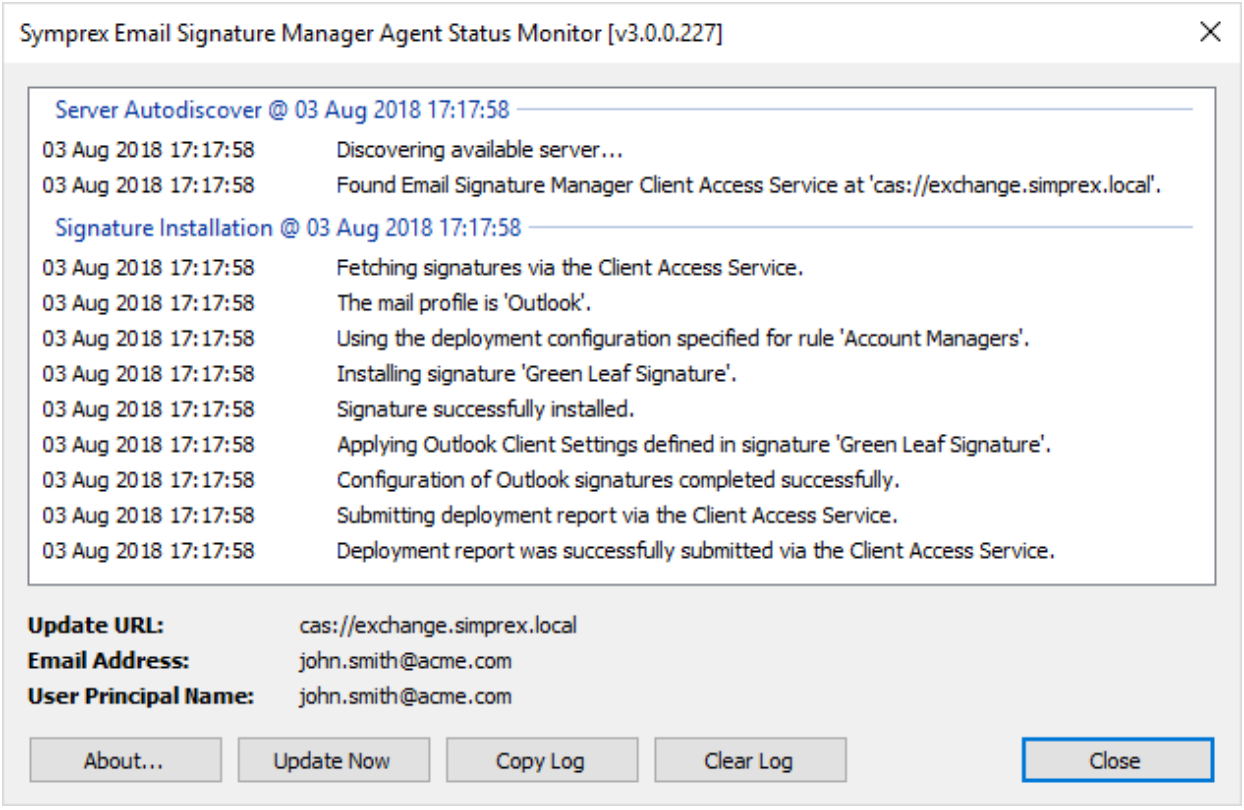


Using Update Now

In the Windows system tray, right-click the Agent icon and select **Update Now** to update Outlook signatures.

Opening Agent Status Monitor

In the Windows system tray, right-click the Agent icon and select **Status Monitor...** to open the Status Monitor dialog:



The main part of the window shows a list of the events that have occurred during the autodiscover and signature installation phases for each update cycle. Below the list, the Update URL (or database, if using a direct database connection), email address and User Principal Name that are being used for the update cycle are shown (see below for how the Agent determines these details). To start an update cycle, click the **Update Now** button and to copy log of events, click the **Copy Log** button. To copy a verbose log, hold down the Shift key whilst clicking the Copy Log button; this verbose log can be very useful for troubleshooting signature installation problems.

How the Agent Determines the Outlook Profile and Email Address

Before the Agent can fetch signatures and settings, it has to determine the Outlook profile to be updated and email address for which signatures are required. The Outlook profile is determined in the following order of precedence:

1. If a specific profile is selected in Agent Options, it is used (see Agent Options below); if the specific profile does not exist, an error is reported.
2. If there is only one Outlook profile, it is used.
3. If there are multiple profiles and the **Always use this profile** option is selected (in the Mail Control Panel applet), the specified profile is used.
4. If there are multiple profiles and the **Prompt for a profile** to be used option is selected, the profile that contains an Exchange account matching either the user's primary SMTP email address (as defined on their domain account) or the specific email address specified in Agent Options, if any.

If the profile cannot be determined using this process, an error is reported and signatures will not be installed. The email address is determined in the following order of precedence:

1. If a specific email address is specified in Agent Options, it is used (see Agent Options below).
2. If available, the email address from first Exchange account on the selected Outlook profile is used.
3. If running using a direct database connection, the email address from the default send account on the selected Outlook profile is used.

If the email address cannot be determined using this process, an error is reported and signatures will not be installed.

How the Agent Determines Credentials for Exchange Web Services

If the Agent needs to read the signature settings written to the user's mailbox using Exchange Web Services, it will need suitable credentials. The credentials are determined in the following order:

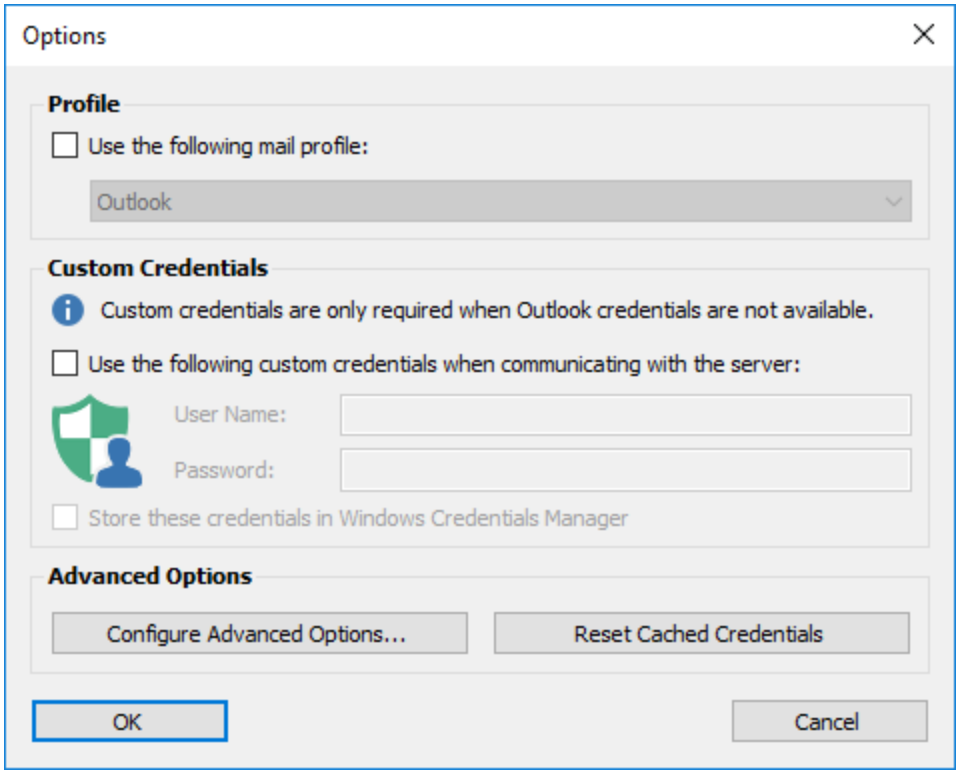
1. Custom credentials entered by the user (see below for how to configure custom credentials).
2. Credentials stored by Outlook in Windows Credentials Manager.
3. User's current Windows logon credentials.

If the credentials do not allow a connection to be made, the Agent will handle this as follows:

- If the mailbox is hosted on Office 365 and the Agent is running under .NET Framework 4.5 or higher, the user is prompted to start the logon process using Modern Authentication. This process supports multi-factor authentication (MFA). Single sign-on (SSO) is also supported and the related configuration document can be requested by email to the Symprex support team.
- Otherwise, the user is prompted to enter custom credentials for establishing the connection.

Configuring Agent Options

In most situations, the Agent should determine the correct Outlook profile and email address for installing signatures, and unless multi-factor authentication (MFA) is being used with Office 365, it should also be able to determine the correct credentials. However, in some cases, it may be necessary to manually configure the Agent. To accomplish this, in the Windows system tray, right-click the Agent icon and select **Configure...** to open the Options dialog:



To use a specific Outlook profile, select the **Use the following mail profile** option and then select the profile from the drop-down list.

To use custom credentials, select the **Use the following custom credentials when communicating with the server** option, and then enter the appropriate user name and password. If the **Store these credentials in Windows Credentials Manager** option is also selected, the credentials will be persisted to Windows Credentials Manager and will be used the next time the Agent is started; otherwise, the credentials will have to be entered again the next time it is started.

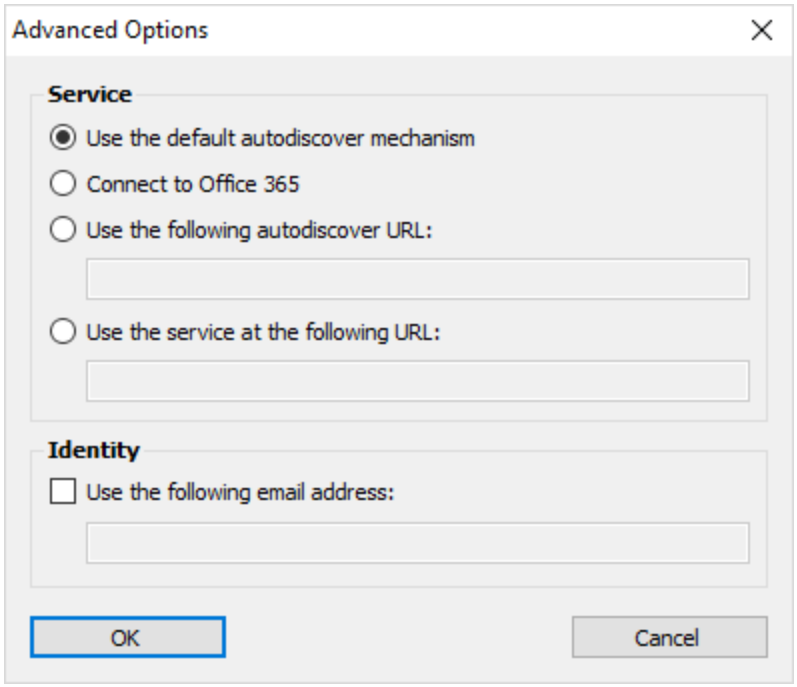
Note When using Modern Authentication, the option to enter custom credentials will not be available.

To configure advanced options, click the **Configure Advanced Options** button to open the Advanced Options dialog (see below). To reset the cached credentials that are being used for Modern Authentication, click the **Reset Cached Credentials** button.

When the settings have been configured as required, click the **OK** button save your changes and close the dialog. Alternatively, **Cancel** button to close the dialog without saving any changes.

Advanced Options

The Advanced Options dialog is opened from the main Options dialog:



The **Service** group allows the service from which the signature settings will be acquired to be customised as follows:

- Select the **Use the default autodiscover mechanism** option to allow the Agent to automatically discover the service.
- To always connect to Office 365, select the **Connect to Office 365** option.
- To use a specific autodiscover service, select the **Use the following autodiscover URL** option and enter the URL (in the format `https://<server>/Autodiscover/Autodiscover.xml`).
- To use a service directly, select the **Use the service at the following URL** option and then enter as suitable URL as follows:
  - To connect to a Client Access Service, enter the URL in the format `cas://<server>`.
  - To connect direct to Exchange Web Services, enter the URL in the format `https://<server>/ews/exchange.asmx`.

To use a custom email address, select the **Use the following email address** option and enter the required email address.

When the settings have been configured as required, click the **OK** button save your changes and close the dialog. Alternatively, **Cancel** button to close the dialog without saving any changes.

Running the Agent from a Logon Script

The **Email Signature Manager Agent** can be run without the need for installation by using your domain logon script. This is accomplished by placing the Agent executable within a shared network folder and updating your logon script to execute it.

Create the Shared Folder

To create the shared folder, use the following steps:

1. On your chosen server, create a new directory.

2. On this new directory, assign the **Domain Users** group the following permissions:

   - Read & Execute
   - List Folder Contents
   - Read

3. Share the folder using a suitable name. It is recommended to hide the share by appending the share name with the dollar ($) character.

4. On the new share, assign the **Domain Users** group the following permissions:

   - Read

Run the Agent from a Logon Script

To run the Agent from a logon script, use the following steps:

1. Download the **Email Signature Manager Agent** executable (`SignAgent.exe`) from the Symprex website and copy it to the shared folder.

2. Modify the script executed by your domain users at logon to execute the Agent; this will be in the form: `\\server\share\SignAgent.exe`

Installing the Agent using Group Policy

Installing the **Email Signature Manager Agent** via Group Policy, using the MSI package, removes the need to start the Agent from a logon script.

- Installing the Agent using Group Policy Per User
- Installing the Agent using Group Policy Per Computer

Note The MSI package does *not* require administrative privileges to be installed on a per-user basis and also supports manual installation by domain users.

Installing the Agent using Group Policy Per User

The following guidelines demonstrate a simple method to create a suitable Group Policy Object (GPO) to install the Agent on a per-user basis on Windows Server 2012 R2 (the steps are the same for previous versions of Windows Server):

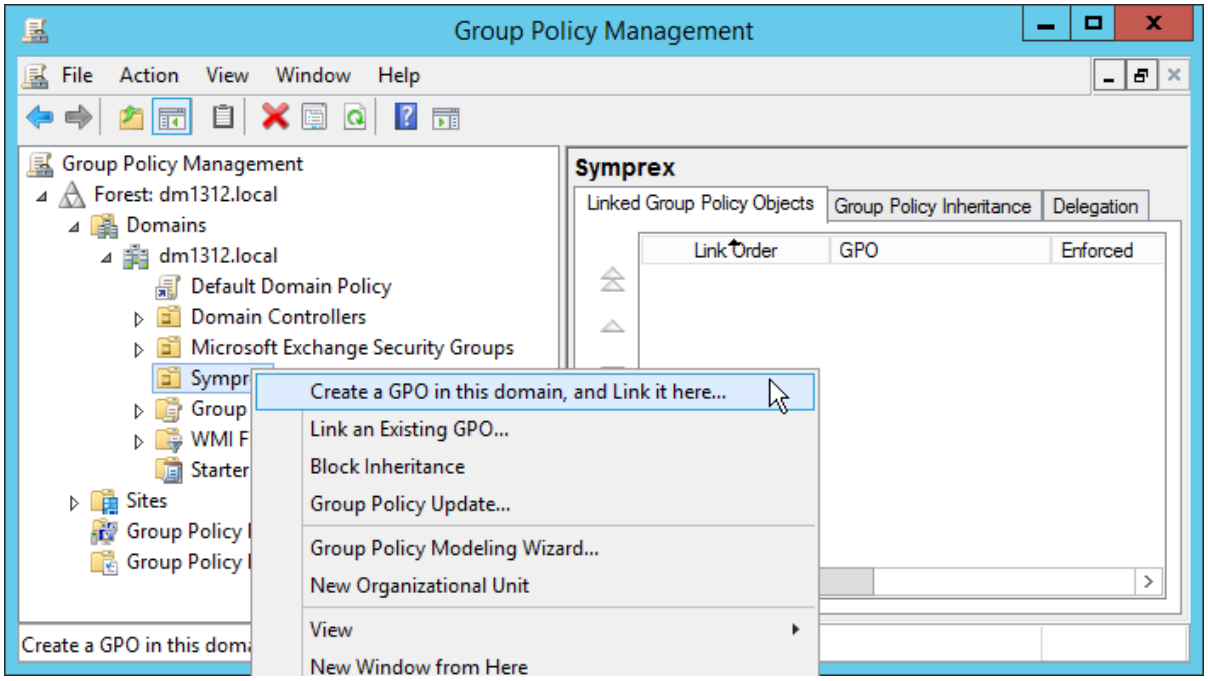
1. Download the **Email Signature Manager Agent** MSI package from the Symprex website and copy it to a shared location to which your domain users have access. To function correctly, the following permissions must be set:

   - On the share itself, ensure that the generic group **Everyone** has **Read** permissions.

