PUBLIC
SAP Single Sign-On 3.0 SP02
Document Version: 1.1 – 2020-03-17

Password Manager for SAP Single Sign-On Implementation Guide

THE BEST RUN SAP

Content

1 Password Manager

Password Manager helps you store strong passwords in a secure store for single sign-on (SSO) to applications and web sites, without the need to remember every password or click a specific logon dialog. After you have logged on to the Password Manager application, logon to applications running under the control of the system happen automatically.

The Password Manger application is a component of SAP Single Sign-On (SAP SSO).

2 Password Manager Installation Guide

Install Password Manager on your Windows PC to make logging on to web sites and Windows applications easier.

This guide enables administrators or business users with administrative rights on their PC to install Password Manager.

Related Information

System Requirements for Password Manager [page 5]
Installing Password Manager [page 6]
Installing Password Manager with Custom Security Questions for Resetting the Master Password [page 7]
Performing an Unattended Installation of Password Manager [page 9]
Upgrading Enterprise Single Sign-On to Password Manager [page 10]
Removing Your Personal Data [page 10]

2.1 System Requirements for Password Manager

The host system for Password Manager for SAP Single Sign-On (SAP SSO) must meet the hardware and software requirements listed in the following sections.

Hardware Requirements

You have 50 MB of free space on your hard drive.

Software Requirements

Software Requirements for Password Manager

Area	Requirement
Operating system	• Microsoft Windows 7 • Microsoft Windows 8 Ensure that you have tuned on the Windows feature *.NET Framework 3.5*. The .NET Framework is available for download from the Microsoft web site.
Support for Java applications	• You have downloaded and installed the Oracle Java Runtime Environment or Oracle Java Development Kit 1.6, 32-bit or 64-bit. • You have downloaded and installed Oracle Java Access Bridge 2.0.2, 32-bit or 64-bit. For more information, see the vendor documentation.

Related Information

https://service.sap.com/swdc
http://help.sap.com/nwsso30

2.2 Installing Password Manager

You want to perform a single installation of Password Manager on your computer.

Prerequisites

- You have administrator rights on the host computer.
- You have closed all SAP applications running on your computer.

Procedure

1. Download the SAP Single Sign-On Password Manager software from the Software Download Center at *SAP Service Market Place*.

2. Start `SAPSetupESC.exe` as administrator.

> **i Note**
>
> If you do not want the Password Manager to start immediately after installation, you can run it in *silent* or *no dialog* mode by typing one of the following in the *Command Prompt*:
>
> - For *Silent* Mode
>   `SAPSetupESC.exe /silent /product:ESC`
> - For *No Dialog* Mode
>   `SAPSetupESC.exe /nodlg /product:ESC`
>
> To run the Password Manager in such case, you have to choose it from the Window's *Start* menu. For more information about the installation options with `SAPSetupESC.exe`, see *SAPSetup Guide*. You can download the latest version from SAP Service Market Place.

3. Follow the on-screen instructions.

   An initialization dialog appears.
4. Enter a master password and a security question and answer for resetting the master password.
5. Save your entries.

Related Information

https://service.sap.com/swdc
System Requirements for Password Manager [page 5]
Master Password [page 35]

2.3 Installing Password Manager with Custom Security Questions for Resetting the Master Password

When installing Password Manager you can change the security questions for resetting the master password to something that is more relevant to you.

Prerequisites

You have not installed Password Manager on the host computer.

Context

Password Manager delivers a set of security questions. During installation, the installer prompts you to choose one question and enter an answer. Password Manager uses the security question and answer to reset your master password in case you forget it. There are no restrictions for the length of the answer.

Procedure

1. Download the SAP Single Sign-On Password Manager software from the Software Download Center at *SAP Service Market Place*.
2. Execute the following command in a command shell: `<path_to_installation_files>\SAPSetupESC.exe /X="<extraction_path>"`
3. Edit the file `<extraction_path>\SAPSetupEsc\Shared\SAP\signon\QuestionsList.xml`.

   Change the questions as required. Be sure to translate the questions into the other languages you want to support.

   > **i Note**
   >
   > If you make a formatting error, Password Manager loads the default questions or ignores lines with syntax errors.

4. Save your entries.
5. Execute the following command in a command shell: `<extraction_path>\Setup\NwSapSetup.exe`
6. Follow the on-screen instructions.

   An initialization dialog appears.
7. Enter a master password and a security question and answer for resetting the master password.
8. Save your entries.

Related Information

https://service.sap.com/swdc
System Requirements for Password Manager [page 5]
Master Password [page 35]
Default Security Questions for Resetting the Master Password [page 9]

2.3.1 Default Security Questions for Resetting the Master Password

The following is a list of the security questions delivered by Password Manager.

During installation, the installer prompts you to choose one security question and enter an answer. Password Manager uses the security question and answer to reset you master password in case you forget it.

- What is your mother's maiden name?
- What is the name of your favorite uncle or aunt?
- What is the last name of your favorite musician?
- What is the last name of your favorite teacher?
- What is the last name of your best childhood friend?
- What is the name of the hospital where you were born?
- What is the name of the town in which you grew up?
- What is the name of your favorite book?

In addition to English, Password Manager delivers these questions in Chinese, French, German, Japanese, Portuguese, Russian, and Spanish.

Related Information

Installing Password Manager with Custom Security Questions for Resetting the Master Password [page 7]
Master Password [page 35]

2.4 Performing an Unattended Installation of Password Manager

You want to install SAP Single Sign-On (SAP SSO) Password Manager on workstations in your landscape.

Procedure

1. Download the SAP Single Sign-On Password Manager software from the Software Download Center at *SAP Service Market Place*.
2. Configure your tools to distribute the installation files to your workstations and start the following command in a command shell: `<path_to_installation_files>\SAPSetupESC.exe /silent /Product="ESC"`

   For more information about further installation options with `SAPSetupESC.exe`, see *SAPSetup Guide*. You can download the latest version from *SAP Service Market Place*.

Results

After installation, an initialization dialog appears. The user must enter a master password and password recovery question and answer.

Related Information

https://service.sap.com/swdc
System Requirements for Password Manager [page 5]
Master Password [page 35]
Password Manager Admininstrator Guide [page 48]
https://service.sap.com/sltoolset

2.5 Upgrading Enterprise Single Sign-On to Password Manager

Enterprise Single Sign-On is a part of SAP Single Sign-On (SAP SSO) release 1.0.

You can upgrade Enterprise Single Sign-On to Password Manager by following the steps described in the topic *Upgrading Enterprise Single Sign-On to Password Manager* in the Password Manager for SAP Single Sign-On Implementation Guide.

2.6 Removing Your Personal Data

Prerequisites

- You have removed Password Manager from your computer.
- You have backed up the system registry of your computer.

> **i** Note
>
> This procedure requires you to edit the system registry. Editing the system registry can damage your computer.

Context

Removing Password Manager with the installer does not remove all user data and files, for example, the password store. Keeping the user data enables you to remove one release of Password Manager and install a higher release without losing passwords and other information in the password store. To remove all your data you must use this procedure.

