

Authentication and Provisioning

Antura AB, www.antura.se

2605 (May 2026)

- Authentication 4
  - Overview 4
  - Form-based authentication 4
    - Security 4
  - Two-factor authentication 4
    - Introduction 5
    - Login with two-factor authentication 5
    - Activate two-factor authentication 8
  - Identity federation 9
    - Solution 9
    - Protocol 9
    - Mixed mode 10
    - Conversion of existing users 11
    - Basic permissions for federated login 12
    - Activate identity federation 12
    - Configuration of trust 12
    - Configuring claims 13
- Provisioning 15
  - Overview 15
  - Provisioning in conjunction with login 15
    - Create users automatically 15
  - Automatic provisioning 16
    - Provisioning with Active Directory 16

- Provisioning with SCIM 21
- Implementation process 33
- Troubleshooting 34
  - Two-factor authentication 34
  - SCIM troubleshooting 34
- SCIM attribute mapping 37
  - User attributes 37
  - User properties 39
  - Group attributes 41
  - Synchronization of extension attributes 42

Authentication

Overview

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 log in 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 are stored in Antura's database. All passwords are hashed using 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 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 set up a secret by scanning a QR code with Google Authenticator. The Authenticator account is named with both the system name and login (for example **`Antura - Demo System:user@example.com`**), which makes entries unique when the same user has access to multiple Antura systems. 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 two-factor login is disabled all secrets will be deleted.

Introduction

With 2-factor authentication enabled, login is not only done with a password, but also with the help of “a second factor”. Antura has chosen to build a solution where a mobile device and an app are used to generate a code that serves as the second factor.

Support for two-factor authentication is aimed at organizations that use what we call “form login”, which means organizations that do not have any other solution for authentication such as identity federation or AD login.

Login with two-factor authentication

When 2-factor authentication is enabled (see section “Activate two-factor authentication” below), the following dialog is shown to a user the first time they log in with form authentication.

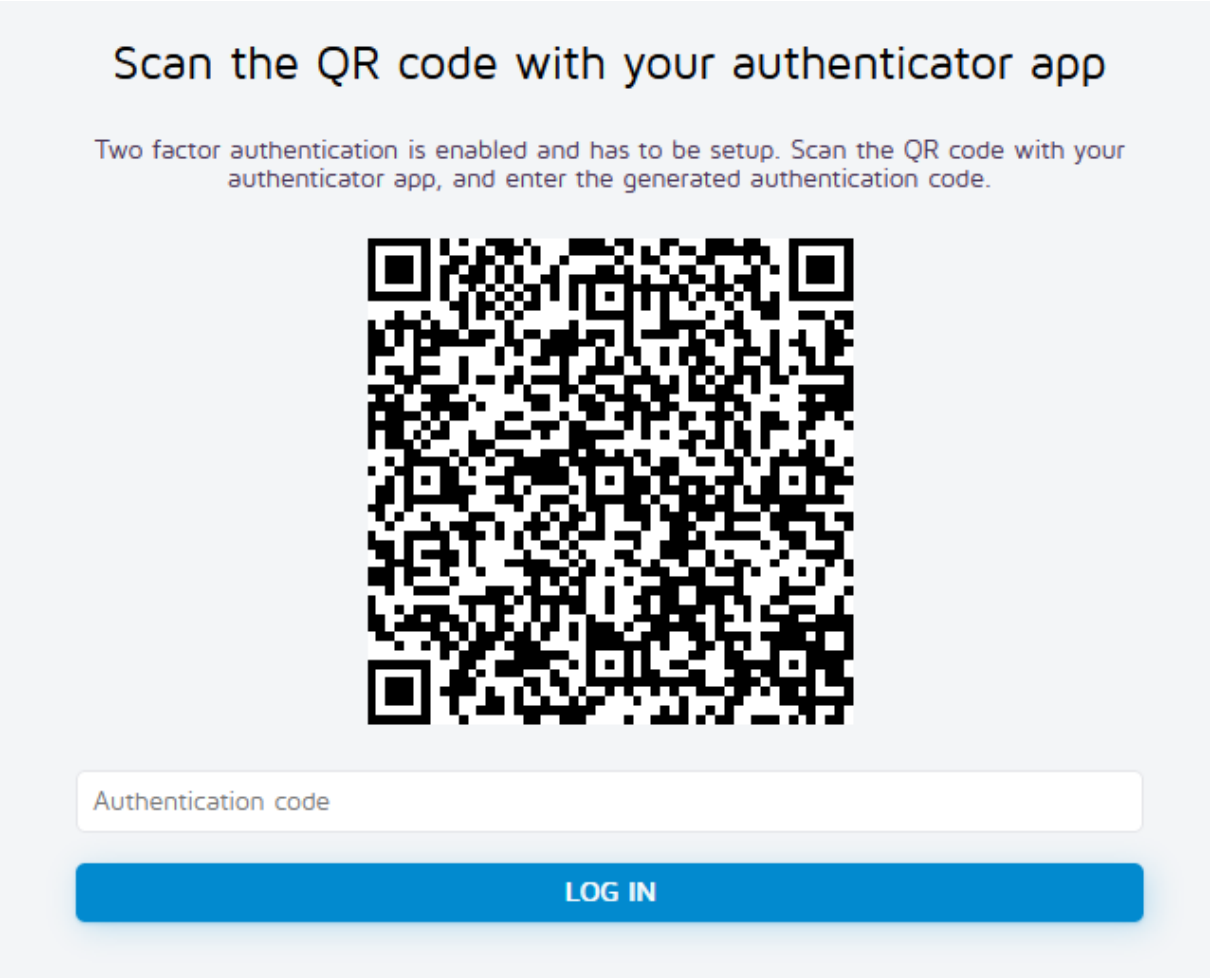


Figure 1 – The first login

The user is presented with a QR code that is scanned in the Authenticator app.

In the Authenticator app, the account is named using both the system name and the login (for example **`Antura - Demo System:user@example.com`**). This makes the entries unique when the same user has access to multiple Antura systems.

After the code is scanned, a code will be generated in the Authenticator app. After the code has been entered into the form, the user will be sent back to the login page.

For subsequent logins with form authentication, the user will instead see the following dialog. The user enters the generated code to log in to Antura.

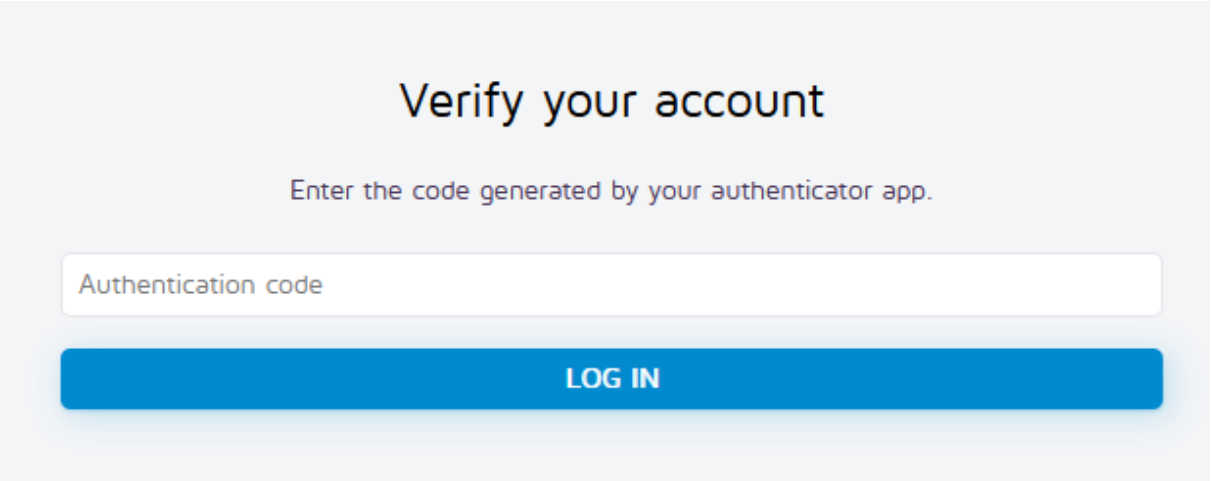


Figure 2 – Subsequent logins

Reset secret

If a user for some reason loses their second factor, it needs to be reset by a user administrator before the user can create a new "secret". This is done for the user in the *Administration - Users* view.