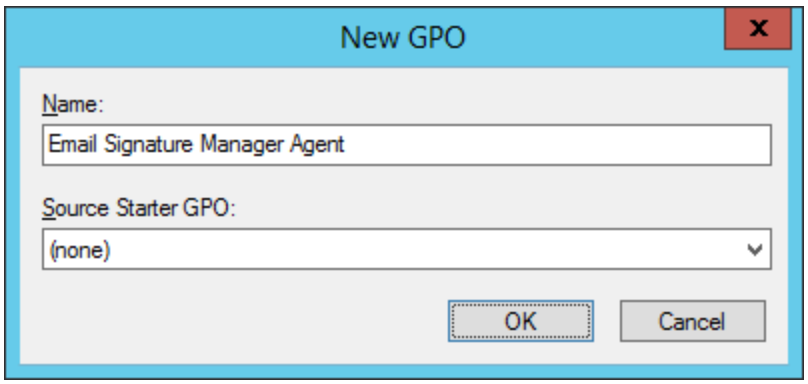
- On the folder containing the MSI package, ensure that the built-in group **Domain Users** has **Read** permissions.

2. On a domain controller, start **Group Policy Management** from **Control Panel** > **Administrative Tools**.

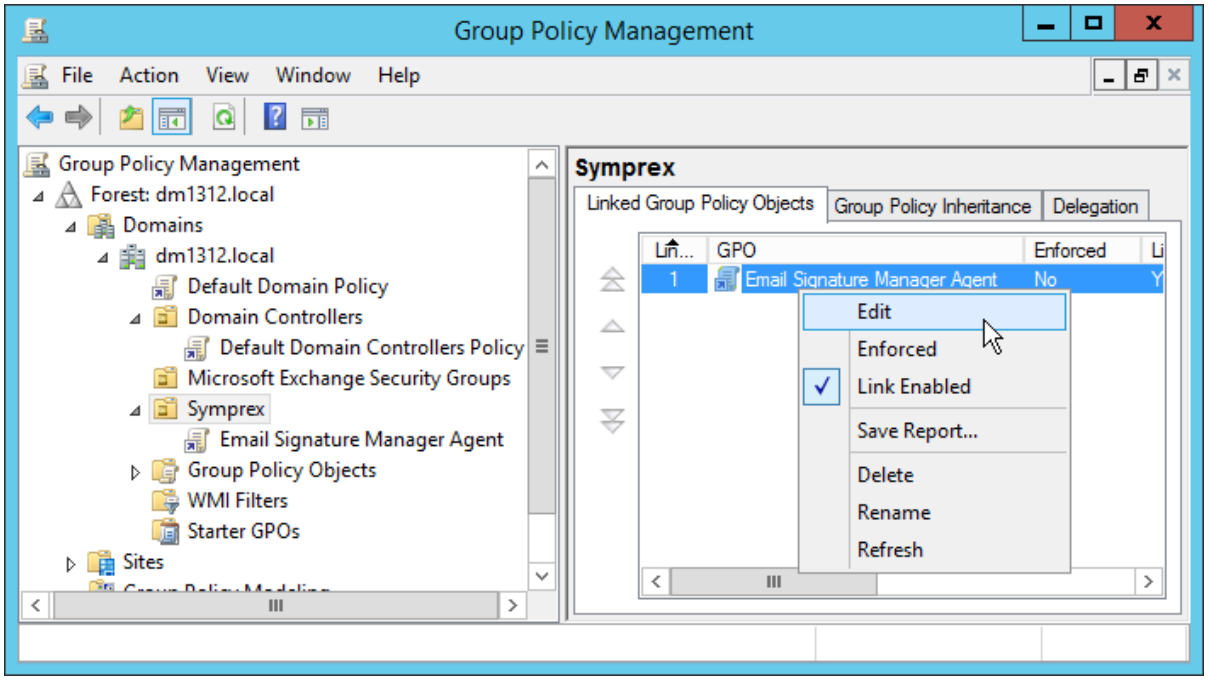
3. Within your domain, choose the Organization Unit (OU) that contains the users for which you wish to install the Agent. Alternatively, you can install to the entire domain but this will include *all* users (e.g. the built-in administrator account), which may not be appropriate. Right-click the chosen OU and select **Create a GPO in this domain, and Link it here...**.



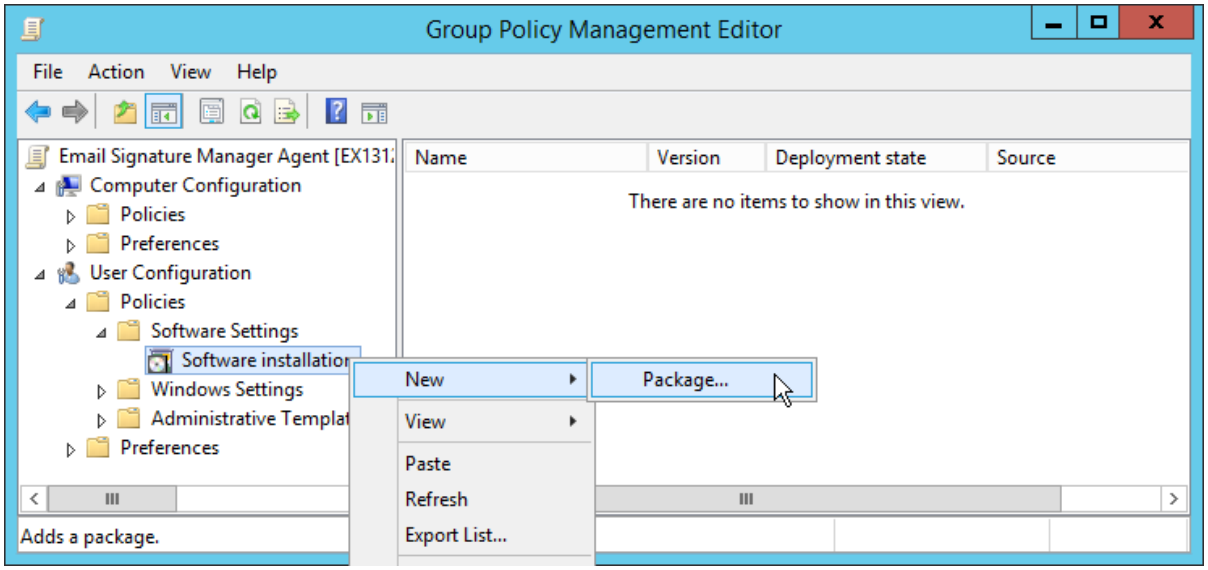
4. In the **New GPO** dialog, enter the name of the new Group Policy Object (for example, "Email Signature Manager Agent") and click the **OK** button.



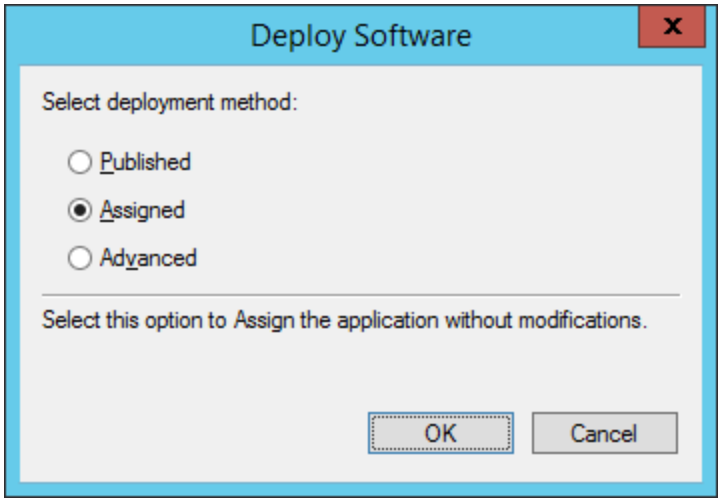
5. The new Group Policy Object (GPO) should now appear in your chosen OU. Right-click it and select **Edit**:



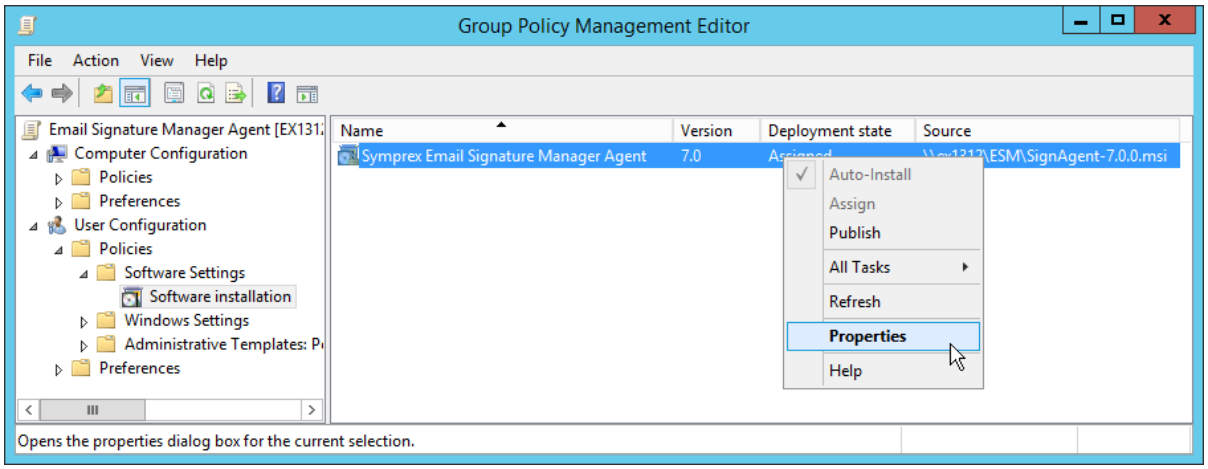
6. In the **Group Policy Management Editor**, expand **User Configuration** > **Policies** > **Software Settings**, right-click Software installation and select **New** > **Package...**:



7. Browse to and select the MSI package for the Agent. In the Deploy Software dialog, select **Assigned** and click the **OK** button:

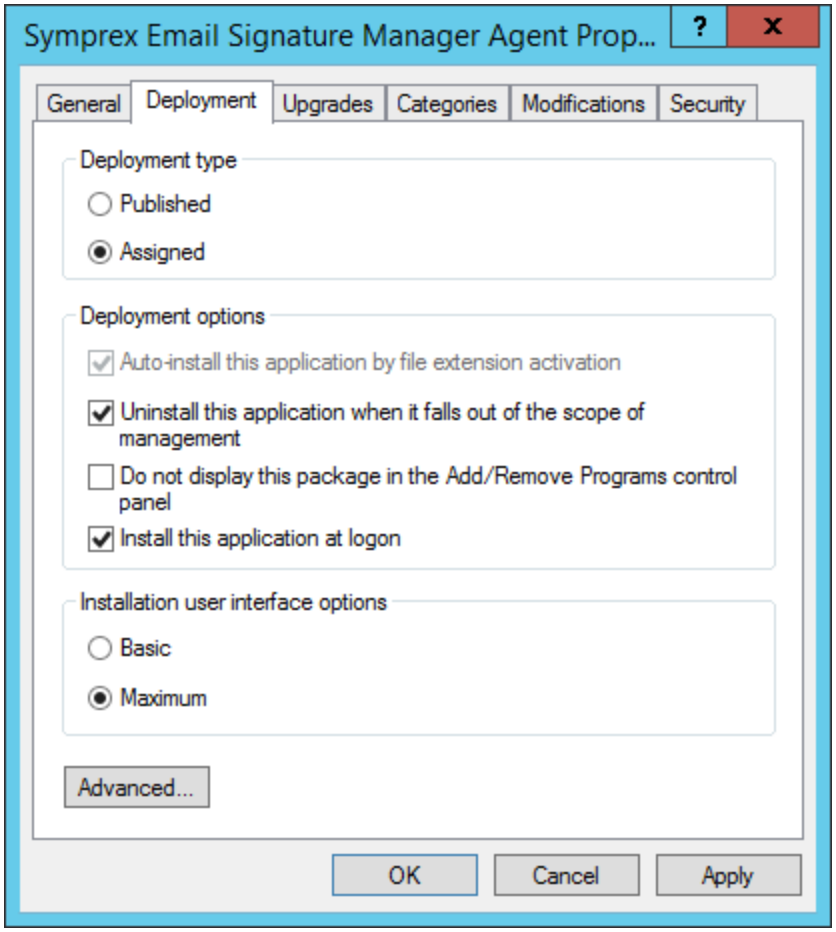


8. Right-click the new **Email Signature Manager Agent** package and select **Properties**:



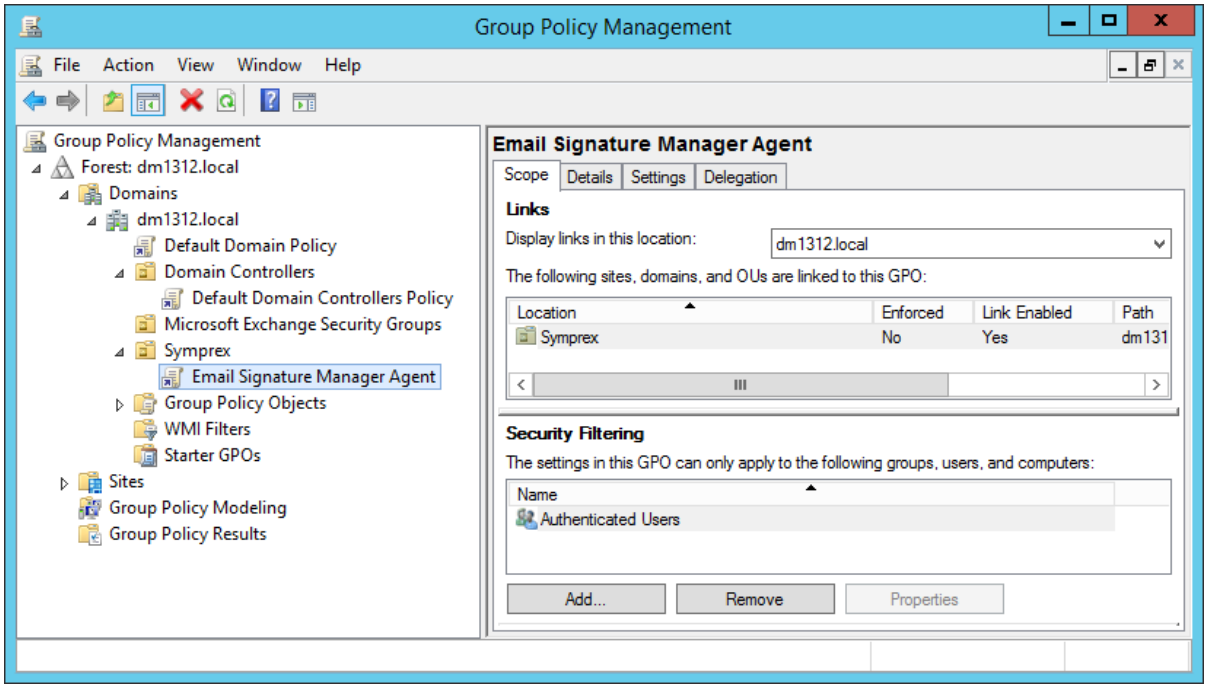
9. On the **Properties** dialog, select the **Deployment** tab and check the following options:

➔ Uninstall this application when it falls of the of he scope of management
➔ Install this application at logon



Click the **OK** button to save the changes.