Although your personal data is encrypted on your computer, a malicious user with sufficient skill and time could break the encryption or your master password and gain access to your password data. So before you give up ownership of a computer with your personal data, you should backup and delete that data.

Procedure

1. Navigate to the installation directory.

   The default installation directory is `C:\Program Files\SAP\FrontEnd`.
2. Delete the `signon` directory.
3. Open the Registry Editor.

   To open the Registry Editor, choose *Start* and enter `regedit` in the search field.
4. Delete the following keys:
   - `HKEY_LOCAL_MACHINE\SOFTWARE\SAP\signon`
   - `HKEY_CURRENT_USER\Software\SAP\signon`

3 Password Manager User Guide

This guide enables business users of the Password Manager application to operate and configure the application.

3.1 Starting Password Manager

Use this procedure to start the Password Manager application.

Context

Procedure

From the *Windows Start* menu, choose *All Programs* > *SAP Front End* > *Password Manager*.

3.2 Password Management

Password Manager enables you to save user names and passwords for Windows applications and web sites.

Related Information

Adding Passwords for Web Sites [page 13]
Adding Passwords for Windows Applications [page 17]
Displaying Passwords [page 19]
Generating Passwords [page 20]
Ignoring Applications and Web Sites [page 21]
Adding Additional Passwords for an Existing Application or Web Site [page 22]
Logging On With Drag and Drop Passwords [page 25]
Password Policies [page 26]

3.2.1 Adding Passwords for Web Sites

Use Password Manager to save your user name and password for web sites so that Password Manager can automatically log you on next time you visit the page.

Prerequisites

- You know your user name and password for the web site.
- Web detection has not been disabled for your web browser.

Context

> **i** Note
>
> If you are using Microsoft Internet Explorer, some web sites open a *Windows Security* dialog box in additon to the Password Manger dialog box. Enter your user name and password in the *Password Manager* dialog box. As long as you have automatic logon enabled, Password Manager automatically enters your user name and password in the *Windows Security* dialog box. Otherwise you must enter this information yourself.

Procedure

1. Open a web site in your browser.
2. Go to the logon screen.
3. Enter your user name and password and submit.
4. In the *Password Manager* dialog that appears, choose how you want to register the site.
    - Domain name (example.com)
    - Fully-qualified domain name (hostname.example.com)
    - URL (http://host.example.com/resource)
5. Choose the *Register Now* pushbutton.

Results

Password Manager adds a password entry for this web site. Next time you navigate to the logon page of the web site, Password Manager can log you on automatically.

Related Information

Ignoring Applications and Web Sites [page 21]
Choosing Between Domain Name, Fully-Qualified Domain Name, and URL [page 14]
Disabling Detection of New Passwords for Web Sites [page 15]
Disabling Automatic Logon to Web Sites [page 16]

3.2.1.1 Choosing Between Domain Name, Fully-Qualified Domain Name, and URL

When you save a web site for Password Manager, you must choose how to register the web site. The following table explains the options.

Registration Options for Passwords

Option	Example	Description
Domain name	`example.com`	Password Manager performs Single Sign-On anytime it gets a logon dialog from any URL with the matching domain name. This is good if the web site only offers one service, but bad if it you have different user IDs for different hosts or services. For example `photos.example.com` and `mail.example.com` and `calendar.example.com`.
Fully-qualified domain name	`hostname.example.com`	This option enables you to separate your services, but it only makes sense if you have different logons for each service.

Option	Example	Description
URL	`http://host.example.com/resource`	With this option you have a different logon for each individual application the web site has to offer. For example, you have different users for applications at the following URLs: `http://host.example.com/resource/mail/login` and `http://host.example.com/resource/photos/login`. Unfortunately, every time there is a change in the application URL you must reregister the password with Password Manager. For example, the owner of the photo application changes the login application and the URL is now as follows: `http://host.example.com/resource/photos/login2`.

3.2.1.2 Disabling Detection of New Passwords for Web Sites

You do not want Password Manager attempt to add new passwords when you log on to a web site. As an alternative, you can choose the *Register Later* or *Never Register* pushbuttons, when Password Manager attempts to add a new password.

Prerequisites

- You are using a web browser that supports the *SAP NetWeaver Single Sign-On Password Manager* toolbar.
- You installed the *SAP NetWeaver Single Sign-On Password Manager* toolbar for your web browser during installation.
- You display the *SAP NetWeaver Single Sign-On Password Manager* toolbar in your web browser.

Context

Procedure

1. Open a web browser.
2. From the *SAP NetWeaver Single Sign-On* toolbar, choose *Settings* > *Turn on Web Detection*.

Results

The menu entry changes to `Turn off Web Detection`. When you log on to a new web site, Password Manager does not offer you the option to save the password.

3.2.1.3 Disabling Automatic Logon to Web Sites

You do not want Password Manager to automatically you log on to web sites. This gives you a chance to select from multiple passwords you have saved for the web site.

Prerequisites

- You are using a web browser that supports the *SAP NetWeaver Single Sign-On Password Manager* toolbar.
- You installed the *SAP NetWeaver Single Sign-On Password Manager* toolbar for your web browser during installation.
- You display the *SAP NetWeaver Single Sign-On Password Manager* toolbar in your web browser.

Context

Procedure

1. Open a web browser.
2. From the *SAP NetWeaver Single Sign-On* toolbar, choose *Settings* > *Automatic Login*.

Results

The menu entry changes from a green check mark to a red X. When you log on to a web site for which you have a password, Password Manager enters the default password, but does not submit the information.

3.2.2 Adding Passwords for Windows Applications

This procedure saves your user name and password for a Windows application so Password Manager can log you on next time you start the application.

Prerequisites

- You know your password and user name, if required, for the application.
- You have enabled *Password Manager Learning Wizard*.

Context

Procedure

1. Start an application that requires logon.
2. In the *Password Manager* dialog box, choose the *Register Now* pushbutton.

   The *SAP NetWeaver Single Sign-On Password Manager Registration* dialog box appears.
3. Determine if the logon dialog of the application asks for just a password or whether it asks for user name and password.

   If the logon dialog only has a field for a password, select the *Login dialog only has password field* checkbox.
4. For each find icon (), click and drag the icon to the relevant field or button in the logon dialog of the application.

   For example, drag the find icon for *Password* to the password field of the logon dialog of the application. The icon becomes a crosshair. When Password Manager highlights the correct field or pushbutton, drop the icon.

   If you drop the find icon in the wrong place, use the trash icon () to remove the setting a try again. Do this until you cannot find any more fields or buttons with corresponding find icons in the *Password Manager Registration* dialog.
5. Choose the *Next* pushbutton.
6. Enter data as required and choose the *Next* pushbutton.
7. Choose the *Finish* pushbutton.

Results

Password Manager enters your password and logs you on to the application.

> **Note**
>
> If you have disabled automatic logon for Windows applications, Password Manager enters your password information automatically, but you must submit the logon data yourself.

Related Information

Disabling Detection of New Passwords for Applications [page 18]
Ignoring Applications and Web Sites [page 21]

3.2.2.1 Disabling Detection of New Passwords for Applications

You do not want Password Manager to attempt to add new passwords when you log on to an application.

