Installing Soffid on your server

Guide to show the installation process os Soffid IAM on your server

- Installing IAM Console
- Installing Sync server
- Configure TLS for IAM Console
- Linux operator guide
- Windows operator guide

Installing IAM Console

Guide to install IAM Console on your own server

Prerequisites

Installing Soffid IAM solution requires the following requirements:

- Windows or Linux (Ubuntu is the most commonly used)
- Java JDK 11 for Soffid 3, Java JDK 17 for Soffid 4
- 8GB RAM
- > 10GB disk space
- Supported database installed

Video Tutorial

Windows

https://www.youtube.com/embed/6c_RuOzb4Y0?rel=0

Linux

https://www.youtube.com/embed/z7YZwb7As74?rel=0

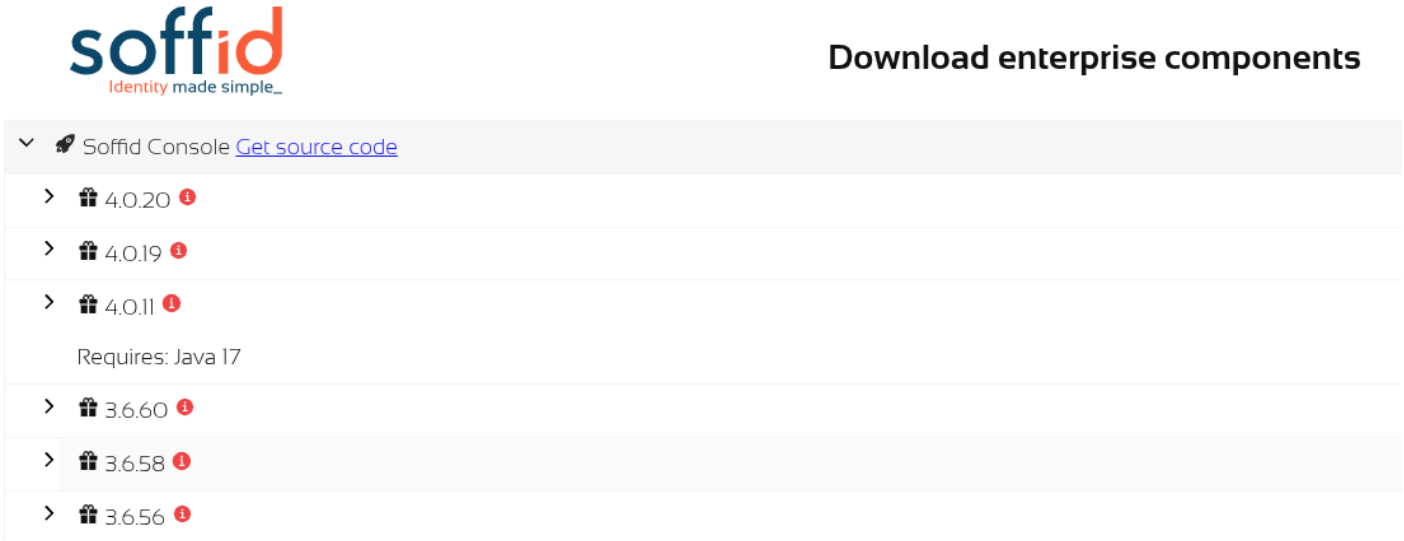
Installation

Download

You can download Soffid 3 and Soffid 4 components from our website Soffid Download Opensource or Soffid Download Enterprise.

> The installation of Soffid 3 and Soffid 4 is the same, although the examples are in Soffid 4, you can do the same for Soffid 3.

Depending on your platform, you can download the MSI, RPM or DEB version.



As soon as the *install-x.y.z.sh* file is in your computer, copy the file into a path of your server.

Installing IAM Console

Windows

Open the installation file. It will create the operating system level service and will start it. After some seconds, the installation wizard will be up and running in port 8080.

