

ESSO Installation Windows (+3.5.0-enterprise)

Introduction

Soffid ESSO is a full Enterprise Single Sign on solution.

Here you can find the details about the **ESSO +3.5.0-enterprise** installation.

Supported platforms

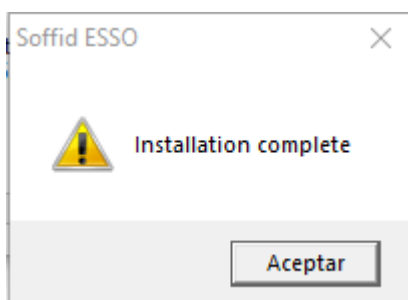
Soffid ESSO supports Windows XP or later workstations.

Windows

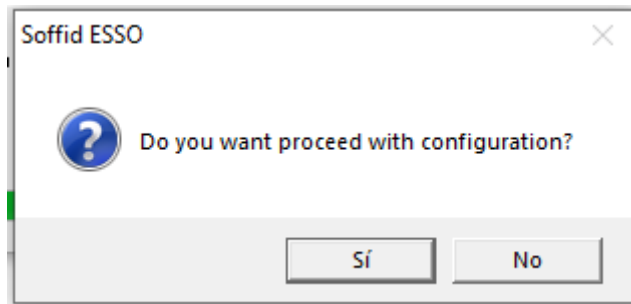
Interactive installation

To install Soffid ESSO, you must follow these steps:

1. Download the latest available installer version from: [Soffid Download Manager](#).
2. Install as administrator. Once the interactive installation has finished, a message window will notice you:

