Symprex Email Signature Manager

User's Guide

Version 6.1.0.

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.
- No software required to install on Exchange server or workstations.
- Emails are not intercepted, re-routed or interfered with 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, Blackberry, 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 or Active Directory.
- 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, how to install the software, and how to get started using the software, which will show you how to deploy your first signature in minutes.

About Symprex

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

Introduction   1

System Requirements

Symprex Email Signature Manager minimum system requirements are:

- Supported email clients:
  Android, iPhone, iPad and Windows Mobile
  Blackberry
  Microsoft Office 365
  Microsoft Office 365 Outlook Web App
  Microsoft Outlook 2003 SP2
  Microsoft Outlook 2007 SP2
  Microsoft Outlook 2010
  Microsoft Outlook 2013
  Microsoft Outlook Web Access 2003
  Microsoft Outlook Web Access 2007
  Microsoft Outlook Web App 2010
  Microsoft Outlook Web App 2013

- Operating system software:
  Microsoft Windows XP SP3 (x86 only)
  Microsoft Windows Vista SP2
  Microsoft Windows 7
  Microsoft Windows 8
  Microsoft Windows 8.1
  Microsoft Windows Server 2003 SP2
  Microsoft Windows Server 2003 R2 SP2
  Microsoft Windows Server 2008
  Microsoft Windows Server 2008 R2
  Microsoft Windows Server 2012
  Microsoft Windows Server 2012 R2
  Microsoft Windows Small Business Server 2008
  Microsoft Windows Small Business Server 2011

- Framework software:
  For the Management software and Deployment Service:
      .NET Framework 3.5 SP1
      .NET Framework 4.0
      .NET Framework 4.5

  For the Deployment Utility (`sign.exe`):
      .NET Framework 2.0
      .NET Framework 3.5 SP1
      .NET Framework 4.0
      .NET Framework 4.5

- System hardware:
  CPU and memory requirements for operating system

Introduction 1

60 MB free hard-disk space
1024 x 768 screen resolution

Installing Email Signature Manager

Symprex Email Signature Manager is designed to be very easy to install. Simply run the setup program and follow the instructions given. If you have a previous version installed, please review the section on [upgrading](#).

To test signatures directly in Outlook and OWA, it is recommended that the following software is also installed locally on the machine where Email Signature Manager is installed and used:

- Microsoft Office 2003, 2007, 2010 or 2013
- Internet Explorer with access to OWA

Note that Email Signature Manager offers exact previews of signatures within the application itself without Outlook or OWA using the [Test Signatures dialog](#).

Upgrading Email Signature Manager

If you have a previous version of Email Signature Manager installed on your system, the following instructions should be followed to upgrade it.

Upgrading Version 5.x and Later

If you are using version 5.x or later, the installers for Email Signature Manager, the Deployment Service and the Transport Agent will automatically upgrade your existing installation. After installation, you should complete the steps in the **Common Upgrade Tasks** set out below.

Note If you are using the Email Signature Manager Transport Agent, the previous v5.x installers for 2007/10 and 2013 have been unified into a single installer that supports all Exchange Server versions. This new installer will upgrade all previous v5.x versions.

Upgrading Version 4.x and Earlier

If you are using version 4.x or earlier, you should upgrade following these steps:

1. Start your current version and determine the database you are using.

   ➔ When using the Email Signature Manager database, `settings.mdb`, the database should be located in a shared folder (e.g. `\\SERVER\SIGNMGR$\\settings.mdb`). If the database you are using is located on the local computer and shared from the installation folder, it is strongly recommended that it is moved to a separate [shared folder](#). It is recommended to **make a backup** of your existing `settings.mdb` database before the upgrade is performed.

   ➔ When using Microsoft SQL Server for the database, it is recommended to **make a backup** of the database before the upgrade is performed.

2. Uninstall the current version using the Windows Control Panel. When prompted, you can elect to keep or remove the current database and settings. If you keep the current database and settings, this does *not* interfere with installing version 5.x or later.

3. Install the new version of Email Signature Manager and then complete the steps in the **Common Upgrade Tasks** set out below.

Note The default installation location for version 4.x and earlier was `C:\Program Files\Symprex\Mail Signature Manager`. In version 5.x it is `C:\Program Files\Symprex\Email Signature Manager`.

Common Upgrade Tasks

Once installation of the new version is complete, start the Email Signature Manager application. If you have upgraded from version 4.x or earlier, you will need to select your previous settings database; refer to the Settings Database dialog. When the settings database is opened for the first time, it will be automatically upgraded to the new version.

Finally, the deployment command line tool, `sign.exe`, needs to be updated depending on how deployment is implemented in your organization.

- If you are using a logon script, the tools located in the shared folder can simply be overwritten with the new version; refer to the section on creating the shared folder for more details.
- If you are deploying using the MSI package via group policy, it will be necessary to update the existing policy to uninstall the original version and to install the new version; refer to the section on deployment via group policy for further details.

Note Version 5.x accepts the same command line arguments as previous versions, except the verbose argument has been replaced with the showwindow argument; refer to the section on command line arguments. Hence, there is no generally need to change any scripts to use new parameters.

Introduction 1

Email Signature Manager Overview

The Symprex Email Signature Manager main application window is illustrated below:
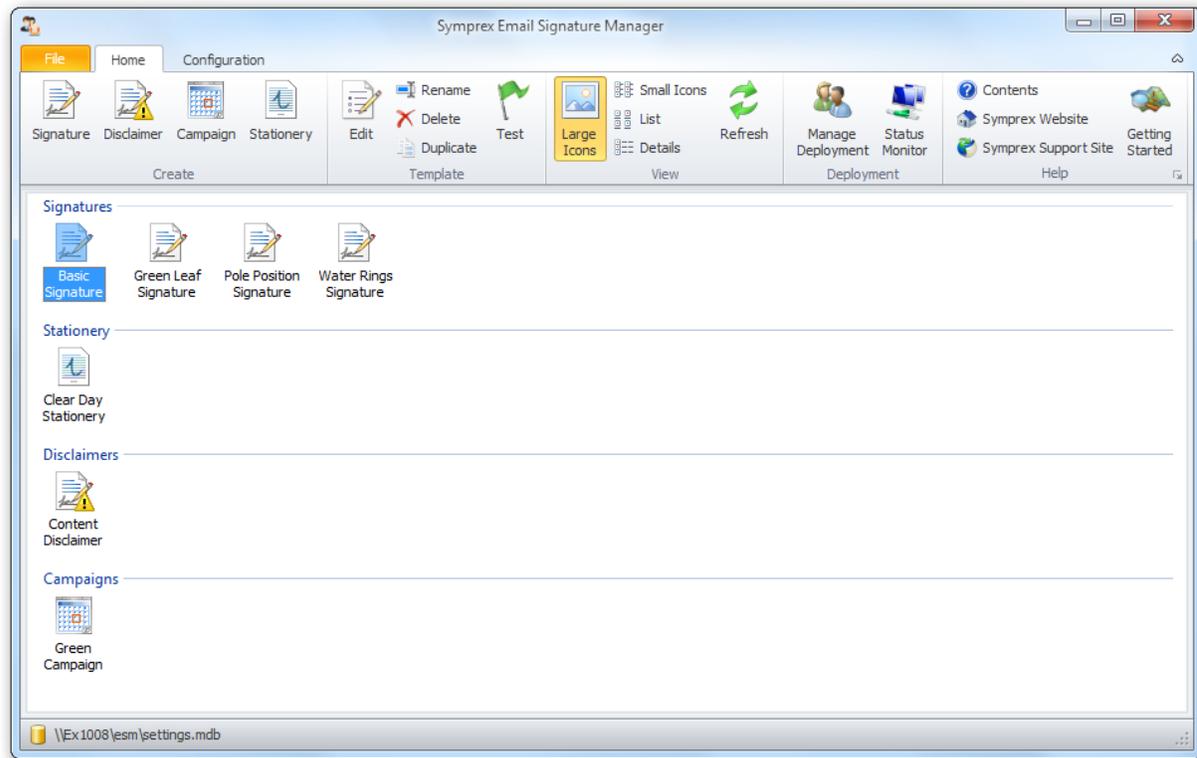
Email Signature Manager is designed in accordance with the current guidelines for Windows applications. The application window is divided into the top ribbon for accessing all of the commands, a work area in the middle, which used to manage and edit templates, and a status bar at the bottom. The basic elements in the user interface work in the same way as in most other Windows applications.

One Single Administration Module

One of the great advantages of Email Signature Manager is that all aspects of the product are managed from within the graphical user interface of the main application. This is where you for example create, design and test your signature templates, define data sources, manage deployment to groups and users, and verify deployment statuses in the status monitor.

Another advantage is that you do not have to install any software on your Exchange Server or workstations for Email Signature Manager to work. Deployment is seamlessly performed with a small command-line utility that is run as part of each user's logon script, or via Active Directory Group Policy (MSI). This means the solution is simple and without risk to Exchange Server stability or performance. For organizations with users who do not log on to the domain, a service is available, which can deploy signatures to OWA and mobile devices from one central location.

With Email Signature Manager signatures will simply, automatically be available to all your users, and

email settings such as default signatures and default fonts will also automatically be configured.

Powerful Built-in Template Editor

Email Signature Manager offers a powerful built-in template editor that is available when you edit a template. This is illustrated below:
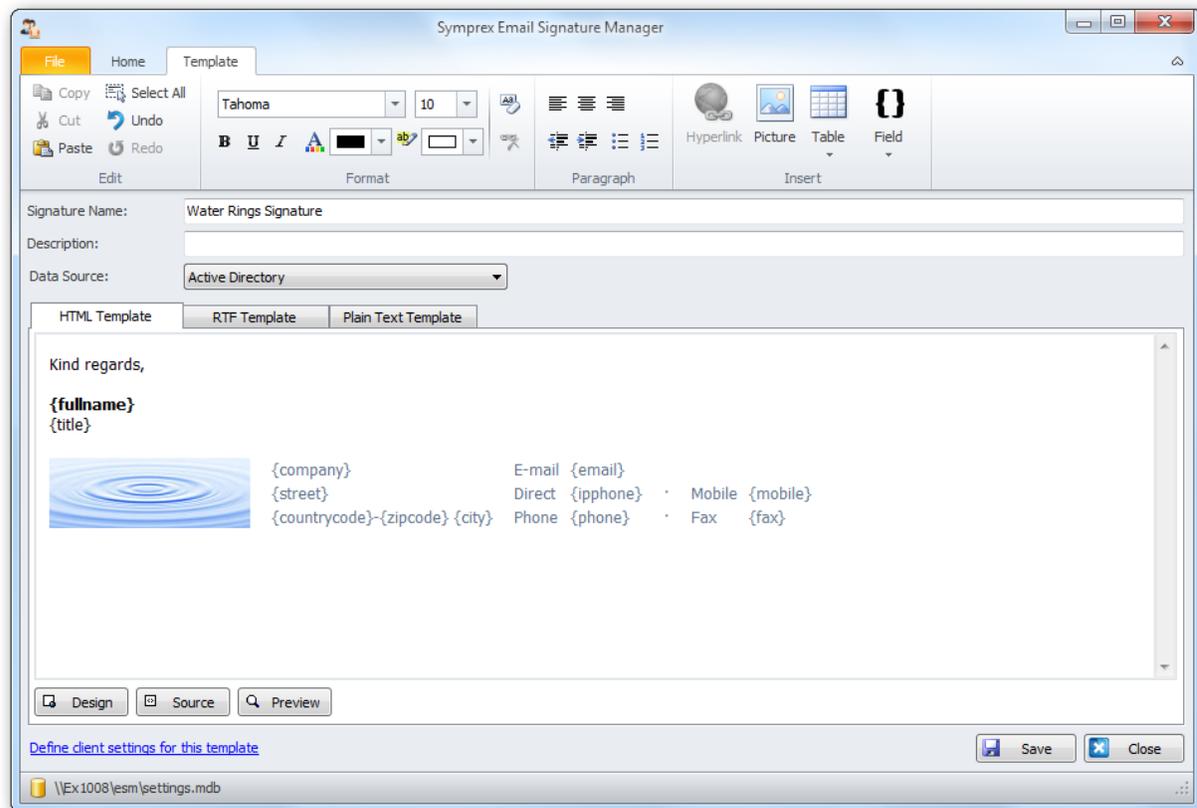
A template consists of the following information:

- Basic properties, such as name, description and default data source
- HTML, RTF and Plain Text templates with dynamic fields
- Optional client settings, such as default fonts and other settings

The dynamic fields in templates are replaced with real data when signatures are deployed.

HTML Template

When designing HTML templates, you can work in WYSIWYG design mode and in syntax color-coded source mode, and switch to preview in preview mode. The syntax color-coded source mode is illustrated below:

Introduction
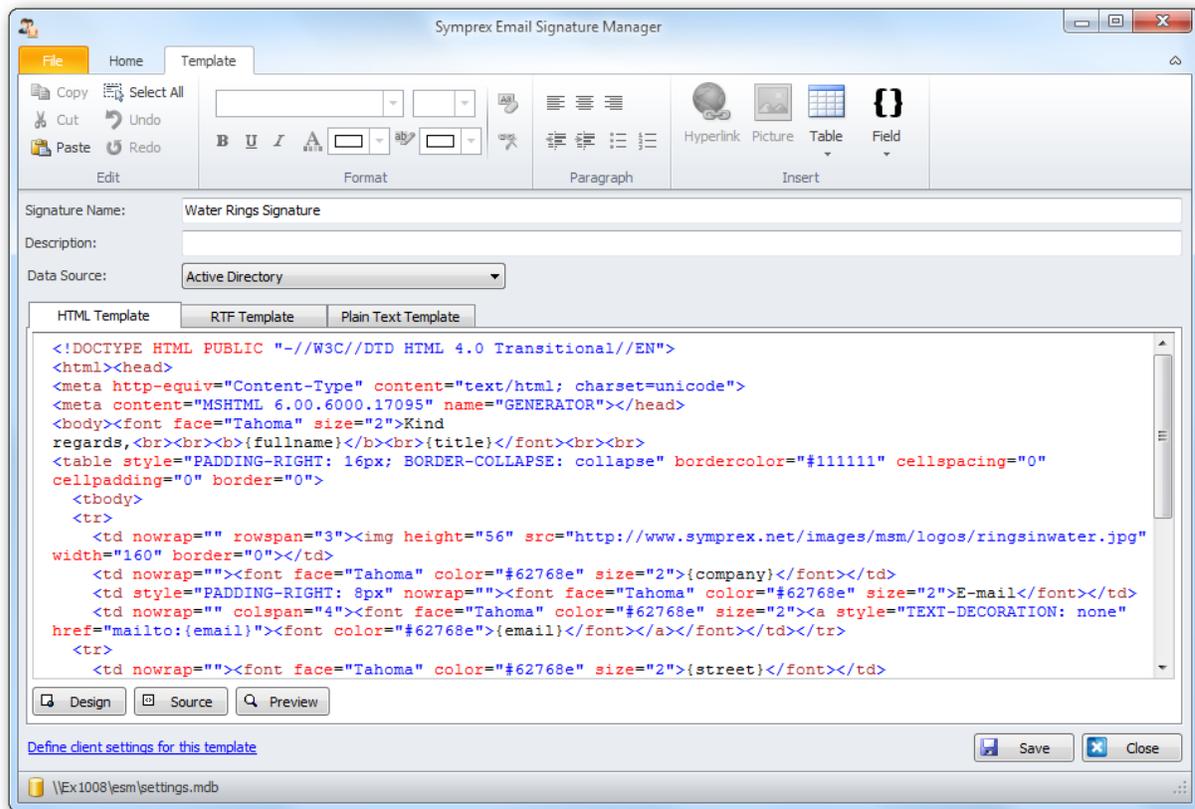
You can copy/paste between the HTML editor in Email Signature Manager and an external HTML editor if you prefer to design the templates in an external editor, such as Microsoft FrontPage or Microsoft Expression Web.

RTF and Plain Text Templates

Rich Text Format (RTF) and Plain Text templates are designed in WYSIWYG mode. You can copy/paste between the editors in Email Signature Manager and external editors if you prefer to design these types of templates in another editor.

Client Settings

A signature can optionally include a set of client settings. The client settings that can be configured are illustrated below:
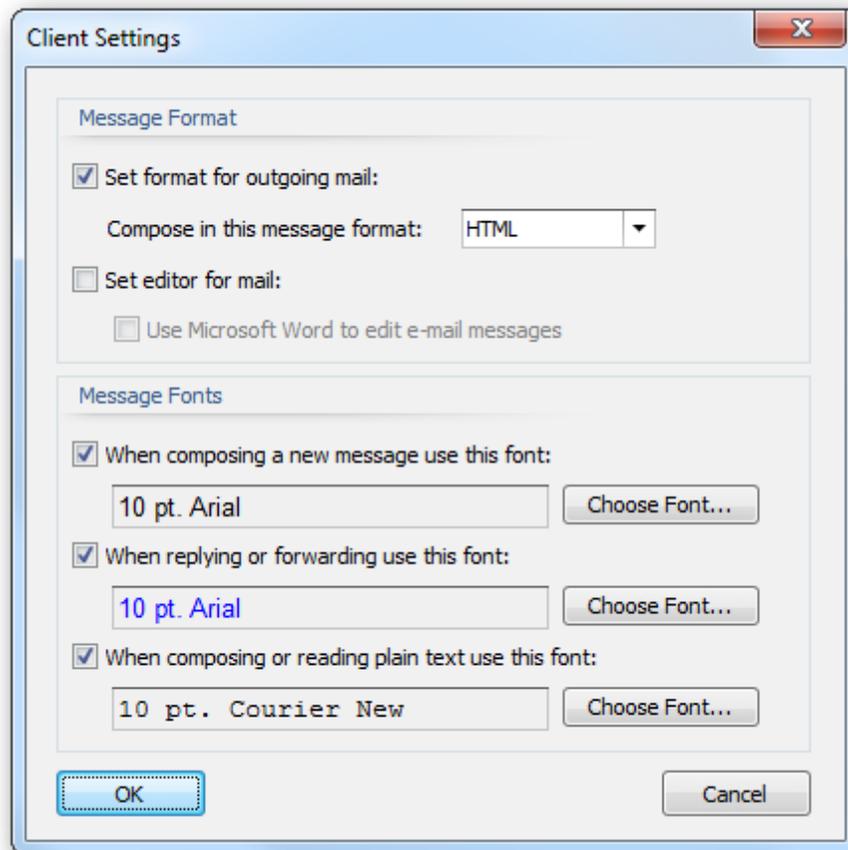
Client Settings can also be defined on a global level so that they are applied automatically when any signature is installed.

Getting Started

The Getting Started dialog is appears automatically when Symprex Email Signature Manager is started, or it can be opened by clicking the **Getting Started** button in the **Help** group of the **Home** ribbon on the main application window. The steps listed guide you through the required configuration to deploy signatures to your users for the first time.

Note These steps assume that you wish to use the built-in database and deployment using a logon script. There are a number of alternatives; please refer to the chapter on deployment for further details.

Introduction
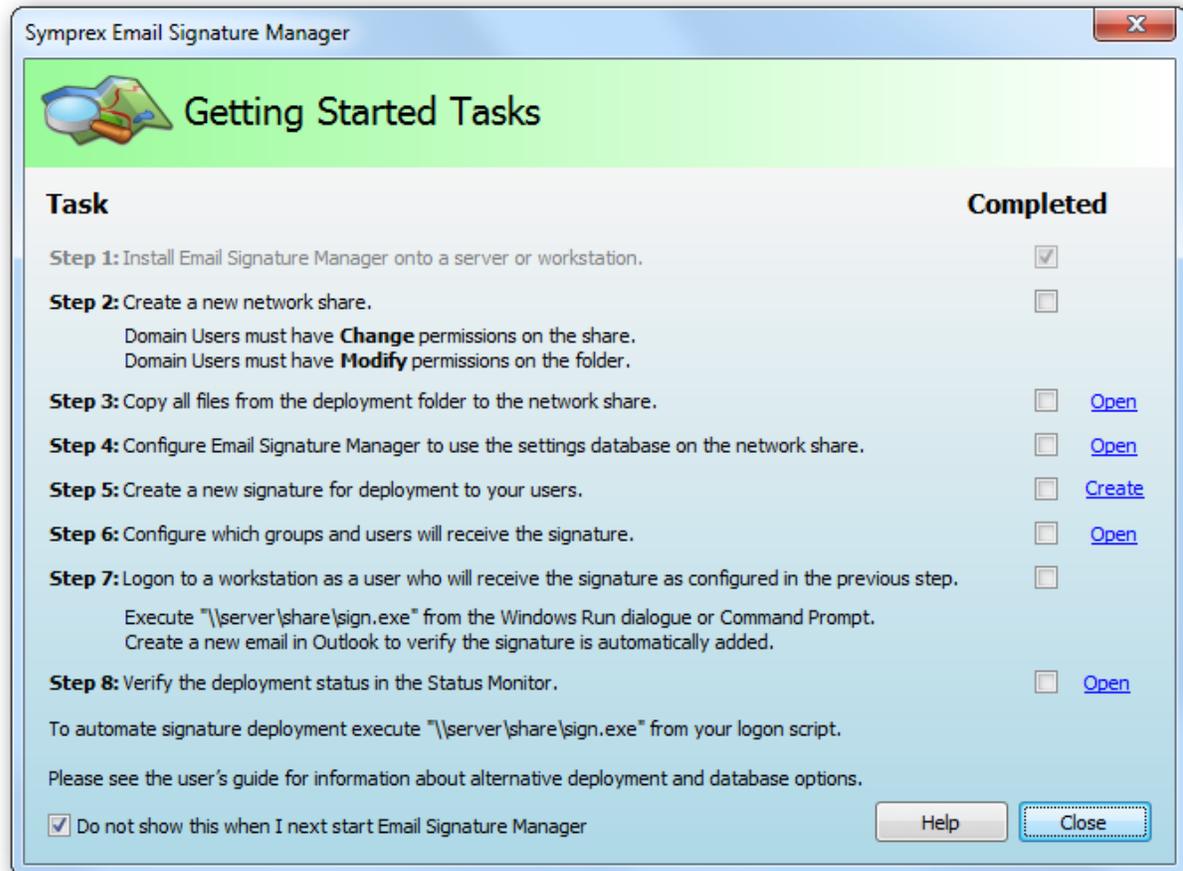
As you complete each step, you can tick the **Completed** checkbox to remind you of the progress you have made. Once you have successfully deployed signatures to your users, you can prevent the dialog from appearing automatically by selecting the **Do not show this when I next start Email Signature Manager** option.