This means that the user will need to enable two-factor authentication again before being able to log in.

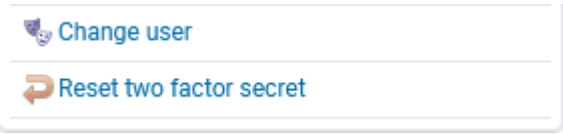


Figure 3 – Reset secret

Authenticator app

There are several apps that can be used for authentication. Two common apps are Microsoft Authenticator and Google Authenticator. Both are available for free download from the Google Play Store or the Apple App Store.

Activate two-factor authentication

Support for two-factor authentication is enabled in the *Administration - System Settings - General* view under the “Forms Authentication Settings” sections.

1. Check *Enable two factor*
2. Click OK

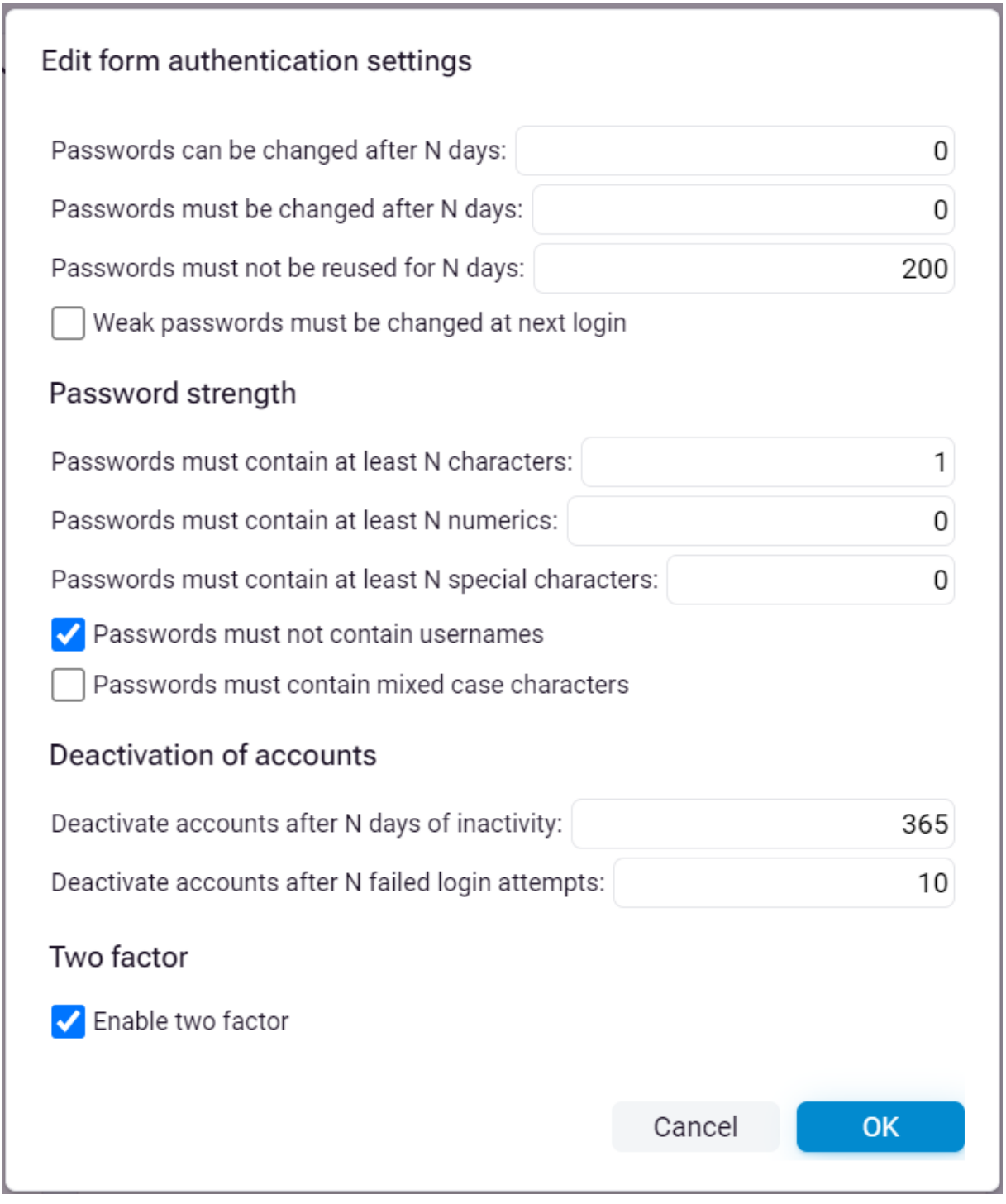


Figure 4 – Activate two-factor authentication

When the setting is enabled, the user will next be asked to set up the “secret” that becomes the second factor during login.

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)

OIDC is the most modern alternative and should be the first choice for new implementations when the customer's Identity Provider supports both OIDC and SAML2. SAML2 remains a supported alternative for environments where it is already established or otherwise the more practical choice.