Context

As an alternative, you can choose the *Register Later* or *Never Register* pushbuttons, when Password Manager attempts to add a new password.

Procedure

In the context menu of the Password Manager icon () in the notification area of the task bar, choose *Disable Password Manager Learning Wizard*.

> **Note**
>
> Your system administrator can disable this function in the policy files. If the icon is not does not appear or you cannot enable the menu item, contact your system administrator.

Results

When you start an application with a logon dialog, Password Manager does not offer you the option to save the password.

> **Note**
>
> You can always manually start the Learning Wizard, by choosing *Register New Application* from the context menu of the Password Manager icon () in the notification area of the task bar.

3.2.3 Displaying Passwords

You can display the password you set for an application or web site.

Prerequisites

You know the master password for your Password Manager installation.

Context

Procedure

1. Start Password Manager.
2. Choose *Passwords*.
3. Choose a password.
4. Choose  (*Show and change password*).

   > **Caution**
   >
   > Be aware that the application shows the password on the screen in clear text (unencrypted).

5. Enter the master password.

   If you forget the master password you can reset it.

Results

The password appears for 5 seconds. You can now edit the `<Password>` and `<Confirm Password>` fields.

Related Information

Resetting the Master Password [page 37]

3.2.4 Generating Passwords

Generated passwords are harder to remember, but if you only access particular applications or web sites from a set of computers where you have installed Password Manager, then this can be a very safe way to protect access to these applications and web sites. Password Manager remembers the passwords so you do not have to.

Context

Generated passwords tend to be much safer than passwords created by human beings. Human beings often rely on words and phrases that a hacker can guess.

Procedure

1. In the context menu of the Password Manager icon () of the notification area in the task bar, choose *Open Password Generator*.
2. Select a password policy or adjust the password policy as required.

   If you change the password policy, enter a new description and choose  (*Save password policy*) to save it.
3. Choose the *Generate* pushbutton.

   To view the password, choose  (*Show and hide password*).

   > ⚠ Caution
   >
   > Make sure no one can look over your shoulder at the screen.
4. Choose  (*Copy to clipboard*).
5. Paste the password in any password fields.

   For example, paste the password in the change password dialog of the application or web site. Then update the password entry in Password Manager with the same password.
6. To close the window, choose the *Cancel* pushbutton.
7. Clear the clipboard cache.

   To clear the clipboard cache select a string of text from a document and copy the text to the clipboard (CTRL + C). This overwrites the password in the memory of the clipboard.

> ⚠ Caution
>
> It is important to remove the password form the clipboard, because other applications, possibly malicious ones, can access this information.

Related Information

Enabling Automatic Change of Passwords for Applications [page 34]

3.2.5 Ignoring Applications and Web Sites

Use this procedure if you have applications or web sites for which you do not want Password Manager to ask you, if Password Manager should register the application or web site.

Prerequisites

The application or web site is not already saved in your password list.

Procedure

1. Start the application or web site.
2. When the *Password Manager* dialog appears, choose the *Never Register* pushbutton.

Results

The application or web site appears on the *Ignored Applications and Web Sites* list. To view the list, choose *Advanced* > *Ignored Applications and Websites*.

3.2.6 Adding Additional Passwords for an Existing Application or Web Site

You already have a password configured for an application or web site. You want to be able to log on with another account. Perhaps you have an account for work and an account for private use or you share this computer with another person.

Prerequisites

You know your user name and password for the web site or application.

Context

Procedure

1. Start Password Manager.
2. Choose *Passwords*.
3. Choose the *New* pushbutton.
4. Enter the required data.

   Required fields indicated by an asterisk (*).
5. Choose + (*Add application*).
6. Select a registered application or website and choose the *Add* pushbutton.
7. Save your entries.

Results

The application or web site now has more than one password registered by Password Manager. Password Manager enters the default password, when you open the application or web site. To prevent Password Manager from logging you on automatically, disable automatic log on. For applications you can enable a multiple password dialog.

Related Information

Working With Multiple Passwords for the Same Application or Web Site [page 24]
Enabling the Multiple Password Selection for Applications [page 33]
Password Attributes [page 43]

3.2.6.1 Changing the Default Password for an Application or Web Site

When you have multiple passwords for the same Windows application or web site, the last password you created for the application or web site is automatically the default password. Password Manager attempts to log on with the default password first.

Prerequisites

You have multiple passwords for the same application or web site.

Procedure

1. Start Password Manager.
2. Choose *Passwords*.
3. Select the password that is not the default password.
4. Choose  (*Show and hide details of this application*).
5. Select the *Default Password* checkbox.
6. Save your entries.

Related Information

Working With Multiple Passwords for the Same Application or Web Site [page 24]

3.2.6.2 Choosing Between Multiple Passwords for Web Sites

You have multiple passwords for a web site. By default, Password Manager automatically logs you on with the default password for that web site. You want to decide which one you log on with.

Prerequisites

- You are using a web browser that supports the SAP Single Sign-On Password Manager toolbar.
- You installed the SAP Single Sign-On Password Manager toolbar for your web browser during installation.
- You display the SAP Single Sign-On Password Manager toolbar in your web browser.
- You have disabled automatic logon for your web browser.

Procedure

1. Open the web site in your web browser.
2. From the SAP Single Sign-On toolbar, choose *Passwords*.
3. Select a password.

Related Information

Working With Multiple Passwords for the Same Application or Web Site [page 24]
Disabling Automatic Logon to Web Sites [page 16]

3.2.6.3 Working With Multiple Passwords for the Same Application or Web Site

You share access to a single computer with one or more people, such as your coworkers. Or you have multiple accounts for the same web site; one for private use and one for business. In both cases you have multiple passwords for the same application or web site.

> ⚠ Caution
>
> If you share the same computer account with multiple people, do not create password entries for applications or web sites that you do not want others to see. Password Manager does not have any way to protect these applications or web sites from others sharing your computer account. If you have passwords to accounts others should not see, we recommend you install Password Manager in a separate computer account or separate computer to which only you have access.

Related Information

Disabling Automatic Logon to Web Sites [page 16]
Disabling Automatic Logon for Applications [page 32]
Changing the Default Password for an Application or Web Site [page 23]
Adding Additional Passwords for an Existing Application or Web Site [page 22]

3.2.7 Logging On With Drag and Drop Passwords

There are thousands of ways that applications and web sites can implement log on. Password Manager can automatically log on to many of them, but not all.

Prerequisites

- You have added a password which allows drag & drop.
- You have opened the application or web site to which you want to log on.

Context

To make log on easier to the applications and web sites for which Password Manager cannot use automatic log on, use *Drag & Drop Passwords*.

Procedure

1. In the context menu of the Password Manager icon () in the notification area of the task bar, choose *Open Drag & Drop Passwords*.

   > **i** Note
   >
   > Your system administrator can disable this function in the policy files. If the icon is not does not appear or you cannot enable the menu item, contact your system administrator.

2. From the *Drag & Drop Passwords* dialog box, drag the relevant key icons to the relevant fields on application or web site.