For further details on how to complete each step, please refer to the following sections of this manual:

- **Step 2** and **3**: Creating the Shared Central Folder
- **Step 4**: The Settings Database dialog
- **Step 5**: Creating and Editing Templates
- **Step 6**: The Manage Deployment dialog
- **Step 8**: The Status Monitor dialog

Tutorial

Symprex 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 pu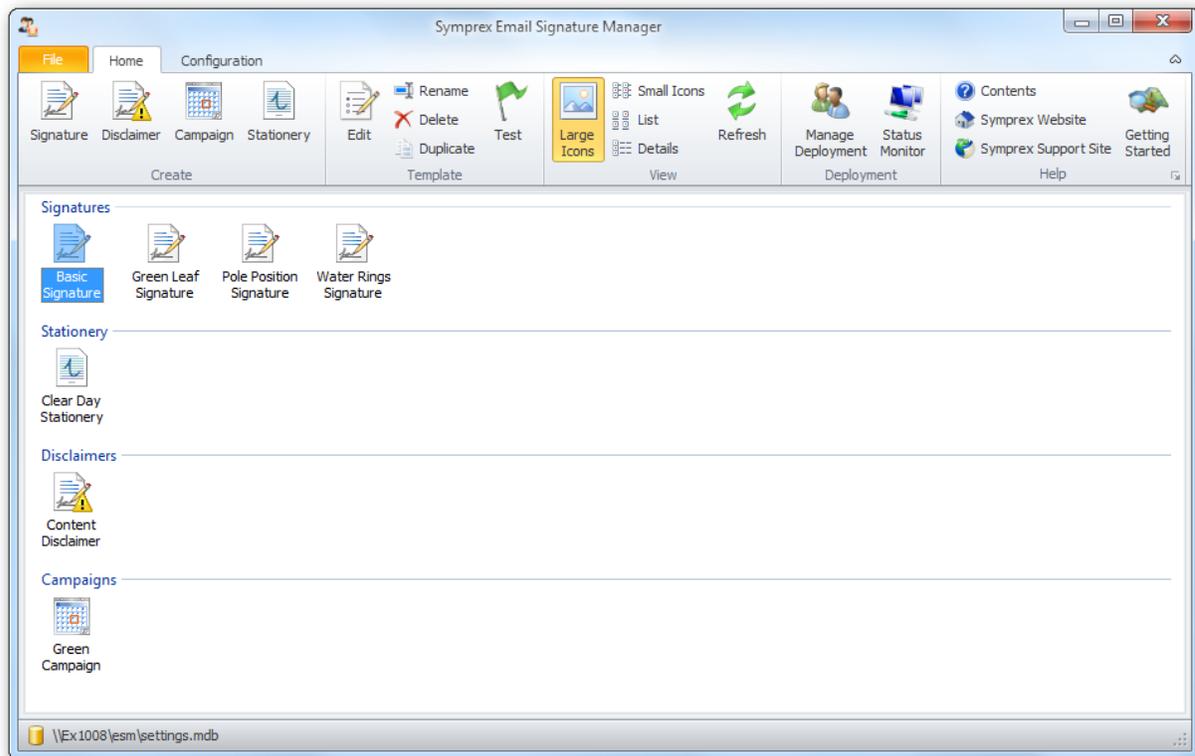rchased an appropriate license, you will need to apply it to fully enable the application and remove the evaluation restrictions; please refer to the chapter on licensing for further information.

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. Further details and options about the application can be found by clicking the File button, which will display the File page.

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, or
- Click the **Rename** button in the **Template** group in the ribbon to rename the selected template, or

Tutorial

2

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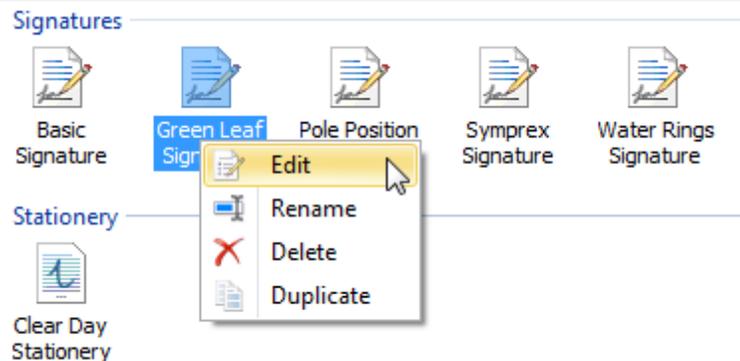
Please see this topic for further information about creating and editing templates. Once you have created your templates, they can be tested by clicking the **Test** button in the **Template** group in the **Home** ribbon to open the Test Signatures dialog.

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.

To change the overall configuration of the application, click the **Configuration** ribbon.

Note When a template is being modified, the Configuration ribbon is not available.

Within the **Settings** group are the following buttons:

- The **Deployment Options** button will open the Deployment Options dialog, which is used to configure system-wide settings for the deployment of signatures to your users.
- The **Office 365 Options** button will open the Office 365 Options dialog, which is used to configure Office 365 signature deployment.

Tutorial

2

- The **Blackberry Options** button will open the <u>Blackberry Options dialog</u>, which is used to configure Blackberry signature deployment.
- The **Configure Service** button will open the <u>Configure Service dialog</u>, which is used to configure and manage the Email Signature Manager Deployment Service.

Within the **Mobile Devices** group are the following buttons:

- The **Transport Agent Rules** button will open the <u>Transport Agent Rules dialog</u>, which is used to configure the rules applied by the Email Signature Manager Transport Agent when processing e-mails.

Within the **Settings Database** group are the following buttons:

- The **Settings Database** button will open the <u>Settings Database dialog</u>, which is used to select the settings database to which the application is connected.
- The **Import Database** button will open the <u>Import Database dialog</u>, which is used to import data from another database in to the current settings database.
- The **Load Connection Settings** button is used to load the settings for connecting to a database from an existing configuration file; please see <u>this topic</u> for further information.
- The **Save Connection Settings** button is used to save the settings for connecting to the current settings database to a configuration file; please see <u>this topic</u> for further information.

Within the **Tools** group are the following buttons:

- The **Define Data Sources** button will open the <u>Manage Data Sources dialog</u>, which is used to configure the custom data sources used to provide data to your templates.
- The **Domain Configuration** button will open the <u>Domain Configuration dialog</u>, which is used to configure how users and groups are found in your local domain.

Tutorial

File Page

The File Page is displayed by the clicking the **File** button in the ribbon of the main application window.
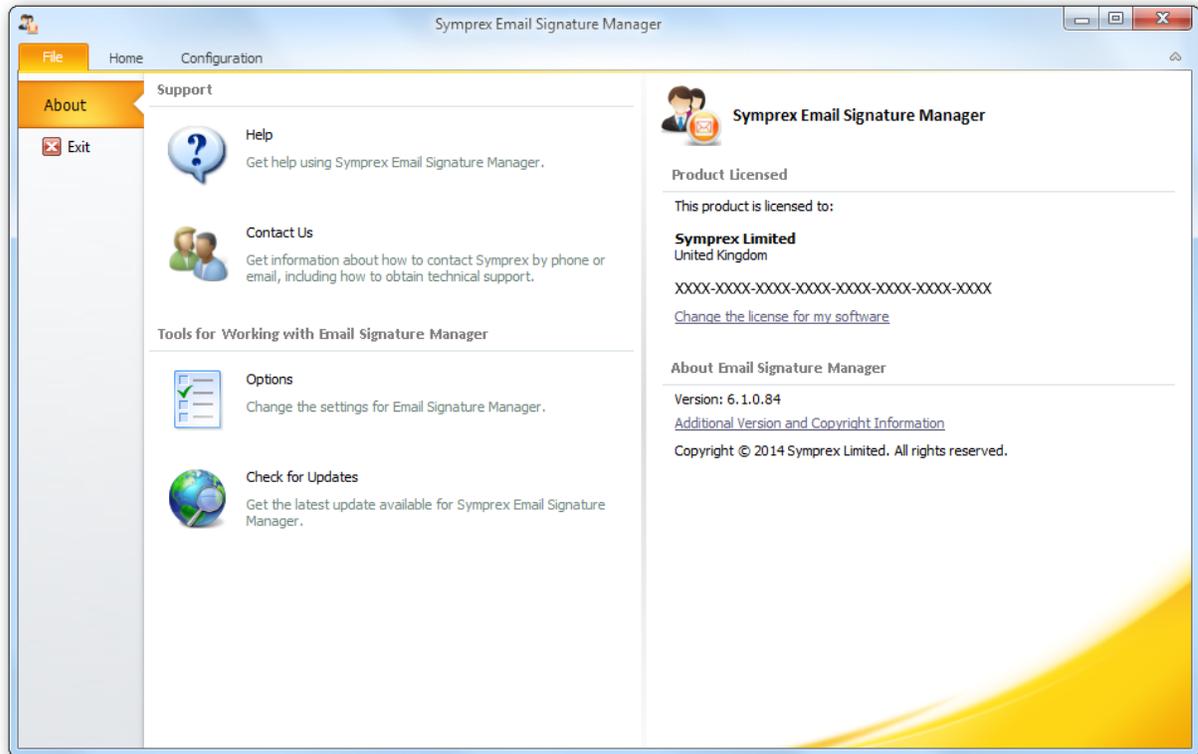
The left side of the window has various options for working with Symprex Email Signature Manager.

Help: Opens the application help on the Introduction page.
Contact Us: Opens the Support Centre on the Symprex website.
Options: Opens the Options dialog to configure application settings.
Check for Updates: Checks for updates to Email Signature Manager

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

Options Dialog

The options dialog is opened by selecting the File page in the main application window and clicking the **Options** button.
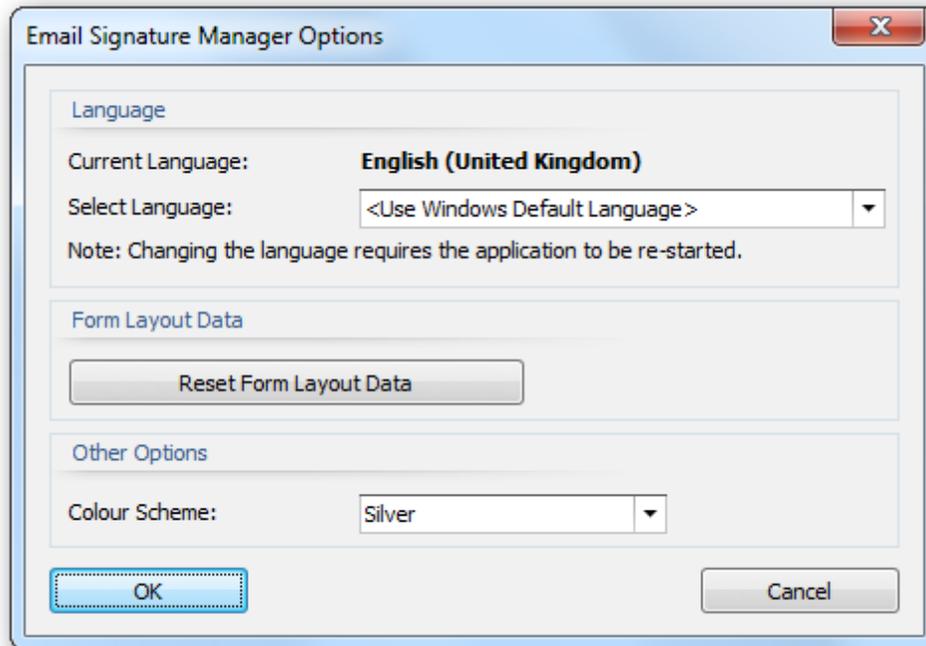
The following settings can be modified:

Language: Allows you to specify the language used by the application. This will default to your current Windows language (if available) or you can choose a specific language from the drop-down list.
Form Layout Data: Clicking the **Reset Form Layout Data** 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.

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. Symprex 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 part of the application window displays the template editor and the **Template** ribbon:
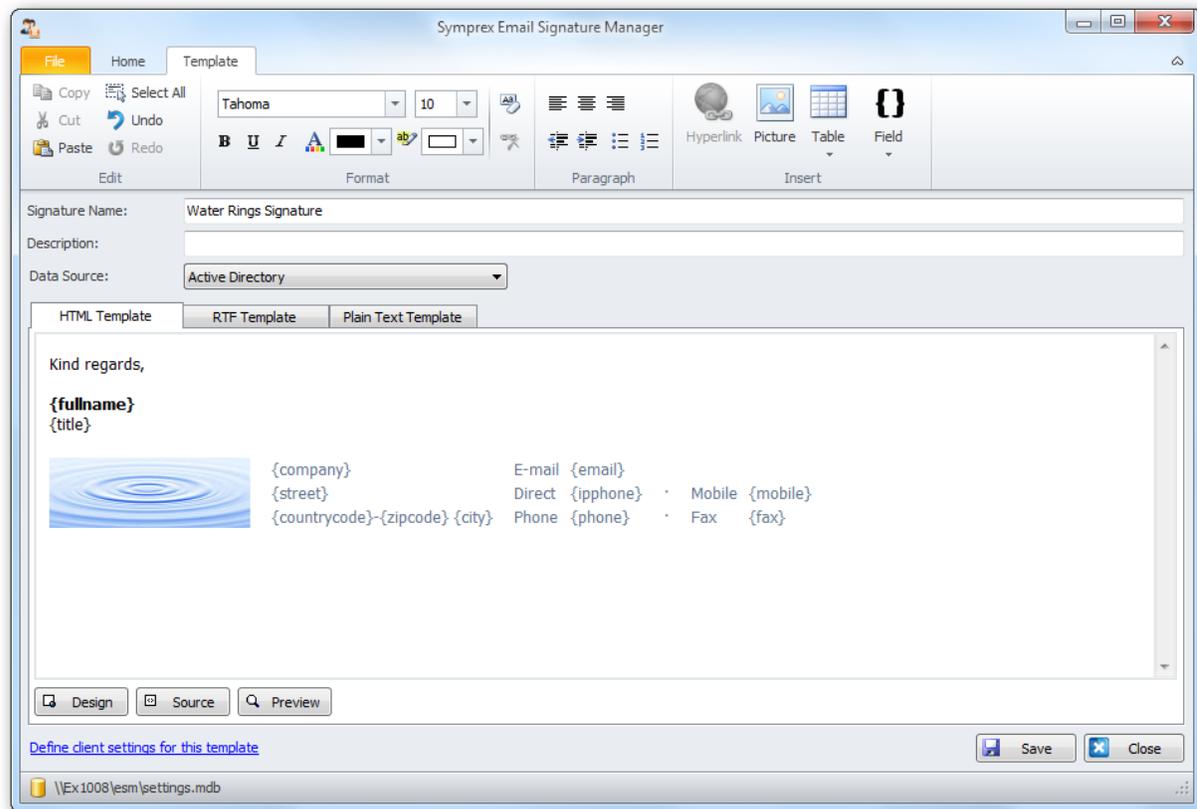
All templates share two common properties:

- The name of the template, used to uniquely identify each template. Template names cannot be blank or duplicated.

- 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 three separate components:

- The **HTML Template**, which defines the content appended to emails authored in HTML, including those authored through OWA.
- The **RTF Template**, which defines the content appended to emails authored in Rich Text Format.
- The **Plain Text Template**, which defines the content appended to emails authored in plain text.

Each component can contain fields (identified by {} braces), which are dynamically replaced by the appropriate information 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.

All templates are designed in a WYSIWYG editor. For the HTML component of each template, the source can be modified directly to provide fine control over the content by clicking the **Source** button:

Tutorial 2
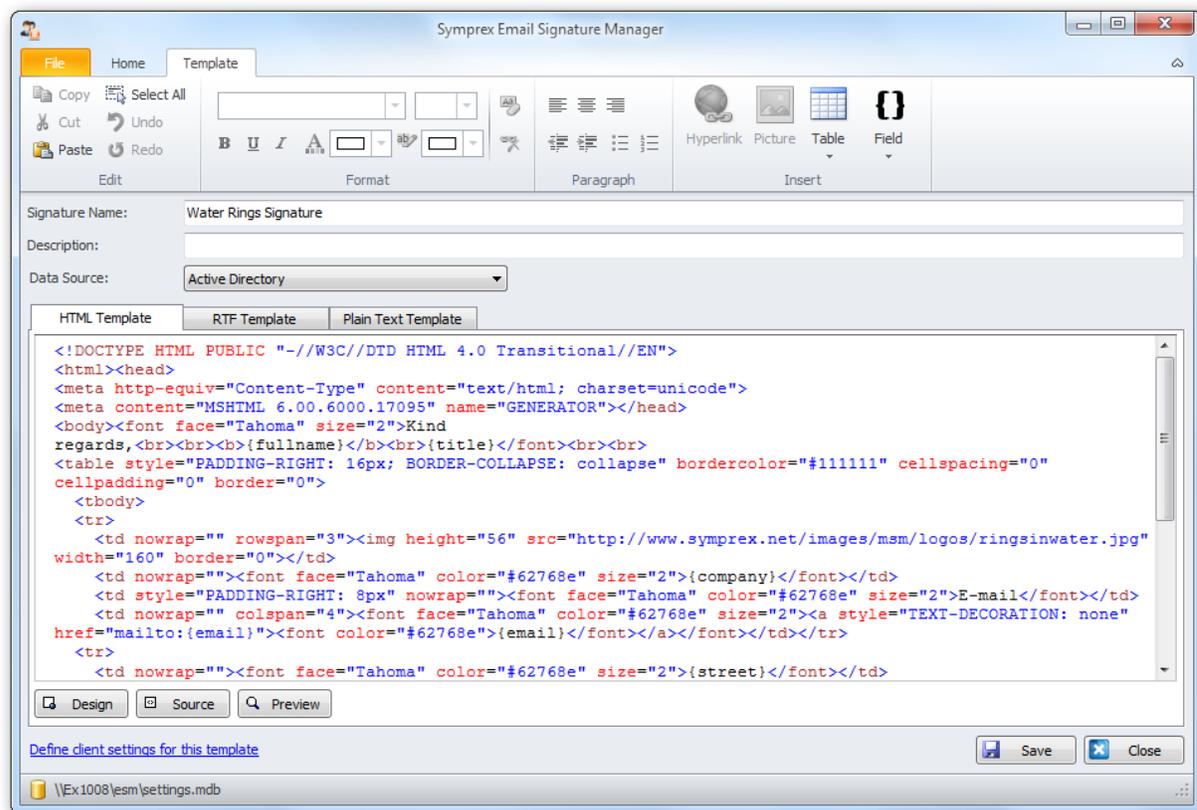
The **Template** ribbon offers various commands whilst designing your templates:

- 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 and RTF templates only).
- The **Paragraph** group contains commands to adjust the style of the text (HTML and RTF templates only).
- The **Insert** group contains commands to insert Hyperlinks, Pictures, Tables and Fields.

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 of 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:
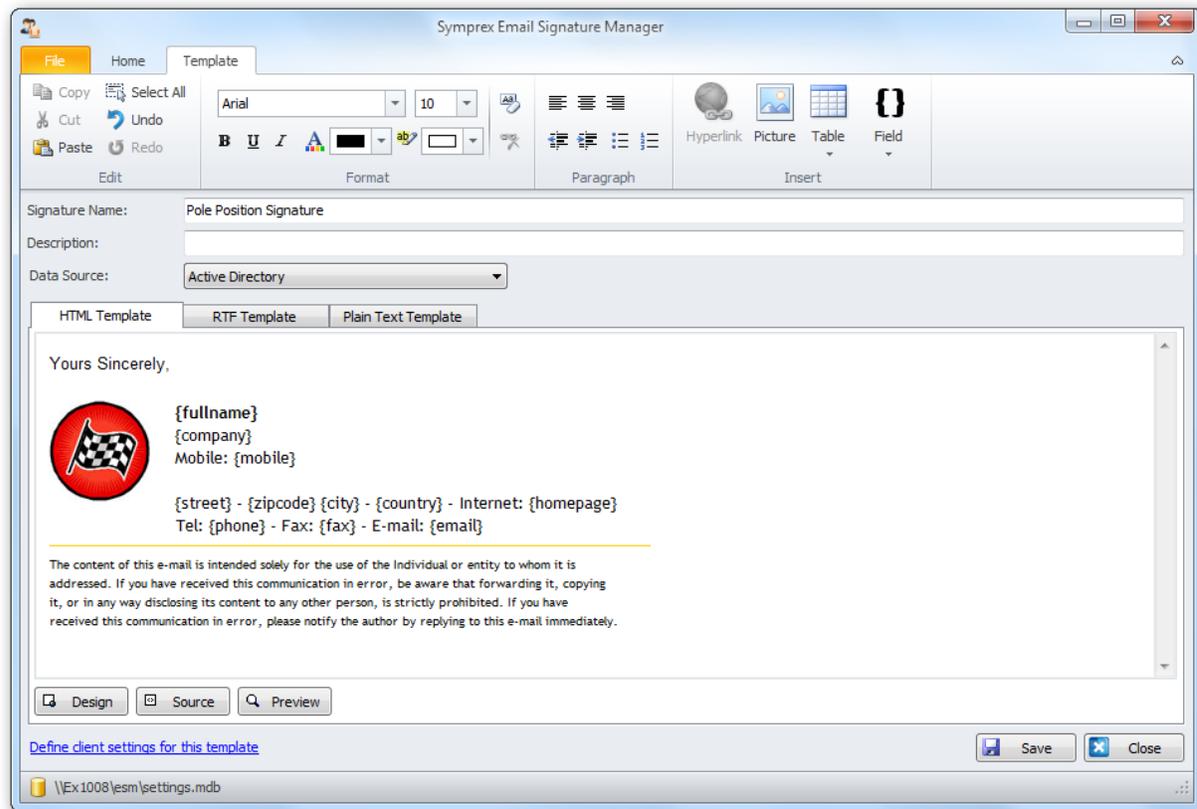
Signatures can have the following properties configured:

- **Name** (mandatory): The unique name of the signature.
- **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.
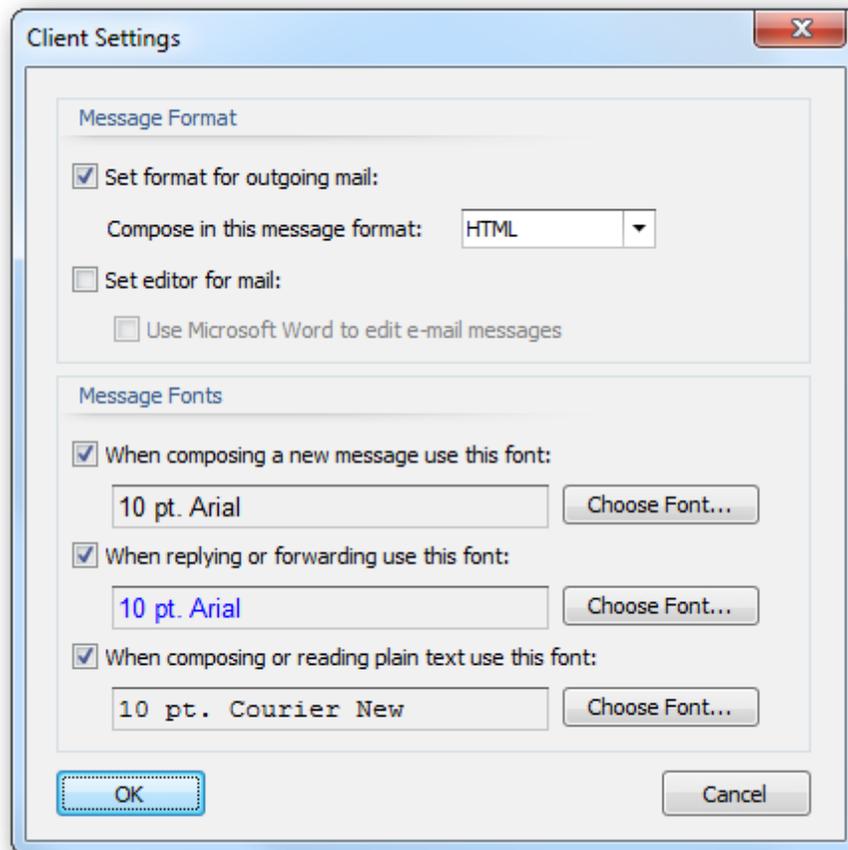
Client settings are used to configure email preferences for writing emails in Microsoft Outlook.