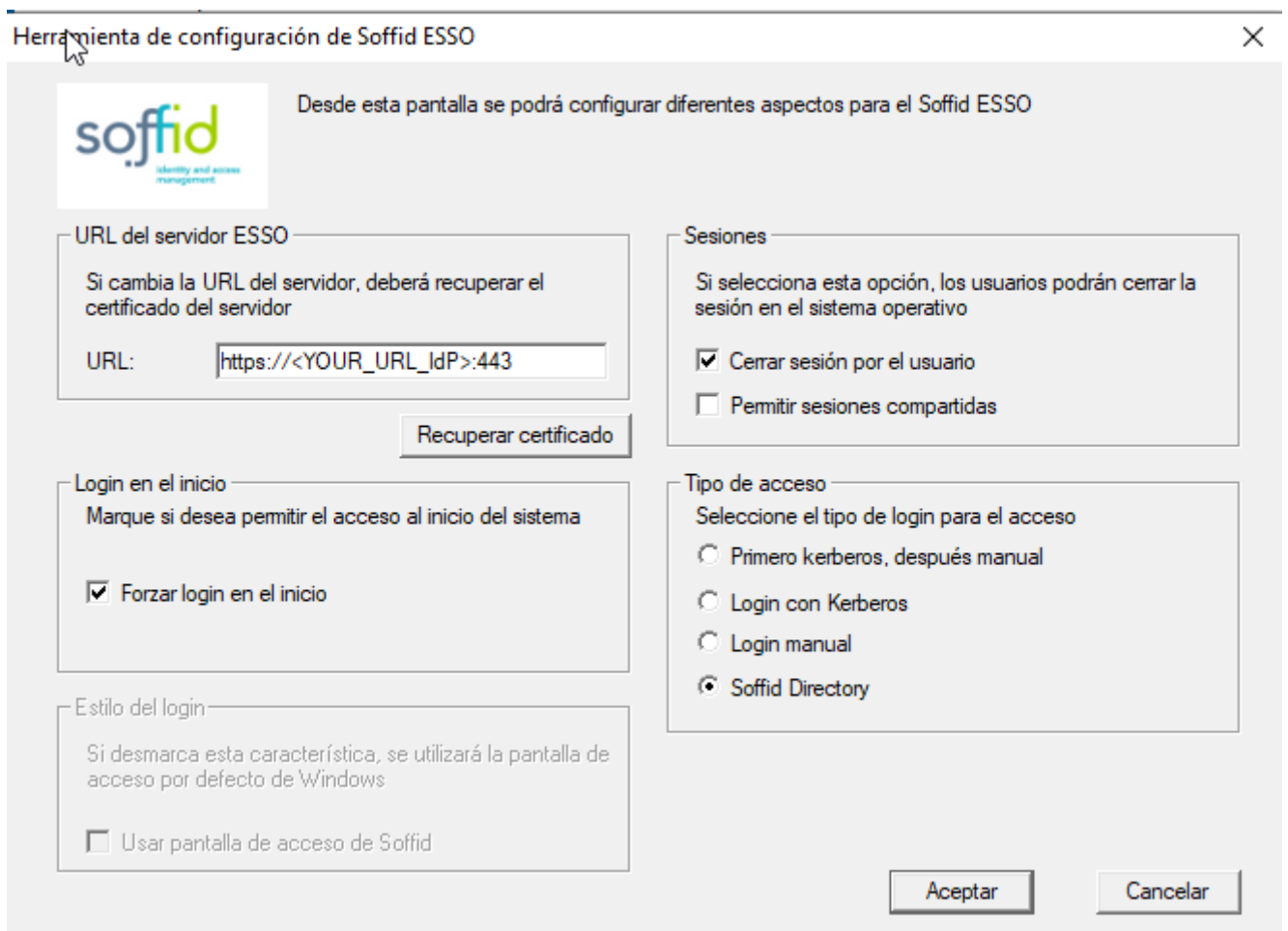


3. Finally, the system will prompt you to configure Soffid ESSO. This prompt will not be shown on updates or silent installations.



3.1. If you click No, the process finish without configuration

3.2. If you clic Yes, you have to configure the URL of the ESSO server, for which you will have to enter the URL of the Soffid identity provider and obtain its digital certificate.




4. After configuring the system, it's **required to reboot the computer**.

For more information, you can visit [the Windows user acces page](#) and [the Windows Administrator access page](#).

Configure the ESSO Profile

1. Then you need to configure the ESSO profile in your Identity Provider

 **Image**

Class :

Esso


Enabled :

Yes

II

Soffid main agent :

soffid

 Soffid system

Seconds to send keep alive from desktop to server :

60

Timeout to close sessions :

180

Enable Windows credential provider :

II

No

Display last logged-on user :

Yes

II

Create local accounts when there is no domain account :

II

No

Maximum number of consecutive days to allow an off-line logon :

Maximum number of consecutive days to allow an off-line logon

Enforce ESSO session when desktop gets on-line. :

II

No

Enforce ESSO sessions :

II

No

Let the user close the ESSO session :

Yes

II

Allow quickly (and insecure) switch between users :


II

No

Hostname format :

Long (fully-qualified host name)


▼



For more information you can visit the following page:

<https://bookstack.soffid.com/books/federation/page/esso>

2. And finally, you can configure the Adaptive authentication rules

 **Image**

Adaptive authentication

Description :

Esso

Condition :

isEsso

Always ask for credentials :

No

| First autl | Password | Kerberos | External | OTP | Email | SMS | PIN | Certifica | FIDO | Push |
|------------|--------------------------|--------------------------|--------------------------|-------------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|-------------------------------------|
| Password | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| Kerberos | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| External | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| OTP | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Email | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| SMS | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| PIN | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Certificat | | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| FIDO | | | | | | | | | <input type="checkbox"/> | <input type="checkbox"/> |
| Push | | | | | | | | | | <input type="checkbox"/> |

+

Close

Silent installation

In order to do a silent installation you can execute the installer from command line with the following parameters:

-q or /q: Quiet installation

-server [url] or /server [url]: to configure the synchronization server URL.

-force or /force: force the installation even if a restart is pending. Not recommended.

-nogina or /nogina: do not modify previos GINA. In this version, this parameter only applies in first installation.

-nopm : to avoid installing Password Manager

To assist in massive deployment scenarios, smart update switch can be set to prevent Soffid to reinstall componenents when the installer version matches the already installed one. This switch does not affect to new installations.