Linux

We recommend to install the package like:

```
sudo dpkg -i '/your-path/Soffid Console-Debian_Ubuntu Installer-4.0.20.deb'
```

You can ckeck the IAM Console service status:

```
systemctl status soffid-iamconsole.service
```

Configuration

Then, open the web browser pointing to http://localhost:8080

The wizard will ask for the following information:

- **Host name:** enter the name that will be used by end-users to access to the console. To use the fully qualified domain name is suggested. A virtual service name can be used as well. Mind that the web server will work even when you put a wrong host names. This host name will be used in email notifications that contain a link to the console.
- **User name**: Enter the name of a user with permissions to create tables and indexes in the selected database.
- **Password**: Enter the database user password.
- **Database type**: select the right database engine: Maria DB, MySQL, PostgreSQL, MS SQL Server or Oracle.
- **Database URL**: complete the database URL. The default template use to be good enough, but you can use advanced features depending on the selected database driver:
  - Maria DB and MySQL: https://mariadb.com/kb/en/about-mariadb-connector-j/
  - PostgreSQL: https://jdbc.postgresql.org/documentation/80/connect.html
  - MS SqlServer: https://docs.microsoft.com/es-es/sql/connect/jdbc/building-the-connection-url?view=sql-server-ver15
  - Oracle: https://docs.oracle.com/cd/B28359_01/java.111/b31224/urls.htm#BEIJFHHB

The next step, allows you to enter the name and password for the initial Soffid user. You must enter:

- **Login name**: by default it's admin, but you can use any other naming convention. To change it is good security practice.
- **First name**: Your first name.
- **Last name**: Your last name.
- **Password**: Enter the initial password to use. Write it twice and don't forget it.

Manual Configuration

Configuring service startup

If you are using the RPM, DEB or MSI installers, the service is automatically configured to start up with the computer. If you are using the .tar.gz file, you must enable it manually. Execute these commands as root to start Soffid IAM console service on boot:

```
ln -fs /opt/soffid/iam-console-3/bin/catalina.sh /etc/init.d/soffid-iamconsole
ln -fs /etc/init.d/soffid-iamconsole /etc/rc2.d/S98soffid-iamconsole
ln -fs /etc/init.d/soffid-iamconsole /etc/rc3.d/S98soffid-iamconsole
ln -fs /etc/init.d/soffid-iamconsole /etc/rc2.d/K10soffid-iamconsole
ln -fs /etc/init.d/soffid-iamconsole /etc/rc3.d/K10soffid-iamconsole
```

If something is not running as expected, please check the log at:

```
root@localhost:~# cd /opt/soffid/iam-console-4/logs
root@localhost:/opt/soffid/iam-console-4/logs# less soffid.YEAR-MONTH-DAY.log
```

> Now you can connect IAM Console http://localhost:8080/soffid The first thing you must do is to configure database parameters and admin user. When the console is created, the password for user admin will be valid for 24 hours.

Installing Sync server

Guide to install Synchronization server on your own server

Prerequisites

Soffid IAM sync server requires the following requirements:

- Windows or Linux (Ubuntu is the most commonly used)
- Java JDK 11 for Soffid 3, Java JDK 17 for Soffid 4
- 8GB RAM
- > 10GB disk space
- Soffid console installed