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.
- **Set editor for mail**: Determines if Microsoft Word is used to edit email messages.

Note The "Send Pictures" option is now configured through the Deployment Options dialog.

Note The "Editor for mail" option only has effect in Microsoft Outlook 2003; in Outlook 2007 and later, Word is always used for editing emails.

The following settings can be configured for the message font:

- The Compose font; specifies the font and color that will be used when a user creates a new email.
- The Reply/Forward font; specifies the font and color that will be used when a user replies to 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 of 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:
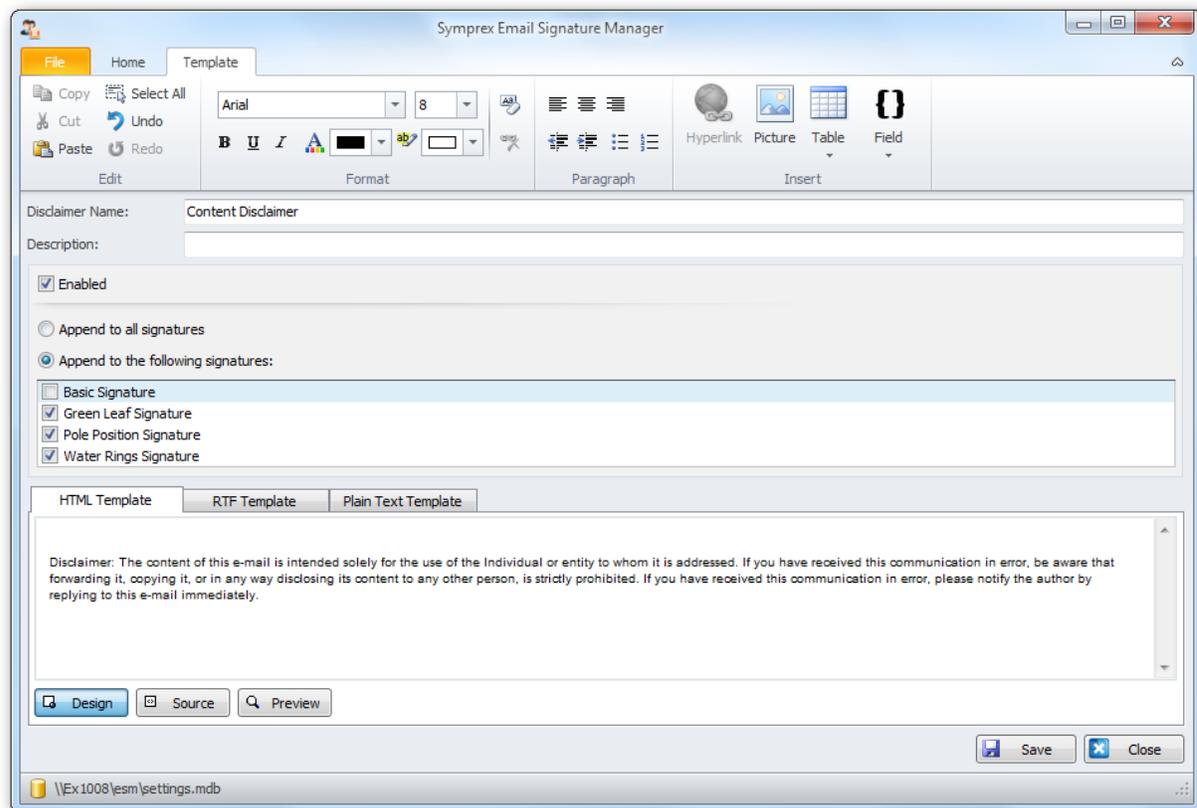
Disclaimers can have the following properties configured:

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

- **Enabled**: Determines if the disclaimer is currently enabled. When enabled, the disclaimer is 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.

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 of 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:
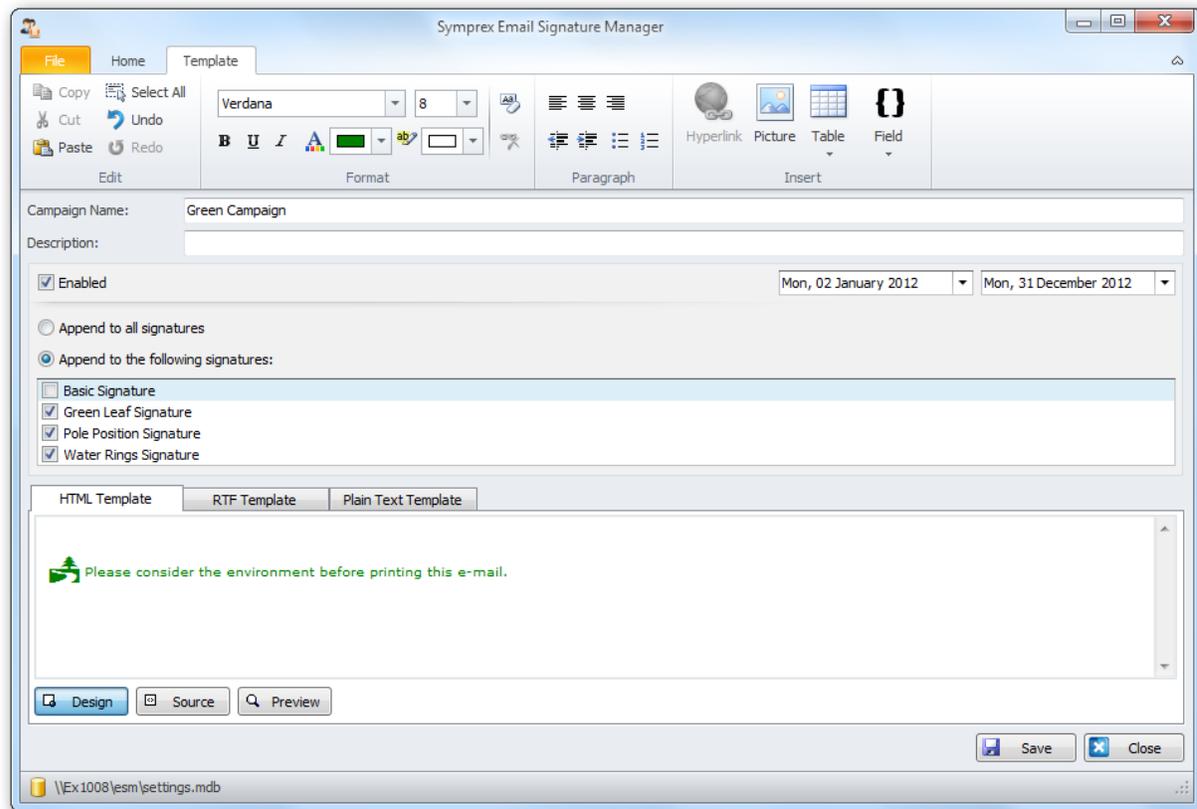
Campaigns can have the following properties configured:

- **Name** (mandatory): The unique name of the campaign.
- **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.

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.

Tutorial 2

Stationery

Stationery can be used to set background images.

To create new stationery, click the **Stationery** button in the **Create** group of 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** (mandatory): The unique name of the stationery.
- **Description**: A description of the stationery.

Note Stationery can only be applied to HTML messages authored in Microsoft Outlook. Hence, the RTF Template and 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
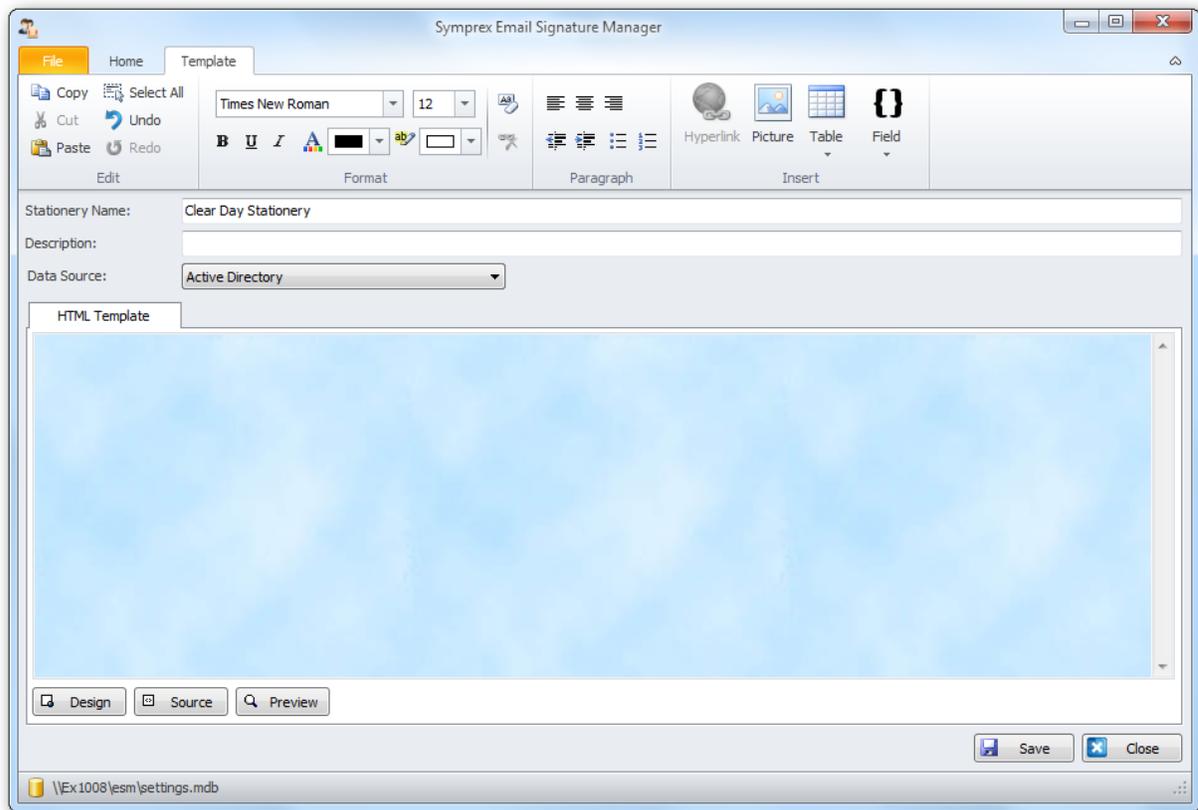
Dynamic Fields is a very powerful feature in Symprex Email Signature Manager. Each component (HTML, Rich Text and Plain Text) of a template is essentially the final content that will be deployed but instead of actual user information, field markers (dynamic fields) are inserted where the real user information 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}`

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](#).

Conditional Statements

Conditional Statements is a very powerful feature in Symprex 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` can be used to test if a field value is equal to a specific value by using the = operand 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` can be used to test if a field value is not equal to a specific value by using the <> operand 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` can be used to test if a field value is like a specific value by using the % operand 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.

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

When authoring templates in HTML, it is important to avoid using 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 CSS styles that may be present in an email with those in the template. This is also true when campaigns and disclaimers are appended to signatures. Therefore, 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 applying the styles (such as bold, italic etc.) to each line as required. It also recommended to avoid pasting into the HTML WYSIWYG editor from other HTML editors, such as Microsoft Word. The reason for this these editors do not produce particularly clean HTML suitable for use in templates, which can lead to formatting problems.

Including Graphics

There are two different ways to include graphics, such as a logo, in HTML email messages and this also applies to HTML signature templates. Graphics, or more precisely images, can either be linked or embedded. This section explains the difference between the methods, the advantages and disadvantages to each method, and how to link or embed images.

Linked or Embedded

Linked images are not a part of the message itself, but are normally placed on a public web server, and then referenced in the message body with an `<img>` tag, as in this example:

`<img src="http://www.company.com/images/logo.gif">`

The advantages of linked images are a small message size and a low risk of interception by antivirus and anti-spam filters. The disadvantages are that the recipient may not see linked images when viewing the message off-line, and that some email clients may block image download by default (please see additional notes on Microsoft Outlook 2003 below).

Unlike linked images, embedded images are part of the message itself. Embedded images are included as embedded attachments, and then referenced in the message body with an `<img>` tag, but with an image identifier, known as the "Content Id", instead of a link, as in this example:

`<img src="cid:embedded-image">`

Note You cannot explicitly create cid references. Microsoft Outlook will do this when configured to embed images, or when an image is stored in a local network location.

The advantages and disadvantages to using embedded images are exactly opposite to using linked images. The message size is (potentially much) larger and the risk of interception by antivirus and anti-spam filters is higher. On the other hand, the recipient will normally see embedded images even when viewing email off-line, and image download blocking issues do not normally apply to embedded images.

How to Include Linked Images

To include linked images, simply insert the image HTTP link in the HTML for the template. Unless the *Send pictures from the Internet* option in Microsoft Outlook is enabled, the picture will not be embedded in the email. You can control this particular Outlook setting via the signature client settings or global client settings in Email Signature Manager, or via Group Policies (GPO).

How to Include Embedded Images

To include embedded images, you can insert the image HTML link using the file name of the image on a

local disk or network share. Microsoft Outlook will automatically recognize that the image is stored locally and embed the image in the email.

Alternatively, when the *Send pictures from the Internet* option is enabled, pictures will always be embedded. However, using this approach will result in all images in an email to be embedded, i.e. also images that the user has added to the email.

Note Embedded images cannot be used in OWA signatures; OWA signatures *must* used linked images.

Linked Images in Microsoft Outlook

By default, Microsoft Outlook 2003 and higher block the automatic download of images from the Internet, i.e. the download of linked images. A recipient using Outlook 2003 or higher will see the message and message formatting, but must manually activate the download of pictures. This applies to linked images only; embedded images will be shown automatically.

Outlook 2003 can be configured to automatically download images as follows:

- In the **Tools** menu, click **Options**.
- Select the **Security** tab and click the **Change Automatic Download Settings...** button.
- Adjust the settings as required.

Outlook 2007 can be configured to automatically download images as follows:

- In the **Tools** menu, click the **Trust Center...** button.
- Select the **Automatic Download** page.
- Adjust the settings as required.

Outlook 2010 can be configured to automatically download images as follows:

- On the **File** page, click **Options.**
- Select the **Trust Center** page and click the **Trust Center Settings...** button.
- Select the **Automatic Download** page.
- Adjust the settings as required.

Outlook 2003 and Outlook 2007 can be configured to automatically download images in email from a specific sender or domain as follows:

- On the **Tools** menu, click **Options.**
- Select the **Preferences** tab and click the **Junk E-mail** button.
- Select the **Safe Senders** tab and add the email addresses and domains to be trusted.

Outlook 2010 can be configured to automatically download images in email from a specific sender or domain as follows:

- In the **Delete** group of the **Home** page of the ribbon, click the **Junk** drop-down menu and select **Junk E-mail Options...**
- Select the **Safe Senders** tab and add the email addresses and domains to be trusted.

<u>**Note**</u> By default, email from Contacts is automatically trusted so images will be automatically downloaded.

Test Signatures

The Test Signatures dialog is opened by clicking the **Test** button in the **Templates** group of the **Home** ribbon on the <u>main application window</u>.
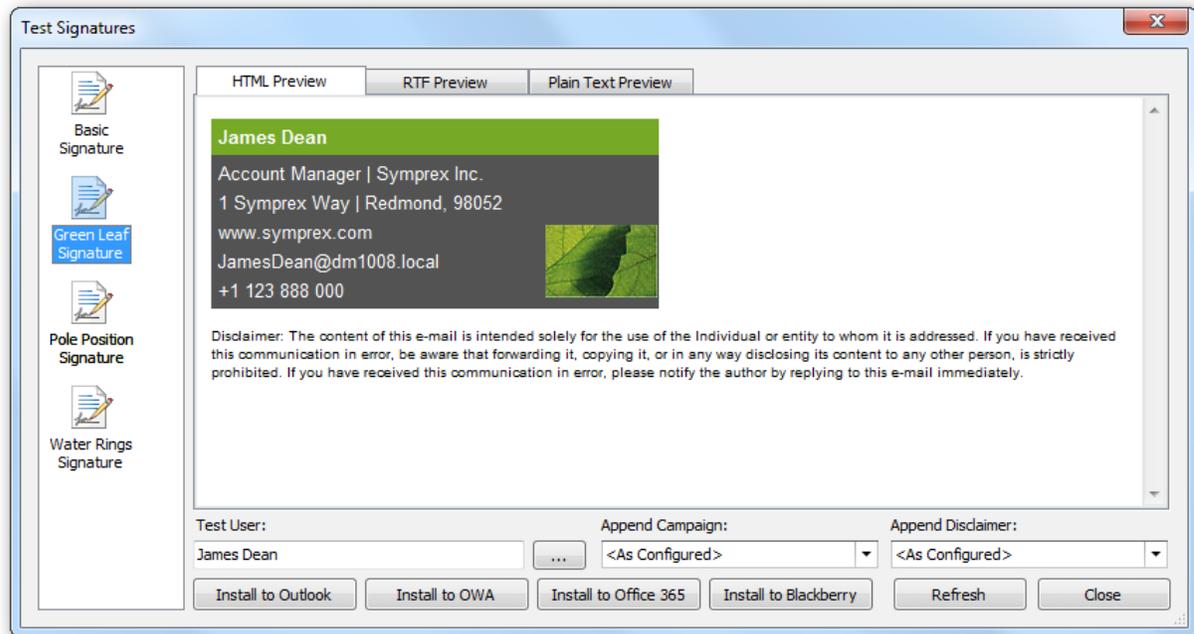
This dialog allows you to test how your signatures will look when deployed to your users in the preview window, but also directly in Outlook, OWA, Office 365 and on Blackberry devices.

- 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 <u>creating and editing signatures</u> 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.doe"), the DOMAIN\Account format (e.g. "MYDOMAIN\john.doe") or the account@domain format (e.g. "john.doe@mydomain.com").
- By default, the configured campaign(s) will be appended to the signature preview (see <u>creating and editing campaigns</u> 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 <u>creating and editing disclaimers</u> for further details). To see how a specific disclaimer will look, select it from the **Append Disclaimer** list and click the **Refresh** button.

