



Authentication and Provisioning

● Authentication	3
● Form-based authentication	3
● Security	3
● Two factor authentication	3
● Identity federation	4
● Solution	4
● Protocol	4
● Mixed mode	5
● Conversion of existing users	6
● Basic permissions for federated login	6
● Provisioning	8
● Provisioning in conjunction with login	8
● Create users automatically	8
● Automatic provisioning	9
● Antura AD Connector	9
● Antura AD Cloud Sync	9
● Implementation process	10
● Appendix	11
● Activate identity federation	11
● Configuration of trust	11
● Configuring claims	12
● Configuring provisioning via claims	12
● Configuring user information via claims	12

Authentication

Authentication refers to checking the user's stated identity in conjunction with login. Antura supports both *form-based authentication* (ie login with username and password) and *federated authentication*, which means that authentication is done via the company's IdP (Identity Provider). Federated login also enables login with Single Sign-On.

Form-based authentication

Form-based authentication is the default authentication method in Antura. All users with a password can login to the system by entering their username and password at the Antura login page

Security

When form-based authentication is used, user information and a password hash is stored in Antura' database. All passwords are transformed through a strong hash function and an individual salt value. No passwords are thus stored in plain text and cannot be restored from the hash.

There is also a password policy which can be activated in Antura to configure how strong passwords that shall be required, how often they shall be changed, how long they shall remain in quarantine etc. The password policy can be configured by the customer himself via the view *Administration - System Settings - Forms Authentication Settings* in the Antura environment (provided that the *Use Forms Authentication Settings* setting is enabled).

Two factor authentication

Two-factor authentication means that you authenticate yourself by using a combination of two different components, such as a bank card / smart card (something that the user has) and a PIN code (something that the user knows). Two-factor login can be enabled via *Activate two factor* in the settings for forms authentication. When enabled, all users will be required to setup a secret by scanning a QR-code with Google Authenticator. On subsequent logins the users will be required to also enter a one-time passcode from the app, along with the username and password. If the two-factor login is disabled all secrets will be deleted. For more details see the document "Antura – Two factor authentication".

Identity federation

Identity federation makes it easier for your users to log in to Antura using your organization's Identity Provider (IdP). This also allows users to log in to several different applications with the same username and password. This is referred to as single sign-on (SSO).

Solution

Internal users are approved by the customer's IdP and then connect to Antura with a valid token. The customer's IdP approves users if they are a member of one or more designated groups (this administration is handled internally by the customer's IT department). If the username is not found in Antura, the login is denied. Antura thus does not check whether the user has permission to log in, but the assumption is that the users that the customer's Identity Provider authenticates and lets through also have access to the system.

You can prevent a user from logging in via federation by deleting or inactivating the user in Antura. It is also possible to allow users who does not in Antura to log in via federation and then automatically be created in Antura during login or alternatively enable disabled users to be activated automatically in Antura (see section "Create users automatically").

External users (i.e. users who are not in the customer's user directory) can continue to log in to Antura even if identity federation for internal users is activated, provided that they are not removed (see section "Mixed mode").

Users can also be provisioned, i.e., user data can be synchronized via the customer's IdP to Antura, see section "Provisioning".

Protocol

Antura supports the following identity federation protocols:

- OpenID Connect (OIDC)
- SAML2 (SAML 2.0 tokens)
 - Requires the customer's Identity Provider to expose metadata endpoints
 - Supports SP-initiated SSO/SLO (no support for IdP-initiated SSO/SLO)
- WS-Federation (SAML 1.1 tokens)

We recommend OIDC or SAML2. These protocols integrate well with Microsoft Entra ID, IBM Tivoli and several other Identity Providers. Antura also supports WS-Federation, which is a protocol that integrates with ADFS, which works in the same way as for SAML2 described in this document.