Video tutorial

Windows

Linux

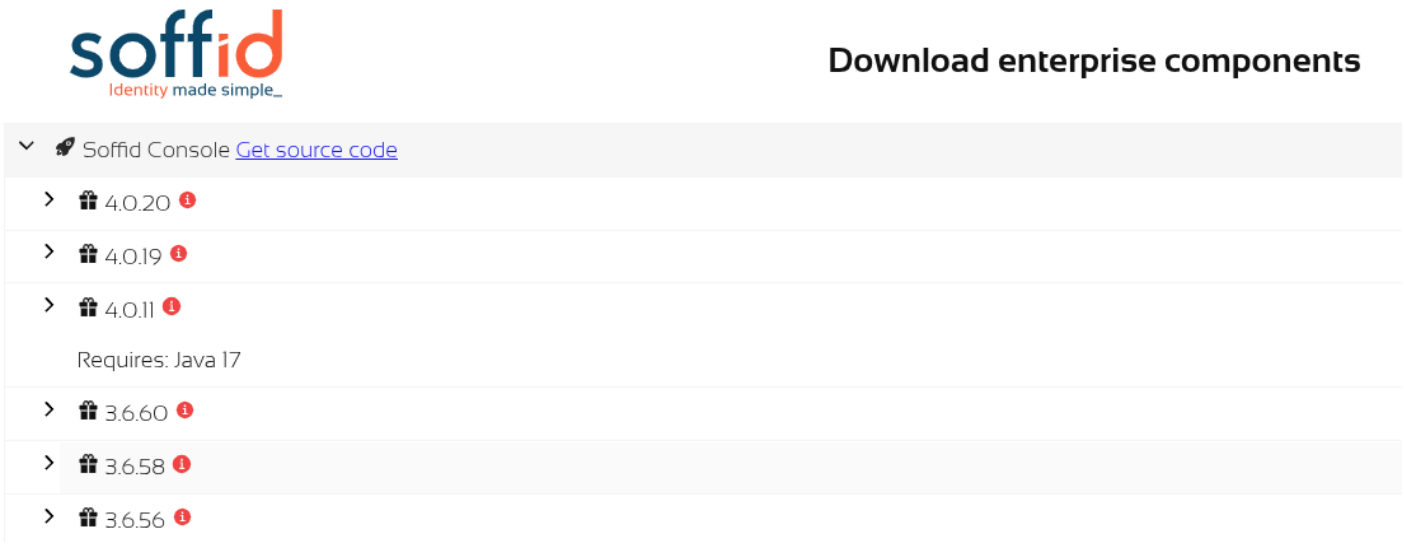
https://www.youtube.com/embed/rvnzwefwBqs?rel=0

Installation

Download

You can download Soffid 3 and Soffid 4 components from our website Soffid Download Opensource or Soffid Download Enterprise.

Click on *Soffid Sync Server* and download the latest version for your OS.



As soon as the *install-x.y.z.sh* file is in your computer, copy the file into a path of your server.

Installing Sync Server

Windows

Open the installation file. It will install the software and will execute the installation wizard.

The installation wizard will ask if it is the first sync server or not.

Linux

```
sudo dpkg -i '/your-path/Soffid Sync Server-Debian_Ubuntu Installer-4.0.0-beta-2.deb'
```

The installation wizard will ask if it is the first sync server or not.

Installing the first sync server

Automatic wizard

If you answer Y to the first question, the wizard will ask for the following information:

- **Database URL**: Use the same URL used to install the console.
- **Database use**r: The user name to connect to the database. It was used during the console installation

- **Database password**: The database user password
- **Host name**: Enter the fully qualified domain name of the host. IP addresses are not accepted.
- **Port to listen**: Enter a TCP port number. The sync server will receive connections from the console or other sync servers through this port. The suggested value is 1760.

After checking the database status, the wizard will register the sync server and will create a new certification authority, as well as a digital certificate for the brand new sync server.

Manual wizard

If the wizar is not launched automatically, you should launch it manually. To do that, you must follow the next steps:

1. Stop syncserver service: `systemctl stop soffid-iamsync.service`
2. Delete previous configuration: `rm /opt/soffid/iam-sync/conf/*`
3. Launch wizard: `/opt/soffid/iam-sync/bin/configure`
4. Start synserver service: `systemctl start soffid-iamsync.service`

The wizard will request about the database configuration:

```
.....
Is this the first sync server in the network (y/n)? y
Database URL (jdbc:....): jdbc:mariadb://localhost/soffid
Database user: ADMIN_USER
Password: xxxxx
This server host name [soffid.my.lab]: localhost
Port to listen to [1760]: 1760
....
```

Installing the next sync servers

If you answer N to the first question, the wizard will ask for the following information:

- **Cloud service**: You can install an on-premise sync server connected to a cloud instance. In this case, the communication stack works in a slightly different way. If this is the case, enter Y. If you are connecting to an on-premise Soffid deployment, enter N.
- **Server URL**: Enter the URL for the first sync server.
- **Tenant name**: Enter the tenant name. If the sync server is not intended to work with a single tenant, enter master.
- **User name**: Enter an administrator user name.