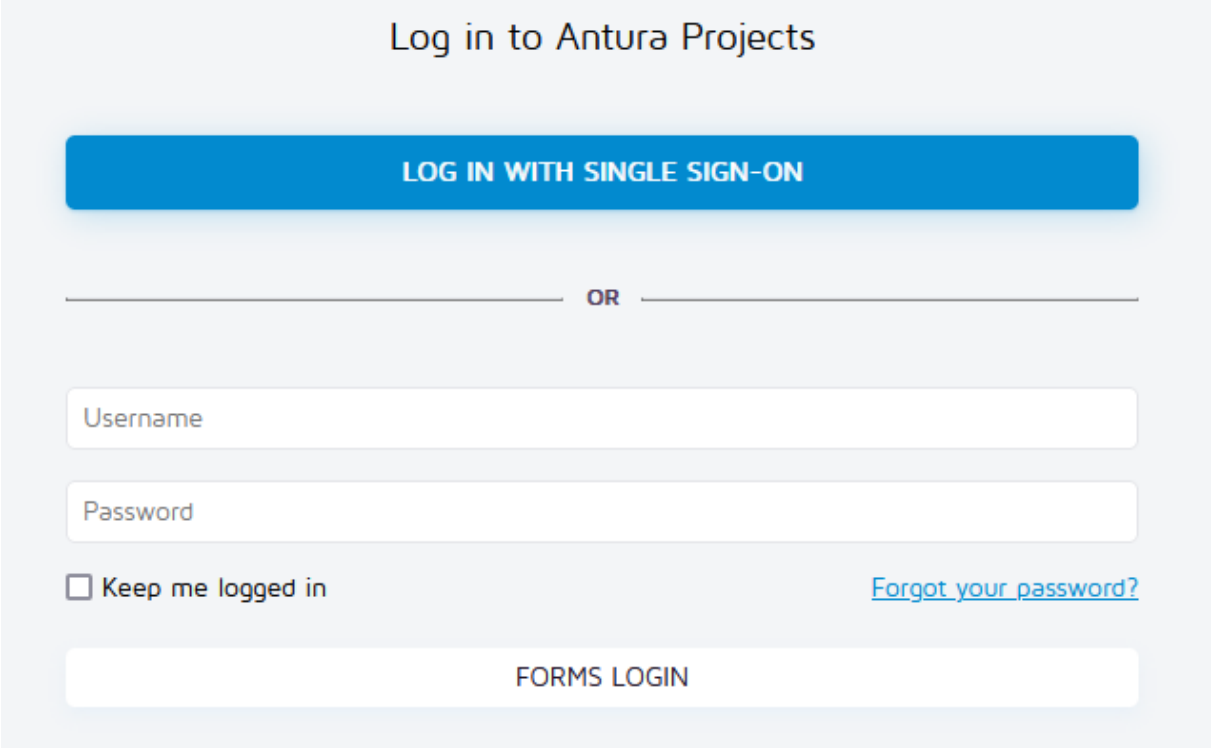
IBM Tivoli

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

Mixed mode

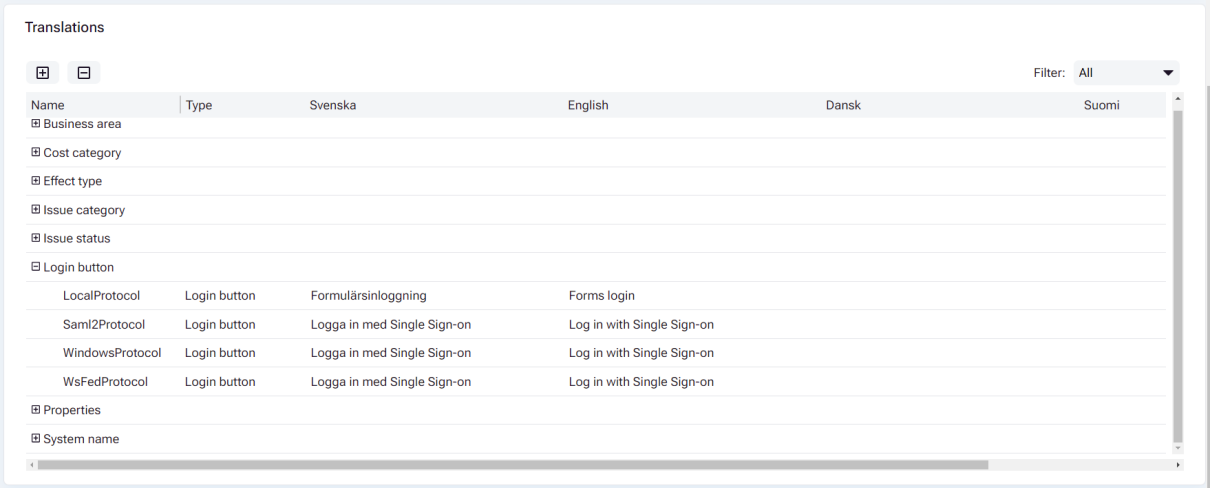
It is possible to combine multiple different ways of logging in. For example, one could have forms-based login enabled meant for external users and a federation protocol enabled meant for internal users.

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



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

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



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.

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:UpdateUsersFromClaim*s 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

Setting	Information	Default
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
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/streetadress
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

Provisioning

Overview

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 information via claims").

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").

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 “Activate identity federation”).

Automatic provisioning

Automatic provisioning from Active Directory and Microsoft Entra ID is provided through the solutions “Provisioning with Active Directory” (for on-prem only) and “Provisioning with SCIM” 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.

Provisioning with Active Directory

With *Provisioning with Active Directory*, 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 solution also includes user authentication.

Introduction

Provisioning with Active Directory allows authorized users to be logged into the system automatically without using the login prompt. The user is logged in automatically without having to enter a username and password. Synchronization is configured by connecting one or more groups in AD to the same number of system groups in Antura.

Configuration

When users connect to Antura, it is verified that they are authorized. Depending on which AD groups the user belongs to, the user becomes a member of the corresponding Antura groups and thereby receives the assigned permissions. If the user is not a member of any corresponding Antura group, login is denied.

Permission control

Below are two options for configuring AD synchronization in Antura:

1. Permissions administered in Antura

A synchronization group is used to synchronize all users from AD. Permissions for synchronized users are managed with separate groups in Antura.

Example: A system group is created in Antura with the name "Synchronization group" and linked to AD with a group reference. No permissions are assigned to the system group. Instead, permissions are assigned by the system administrator adding users to additional system groups (that are not synchronized with AD).

2. Permissions administered in AD

Several synchronization groups are used to synchronize users from AD. Permissions are assigned directly to the synchronization groups in Antura.

Example: Three system groups are created in Antura: "Project managers", "Administrators" and "Users". These are linked to three different group references in AD. A system administrator assigns permissions to the system groups and the synchronized users receive permissions depending on which group they are synchronized to.

The same user can be included in several synchronized groups, for example both "IT" and "Management". The user will then receive permissions from both groups.

Group structures

Antura does not use a hierarchical group structure (as can be used in AD). However, Antura supports synchronizing users against a hierarchical group structure in AD via a configuration per synchronized group.

Example: Given the following group structure in AD: "IT => Development => .NET" (three groups in a tree structure). If the group "IT" is synchronized, it is possible to choose whether only direct members of IT or also subgroups should be included (that is, Development and .NET).

Network and domains

If integration with AD is to be used, the web server running Antura should be part of the domain included in the company's forest. The standard case is that synchronization takes place against the server's domain controller and that Antura authenticates itself using the user identity configured on the application pool in the web server (IIS).
It is also possible to configure address, username and password for one or more specific AD servers. This requires AD communication to be open to those servers. In that case, the Antura server does not need to be part of the domain.