Controls for Drag & Drop Passwords

Icon	Name	Use
	User Name & Password	From the *Drag & Drop Passwords* dialog box, drag the relevant key icons to the relevant fields on application or web site.
	User Name	Use this icon to enter only the user name in a field.
	Password	Use this icon to enter only the password in a field.

Related Information

Adding Additional Passwords for an Existing Application or Web Site [page 22]
Password Attributes [page 43]

3.2.8 Password Policies

Password Manager uses password policies to regulate what kind of passwords you can use. Use password policies to ensure you create safe passwords.

With the password policy you define how long or short the password can be, what special characters you can use, whether numbers are required, and other settings. A good password policy means that Password Manager generates safe passwords. A bad password policy results in passwords that are easy to guess.

Password Manager checks passwords against password policies in the following instances:

- You use Password Manager to generate a password for an application or web site.
- Password Manager automatically generates a new password for an expired password of an application. Automatic password generation is disabled by default. You must enable this feature to use it.

> **i Note**
>
> Password Manager cannot automatically generate new passwords for expired passwords of web sites.

Applications and web sites can have their own password policies. When you use Password Manager to generate passwords for these applications and web sites, ensure that your password policy of the Password Manager matches the policy of the application or web site. For example, if you have a password policy that requires numbers (0-9), but the application or web site does not allow numbers in passwords then you will get an error from the application or web site.

→ Tip

We recommend that you try and match the security policy of the application or web site as much as possible.

Related Information

Adding Password Policies [page 27]
Adding Password Policies to Applications [page 28]

3.2.8.1 Adding Password Policies

Password Manager uses password policies to define the rules for generating passwords.

Procedure

1. Start Password Manager.
2. Choose *Advanced* > *Password Policies*.
3. Choose the *New* pushbutton.
4. Enter the required data.

   Required fields indicated by an asterisk (*).
5. Save your entries.

Results

The password policy appears in the list of password policies.

Related Information

Password Policy Attributes [page 44]

3.2.8.2 Adding Password Policies to Applications

To enable Password Manager to generate new passwords to replace the expired passwords of applications, ensure that Password Manager has an appropriate password policy assigned. Only then can Password Manager automatically generate passwords that will be accepted by your application.

Prerequisites

- You have created a password entry for your application.
- You have created a password policy that matches the password policy of your application.

Context

Procedure

1. Start Password Manager.
2. Choose *Passwords*.
3. Choose an application (not web site).
4. Choose  (*Show and hide details of this application*).
5. Enter a password policy.
6. Save your entries.

Related Information

Enabling Automatic Change of Passwords for Applications [page 34]

3.3 Adding Credit Card Information

Use Password Manager to store your credit card information on your computer. Once stored on your computer, you no longer need to pull out your wallet to look up your credit card information. Storing your credit card

information on your computer also provides you a backup of your credit card information, should you ever lose your credit card.

Context

> **i** Note
>
> Password Manager stores your information in an encrypted format, protected by the master password of the Password Manager.

Procedure

1. Start Password Manager.
2. Choose *Credit Cards*.
3. Choose the *New* pushbutton.
4. Enter the required data.

   Required fields indicated by an asterisk (*).
5. Save your entries.

Related Information

Credit Card Attributes [page 45]

3.4 Adding Identities

Add identities so that you can remember private information about yourself or other people.

Context

> **i** Note
>
> Password Manager stores your information in an encrypted format, protected by the master password of the Password Manager.

Procedure

1. Start Password Manager.
2. Choose *Identities*.
3. Choose the *New* pushbutton.
4. Enter the required data.
   Required fields indicated by an asterisk (*).
5. Save your entries.

Related Information

Identity Attributes [page 46]

3.5 Adding Notes

Use Password Manager to save private text messages.

Context

> **i** Note
>
> Password Manager stores your information in an encrypted format, protected by the master password of the Password Manager.

Procedure

1. Start Password Manager.
2. Choose *Notes*.
3. Choose the *New* pushbutton.
4. Enter the required data.
   Required fields indicated by an asterisk (*).
5. Save your entries.

Related Information

Note Attributes [page 47]

3.6 Disabling Password Manager

You want to stop all functions of the Password Manager. You do not want Password Manager to learn new passwords or log you on automatically to any applications or web sites.

Procedure

In the context menu of the Password Manager icon ( ) in the notification area of the task bar, choose *Disable Password Manager*.

> **i Note**
>
> Your system administrator can disable this function in the policy files. If the icon is not does not appear or you cannot enable the menu item, contact your system administrator.

3.7 Terminating the Password Manager

You can either exit or log off the Password Manager.

Context

- If you exit or log off the manager, you must enter your master password the next time you try to log on. In this case, your logon attempt fails if you do not enter the right master password in three attempts.
- If you exit the manager, you can access it again by following the instructions for starting the Password Manager.

Procedure

1. Right-click the Password Manager icon ( ) in the notification area of the taskbar.
2. In the context menu for the Password Manager icon ( ) in the notification area of the taskbar, choose *Log Off* or *Exit*.

Related Information

Starting Password Manager [page 12]

3.8 Advanced Settings

The advanced settings are either one time configurations that change the behavior of Password Manager or emergency recovery operations.

Related Information

Application Settings [page 32]
Master Password [page 35]
Importing Password Manager Data [page 38]
Exporting Password Manager Data [page 39]
Setting the Default Web Browser [page 39]
Enabling Automatic Logon to Password Manager [page 40]

3.8.1 Application Settings

Application settings determine the behavior of Password Manager during logon to Windows applications.

Related Information

Disabling Automatic Logon for Applications [page 32]
Enabling the Multiple Password Selection for Applications [page 33]
Enabling Automatic Change of Passwords for Applications [page 34]

3.8.1.1 Disabling Automatic Logon for Applications

By default Password Manager logs you on to Windows applications for which you have registered a password as soon as the logon screen apears. You can disable automatic log on. Password Manager then enters the user name and password as appropriate, but does not submit the information to the application. You decide when to submit the logon data. Use this function when you have multiple accounts for the application and you want to be able to enter an alternative user name and password.

Prerequisites

You have added a password entry for an application registered the change password screen of the application in Password Manager.

Context

Procedure

1. Start Password Manager.
2. Choose *Advanced* > *Settings*.
3. Clear the *Enable automatic logon for Windows applications* checkbox.
4. Save your entries.

Related Information

Working With Multiple Passwords for the Same Application or Web Site [page 24]
Enabling the Multiple Password Selection for Applications [page 33]

3.8.1.2 Enabling the Multiple Password Selection for Applications

If you have multiple passwords for a single application, you can configure Password Manager to offer a list of passwords to log on with.

Procedure

1. Start Password Manager.
2. Choose *Advanced* > *Settings*.
3. Select the *Show multiple passwords dialog* checkbox.
4. Save your entries.

Results

The next time you start a Windows application for which you have multiple passwords saved in Password Manager, Password Manager offers you a choice of which password to log on with.

Related Information

Working With Multiple Passwords for the Same Application or Web Site [page 24]
Adding Additional Passwords for an Existing Application or Web Site [page 22]

3.8.1.3 Enabling Automatic Change of Passwords for Applications

The security policies of some applications require you to periodically change your password. Applications do this to limit the amount of time someone can misuse your account. Password Manager can change your password for you automatically.