- **Password**: Enter the administrator password.
- **Host name**: Enter the fully qualified domain name of the host. IP addresses are not accepted.
- **Port to listen**: Enter a TCP port number. The sync server will receive connections from the console or other sync servers through this port. The suggested value is 1760.

The wizard will connect to the sync server and create a sync server connection request. The administrator must open the "My tasks" page and approve the request. Once the request is approved, the wizard will finish.

https://www.youtube.com/embed/1OIwWEBKXKs?rel=0

Running synchronization server in root mode

Sometimes it is necessary to run the sync server in root mode to solve a problem. To do this it is necessary to edit the service, modify some data and finally restart the service.

```
sudo systemctl edit --full soffid-iamsync
```

```
User=root
group=root
protectSystem=false
```

```
sudo systemctl restart soffid-iamsync
```

Manual Configuration

Manual service configuration

If you are using the RPM, DEB or MSI installers, the service is automatically configured to start up with the computer. If you are using the .tar.gz file, you must enable it manually. Execute these commands as root to start Soffid IAM sync server service on boot:

```
ln -fs /opt/soffid/iam-sync/bin/soffid-sync /etc/init.d/soffid-sync
ln -fs /etc/init.d/soffid-sync /etc/rc1.d/K01soffid-sync
ln -fs /etc/init.d/soffid-sync /etc/rc2.d/S06soffid-sync
ln -fs /etc/init.d/soffid-sync /etc/rc3.d/S06soffid-sync
```

```
ln -fs /etc/init.d/soffid-sync /etc/rc4.d/S06soffid-sync
ln -fs /etc/init.d/soffid-sync /etc/rc5.d/S06soffid-sync
ln -fs /etc/init.d/soffid-sync /etc/rc6.d/K01soffid-sync
```

Note that if you are running Centos, Redhat7 o version higher than Ubuntu 16.04, you should enable the service in systemctl

```
sudo systemctl enable soffid-sync
```

Once you have installed and configured Soffid Sync Server as a service, you could manage it with the following operations

```
service soffid-sync status
service soffid-sync restart
service soffid-sync start
service soffid-sync stop
```

First synchronisation server configuration

It is not recommended to install the first sync server on the same host where the database is installed.

To configure the server, please execute the following commands:

On Linux:

```
/opt/soffid/iam-sync/bin/configure -main -hostname [hostname] -port 760 -dbuser [soffid] -dbpass [pass] -dburl [jdbc:mysql://localhost:3306/soffid]
```

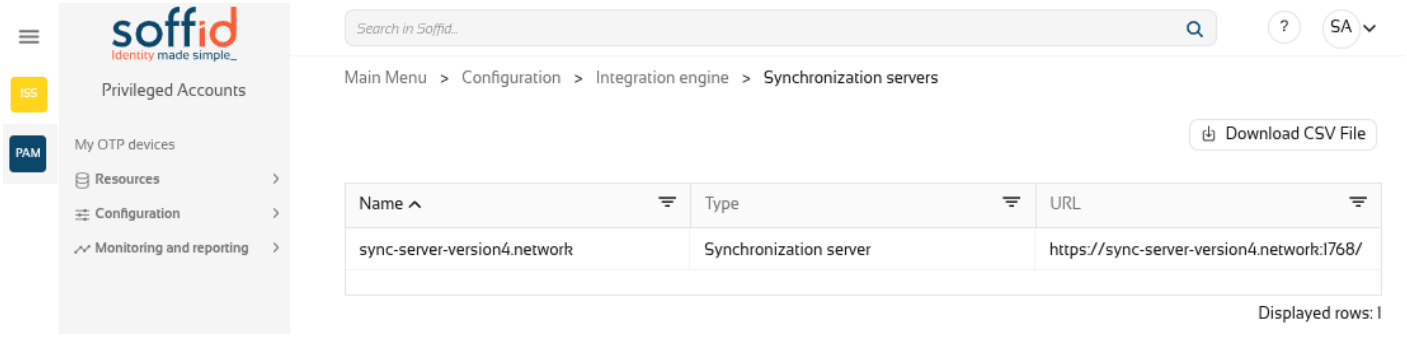
On Windows:

```
%ProgramFiles%\soffid\iam-sync\bin\configure -main -hostname [hostname] -port 760 -dbuser [soffid] -dbpass [pass] -dburl [jdbc:mysql://localhost:3306/soffid]
```