10. Close **Group Policy Management Editor** to return to **Group Policy Management**, and select the Agent GPO in the OU. By default, the **Authenticated Users** group will have been added under **Security Filtering**:



This is suitable for per-user installations based on membership of the selected Organization Unit. The users and groups to which the Agent is installed can be further refined by adding to the filtering list.

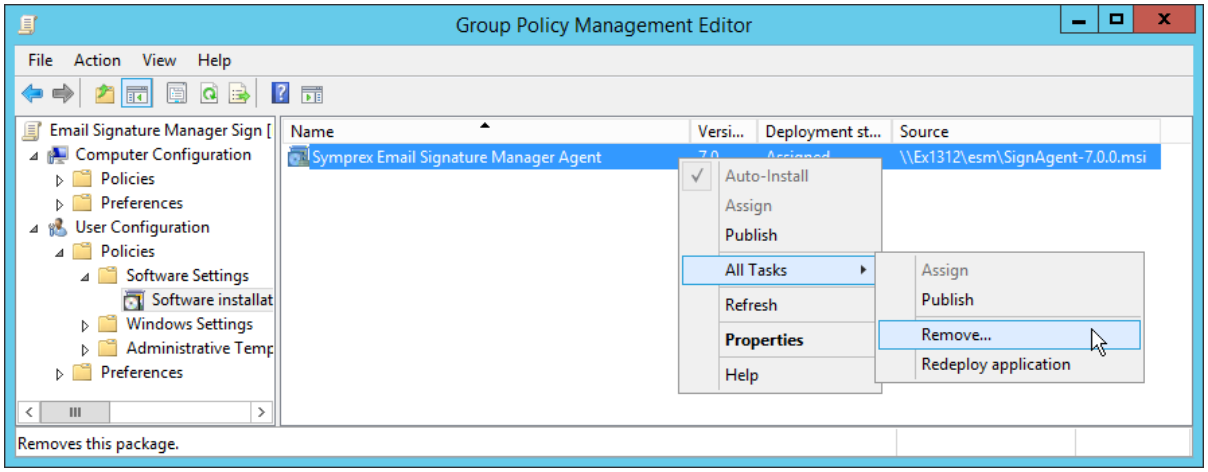
Upgrading when Using Group Policy

The simplest way to upgrade the Agent when using Group Policy is as follows:

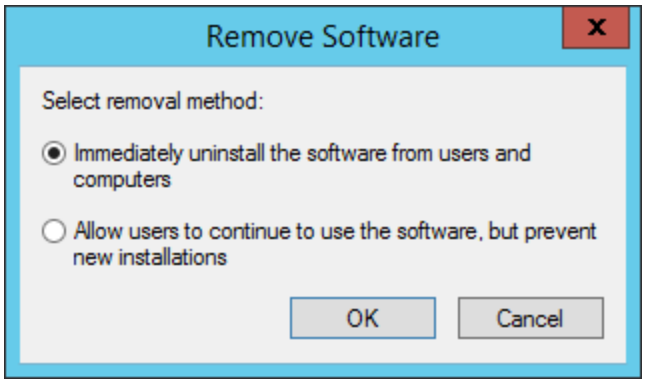
1. Open **Group Policy Management** and in the **Group Policy Objects** node, edit the GPO that installs the Agent.

2. In the **Group Policy Management Editor**, expand **User Configuration** > **Policies** > **Software Settings**.

3. Right-click the package that installs the previous version and select **All Tasks** > **Remove...**.



4. In the **Remove Software** dialog, ensure the **Immediately uninstall the software from users and computers** option is selected, and click the **OK** button.



5. Create a new package to install the new version of the Agent i.e. follow from step 6 above using the new version of the MSI package.

Installing the Agent using Group Policy Per Computer

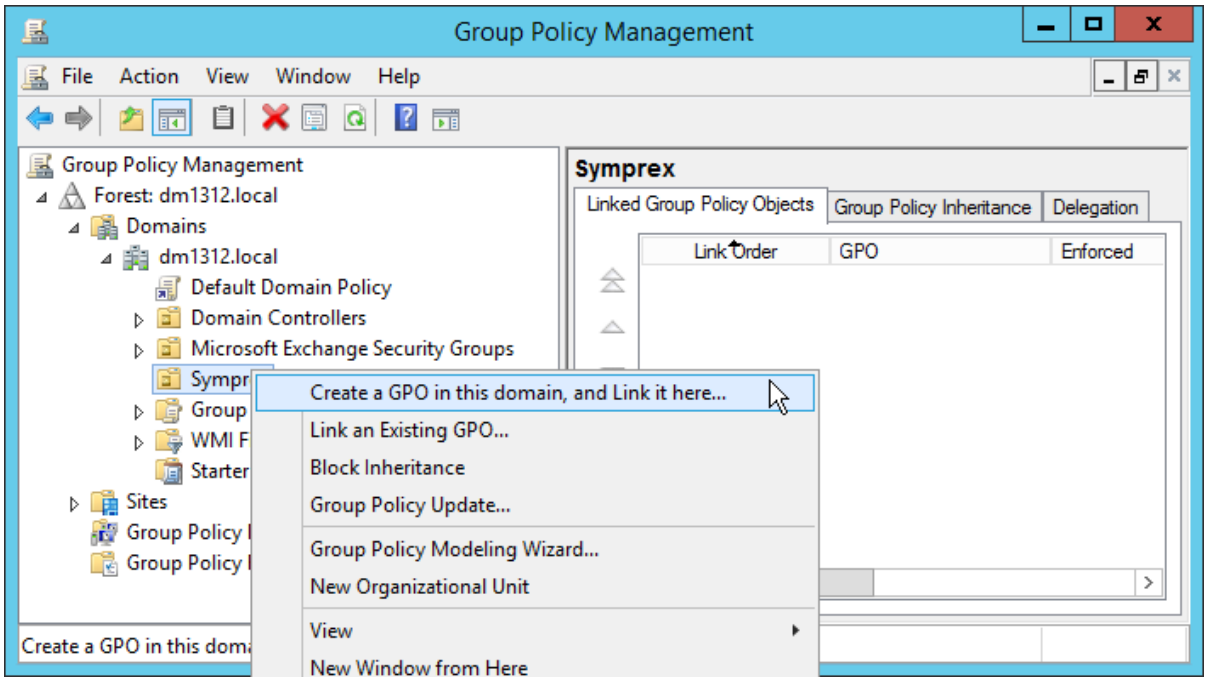
The following guidelines demonstrate a simple method to create a suitable Group Policy Object (GPO) to install the Agent on a per-computer basis on Windows Server 2012 R2 (the steps are the same for previous versions of Windows Server):

1. Download the **Email Signature Manager Agent** MSI package from the Symprex website and copy it to a shared location to which your domain users have access. To function correctly, the following permissions must be set:

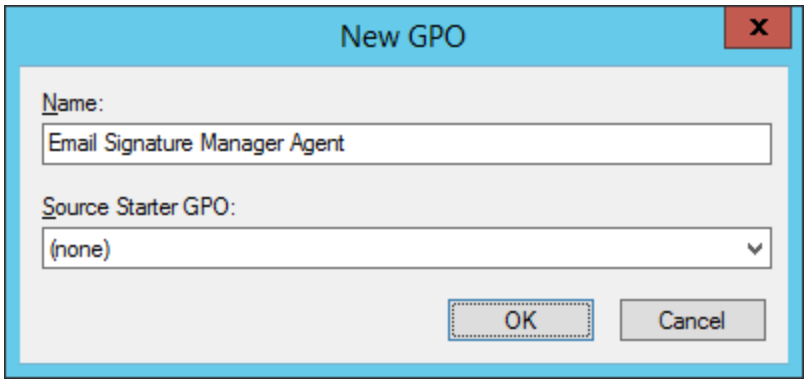
   - On the share itself, ensure that the generic group **Everyone** has **Read** permissions.
   - On the folder containing the MSI package, ensure that the built-in group **Domain Computers** has **Read** permissions.

2. On a domain controller, start **Group Policy Management** from **Control Panel** > **Administrative Tools**.

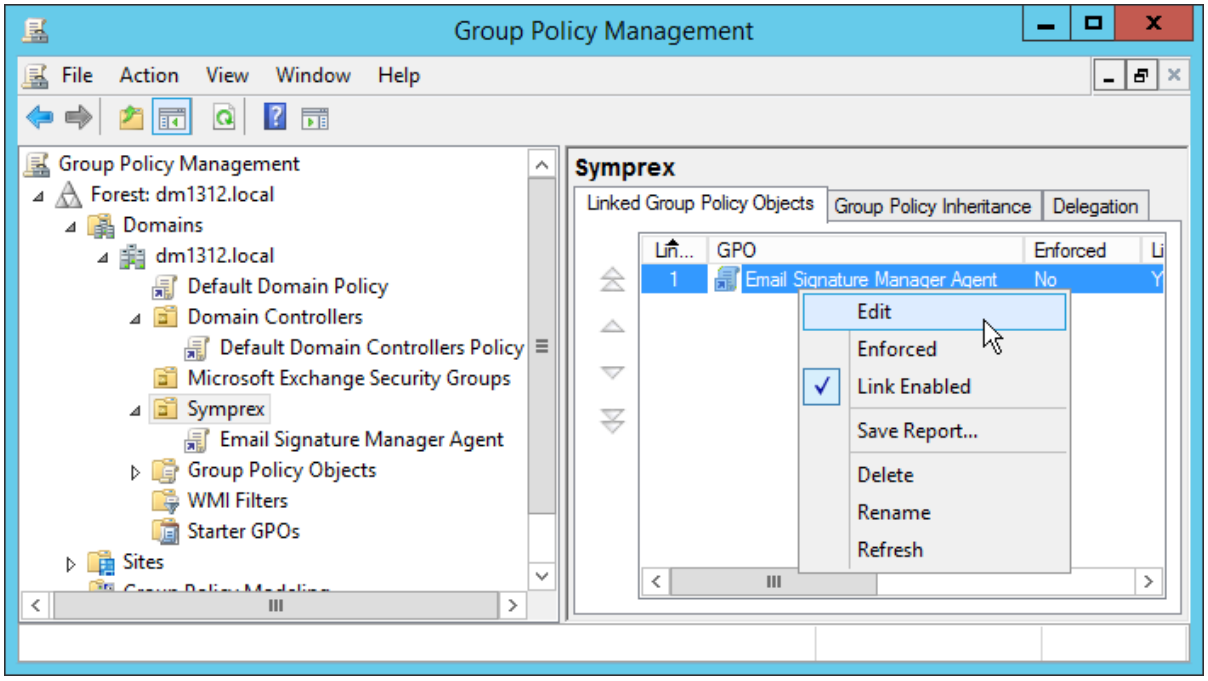
3. Within your domain, choose the Organization Unit (OU) that contains the computers to which you wish to install the Agent. Alternatively, you can install to the entire domain but this will include *all* computers (e.g. domain controller servers), which may not be appropriate. Right-click the chosen OU and select **Create a GPO in this domain, and Link it here...**.



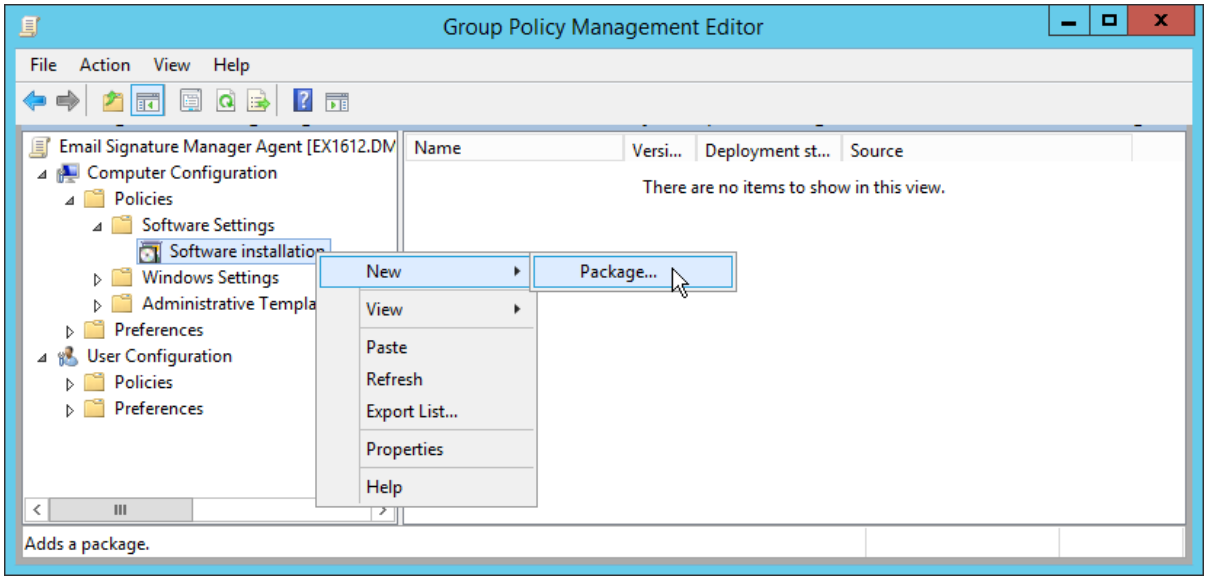
4. In the **New GPO** dialog, enter the name of the new Group Policy Object (for example, "Email Signature Manager Agent") and click the **OK** button.