Prerequisites

You have added a password entry for an application registered the change password screen of the application in Password Manager.

Context

> **i** Note
>
> Password Manager can only automatically change your passwords for application, not web sites.

When Password Manager generates new passwords for you, Password Manager uses the password policy that you assigned to the application. If you have not assigned a password policy, Password Manager uses the default password policy.

Procedure

1. Start Password Manager.

2. Choose *Advanced* > *Settings*.
3. Select the *Change my password automatically when required* checkbox.
4. Determine if you want to be notified when Password Manager changes the password.

   To enable notification, select the *Notify me about password changes* checkbox. When enabled, Password Manager displays a dialog box informing you that it has changed your password.
5. Save your entries.

Related Information

Adding Password Policies to Applications [page 28]

3.8.2 Master Password

When you install Password Manager, Password Manager creates a key from the master password you enter. Password Manager uses this key to encrypt and decrypt the data that Password Manager saves, such as passwords for applications and web sites, credit card information, identity information, and notes.

> ⚠ Caution
>
> Use a strong password. If someone can open your Password Manager and guess your master password, that person has access to all the other passwords and information that you have saved. You can find plenty of advice on how to create strong passwords on the Internet.

Password Manager uses the master password to protect some functions.

- Starting Password Manager
- Viewing or changing passwords
- Change or resetting the master password
- Exporting your data to a file

> ℹ Note
>
> You need the master password used to save the file to import that data back into Password Manager.

You can configure Microsoft Windows to log you on automatically to Password Manager during your Windows logon.

When Password Manager requests your master password, you have 3 chances to enter the password correctly. If you fail, Password Manager deletes the key it used to encrypt your data.

If you forget the master password, you can reset the master password and regenerate the key with the security question and answer.

Related Information

Changing the Master Password [page 36]
Changing the Security Question [page 37]
Resetting the Master Password [page 37]

3.8.2.1 Changing the Master Password

We recommend that you periodically change the master password to limit the time someone can compromise your account. If you forget the master password, you can use the security question to reset it.

Prerequisites

You know the current master password.

Procedure

1. Start Password Manager.
2. Choose *Advanced* > *Settings*.
3. Under *Master Password*, choose *Password Options*.
4. Choose the *Change Master Password* pushbutton.
5. Enter data as required.
6. Save your entries.

Related Information

Resetting the Master Password [page 37]

3.8.2.2 Changing the Security Question

Password Manager uses the security question to reset the master password.

Prerequisites

You know the master password.

Procedure

1. Start Password Manager.
2. Choose *Advanced* > *Settings*.
3. Under *Master Password*, choose *Password Options*.
4. Choose the *Change Security Question for Resetting Master Password* pushbutton.
5. Enter data as required.
6. Save your entries.

3.8.2.3 Resetting the Master Password

You need the master password to start Password Manager and to carry out some of its more important functions. If you forget the master password, use this procedure to reset it.

Prerequisites

You know the security question and answer.

> **i** Note
>
> If you do not remember your security question and answer, follow the procedure described in SAP note 2194259.

Procedure

1. Start Password Manager.
2. Choose *Advanced* > *Settings*.

3. Under *Master Password*, choose *Password Options*.
4. Choose the *Reset Master Password* pushbutton.
5. Enter data as required.
6. Save your entries.

3.8.3 Importing Password Manager Data

Use this procedure to import your password data from another computer, where you are using SAP Single Sign-On Password Manager or to restore a backup of your password data.

Prerequisites

- You have a password data file from Password Manager.
- You know the master password used to encrypt the password data file.

Context

> ⚠ Caution
>
> Password Manager overwrites any entries, for example passwords, notes, identities, and credit cards, with the same description.

Procedure

1. Start Password Manager.
2. Choose *Advanced* > *Settings*.
3. Choose the *Import Storage File* pushbutton.
4. Enter a file name and path.
5. Enter the master password used to export the file.

3.8.4 Exporting Password Manager Data

Use this procedure to copy your password data to another computer, where you are using SAP Single Sign-On Password Manager or to create a backup of your password data.

Procedure

1. Start Password Manager.
2. Choose *Advanced* > *Settings*.
3. Choose the *Export Storage File* pushbutton.
4. Enter a file name and location.
5. Enter the master password for Password Manager.

Results

Password Manager saves the file with the `*.sso` extension in an encrypted format.

> ⚠ Caution
>
> When you import this file back into Password Manager, you must have the master password with which you saved this file. Otherwise you cannot recover this information.

3.8.5 Setting the Default Web Browser

From the list of passwords you can directly launch the relevant web sites. Which web browser Password Manager opens depends on what you have set as the default browser.

Context

Procedure

1. Start Password Manager.
2. Choose *Advanced* > *Settings*.
3. Choose a default web browser.

4. Save your entries.

3.8.6 Enabling Automatic Logon to Password Manager

You can log on to Password Manager automatically when you log on to your Windows session by enabling this feature.

Context

> ⚠ Caution
>
> Do not enable this feature unless you protect your Microsoft Windows account with a strong password or similar logon method.

By default you must enter the master password when you start Password Manager. This is a security measure taken to ensure that no one but you can start your computer and automatically have access to a list applications or web sites with the passwords. Such a person cannot view your passwords, because Password Manager requires the master password to show passwords, but the person could connect to a web site, such as your online banking web site, and view your data.

Procedure

1. Start Password Manager.
2. In the context menu of the *Password Manager icon* () in the notification area of the *task bar*, choose *Password Options*.

   > i Note
   >
   > Your system administrator can disable this function in the group policy files. If the icon is not does not appear, contact your system administrator.

3. Choose the *Enable Automatic Logon to SSO Password Manager* pushbutton.

Results

The next time you log on to your Microsoft Windows account, you also log on to Password Manager automatically.

3.9 Troubleshooting

If an errors occur while using Password Manager, troubleshooting provides your first clues to fixing problems yourself.

If you cannot solve the problem yourself, contact your system administrator.

SSO is not working for my registered web site

Reason or Action	Description or Solution
The password is on the list of ignored web sites.	Ignoring Applications and Web Sites [page 21]
Web detection is disabled.	Disabling Detection of New Passwords for Web Sites [page 15]
Password Manager is disabled.	Disabling Password Manager [page 31]
Try logging on with drag and drop.	Logging On With Drag and Drop Passwords [page 25]

Password Manager does not recognize the login dialog or the change password dialog of my Windows application

Reason or Action	Description or Solution
Detection of new passwords is disabled.	Disabling Detection of New Passwords for Applications [page 18]
Start Password Manager Learning Wizard manually.	1. In the context menu of the Password Manager icon ( ) in the notification area of the task bar, choose *Register New Application*. 2. Follow the onscreen instructions.
The Windows application runs at a higher integrity level than Password Manager (medium) according to the Windows Integrity Mechanism.	This is part of the security architecture of Microsoft Windows. You cannot use Password Manager for this application. Microsoft provides a tool to check if an application runs at a higher integrity level on its web site. Download and install the Process Explorer from Microsoft to determine if the application has a higher integrity level.

