INTERNAL / EXTERNAL

Your NEW SuccessFactors Instance is connected to SAP Cloud Identity Authentication Service (IAS).

What happens next?

When SAP Cloud Identity Authentication Service is first connected to your SAP SuccessFactors system, it is set up with the following default configuration:

* Password-based logins only
* Standard password policy
* Authentication rules configured to send all users to password-based login
* No user groups configured
* No corporate identity provider (IdP) configured to handle single-sign on
* User sync setup but not enabled

# 1: Logging in for the first time

**SAP Cloud Identity Authentication Service (IAS) Access**:

If you have been provided a new IAS tenant, your IAS admin will be the S-User associated with your SuccessFactors customer account. That person will have received a registration email. The admin should register and ensure they have access. For existing IAS tenants, please contact your existing IAS admins for support.

**You have a newly created SuccessFactors Instance**:

The S-User associated with the SuccessFactors customer account will already exist in the new instance and in IAS. If a consultant (SuccessFactors or Partner) is the first user to log in, they should follow their normal process for creating their user in SuccessFactors. Then, the IAS admin will need to create these new users manually in IAS to allow them to login to the instance. Once created by the Admin, they will get a user registration email from IAS. After registering, they will be able to access the instance. From that point, the consultant or the customer’s SF Admin will follow their normal steps for setting up Role Based Permissions and adding other users to SF. The user sync process is not turned on at this point, so users must be manually added to IAS.

## 2: ADDING A USER TO IAS

* Login to IAS using the link from the Registration Email
* Select ‘User Management’
* +Add User
* Enter First Name, Last Name and Email Address
* Enter Login Name. This must exactly match the Username of the user in SuccessFactors including case
* By default, the user will receive a registration email. You can choose to set the user’s initial password and communicate the login information through some other option
* Hit ‘Save’

The admin will use a standard login URL to the SF instance. Rather than seeing the SF login page, they will see the IAS login page.

**3: ENSURING THERE IS A USER WITH PERMISSION TO SYNC THE USERS.**

After you have an admin assigned that can update Role Based Permissions you need to ensure that the user setup for the User Sync process has the correct role and permissions. In new instances you will find a user called IPSADMIN that has been created for this role.

If you received both a new SF Instance and a new IPS Tenant, the user password will be set correctly in both places.

*NOTE: If you have an existing IPS tenant you will need to reset the password in both SF and IPS.*

* Login as an SF Admin.
* Go to Admin Tools/Admin Center
* Go to Reset User Passwords
* Go to Reset individual user password (with supplied password)
* Enter Username. IPSADMIN unless you created another user for some reason.
* Search Users.
* Check the box on the left of the appropriate user.
* Enter new password twice.
* Hit Reset User password.

*In either case, you will need to set the Role Based Permissions and the API exception.*

SAP Help has information about the specific RBP settings and the API exception to set:

<https://help.sap.com/viewer/d599f15995d348a1b45ba5603e2aba9b/latest/en-US/2c56095be88043579566be1423d154cd.html>

<https://help.sap.com/viewer/d599f15995d348a1b45ba5603e2aba9b/latest/en-US/265b5fa29d0a426d943cba2ae57e079b.html>

**4: GENERAL SETUP ALL INSTANCES**

**Email Templates.** IAS has email templates for new users, password resets, etc. You will want to review these and customize to meet your needs. In addition, you will want to be sure to NOT enable the internal SuccessFactors version of these emails. That includes the Welcome Message when importing new users. There are predefined email templates for user and administrator related emails. You can also create a custom template set. Unless you have another way to communicate the initial login URL to your users, we recommend you add a basic login URL to the New User email.

SAP Help has more information about Email Templates:

[About Email Notification Templates in Identity Authentication service](https://help.sap.com/viewer/6d6d63354d1242d185ab4830fc04feb1/Cloud/en-US/bb2c79b71f8d47ec877882d78e0ceb39.html)

**Themes and Branding.** IAS supports basic settings for themes and branding. You can add logos, change colors etc. to the login page and others in IAS. You will want to review and set them up to meet your needs.

SAP Help has more information about Themes and Branding:

[About Branding in Identity Authentication](https://help.sap.com/viewer/6d6d63354d1242d185ab4830fc04feb1/Cloud/en-US/32f8d337f0894d269f5f89956803efac.html)

**5: SETTING UP USER GROUPS (OPTIONAL)**

One option for sorting users to different login methods is Groups. These are manually added to the IAS tenant. They can be assigned to users manually or as part of the data sync (see above).

