One Identity Manager 8.1.4

# Secure Password Extension Administration Guide

**Legend**

**WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.**

**CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

One Identity Manager Secure Password Extension Administration Guide
Updated - 19 October 2020, 07:32
Version - 8.1.4

# Contents

# 1

# Secure Password Extension

It is very common for business users to forget their password and be unable to log in to the system. One Identity Manager allows users to securely and conveniently reset their network passwords, or manage their passwords in multiple enterprise systems, before even logging in to the system. To enable users to access the Password Reset Portal from the Windows login screen, One Identity Manager implements Secure Password Extension.

Secure Password Extension is an application that provides one-click access to the complete functionality of the Password Reset Portal from the Windows login screen. Secure Password Extension is included on the installation CD and is deployed through a group policy. For information on how to deploy and configure Secure Password Extension on end-user workstations in the managed domain, see Deploying and configuring Secure Password Extension on page 5.

Secure Password Extension supports the authentication model in the following systems:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10

On workstations running Windows 7, Secure Password Extension adds the **Forgot My Password** link to the Windows login screen. In Windows 8, 8.1 and 10, Secure Password Extension adds an icon under the login options to the user tile on the login screen. By clicking these buttons and links, users open the Password Reset Portal.

When users connect to the Password Reset Portal from the Windows login screen, anonymous access is enabled and the functionality of Microsoft Internet Explorer is restricted, thereby preventing the actions that may pose a security threat. Once users open the Password Reset Portal home page from the Windows login screen, they cannot access any other website, or open a new browser window or a context menu.

For Secure Password Extension to function properly, you must specify the corresponding URL to the Password Reset Portal in the supplied administrative template `prm_gina.adm` or `prm_gina.admx` located in the `\Password Manager\Setup\Administrative Template\` folder of the installation CD and apply the template to selected users. For more information, see Configuring Secure Password Extension on page 7.

# 2

# Deploying and configuring Secure Password Extension

This section describes the prerequisites and steps for deploying and configuring Secure Password Extension to provide access to the Password Reset Portal from the Windows login screen on end-user computers.

**Detailed information about this topic**



## Configuring the Password Reset Portal

To ensure that forwarding to the Password Reset Portal works correctly, you must configure the Password Reset Portal (server-sided configuration).