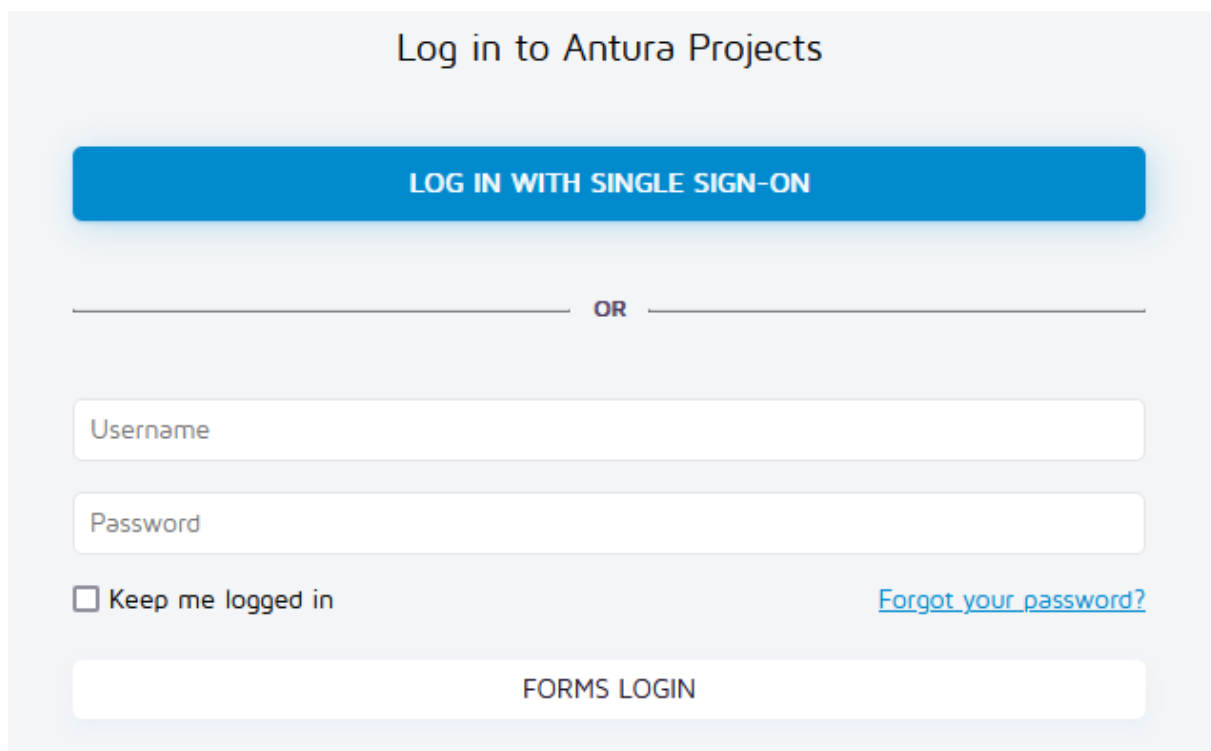
IBM Tivoli

By default, Tivoli sends tickets containing a Renewal element. Antura cannot handle this if WS-Federation is used and the connection will not work. Renewal must be configured away in Tivoli.

Mixed mode

It is possible to combine multiple different ways of logging in. For example, one could have forms-based login enabled meant for external users and a federation protocol enabled meant for internal users.

In this case, the login page would look like this:



The image shows a login page titled "Log in to Antura Projects". At the top, there is a large blue button with the text "LOG IN WITH SINGLE SIGN-ON". Below this button, there is a horizontal line with the word "OR" in the center. Underneath the line, there are two input fields: "Username" and "Password". Below the "Password" field, there is a checkbox labeled "Keep me logged in" and a link that says "Forgot your password?". At the bottom of the form, there is a white button with the text "FORMS LOGIN".

The internal users login by clicking on the button with the text "LOG IN WITH SINGLE SIGN-ON", while the external users login by using the forms-based authentication form.

Which texts are displayed on the buttons is configurable via the view *Administration – System – Language settings – Translations*.