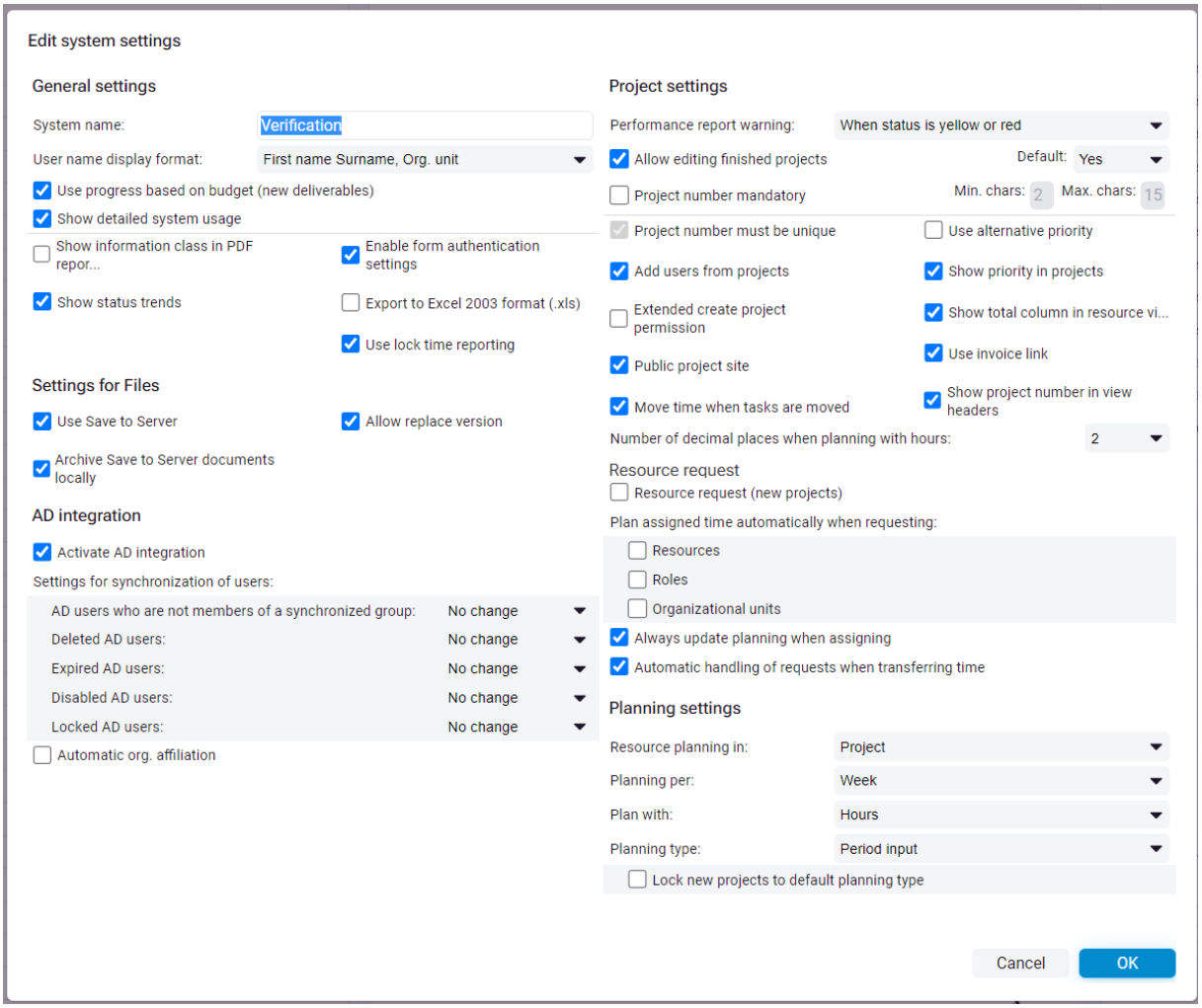
Synchronization of information

When a user is synchronized, some of the information from AD is copied to Antura. Synchronization takes place automatically once per day and per user during login. The following fields are read from AD and updated in Antura:

ADSI name	Antura
givenName	First name
sn	Last name
displayName	Display name
company	Company
department	Department
streetAddress	Address
postalCode	(Postal code) First part of postal address
mail	E-mail address
mobile	Mobile number
telephoneNumber	Telephone number
facsimileTelephoneNumber	Fax number
L	(City) Second part of postal address

Automatic organizational affiliation

To automatically set a user's organizational affiliation, use the system setting "Automatic organizational affiliation" in (*Administration - System - General*).



When the setting is enabled, the user is linked to an organizational unit that has the same name as the text in the “Department” field (that is, “department” in AD). The link to organizational affiliation happens during each synchronization of the user.

Synchronization of groups (provisioning)

Each night the groups in Antura that are linked to AD are synchronized. New members in the AD groups are automatically created as users in Antura. All information for existing users is updated from AD. In cases where a user has been removed from the AD group, the user will be deactivated in Antura (indicated by a red status light in Antura) and will no longer be able to log in. If the user is added back to the AD group, the user will be activated again (indicated by a green status light in Antura) at the next synchronization.
It is also possible to synchronize the groups manually, which has the same effect as the automatic synchronization.

Access for new users

When new users have been added to any of the AD groups that are synchronized, they will be given access immediately. The users will be able to log in to Antura. A user object will be created in Antura (or updated if the user already exists). Users who have been added to the AD group but have not logged in will be created in Antura at the next synchronization.

Revocation of access

When users have been removed from AD groups that are synchronized, their access will be revoked immediately. The users will not be able to log in to Antura. The user objects in Antura will be deactivated. Users who have been removed from the AD groups but have not tried to log in will be deactivated at the next synchronization.

Users not found in AD

In some cases, external users who do not have AD accounts need to be able to log in to the Antura environment (for example consultants). To handle this, there is support for both AD login and form login in parallel (so-called “Mixed Mode”).

With mixed mode authentication, AD login can be combined with form login. This can be used if all internal users come from an internal network (for example 192.168..) and external users come from other networks. In that case, Antura can be configured so that external users are presented with a login prompt while internal users are logged in automatically with SSO (Single Sign-On). For more information, see the “Mixed mode” section above.

Activation of Active Directory synchronization with Antura

Preparations in AD

The customer creates one or more groups in AD, depending on which configuration is chosen in the previous section *“Configuration in Antura”*. The users who should have access to Antura are linked to the respective group. Finally, the full path to the groups in DN format (“Distinguished Name”) is sent to Antura. Example of a group reference:
CN=AnturaProjectsSyncGroup,CN=Users,DC=antura,DC=se

Existing users in Antura

In cases where synchronization with AD is activated while there are already existing users in the system, these need to be remapped to their corresponding usernames in AD. Antura provides the customer with an Excel file that contains all users in the system together with an empty column for each user: *"Username in AD"*, which the customer fills in. Example: *DOMAIN\username*. When the file has been completed and sent back, the existing users are changed and are then ready for synchronization with AD.

Activate Active Directory and initial synchronization

When the groups have been created and Antura has received the group references and any mapping table, it is ready to activate the AD connection. This is done by Antura and involves a short downtime of the system (about one hour). In connection with the activation, the new system groups are created in Antura (to synchronize against AD) and any existing users are rewritten to their corresponding usernames in AD (with the help of the mapping table). After the activation is complete, the environment is opened and the users will automatically be logged in to the system without having to enter a username and password.

The change is first made in the **test environment** to verify that everything works correctly and that the solution meets expectations. When the synchronization works in test and has been approved, the same change is made in the production environment.

Configuration of Mixed Mode

If Mixed Mode authentication is to be used, a technician from Antura needs to discuss with a technician on the customer side whether it is possible, with the help of IP addresses, to determine whether a user should be authenticated with AD or be directed to the login page (for example if all consultants come through external networks). This does not need to be done separately as a later step after the AD synchronization is complete.

Provisioning with SCIM

With *Provisioning with SCIM*, 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 and deleted AD users) are controlled from Microsoft Entra ID.

Introduction

With *Provisioning with SCIM*, it is possible to configure automatic provisioning of users and groups from identity providers such as Microsoft Entra ID and Okta to Antura, which facilitates the management of new users and keeps users and groups synchronized.

Provisioning with SCIM uses the SCIM protocol, which is a standard for provisioning. Compared to AD synchronization, the solution does not require the AD to be installed on the same network as Antura. When Provisioning with SCIM is installed, there is a REST API in Antura that implements a SCIM API according to https://tools.ietf.org/html/rfc7644#section-3.2.

In the identity provider, Antura is registered as a client application by the administrator. Through attribute mapping, it is defined which attributes in the identity provider are to be mapped to which attributes in Antura. E-mail address, first name and last name must exist on users for new users to be created in Antura.

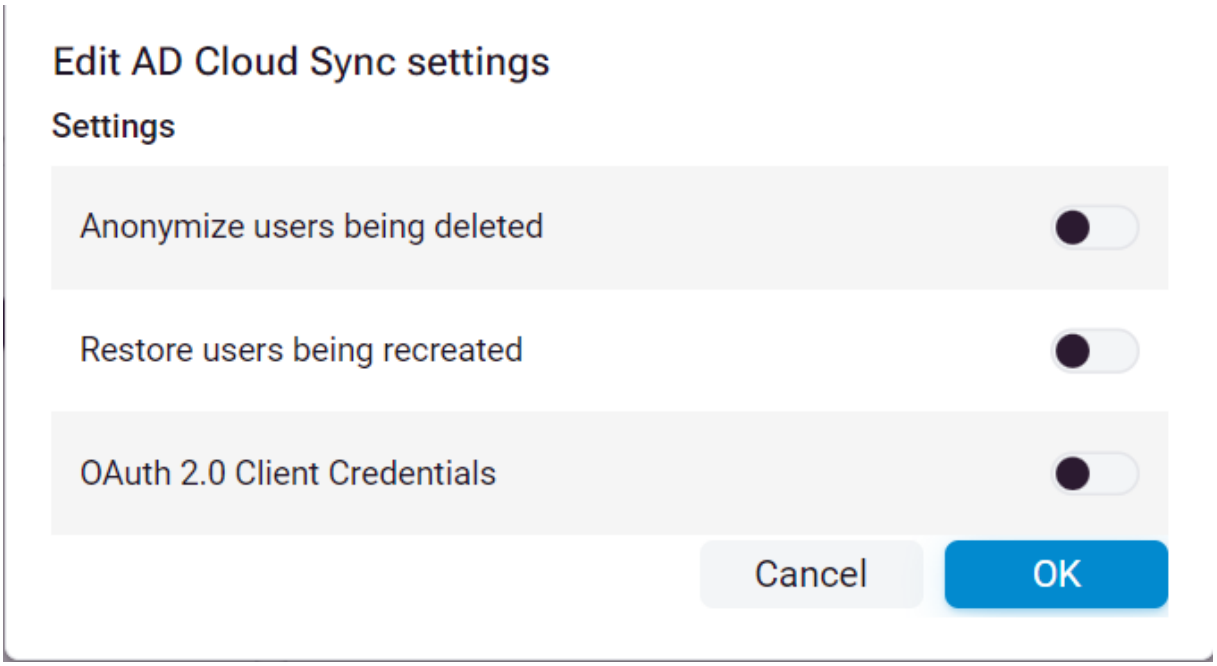
The scope of the provisioning is defined in the identity provider by choosing that all users and groups should be provisioned or by specifying which users and groups should be included in the provisioning to Antura.