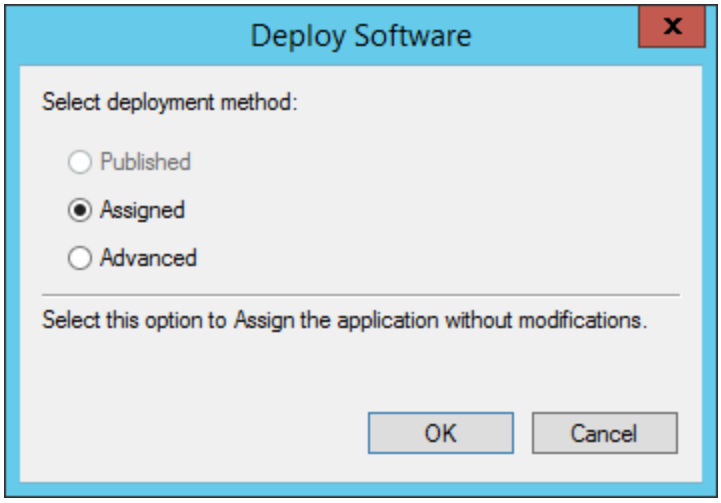
5. The new Group Policy Object (GPO) should now appear in your chosen OU. Right-click it and select **Edit**:



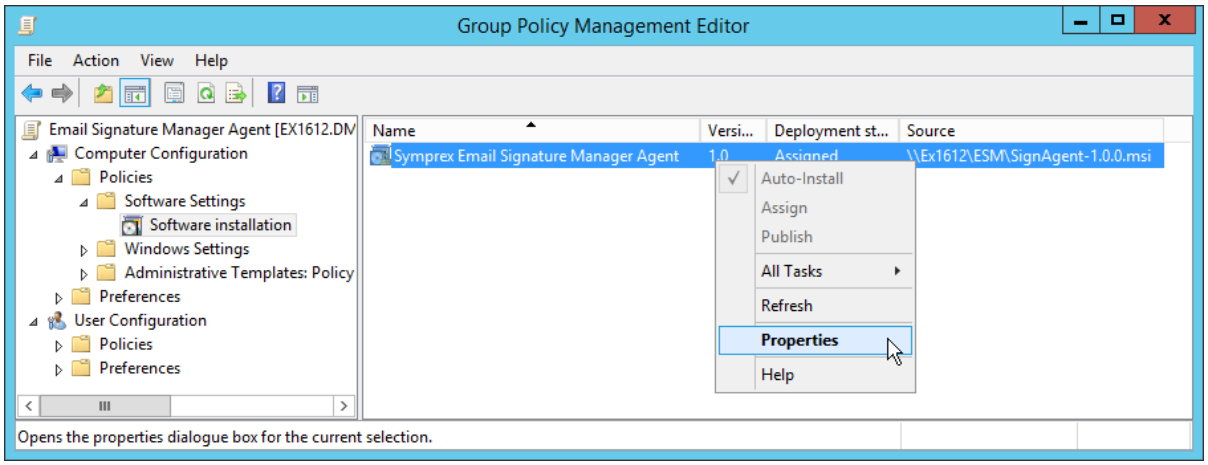
6. In the **Group Policy Management Editor**, expand **Computer Configuration** > **Policies** > **Software Settings**, right-click Software installation and select **New** > **Package...**:



7. Browse to and select the MSI package for the Agent. In the Deploy Software dialog, select **Assigned** and click the **OK** button:

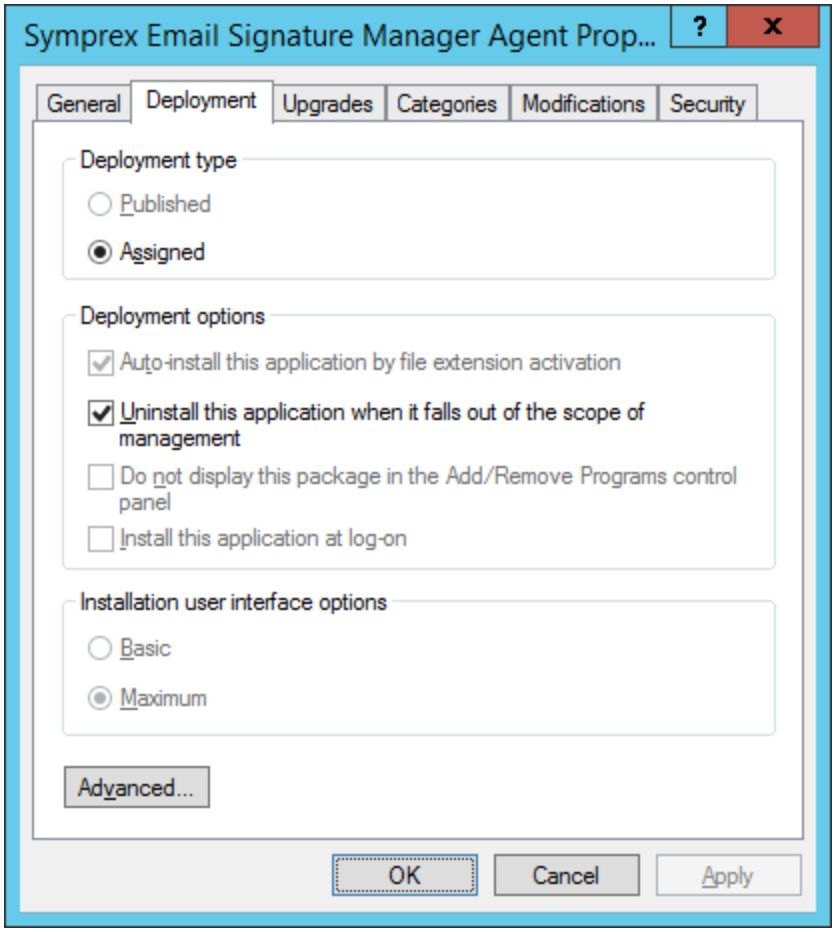


8. Right-click the new **Email Signature Manager Agent** package and select **Properties**:



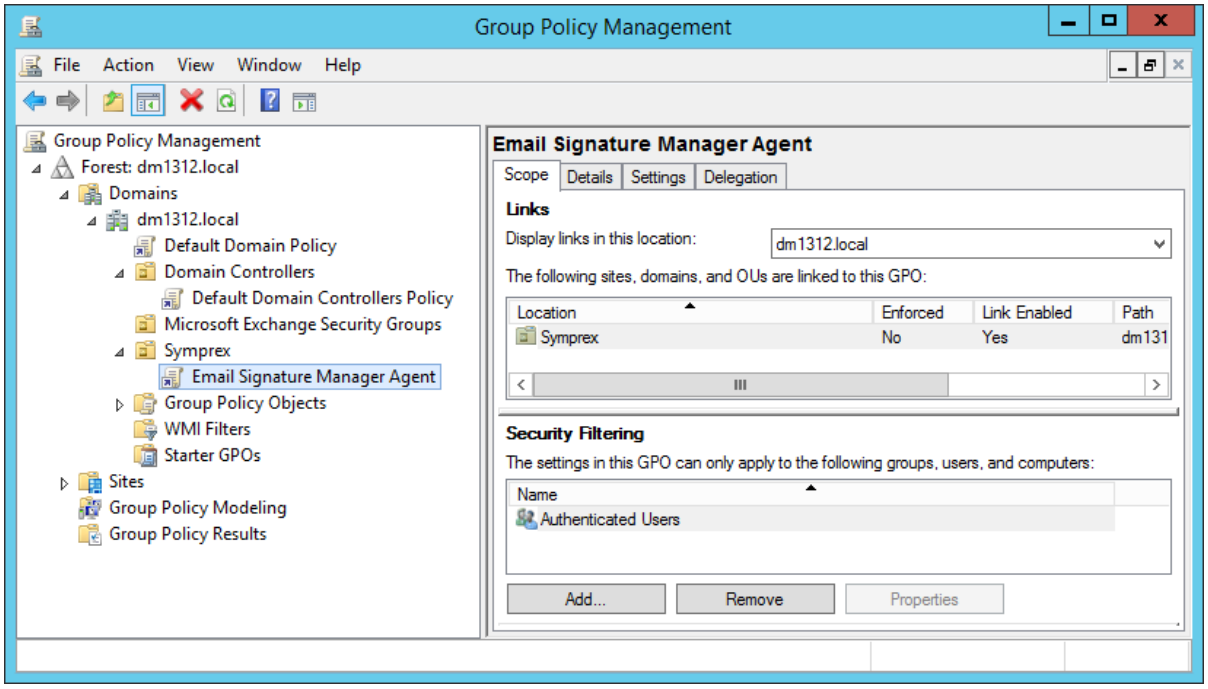
9. On the **Properties** dialog, select the **Deployment** tab and check the following option:

   ➔ Uninstall this application when it falls of the of he scope of management



Click the **OK** button to save the changes.

10. Close **Group Policy Management Editor** to return to **Group Policy Management**, and select the Agent GPO in the OU. By default, the **Authenticated Users** group will have been added under **Security Filtering**:



This is suitable for per-computer installations based on membership of the selected Organization Unit. The computers to which the Agent is installed can be further refined by adding to the filtering list.

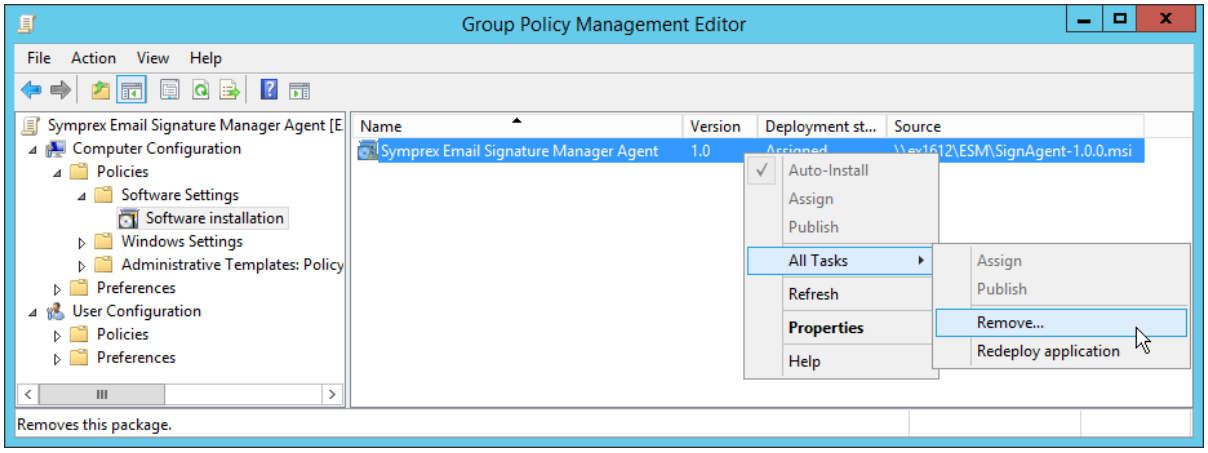
Upgrading when Using Group Policy

The simplest way to upgrade the Agent when using Group Policy is as follows:

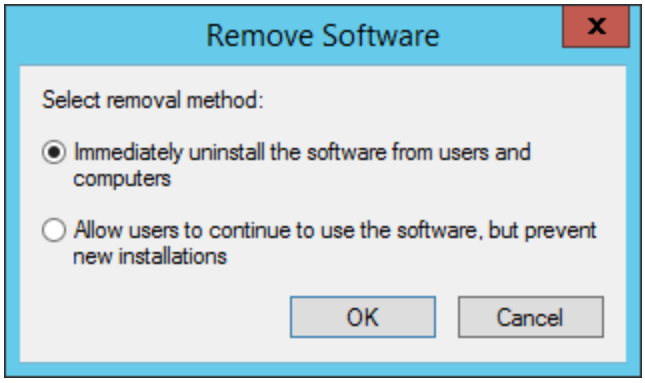
1. Open **Group Policy Management** and in the **Group Policy Objects** node, edit the GPO that installs the Agent.

2. In the **Group Policy Management Editor**, expand **Computer Configuration** > **Policies** > **Software Settings**.

3. Right-click the package that installs the previous version and select **All Tasks** > **Remove...**.



4. In the **Remove Software** dialog, ensure the **Immediately uninstall the software from users and computers** option is selected, and click the **OK** button.



5. Create a new package to install the new version of the Agent i.e. follow from step 6 above using the new version of the MSI package.

Additional Group Policy Settings

The following Group Policy settings can help to overcome problems if the Agent is not working properly when started from a logon script or when installed on a per-user or per-computer basis:

- Under **Computer Configuration** > **Administrative Templates** > **System** > **Logon**, enable the **Always wait for the network at computer startup and logon** setting.
- Under **Computer Configuration** > **Administrative Templates** > **System** > **Group Policy**, configure the **Specify startup policy processing wait time** setting to a suitable value (for example, 120 seconds; the default used by Windows is normally 30 seconds).

Note These settings can have an impact on the startup performance of the computer; please refer to Microsoft documentation before adjusting them.

Installing the Agent using ClickOnce

ClickOnce is a Microsoft technology that enables any user to install and run a Windows-based client application by clicking a link on a web page.

ClickOnce works whether the user is logged on to a domain or not, and does not require administrator permissions.

The **Email Signature Manager Agent** can be installed using ClickOnce from this web page:

https://clickonce.symprex.com

The application is installed per user, and can be uninstalled from the **Programs and Features** control panel application in Windows.

When installed using ClickOnce, an additional **Check Now** button is available on the **Options** dialog to check if a new version of the Agent is available.

Note In order to install using ClickOnce, .NET Framework 4.5 or higher must be installed on the target computer.

Mobile Device Signature Injection

Signature injection is used to process emails sent from mobile devices. Unlike deployment to other platforms (such as Outlook, where the signatures are automatically included when the message is being composed by the user), pre-generated signatures for mobile devices are injected into emails during delivery through either Exchange Server or Office 365. This is accomplished by defining a set of rules to identify where the signature should be injected into the email using the Mobile Device Signatures dialog.

- If your organization is using Exchange Server, you will need to use the Email Signature Manager Transport Agent.
- If your organization is using Office 365, you will need to use the Signature Injection Service for Office 365.

Using the Email Signature Manager Transport Agent

The **Email Signature Manager Transport Agent** is used to inject signatures into emails sent from mobile devices during delivery through your organization's Exchange Server.

Note The Email Signature Manager Transport Agent can normally only be used in conjunction with On-Premises Exchange Server, although some Hosted Exchange providers may allow the Transport Agent to be installed.

Basic Architecture

The following work flow sets out the basic architecture of how signatures are injected to emails sent from mobile devices:

- The administrator authors the signatures for deployment to users in the usual manner.
- Using the Manage Deployment dialog, mobile device signatures are specified for the appropriate groups and users.
- Each user's signature is generated by the Email Signature Manager Service.
- The administrator defines the rules for identifying where signatures should be injected into emails.
- The Email Signature Manager Transport Agent is installed onto each Exchange Server that has the appropriate role.
- When an email is delivered through Exchange Server, the Transport Agent injects the appropriate signature at the location identified by the rules.

Getting Started with the Transport Agent

To get started with the Transport Agent, please follow these instructions:

1. Install the Transport Agent on to the appropriate Exchange Server(s) and complete configuration.
2. Configure which your users will receive mobile signatures in the Manage Deployment dialog.
3. Define the rules used by the Transport Agent and enable signature injection.

Injecting Signatures using the Injection Rules

When the Transport Agent processes an email, the following steps occur:

- The signature injection rules in the order in which they are defined.
- Each rule is only applied if (a) it is active, and (b) the email is in a format supported by the rule.
- If the rule is to be applied, the email is parsed for the first instance of the **Text to Replace**; this will take into consideration the settings for detecting new lines before and/or after the text, as well as separators between emails in reply/forward emails. When found, the generated mobile device signature is used to replace the text and hence, the signature is injected into the email.
- If a rule results in a signature being injected, then no further rules are evaluated.

Note It is not always possible to correctly identify the separator between emails; this is particularly relevant on the Apple iOS devices, which do not insert identifiable characters to separate emails.

Installing the Transport Agent

The **Email Signature Manager Transport Agent** must be installed on to each On-Premises Exchange Server that has the **Mailbox Server** role installed.

Note For further information about the Mailbox Server role, please refer to the appropriate Technet articles for Exchange Server 2013, Exchange Server 2016 and Exchange Server 2019.

To install the Transport Agent, please follow these steps:

1. Download the Email Signature Manager Transport Agent Setup package from the Symprex website.

2. Run the Setup package on each Exchange Server in your organization that has the Mailbox Server role installed.

Important If you install the Transport Agent to a custom location that is not contained with the main Program Files directory, you must ensure that the account under which the Microsoft Exchange Transport service is running has read permissions on the installation folder.