Drag and Drop data from Password Manager to an application and nothing happens

Reason or Action	Description or Solution
The Windows application runs at a higher integrity level than Password Manager (medium) according to the Windows Integrity Mechanism.	This is part of the security architecture of Microsoft Windows. You cannot use Password Manager for this application. Microsoft provides a tool to check if an application runs at a higher integrity level on its web site. Download and install the Process Explorer from Microsoft to determine if the application has a higher integrity level.

3.9.1 Auditing and Logging for Password Manager

To troubleshoot or log user activities, enable the user activity trace for Password Manager.

Prerequisites

You have administrator rights on your computer.

Procedure

1. Enable the *Password Manager user activity trace and log* option of the Password Manager group policy file.
2. Restart your computer.

Results

View the logs in a text editor at `<%AppData%>\Local\SAP\SecureLogin\Traces`.

Related Information

Security Relevant Logging and Tracing [page 59]
http://help.sap.com/nwsso30

3.10 Appendix

Use the reference information to understand how to create passwords, identities, and such in Password Manager or understand the configuration options.

Related Information

Password Attributes [page 43]
Password Policy Attributes [page 44]
Credit Card Attributes [page 45]
Identity Attributes [page 46]

Note Attributes [page 47]

3.10.1 Password Attributes

The following table describes the attributes for passwords.

Passwords Attributes

Name	Description
<Description>	Enter a unique name or title for this password entry. Required entry.
<Allow Drag&Drop>	There are thousands of ways that applications and web sites can implement log on. Password Manager can automatically log on to many of them, but not all. To make log on easier to the applications and web sites for which Password Manager cannot use automatic log on, select the *Allow Drag&Drop* checkbox. Use *Drag & Drop Passwords* to log on. Some applications or web sites also require that you end the user name and password with a simulated keystroke. You define that keystroke in the fields that follow *User Name* and *Password*. Default value is No key.
<User Name>	Enter the name you use to log on to the application or web site. Required entry.
<Password>	Enter the password that you use to log on to the application or web site. The password must satisfy the password policy of Password Manager and the policy of the web site or application. Required entry.
<Confirm Password>	To ensure that you have entered the password correctly, Password Manager requires you to enter the password a second time. Required entry.
<Password Parameter 1> <Password Parameter 2> <Password Parameter 3>	The optional fields for additional parameters other than user name and password.
<Application/Web Site>	This field displays the name of the application or web site that uses this password.

Related Information

Password Policies [page 26]
Logging On With Drag and Drop Passwords [page 25]

3.10.2 Password Policy Attributes

The following table describes the attributes for password policies.

Password Policy Attributes

Name	Description
<Description>	Enter a unique name or title for this policy entry. Required entry.
<Password Length>	Determines the minimum and maximum length of generated passwords. Default value is a minimum length of 6 characters and a maximum length of 8 characters.
<Uppercase Characters (A-Z)>	Determines if uppercase characters are allowed, required, or forbidden. If you choose **Required**, set the minimum number of characters that must be uppercase. Uppercase characters are allowed by default.
<Lowercase Characters (a-z)>	Determines if lowercase characters are allowed, required, or forbidden. If you choose **Required**, set the minimum number of characters that must be lowercase. Lowercase characters are allowed by default.
<Numbers (0-9)>	Determines if numbers are allowed, required, or forbidden. If you choose **Required**, set the minimum number of numbers that must be included. Numbers are allowed by default.
<Special Characters>	Determines if special characters are allowed, required, or forbidden. If you choose **Required**, set the minimum number of special characters that must be included. Special characters are allowed by default.
<Allowed Special Characters>	The number of possible special characters is quite large. This attribute determines, which special characters are allowed. The list of default characters is !@#$%^&*()_-+=?><,./:;'~`|{}[].
<Must Start with an Uppercase Character>	Enable this attribute to only allow passwords that start with an upper case character.

Name	Description
< Allow Sequential Characters (123abc)>	Enable this attribute to allow passwords that contain a sequence of ASCII characters, such as **1234** and **ABCD**.
<Allow Duplicate Characters (abcabc)>	Enable this attribute to allow passwords that contain a duplicate characters in the password. For example, **ACDA** contains duplicate characters and **ACDa** does not.
<Allow Repeated Characters (aabbcc)>	Enable this attribute to allow passwords that contain a repeated characters- For example, **AA19zx** contains repeated characters and **A19zxA** does not.

Related Information

Password Policies [page 26]

3.10.3 Credit Card Attributes

The following table describes the attributes for credit cards.

Credit Card Attributes

Name	Description
<Description>	Enter a unique name for this credit card. Required entry.
<Card Type>	Enter the type of credit card: American Express, Diners Club, Discover, JCB, Master Card, VISA.
<Card Holder>	Name of person to the credit card is issued. Required entry.
<Card Number>	Bank identification number. Required entry.
<Valid Thru>	The month and year that the credit card expires. Use the format MM/YYYY. Required entry.
<Security Code>	Enter the three to four-digit number located on the back of the card to help prevent credit card fraud when using the card on the Internet. Required entry.
<Service Phone>	Telephone number of the service organization for the credit card company.

Name	Description
<Additional Code>	Enter any additional codes that appear on the back of the credit card.
<Service URL>	Enter the web site of the service organization for the credit card company.
<Additional Info>	Free text field for any additonal information.
<Comments>	Free text field for any comments about this credit card.

Related Information

Credit Card Attributes [page 45]

3.10.4 Identity Attributes

The following table describes the attributes for identities.

Identity Attributes

Name	Description
<Description>	Enter a unique name for this identity. Required entry.
<E-Mail Address>	Enter an e-mail address.
<First Name>	Required entry.
<Last Name>	Required entry.
<Date of Birth>	Enter when the person was born. Use the format DD/MM/YYYY.
<Company>	Name of the company the person works for.
<Address 1>	First line of the person's mailing address.
<Address 2>	Second line of the person's mailing address.
<City>	Self-explanatory.
<State>	State or province.
<Zip>	ZIP or postal code.

Name	Description
<Country>	Self-explanatory.
<Phone>	Self-explanatory.
<Mobile>	Mobile or cell phone number.
<Fax>	Self-explanatory.
<Web Site>	Enter the personal web site of the person.
<Comments>	A free text field for your comments.

Related Information

Adding Identities [page 29]

3.10.5 Note Attributes

The following table describes the attributes for notes.

Note Attributes

Name	Description
<Description>	Enter a unique name or title for your note. Required entry.
<Comments>	Enter the text of your note.

Related Information

Adding Notes [page 30]

4 Password Manager Admininstrator Guide

System administrators use these functions to configure Password Manager for all users in a Windows domain.

Related Information

Options of the Password Manager Group Policy File [page 51]
Configuring Policy Files for Password Manager [page 50]
Distributing Applications, Web Sites, and Password Policies to Users [page 48]

4.1 Distributing Applications, Web Sites, and Password Policies to Users

You want to preconfigure installations of Password Manager for users in your network with specific applications, web sites, and password policies. Create a dummy installation and define the data you want to distribute. Then distribute this data in your Windows landscape.