Unlike users, there is no support for *creating* and *deleting* groups via SCIM.

For information regarding authentication and login via SSO, see the “Authentication” section above.

Settings

There are three settings for Provisioning with SCIM: *Anonymize users being deleted*, *Restore users being recreated* and *OAuth 2.0 Client Credentials*.



Activating the setting "*Anonymize users being deleted*" means that users who are removed in the identity provider are anonymized in Antura. This means the following:

- Username, first name / last name and e-mail address are set to random values
- Company, department, street address, postal address and phone / mobile / fax are cleared
- Any profile picture is removed
- Organizational unit is set to "No organizational unit"
- User properties are not affected

This setting is enabled by default.

Activating the setting "*Restore users being recreated*" means that users who are recreated in the identity provider are reactivated in Antura, provided the user can be identified, that is, one (and only one) user can be matched via the "externalId" attribute first and the "userName" attribute second. This setting is not enabled by default.

Note that if both of these settings are enabled, the "externalId" attribute (see "SCIM attribute mapping") must be mapped and synchronized for the user to be recreated.

Activating the setting "*OAuth 2.0 Client Credentials*" means that the identity provider can call Antura's REST API using OAuth 2.0 Client Credentials Grant instead of only a token. After activation, the following fields are shown and required to connect the identity provider:

- Client ID
- Client scope
- Client callback URL

- Secret token (if the value is hidden, the value most recently shown is still valid)

This setting is not enabled by default.

Provisioning from Microsoft Entra ID to Antura

Create users

If a user in Microsoft Entra ID is missing in Antura, the user is created provided that the “Create” action is configured for users in Microsoft Entra ID.

Activation and deactivation of users

For a user to become active in Antura, the SCIM attribute *active* must be set to true for the user. It is recommended to use the Microsoft Entra ID attribute “isSoftDeleted” and set this to false to activate the user, and to true to deactivate the user (see SCIM attribute mapping for what the expression looks like in Microsoft Entra ID). New users in Microsoft Entra ID will thus be created as active in Antura and users who are removed (without being permanently deleted) in Microsoft Entra ID will be deactivated in Antura.

However, it is possible to implement more complex logic for when users should be considered active. For more details on how to write these expressions, see https://learn.microsoft.com/en-us/entra/identity/app-provisioning/functions-for-customizing-application-data

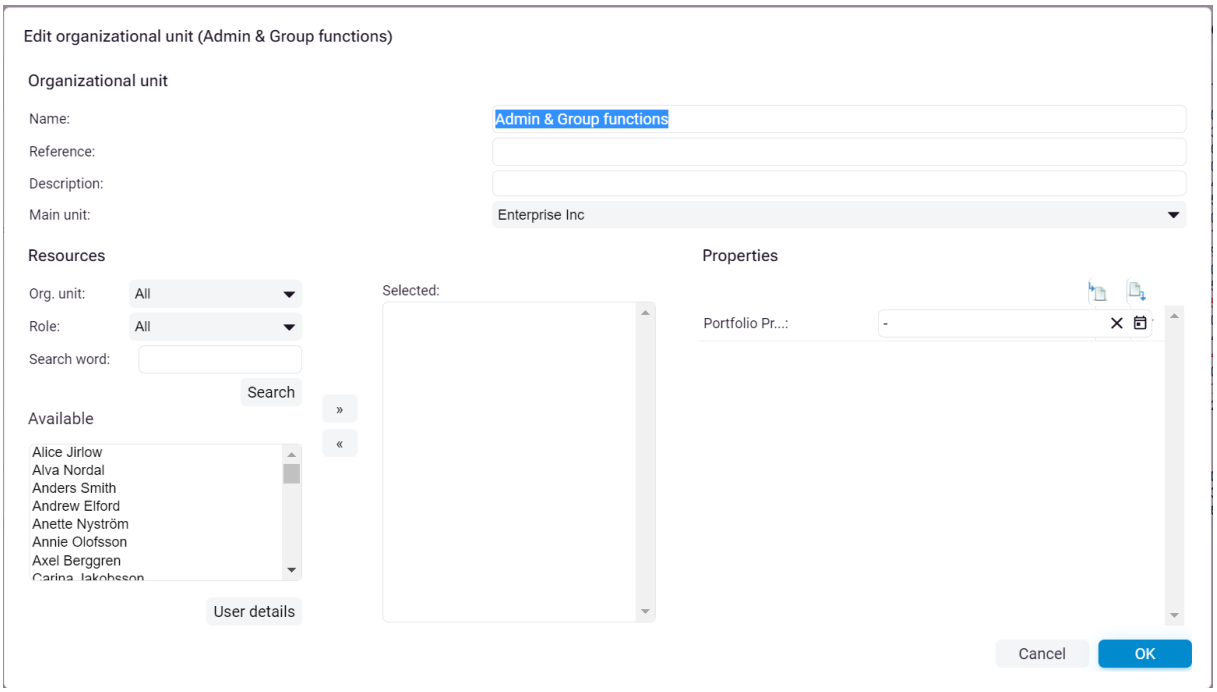
Removal of users

If a user is permanently deleted in Microsoft Entra ID, the user is deleted in Antura provided that the “Delete” action is configured for users in Microsoft Entra ID. Since users cannot be permanently deleted in Antura, a so-called “soft delete” will be done (that is, the user is marked as deleted). It is configurable whether users who are removed should be anonymized or not (see section “Settings”). If anonymization is enabled, username, name (first name, last name) and e-mail address will be updated with random values and other details will be cleared.

Whether users recreated in Microsoft Entra ID should be created again in Antura or restored is also configurable (see section “Settings”).

Organizational affiliation

Which organizational unit a user belongs to is determined by comparing the company name in Microsoft Entra ID with the value in the “Reference” field that is set on an organizational unit in Antura (Project portfolio - Org.units - Projects). *Note that the comparison is case-sensitive.*