Tutorial 2

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 Deployment Options dialog.
- 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 Office 365 Options dialog and the current user must have an Office 365 hosted email account for the deployment to succeed.
- To install to Blackberry, click the **Install to Blackberry** button. You will be prompted to confirm this action before the preview is deployed to the Blackberry Enterprise Server database. This option is not available unless deployment to Blackberry has been configured using the Blackberry Options dialog and the current user must have a Blackberry device configured 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 of the **Home** ribbon on the main application window.
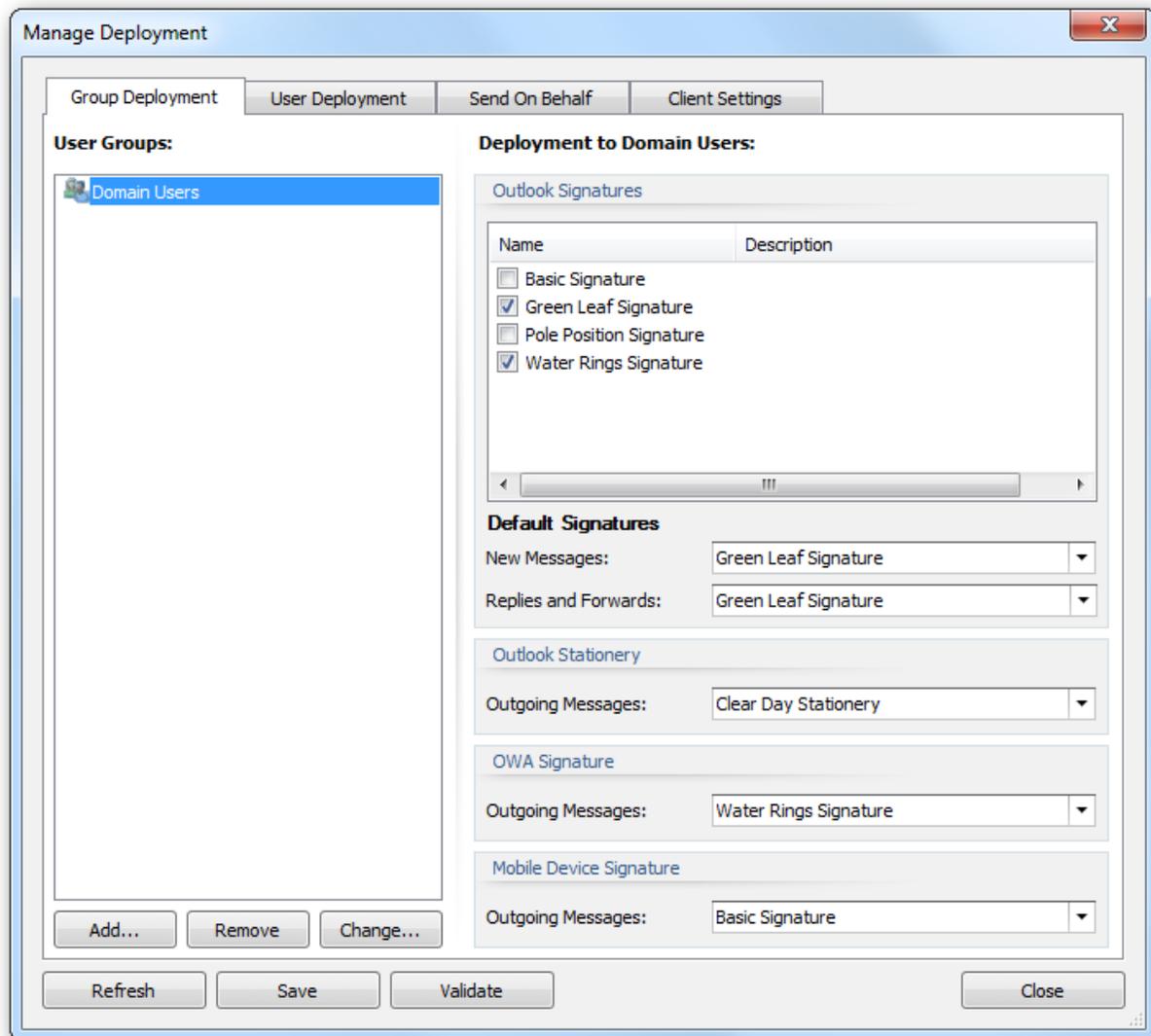
Deployment of signatures to the users in your organization can be configured either by group membership (i.e. users will receive the signatures for the group to which they belong) or individually (i.e. per-user). The **Group Deployment** page manages the Active Directory groups for which deployment has 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 membership of one or more groups, and individually, then the individual deployment settings will take precedence.

The **Group Deployment** and **User Deployment** pages work in an identical manner:

- The list of objects (i.e. groups or users, as appropriate to the selected page) is displayed on the left of the page; selecting an object will display the deployment settings on the right of the page.
- To refresh the list of objects, click the **Refresh** button.
- To add a new object, 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 object, click the **Remove** button.
- To change the selected object whilst preserving the deployment configuration, click the **Change...** button; you will be presented with a new dialog to select the group or user to replace the selected object.
- To ensure that deployment is valid, click the **Validate** button; this will start a process that verifies each group and user can be loaded from Active Directory, and updates them 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.

With an object selected, 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/user. The selected signatures will then be available for the user to choose within Outlook for signing emails.
- **Default Signature - 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>".
- **Default Signature - 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 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 App/Outlook Web Access). 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>".

Note: The Mobile Device Signature specifies the signature that is deployed to the Blackberry Enterprise Server database (if you have configured Blackberry deployment) and the signature that is used by the Transport Agent to inject signatures into emails sent from your users' mobile devices (if you have the Transport Agent configured).

The **Client Settings** page can be used to configure global client settings.

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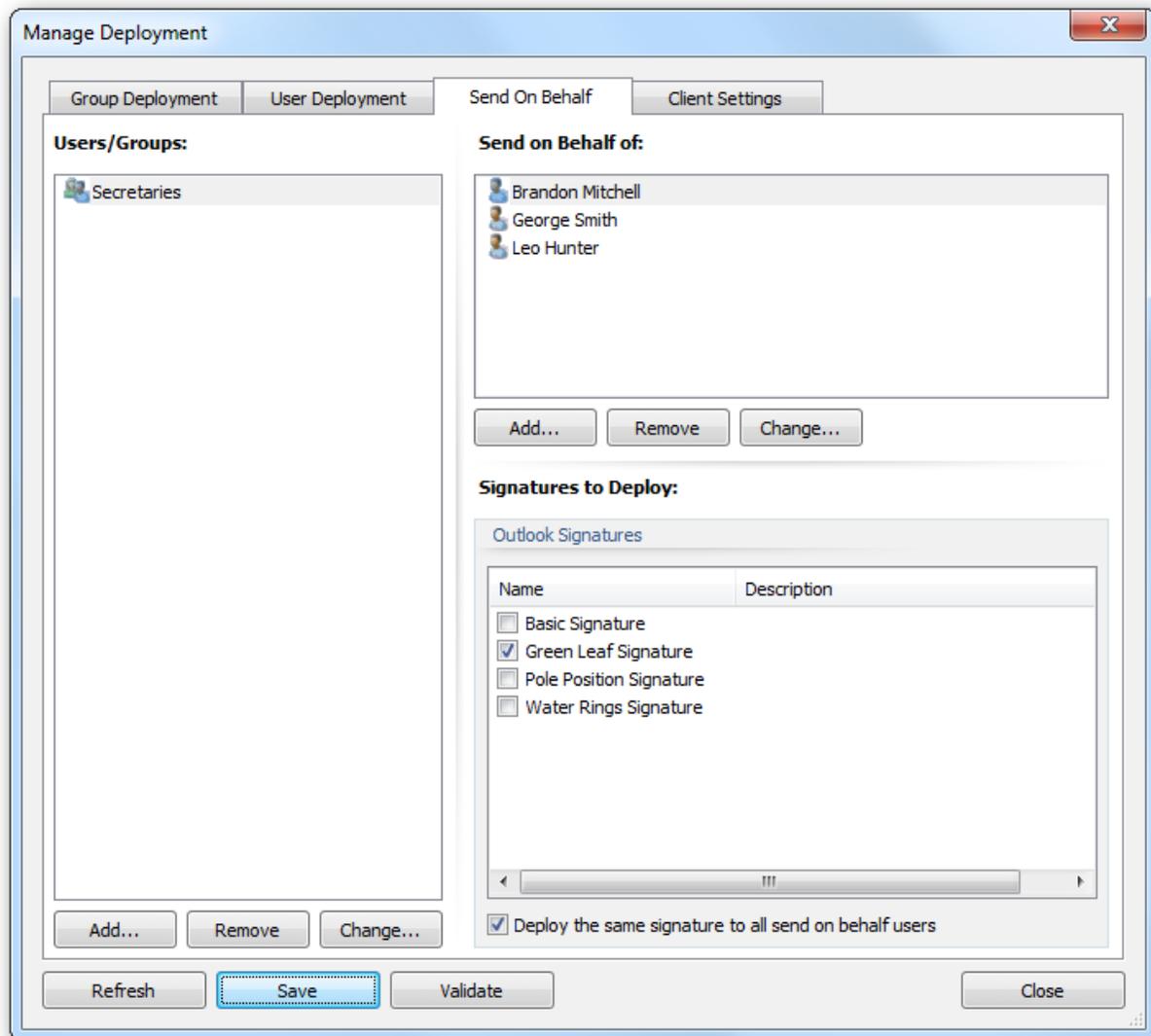
The users who will receive send on behalf signatures during deployment are shown in the **Users/Groups** list on the left-hand side of the tab; users can be specified either individually or by group membership. The list can be modified using the buttons beneath it:

- 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 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:

Tutorial

2

- 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 *Secretaries* group will have the *Green Leaf Signature* deployed with the details for *Brandon Mitchell, George Smith,* and *Leo Hunter.*

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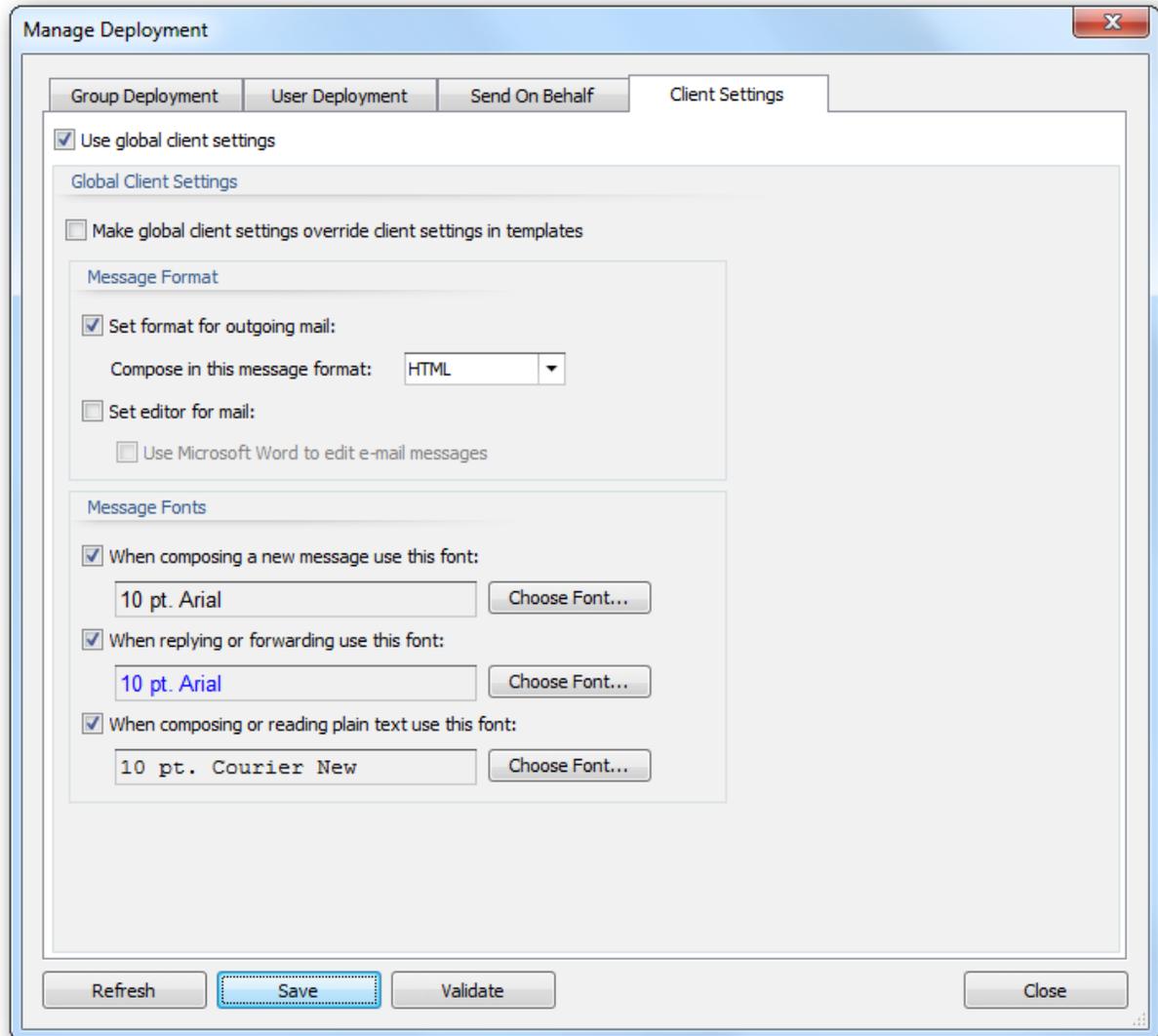
Select the **Enable global client settings** option to configure the client settings that will be applied to all users when templates are deployed.

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.
- **Set editor for mail**: Determines if Microsoft Word is used to edit email messages

Note The "Send Pictures" option is now configured through the Deployment Options dialog.

Note The "Editor for mail" option only has an effect in Microsoft Outlook 2003; in Outlook 2007 and later, Word is always used for editing emails.

The following settings can be configured for the message font:

- The Compose font; specifies the font and color that will be used when a user creates a new email.
- The Reply/Forward font; specifies the font and color that will be used when a user replies to 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 deployed.

Status Monitor

The Status Monitor dialog is opened by clicking the **Status Monitor** button in the **Deployment** group of the **Home** ribbon on the main application window.
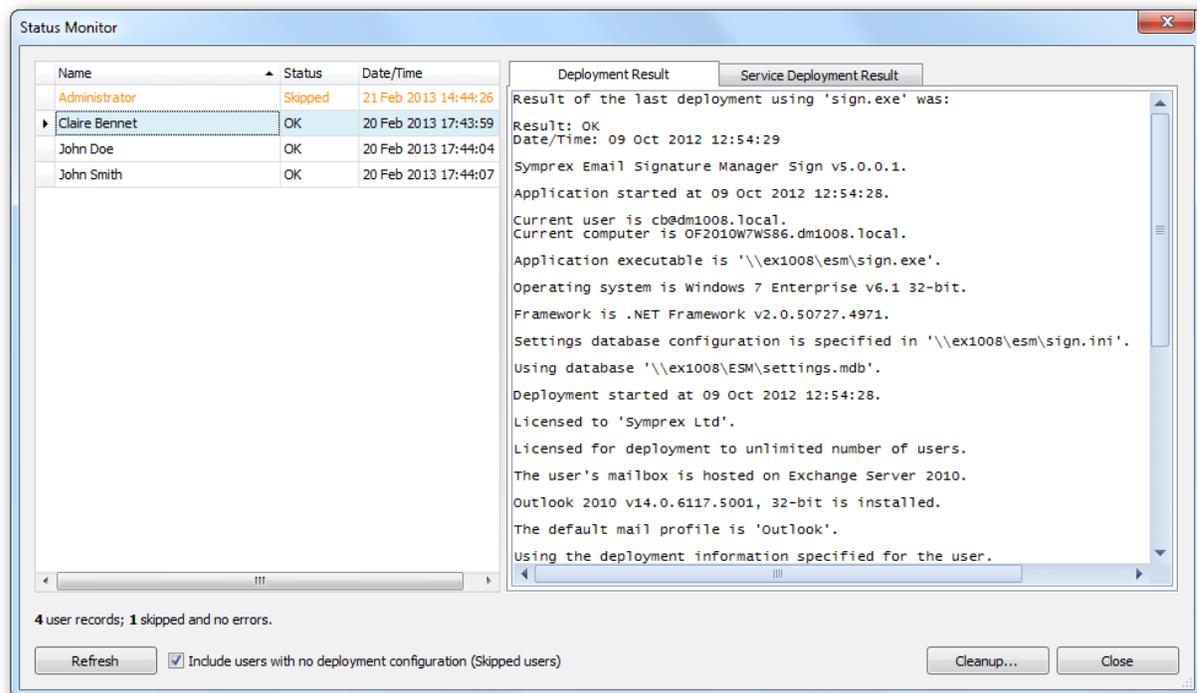
Whenever signatures are deployed to a user (using either the command line tool or the Email Signature Manager Deployment Service), the results are written to the Status Monitor; this allows deployment to be monitored and verified remotely. The left side of the dialog lists all of the users to which signatures have been deployed, together with an overall status describing the result:

- **OK** indicates that the deployment was successful.
- **Error** indicates that an error occurred during the deployment.
- **Skipped** indicates that no signature deployment was configured for the user (in the Manage Deployment dialog).

- **License Exceeded** indicates that the limit of users licensed for the application 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 two logs available, depending on your deployment method:

- **Deployment Result**; this log records the result of deploying the signatures using the command line tool, `sign.exe`.
- **Service Deployment Result**; this log records the result of deploying the signatures via the Email Signature Manager Deployment Service.

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

To refresh the list of users, click the **Refresh** button. Users who were skipped can be shown or hidden by changing the **Include users with no deployment configuration (Skipped Users)** option as required; after changing this option, click the **Refresh** button to refresh the list of users. To clean-up the list of users (for example, to remove users no longer in your organization's Active Directory structure), click the **Cleanup...** button to open the Status Monitor Cleanup dialog. To close the dialog, click the **Close** button.

Status Monitor Cleanup

This Status Monitor Cleanup dialog is opened by clicking the **Cleanup...** button in the Status Monitor dialog.
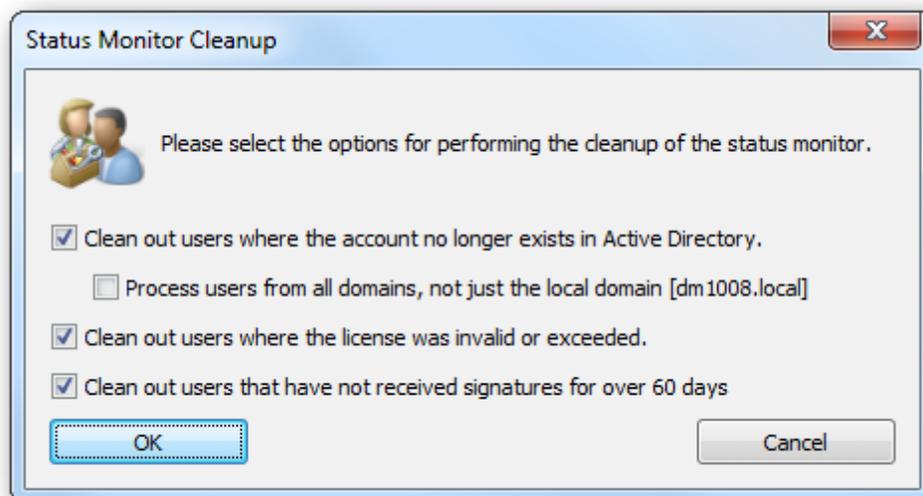
The cleanup process will delete users from the status monitor using the following options:

Setting	Description
Clean out users where the account no longer exists in Active Directory.	This option will scan the status monitor and remove users that are no longer present in your local Active Directory domain; this is particularly useful if users has left your organization and you wish to make use of their license for another user.
Process users from all domains, not just the local domain	This option extends the Active Directory check to all users in the Status Monitor, not just those in the local domain.
Clean out users where the license was invalid or exceeded.	This option will scan the status monitor and remove any users where the license was invalid or the license limit was exceeded; this is useful to keep the status monitor clean, allowing you to clearly see only the active users.
Clean out users that have not received signatures for over 60 days	This option will scan the status monitor and remove any users that have not received signatures for over 60 days; this option ensures that users who no longer receive signatures are not consuming a license.

To perform the cleanup, click the **OK** button; once the process is complete, the dialog will be closed. Alternatively, click the **Cancel** button to close the dialog without performing any cleanup.

Deployment Options

The Deployment Options dialog is opened by clicking the **Deployment Options** button in the **Settings** group of the **Configuration** ribbon on the main application window.
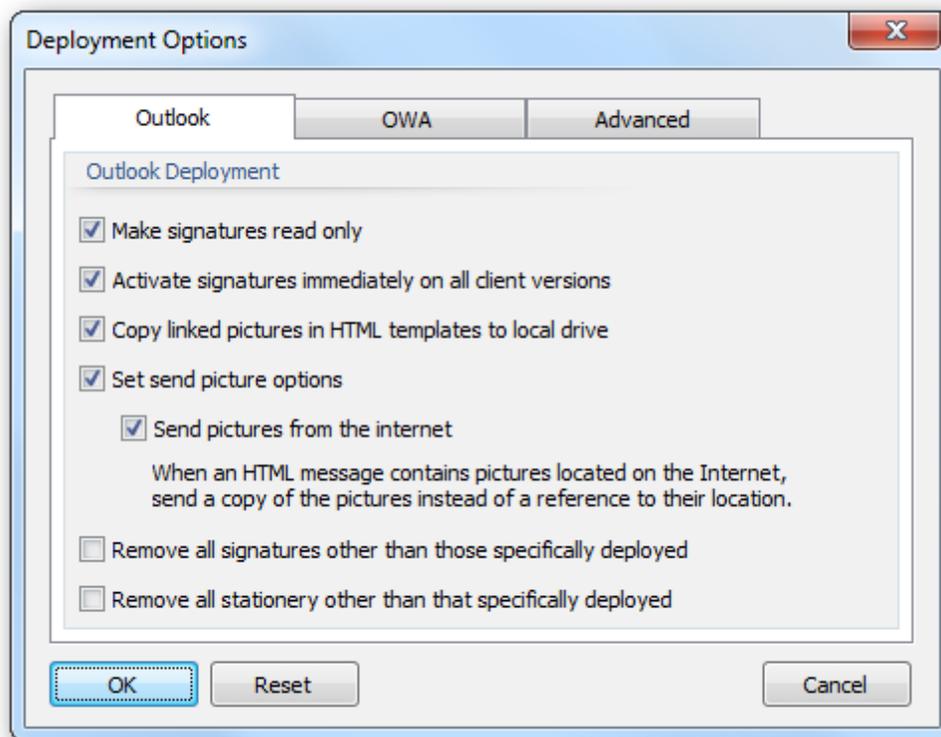
The Deployment Options dialog is used to configure system-wide settings used when deploying signatures to the users in your organization.

By default, the dialog is opened on the **Outlook** 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.
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 command line tool `sign.exe.`
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.
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.

Note The "Send Pictures" option is applied by `sign.exe` *after* client settings (either global or per-signature) have been applied.

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.