Translations

Filter: All

Name	Type	Svenska	English	Dansk	Suomi
Business area					
Cost category					
Effect type					
Issue category					
Issue status					
Login button					
LocalProtocol	Login button	Formulärsinloggning	Forms login		
Saml2Protocol	Login button	Logga in med Single Sign-on	Log in with Single Sign-on		
WindowsProtocol	Login button	Logga in med Single Sign-on	Log in with Single Sign-on		
WsFedProtocol	Login button	Logga in med Single Sign-on	Log in with Single Sign-on		
Properties					
System name					

It is also possible to enable different protocols depending on which network a user is on. For example, this makes it possible to hide the forms login for internal users and the federated protocol login for external users. If only one federated protocol is enabled for a user, the user will be sent to the login page of that protocol automatically.

Conversion of existing users

Before the solution is activated in the test and production environment, existing internal users need to be updated so that their username matches the username that the customer's Identity Provider sends as a claim. External users can retain previous usernames. Antura can help to mass-update users via a script run if needed. The customer then needs to assist Antura with an Excel file that contains all existing, respectively new, usernames. It can also be done manually via the view *Administration - Users* in the Antura environment.

Note that a user who is created manually in Antura and then logs in via federation (with the same username) will be converted to a federated user. This means that the user's information is overwritten with information from the customer's Identity Provider and the user will no longer be able to log in other than via federation.

Basic permissions for federated login

All users who log in via SSO are automatically added to a user group so that an administrator can easily set permissions for the entire group. The user group is created by the system and is named "Internal users", but the group name can be changed after the system has created it.

This group can be used to give internal users some basic permissions in Antura. Extended permissions can be handled manually in Antura.

Permissions for external users are handled manually in Antura in the usual way by assigning these users to a user group with configured permissions.

Provisioning

Provisioning means synchronization of users and user data. All information for users is updated from the company's Identity Provider.

There are three different ways to provision users:

- When logging in
- Automatically
- Manually

Provisioning in conjunction with login means that the user information is updated every time a user logs in to Antura via so-called claims sent from an Identity Provider. New users can be created automatically when logging in to Antura.

Automatic provisioning means that the user data is continuously updated based on synchronized AD groups. This allows user data and user accounts to be created long before a user logs in to Antura for the first time. Provisioning can also be run on manual request.

Provisioning in conjunction with login

Users found in the Antura environment will be automatically logged in to Antura via SSO. If the user already exists in Antura, user information sent from an Identity Provider can be updated when a user logs in to Antura. How the user data is to be mapped can be configured in Antura. If no configuration of synchronized user data is done, a default mapping is used (for more details see section "Configuring user data via claims" in Appendix).

Whether user information is to be updated in conjunction with login is controlled via a setting that Antura Support is handling (for more details see section "Configuring provisioning via claims" in the Appendix).

Create users automatically

Users who are allowed to log in by the company's IdP can either have their account in Antura created automatically at the first login or be denied login if an account is missing. Accounts can then be created manually via the user interface in Antura. Whether the customer wants users to be created automatically or not is controlled via a setting (for more details see section "Activating identity federation" in the Appendix).

Automatic provisioning

Automatic provisioning from Active Directory and Microsoft Entra ID is provided through the add-on products "Antura AD Connector" (for on-prem only) and "Antura AD Cloud Sync" respectively according to the sections below. Unlike provisioning via login, users are created and updated from synchronized AD groups that take place continuously or automatically via a nightly job.

Antura AD Connector

With the add-on product *Antura AD Connector*, it is possible to configure provisioning of users and groups from Active Directory to Antura. New users are created and existing users are updated from synchronized AD groups at night in Antura. Actions for synchronized users (such as deleted AD users, disabled AD users, AD users who do not belong to a synchronized group, etc.) are controlled via synchronization settings for users in Antura. The add-on product also includes user authentication. For more information, see the document "Antura AD Connector".

Antura AD Cloud Sync

With the add-on product *Antura AD Cloud Sync*, it is possible to configure automatic provisioning of users and groups from Microsoft Entra ID to Antura via SCIM. New users are created and existing users are updated from synchronized AD groups continuously in Antura. Actions for AD users (such as new, updated, deleted AD users) are controlled from Microsoft Entra ID. For more information, see the document "Antura AD Cloud Sync".

