How to install ESSO?

- ESSO Installation Windows (from 3.3.3-enterprise to 3.4.3-enterprise)
- ESSO Installation Windows (+3.5.0-enterprise)
- ESSO Installation Linux
- Startup process
- Enforcing browser addons

ESSO Installation Windows (from 3.3.3-enterprise to 3.4.3-enterprise)

Introduction

Soffid ESSO is a full Enterprise Single Sign on solution.

Here you can find the details about the **ESSO from 3.3.3-enterprise to 3.4.3-enterprise** iversions nstallation.

Supported platforms

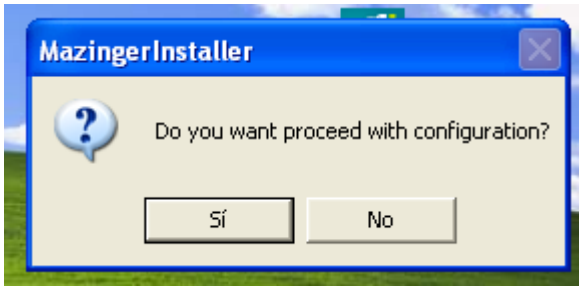
Soffid ESSO supports Windows XP or later workstations.

Interactive installation

To install Soffid ESSO, you must follow these steps:

1. Download the latest available installer version from: Soffid Download Manager.
2. Run it as adminve installation has finished, a message window will notice you:

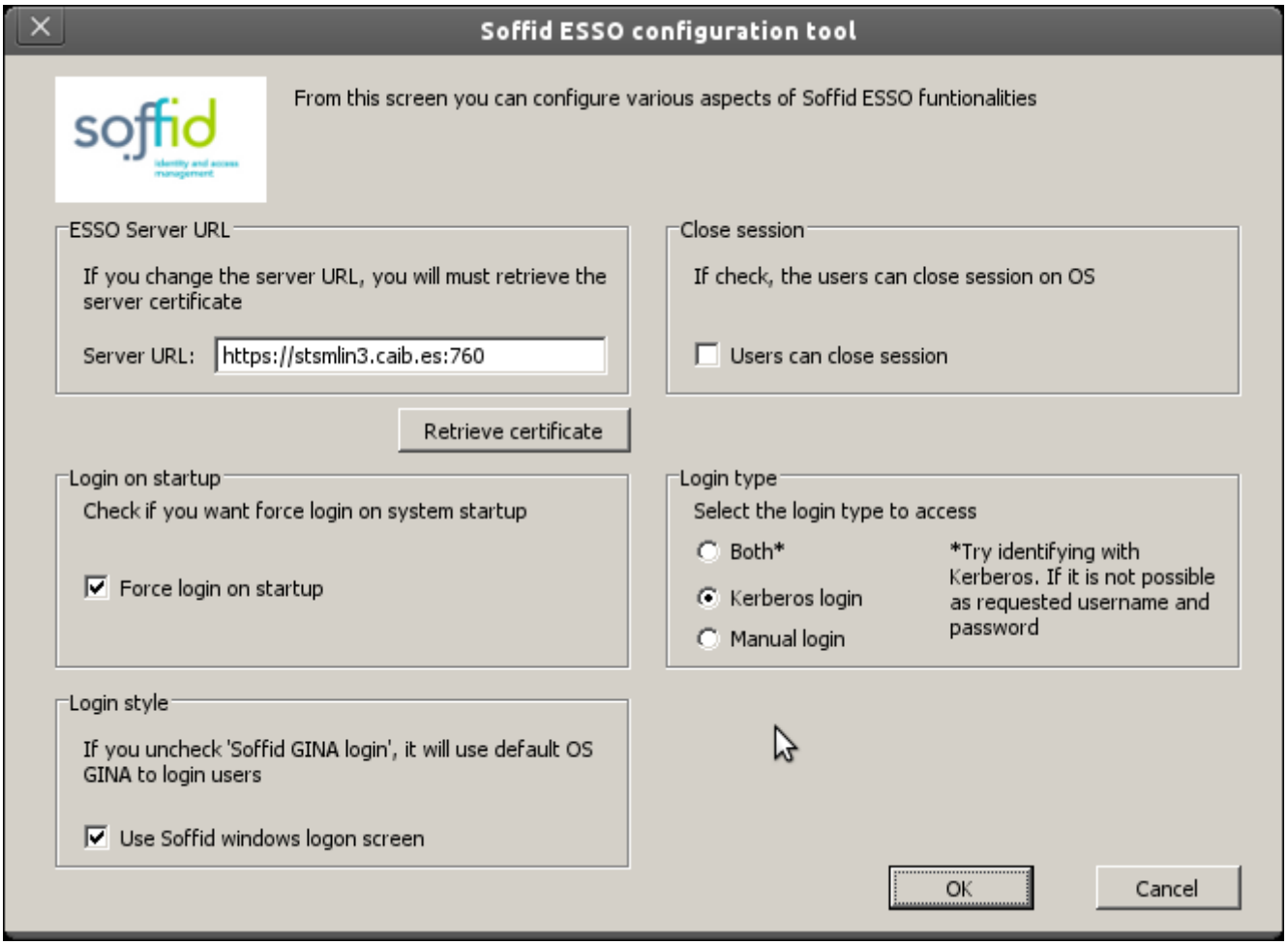
3. Finally, the system will prompt you to configure Soffid ESSO. This prompt will not be shown on updates or silent installations.