3. When the setup has finished, run the Configuration Utility to complete the final configuration tasks.

Configuring the Transport Agent

The **Email Signature Manager Transport Agent** is configured using the installed Configuration Utility, which can be started from the Start menu.

There are two steps to complete once installation has been completed:

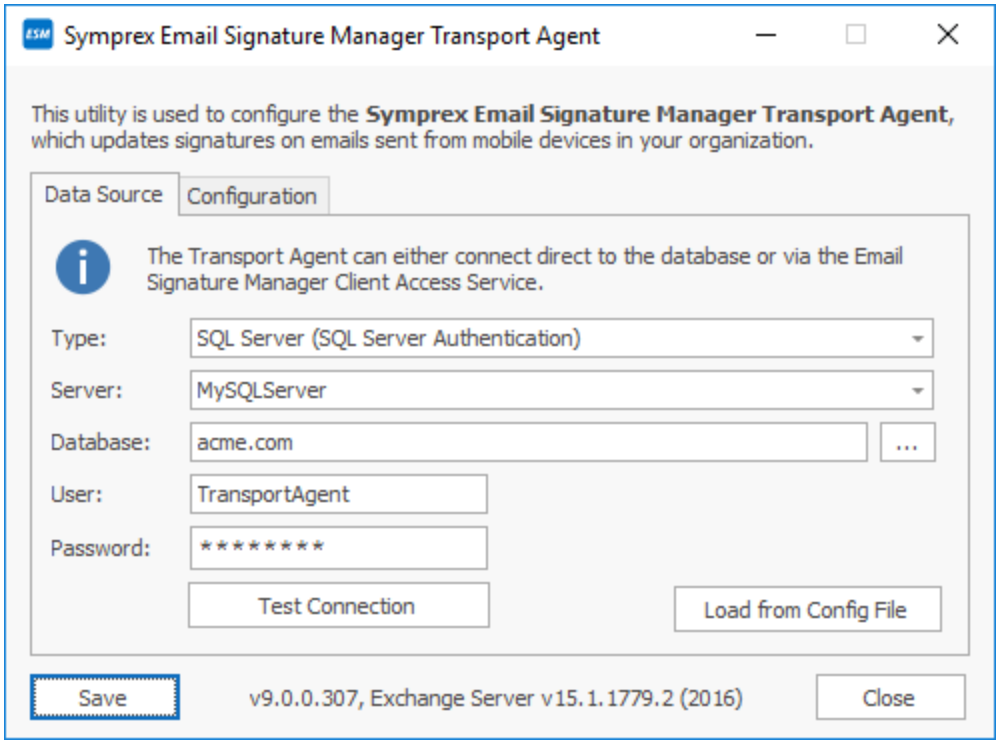
1. Specify the connection to the Email Signature Manager database.

2. Configure the various settings for the Transport Agent.

Note You will need administrative privileges on the server to run the Configuration Utility.

Specifying the Database Connection

The connection to the Email Signature Manager database is configured on the **Data Source** tab in the Configuration Utility:



Configure the following settings as required:

- **Type:** Select the type of the database, which can be one of the following:
  - Client Access Service: Connects the Transport Agent to the Client Access Service
  - SQL Server: Connects the Transport Agent direct to the SQL Server database
  - Built-in Database: Connects the Transport Agent direct to the built-in database (only when the installed on the same server as the Full Installation)
- **URL** (Client Access Service only): Enter the URL of the Client Access Service or leave blank to the use the Service Connection Point in Active Directory (recommended).
- **Server** (SQL Server only): Enter the name of the server where the database is located or select it from the drop-down list of available servers.
- **Database** (SQL Server only): Enter the name of the database on the server or select it by clicking the ellipses ("...") button.
- **User** (SQL Server only): Enter the login to connect to the server; when using SQL Server, it is recommended that you use the same login as the main application.
- **Password** (SQL Server only): Enter the password for the login.

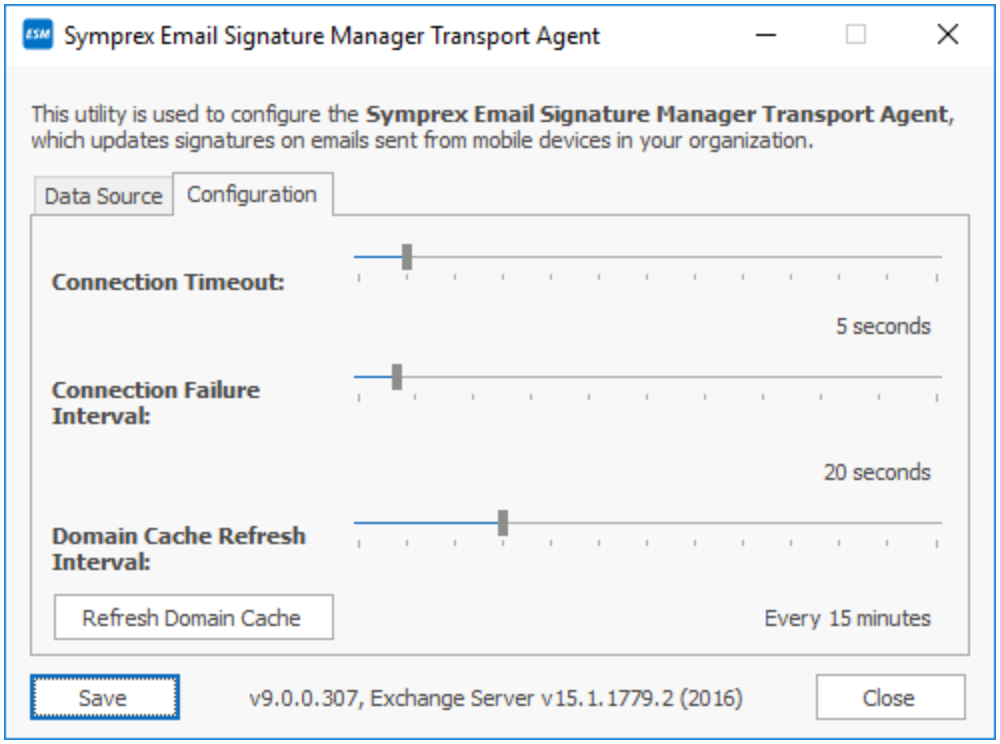
To verify that you have entered the details of the database correctly, click the **Test Connection** button.

Note When the Email Signature Manager database is hosted on SQL Server it is recommended to connect the Transport Agent directly to the database.

When ready, click the **Save** button to save the settings.

Configure Settings

The following settings can be configured on the **Configuration** tab:



- **Connection Timeout:** Specifies the timeout for connecting to SQL Server when processing an email. It is recommended that this timeout is kept fairly short as connections should be made quickly under normal operating conditions.

- **Connection Failure Interval**: If connecting to SQL Server fails when processing an email, this interval specifies how long the Transport Agent will wait until trying to connect again. During this interval, any emails processed by the Transport Agent will not have signatures applied.

- **Domain Cache Refresh Interval**: For efficiency, the Transport Agent maintains a list of the local domains from which emails should be processed; this allows emails to be examined very quickly without the need for a database connection to be established to determine if they need processing. This interval specifies how often the cache should be refreshed. If necessary, the cache can be refreshed on demand by clicking the **Refresh Domain Cache** button. The domain cache is not supported when using the Client Access Service.

When ready, click the **Save** button to save the settings.

Registering on Exchange Server

In order for the Transport Agent to be used to process email, it must be registered with Exchange Server. This is accomplished by executing the appropriate commands within the Exchange Management Shell. The installer for the Transport Agent will execute these commands when the agent is installed, so there are no manual steps required. Should you wish, you can verify that the Transport Agent is registered as follows:

1. Start an instance of the **Exchange Management Shell**.

2. Type the following command:

```
Get-TransportAgent -Identity "Symprex Email Signature Manager Agent" | fl
```

3. The details of the agent should be listed. If they are not, the Agent is not registered. Please refer to the Knowledge Base article "Managing the Transport Agent Registration" for more details on how to register the Agent manually.

When ready, click the **Close** button to close the Configuration Utility.

Using the Signature Injection Service for Office 365

The **Signature Injection Service for Office 365** is designed to inject email signatures into emails sent from mobile devices on Office 365. The service is implemented as a cloud solution hosted by Symprex on the Microsoft Azure platform inside secure ISO 27001 certified Microsoft data centres. If you subscribe to this service, your license will be enabled as appropriate, and the Email Signature Manager Service will upload your mobile device signatures and settings to the cloud.

In order to use the service, your Office 365 tenant must be configured to route email through the Signature Injection Service for Office 365, which then injects email signatures into email that passes through. The service is transparent and emails continue to be delivered to recipients by your Office 365 tenant; the email flow is as follows:

- Sender → Office 365 → Signature Injection Service for Office 365 → Office 365 → Recipients

Where:

- "Sender" is the sender of the email.
- "Office 365" is your Office 365 tenant.
- "Signature Injection Service for Office 365" is the signature injection service managed by Symprex and hosted on Microsoft Azure servers.
- "Recipients" are the recipients of the email as specified by the sender.

The service is hosted in the following Azure regions at the time of writing:

- UK South
- West Europe
- North Central US
- Canada East
- Australia East

The service offers the following features:

- Email is relayed only inside secure ISO 27001 certified Microsoft data centres, and only within your associated geolocation to help you stay GDPR compliant.
- The architecture includes load balancing and fault tolerance with redundancy configured according to Microsoft guidelines for the 99.95% Azure SLA.

- Email is not stored for any other purpose than signature injection and is immediately deleted from any server upon successful relay back to Office 365.

You can check if your license is enabled for the service, and perform most of the configuration automatically, using the Office 365 Integration dialog.

To subscribe to this service, please contact sales@symprex.com.

For technical support relating to this service, please contact support@symprex.com.

Mobile Device Signature Distribution by Email

Distribution of mobile device signatures by email is an alternative to using the Email Signature Manager Transport Agent or Signature Injection Service for Office 365 for customers that are unable to use those. Email Signature Manager generates the users' mobile device signature and sends it to them (as an attachment) by email. It is then the responsibility of each user to copy and paste the new signature into the mail app on their mobile device.

To send mobile device signatures by email, follow these steps:

1. In the Manage Deployment dialog, select the **Mobile Device** signature for each group and user as required.

2. In the Mobile Device Signatures dialog, on the **Send Signatures** tab, select the appropriate option to send the Mobile Device Signature to users who have their mailbox hosted on Exchange Server and/or Office 365.

3. In the Mobile Device Signatures dialog, on the **Send Signatures** tab, configure the email that will be sent to each user.

Note The service will only send the plain-text version of the signature; it is therefore important to ensure that all signature templates have a plain-text definition.

Once the configuration is completed, the Service will generate (on its next cycle) the mobile device signatures for users and send it to them by email. Once the signature has been sent, it will not be sent again unless the content of the signature changes (for example when the definition of the signature is altered or the user's information changes).

Appendices 4

This section contains additional information for using Email Signature Manager.

Using Microsoft SQL Server

Email Signature Manager fully supports using Microsoft SQL Server.

The following versions are supported:

- SQL Server 2012
- SQL Server 2014
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019

SQL Server must be used as the database for Email Signature Manager in any of the following scenarios:

- You wish to manage the database from more than one computer.
- You wish to use the Email Signature Manager Transport Agent.

Migrating to SQL Server

To migrate from using the Built-in Database to SQL Server, please use the following steps:

1. If you do not have a SQL Server available within your organization, please read the topic on how to install and configure SQL Server Express.

2. Create the Email Signature Manager database on the appropriate instance of SQL Server.

3. Using Services Control Manager, stop the Email Signature Manager Service.

4. Start the main Email Signature Manager application.

5. Connect to the Email Signature Manager database created in step 2 using the Settings Database dialog. You must connect to the database using SQL Server Authentication.

6. Open the Import Database dialog. Ensure the **Type** is selected as **Access** and then click the ellipses ("...") button next to the **Database** text box. Select the **Built-in Database**. The default location is `C:\ProgramData\Symprex\Symprex.EmailSignatureManager.Database.mdb`.

7. Click the **OK** button and confirm that you wish to import the database. The data from the Built-in Database is now imported to the SQL Server database.

8. Using Services Control Manager, restart the Email Signature Manager Service.

9. If you wish to install Email Signature Manager on additional computers to manage the database, please read the section on Manager Only mode.

Creating the Email Signature Manager Database on SQL Server

This topic will guide you through the basic process of creating a new Email Signature Manager database on an instance of Microsoft SQL Server.

If your organization already has a SQL Server available, ensure that the database is created following any established policy.

If your organization does not have SQL Server, please follow our guide for installing and configuring SQL Server Express.

Creating the Database

1. Download the script to create the database from the Symprex website:

   https://www.symprex.com/support/files/esm/v9/sql/esmdb.zip

   This zip file contains one file, `esmdb.sql`, which should be extracted to a known location.

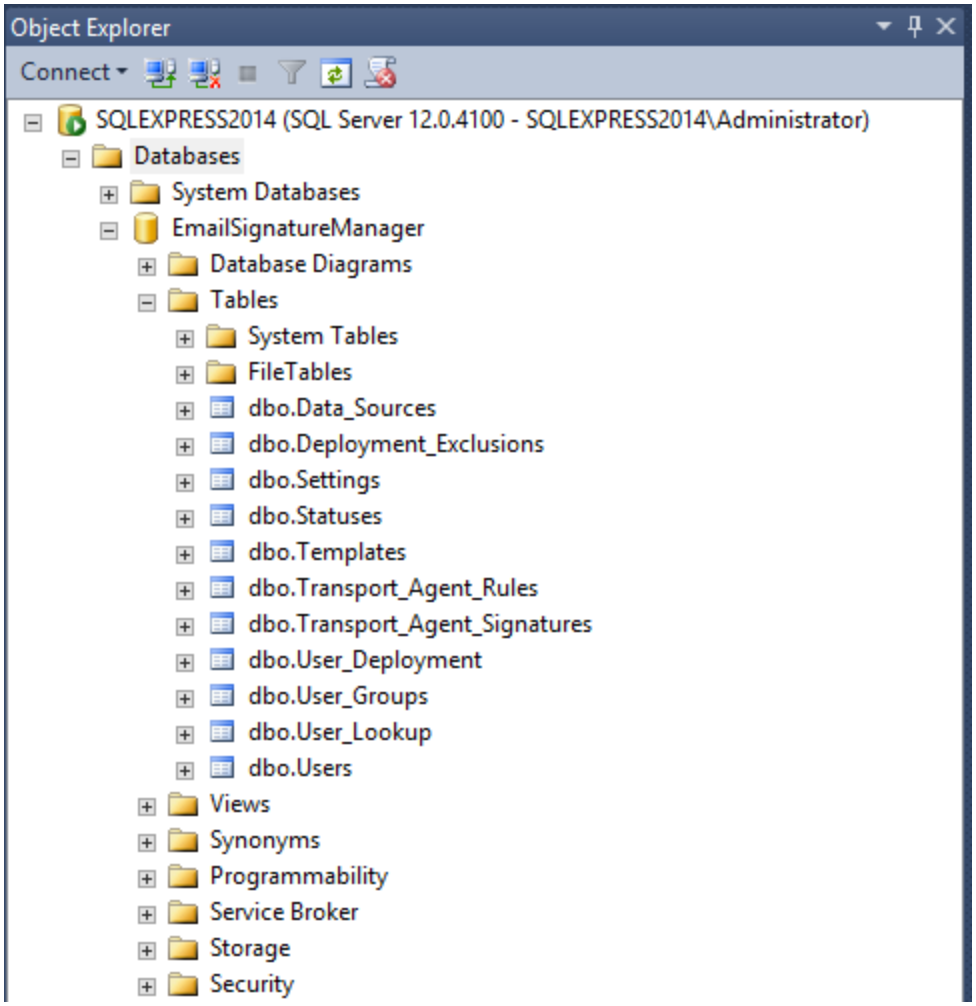
2. Start **SQL Server Management Studio** and connect to the appropriate instance of SQL Server. Right-click **Database** and select **New Database...**.