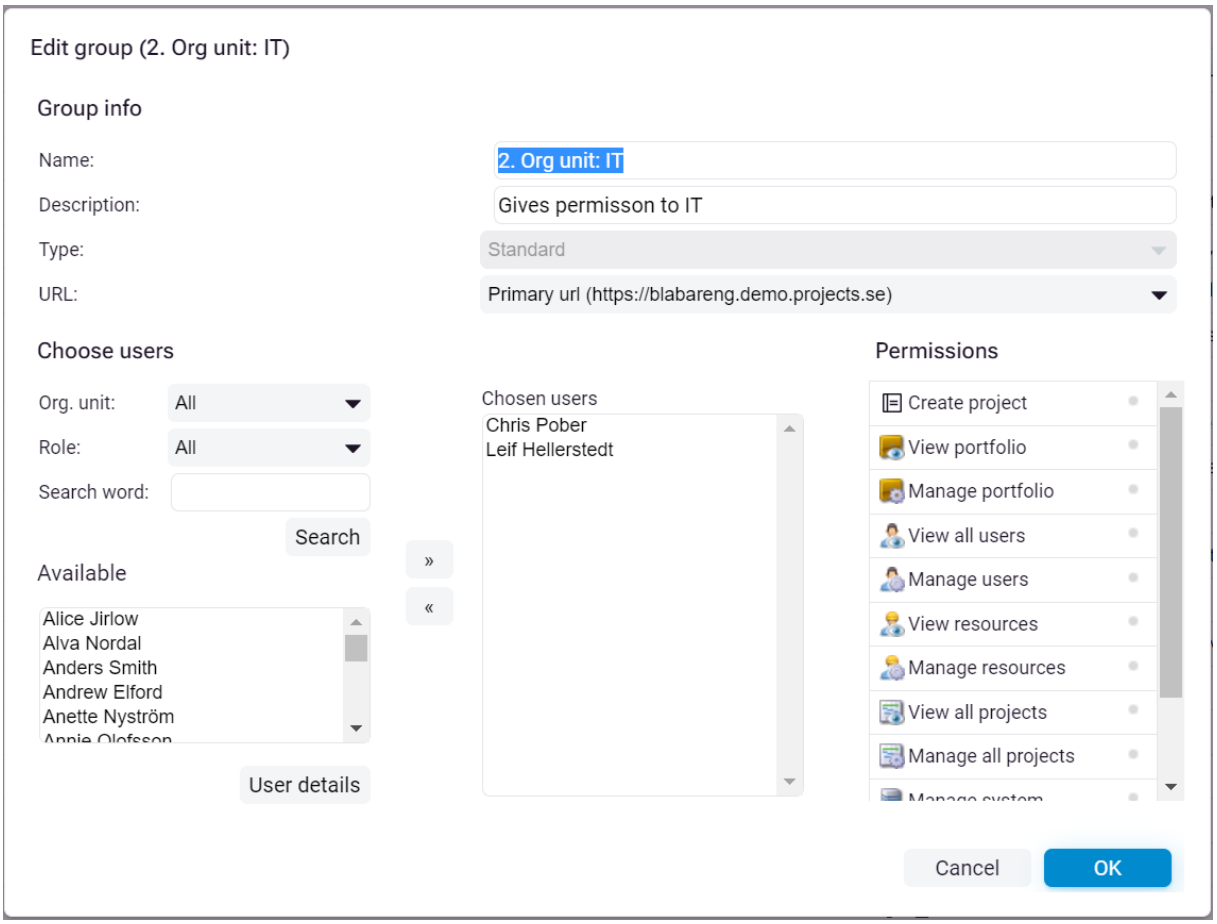


If exactly one organizational unit matches, the user is updated to belong to the organizational unit in Antura. If none or more than one organizational unit matches, the user is updated without organizational affiliation and a warning is logged.

Note that provisioning of organizational affiliation is controlled via attribute mapping in Microsoft Entra ID (see SCIM attribute mapping) and is not affected by what the system setting "Automatic organizational affiliation" (Administration - System - General) is set to.

Group affiliation

Which user group a user belongs to is determined by comparing the group name in Microsoft Entra ID with the value in the "Group reference" field that is set on a group in Antura (Administration - Groups). The field is shown only if Provisioning with SCIM is enabled (see the section "Activate Provisioning with SCIM") and if the group is a standard group (that is, the field Type = "Standard"). *Note that the comparison is not case-sensitive.*



If the group matches, the user is updated to belong to the group in Antura. If a user is removed from a group in Microsoft Entra ID, the user is removed from the corresponding group in Antura (provided that the group matches).

Multiple groups

A user can belong to multiple groups in Microsoft Entra ID. This can mean that the user becomes a member of multiple groups in Antura.

However, it is not possible to have multiple Microsoft Entra ID groups that are all mapped to the same group in Antura, or vice versa. If the same group reference is specified for multiple groups, this can result in undefined behavior.

Hierarchical groups

Microsoft Entra ID allows hierarchical groups, which are not supported by Antura.

If you choose which users and groups should be provisioned, hierarchical groups will not work, that is, only users and groups that are directly connected to the designated group in Microsoft Entra ID will be synchronized to Antura (that is, to include all users in a certain tree structure of users / groups, all groups except the leaf level must be explicitly selected for provisioning).

If you choose that all users and groups should be provisioned, hierarchical groups and users in a hierarchical structure will be provisioned provided that the group in Microsoft Entra ID matches a group in Antura.

SCIM installation manual

Configuration in Antura

Activate Provisioning with SCIM

Provisioning with SCIM needs to be activated manually in the administration interface. Activate Provisioning with SCIM via the Status button. Note the secret token that is generated and shown when activated. This key will be used later when registering Antura as a client application in Microsoft Entra ID.

Microsoft Entra ID talks to Antura via a REST API and uses OAuth 2.0 Client Credentials Grant to authenticate. Microsoft Entra ID does not fully implement support for Client Credentials Grant, but is configured with a token instead. Antura generates a token with an infinite lifetime. This is a limitation in Microsoft Entra ID and not in Antura.

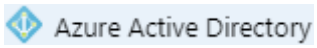


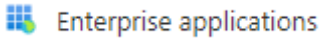
Configuration in Microsoft Entra ID

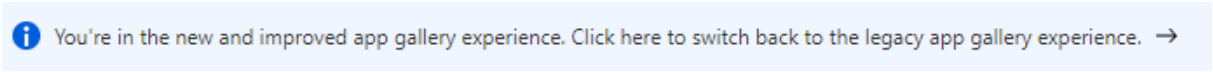
Integration between Provisioning with SCIM and Microsoft Entra ID requires configuration in Microsoft Entra ID. This configuration is done by the Microsoft Entra ID administrator since it requires Microsoft Entra ID admin privileges.

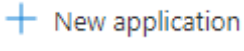
Register Antura as a client application in Microsoft Entra ID

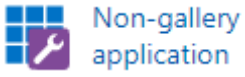
For Antura to receive provisioning data from Microsoft Entra ID, Antura must be manually registered as a client application in Microsoft Entra ID.

1. Log in to https://entra.microsoft.com/ (Microsoft Entra admin center) with your Microsoft 365 account. You can also use https://portal.azure.com if you prefer.
2. Click the service 