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

Interactive configuration

The first task to do at configuration panel is to enter the Soffid synchronization server URL and fetch its digital certificate. To do it, enter its URL on the textbox and press “Retrieve Certificate” button in order to obtain a certificate from the server.



If the URL is correct and the synchronization server is effectively running, the digital certificate will be downloaded and stored at Soffid ESSO directory. Mind that this initial configuration step is highly insecure. Should a man be in the middle, the certificate could be tampered, compromising any further security check.

It is a suitable procedure for testing and quick configuring, but a secure way to install and configure your installation certificate is preferred.

“**Users can logout”** checkbox enable users to open the Soffid notifier menu and close it's Soffid session. After logging out, the user will be allowed to start a new Soffid session with the same or another user name. If the checkbox is not selected, the user will not be allowed to close Soffid session without closing Windows session.

When **“Force login at startup”**, checkbox is selected, the Windows session (explorer.exe) won't start until Soffid session is completely verified and set up. Otherwise, the windows session will start regardless Soffid session is not started yet. If there is an error or denied log-on at Soffid ESSO, windows session will go on without any single sign on feature.

“**Use Soffid windows logon screen**” checkbox is only available on Windows XP. It changes the default (GINA) Windows logon screen, allowing the use of self-registered SmartCard certificates or one-time-password devices. It is not needed on Vista and later.

There are three ways to logon to Soffid:

- **Kerberos login** will reuse the Windows credential acquired by the operating system. If they belong to a managed Active Directory, the user won't need to enter any user name or password to access Soffid.
- When **manual login** is selected, the user must enter a valid user name and password in order to access Soffid.
- When **both** is selected, the system will try first a Kerberos login. Whenever it is not possible (the user is not a domain user), a manual login will be prompted to the user.

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.

Example:

```
C:\> soffidesso.exe -q -server https://server.domain.local:760 -force -nogina
```

Smart update

To assist in massive deployment scenarios, smart update swich 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

Example:

```
C:\> soffidesso.exe -q -server https://server.domain.local:760 -force -nogina -smartupdate
```

MSI Package

MSI Installation is also available for enterprise customers.

To customaize configuration parameters, the PARAM variable can be used:

Example:

```
C:\> msiexec /i soffidesso.mssi PARAM="-q -server https://server.domain.local:760 -force -nogina -smartupdate"
```

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	stsmlin3.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 fullfilled.

Startup script

The workstation connects to Synchronization Server to get the session logon script (LogonEntry registry entry with deafault 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 Sofifd 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 GUUID of Soffid ESSO group policy is {53252A52-D536-11DF-866D-5B82D67A00D1}

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.

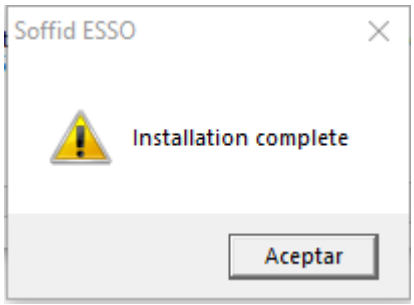
Windows

Interactive installation

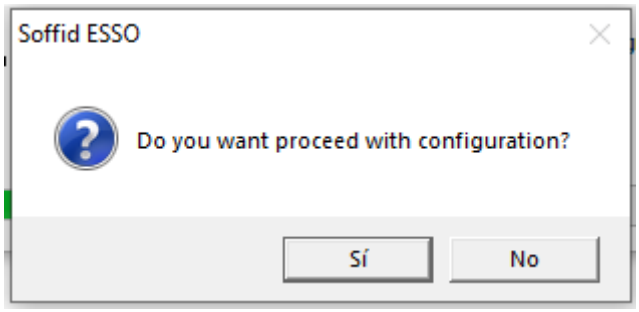
To install Soffid ESSO, you must follow these steps:

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:



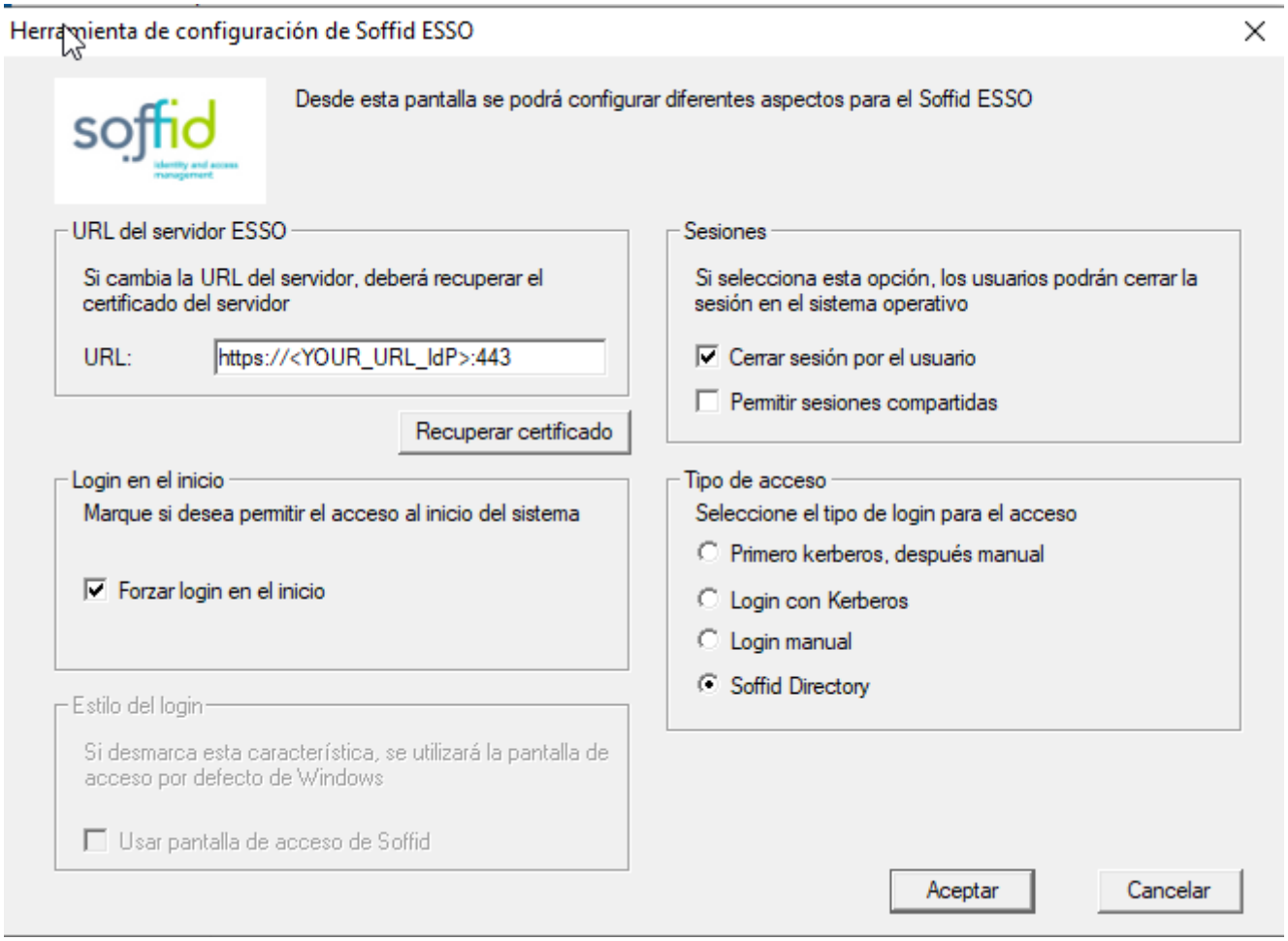
3. Finally, the system will prompt you to configure Soffid ESSO. This prompt will not be shown on updates or silent installations.