***To configure the forwarding to the Password Reset Portal***

1. Start Internet Information Services Manager.
2. Navigate to the Password Reset Portal entry.
3. Right-click the Password Reset Portal entry and in the context menu, click **Explore**.
4. In the Explorer window, create the subfolder `EntryPoint`.
5. Open the subfolder `EntryPoint` and create the `web.config` file.
6. Edit the `web.config` file and insert the following content:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
    <system.webServer>
        <httpRedirect enabled="true" destination="<URL-path-to-the-Password-
Reset-Portal>" exactDestination="true" />
    </system.webServer>
</configuration>
```

7. Save the file changes.

# Deploying Secure Password Extension

Secure Password Extension is deployed on client computers through a group policy. You can create a new group policy object (GPO) or use an existing one to assign the installation package with Secure Password Extension for installing it on the destination computers. Secure Password Extension is then installed on computers to which the GPO applies. Depending on the operating system running on the destination computers, you must apply one of the following installation packages included on the installation CD:

- `SecurePasswordExtension_x86.msi` - Installs Secure Password Extension on computers running **x86** versions of operating systems.
- `SecurePasswordExtension_x64.msi` - Installs Secure Password Extension on computers running **x64** versions of operating systems.

You can modify the behavior and on-screen appearance of Secure Password Extension components by configuring the settings of an administrative template, and then applying the template to the target computers through a group policy.

The administrative template is available in two formats: `prm_gina.adm` and `prm_gina.admx`.

The `prm_gina.adm` administrative template file is located in the `Modules\ADS\dvd\AddOn\SecurePasswordExtension\Administrative Template` folder of the installation CD. Before using the file, copy it from the installation CD. The recommended target location is the `\inf` subfolder of the Windows folder on a domain controller.

The `prm_gina.admx` administrative template file is located in the `Modules\ADS\dvd\AddOn\SecurePasswordExtension\Administrative Template` folder of the installation CD. This administrative template is designed to be used with Windows Server 2008 R2 or later operating systems. Before using this administrative template, copy the `prm_gina.admx` and `prm_gina.adml` files from the installation CD to the following locations: `%systemroot%\policyDefinitions` (for the `prm_gina.admx` file) and `%systemroot%\policyDefinitions\En-US` (for the `prm_gina.adml` file).

Follow these steps to configure and deploy the Secure Password Extension on end-user computers.

***To deploy and configure Secure Password Extension***

1. Copy the required installation package (`SecurePasswordExtension_x86.msi` or `SecurePasswordExtension_x64.msi`) from the installation CD to a network share accessible from all domain controllers where you want to install Secure Password Extension. The MSI packages are located in the `Modules\ADS\dvd\AddOn\SecurePasswordExtension` folder of the installation CD.
2. Create a GPO and link it to all computers, sites, domains, or organizational units where you want to use Secure Password Extension. You may also choose an existing GPO to use with Secure Password Extension.
3. Open the GPO in the Group Policy Management Editor, and perform the following actions:
    a. Expand **Computer Configuration** | **Policies** | **Software Settings**.
    b. Right-click **Software installation** and select **New** | **Package**.
    c. Browse for the MSI package you have copied in step 1, and click **Open**.
    d. In the **Deploy Software** window, select a deployment method and click **OK**.
    e. (Optional) Verify and configure the properties of the installation.

### Related topics

- Uninstalling Secure Password Extension on page 20

# Configuring Secure Password Extension

This section describes how to override automatic location of the Password Reset Portal and customize Secure Password Extension.

### Detailed information about this topic

- Specifying the Password Reset Portal location on page 7
- Customizing the logo for Secure Password Extension on page 9