**To create a new group:**

* Select ‘User Groups’
* +Add
* Enter Name, Display Name and Description (optional)
* Hit ‘Save’

**To manually set a user to one or more groups:**

* Select ‘User Management’
* Select a user
* Select ‘User Groups’
* Select ‘Assign Groups’
* Check any groups you want to add the user to
* Hit ‘Save’

SAP Help has information about Groups in IAS:

[About User Groups in the Identity Authentication service](https://help.sap.com/viewer/6d6d63354d1242d185ab4830fc04feb1/Cloud/en-US/ddd067c899f94e2f9006cc4dd417be80.html)

**6: PASSWORD BASED LOGINS (OPTIONAL)**

All instances come pre-configured with password-based logins by default. If you will be using password or 2 Factor logins you will need to review and update Password Policy Settings.

If the default standard password policy doesn't meet your requirements, you can:

* Change to the Enterprise password policy
* Create a custom password policy
* These settings apply to 2 Factor Authentication logins as well

For users of single sign-on (SSO) or other non-password login options (like social sign-on), these password policy settings are ignored.

SAP Help has more details on Password Policy Setting:

[About Password Policies in the Identity Authentication service](https://help.sap.com/viewer/6d6d63354d1242d185ab4830fc04feb1/Cloud/en-US/12b33953a9164b6084319f4785808a8e.html)

**7: 2-FACTOR AUTHENTICATION (OPTIONAL)**

If you will be using 2 Factor Authentication, you will need to setup password policies (see above) and some additional 2 Factor settings. Users will need to be sorted to - Factors using Risk Based Authentication. The users will also need to register their token generator. We support SAP Authenticator, Google Authenticator and other apps that follow the same standard.

SAP Help has more details on 2 Factor and Risk Based Authentication:

[About Two-Factor Authentication in Identity Authentication service](https://help.sap.com/viewer/6d6d63354d1242d185ab4830fc04feb1/Cloud/en-US/0d41cd49f6504f3eaf29b58d616b040f.html)

[About Risk-Based Authentication in the Identity Authentication service](https://help.sap.com/viewer/6d6d63354d1242d185ab4830fc04feb1/Cloud/en-US/bc52fbf3d59447bbb6aa22f80d8b6056.html)

[About setting up SAP Authenticator on your phone](https://help.sap.com/viewer/6d6d63354d1242d185ab4830fc04feb1/Cloud/en-US/ab8a3237cd424a0c97b921100d263b8a.html)

**8: CORPORATE IDENTITY PROVIDER (OPTIONAL)**

Any SAML 2 SSO logins you preform from your corporate identity provider software need to be setup in IAS. You can use the same corporate identity provider for multiple SF instances or use different ones. In addition to setting up the identity provider, you will need to setup Conditional Authentication to send the users to the correct provider. Some settings for corporate identity provider can be accessed directly by SuccessFactors Admins.

NOTE: The following are typical instructions. They will work for most integrations. Please see the additional document links if your architecture is more complex.

**Setting up Corporate Identity Provider in IAS Console:**

* Go to ‘Identity Providers’
* Go to ‘Corporate Identity Providers’
* Hit +Add
* Type a name
* Hit ‘Save’
* Select ‘SAML2 Configuration’
* Browse for the metadata from your corporate IDP
* Import the metadata
* If your provider is ADFS or Azure AD, go to ‘Identity Provider Type’ and Select ‘Microsoft ADFS/Azure AD’
* Hit ‘Save’

**Getting IAS Metadata to Import into Your Corporate IDP:**

* Go to ‘Applications and Resources’
* Go to ‘Tenant Settings’
* Go to ‘SAML 2.0 Configuration’
* Select ‘Download MetaData File’ and save the file
* Import this file into your corporate identity provider to configure the connection to IAS.

SAP Help has information about Corporate Identity Providers and Conditional Authentication:

Setting up Corporate Identity Provider From SuccessFactors Admin Tools

Your Admin can setup a corporate IDP from within SF rather than using the IAS Admin Console:

* Go to ‘Admin Tools/Admin Center’
* Go to ‘Manage SAML SSO Settings’
* Select ‘Upload Asserting Party Metadata’
* Enter a name and select the metadata file from your Corporate Identity Provider
* Hit ‘Upload’

You can also edit the setting, set redirects (see below) and export the IAS Metadata file from this screen:

[Process to Set Up Single Sign-On with Identity Authentication](https://help.sap.com/viewer/568fdf1f14f14fd089a3cd15194d19cc/1902/en-US/1f4783b4b6e64947b9ffc284f3cc6cef.html)

**9: REDIRECT PAGES ALL INSTANCES**

Whatever login options above you are offering, your users need to be sent somewhere when they logout of SuccessFactors or take other actions. These are called Redirect Pages. Password and 2 Factor have one set of redirects. Corporate Identity Provider Logins have another set.