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

3.2. If you click Yes, you must configure the ESSO server URL and obtain its digital certificate.

- In Soffid 2, the URL was the syncserver URL.
- In Soffid 3, the URL could be the syncserver URL or the IdP URL, depending on Soffid version and features used.
- In Soffid 4, the URL must be the IdP URL.



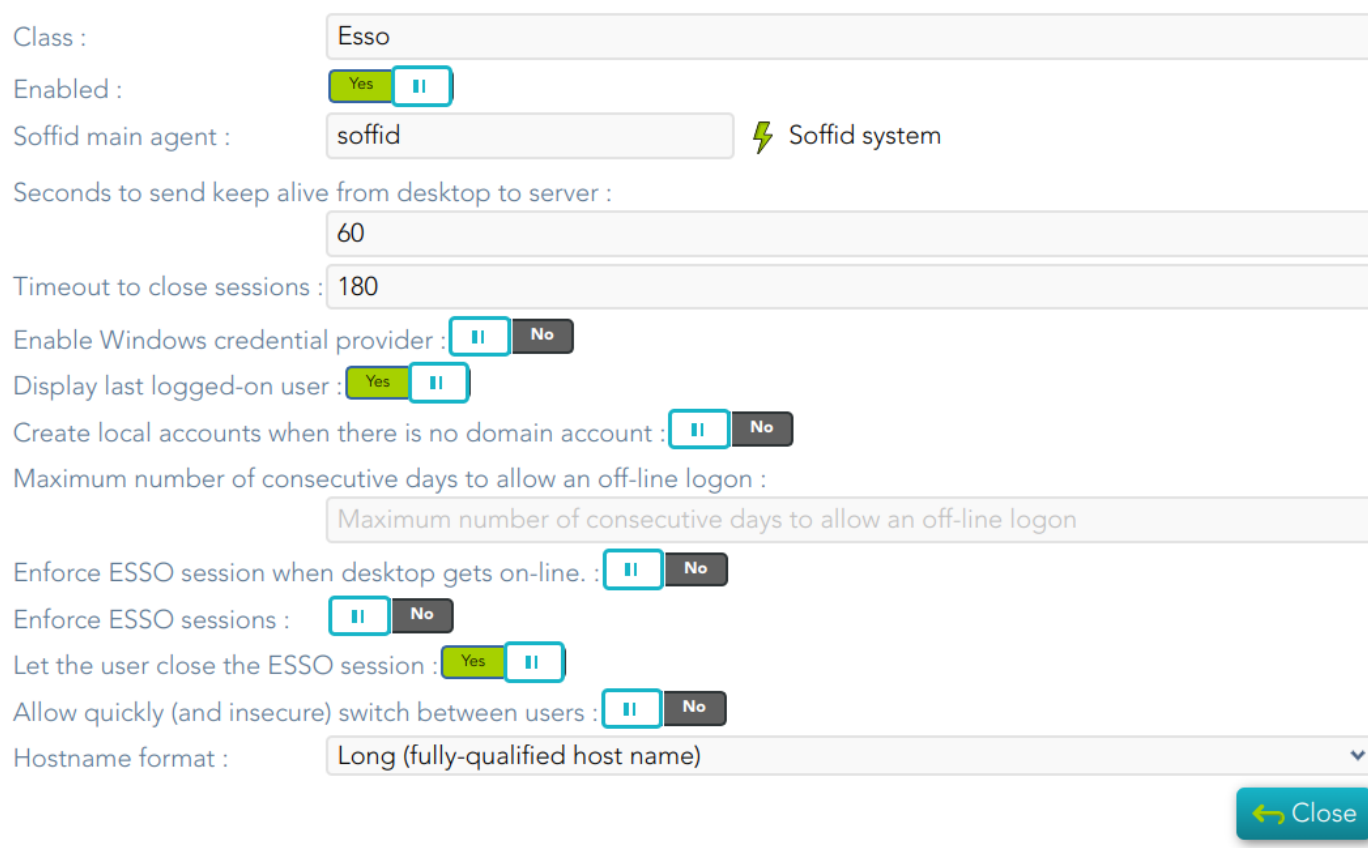
4. After configuring the system, it's **required to reboot the computer.**