Tutorial 2

OWA Page

The OWA page on the Deployment Options dialog is used to configure the settings specific to deployment to Outlook Web App/Outlook Web Access.
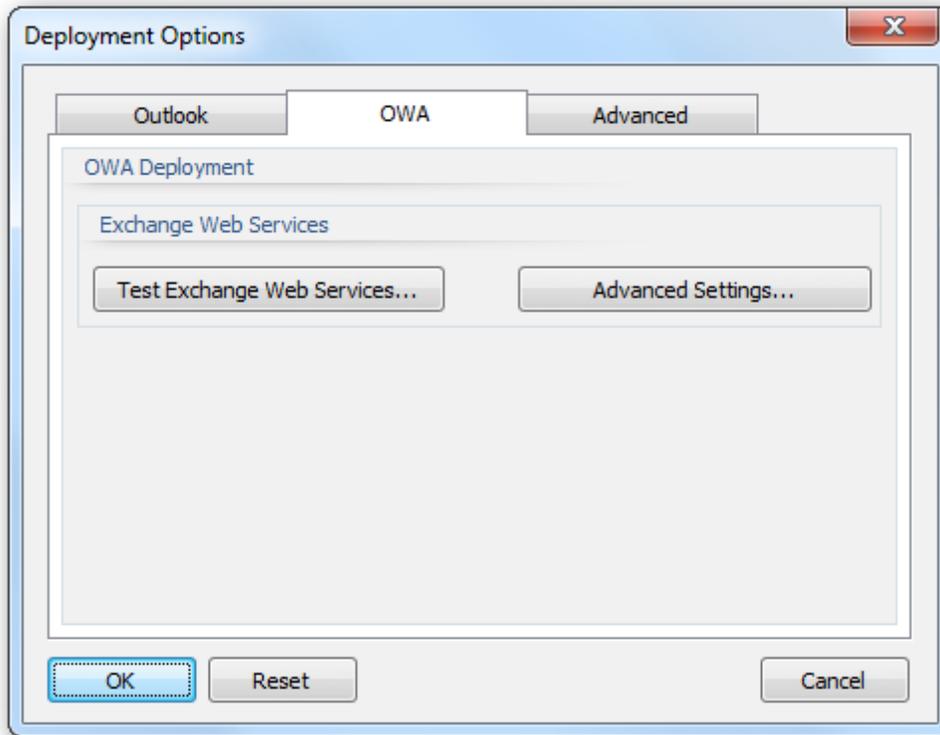
Note: Starting from v6.0 of Email Signature Manager, the Access Method for each version of Exchange Server has been fixed as follows:

- **Exchange Server 2013** (and higher): Exchange Web Services (EWS)
- **Exchange Server 2010**: Exchange Web Services
- **Exchange Server 2007**: MAPI
- **Exchange Server 2003**: MAPI

Exchange Web Services

Click the **Test Exchange Web Services...** button to open the Exchange Web Services Connectivity Test dialog, which is used to test connectivity to Exchange Web Services within your domain. Click the Advanced Settings... button open the Advanced EWS Settings dialog, which is used to configure how connections to Exchange Web Services are established.

2

Advanced EWS Settings

The Advanced EWS (Exchange Web Services) Settings dialog is opened by clicking the **Advanced Settings...** button on the Deployment Options dialog.
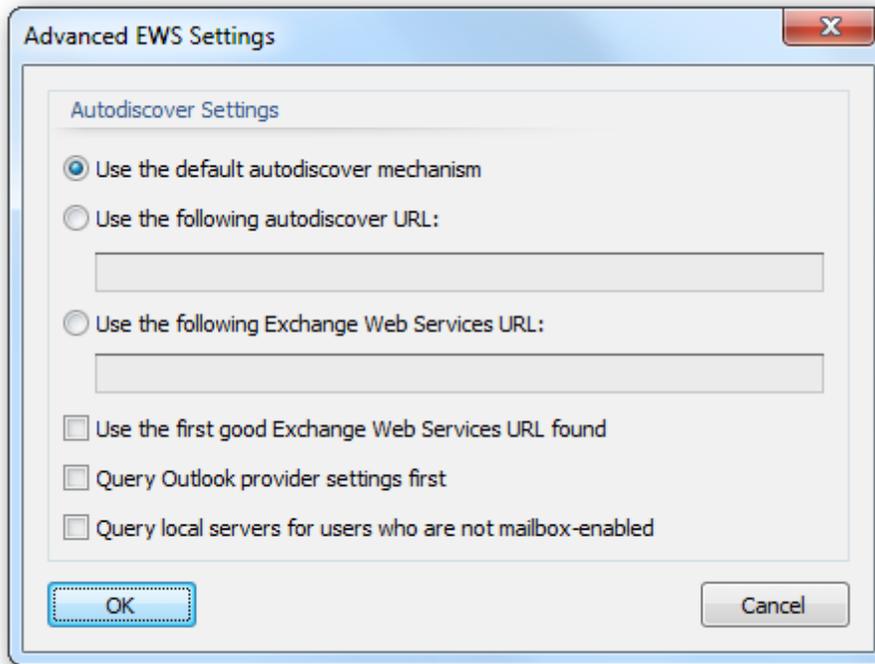
Note: In normal conditions, the connection to Exchange Web Services will be configured automatically using the autodiscover mechanism built into Exchange Server. It should only be necessary to change these advanced settings if specific problems are being encountered that prevent autodiscover from working correctly and/or performance problems are being encountered.

The following settings can be configured:

| Setting	Description
Use the default autodiscover mechanism	Specifies that the default autodiscover mechanism should be used; this is the normal setting. The default mechanism will query Active Directory for the appropriate Service Connection Points (SCPs) and then attempt to connect to each one to obtain the URL to Exchange Web Services. Each SCP is a URL to an autodiscover service hosted on an Exchange Server.
Use the following autodiscover URL	Specifies that the autodiscover mechanism should use the specified fixed URL, instead of querying Active Directory for the Service Connection Points.
Use the following Exchange Web Services URL	This setting disables the autodiscover mechanism and forces the connection to Exchange Web Services to use the specified fixed URL *for all users*.
Use the first good Exchange Web Services URL found	When the default autodiscover mechanism is being used, this setting stipulates that once the first good EWS URL has been discovered (from an SCP), the mechanism should stop and use that URL alone (rather than continuing and querying further SCPs). This can be useful if you have a number of autodiscover servers (i.e. a number of SCPs), some of which are not currently available.
Query Outlook provider settings first	When using the autodiscover mechanism, each autodiscover service (i.e. each SCP) 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.
Query local servers for users who are not mailbox-enabled	By default, the autodiscover mechanism will only query local SCPs for users who are mailbox-enabled. However, in some circumstances, it is possible for users who are *not* mailbox-enabled to have a mailbox on Exchange; for example, if your organization is using a hosted Exchange. Enabling this setting will force the autodiscover mechanism to query the local Active Directory for SCPs and query them for a user's details, even when the user is not mailbox-enabled.

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.

Exchange Web Services Connectivity Test

The Exchange Web Services Connectivity Test dialog is opened by clicking the **Test Exchange Web Services...** button in the OWA Page of the Deployment Options dialog.

2
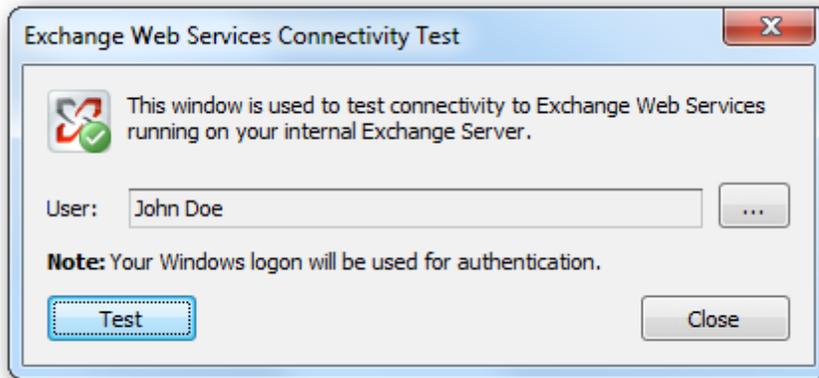
This dialog is used to test connectivity to Exchange Web Services (EWS) running on Exchange Server within your local domain. This is helpful to test that EWS is functioning as expected for the deployment of OWA signatures.

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.

Note You must be logged on to Windows as an account that has appropriate privileges on Exchange Server in order to test against a different user.

When ready, click the **Test** button. After a few moments, a summary message will be displayed indicating the overall result of test, which includes reading the number of items in the specified user's inbox and checking if the basic OWA settings could be found. A detailed log of the test can be viewed by clicking the link to the `Symprex.Connectivity.LogFile.txt` file, which is written to the current temporary folder.

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

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
Require users to be mailbox enabled to receive signatures	Specifies that users must have an Exchange Server mailbox in order to receive signatures.
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.
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.
Use ASCII format for all Outlook signature files	Specifies that `sign.exe` 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.
Record status information about signature generation and injection (SQL Server databases only)	Specifies that additional information is recorded to the Deployment Status log when signatures are generated (for use by the Transport Agent) or injected into emails (by the Transport Agent). It is recommended that this option is not enabled unless specific logging information about the Transport Agent is required.
Store deployment status information in files (Access databases only)	Specifies that deployment status information should be stored in files (located in a sub-folder of the folder containing the database), rather than being stored in the database itself.

Office 365 Options

The Office 365 Options dialog is opened by clicking the **Office 365 Options** button in the **Settings** group of the **Configuration** ribbon on the main application window.
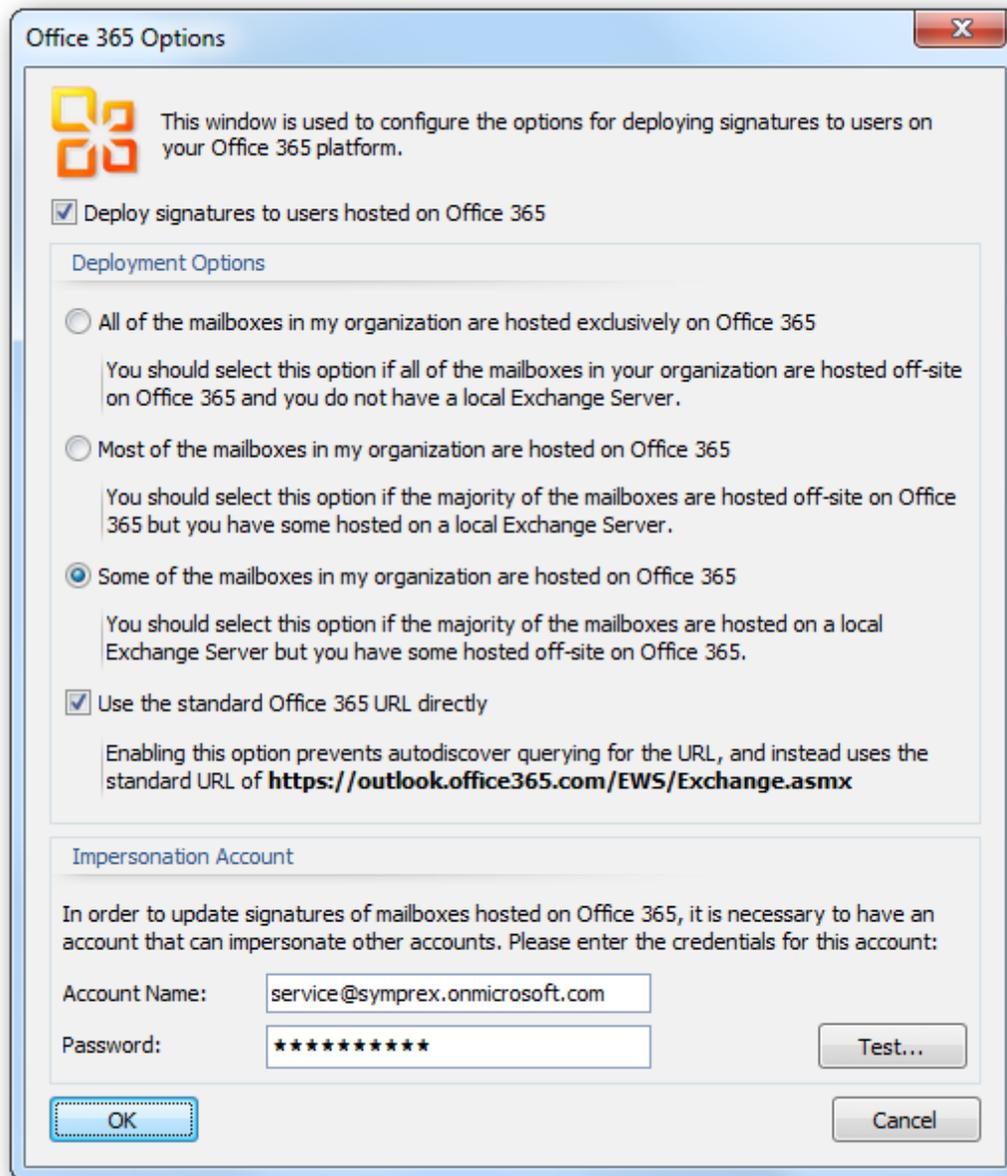
This window is used to configure deployment of signatures to your Office 365 platform. If you have users with their mailboxes hosted on Office 365, select the **Deploy signatures to users hosted on Office 365** checkbox and then select the most appropriate option which describes your organization, which controls the autodiscover lookup:

- **All of the mailboxes in my organization are hosted exclusively on Office 365**; you should select this option when all of your users' mailboxes are hosted on Office 365 and you do not use a local Exchange Server. When this option is selected, Email Signature Manager will not attempt to query any local Exchange Servers in your local domain and will only deploy to the Office 365 servers.

- **Most of the mailboxes in my organization are hosted on Office 365**; you should select this option when most of your users' mailboxes are hosted on Office 365 and only some are hosted on a local

Exchange Server. When this option is selected, Email Signature Manager will first attempt to deploy signatures to your Office 365 platform and, if this fails, will then look for an internal Exchange Server on your local domain.

- **Some of the mailboxes in my organization are hosted on Office 365**; you should select this option when some of your users' mailboxes are hosted on Office 365 but most are hosted on a local Exchange Server. When this option is selected, Email Signature Manager will first attempt to deploy signatures to an internal Exchange Server on your local domain and, if this fails, will deploy to your Office 365 platform.

It is possible to bypass the autodiscover mechanism by enabling the **Use the standard Office 365 URL directly** option. When enabled, this will cause deployment to *not* autodiscover the URL for the Office 365 Exchange Web Services (EWS), and to use the standard Office 365 EWS URL directly.

Important: It is recommended that the **Use the standard Office 365 URL directly** option is only enabled if there is a specific requirement to do so; for example, if the autodiscover service is not working as expected.

In order for signatures to be deployed on your Office 365 platform, it is necessary to provide the credentials of an account that can impersonate your users. This account must be a member of a role group that has the roles *ApplicationImpersonation* and *View-Only Recipients* assigned, and can be configured as follows:

1. Start a new remote Power Shell and connect to your Office 365 platform.

2. Type the following line, and then press **ENTER**:

```
New-RoleGroup -Name "Symprex Office 365" -Roles "ApplicationImpersonation",
"View-Only Recipients" -Members <Account>
```

where *<Account>* is the name of the account to include as a member in the new role group.

3. You can enter the following command to show the role group configuration:

```
Get-RoleGroup "Symprex Office 365" | fl
```

4. You can enter the following command to list the role group members:

```
Get-RoleGroupMember "Symprex Office 365"
```

For more information about role groups in Exchange Online, and how to work with role groups in the Exchange Control Panel rather than using PowerShell, please refer to http://help.outlook.com/en-us/140/ee441216.aspx.

Once the impersonation account has been configured, enter the full account name in the **Account Name** box and the password in the **Password** box.

Click the **Test...** button to open the Office 365 Connectivity Test dialog, which is used to test connectivity to the Microsoft Office 365 servers located on the Internet and the specified impersonation account.

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 Connectivity Test

The Office 365 Connectivity Test dialog is opened by clicking the **Test...** button in the Office 365 Options dialog.
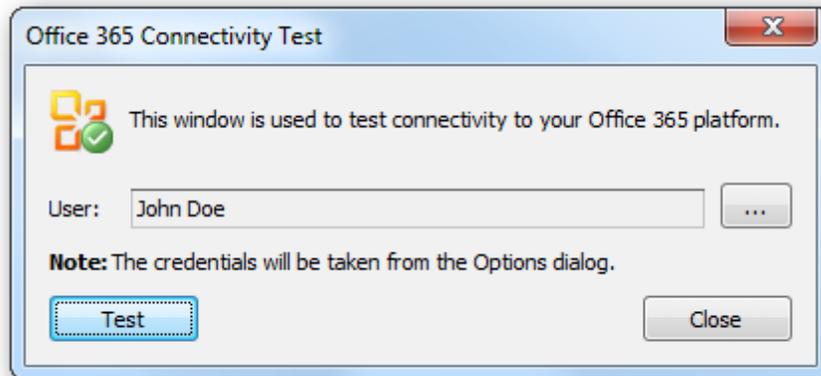
This dialog is used to test connectivity to the Microsoft Office 365 servers located on the Internet. This is helpful to test that the deployment of signatures to Office 365 will work as expected using the specified impersonation account.

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.

Note The credentials for the impersonation account to use will be taken from the Options dialog.

When ready, click the **Test** button. After a few moments, a summary message will be displayed indicating the overall result of test, which includes reading the number of items in the specified user's inbox and checking if the basic OWA settings could be found. A detailed log of the test can be viewed by clicking the link to the `Symprex.Connectivity.LogFile.txt` file, which is written to the current temporary folder.

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

Blackberry Options

The Blackberry Options dialog is opened by clicking the **Blackberry Options** button in the **Settings** group of the **Configuration** ribbon on the main application window.
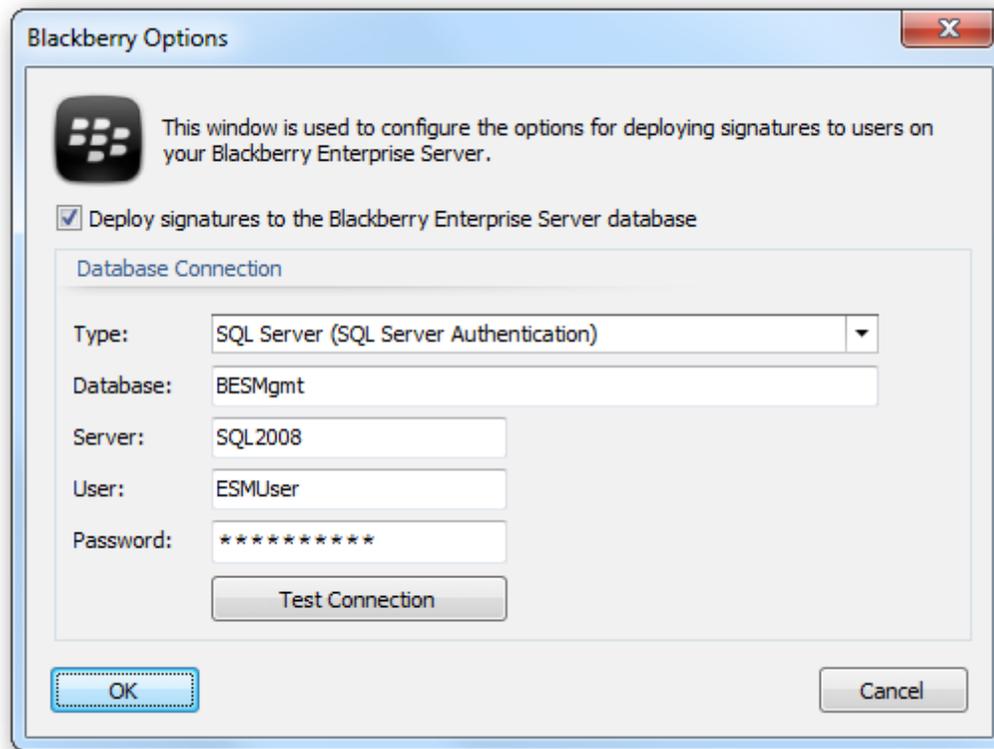
Important Only Blackberry Enterprise Server v5.x (Full and Express editions) is supported by Email Signature Manager. Users of other versions are advised to use the Email Signature Manager Transport Agent.

This window is used to configure deployment of signatures to your Blackberry Enterprise Server database. If you have users to which you wish to deploy signatures, select the **Deploy signatures to the Blackberry Enterprise Server database** checkbox and enter the details of your Blackberry Enterprise Server database:

- **Type:** Specifies the type of the connection to the database, using either Windows Authentication or SQL Authentication.
- **Database**: Specifies the name of the Blackberry Enterprise Server database; the usual name is `BESMgmt`.
- **Server**: Enter the name of the server where the database is located.
- **User**: When connecting using SQL Authentication, enter the login to connect to the server.
- **Password**: When connecting using SQL Authentication, enter the password.

It is recommend to use SQL Authentication as the authenticating user must have db_datareader and db_datawriter permissions on the UserConfig table in the Blackberry Enterprise Server 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, with the result being displayed in a message box.

Note You need to configure which signatures are deployed to your Blackberry users by setting the

"Mobile Device Signature" in the Manage Deployment dialog. As Blackberry does not support HTML signatures, the **Plain Text Template** of the specified signature will be used, *not* the HTML Template.

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

Settings Database

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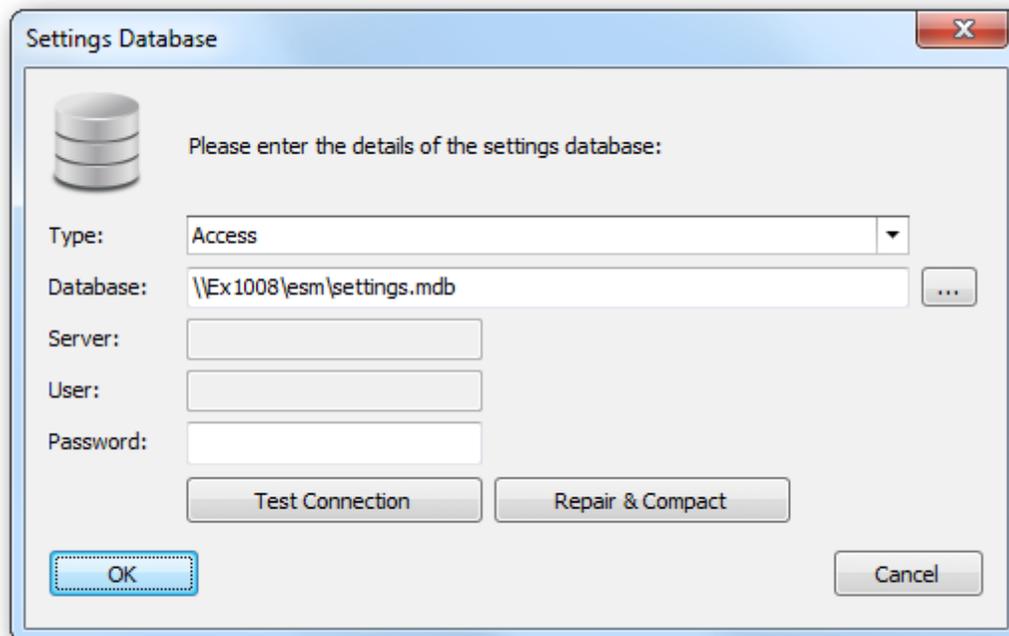
The Settings Database dialog is used to connect the application to the database storing your templates and deployment configuration. When the dialog is first opened, the settings for connecting to the current database are displayed. If required, select the type of the database in the **Type** drop-down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

- **Database**: Specifies the actual database for the settings database:
  o When connecting to a Microsoft Access database, enter the full path to the database or select it by clicking the ellipses (". . .") button.
  o When connecting to a Microsoft SQL Server database, enter the name of the database.
- **Server**: When connecting to Microsoft SQL Server, enter the name of the server where the database is located.
- **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.