User and password must be the ones created during the installation process.

The hostname value must be a FQDN (fully qualified domain name), for instance, "myhost.mydomain.com" or in a test environment "syncserver.soffid.lab"

Mind the configuration wizard will refuse to register the sync server if this is not really the first sync server. If you really want to register this sync server as the first one, you must open the Synchronization servers page and remove any already registered sync server.



Next servers configuration

In order to configure the next server syncservers, a two step process is required: first, a normal user installs and configure the sync server software; next, a Soffid administrator allows the sync server to join the sync servers network.

To perform the next step, you do not need to enter the database credentials. Instead, the primary sync server URL and a Soffid console user name and password are required.

For instance, you can execute:

On Linux:

```
/opt/soffid/iam-sync/bin/configure -hostname [hostname] -user [user] -pass [pass] -server
[https://yourserver:760] -tenant [master]
```

On Windows:

```
%ProgramFiles%\soffid\iam-sync\bin\configure -hostname [hostname] -user [user] -pass [pass] -server
[https://yourserver:760] -tenant [master]
```

After executing the command, an approval task will appear in Soffid console. The administrator can take ownership of the task and approve or reject it. After approving the server creation, the server will be configured as a proxy sync server (without database access).

The administrator can open the sync servers configuration page to change the sync server role at any time.

Configure a synchronization server proxy without approval in UI

If you want to bypass the appoval process, there is a configuration setting that allows it:

- Open console and click on *Start → Soffid Configuration → Soffid Parameters*:
- Click on *Add New* and, then, write the parameter **soffid.server.register**, set the value to ***direct*** and *Confirm changes*.

https://www.youtube.com/embed/hpgTVeXmChs?rel=0

- Execute the configuration of a synchronization server proxy as follows:
  On Linux:

  ```
  /opt/soffid/iam-sync/bin/configure -hostname hostname -user usuario -pass pass -server https://<yourserver>
  ```

  On Windows:

  ```
  %ProgramFiles%\soffid\iam-sync\bin\configure -hostname hostname -user usuario -pass pass -server https://<
  ```

  Where **hostname** is the name of the synchronization server proxy, **user** and **pass** are the Soffid console user name and password and, finally, **URL** is the first synchronization server URL.

- In the Soffid console, go to *Start→ Soffid Configuration → Agents* and click on *Synchronization Servers* to check if the synchronization server proxy has been registered.

Thus, you can bypass the standard workflow needed for a sinchronization server to join the synchronization servers security network. Otherwise, the standard approval workflow will be required.

Renaming a sync server

You can rename any sync server at any time by removing the conf directory and executing the configure process again, but the main sync server is a special case. If you remove the conf directory, the certification authority managed by the main sync server will be lost, and every single sync server will be thrown out of the security domain.

Instead, to reconfigure the main sync server you can execute

On Linux:

```
/opt/soffid/iam-sync/bin/configure -main -force -hostname hostname -port port -dbuser soffid -dbpass pass -dburl jdbc:mysql://localhost:3306/soffid
```

On Windows:

```
%ProgramFiles%\soffid\iam-sync\bin\configure -main -force -hostname hostname -port port -dbuser soffid -dbpass pass -dburl jdbc:mysql://localhost:3306/soffid
```

User and password must be the ones created during the installation process.