-smartupdate or /smartupdate: Smart update installation

Install EXE Package

EXE Installation is also available for enterprise customers.

Example:

```
C:\> MazingerInstaller-3.5.3-enterprise.exe -q -server https://idp.your-soffid.com:443 -force -nogina -smartupdate -nopm
```

Install MSI Package

MSI Installation is also available for enterprise customers.

To customize configuration parameters, the PARAM variable can be used.

Example:

```
C:\> msixexec /i soffidesso.msi PARAM="-q -server https://idp.your-soffid.com:443 -force -nogina -smartupdate -nopm"
```

Registry configuration entries

The system stores all its settings in the registry branch **HKLM\SOFTWARE\Soffid\esso**.

The values used are as follows:

| Entry | Default Value | Description |
|------------------|---------------|--|
| LogonEntry | Logon | After identifying the user, Soffid ESSO will look at the defined application tree for an application with this key, in order to execute it. |
| OfflineEntry | Offline | If synchronization servers are not reachable, an alternative script will be execute. This entry contains the key of the application entry point to execute in such a case. |
| LocalCardSupport | 2 | Indicate whether to ask for coordinates card at logon time or not. Four values are allowed. 1 - Coordinates card is required 2 - Coordinates card is required if and only if the user is the owner of one card. 3 - Coordinates card is required if the user is connecting from a not registered device. 4 - Never ask for coordinates card. |

| | | |
|----------------------|--------------------------------------|---|
| RemoteCardSupport | 1 | Indicate whether to ask for coordinates card when performing a remote logon. Four values are allowed. 1 - Coordinates card is required 2 - Coordinates card is required if and only if the user is the owner of one card. 3 - Coordinates card is required if the user is connecting from a not registered remote device. 4 - Never ask for coordinates card. |
| LocalOfflineAllowed | 1 | Specifies whether is it permitted to use the workstation when no Soffid synchronization servers are reachable. 1 - It's permitted. 0 - It's forbidden. |
| RemoteOfflineAllowed | 0 | Specifies whether it is permitted to open a terminal server connection against this host when no Soffid synchronization servers are reachable. 1 - It's permitted. 0 - It's forbidden. |
| CertificateFile | root.cer | Specifies the name of the file containing the Certificate Authority certificate used by the synchronization server (X509 DER format) |
| SSOServer | stsm1n3.caib.es, sticlin2.caib.es | Comma-separated list of synchronization server names |
| seycon.https.port | 760 | TCP/IP port used for connecting to SEYCON |
| debuglevel | | Indicates the level of detail of the log: 0 = not recorded anything 1 = Basic Information 2 = Detailed Information |
| ginalogFile | | Name of the file which records the actions taken by GINA. Do not enable it unless needed. |
| ShiroHostName | | Do not modify: It contains the name that the host had when it was registered at Soffid server. |
| startDisabled | false | When it contains the value "true", Soffid ESSO will be started in disabled (or pause) state. Thus, it will not inject any user name or password on user applications. |

| | | |
|-----------------|------------|---|
| MazingerVersion | | It contains the version number of Soffid ESSO. |
| sayaka.domain | | It contains the Active Directory name the workstations belongs to. |
| sayaka.pkcs11% | (reserved) | Each crypto card used by the user will have a corresponding entry indicating the name of the PKCS#11 DLL that can handle it. Do not modify. |

Startup process

Windows XP GINA logon

Soffid GINA is an optional part of Soffid ESSO. It's features are:

- Allows users to log on using smart cards. The digital certificates can be auto enrolled as long as there is a method to know which user it belongs to.
- Allows authorized users to log on with Local Administrator privileges.

Windows Vista Credential Provider

Soffid Credential Provider is an optional part of Soffid ESSO. It's features are:

- Allows users to log on using smart cards. The digital certificates can be auto enrolled as long as there is a method to know which user it belongs to.
- Allows authorized users to run with Local Administrator privileges.