- Customizing position of the Secure Password Extension window on page 10

# Specifying the Password Reset Portal location

You must manually specify the URL path of the Password Reset Portal.

***To specify the Password Reset Portal location on a computer running Windows Server 2008 R2 or later***

1. In Windows, click **Start** and open the **Run** application.
2. In the **Run** dialog, enter `mmc` and click **OK**.
3. In the **Console** window in the **File** menu, click **Add/Remove Snap-in**.
4. In the **Add or Remove Snap-ins** dialog in the list of available snap-ins, double-click **Group Policy Management Editor**.
5. In the **Group Policy Wizard** window, click **Browse**, select **Default Domain Policy**, and click **OK**.
6. Click **Finish**.
7. In the **Add or Remove Snap-ins** dialog, click **OK**.
8. In the **Console** window in the left pane, expand **Default Domain Policy** | **Computer Configuration**.
9. Right-click the **Administrative Templates** node and select **Add/Remove Templates**.
10. In the **Add/Remove Templates** dialog, click **Add**.
11. In the file browser, browse for the `prm_gina.adm` or `prm_gina.admx` file, select it, and then click **Open**.
12. In the **Add/Remove Templates** dialog, click **Close**.
13. Perform one of the following actions:
    - If you used the `prm_gina.admx` file: In the **Console** window under **Computer Configuration**, select the **Administrative Templates** node and then, on the right pane, double-click the **One Identity Password Manager** template.
    - If you used the `prm_gina.adm` file: In the **Console** window under **Computer Configuration**, select the **Classic Administrative Templates (ADM)** node and then, on the right pane, double-click the **One Identity Password Manager** template.
14. Double-click **Generic Settings**.
15. Double-click **Specify URL path to the Self-Service site**.
16. In the **Specify URL path to the Self-Service site** window in the **Settings** tab, select the **Enabled** option.
17. In the field, enter the URL path to the Password Reset Portal.
18. Click **OK**.
19. Double-click **Override URL path to the Self-Service site**.
20. In the **Settings** tab, select the **Enabled** option.
21. Click **OK**.
22. Apply the updated policy to the computers in the managed domain.

NOTE: Application of the updated policy to the computers in the managed domain may take some time to complete.

# Customizing the logo for Secure Password Extension

You can change the logo for Secure Password Extension that is displayed on end-user computers.

***To deploy a custom logo for Secure Password Extension on end-user computers***

1. Create a startup script to deploy your logo image.

   TIP: See the sample script following this procedure.

2. Create your logo image file and place it on a network share that is accessible to all network hosts on which the script is run.
3. In Windows, click **Start** and open the **Run** application.
4. In the **Run** dialog, enter `gpmc.msc` and click **OK**.
5. In the **Group Policy Management Editor** window, open the GPO that includes the `prm_gina.adm` administrative template.
6. Expand **Computer Configuration** | **Administrative Templates** | **One IdentityPassword Manager** | **Pre-Windows Vista Settings** and click **Secure Password Extension Logo**.
7. Enable the **Set dialogue background image** policy setting by specifying a local path to the logo image file on end-user computers.

   NOTE: The local path you specify in these policy settings must be the same as in the startup script specified later in this section.

8. Expand **Computer configuration** | **Windows Settings** and click **Scripts (Startup/Shutdown)**.
9. In the right pane, double-click **Startup**.
10. In the **Startup Properties** window, click **Add**.
11. In the **Add a Script** dialog, click **Browse** and browse for the script file you have created in step 1.
12. Specify the script parameters.
13. Click **OK**.

The following example startup script is a batch file that runs on end-user computers during the system startup, and copies the custom logo image from the network share to a local folder:

IMPORTANT: `[SharedDir]` is a shared domain directory that must be available during startup.

The script lines containing target paths must be entered as a single line. The lines are wrapped in this article only for readability purposes.