> 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

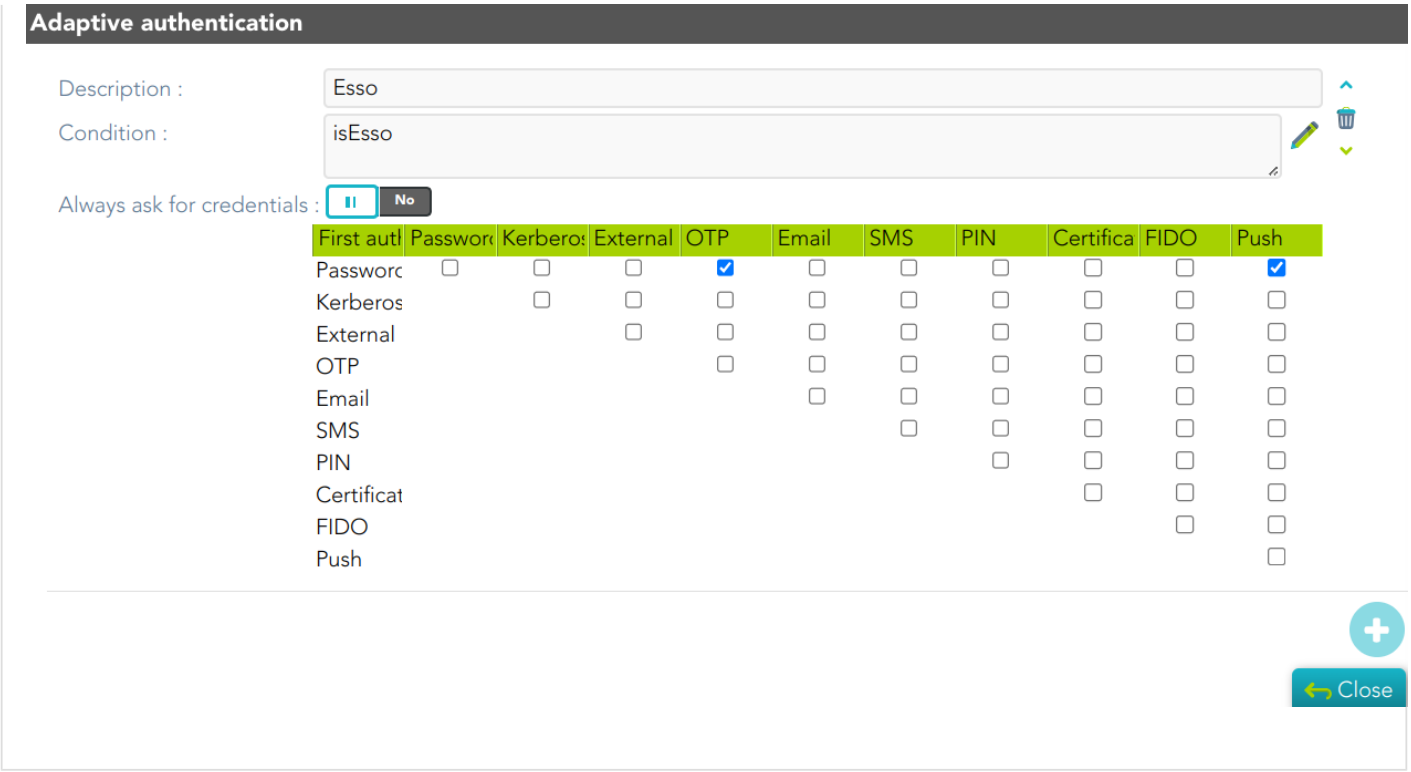
Image



> 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



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 ESSO server URL.

- In Soffid 2, the URL was the syncserver URL.
- In Soffid 3, the URL could be the syncserver URL or the IdP URL, depending on Soffid version and features used.
- In Soffid 4, the URL must be the IdP 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

-forceStartupLogin [true|false]: Enforces or skips Soffid login before displaying the user desktop

-loginType: Specify login type to use:

kerberos: to perform windows SSO

manual: to enter user name and password

both: try kerberos, fallback to manual in case of failure

soffid: use the Soffid credential provider

To assist in massive deployment scenarios, smart update swich 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 customaize configuration parameters, the PARAM variable can be used.

Example:

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

> **Installation problems can be reviewed in the installer log: C:\Windows\SysWOW64\mazinger-install.log**

Install MSI Package with parameters

From version 3.5.52 of the ESSO component onwards, it is possible to **configure parameters** in the installation command.