3. On the **General** page, enter a suitable name for the database. The database script uses `EmailSignatureManager` as the default name.

4. On the **Options** page, configure the appropriate settings for the database according to your organization's policy. If you are using SQL Server Express, the **Recovery Model** can be set to **Simple** and database backups taken manually (see the topic on installing and configuring SQL Server Express).

5. Select **File** > **Open** > **File...** (or press Control+O) and open the esmdb.sql script. If necessary, change the [USE] statement on the first line to point to the database created in step 3.

6. Execute the script (press F5), which will create the database structure. Verify that there are no error messages reported. To check the structure has been correctly created, expand the database node and then the **Tables** node. You should see the list of tables as follows:

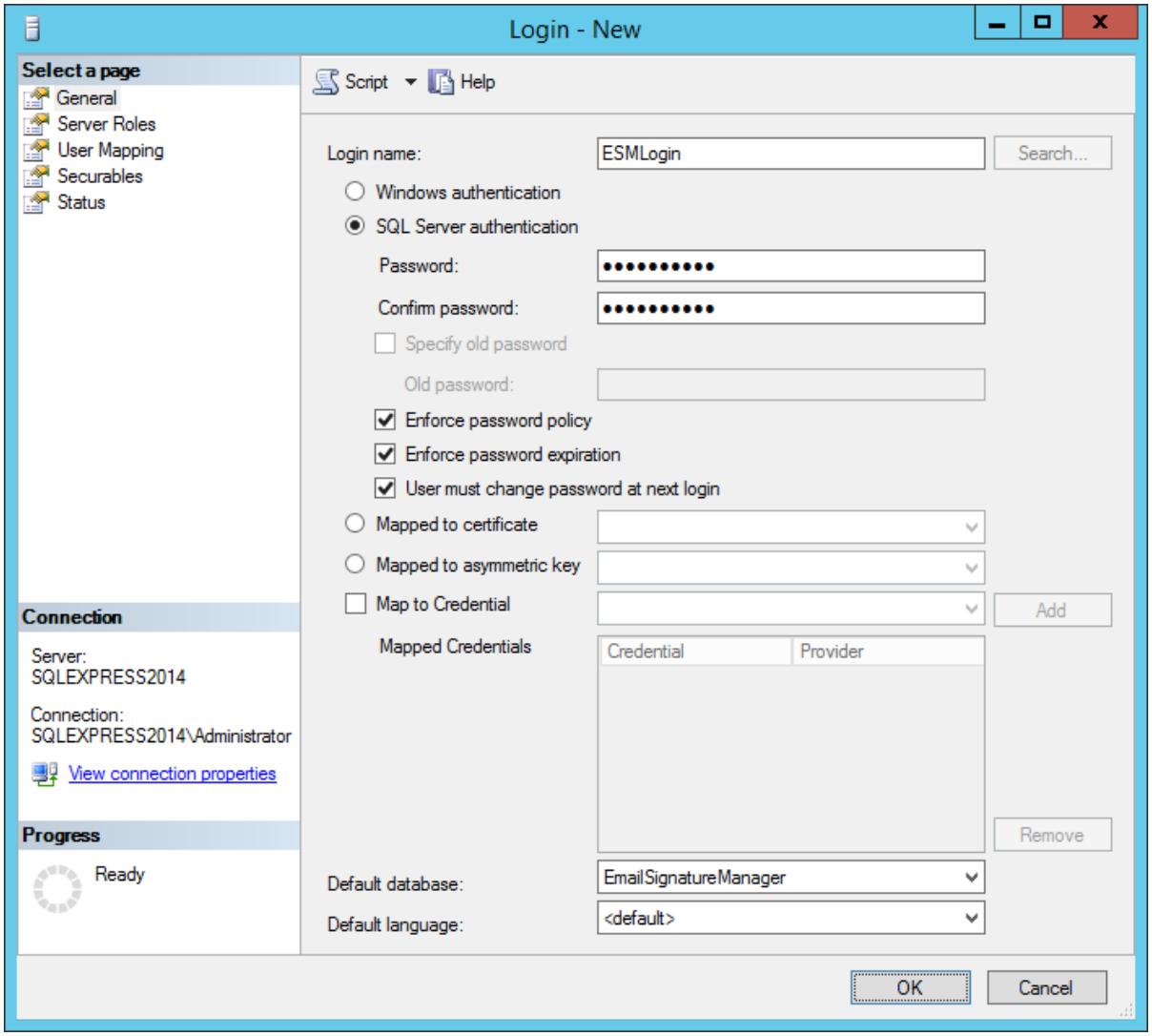


Dedicated Login

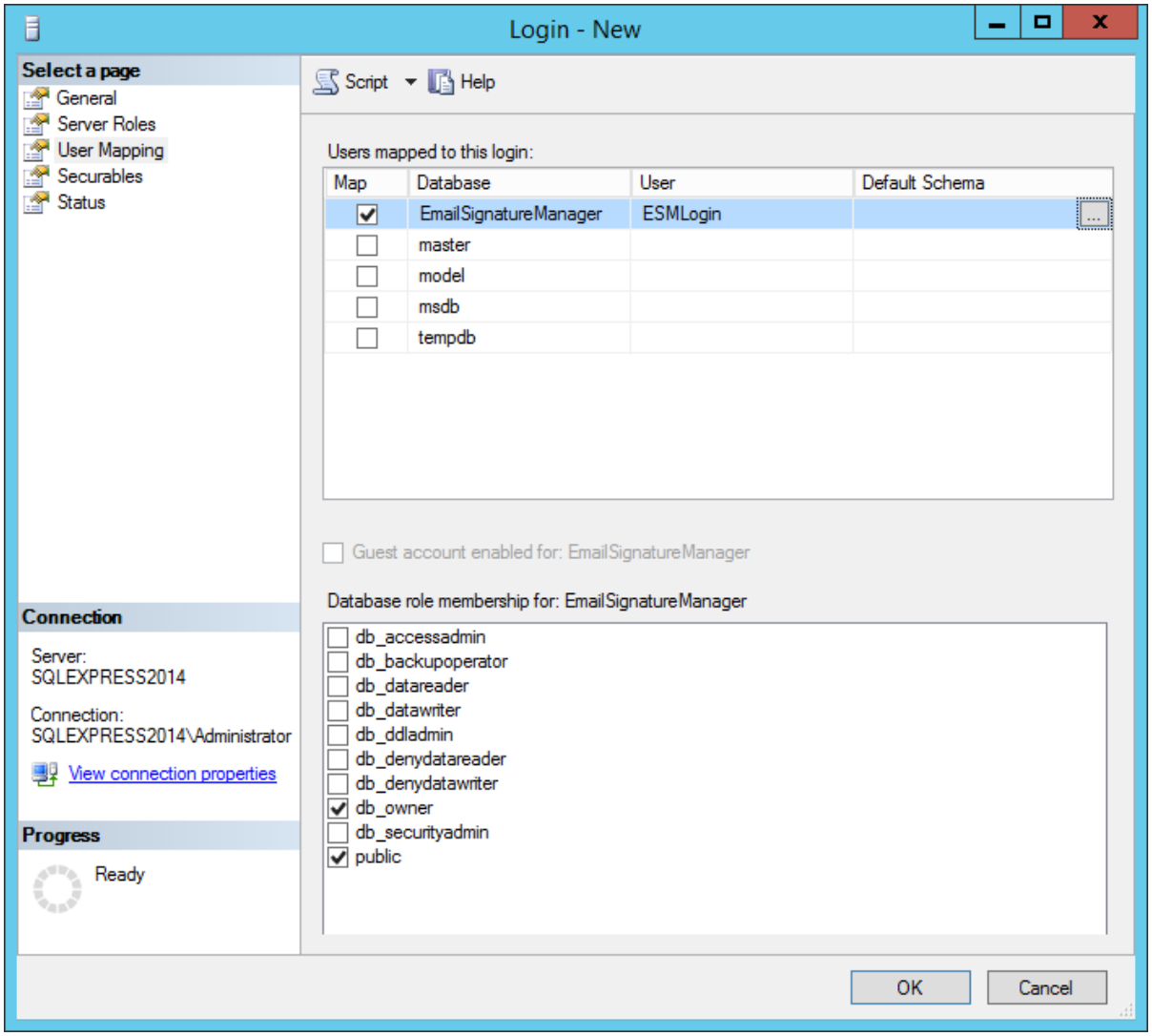
The Full Installation of Email Signature Manager requires a dedicated login using SQL Server Authentication and with **db_owner** role. This ensures that the service (which uses the same login as the main application) can connect to the database and that the database schema can be updated during upgrades of Email Signature Manager. The login can be created as follows:

1. Start **SQL Server Management Studio.** Expand the **Security** node, right-click the **Logins** node and select **New Login...**.

2. On the **General** page, enter a suitable name for the login. Select the **SQL Server Authentication** option and enter an appropriate password. Change the **Default Database** to the Email Signature Manager database. The configuration of the login should look similar to this:



3. On the **User Mapping** page, check the **Map** column for the Email Signature Manager database and then check the **db_owner** role:



4. Click the **OK** button to save the login.

The login can be now be used in the Settings Database dialog to connect to the database.

Installing and Configuring SQL Server Express

This topic will guide you through the process of installing and configuring SQL Server Express for use with Email Signature Manager.

Note This guide is based on SQL Server Express 2014 and assumes that it will be installed on to a clean machine where no other instance of SQL Server is installed.

Before You Start

1. Download the **SQL Server Express 2014 with Tools** installer from the Microsoft website. The main download page can found here:

https://www.microsoft.com/en-gb/download/details.aspx?id=42299

You should download either `ExpressAndTools 32BIT\SQLEXPRWT_x86_ENU.exe` (for 32-bit operating systems) or `ExpressAndTools 64BIT\SQLEXPRWT_x64_ENU.exe` (for 64-bit operating systems).

2. It is recommended that after installation, SQL Server Express 2014 is updated to Service Pack 1 or later. The main download page can be found here:

   https://www.microsoft.com/en-us/download/details.aspx?id=46694

   You should download either `SQLServer2014SP1-KB3058865-x86-ENU.exe` (for the 32-bit version) or `SQLServer2014SP1-KB3058865-x64-ENU.exe` (for the 64-bit version).

Install and Configure SQL Server Express 2014

1. Start the installer for the appropriate version of SQL Server Express (either `SQLEXPRWT_x86_ENU.exe` or `SQLEXPRWT_x64_ENU.exe`) and extract the installation files to a suitable location (this can take several minutes).

2. In the **SQL Server Installation Center**, select the new **SQL Server stand-alone installation** option.

3. Read the License Terms and then check the **I accept the license terms** check box. Click the **Next** button.

4. In the **Feature Selection** step, the following components are mandatory:

   - Database Engine Services
   - Client Tools Connectivity
   - Management Tools - Basic (Management Tools - Complete is recommended)

   Check the installation folders are acceptable and click the **Next** button.

5. In the **Feature Rules** step, install any prerequisites and complete any other steps that are required to continue with the installation.

6. In the **Instance Configuration** step, select the **Default Instance** option (the instance will be named `MSSQLSERVER`) and click the **Next** button.

7. In the **Server Configuration** step, it is recommended to change the **Startup Type** of the **SQL Server Browser** service to **Automatic** (which allows the instance of SQL Server to be discoverable on the network). Otherwise, the default configuration is suitable. click the **Next** button to continue.

8. In the **Database Engine Configuration** step, select the **Mixed Mode** option (this is mandatory for Email Signature Manager) and enter a suitable password for the `sa` account. The password must meet the complexity requirements specified by the Local Security Policy of the computer. It is also recommended that the **Domain Administrators** group is added to the list of **SQL Server Administrators**. Otherwise, the default configuration is suitable. Click the **Next** button to continue.

9. The installation process will now start. This can take several minutes to complete.

10. Review the actions taken in the **Completed** step, click the **Close** button to dismiss the installation wizard, and then close the **SQL Server Installation Center**.

11. At this stage, it is recommended to either install the latest Service Pack and use Windows Update to check for the latest updates.

Enabling Network Protocols

By default, only the Shared Memory protocol is enabled, which means that it is not possible to connect to SQL Server Express across the network. To enable the other protocols, use the following steps:

1. Start **SQL Server Configuration Manager**.

2. Expand **SQL Server Network Configuration** and **Protocols for MSSQLSERVER** (where `MSSQLSERVER` is the default instance name).

3. In the list of protocols, right-click the disabled protocols and select **Enable** from the context menu. It is recommended that all protocols (**Shared Memory**, **Named Pipes** and **TCP/IP**) are enabled for best connectivity to the server.

4. Right-click the **TCP/IP** protocol and select **Properties**. Select the **IP Addresses** tab and scroll down to **IPAll**. Check that the **TCP Port** is set to 1433 (the standard default for SQL Server). Close the **TCP/IP Properties** dialog.

5. Select **SQL Server Services**, right-click **SQL Server (MSSQLSERVER)** (where `MSSQLSERVER` is the default instance name) and select **Restart** to restart the SQL Server Database Engine.

6. Ensure that the firewall on the machine hosting SQL Server Express has been configured to allow the appropriate inbound TCP/IP connections. These are TCP port 1433 for the Database Engine and UDP port 1434 for the Browser Service.

Backing Up a Database

Assuming that the **Recovery model** for the database is set to **Simple**, you can create a manual backup of a database using the following steps:

1. Start **SQL Server Management Studio** and connect to the appropriate instance of SQL Server Express.

2. Expand the **Databases** node, right-click the Email Signature Manager database and select **Tasks** > **Back Up...**.

3. Ensure the **Backup type** is **Full**.

4. By default, a backup file matching the name of the database will be created (for example, `C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\Backup\EmailSignatureManager.bak`). SQL Server is able to store multiple backups in the same file. You can therefore either choose to use a single backup file or

to use a distinct file for each backup that you take. To use a distinct backup (or to alter the location where the backup is stored), click the **Remove** button to remove the default backup and then click the **Add** button to a new destination backup file. Alternatively, if you wish to use the default backup file but only store the latest backup, select the **Media Options** page and check the **Overwrite all existing backup sets** option; this will erase any existing backup in the specified backup file.

5. Click the **OK** button to create the backup.

Important This is a description of the simplest method to backup your database. It is recommended that you read this Microsoft article that fully explains backup options for SQL Server.

Restoring a Database

Before restoring the database, the Email Signature Manager Service should be stopped and any instances of the main application closed. To perform a full restore of the database, use the following steps:

1. Start **SQL Server Management Studio** and connect to the appropriate instance of SQL Server Express.

2. Expand the **Databases** node, right-click the Email Signature Manager database and select **Tasks** > **Restore** > **Database...**.

3. Select the **Device** option and click the ellipses ("...") button.

4. Check that the **Backup media type** is selected as **File** and then click the **Add** button. Select the backup file that you wish to use to restore the database and the click the **OK** button.