```
@echo off
rem "SPE startup script"
rem *Check target directory existence*
if exist "c:\Program Files\One Identity\Secure Password Extension"
goto :COPY_FILE
md "c:\Program Files\One Identity\Secure Password Extension"
rem *Copy BMP image - %1*
:COPY_FILE
copy [SharedDir]\%1 "c:\Program Files\One Identity\Secure Password
Extension\"
rem pause
:out
@echo off
rem "SPE startup script"
rem *Check target directory existence*
if exist "c:\Program Files\One Identity\Secure Password Extension"
goto :COPY_FILE
md "c:\Program Files\One Identity\Secure Password Extension"
rem *Copy BMP image - %1*
:COPY_FILE
copy [SharedDir]\%1 "c:\Program Files\One Identity\Secure Password
Extension\"
rem pause
:out
```

# Customizing position of the Secure Password Extension window

You can specify the position of the Secure Password Extension window on the login screen of end-user computers.

***To change the position of the Secure Password Extension window on end-user computers***

1. In Windows, click **Start** and open the **Run** application.
2. In the **Run** dialog, enter `gpmc.msc` and click **OK**.
3. In the **Group Policy Management Editor** window, open the GPO that includes the `prm_gina.adm` administrative template.
4. Expand **Computer Configuration** | **Administrative Templates** | **One IdentityPassword Manager** | **Pre-Windows Vista Settings** | **Secure Password Extension Window Settings** and enable the **Set Secure Password Extension Window Position** policy by specifying the position of the Secure

Password Extension window on the Windows login screen of end-user computers.

5. Click **OK**.

# Configuring Secure Password Extension using administrative templates

The administrative template features a powerful set of options that allow you to customize the behavior and appearance of Secure Password Extension according to your requirements.

The administrative template layout includes the following folders:

- Generic Settings: Includes policy settings that can be applied to computers running Windows 8, 8.1, and 10 operating systems.
- Pre-Windows Vista Settings: Includes policy settings that can be applied to computers running only pre-Vista operating systems.
- Windows 8 Settings: Includes policy settings that can be applied to computers running Windows 8, 8.1, and 10 operating systems.

Brief descriptions of the administrative template policy settings are outlined in the following sections. For more information about policy settings, see the **Explain** tab on the **Properties** page of each policy.

### Detailed information about this topic


- Generic settings on page 11
- Pre-Windows Vista settings on page 15
- Windows 8 settings on page 16


# Generic settings

The following table outlines generic administrative template policy settings you can use to customize the behavior of Secure Password Extension.

NOTE: One Identity Manager does not support all settings displayed in the administrative template. This document only lists settings supported by One Identity Manager.

**Table 1: Generic administrative template policy settings**

| Policy name | Description |
|---|---|
| **Generic Settings** | |

| Policy name | Description |
|---|---|
| Specify URL path to the Self-Service site | Specify the URL to access the Password Reset Portal from the Windows login screen. This URL is opened when users click the **Forgot My Password** or **Manage My Password** buttons on the Windows login screen in pre-Vista operating systems, and the **Forgot My Password** command link in Windows 7 operating systems. |
| Override URL path to the Self-Service site | Enable the use of the URL to the Password Reset Portal specified in the **Specify URL path to the Self-service site** setting. |
| Maximum number of attempts to connect to the Self-Service site | Specify the maximum number of attempts to connect to the Password Reset Portal from Secure Password Extension.<br>If you disable or do not configure this policy setting, the maximum number of attempts is five. |
| Add the Forgot My Password link to credential provider tile | Enable this policy setting to add the **Forgot my password** link to the tile of the selected credential provider on the login screen.<br>You can select a credential provider from the list or specify the GUID of another credential provider. The GUID must be specified in the following format: `{00000000-0000-0000-0000-000000000000}`<br>If you disable or do not configure this policy setting, the **Forgot my password** link is added to the default Microsoft Password provider tile. |
| Create a separate tile for Secure Password Extension | Enable this policy setting to create a separate tile for Secure Password Extension on the Windows login screen. You can enable this setting when there are compatibility issues with other credential providers.<br>If you disable or do not configure this policy setting, the **Forgot my password** link is added to a default Microsoft Password provider tile or tiles of the credential provider selected in the **Add the Forgot my password link to credential provider tile** policy. |
| Refresh interval | Specify how often domain settings are refreshed for Secure Password Extension.<br>The default value is 5 minutes. If you want to reduce network load, you can increase the refresh interval. If you disable or do not configure this policy setting, the default refresh interval will be used. |
| **Proxy Settings** | |
| Enable proxy server access | Enable this policy setting to establish the connection from the Windows login screen to the Password Reset Portal through a proxy server. |
| Configure required proxy | Specify the settings required to enable proxy server access to the Password Reset Portal from the Windows login screen. |

| Policy name | Description |
|---|---|
| settings | |
| Configure optional proxy settings | Specify optional settings for the proxy server access. |
| **Shortcut Policies** | |
| Restore desktop shortcuts for the Self-Service site | Enable this policy setting to re-create the desktop shortcut to the Password Reset Portal on a user's computer by Secure Password Extension if the user deletes the desktop shortcut. |
| Do not create desktop shortcuts for the Self-Service site | Enable this policy setting if you do not want desktop shortcuts to be created by Secure Password Extension on end-user computers. |
| Do not create any shortcuts for the Self-Service site | Enable this policy setting if you do not want any shortcuts to be created by Secure Password Extension on end-user computers. |