2

Note The settings.mdb database that is included with Email Signature Manager is in Microsoft Access format.

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. If the Access database being used becomes corrupted, click the **Repair & Compact** button to rectify the fault.

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.

Note You can save and load connection settings (which store the settings for connecting to the database) to files for re-use.

Import Database

The Import Database dialog is opened by clicking the **Import Database** button in the **Settings Database** group of the **Configuration** ribbon on the main application window.
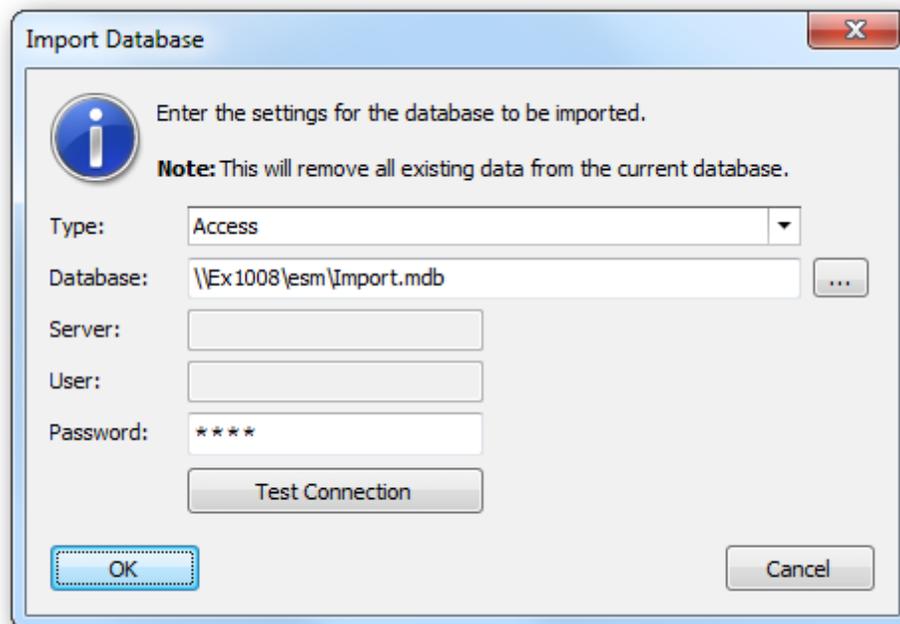
Importing an existing database is normally used as part of migrating from using the settings.mdb database that is included with Email Signature Manager to using Microsoft SQL Server. Full details about how to configure a SQL Server database for use with Email Signature Manager can be found in a separate chapter.

Important All existing data in the current database <u>will be deleted</u> 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 <u>Settings Database dialog</u>.

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

- **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.
- **Server**: When connecting to Microsoft SQL Server, enter the name of the server where the database is located.
- **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 settings.mdb database that is included with Email Signature Manager is in Microsoft Access format.

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 **Define Data Sources** button in the **Tools** group of the **Configuration** ribbon on the main application window.
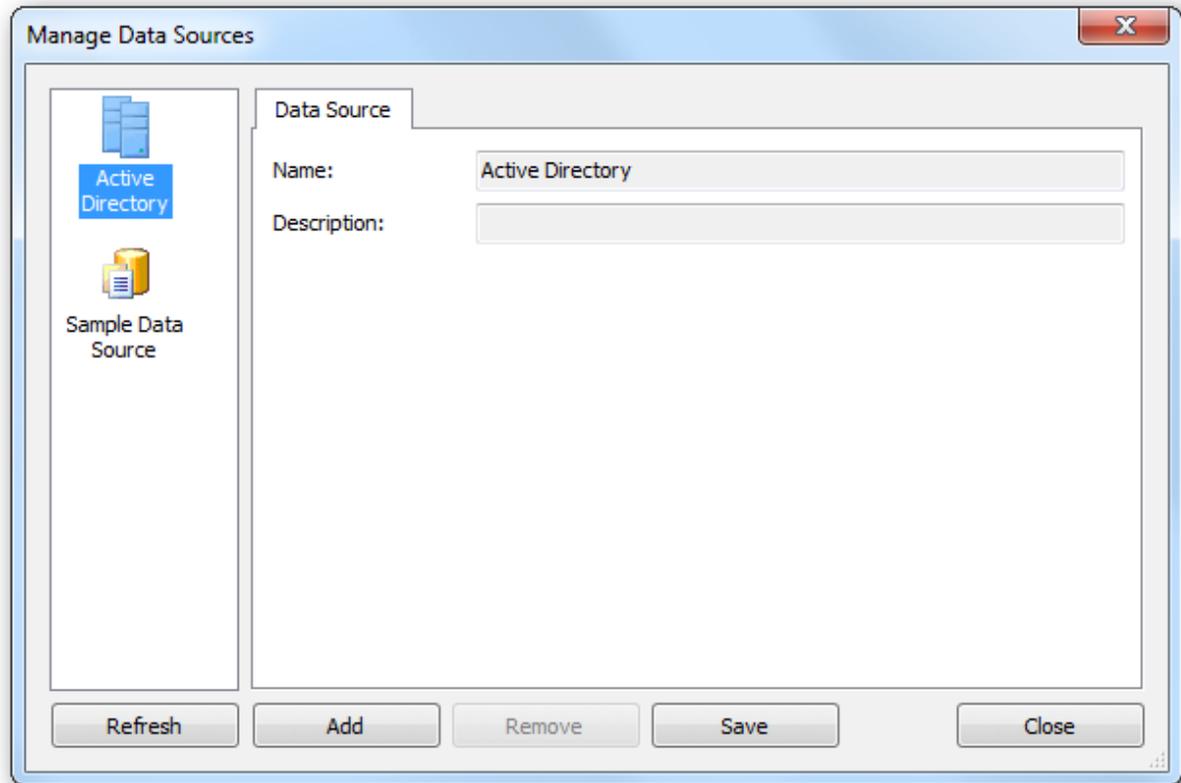
A data source is used to supply information when a signature is being deployed to a user; specifically, it is used to fetch the data used to populate the fields in the signature. The default data source available for all signatures is Active Directory, where the fields in the signatures are mapped to 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** (mandatory): Specifies the unique name of the data source.
- **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 Sources

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:

- **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.

- o When connecting to a Microsoft SQL Server database, enter the name of the database.
- **Server**: When connecting to Microsoft SQL Server, enter the name of the server where the database is located.
- **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.

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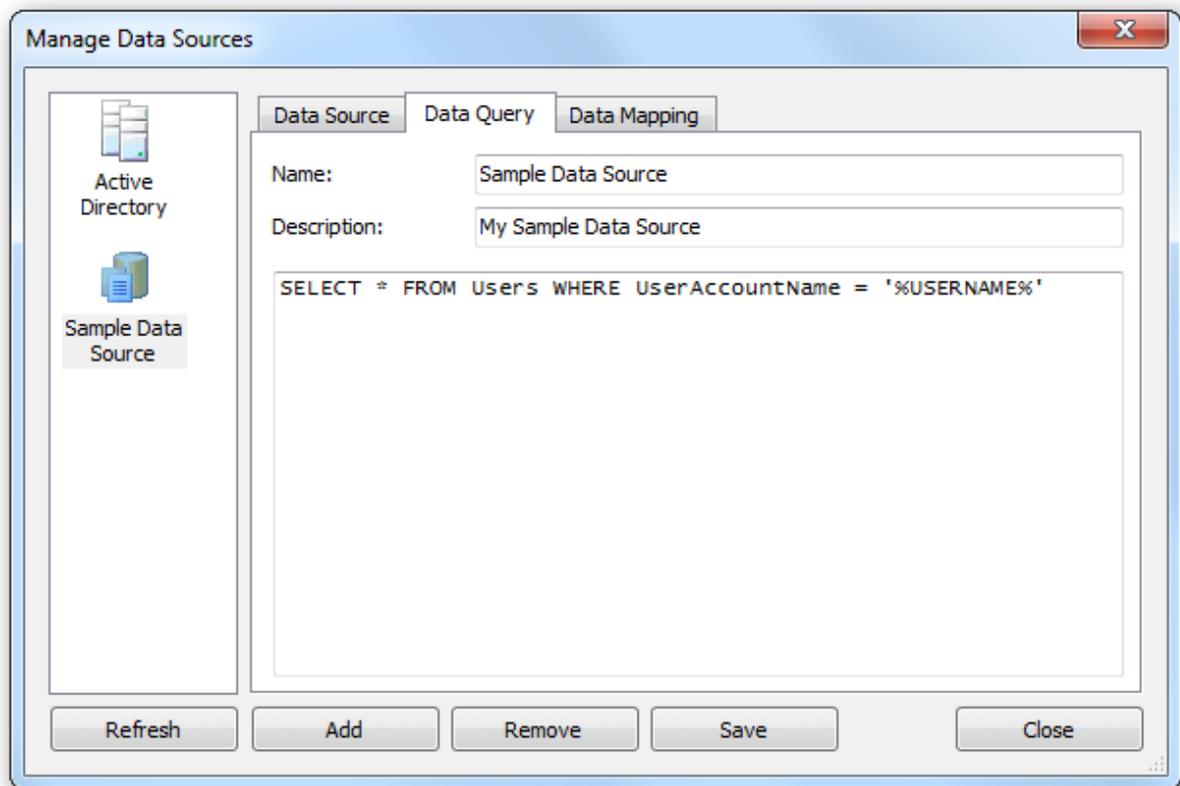
The query needs to be specified such that it will return a single row of data for the user to which a signature is being deployed. To accomplish this, the `WHERE` clause of the query can be customised using the following tokens:

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.

Specify the Data Query

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:
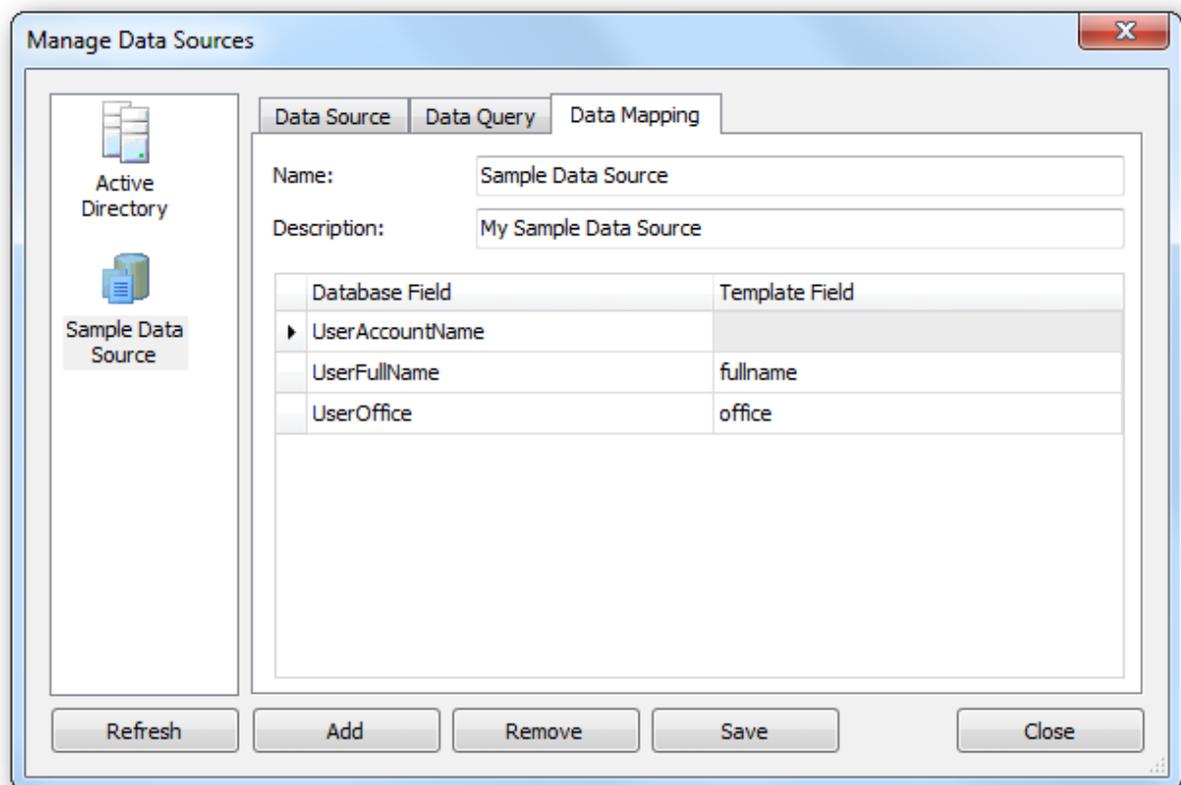
When the *Data Mapping* page is selected, a connection to the database specified on the *Data Source* page will be established and the query specified on the *Data Query* page will be executed to determine the fields available; these fields are displayed in the **Database Field** column of the grid. 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 deployed, 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 in the **Tools** group of the **Configuration** ribbon on the main application window.
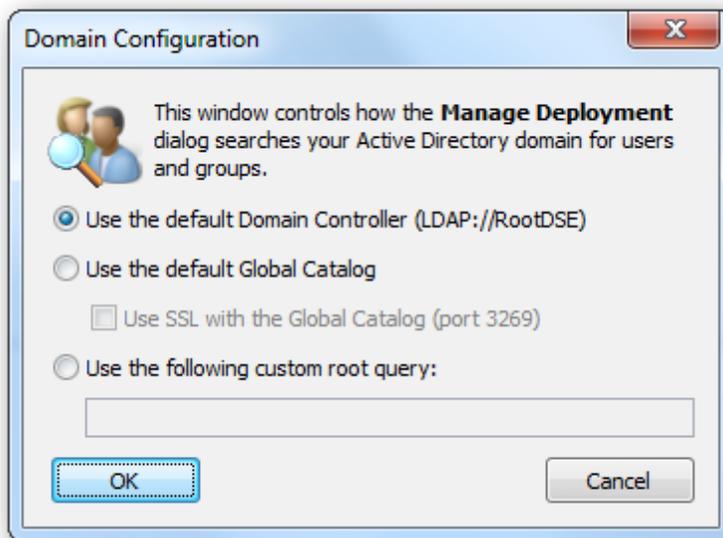
This dialog configures how the Manage Deployment dialog will search your Active Directory domain for users and groups:

- **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"`);

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.

Configure Service

The Configure Service dialog is opened by clicking the **Configure Service** button in the **Settings** group of the **Configuration** ribbon on the main application window.
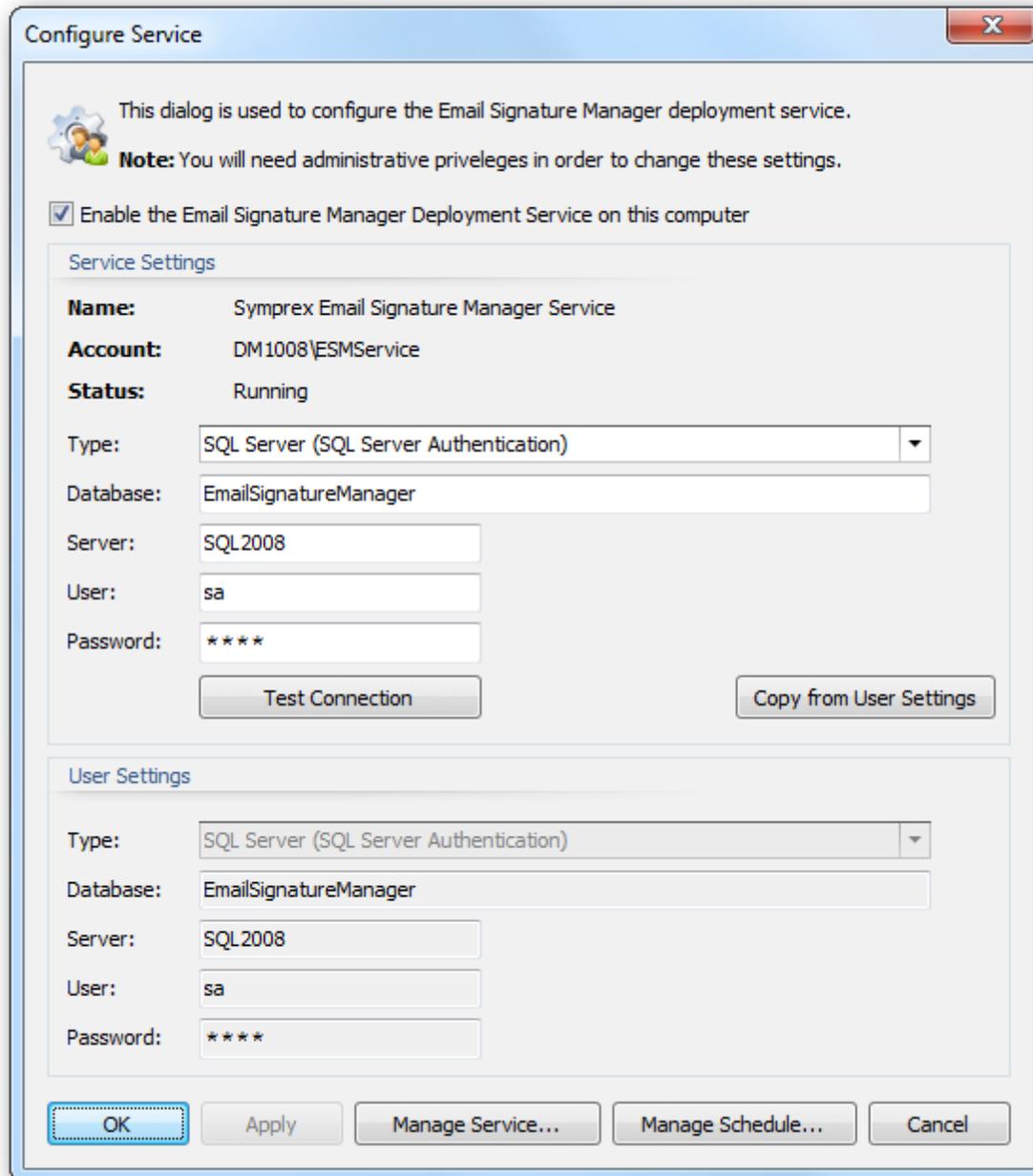
To enable the <u>Email Signature Manager Deployment Service</u> on the local computer, select the **Enable the Email Signature Manager Deployment Service on this computer** option.

The **Service Settings** displays the configuration of the service:

- **Name**: The name of the service, as displayed in the Service Control Manager.
- **Account**: The Windows logon account being used by the service.
- **Status**: The current status of the service (running, stopped etc.).

The service needs to be configured to use the correct settings database; select the type of the database

in the **Type** drop-down and then configure the following settings:

- **Database**: Specifies the actual database for the settings database:
  - 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.
- **Server**: When connecting to Microsoft SQL Server, enter the name of the server where the database is located.
- **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 settings.mdb database that is included with Email Signature Manager is in Microsoft Access format.

Alternatively, click the **Copy from User Settings** button to copy the settings for the current database being used by the application (the current database is displayed under **User Settings**). 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.

To configure the service logon account and start mode, click the **Manage Service...** button to open the Manage Service dialog.

To configure the schedule for the service (which determines how often signatures are deployed and generated), click the **Manage Schedule...** button to open the Manage Schedule dialog.

When the configuration for the service has been completed, click the **OK** button to apply the changes and close the dialog, or click the **Apply** button to apply the changes without closing the dialog. To close the dialog without making any changes, click the **Cancel** button.

Note When the changes are saved, the following actions will occur:

- If the service is being *enabled*, the start mode will be changed to Manual and the service must be started manually.
- If the service is being *disabled*, the service will be stopped and the start mode changed to Disabled.

Deployment Method

The service deploys to the users and groups configured in the Manage Deployment dialog. Where a user is a member of a group for which deployment is defined as well as having their own deployment defined, their own deployment will take precedence (in other words, the same rule as that applied by `sign.exe`).

The service will deploy OWA signatures using the method configured in the Deployment Options dialog with the following exceptions:

- It is not possible for the service to deploy signatures on Exchange Server 2003 using WebDAV (an error will be reported for each user in the Status Monitor if the selected deployment method for Exchange

Server 2003 is WebDAV).

- If a user is not mailbox-enabled, the service will assume that the user's mailbox is accessible via a server that has Exchange Web Services (EWS) capabilities compatible with Exchange Server 2010 or later and use EWS for deployment.
- The service will deploy to Office 365 using the settings specified in the Office 365 Options dialog.

Note In order for the service to deploy to users who are not mailbox-enabled, the "Require users to be mailbox enabled to receive signatures" option must be off (configure this in the Advanced page of the Deployment Options dialog).