Implementation process

Implementation usually follows the steps below:

- 1.** Antura and the customer agree on the configuration to be used. For example, which protocol to use and what claims are to be sent.
- 2.** Both parties prepare by configuring their systems (Antura and IdP) with what can be done before the implementation.
- 3.** A date is determined when the configuration is to be implemented.
- 4.** On the date of the implementation, the final configuration is made, federation is activated and existing users are migrated if needed.

Appendix

Activate identity federation

To activate identity federation with SAML2, the following configuration is made:

1. Set the setting *Authentication:Protocols:Saml2:Enabled* in the *Application.config* file to true to activate identity federation via SAML2.
2. In the setting *Authentication:Protocols:Saml2:EnabledNetworks* in the *Application.config* file, specify the networks (IP addresses) for the users that should be able to reach the SAML2 login. If no network is specified, all users can access the SAML2 login page.
3. The setting *Provisioning:SsoCreateNewUsersAutomatically* in the *Application.config* file is set to true if the customer wants synchronized users to be created automatically in conjunction with login via SSO.

Configuration of trust

Below follows instructions on how to set up a federation trust with Antura in Microsoft Entra ID.

1. Log in to the Microsoft Entra admin center (<https://entra.microsoft.com/>) with your Microsoft 365 account.
2. Navigate to Enterprise applications.
3. Click on "New application".
4. Click on "Create your own application".
5. Write what you want to name the trust, usually you set up a trust for Antura production environment and a trust for Antura test environment. One suggestion is to include "Prod" or "Test" in the application name.
6. Select "Non-gallery application" and click on "Create".
7. Once the application is created, navigate to "Single sign-on". Select "SAML". Under "Identifier (entity ID)" enter the actual URL to the Antura site: "https://customer.projects.se". Under "Reply URL" enter the actual URL to the Antura site: "https://customer.projects.se/oauth/Saml2".
8. Antura will need the URL to the "App federation metadata url".
9. Navigate to "Users and groups". Here we can choose which Microsoft Entra ID users/groups will be allowed to log in to Antura Project's production/test environment.

Configuring claims

Username, first name, last name and e-mail are mandatory fields that must be sent from an Identity Provider. Other fields are updated if they are sent from the customer's IdP (see the section "Configuring user information via claims") provided that provisioning via claims is activated (see the section "Configuring provisioning via claims").

Configuring provisioning via claims

To enable provisioning of user data via claims, the setting *Provisioning:UpdateUsersFromClaims* in the Application.config file is activated. If this is set to true, the user information will be updated automatically in conjunction with login via SSO.

Configuring user information via claims

Mapping of claims from an Identity Provider can be done by configuration of settings set in the Application.config file. If the respective system setting for the claim is not set, the default value listed in the column "Default" is set.

If the claim is not found, the field gets an empty value. Claims are accepted regardless of whether uppercase or lowercase letters are used.

Setting	Information	Default
Authentication:Protocols:Saml2:ClaimTypes:Login	Username	http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname
Authentication:Protocols:Saml2:ClaimTypes:FirstName	First name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
Authentication:Protocols:Saml2:ClaimTypes:LastName	Last name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
Authentication:Protocols:Saml2:ClaimTypes:Initials	Initials	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/initials
Authentication:Protocols:Saml2:ClaimTypes:Email	E-mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Setting	Information	Default
Authentication:Protocols:Saml2:ClaimTypes:Company	Company	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/company
Authentication:Protocols:Saml2:ClaimTypes:Department	Department	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/department
Authentication:Protocols:Saml2:ClaimTypes:StreetAddress	Address	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/streetaddress
Authentication:Protocols:Saml2:ClaimTypes:PostalCode	Postal code	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/postalcode
Authentication:Protocols:Saml2:ClaimTypes:City	City	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/city
Authentication:Protocols:Saml2:ClaimTypes:Telephone	Phone	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/otherphone
Authentication:Protocols:Saml2:ClaimTypes:MobilePhone	Mobile	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/mobilephone
Authentication:Protocols:Saml2:ClaimTypes:Facsimile	Facsimile	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/facsimileTelephoneNumber