| **Secure Password Extension Title Settings** | |
| Display custom names for the Secure Password Extension window title | Enable this policy setting to use custom titles for the Secure Password Extension window. |
| Set custom name for the Secure Password Extension window title in <Language> | Specify a custom title for the Secure Password Extension window. You can specify the title for each of the required login languages. There are 36 language-specific policy settings available.<br>The title you specify must not exceed 32 characters. If you use a hieroglyphic font, the title must not exceed 14 characters (because of hieroglyph's width). |
| **Usage Policy Settings** | |
| Display the usage policy button (command link) | Enable this policy setting to use custom usage policy buttons and command links.<br>The usage policy command link on Windows 7 operating system is displayed on the Windows login screen, and is intended to open an HTML document that describes the enterprise usage policy or contains any information that you may want to make available to end-users. |
| Set default URL | Specify a URL referring to the usage policy document that is opened by clicking the usage policy button (command link) if no login language-specific URLs are set. The default URL may refer to an HTML |

| Policy name | Description |
| --- | --- |
| | file. |
| Set name and URL for the usage policy button (command link) in <Language> | Specify the labels of the usage policy buttons (command link) and set the links to the usage policy documents that are opened by clicking the usage policy button or command link. You can specify the label and URL for each of the required login languages. There are 36 language-specific policy settings available.<br>The label you specify must not exceed 32 characters. If you use a hieroglyphic font, the label must not exceed 14 characters (because of hieroglyph's width). The length of the URL must not exceed 256 characters. |
| **Forgot My Password Settings** | |
| Display custom names for the Forgot My Password button (command link) | Enable this policy setting to use custom labels for the **Forgot My Password** button and the command link.<br>The **Forgot My Password** button (command link) opens the Password Reset Portal from the Windows login screen. On Windows 7 operating system, the command link is displayed on the Windows login screen irrespective of whether the user is logged in to the system or not. |
| Set custom name for the Forgot My Password button (command link) in <Language> | Specify a custom label for the **Forgot My Password** button (command link). You can specify the label for each of the required login languages. There are 36 language-specific policy settings available. |
| **Secure Password Extension Separate Tile Settings** | |
| Create a separate tile for Secure Password Extension | Enable this policy setting to create a separate tile for Secure Password Extension on the Windows login screen. You can enable this setting when there is a compatibility issue with other credential providers.<br>If you disable or do not configure this policy setting, the **Forgot My Password** link is added to a default Microsoft Password provider tile or tiles of the credential provider specified in the **Add the Forgot my password link to credential provider tile** policy. |
| Set tile image | Select an image that is used for the Secure Password Extension tile on the Windows login screen.<br>You can use the following image types: bmp, gif, jpg, or png. The image may have any size suitable for your requirements. The recommended size is 128 x 128 pixels.<br>If you disable or do not configure this policy setting, the default tile picture is displayed. |

| Policy name | Description |
|---|---|
| **Set Custom Names** | |
| Display custom names of the tile | Enable this policy setting to use custom titles for the Secure Password Extension tile.<br>The Secure Password Extension tile is displayed under the credential tile on the Windows login screen.<br>If you disable or do not configure this setting, the default tile title (**Secure Password Extension**) is displayed.<br>NOTE: If you disabled the **Create a separate tile for Secure Password Extension** policy setting, this policy setting has no effect. |
| Set custom tile name in <language> | Specify a custom title for the Secure Password Extension credential tile on the Windows login screen. You can specify the title for each of the required login languages.<br>If you disable or do not configure this setting, the default tile title is displayed. |

# Pre-Windows Vista settings

The following table outlines administrative template policy settings for Secure Password Extension in pre-Windows Vista operating systems.

NOTE: One Identity Manager does not support all settings displayed in the administrative template. This document only lists settings supported by One Identity Manager.

**Table 2: Settings for pre-Windows Vista OS**

| Policy name | Description |
|---|---|
| **Secure Password Extension Logo** | |
| Set dialog background image | Select an image that is used as background for the Secure Password Extension dialog that is displayed on the Windows login screen. |
| **Secure Password Extension Window Settings** | |
| Set the Secure Password Extension Window Position | Specify the position of the Secure Password Extension window on the Windows login screen of end-user computers. |
| **Manage My Password Settings** | |
| Display custom names for the Manage My Password | Enable this policy setting to use custom labels for the **Manage My Password** button. |

| Policy name | Description |
|---|---|
| button | The **Manage My Password** button opens the Password Reset Portal on pre-Windows Vista operating systems, and is displayed on the Windows login screen provided that you are logged in to the system. |
| Set custom name for the Manage My Password button in <Language> | Specify a custom label for the **Manage My Password** button. You can specify the label for each of the required login languages. There are 36 language-specific policy settings available. |

# Windows 8 settings

The following table outlines administrative template policy settings for Secure Password Extension in Windows 8, 8.1, and 10 operating systems.

NOTE: One Identity Manager does not support all settings displayed in the administrative template. This document only lists settings supported by One Identity Manager.