Manage Service

The Manage Service dialog is opened by clicking the **Configure** button in the Configure Service dialog.
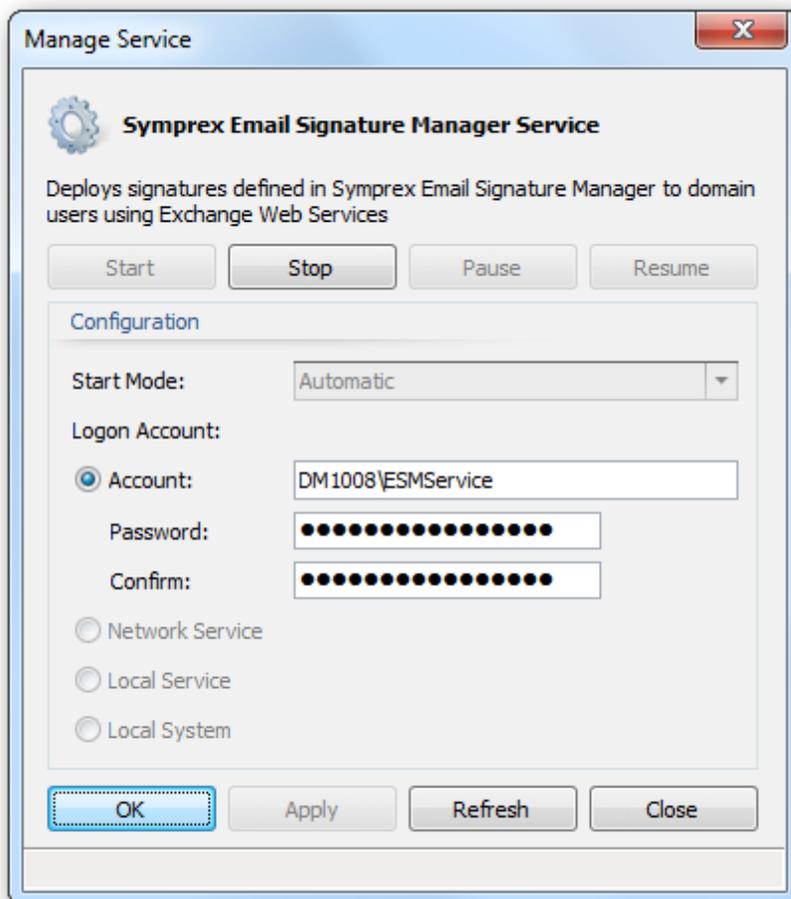
The top portion of the window displays the details and status of the Email Signature Manager Deployment Service. If it is not running, the service can be started by clicking the **Start** button, or it can be stopped by clicking the **Stop** button.

Note The service can not be paused, so the *Pause* and *Resume* buttons will remain disabled.

Tutorial 2

The **Configuration** area is used to configure how the service behaves.

- The **Start Mode** option determines how the service behaves when Windows is started. The start mode for the service is changed by the Configure Service dialog; it is set to Manual when the service is enabled (if it is not already Automatic)) or is set to Disabled when the service is disabled.
- The **Logon Account** is used to specify the Windows account under which the service runs. This account must be granted specific permissions to be able to access mailboxes on your Exchange Server. Please refer to this topic for further details.

Note The service must always run using a logon account that has appropriate permissions. The *Network Service*, *Local Service* and *Local System* options will not work.

Once the configuration has been updated, click the **OK** button to apply the changes and close the dialog, or click the **Apply** button to apply the changes without closing the dialog. Click the **Refresh** button to refresh the dialog, or click the **Close** button to close the dialog without saving changes.

Manage Schedule

The Manage Schedule dialog is opened by clicking the **Manage Schedule...** button in the Configure Service dialog.
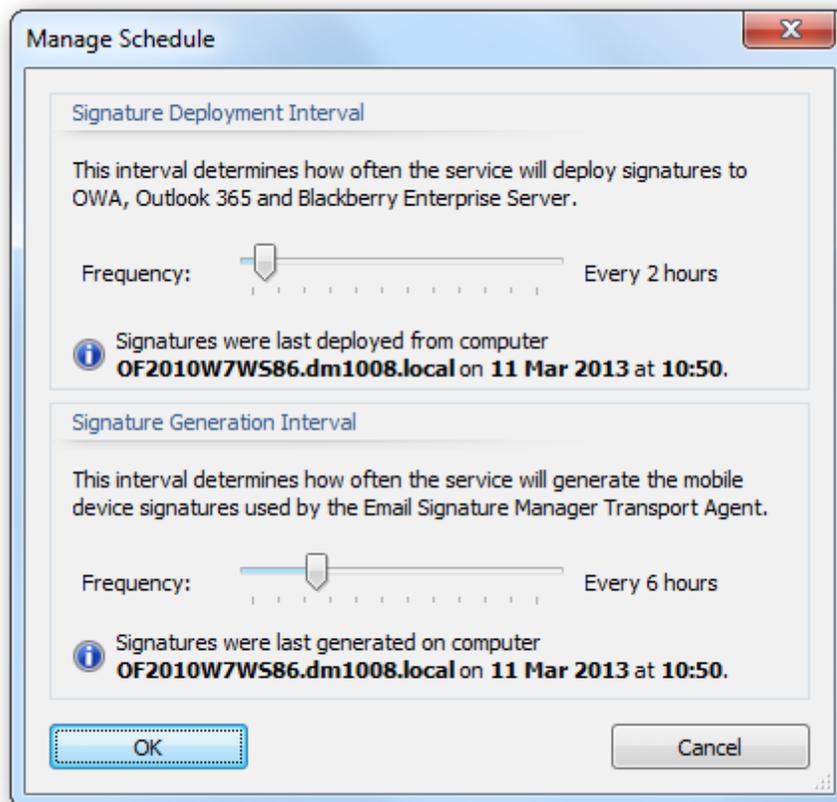
When the service is enabled it will deploy signatures to OWA, Office 365 and Blackberry Enterprise Server in place of the command line deployment utility (sign.exe). The frequency of this deployment is controlled

using the slider in the **Signature Deployment Interval** box. This can be configured from once every hour to once a day. When the service is started, an initial deployment of signatures is performed. From there, signatures are deployed as follows:

- When the interval is set to *once a day*, the deployment will always occur at midnight of each subsequent day.
- When the interval is set to a shorter frequency (i.e. less than every day), the deployment will occur at the specified interval after the service is started.

When the service is enabled it will generate signatures to be applied to emails sent from mobile devices by the Transport Agent, if this is enabled in the Transport Agent Rules dialog. The frequency of this generation is controlled using the slider in the **Signature Generation Interval** box. This can be configured from once every hour to once a day. When the service is started, an initial generation of signatures is performed. From there, signatures are generated as follows:

- When the interval is set to *once a day*, the generation will always occur at midnight of each subsequent day.
- When the interval is set to a shorter frequency (i.e. less than every day), the generation will occur at the specified interval after the service is started.

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

Transport Agent Rules

The Transport Agent Rules dialog is opened by clicking the **Transport Agent Rules** button in the **Mobile Devices** group of the **Configuration** ribbon on the main application window.
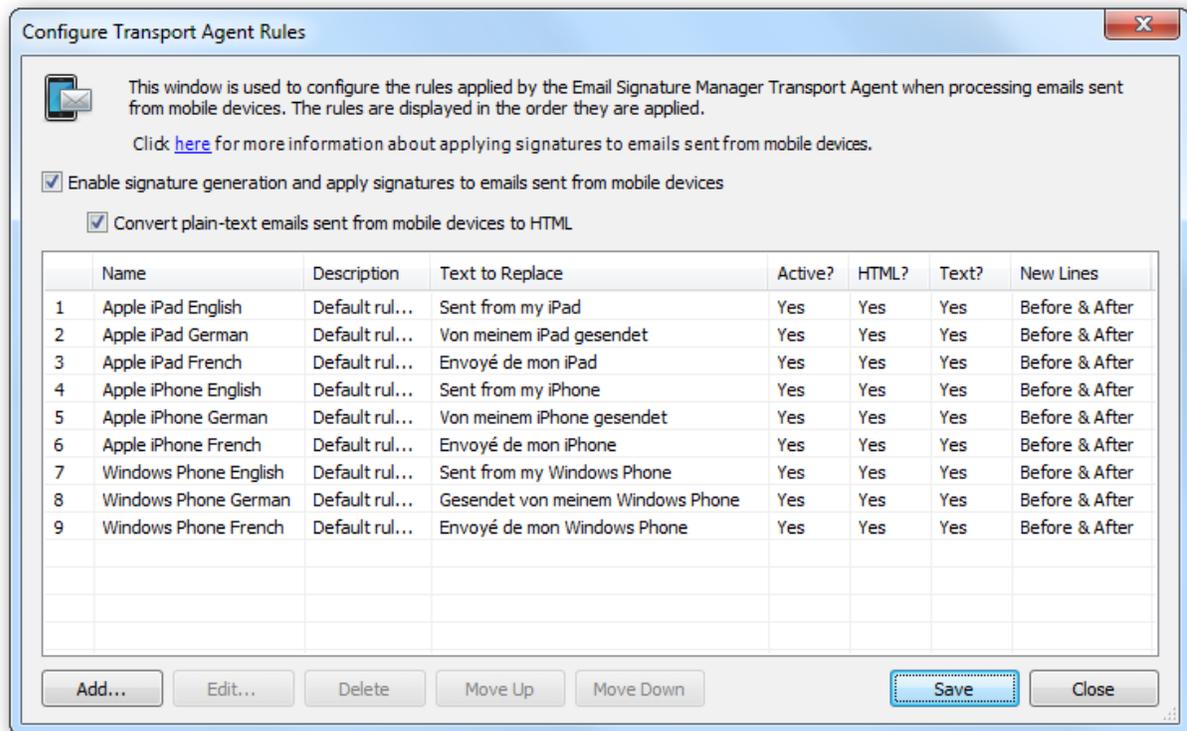
Selecting the **Enable signature generation and apply signatures to emails sent from mobile devices** option will configure `sign.exe` or the [Email Signature Manager Deployment Service](#) to generate the signatures that will be applied by the [Email Signature Manager Transport Agent](#) to emails sent from mobile devices within your organization.

By default, the Apple iPhone™ and Apply iPad™ send new emails in plain-text format, unless some formatting is applied (such as marking some text as bold). Selecting the **Convert plain-text emails sent from mobile devices to HTML** option will cause the Transport Agent to convert plain-text emails into HTML format and inject the HTML signature.

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 main part of the dialog displays a grid showing all of the defined rules for use by the Email Signature Manager Transport Agent, in the order in which they are applied. The following actions can be performed:

- To create a new rule, click the **Add...** button, which opens the [Manage Transport Agent Rule dialog](#).
- To edit an existing rule, select it in the grid and click the **Edit...** button, which opens the [Manage Transport Agent 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 applied earlier), select it in the grid and click the **Move Up** button.

Tutorial

<div style="text-align: right; font-size: 2em; font-weight: bold">2</div>

- To move a rule lower in the list (so it is applied later), select it in the grid and click the **Move Down** button.

Note When generation of signatures is disabled, you may still edit the rules but they will not be applied.

When the rules 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.

Applying Rules to Messages

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

- The Transport Agent processes the 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 each instance of the **Text to Replace**; this will take into consideration the settings for detected new lines before and/or after the text. When found, the pre-generated 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.
- The Transport Agent will detect separators in reply/forward emails, and will not inject any signatures after the first separator.

Note It is not always possible to correctly identify the separator between emails. This is particularly relevant on the Apple iPhone™ and Apply iPad™, which do not insert identifiable characters to separate emails.

For more information about the Email Signature Manager Transport Agent, please refer to this topic.

Manage Transport Agent Rule

The Manage Transport Agent Rules dialog is used to create or modify a Transport Agent Rule. It is opened using either the **Add...** or **Edit...** button on the Transport Agent Rules dialog.
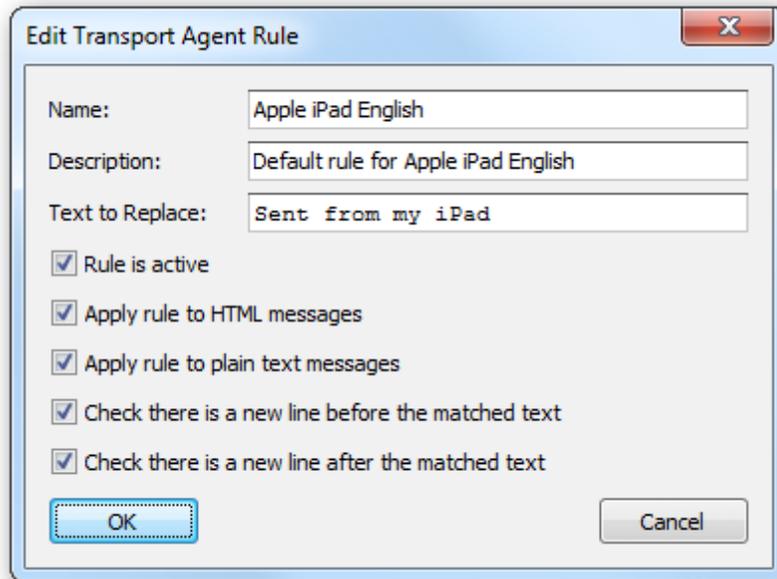
Each Transport Agent Rule has the following properties that can be modified:

Name	Description
Name	The name of the rule.
Description	A description of the rule.
Text to Replace	The text 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.
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.
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 **Close** button to close the dialog without saving changes.

Deployment

<div style="text-align: right; font-size: 2em; font-weight: bold;">3</div>

This chapter explains how to set up the deployment of signatures and settings created with Symprex Email Signature Manager.

The most common deployment model is to use a small command line utility, `sign.exe`, which runs locally on each user's computer (typically during logon) and connects to the central Email Signature Manager database in order to perform the following deployment actions:

- Deploy the user's signatures, stationery and client settings locally to Outlook.
- Deploy the user's signature to OWA on Exchange Server.
- Deploy the user's signature to Office 365.
- Deploy the user's signature to the Blackberry Enterprise Server database.
- Generate the user's signature for the Email Signature Manager Transport Agent to apply to emails sent from mobile devices.

There are two ways to set up the usage of `sign.exe` for the users in your organization:

- Using Logon Script (the logon script executes `sign.exe` when the user logs on).
- Using Group Policy (a small MSI package installs `sign.exe` to be executed when the user logs on).

Using the Logon Script method is simplest and therefore also recommended for evaluation of Email Signature Manager.

There are two ways to configure the central database:

- Using the Email Signature Manager database.
- Using a Microsoft SQL Server database.

Using the Email Signature Manager database is simplest and therefore also recommended for evaluation of Email Signature Manager.

To get started, please follow these steps:

1. Create the central shared folder.

2. Configure Email Signature Manager to connect to your database.

3. Configure the deployment via logon script or group policy.

Service Deployment

The Email Signature Manager Deployment Service is used to perform the majority of deployment actions otherwise undertaken by `sign.exe`. Instead of running on each user's computer, the service is installed on a server (i.e. a central location within your organization's domain), and performs signature deployment and generation at configurable intervals. The primary benefit of using the service is that it can deploy signatures to users who do not log on to the domain and hence are unable to run `sign.exe`. The service can perform all of the deployment actions detailed above *except* deployment to Outlook, which must still be accomplished using `sign.exe`. Indeed, `sign.exe` will *only* deploy to Outlook when the service is enabled; all other deployment actions are handled by the service.

Deployment 3

Mobile Devices

Signatures are applied to emails sent from mobile devices (excluding Blackberry devices) using the Email Signature Manager Transport Agent, which processes emails centrally on each Exchange Server within your organization. The Transport Agent needs to be installed and configured if you want to apply signatures to emails sent from your users' Android, iPhone, iPad and Windows Mobile devices.

Additional Information

For information about setting up the Deployment Service, please see the topic about deployment via the Email Signature Manager Service.

For information about setting up the Transport Agent, please see the topic about deployment via the Email Signature Manager Transport Agent.

For information about setting up a Email Signature Manager database on Microsoft SQL Server, please see the topic about using Microsoft SQL Server.

Creating the Shared Folder

This topic explains how to set up the central shared folder for deployment of signatures and settings created with Symprex Email Signature Manager.

Note If you specifically want to set up deployment via Group Policy *and* to use Microsoft SQL Server for the database, you do *not* need to follow any of the steps below.

Please follow these steps:

1. On your chosen server, create a new network share; it is recommended to create a hidden share, which is done by ending the share name with a dollar sign ($).

2. Set the following permissions on the network share:

   Users and Groups must have *allow* **Read** and **Change** rights on the network share.

   ➔ When using Microsoft SQL Server for the database, the **Change** right is not required.

3. Set the following permissions on the directory:

   Users and Groups must have *allow* **Read & Execute**, **List Folder Contents**, **Read** and **Write** rights on the directory.

   ➔ When using Microsoft SQL Server for the database, the **Write** right is not required.

4. Copy `settings.mdb` from the `Deployment` directory where Email Signature Manager is installed to the network share.

   Users and Groups will automatically have the appropriate inherited rights from the holding directory.

➔ When using Microsoft SQL Server for the database, skip this step.

5. Copy `sign.exe` from the `Deployment` directory where Email Signature Manager is installed to the network share.

Users and Groups will automatically have the appropriate inherited rights from the holding directory.

➔ When using Group Policy for deployment, skip this step.

Note: Users of versions 5.0.x and 5.1.0 will notice that `SignMAPI32.exe` and `SignMAPI64.exe` are no longer present in the `Deployment` directory. This is because they are now contained with `sign.exe` itself. If present, you may delete them from your shared folder.

6. Set the following permissions on the executable files:

Users and Groups must have *deny* **Write** right on the `sign.exe`, `SignMAPI32.exe` and `SignMAPI64.exe` executable files.

➔ When using Group Policy for deployment, skip this step.

7. Configure Email Signature Manager to connect to the database on the network share; refer to the Settings Database dialog.

➔ When using Microsoft SQL Server for the database, skip this step and see the topic on using Microsoft SQL Server.

Additional information:

By default Email Signature Manager is installed to `C:\Program Files\Symprex\Email Signature Manager`.

Deployment via Logon Script

In order to deploy signatures and settings via your logon script, simply call `sign.exe` located on the network share. For example, if the shared folder containing the Symprex Email Signature Manager files is on a server called `SERVER` in a hidden share called `SIGNMGR$`, execute the following command from your logon script:

```
\\SERVER\SIGNMGR$\sign.exe
```

If the settings database `settings.mdb` is stored in the same directory as `sign.exe`, no command-line parameters or settings are required as `sign.exe` will automatically use the database in that directory.

If, however, the settings database is not stored in the same directory as `sign.exe`, or if you are using Microsoft SQL Server, it is necessary to tell `sign.exe` how to connect to the database, which can be accomplished using one of the following methods:

Deployment

3

- Specify the appropriate [command line arguments](#).
- Create a configuration file `sign.ini` and place it in the same directory as `sign.exe`; see [saving the connection settings](#).

The result of the deployment to each user is logged to the Email Signature Manager database and is available via the [Status Monitor](#). In the event of any problems that prevent `sign.exe` from logging results to the database, a log of output and error information can be found in the user's default TEMP directory on the user's machine. To open the log, simply open the file `%TEMP%\sign.log`.

NETLOGON

Using NETLOGON is not recommended, but is possible and works in the same way as using logon script, except that the deployment files are placed in, and called from, the NETLOGON folder.

Note Because the NETLOGON folder is replicated between domain controllers across your organization, you must **not** put the settings database in the NETLOGON folder; it must be placed in a separate, shared folder that is not replicated and on which the users in your organization have read/write access.

In all other regards, using the NETLOGON folder is the same as using a shared folder. A suitable script is created to execute `sign.exe`, which is then executed as part of the logon process. You can specify the database connection settings on the command line or via a `sign.ini` file.

Deployment via Group Policy

Deployment via Group Policy installs `sign.exe` and an associated `sign.ini` file on to each user's computer using an MSI package, removing the need to call `sign.exe` from a logon script. The following guidelines can be used to deploy signatures using this method:

1. Download the latest MSI package from the Symprex website:

   http://www.symprex.com/products/msm/link/msi.asp

2. Place the MSI package in a shared location to which your domain users have access.

3. Create a configuration file `sign.ini` and place it in the same directory as the MSI package; see [saving the connection settings](#).

4. Using Group Policy Manager, define a new rule for deploying the MSI package to the appropriate domain users (details on how to accomplish this are out of the scope of this documentation; if you need assistance with this please contact the Symprex support team).

Once the group policy has been configured in your domain, the `sign.exe` deployment tool will be automatically installed on each user's machine. During this process, the `sign.ini` file created in step 3 will also be copied to the installation folder (normally `C:\Program Files\Symprex\Email Signature Manager Sign`). Subsequently, when the user logs on, `sign.exe` will be automatically run and connect to the database specified in the configuration file to deploy signatures and settings.

Deployment

3

Deployment via the Email Signature Manager Service

The Email Signature Manager Deployment Service performs the following tasks from a central location:

- Deployment of signatures to OWA within your organization.
- Deployment of signatures to Office 365.
- Generation of mobile device signatures delivered through the Transport Agent.

This is useful for including users who do not logon to the domain (where `sign.exe` will not run for those users) or if your organization does not require deployment of signatures to Microsoft Outlook.

Note The service does not deploy signatures to Outlook; you **must** continue to use `sign.exe` for deployment of signatures to Outlook.

Note The service does not support deployment of signatures to Exchange Server 2003 using WebDAV as the OWA deployment method; you **must** use MAPI as the deployment method.

To install the service, please perform the following steps:

1. Download the Email Signature Manager Deployment Service setup package from the Symprex website.

2. Install the service on to the most appropriate central computer; this computer **must** also have Email Signature Manager installed.

3. Create an account for the service to run under; this account must be given the appropriate permissions, depending on the version of Exchange Server you are using:

   - Exchange Server 2013
   - Exchange Server 2010
   - Exchange Server 2007
   - Exchange Server 2003

4. If you are using Exchange Server 2010 or Exchange Server 2013, create a suitable policy to disable throttling for the service account.

5. With the service installed, start Email Signature Manager. To complete configuration, click the **Configure Service** button, in the **Settings** group of the **Configuration** ribbon on the main application window to open the Configure Service dialog.

Important The service must only be installed on one computer.

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:

Deployment   3

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 in v6.x

Permissions for the Service Account on Exchange Server 2010

Permissions requirements for the service account on Exchange Server 2010 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 in v6.x

Permissions for the Service Account on Exchange Server 2007

Permissions requirements for the service account on Exchange Server 2007 are:

- **Receive As**

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

1. Open the **Exchange Management Shell** and connect to Exchange Server.

2. Type the following line, and then press **ENTER**:

```
Get-MailboxServer <Exchange2007> | Add-ADPermission -User <Account> -
AccessRights GenericRead, GenericWrite -ExtendedRights Receive-As
```

where *<Exchange2007>* is the name of the Exchange Server and *<Account>* is the name of the service account to which the permissions will be assigned.

If inheritance to the individual stores is not enabled, to set the required permissions at the store level, follow these steps:

1. Start the **Exchange Management Shell**.

2. Type the following line, and then press **ENTER**:

```
Get-MailboxDatabase <MailboxDatabase> | Add-ADPermission -User <Account> -
AccessRights GenericRead, GenericWrite -ExtendedRights Receive-As
```

where *<MailboxDatabase>* is the name of the mailbox database and *<Account>* is the name of the service account to which the permissions will be assigned. If *<MailboxDatabase>* is omitted, the rights will be assigned to *all* databases in your organisation.