3. Click 

4. Click


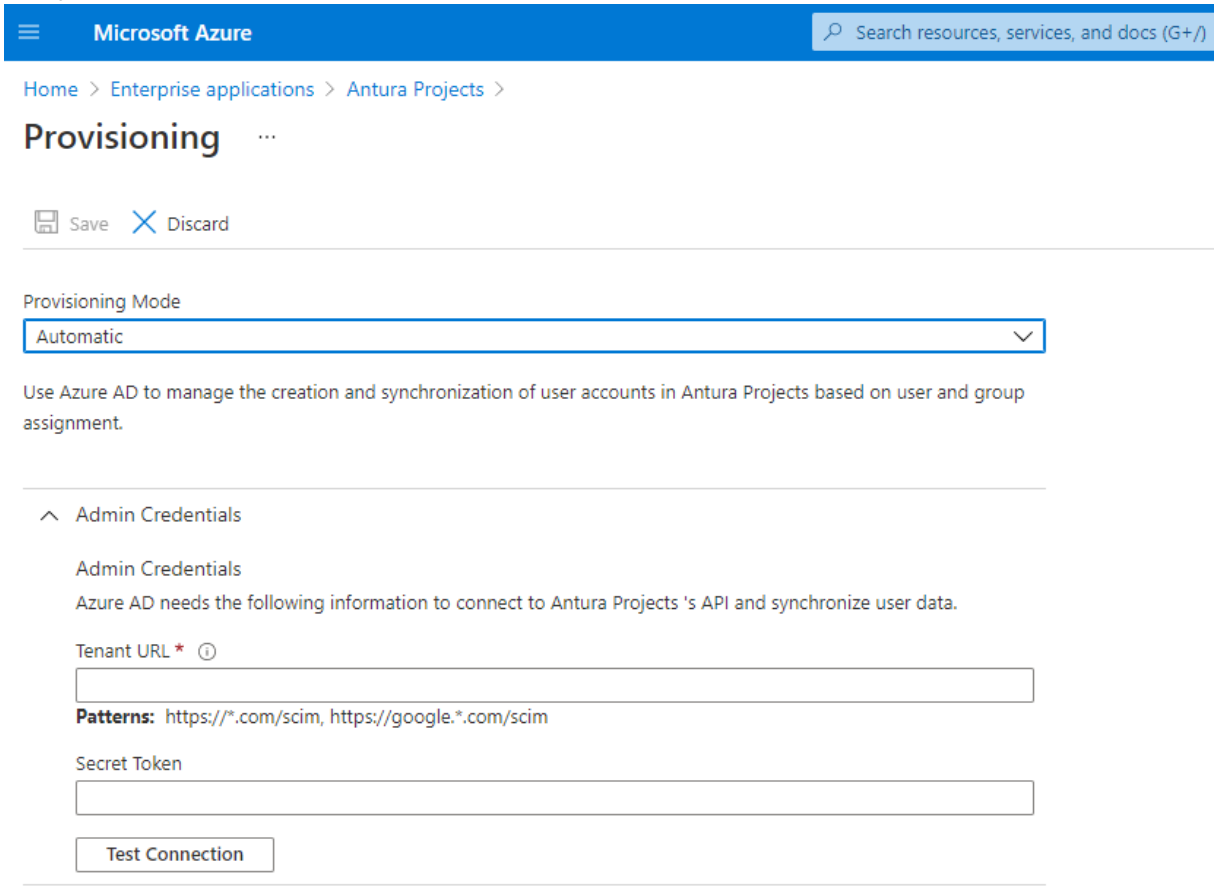
5. Click 

6. Click 

7. Enter the following information:
    1. Name - the application name can be anything, for example “Antura”.
8. Click “Add”

Configure automatic provisioning with SCIM

1. Navigate to the newly created application and click “Provisioning” and then “Get started”. Select “Automatic” in the dropdown. This means the information will be synchronized automatically every 40 minutes.

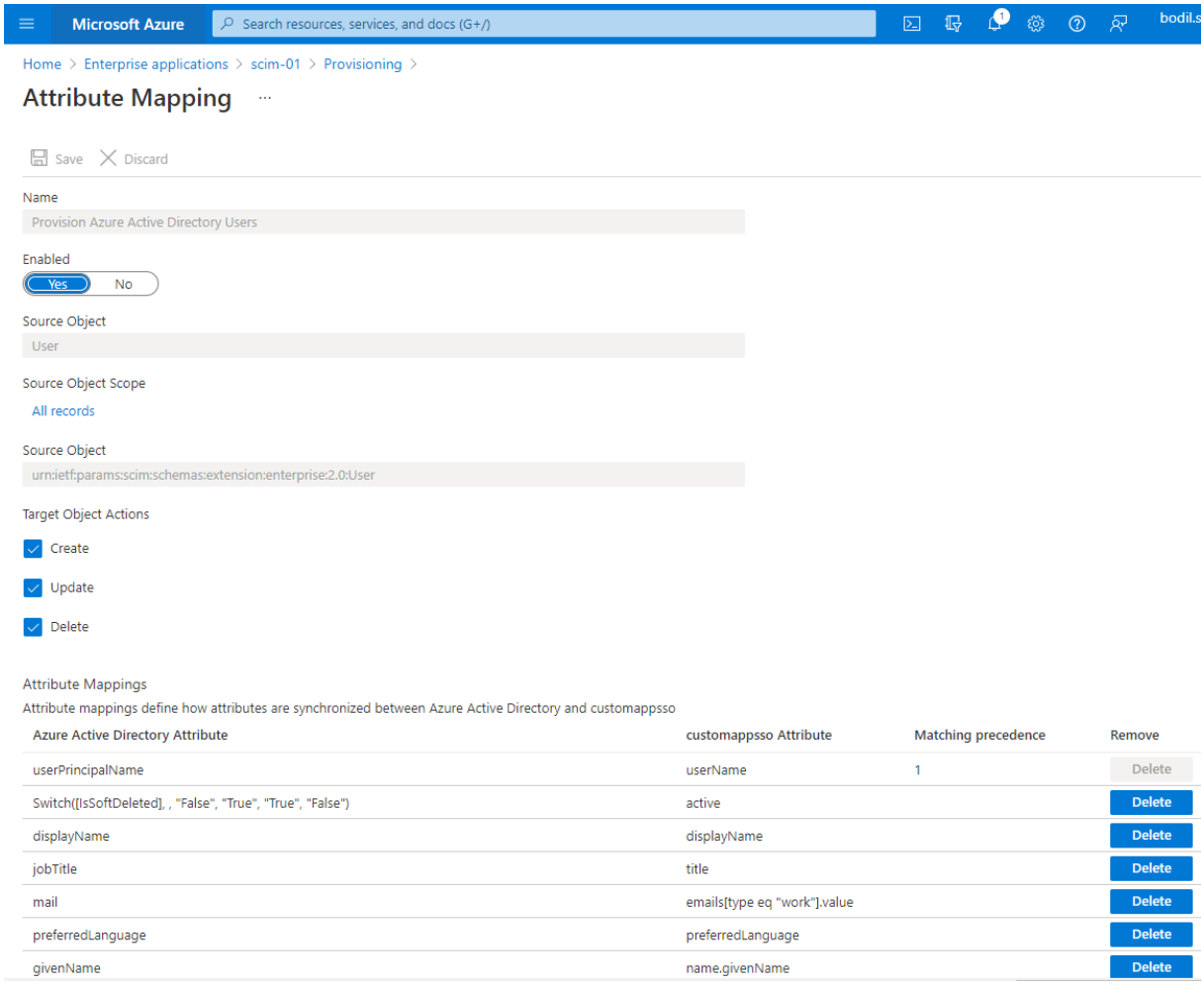


2. Expand “Admin credentials” and enter the base URL to Antura plus the path to its SCIM API, for example *https://{customer}.projects.se/app/api/scim/v2/*, as *Tenant URL*.
3. Enter the secret token generated by Antura. It is a cryptographically unique key generated when Provisioning with SCIM is activated (see section “Activate Provisioning with SCIM”).
4. Click “Test connection” to verify that the settings are correct.
5. Click Save which opens additional sections.
6. Expand “Settings” and enter an e-mail address for where errors should be sent.
7. Check “Send an email notification when a failure occurs”.
8. Click Save

Configure user mapping

To be able to provision users, you need to configure mapping for the provisioning.