The Soffid installation process changes console setup to reflect the new sync server name

The url connection parameter depends on the database system:

- For Oracle by SID: jdbc:oracle:thin:@localhost:1571:XXXX
- For Oracle by Service Name: jdbc:oracle:thin:@localhost:1571/XXXX
- For Mysql: jdbc:mysql://localhost:3306/XXXX
- For SQLServer: "jdbc:sqlserver://localhost:1433;databaseName=XXXX"
- For Postglesql: "jdbc:postgresql://localhost:5432/XXXXX

> Now you can connect to the IAM console http://localhost:8080/soffid and chek if Console and Syncserver are connected.

Configure TLS for IAM Console

Introduction

The TLS protection of Soffid IAM Console is applied through the configuration of the Apache TomEE embedded in the installation.

This solution is running under java technology therefore we need a jks file (Java Key Store) or a PKCS#12 file with the information of your certificate.

Once you have the Console installed and your certificate in jks format you can follow this steps to configure it the first time or for an update.

Mind that sometimes, the network encryption algorithm is named SSL, in fact, the configuration file still displays the word SSL. However, SSL protocol is now outdated, and TLSv1.2 is used instead.

Preliminary step

Load a PKCS#12 (.pfx) file into jks file

There are many standard ways to store and transfer private keys and certificates, but the most common one is the PKCS#12 format. Its main advantage is that it contains, in a single file, both the private key and the public certificate.

To transform the .PFX file to a java key store (.JKS), and can use the next command (you have to adapt it to your system):

> Replace <YOUR_FILE> for your file name.

```
keytool -v -importkeystore -srckeystore <YOUR_FILE>.pfx -srcstoretype PKCS12 \
  -destkeystore /opt/soffid/iam-console-4/conf/<YOUR_FILE>.jks \
  -deststoretype JKS \
  -destkeypass 12345678 -srcstorepass 12345678 -deststorepass 12345678
```

Next, you will be asked for the PFX encryption password. It must be provided to you along the PFX file.

Next, you will be asked (probably twice) for the password to be used to encrypt the .JKS file. This password must be written down in the server.xml file. At the sample SSL configuration file placed at the top of this page, the sample password is 123456.

> If we have a key and certificate (key, crt), the step to perform the conversion is:

```
openssl pkcs12 -inkey keyfile.key -in certificate.crt -out name_to_export -export


keytool -v -importkeystore -srckeystore name_to_export -srcstoretype PKCS12
    -destkeystore /opt/soffid/iam-console-4/conf/new_certificate_name.jks
    -deststoretype JKS
    -destkeypass password
    -srcstorepass password
    -deststorepass password
```

Configuration

Your certificate

Copy or **replace** your jks file into to the file.

> /opt/soffid/iam-console-4/conf/**YOUR-CERT.jks**

File

The configuration file to modify is the following one.

> /opt/soffid/iam-console-4/conf/server.xml

Sample

Uncomment or add the following sample, that enables the TLS configuration.

The file can contain one or more connectors. This example only allows protocols TLSv1.3.

```
.............
<!-- Define a SSL/TLS HTTP/1.1 Connector on port 8443
        This connector uses the NIO implementation. The default
        SSLImplementation will depend on the presence of the APR/native
        library and the useOpenSSL attribute of the
        AprLifecycleListener.
        Either JSSE or OpenSSL style configuration may be used regardless of
        the SSLImplementation selected. JSSE style configuration is used below.
    -->

    <Connector port="8443"
               protocol="org.apache.coyote.http11.Http11NioProtocol"
               maxThreads="150"
               SSLEnabled="true">
        <SSLHostConfig protocols="TLSv1.3">
            <Certificate certificateKeystoreFile="conf/YOUR-CERT.jks"
                         certificateKeystorePassword="YOUR-PASS"
                         certificateKeyAlias="YOUR-ALIAS"
                         type="RSA"
                         xpoweredBy="false"
                         server="Apache TomEE" />
        </SSLHostConfig>
    </Connector>
.............
```

Parameters

These are the parameters that you have to configure.