Prerequisites

- You have a dummy installation to create content to distribute.
- You have administrator rights in your network to distribute and overwrite business user data.
- You know the domain and user ID of your business users.

Context

You can distribute the following Password Manager data to users in your network:

- Application information
- Web site information
- Ignored applications and webs sites
- Password policies

Distributing this data ensures that all users in your network have a common starting point.

> ⚠ Caution
>
> When you distribute data, you overwrite the any existing data the user has configured. We recommend that you only distribute data to business users, whose accounts or Password Manager configurations are in an initial state.

Procedure

1. Create a dummy installation of Password Manager.
2. Add passwords for applications and web sites, ignored applications and web sites, and password policies.

   > i Note
   >
   > Although you are adding passwords to your dummy installation, **this procedure does not copy user ID and password data**. The user ID and passwords that you enter do not need to function, but you can use real password data to test that you have set up the information correctly.

3. Copy the data files from your dummy installation.

   The data files are named as follows:

   - `<domain>_<user ID>_APP.xml`
   - `<domain>_<user ID>_PLC.xml`

   The files are located at `<%APPDATA%>\SAP\signon\AppInfo`
4. Distribute and rename files in the network to fit the location and naming convention described in the previous step.

Results

Once distributed, business users should restart their Password Manager application. After restart, users can add passwords to the applications and web sites in the new files.

Related Information

Adding Additional Passwords for an Existing Application or Web Site [page 22]
Password Policies [page 26]
Ignoring Applications and Web Sites [page 21]

4.2 Configuring Policy Files for Password Manager

Use this procedure to set the configuration settings of Password Manager for all Microsoft Windows systems in your network.

Prerequisites

- You must work with the administrator of your Windows domain.
- This procedure uses the standard tools for managing policies in Microsoft Windows. For more information, refer to the relevant Microsoft documentation.

Procedure

Work with your Microsoft Windows domain administrator to prepare and configure the policy file.

`<package path>\SAPSetupESC\ESC\ADM\PasswordManager.adm`

Depending on the tool you use, the template appears under *Administrative Template* > *Classic Administrative Templates (ADM)* > *SAP AG* > *Password Manager*.

Next Steps

Have your domain administrator import the file into the Windows domain and allow the policy file to be distributed to the domain users.

Related Information

Password Manager Options [page 51]
Soft Token Settings [page 53]
Terminal Emulator Host Configuration [page 54]

4.3 Options of the Password Manager Group Policy File

The policy file for Password Manager enables you to control the configuration options of Password Manager. You can distribute the policy file to all workstations in your Microsoft Windows domain.

Related Information

Password Manager Options [page 51]
Soft Token Settings [page 53]
Terminal Emulator Host Configuration [page 54]
Configuring Policy Files for Password Manager [page 50]

4.3.1 Password Manager Options

Password Manager Options

Option	Description
`<Disable Password Manager Wizard>`	Enable this option to prevent Password Manager from detecting and adding new passwords for Windows applications. Enabling this option also prevents single sign-on to Windows applications. Enabling this option has no effect on single sign-on or learning passwords for web sites.
`<Interval between characters in ms>`	Determines the speed with which Password Manager sends character to the destination window during a drag and drop operation. Some applications, such as terminal service clients on slow bandwidth connections, need a slower send speed to guarantee that all characters reach the destination. For such applications increase the interval in this setting. The default value is 40 ms. During a drag and drop operation, Password Manager sends a character `KeyDown`, then waits half the latency period until Password Manager sends a `KeyUp`. Then Password Managerwaits the second half of the latency period until Password Manager sends the next character `KeyDown`.

Option	Description
`<Pre-erase Drag Drop destination fields>`	Enable this option to have Password Managererase the content of a destination field before it inserts drag and drop content into the field. Some application supply sample text in these fields. Enabling this option ensures that all the sample text is removed before Password Manager enters the Drag & Drop data. Otherwise users can drop their credentials in the middle of the sample text.
`<Password Manager trace and log>`	Only enable this option at the request of SAP Support. The trace provides additional information for the localization of problems.
`<Password Manager user activity trace and log>`	Enable this option to log user activities. For more information, see Auditing and Logging for Password Manager [page 42].
`<Hide Password Manager taskbar context menu>`	Enable this option to hide the Password Manager icon of the notification area of the task bar. If enabled, users cannot do the following: • Enable or disable automatic logon to Password Manager • Log on with Drag & Drop passwords • Enable or disable detection of new passwords for applications. • Enable or disable Password Manager
`<Disable auto-registration and single sign-on>`	Enable this option to disable the recognition of unregistered Windows applications and web sites. This option also disables single sign-on to registered Windows applications and web sites. You can still edit entries in Password Manager.
`<Disable Password Manager Learning Wizard>`	Enable this option to prevent Password Manager from detecting and adding new passwords for Windows applications. Disabling the Password Manager Learning Wizard has no effect on single sign-on or learning passwords for web sites.
`<Disable Drag & Drop passwords submenu>`	Enable this function to disable the *Open Drag & Drop Passwords* menu item in the context menu of the notification area of the task bar for Password Manager. Some security policies do not allow drag & drop methods, since it can be considered an open means of transmitting the password. Drag & drop uses `SendKey`, which can be considered unsafe.

Option	Description
`<Online help URL>`	Determines the URL used for the online help. If your security policy does not allow you to access the default URL on SAP Help Portal, you can download the online help and access from a local file share. Or you can write your own custom online help that supports the features you have enabled.

Related Information

Configuring Policy Files for Password Manager [page 50]

4.3.2 Soft Token Settings

The password store settings configure the minimum length of the answers to the security question and the master password. It also sets the location of the password storage file.

These options are divided between the following settings:

- *Minimum character of answer or password string*
- *Password store path*

Options for Password Store

Option	Description
`<Minimum character of answer>`	Determines the minimum length of an answer to a security question for resetting the master password. The value range is from 0-125.
`<Minimum character of password>`	Determines the minimum length of the master password. The default value is 8. The value ranges from 8-20.
`<Password store path>`	Determines the path to folder where Password Manager stores the password files. The default value or the value used if there is no configuration is `<%APPDATA%>\SAP\signon\Softtoken`. **! Restriction** Every user requires read and write access to this folder. Choose a network or local folder depending on your security and backup policies.

Related Information

Configuring Policy Files for Password Manager [page 50]

4.3.3 Terminal Emulator Host Configuration

You can configure up to five terminal emulator hosts under the following options:

- *Configure the first host*
- *Configure the second host*
- *Configure the third host*
- *Configure the fourth host*
- *Configure the fifth host*

Options for Terminal Emulator Host Configuration

Option	Description
`<Hostname or IP:>`	The host name or IP address of the host to connect to.
`<The string to detect Username:>`	The title of the user name field. This string must be the same as the label of the field in which the user enters his or her user name for the host machine.
`<The string to detect Password:>`	The title of the password field. This string must be the same as the label of the field in which the user enters his or her password for the host machine.
`<Control key after Username:>`	The key a user enters after he or she enters his or her user name. For example, If the user enters the `Enter` key after entering his or her user name, enter **`{ENTER}`**. If the user enters the `Tab` after entering his or her user name, enter **`{Tab}`**.
`<Control key after Password:>`	The key a user enters after he or she enters his or her password. For example, If the user enters the `Enter` key after entering his or her password, enter **`{ENTER}`**. If the user enters the `Tab` after entering his or her password, enter **`{Tab}`**.
`<MaxLength of Username field:>`	The maximum number of characters a user can enter into the user name field.
`<MaxLength of Password field:>`	The maximum number of characters a user can enter into the password field.