5. On the **General** page, verify that the correct database has been selected. If the backup file contains multiple backup sets, the latest one will be selected by default. If you wish to use an early backup set, click the **Timeline** button, select the **Specific date and time** option and choose the appropriate backup set to use.

6. On the **Options** page, select the **Overwrite the existing database (WITH REPLACE)** option.

7. Click the **OK** button to restore the database.

Using Email Signature Manager in Manager Only Mode

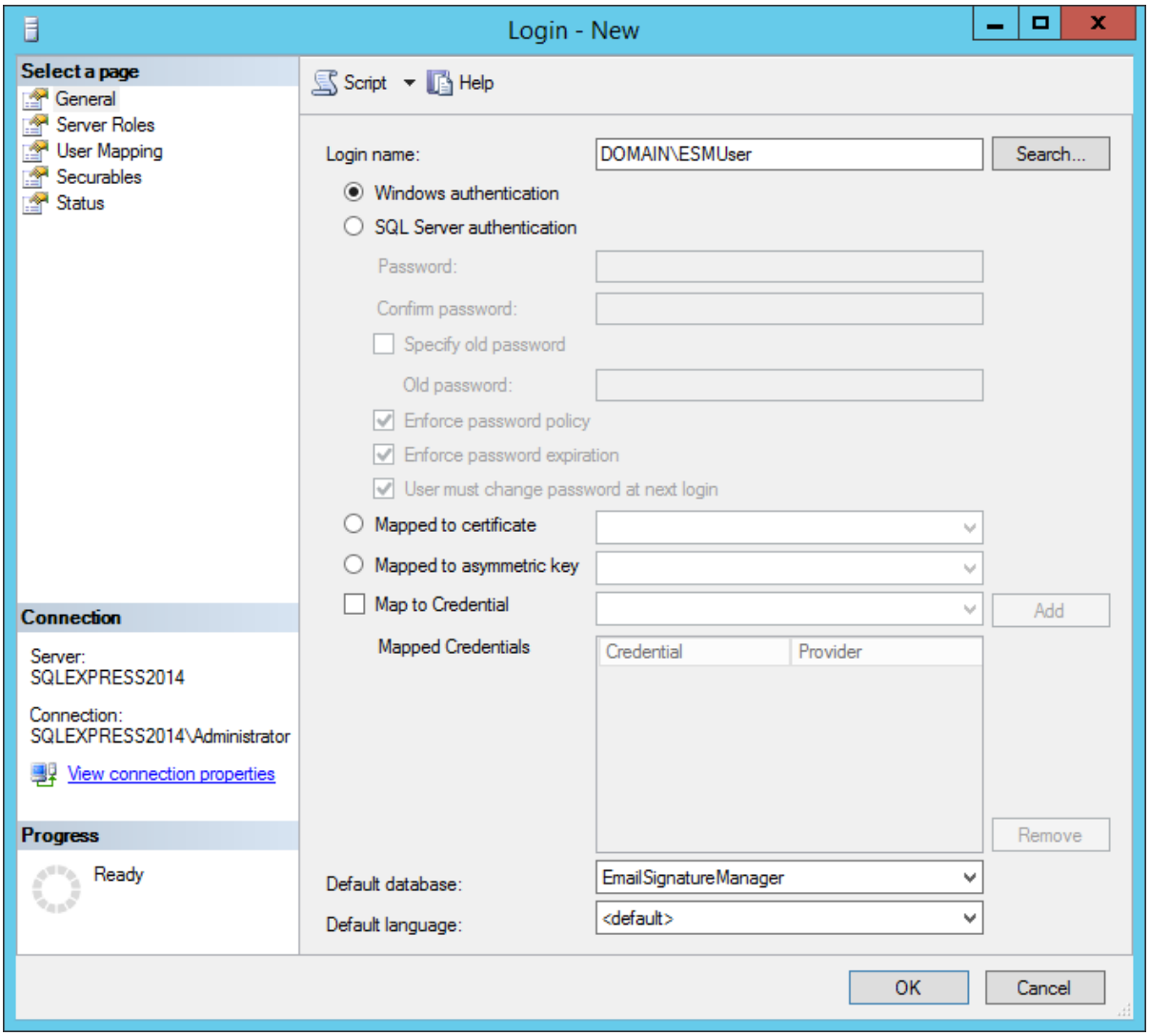
Where required, Email Signature Manager can be installed in Manager Only mode to allow other users in your organization to use Email Signature Manager on their own computers connected to the shared database. When running in Manager Only mode, the main application has certain limitations:

- The Email Signature Manager database must be hosted on Microsoft SQL Server.
- The Environment Configuration dialog is disabled.
- The Import Database function is not available.
- The Update functions (in the main application window and the Status Monitor) are not available.

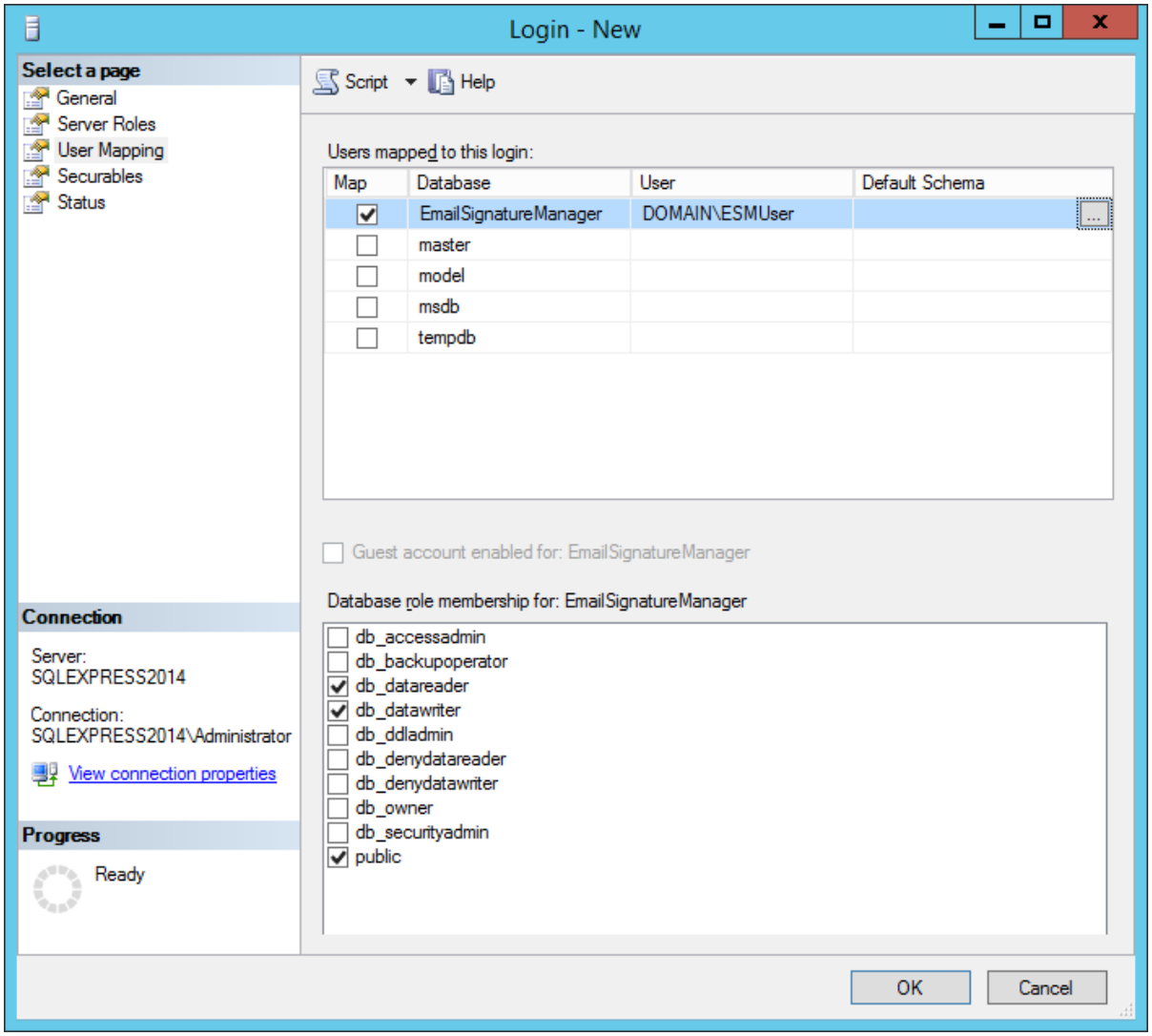
When using Manager Only mode, it is recommended that Windows Authentication is used (instead of the dedicated login) and that the user of the product is added to the **db_datareader** and **db_datawriter** roles. For example, to add a domain user as a user of the database, use the following steps:

1. Start **SQL Server Management Studio.** Expand the **Security** node, right-click the **Logins** node and select **New Login...**.

2. On the **General** tab, click the **Search** button and locate the domain user (or group) for the new login. Change the **Default Database** to the Email Signature Manager database. The configuration of the login should look similar to this:



3. On the **User Mapping** page, check the **Map** column for the Email Signature Manager database and then check the **db_datareader** and **db_datawriter** roles:



4. Click the **OK** button to save the login.

The domain user can now connect to the Email Signature Manager database by selecting **SQL Server (Windows Authentication)** in the Settings Database dialog.

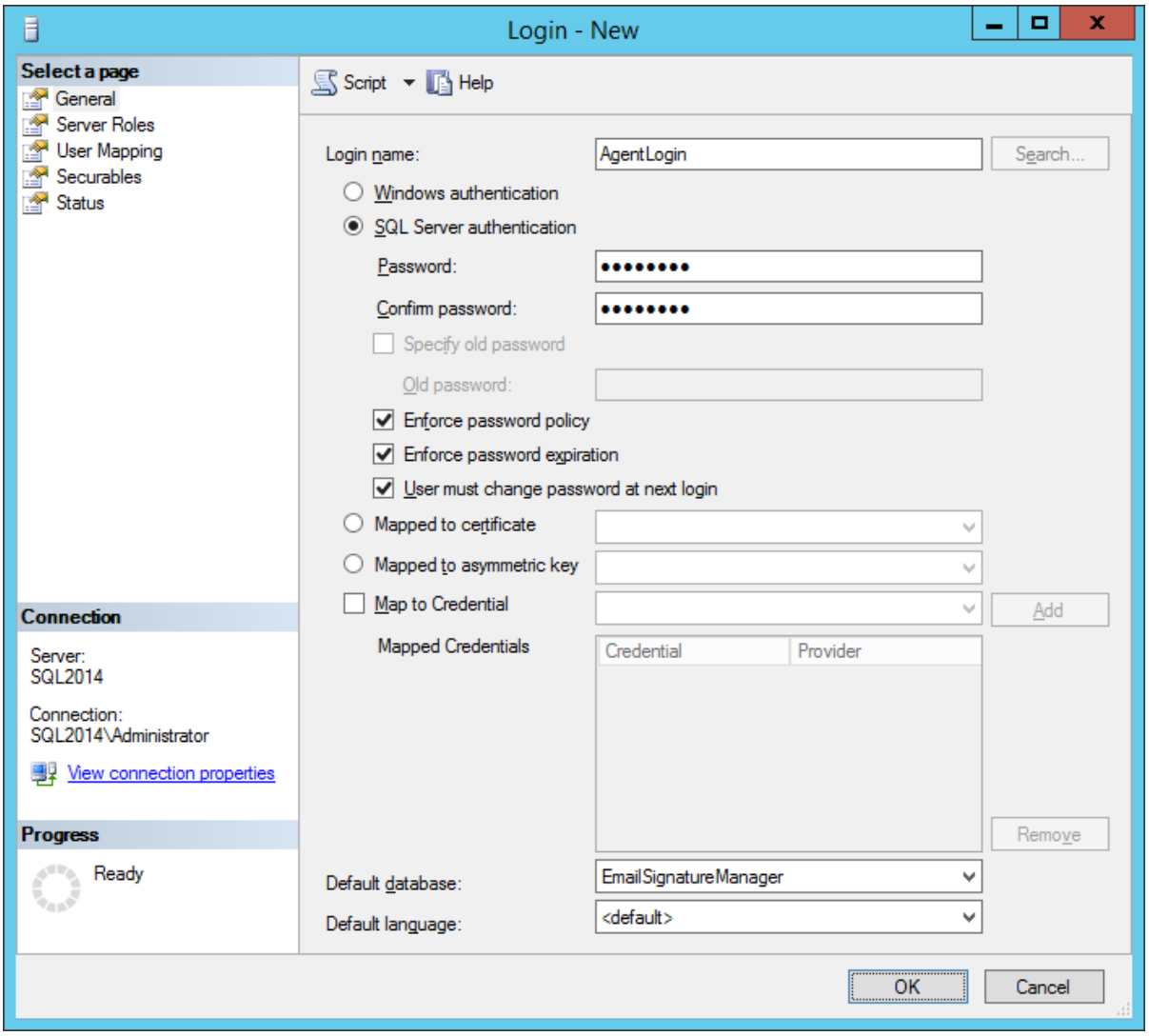
Direct Database Mode and Creating a Login for the Agent

This topic only applies when you use Email Signature Manager in direct database mode.

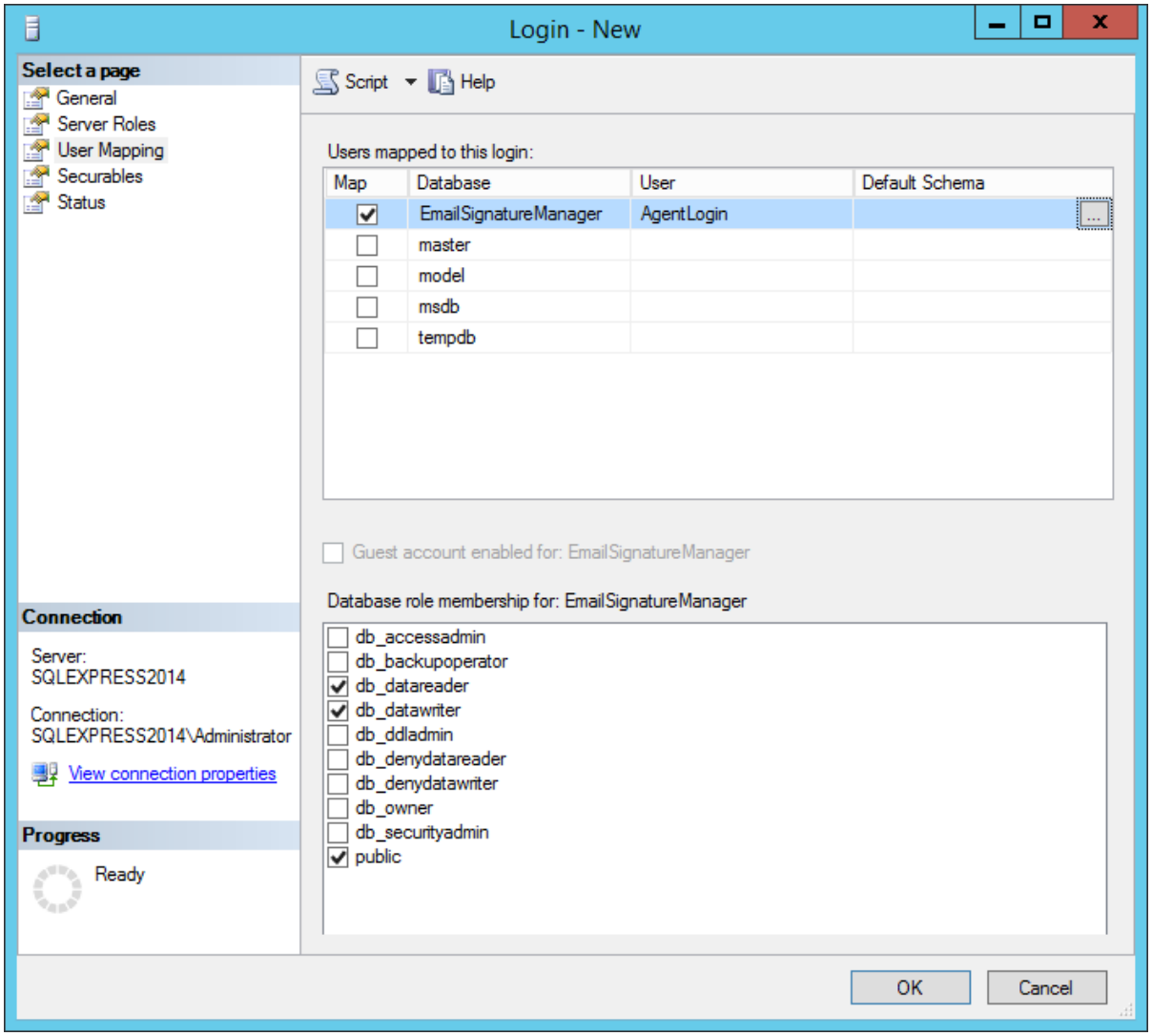
When using Email Signature Manager in direct database mode, the **Email Signature Manager Agent** connects directly to the database. It is recommended to create a specific SQL login for the Agent to use to connect to the database. This login can be created using the following steps:

1. Start **SQL Server Management Studio.** Expand the **Security** node, right-click the **Logins** node and select **New Login...**.