The **command syntax** is as follows:

```
msiexec /i “msi_name” + PARAM="... /cfg PARAM VALUE /cfg PARAM VALUE /cfg PARAM VALUE ..." /quiet
```

An example:

```
msiexec /i "MazingerInstaller-3.5.52-enterprise-msi.msi" PARAM="-q -server
https://yourCompany.idp.prod.soffid.net -nogina -smartupdate -nopm -forceStartupLogin false /cfg
SSOcredentialprovider true /cfg ManualStartupLogin true /cfg legacyESSO true" /quiet
```

> The parameters included as **/cfg** can be any of the **Registry configuration entries** of the next point.

Registry configuration entries

The system stores all its settings in the registry branch **HKEY_LOCAL_MACHINE\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	stsmlin3.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.
ManualStartupLogin	false	If it contains the value "false", when you start up your computer, a pop-up window appears offering to log you directly into Soffid.
SSOcredentialprovider	true	When it contains the value “true”, Soffid ESSO allow to elevate privileges.
legacyESSO	true	When it contains the value “true”, it allows Soffid ESSO to inject the credentials in native Windows applications.

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 fullfilled.

Startup script

The workstation connects to Synchronization Server to get the session logon script (LogonEntry registry entry with deafault 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 Sofifd 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 GUUID of Soffid ESSO group policy is {53252A52-D536-11DF-866D-5B82D67A00D1}

ESSO Installation Linux

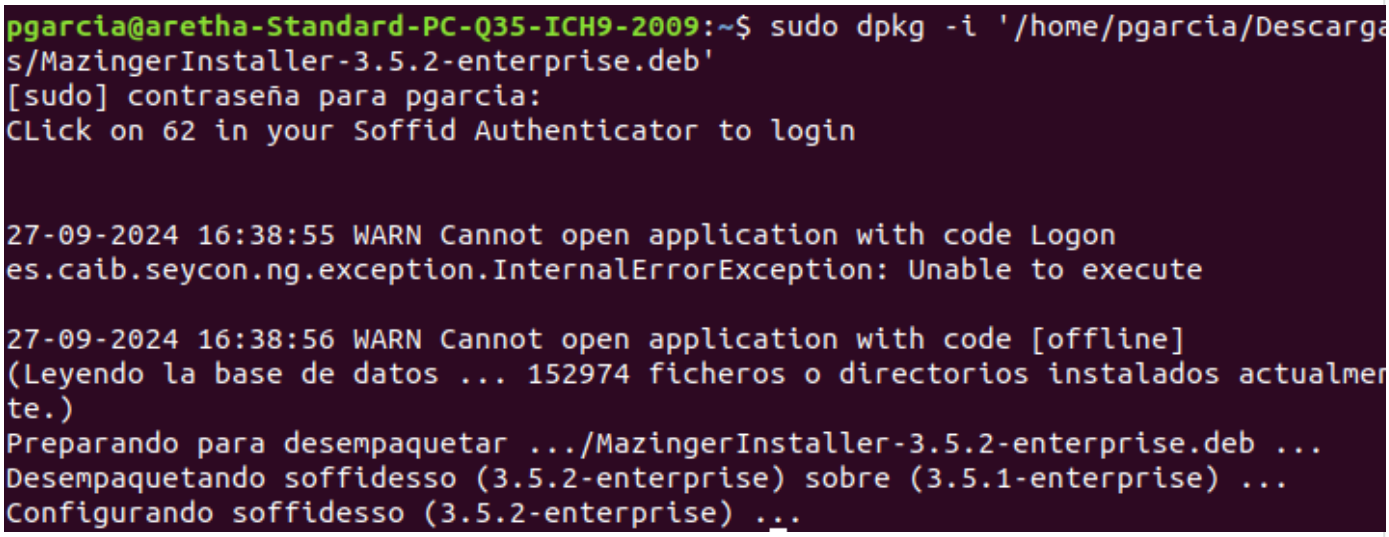
Introduction

Here you can find the details about the ESSO installation.