Related Information

Configuring Policy Files for Password Manager [page 50]

5 Password Manager Security Guide

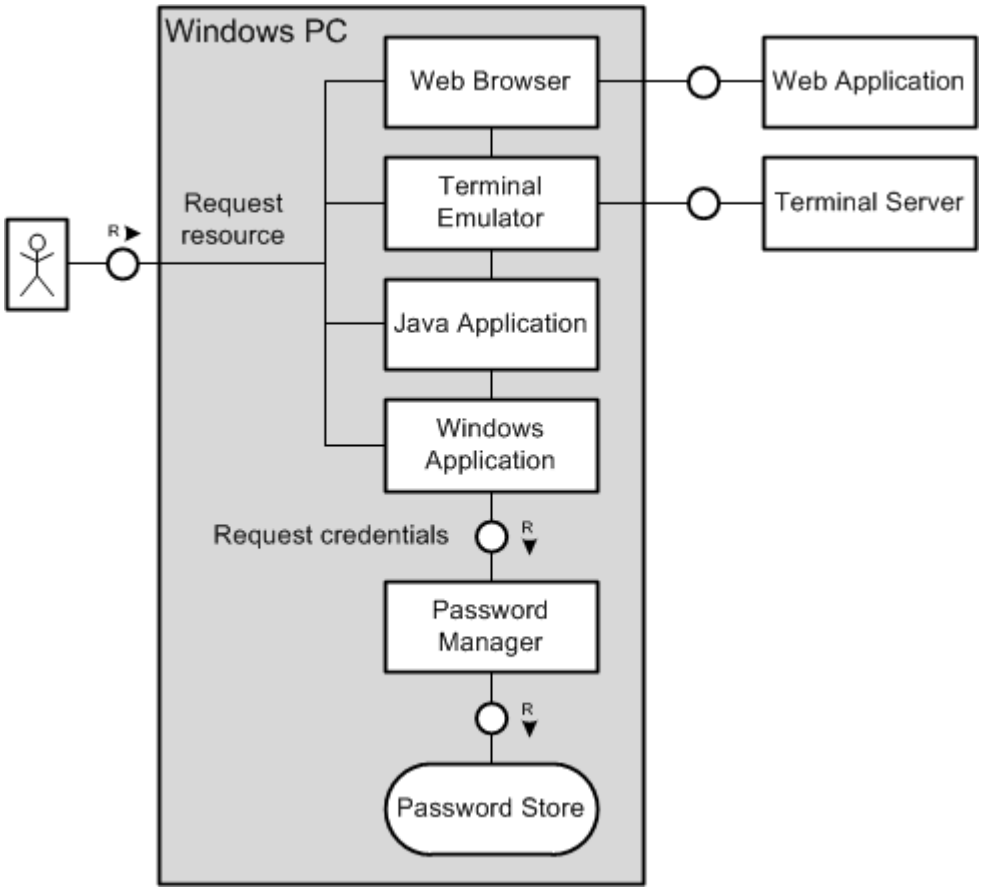
The security guide provides an overview of the security-relevant information that applies to Password Manager.

Related Information

Technical System Landscape [page 57]
Data Storage Security [page 57]
Password Security [page 58]
Security Relevant Logging and Tracing [page 59]

5.1 Technical System Landscape

The following figure shows an overview of the technical system landscape for the Password Manager.



Technical System Landscape of Password Manager

Password Manager resides on a Windows PC. When the user access applications, web sites, or terminal emulators, Password Manager can recognize the access and capture or provide credentials for single sign-on. Password Manager stores the credentials in an encrypted file, labeled here *Password Store*.

5.2 Data Storage Security

Password Manager stores private data.

The user's private data is encrypted with a private key generated from a master password entered by the user during initial configuration of the client installation. The user has full control over this data and can delete it with the Password Manager application.

By default, Password Manager stores credential data locally. The default directory is in the user-specific directory of the `Users` folder of Microsoft Windows operating system. The operating system protects this folder from unauthorized access.

You can configure Password Manager to store user data in a network location. You must ensure that the network configuration restricts access to the user who owns the data. The option `<Password store path>` of the Password Manager policy file controls this configuration.

Whether local or at a network location, ensure that the files at the storage location are backed up regularly.

Related Information

Configuring Policy Files for Password Manager [page 50]

5.3 Password Security

Password manager stores and manipulates passwords, which are the keys to your identity and data in a computer network. Handle this data with utmost care.

Always use the strongest possible passwords, especially for your master password. Your master password protects all other passwords you store with Password Manager. As system administrator, you can define the minimum length of the master password in the group policy files. For other passwords, you can define password policies appropriate to the sensitivity of the application or web site you access.

You can cause Password Manager to display passwords in plain text. Use this feature sparingly and always check that no one can view your screen while you do.

Be careful how you use the drag & drop feature. If you drag & drop your user ID and password into a text editor, the system reveals the password in plain text. Similarly, the terminal emulator function uses the SendKey method.

Related Information

Soft Token Settings [page 53]
Password Policies [page 26]
Displaying Passwords [page 19]
Logging On With Drag and Drop Passwords [page 25]

5.4 Security Relevant Logging and Tracing

The tables below list the relevant security events.

Security Events of Password Manager

Event	Description
Register new application or web site	Log application name, password processing information, and register application processing information
Log on to application or web site	Log application name, password (except password entry information) and login processing information
Change password for application	Log application name, and change password processing information
Add new password, identity, credit card, or notes	Log new entry information
Remove password, identity, credit card, or notes	Log removed entry information
Update password, identity, credit card, or notes	Log updated entry information
Change master password	Log success or error code
Reset master password	Log success or error code
Change security question	Log success or error code
Enable or disable automatic log on to Password Manager	Log status change
Import, export, or migration of data	Log status for import or export
Initialize master password	Log success or error code
Log on or log off from Password Manager	Log error code and description when user enters wrong, invalid, or locked master password

Related Information

Auditing and Logging for Password Manager [page 42]

6 Disclaimer

SAP Library document classification: **PUBLIC**.

This document is for informational purposes only. Its content is subject to change without notice, and SAP does not warrant that it is error-free. SAP MAKES NO WARRANTIES, EXPRESS OR IMPLIED, OR OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

Coding Samples

Any software coding and/or code lines/strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

Accessibility

The information contained in the SAP Library documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP specifically disclaims any liability with respect to this document and no contractual obligations or commitments are formed either directly or indirectly by this document.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you, or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

www.sap.com/contactsap

THE BEST RUN SAP