Soffid session startup

After being identified by Windows, the Soffid session startup takes place. Either sequentially or in parallel to desktop startup, the Soffid ESSO session manager (named KojiKabuto after the best ever hero) is the responsible for making the following steps.

Update settings

KojiKabuto will contact Soffid servers o update registry entries using the system configuration introduced at Soffid console (LogonEntry, OfflineEntry, SSOServer, seycon.https.port)

Kerberos handshake

If it's enabled by system administrator, Soffid Synchronization server and the user desktop will perform a Kerberos handshake. If the Credential token shown by user desktop is accepted by any managed Active Directory, Soffid will accept that credential as a prove of identity.

In order to do that handshake, Soffid will create an special user named SEYCON_xxxx for each one of the synchronization servers involved in the login process.

Manual login

If it's enabled by system administrator, or Kerberos handshake has failed, the user will have the chance to enter it's user name and passwords. They will be verified by synchronization server against its internal user database.

Coordinates card

Once logged in, KojiKabuto requested permission to log. At this time, synchronization server could issue a coordinates card challenge. If the user fails to enter the right value for the coordinates requested, the Soffid session will be canceled.

Multiple sessions prevention

At this phase, Synchronization Server will check if the user has any other, not linked, session. If there is any other active session, and the user has not been granted the capability to open more than one (at Soffid console), the system will notice it to both, the new session and the ancient one.

Finally, the new session will take the decision to close the ancient one or to give up. If the user chooses to close the ancient one, the later will show a prompt, and its user will have 30 seconds to answer if he agrees to close that session. Usually the user has left the ancient session open and no user will be present at the ancient session. So, after 30 seconds the session will be closed and the new one will proceed.

SSO Rules activation

Once the session has been created, the SSO rules present at Soffid Console will be compiled and loaded into the Windows Session. Since this moment, every application launched will have its credentials automatically fulfilled.

Startup script

The workstation connects to Synchronization Server to get the session logon script (LogonEntry registry entry with deaefault value "Logon"), and the session offline script (registry entry "OfflineEntry" with default value "offline"), which will be executed at next logon whether no Synchronization server is reachable.

The offline script is stored at %ProgramFiles%\SoffidESSO\Cache\offline.mzn file.

Afterwards, the application menu is populated using the application entries configured at Soffid Console.

Desktop start

Unless the system configuration enables the user to use the desktop before opening the Soffid Sesion, the Desktop is started right now. Otherwise, the desktop would have been started at the initial steps.

System operation

Once the session is started, Soffid ESSO has two main tasks to do:

First. Timely keeps in touch with Synchronization server to confirm the validity of the soffid session.

Second. Performs injection or user names and password to applications, based on the SSO rules bound to each application entry point the user is authorized to execute.\

Enforcing browser addons

Modern browsers, apply certain restrictions to automatically enable browser addons without user intervention:

Google chrome

Google chrome extension is automatically enabled, but requires internet access, as Chrome is going to download the addon directly from Chrome store rather than using the locally installed version. This addon is compatible with Microsoft Edge.

Mozilla Firefox

There is a Mozilla firefox group policy to automatically enable any extension. Follow this link to get it: https://github.com/mozilla/policy-templates/releases/download/v1.11/policy_templates_v1.11.zip

You can alternatively, add the following registry key:

HKEY_LOCAL_MACHINE\Software\Policies\Mozilla\Firefox\Extensions\Locked\1 = "esso@soffid.com"

Internet Explorer (deprecated)

As well, there is a group policy for Internet Explorer. Please, follow this Microsoft link to get it:
<https://docs.microsoft.com/es-es/internet-explorer/ie11-deploy-guide/enable-and-disable-add-ons-using-administrative-templates-and-group-policy>

The GUID of Soffid ESSO group policy is {53252A52-D536-11DF-866D-5B82D67A00D1}

Revision #30

Created 24 September 2024 06:24:43 by pgarcia@soffid.com

Updated 5 March 2025 07:14:16 by dcompany@soffid.com