Installation

```
sudo dpkg -i '<your_path>/MazingerInstaller-3.5.2-enterprise.deb'
```

Image

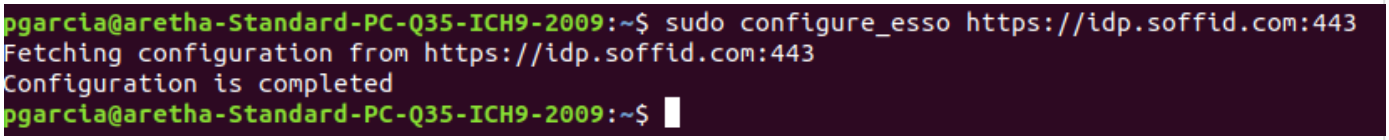


Interactive configuration

1. To configure, you need to run the following command with your Soffid Identity Provider URL.

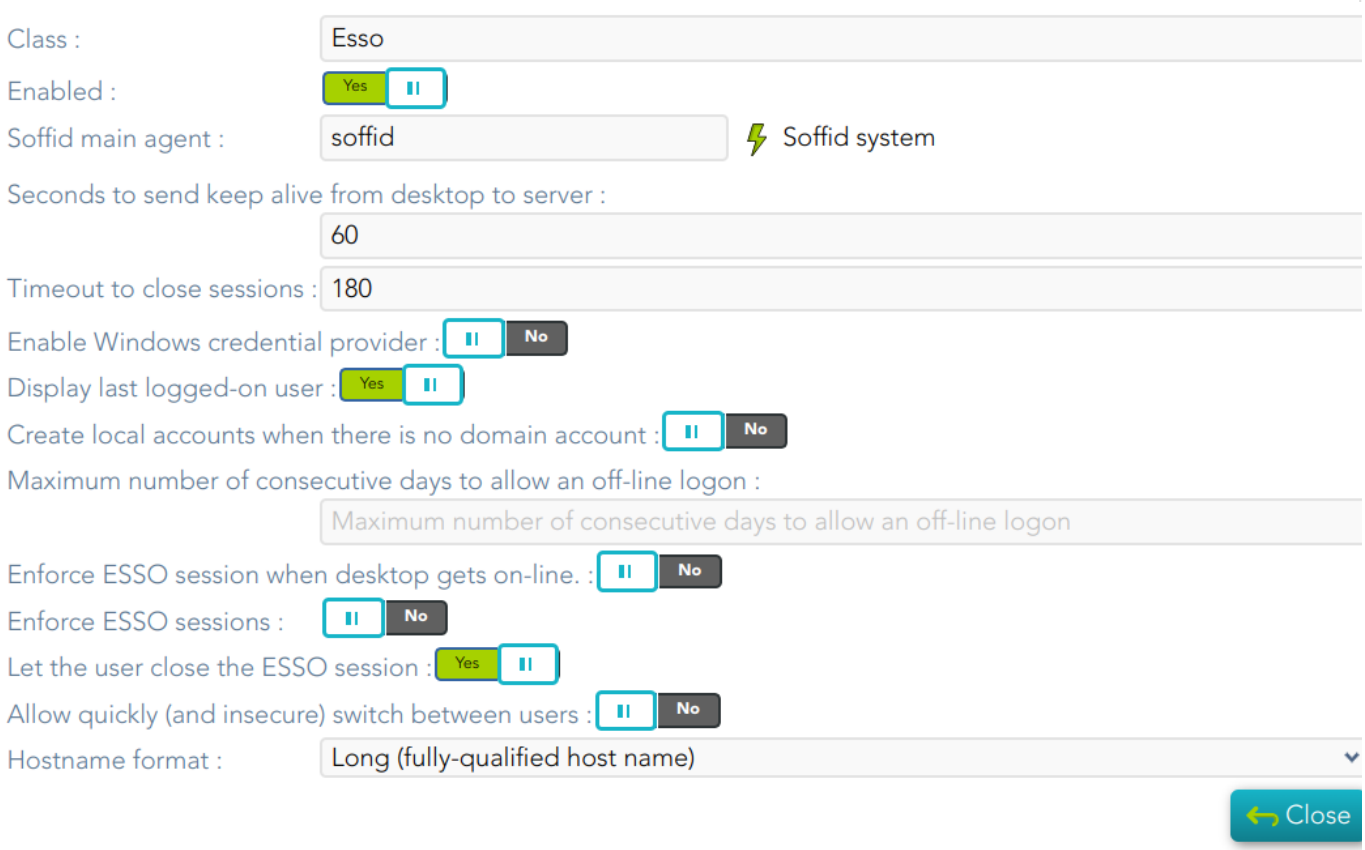
```
sudo configure_esso https://<YOUR_IdP_URL>:443
```