Attribute	Comment
port	You can choose the standard 443 or another custom port
protocols (inside SSLHostConfig tag) **sslEnabledProtocols** (inside Connector tag)	You can configure the protocols allowed. For intance, protocols="TLSv1.3" or sslEnabledProtocols="TLSv1.3"
certificateKeystoreFile	The source by default starts from /opt/soffid/iam-console-4/ (the installation directory)

Attribute	Comment
certificateKeystorePassword	The password used to encrypt the jks file
certificateKeyAlias	The alias to identify your key and certificate

To know the key **alias**, you can run:

```
keytool -list -keystore yourcert.jks
```

Restart

> After that, you have to **restart** the **iam-console** services.

```
sudo systemctl restart soffid-iamconsole
```

Logs

> If you have some configuration error, you can search for more information in the Console log (the current day log):
> /opt/soffid/iam-console-4/logs/soffid-YYYY-MM-DD.log

Further information

Additional information can be found at Tomcat website: https://tomcat.apache.org/tomcat-7.0-doc/ssl-howto.html

---

https://es.wikipedia.org/wiki/TLS

Linux operator guide

Startup / Shutdown console

Start Soffid IAM console

```
systemctl start soffid-iamconsole.service
```

Stop Soffid IAM console

```
systemctl stop soffid-iamconsole.service
```

Status

```
systemctl status soffid-iamconsole.service
```

Logs

You can find the console logs at: /opt/soffid/iam-console-4/logs

Startup / Shutdown Synchronization servers

Start Sync server

```
systemctl start soffid-iamsync.service
```

Start Sync server

```
systemctl stop soffid-iamsync.service
```

Status

```
systemctl status soffid-iamsync.service
```

Logs

You can find the syncserver logs at: /opt/soffid/iam-sync/logs and the syncserver service log at: /var/log/soffid/

System backup

Soffid relies on a database to store almost every identity data. So, the first step to perform a daily database backup.

- For Maria DB, look at: Backup and restore overview
- For Oracle, look at: Backing Up The Database
- For SQL Server, look at: Create a Full Database Backup (SQL Server)

Soffid console installation directory should be backed up after every installation or upgrade. Once the upgrade or installation has been done, only the log directory needs to be backed up.

Soffid synchronization servers configuration directory (conf) should be backed up just after configuration. In case of system failure, a new synchronization server should be installed and the conf directory can be restored onto it. The conf directory should be backed up on a different media than the database, due to conf directory contains the private keys that can decrypt the data stored in the database.

Windows operator guide

Startup / Shutdown console

Start Soffid IAM console

To start Soffid console, use service manager, or execute:

```
net start soffid-iamconsole
```

Stop Soffid IAM console

To stop Soffid console, use service manager or execute:

```
net stop soffid-iamconsole
```

Logs

You can find the console logs at: c:\program files\soffid\iam-console-4\logs

Startup / Shutdown Synchronization servers

Start Sync server

To start Soffid Sync server, use service manager or execute:

```
net start SoffidSyncServer
```

Start Sync server

To stop Soffid Sync server, use service manager or execute:

```
net stop SoffidSyncServer
```

Logs

You can find the console logs at: c:\program files\soffid\iam-sync\logs

System backup

Soffid relies on a database to store almost every identity data. So, the first step to perform a daily database backup.

- For Maria DB, look at: Backup and restore overview
- For Oracle, look at: Backing Up The Database
- For SQL Server, look at: Create a Full Database Backup (SQL Server)

Soffid console installation directory should be backed up after every installation or upgrade. Once the upgrade or installation has been done, only the log directory needs to be backed up.

Soffid synchronization servers configuration directory (conf) should be backed up just after configuration. In case of system failure, a new synchronization server should be installed and the conf directory can be restored onto it. The conf directory should be backed up on a different media than the database, due to conf directory contains the private keys that can decrypt the data stored in the database.