Note The service account must be a member of the **Domain Users** group only. Membership of the **Domain Admins** group or any of the built-in Exchange security groups may deny required permissions.

Permissions for the Service Account on Exchange Server 2003

Permissions requirements for the service account on Exchange Server 2003 are:

- **Receive As**
- **Administer information store**

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

1. Click **Start** > **Programs** > **Microsoft Exchange** > **System Manager**.
2. Select **Administrative Groups** > **First Administrative Group** > **Servers**.
3. Right-click the Microsoft Exchange Server name and then click **Properties**.
4. On the **Security** tab, add and select the account to assign the required permissions to.
5. Select the following permissions from the **Permissions** list:
     Receive As
     Administer information store
6. Click the **Advanced** button.
7. Verify that the **Select the Allow inheritable permissions from parent to propagate to this object and all child objects** option is selected.
8. Click **OK**.
9. Repeat the preceding steps for each Exchange Server that will be accessed by Symprex Email Signature Manager.

Note The service account must be a member of the **Domain Users** group only. Membership of the **Domain Admins** group or any of the built-in Exchange security groups may deny required permissions.

Deployment 3

Exchange Server 2010 and 2013 Client Throttling Policies

In order for the Email Signature Manager Deployment Service to function correctly on Exchange Server 2010 and 2013, 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**, 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**, 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-Mailbox <Account> -ThrottlingPolicy <Policy>
```

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.

Using Microsoft SQL Server

This topic explains how to use Microsoft SQL Server for the Symprex Email Signature Manager database.

Please follow these steps:

1. Download the script to create the Email Signature Manager database on your SQL Server from the Symprex website:

   http://www.symprex.com/support/files/symprex/msm/signdbssql.zip

   This zip file contains one file, `signdbs.sql`, which should be extracted to a known location.

2. Using SQL Server Management Studio, create a new database on your SQL Server for Email Signature Manager according to your organization's policy. The database can be given any name.

Deployment

3. Remaining in SQL Server Management Studio, open the `signdbs.sql` script and change the `[USE]` statement on the first line to point to the database created in step 2.

4. Execute the script modified in step 3, which will create the database structure.

5. Configure permissions on the tables in the database created in step 2. Email Signature Manager supports using both Windows Authentication and SQL Server Authentication:

   When using SQL Server Authentication, add each SQL logon to the **db_datareader** and **db_datawriter** roles for the database.

   When using Windows Authentication, add each user of the product to the **db_datareader** and **db_datawriter** roles for the database.

   Note: It is recommended that **SQL Server Authentication** is chosen, as it keeps assigning permissions as simple as possible by creating a single, dedicated logon for just the Email Signature Manager database. This logon can then be re-used amongst all of the components of the product that require database access.

   Note: The **db_datareader** role gives a logon/user SELECT permissions on all tables/views in the database, and the **db_datawriter** role gives a logon/user INSERT, UPDATE and DELETE permissions. Please review this MSDN article for more information.

6. Configure Email Signature Manager to connect to the database using the Settings Database dialog.

7. If you have templates and settings in an existing database, this data can be imported to the SQL Server database using the Import Database dialog.

8. Configure `sign.exe` to connect to your SQL Server database by supplying the appropriate command line arguments or by placing a `sign.ini` configuration file in the same directory as `sign.exe` (or the MSI package); see saving the connection settings.

Deployment 3

Command Line Arguments for sign.exe

The deployment command line utility `sign.exe` accepts the following command line arguments:

Switch	Description
`/type=<database`	Specifies the type of the database to which the utility is connecting. The available values are as follows: 0 = Microsoft Access (the default value) 1 = Microsoft SQL Server using Windows Authentication 2 = Microsoft SQL Server using SQL Authentication
`/database=<name`	Specifies the name of the database to which the utility will connect. For Microsoft Access databases, this should be the full path to the database file (e.g. `\` `\SERVER\SHARE\settings.mdb`). For Microsoft SQL Server, this should be the name of the database on the specified server.
`/server=<name>`	Specifies the name of the Microsoft SQL Server to which the utility will connect.
`/user=<name>`	When connecting to a Microsoft SQL Server database using SQL Authentication, specifies the logon name for the connection.
`/password=<pass`	When connecting to a Microsoft SQL Server database using SQL Authentication, specifies the password for the connection. When connecting to a Microsoft Access database that is password-protected, specifies the password to use.
`/showwindow`	Show the log window during deployment.
`/apppath=<path>`	Specifies the path for the application to search for files (the default assumes the current path from where `sign.exe` is started). The utility will first look for the configuration file `sign.ini` and, if not found, the settings database `settings.mdb`.

Note The settings.mdb database that is included with Email Signature Manager is in Microsoft Access format.

For users of previous versions of Email Signature Manager (prior to v5.0) the following points should be noted:

- The `/verbose` switch has been replaced by `/showwindow`.
- The `/debug` switch is no longer available.

Save and Load Connection Settings

Saving the database connection settings to a file allows you to easily create the `sign.ini` file that can be used with the command line deployment tool `sign.exe` to specify the central database, instead of specifying this using command line arguments. It also allows you to create a file in a shared location that can be used by new users of Email Signature Manager to quickly configure Email Signature Manager to connect to the central database by loading the database connection settings from the file.

To create a new configuration file containing the connection settings in use by Email Signature Manager:

1. Click the **Save Connection Settings** button in the **Database** group of the **Configuration** ribbon on the main application window.
2. Enter the name of the configuration file to be created and select the location to save the file to.
3. Click the **Save** button to save the file or the **Cancel** button to cancel without saving the file.

To load an existing configuration file containing the connection settings for Email Signature Manager to use:

1. Click the **Load Connection Settings** button in the **Database** group of the **Configuration** page of the ribbon.
2. Select the configuration file to be loaded., and click the **Open** button to continue or the **Cancel** button to cancel without loading the file.
3. The settings contained in the specified file will be loaded and displayed in the Settings Database dialog .

Deployment via the Email Signature Manager Transport Agent

The Email Signature Manager Transport Agent is used to process emails sent from your users' Android, iPhone, iPad and Windows Mobile devices[1]. Unlike the deployment to other platforms (such as Outlook and OWA, 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 by the Transport Agent during delivery through your organization's Exchange Server. This is accomplished by defining a set of rules that allow the Transport Agent to identify where in each email the signature should be injected.

Important The Email Signature Manager Transport Agent can only used in conjunction with Microsoft SQL Server. If you are currently using the Email Signature Manager database, you will need to migrate; please refer to this topic for instructions on migrating the database to SQL Server.

Note The Email Signature Manager Transport Agent can only used in conjunction with on-premise Exchange Server; it cannot be used in an off-premises environment, such as Office 365 or other hosted Exchange platforms.

Basic Architecture

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

- The Email Signature Manager 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 pre-generated either by `sign.exe` or the Email Signature Manager Deployment Service.

- The administrator defines the rules for identifying where signatures should be injected into emails.

Deployment   **3**

- 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 pre-generated 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. If you haven't already, configure Email Signature Manager to use Microsoft SQL Server.

2. Install the Transport Agent on to the appropriate Exchange Server(s) and complete configuration.

3. If you are using the Email Signature Manager Deployment Service, configure the interval for generating signatures.

4. Configure which your users will receive mobile signatures in the Manage Deployment dialog.

5. Define the rules used by the Transport Agent and enable signature generation.

---

[1] The Transport Agent can also be used to process emails sent from Blackberry devices where appropriate; only Blackberry Enterprise Server v5.x is natively supported by Email Signature Manager.

Installing the Transport Agent

The Email Signature Manager Transport Agent needs to be installed on to each Exchange Server in your organization that is responsible for the transport of emails within your organization. It is easy to identify the servers on to which the Transport Agent must be installed:

- On Exchange Server 2007 and 2010.
- On Exchange Server 2013.

Installing the Transport Agent on Exchange Server 2007 and 2010

On Exchange Server 2007 and 2010, the Transport Agent must be installed on each server that has the **Hub Transport** role installed.

Note For further information about the Hub Transport role, please refer to the appropriate Technet articles for Exchange Server 2007 and Exchange Server 2010.

To install the Transport Agent on Exchange Server 2007 and 2010, 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 Hub Transport 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.

Installing the Transport Agent on Exchange Server 2013

On Exchange Server 2013, the Transport Agent must be installed on each Exchange Server that has the **Mailbox Server** role installed.

Note For further information about the Mailbox Server role, please refer to this Technet article for Exchange Server 2013.

To install the Transport Agent on Exchange Server 2013, 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.
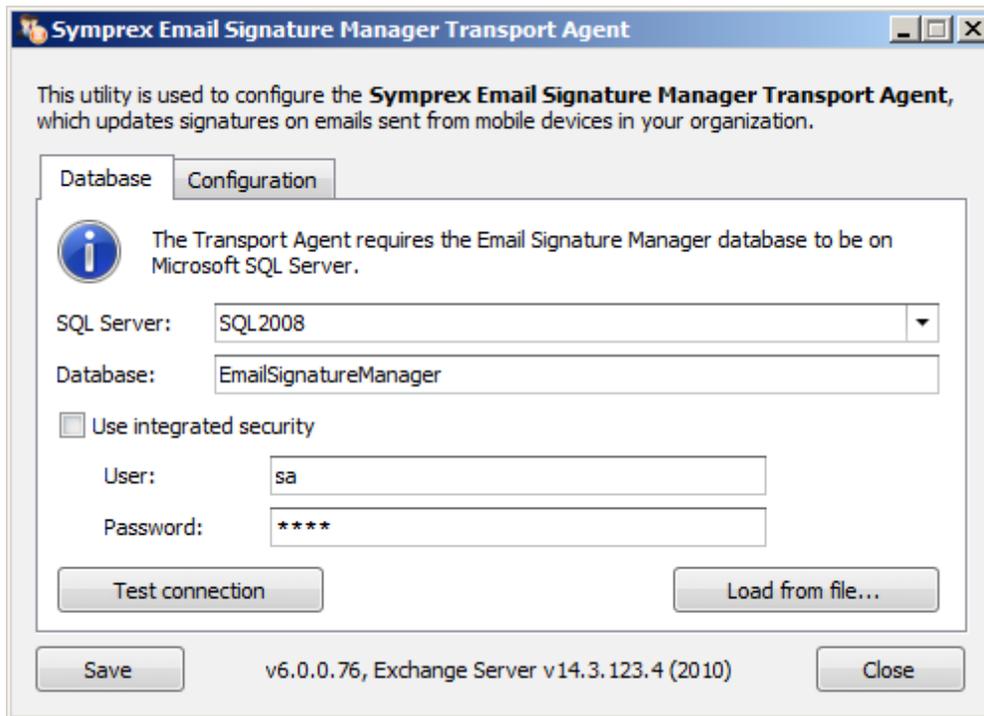
Configuring the Transport Agent

The Transport Agent is configured using the installed Configuration Utility, which can be started through 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

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

Deployment

3

The Transport Agent only supports Microsoft SQL Server. Configure the following settings as required:

- **Server**: Enter the name of the server where the database is located or select it from the drop-down list of available servers.
- **Database**: Enter the name of the database on the server.
- **Use integrated security**: Check this option to allow the Transport Agent to connect to the database using integrated Windows security.
- **User**: When using SQL Security, enter the login to connect to the server.
- **Password**: When using SQL Security, enter the password for the login.

Note It is recommended that **SQL Server Authentication** is used for the Transport Agent; Integrated security is not normally suitable because the Exchange Transport service will be running under a built-in account and hence cannot be configured as a user on SQL Server.

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

Note that in order to simplify configuration, the settings for connecting to the database can be saved from Email Signature Manager and loaded by clicking the **Load from file...** button.

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

Configure Settings

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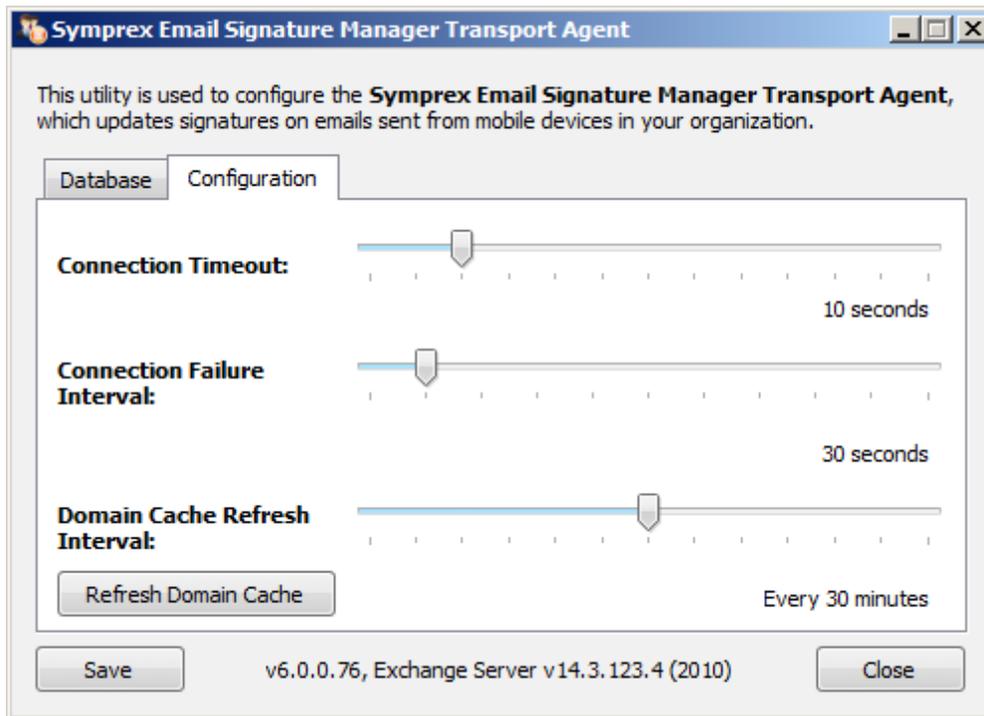
- **Connection Timeout:** Specifies the timeout for connecting to SQL Server when processing an email. It is recommended that this timeout is kept fairly short as connections should be made quickly under normal operating conditions.

- **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 needs processing. This interval species how often the cache should be refreshed. If necessary, the cache can be refreshed on demand by clicking the **Refresh Domain Cache** button.

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:

Deployment

3

```
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,

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

Appendices **4**

This section contains additional information for using Symprex Email Signature Manager.

Template Fields

The below template fields are the standard template fields in Symprex 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

This section of the help file describes how Symprex 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 **File** tab in the main application window 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).
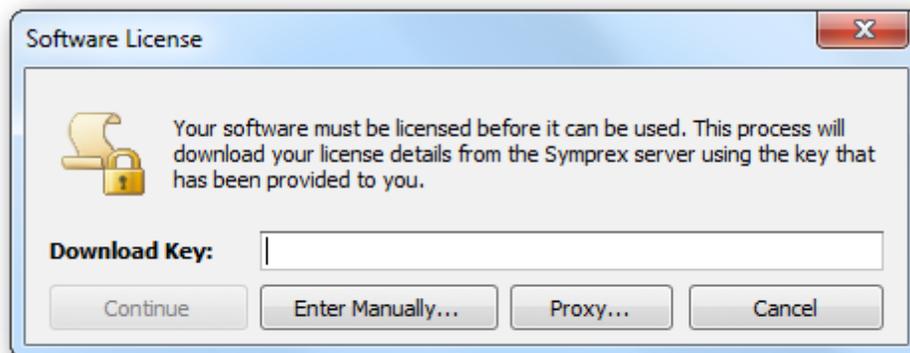
When you purchased the license for your software, you should have been provided with a unique download key. Enter this key into the **Download Key** textbox and click the **Continue** button. The software will then connect to the Symprex licensing server to download and install your license.

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 distributor 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.

Licensing
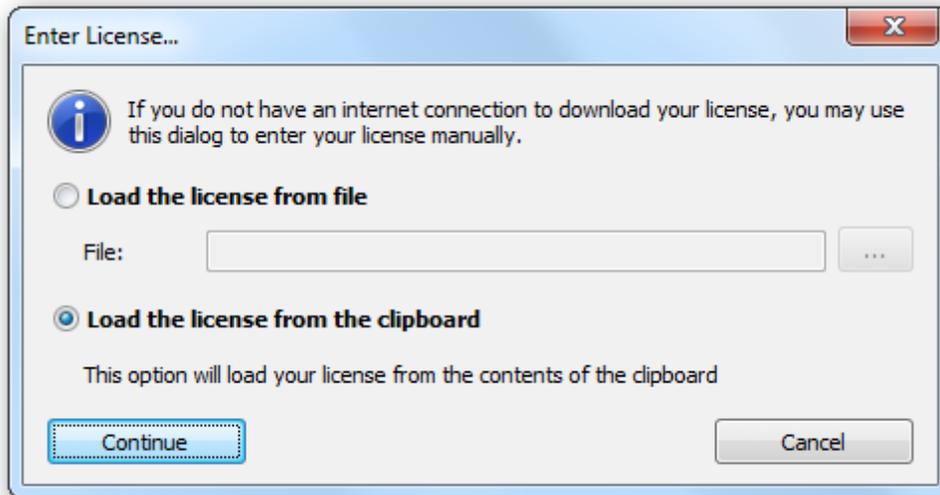
- If you have been provided with a file containing your license, select **Load the license from file** and locate the appropriate file.
- If you have been provided with a text-based version of your license (for example, in an e-mail), copy the text into the clipboard.

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 distributor 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.
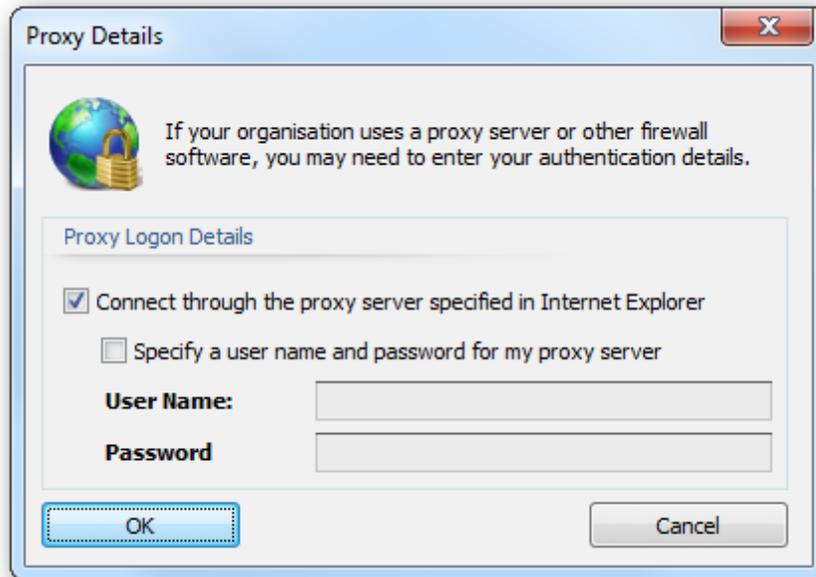
To connect through your default proxy server using your Windows logon credentials, check the **Connect through the proxy server specified in Internet Explorer** checkbox. If you need to specify your authentication details, check the **Specify a user name and password for my proxy server** checkbox, and 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.
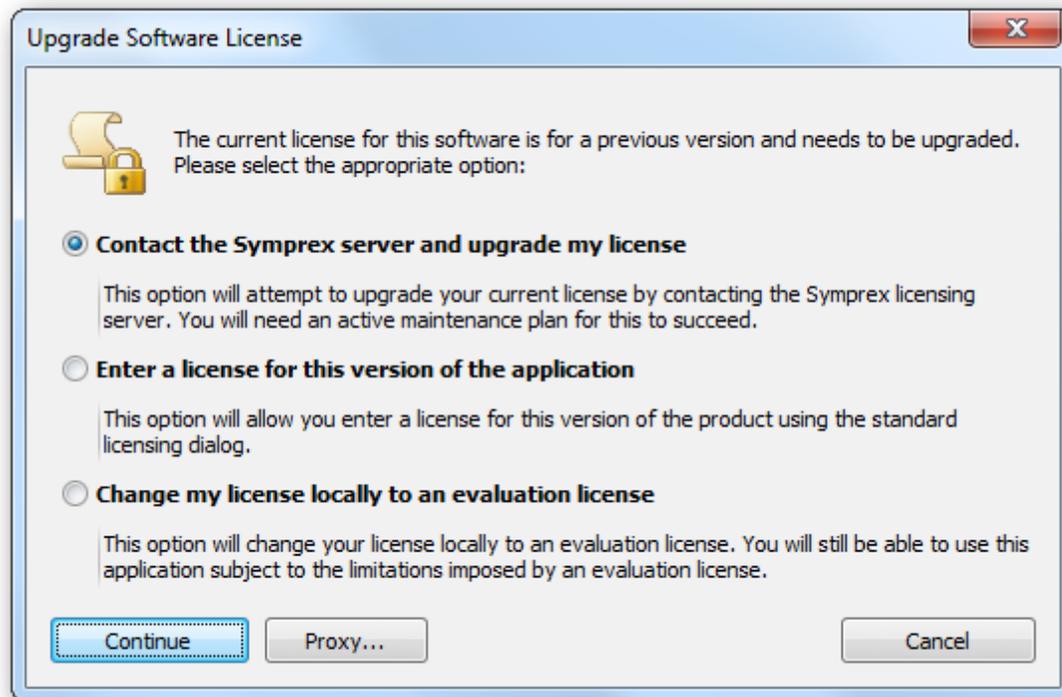
Licensing 5

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 your distributor 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

<div style="text-align:right">**6**</div>

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, email addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Symprex Limited.

Symprex may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Symprex, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 2014 Symprex Limited. All Rights Reserved.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Published: July 2014
Applies To: Symprex Email Signature Manager 6.1.0

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:
http://www.symprex.com

If you experience technical problems with one of our products, please visit our support page:
http://www.symprex.com/support

Contact Us by Email

Please email general enquiries about Symprex or our products to:
info@symprex.com

Please email sales enquiries to:
sales@symprex.com

Please email support enquiries to:
support@symprex.com

Contact Your Local Reseller or Distributor

Symprex has partners and resellers in most countries. You can find your local reseller here:
http://www.symprex.com/partners/resellers

Alternatively, check for an authorised distributor here:
http://www.symprex.com/partners/distributors