**Setting up Redirects to Handle Password or 2 Factor Login Users:**

These settings can be changed in Admin Tools/Manage SAML SSO Settings. You will need to give your admin user permission to this tool in Role Based Permissions before completing the steps below:

* Login to the instance as an admin.
* Go to ‘Manage SAML SSO Settings’
* Go to ‘Set Non SAML Redirect Pages’
* You will see the following redirects. Update the four redirects as needed:
* Redirect URL when logout
* Redirect URL when session timeout
* Redirect URL for Invalid Login
* Redirect URL for Invalid Manager
* Hit ‘Update Asserting Party’

These are set to default SF pages initially. Customer should provide their own pages. Customer can also change them to point back to IAS so the user can log back in. Handy for the logout and timeout redirects. To get the URL for that, the customer should go to IAS and follow these steps:

* Go to ‘Applications and Resources’
* Go to ‘Applications’
* Select the application for their SF instance
* Go to the very bottom of the page under the title ‘Allow Identity Authentication Users Log On’, copy the URL found there. It will be in this format:

https://IAS\_TENANT\_NAME/saml2/idp/sso?sp=https://www.successfactors.com/SF\_INSTANCE\_NAME&idp=IAS\_TENANR\_NAME

**Setting up Corporate Identity Provider Redirects from SuccessFactors Admin Tools:**

* Your Admin can setup a corporate IDP from within SF Admin Tools
* Go to Admin Tools/Admin Center
* Go to Manage SAML SSO Settings
* Select the Pencil to the right of your Corporate Identity Provider Settings
* At the bottom of the settings you will find four redirects under Enable Additional Setting
* Redirect URL when logout
* Redirect URL when session timeout
* Redirect URL for Invalid Login
* Redirect URL for Invalid Manager
* Customers are strongly encouraged to create and host their own pages to send users to when these events happen. If they are blank, users will be sent to the IAS login screen. To change them
* Select the check box(es) to the left
* Enter the full URL (with HTTP/HTTPS etc.) of the page you want to send the users to
* Select ‘Done’

**10: IDENTITY PROVISIONING SERVICE**

Once admins have configured everything to meet their needs, the last step before having users access the instance is to sync them all from the SF instance to IAS. See the earlier step on insuring there is an API User for this task.

**Make sure you Source data is setup as a Source System in your Target:**

While most of the setup will be done automatically, you will need to ensure that your instance is listed in the sources being sent to IAS:

* Login to your IPS tenant
* Go to ‘Source Systems’
* Select the source that has a name reflecting your SuccessFactors instance
* Go to ‘Properties’
* Scroll down to user
* Your exact SF instance name will be to the right of the user name. If it’s not, select a different source until you find yours
* Go to the ‘Details’ setting for the source and note the System Name
* Go to the ‘Properties’ setting for the source
* Insure that the username in the User settings matches the one from the earlier user sync username step
* Insure that the password matches that of the same user
* Go to ‘Target Systems’
* Select your IAS Tenant
* Go to ‘Properties’
* The URL should match your IAS URL. If not, select a different target until you find the right one.
* Go back to ‘Details’
* Make sure the Source you noted earlier is listed in the Source Systems. If it is not, hit ‘Edit’
* Use the pull-down list to check on your source. DO NOT uncheck any existing sources.

Hit ‘Save’

At this point, you will run the user sync manually one time to insure your users are loaded. If you have a large user population, this may take a long time. So, do it in advance of your go live. Once the initial user load is completed, you will need to enable the job to run on a schedule.

**Running and scheduling the User Sync:**

You should still be on your source settings from the previous step:

* Select Jobs
* In the’ Read Job’ section you can do three things
* Run Job. This will run the delta job that finds changed records only
* Schedule. You can set the run schedule in minutes. If you schedule more than once a day, please make the schedule long enough to insure each run completes before another starts.
* Pause/Resume. Use to stop and start the schedule
* In the Resync Job section you can hit ‘Run Now’ to do a full reload

SAP Help has more information about enabling User Sync:

<https://help.sap.com/viewer/f48e822d6d484fa5ade7dda78b64d9f5/Cloud/en-US/e5b5176c17ae4ae4bd32ae07877ddd79.html>

**Important Legal Disclaimers:**

**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 to 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, unless damages were caused by SAP intentionally or by SAP's gross negligence.

**Accessibility**

The information contained in the SAP 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 in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of wilful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

**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.

**Internet Hyperlinks**

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).

[Copyright/Trademark](https://www.sap.com/copyright)