Image



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

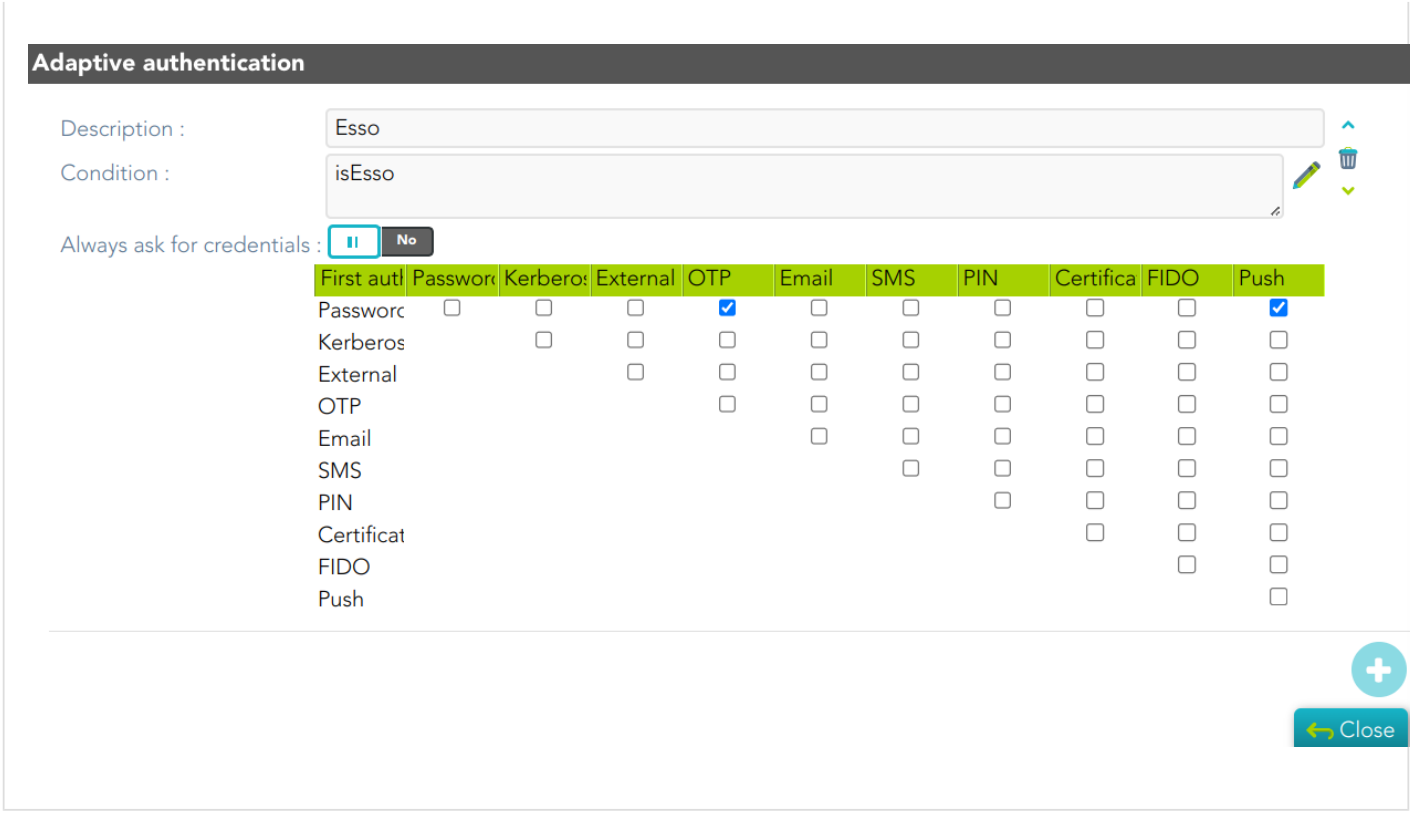
Image



> For more information you can visit the following page:
> https://bookstack.soffid.com/books/federation/page/esso

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

Image



> For more information, you can visit **the Linux Administrator access page** and **the Linux user acces page**.

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

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 fullfilled.

Startup script

The workstation connects to Synchronization Server to get the session logon script (LogonEntry registry entry with deafault 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 Sofifd 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 GUUID of Soffid ESSO group policy is {53252A52-D536-11DF-866D-5B82D67A00D1}