2. On the **General** page, enter a suitable name for the login. Select the **SQL Server Authentication** option and enter an appropriate password. Change the **Default Database** to the Email Signature Manager database. The configuration of the login should look similar to this:



3. On the **User Mapping** page, check the **Map** column for the Email Signature Manager database and then check the **db_datareader** and **db_datawriter** roles:



4. Click the **OK** button to save the login.

The login can now be used by the Agent to connect to the database when using Email Signature Manager in direct database mode.

Template Fields

The below template fields are the standard template fields in Email Signature Manager.

Note The topic dynamic fields explains how to use any Active Directory property in templates and conditional statements are also supported.

Field Name	Description
{FIRSTNAME}	Replaced by the user's first name, as defined by the "givenName" property in Active Directory.

{LASTNAME}	Replaced by the user's last name, as defined by the "sn" property in Active Directory.
{FULLNAME}	Replaced by the user's full name, as defined by the "displayName" property in Active Directory.
{INITIALS}	Replaced by the user's initials, as defined by the "initials" property in Active Directory.
{COMPANY}	Replaced by the user's company, as defined by the "company" property in Active Directory.
{DESCRIPTION}	Replaced by the user's description, as defined by the "description" property in Active Directory.
{TITLE}	Replaced by the user's (job) title, as defined by the "title" property in Active Directory.
{OFFICE}	Replaced by the user's office, as defined by the "physicalDeliveryOfficeName" property in Active Directory.
{DEPARTMENT}	Replaced by the user's department, as defined by the "department" property in Active Directory.
{PHONE}	Replaced by the user's (primary) telephone number, as defined by the "telephoneNumber" property in Active Directory.
{HOMEPHONE}	Replaced by the user's home telephone number, as defined by the "homePhone" property in Active Directory.
{MOBILE}	Replaced by the user's mobile telephone number, as defined by the "mobile" property in Active Directory.
{PAGER}	Replaced by the user's pager number, as defined by the "pager" property in Active Directory.
{FAX}	Replaced by the user's fax number, as defined by the "facsimileTelephoneNumber" property in Active Directory.
{IPPHONE}	Replaced by the user's IP phone details, as defined by the "ipPhone" property in Active Directory.
{STREET}	Replaced by the user's street, as defined by the "streetAddress" property in Active Directory (not to be confused with the "street" property, which is a different field).
{POBOX}	Replaced by the user's PO Box, as defined by the "postOfficeBox" property in Active Directory.
{CITY}	Replaced by the user's city, as defined by the "l" (short for locality) property in Active Directory.
{STATE} -or- {PROVINCE} -or- {COUNTY}	Replaced by the user's state, as defined by the "st" property in Active Directory.
{ZIPCODE} -or- {POSTALCODE}	Replaced by the user's zip (postal) code, as defined by the "postalCode" property in Active Directory.
{COUNTRY}	Replaced by the user's country, as defined by the "co" property in Active Directory.

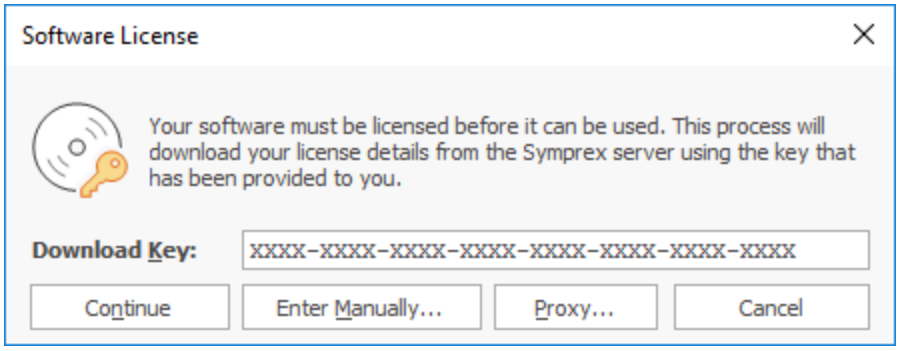
{COUNTRYCODE}	Replaced by the user's country code, as defined by the "c" property in Active Directory.
{EMAIL}	Replaced by the user's email address, as defined by the "mail" property in Active Directory.
{HOMEPAGE}	Replaced by the user's home page, as defined by the "wWWHomePage" property in Active Directory.
{MANAGER}	Replaced by the full name of the user's manager, as defined by the "manager" property in Active Directory.
{EXTATTRIB1} -to- {EXTATTRIB15}	Replaced by the user-defined extension attributes configured through Exchange Server, as defined in the "extensionAttribute1" through "extensionAttribute15" properties in the Active Directory.

Licensing 5

This section of the help file describes how Email Signature Manager is licensed using either a download key or a license supplied separately.

License Dialog

The License dialog is accessed by selecting the **Configuration** tab in the main application window, selecting the **Tools** page, and clicking the **License my software** link (if the application has not previously been licensed) or **Change the license for my software** link (if the application has been licensed):



When you purchased the license for your software, you should have been provided with a unique download key. Enter this key into the **Download Key** textbox and click the **Continue** button. The software will then connect to the Symprex licensing server to download and install your license.

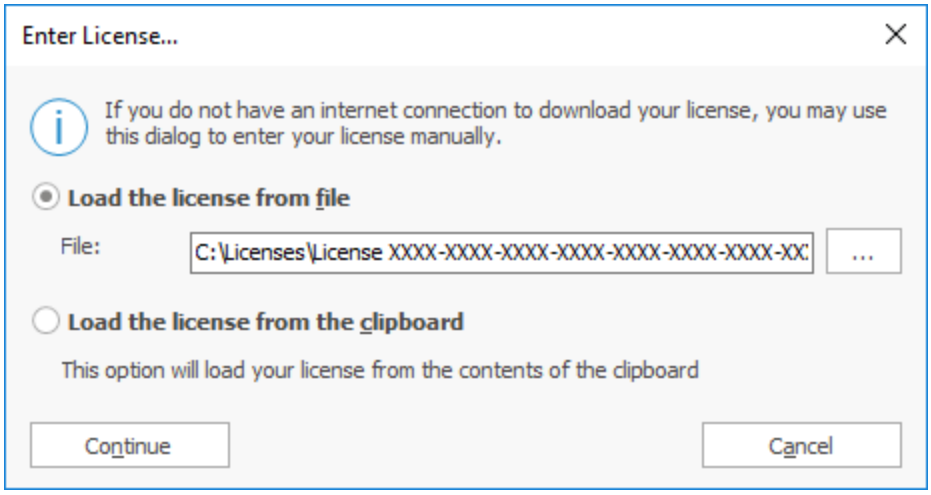
If the computer you wish to license does not have an Internet connection, you may be provided with a file containing you license information. To license your software using such a file, click the **Enter Manually...** button to open the Manual License dialog.

In some organisations, the computer you wish to license may connect to the Internet through a proxy server that requires authentication. If this is the case, click the **Proxy...** button to open the Proxy Details dialog.

If you experience any problems in licensing your software, please contact Symprex or your reseller for assistance.

Manual License Dialog

If necessary, the license for your software can be entered manually by clicking the **Enter Manually...** button on the License dialog:

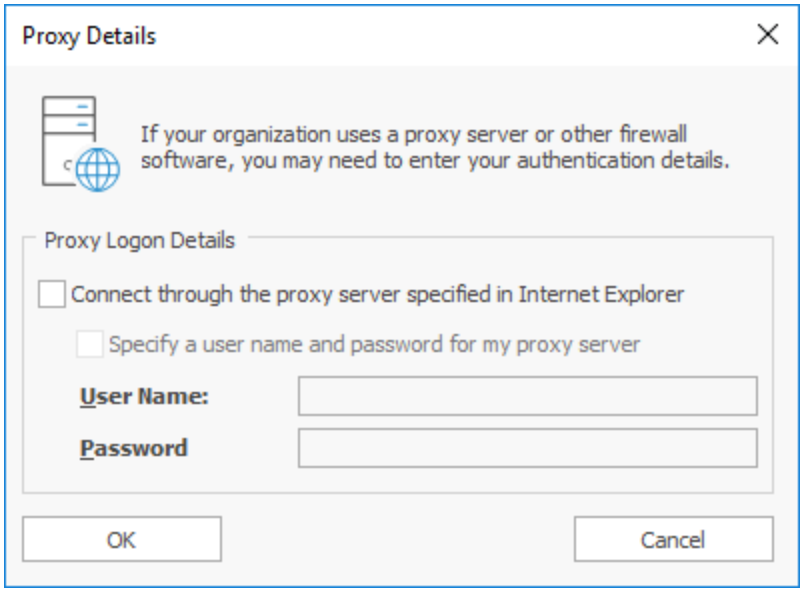


- If you have been provided with a file containing your license, select **Load the license from file** and locate the appropriate file.
- If you have been provided with a text-based version of your license (for example, in an e-mail), copy the text into the clipboard.

When ready, click the **Continue** button. If the selected file is valid or there is valid data in the clipboard, your license will be installed. Otherwise, please contact Symprex or your reseller for assistance.

Proxy Details Dialog

If necessary, the details of your default proxy server (as configured using Microsoft Internet Explorer) for connecting to the Internet can be entered manually by clicking the **Proxy...** button on the License dialog and the Upgrade License dialog:

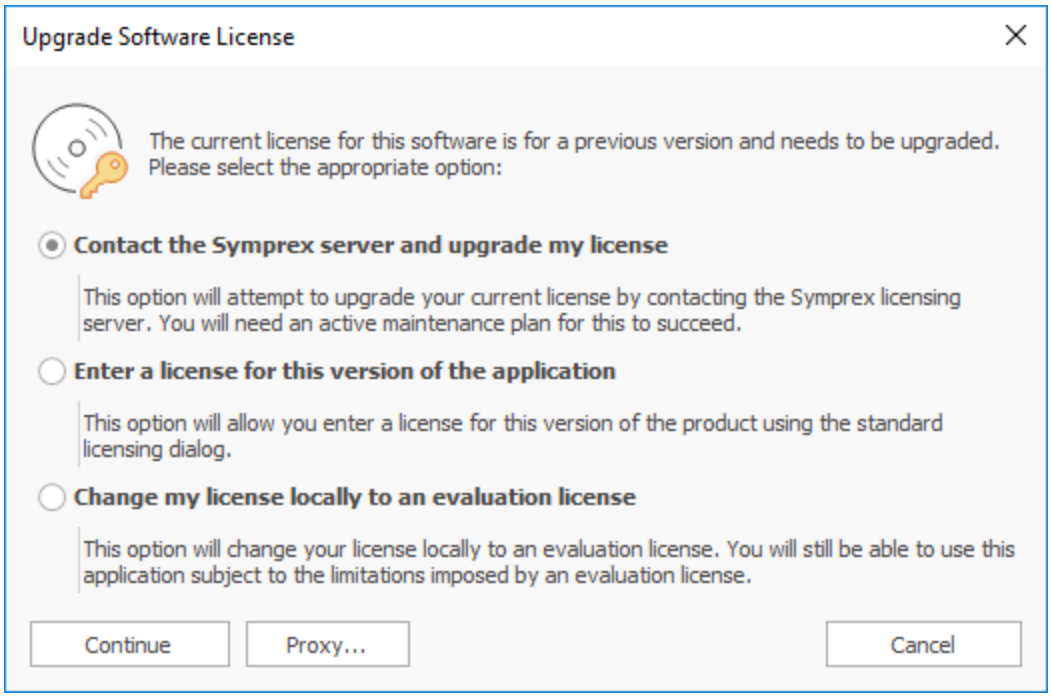


To connect through your default proxy server using your Windows logon credentials, check the **Connect through the proxy server specified in Internet Explorer** checkbox. If you need to specify your authentication details, check the **Specify a user name and password for my proxy server** checkbox, and then enter the appropriate details in the **User Name** and **Password** boxes. When ready, click the **OK** button to accept the changes or click the **Cancel** button to close the dialog without saving any changes.

Note The details you enter will be stored in the registry of your computer and will be re-used amongst all Symprex products.

Upgrade License Dialog

The Upgrade License dialog is displayed automatically when Email Signature Manager detects that it is using a license from a previous version:



There are three options available:

- **Contact the Symprex server and upgrade my license**: When you select this option, Email Signature Manager will contact the Symprex licensing server and attempt to upgrade your existing license to the current version. In order for this to succeed, there must be an active maintenance plan for the license that is currently in use. If the maintenance plan has expired, you will need to contact Symprex or your reseller to restart maintenance and obtain an upgraded license. In some organisations, the computer you wish to license may connect to the Internet through a proxy server that requires authentication. If this is the case, click the **Proxy...** button to open the Proxy Details dialog.

- **Enter a license for this version of the application**: Choose this option if you have already been supplied with the download key or license file for your the current version; this will open the License

dialog and allow you to enter the details of your license.

- **Change my license locally to an evaluation license**: This option will change the existing license to an evaluation license for the current version, which means that you can continue using Email Signature Manager but subject to the evaluation restrictions imposed.

When you have selected the appropriate option, click the **Continue** button. Alternatively, if you do not wish to modify the license (for example, because you wish to reinstall the previous version to continue using your existing license), click the **Cancel** button.

Copyright

6

Published: October 2021
Applies To: Symprex Email Signature Manager 9.0.1

Contacting Symprex

7

There are several ways to contact Symprex.

Visit Our Web Site

Our web site provides general information about Symprex and our products:
https://www.symprex.com

If you experience technical problems with one of our products, please visit our support page:
https://www.symprex.com/support

Contact Us by Email

Please email sales enquiries and general enquiries about Symprex or our products to:
sales@symprex.com

Please email support enquiries to:
support@symprex.com

Contact Your Local Partner or Reseller

Symprex has partners and resellers in most countries. You can find your local reseller here:
https://www.symprex.com/partners/resellers