**Table 3: Settings for Windows 8, 8.1, and 10 OS**

| Policy name | Description |
|---|---|
| **Credential Provider's Description** | |
| Display custom description of the Secure Password Extension credential provider | Enable this policy setting to use custom descriptions for the Secure Password Extension credential provider.<br>The credential provider description is displayed when users select the Secure Password Extension credential provider in the Sign-in options under their user tiles in the login screen.<br>If you disable or do not configure this policy setting, the default language-specific description of the Secure Password Extension credential provider is displayed. |
| Set the custom description in <Language> | Specify a custom description for the Secure Password Extension credential provider. You can specify the description for each of the required login languages.<br>If you disable or do not configure this policy setting, the default language-specific description of the Secure Password Extension credential provider is displayed. |
| **Icon's Text Label** | |
| Display custom labels for the Secure Password Extension credential provider's icon | Enable this policy setting to use custom labels for the icon of the Secure Password Extension credential provider.<br>The text label for the credential provider icon is displayed in a tooltip when a user hovers over the credential provider's |

| Policy name | Description |
| --- | --- |
| | icon under the Sign-in options on the login screen.<br>If you disable or do not configure this policy setting, the default language-specific label for the Secure Password Extension credential provider's icon is displayed. |
| Set the custom label in <Language> | Specify a custom label for the icon of the Secure Password Extension credential provider. You can specify the label for each of the required login languages.<br>If you disable or do not configure this policy setting, the default language-specific label for the Secure Password Extension credential provider's icon is displayed. |
| **Link to the Self-Service Site** | |
| Display custom names of the Open the Self-Service site link | Specify a custom name for the **Open the Password Reset Portal** link. You can specify the name for each of the required login languages.<br>This link opens the Password Reset Portal from the login screen.<br>If you disable or do not configure this policy setting, the default language-specific name of the **Open the Password Reset Portal** link is displayed. |
| Set the custom names of the Open the Self-Service site link in <Language> | Specify a custom name for the **Open the Password Reset Portal** link. You can specify the name for each of the required login languages.<br>If you disable or do not configure this policy setting, the default language-specific name for the link is displayed. |

# 3

# Logging

For diagnostic purposes you can turn on logging in Secure Password Extension. The log file can contain the following information: exceptions and errors, debug messages and functions' returns, and so on. You can use this diagnostic data to identify issues with Secure Password Extension.

**CAUTION: This section describes how to modify the registry. However, incorrectly modifying the registry may severely damage the system. Therefore, you should follow the steps carefully. It is also recommended to back up the registry before you modify it.**

***To enable logging***

1. In Windows, click **Start** and open the **Run** application.
2. In the **Run** dialog, enter `regedit` and click **OK**.
3. In the **Registry Editor**, create the following key: `HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging`.
4. Add a new string value to the `HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging` registry key by performing the following actions:
    a. Click the `HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging` registry key.
    b. In the menu bar, click **Edit** | **New** | **String Value**.
    c. Enter `LogLevel` and press Enter.
    d. Right-click the **LogLevel** value.
    e. In the context menu, click **Modify**.
    f. In the **Edit String** dialog under **Value data**, enter `All`.
    g. Click **OK**.
5. Add a new string value to the `HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging` registry key by performing the following actions:
    a. Click the `HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging` registry key.
    b. In the menu bar, click **Edit** | **New** | **String Value**.

c. Enter `LogFolder` and press Enter.

d. Right-click the **LogFolder** value.

e. In the context menu, click **Modify**.

f. In the **Edit String** dialog under **Value data**, enter the path to the log file. For example, `C:\Logs`.

g. Click **OK**.

6. Exit the Registry Editor.
7. Restart the computer.

***To disable logging***

1. In Windows, click **Start** and open the **Run** application.
2. In the **Run** dialog, enter `regedit` and click **OK**.
3. In the **Registry Editor**, click the `HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Password Manager\Logging` registry key.
4. Right-click the **LogLevel** value.
5. In the context menu, click **Modify**.
6. In the **Value data** box, enter **Off**.
7. Click **OK**.

# 4

# Uninstalling Secure Password Extension

You uninstall Secure Password Extension from end-user computers by removing the appropriate installation packages assigned through a group policy. Uninstalling Secure Password Extension makes the Password Reset Portal no longer available from the Windows login screen.

***To remove an assigned MSI package***

1. In Windows, click **Start** and open the **Run** application.
2. In the **Run** dialog, enter `gpmc.msc` and click **OK**.
3. In the **Group Policy Management Editor** window, click the GPO with which you deployed the package.
4. Click **Edit**.
5. Expand the **Software Settings** container that contains the **Software installation** item with which you deployed the package.
6. Click the **Software installation** container that contains the package.
7. In the right pane of the **Group Policy** window, right-click the package name
8. In the context menu, click **All Tasks**.
9. Click **Remove**.
10. Click **Immediately uninstall the software from users and computers**.
11. Click **OK**.

# About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

## Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

## Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product