1. Navigate to the newly created application and click “Provisioning” and then “Edit provisioning”.
2. Expand “Mappings” and click Provision Azure Active Directory Users

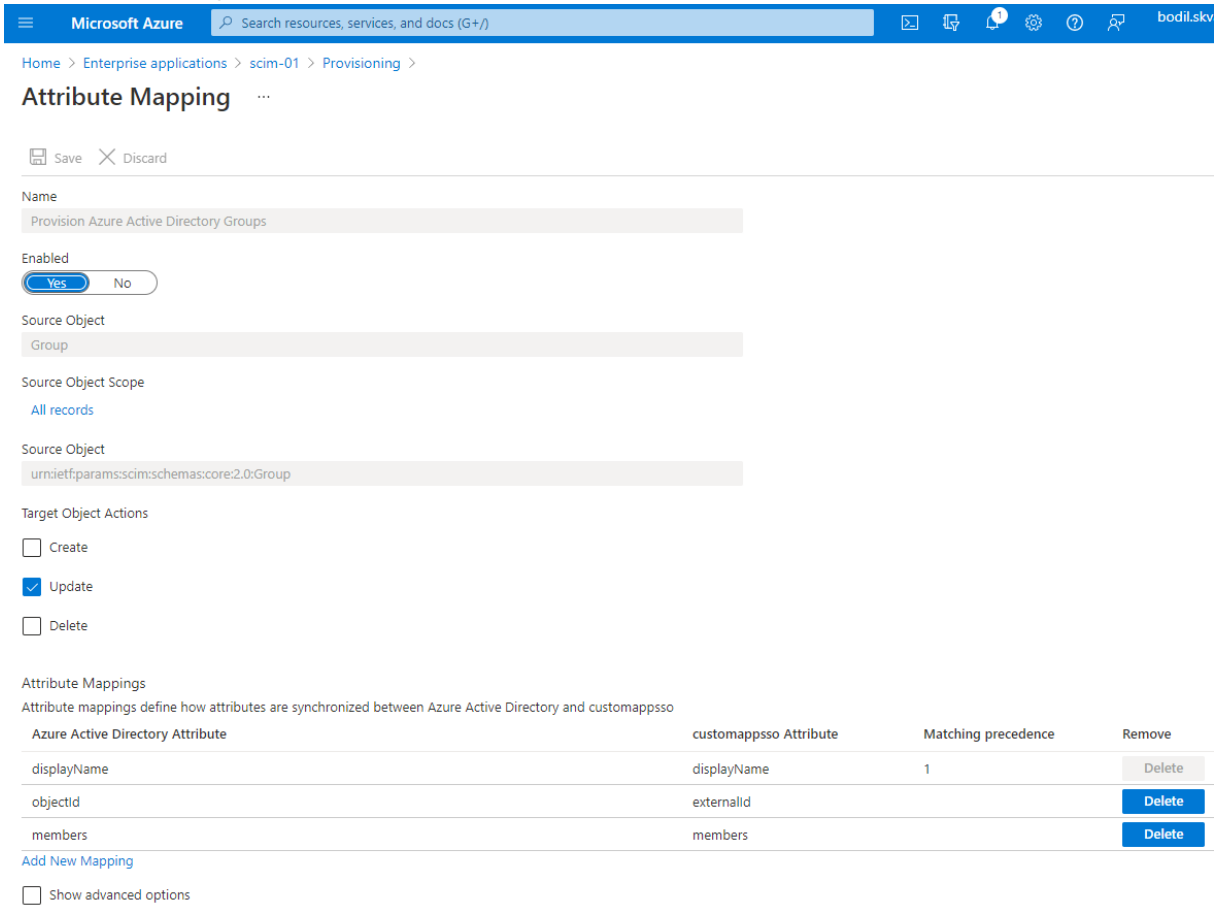


3. Select which actions should be included in the provisioning. If new users should not be created in Antura, clear “Create”. If users should not be deleted in Antura, clear “Delete”.
4. Map “userName” (in the column called “customappsso Attribute”) to a unique attribute in Microsoft Entra ID (the column is called “Microsoft Entra ID attribute” in the portal). **Important! Use the same mapping of userName as in federation so that users who are to be provisioned match any existing users in Antura, otherwise the user will not be able to log in. If userName does not match, it will not be possible to authenticate users.**
5. These fields must be set to create users in Antura:
    1. emails[type eq “work”].value
    2. name.givenName
    3. name.familyName

Configure group mapping

To be able to provision groups, you need to configure group mapping for the provisioning.

1. Navigate to the newly created application and click “Provisioning” and then “Edit provisioning”.
2. Expand “Mappings” and click Provision Azure Active Directory Groups



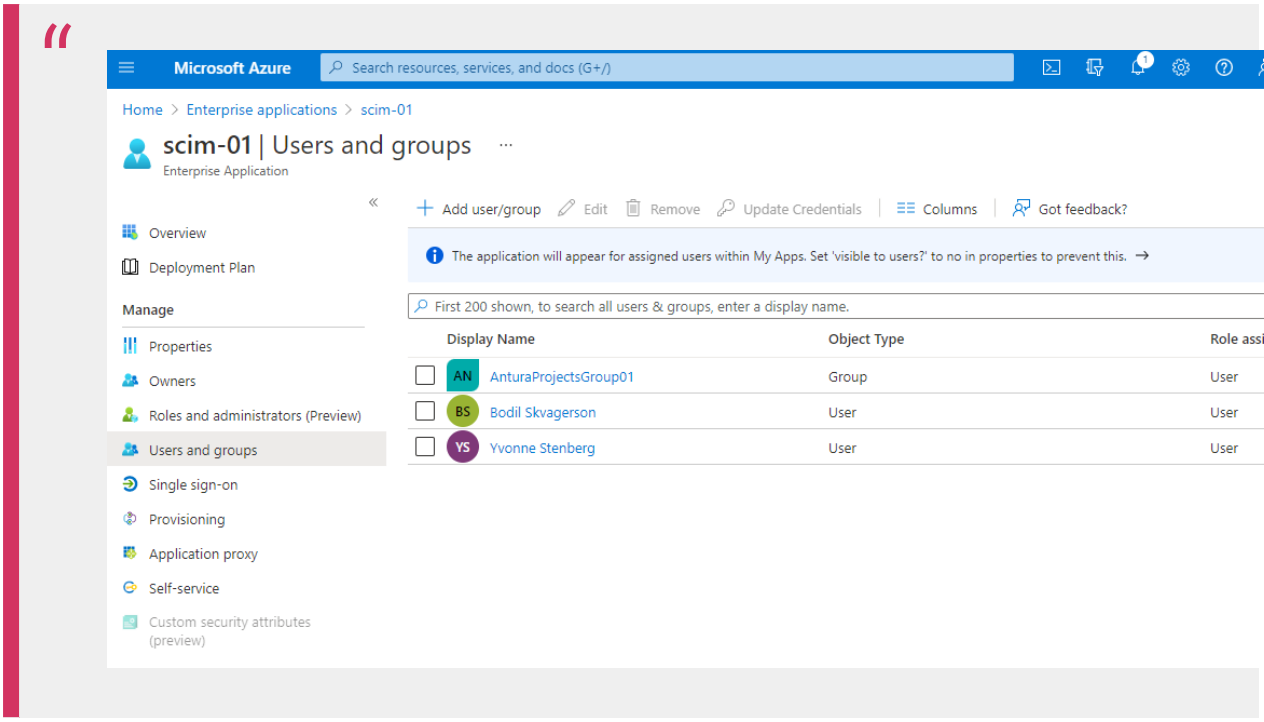
3. Clear “Create” and “Delete”. *Important:* Antura does **not** support creating and deleting groups via SCIM.
4. Map “displayName” to a unique attribute in Microsoft Entra ID.
5. Map groups in Microsoft Entra ID to groups in Antura by entering the name of the Microsoft Entra ID group as a group reference in Antura. *Note that this mapping is intended to be one-to-one. There is no support for mapping one group in Microsoft Entra ID to multiple groups in Antura.*

Configure users and groups to be included in the provisioning

To provision the correct users, you need to configure which users are to be included in the provisioning. If all users and groups are to be provisioned, continue to the section “Configure scope”.

1. Navigate to the newly created application and click “Users and groups”.

2. Assign users and groups to the application by clicking “Add user/group” and searching for the relevant users and groups.



Configure scope

1. Navigate to the application and click “Provisioning” and then “Edit provisioning”.
2. Expand “Settings”. In the “Scope” dropdown, select “Sync only assigned users and groups” or “Sync all users and groups”.
   Note that if you select “Sync only assigned users and groups”, you must select which users and groups are to be provisioned, see the earlier section “Configure users and groups to be included in the provisioning”.

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.

Troubleshooting

Two-factor authentication

If it does not work to log in with the authentication code, it may be because the phone's time settings are not synchronized. This means that the authentication code shown in the app (Google Authenticator or Microsoft Authenticator) is never valid. Try turning time synchronization off and on again on the phone and then test once more.

If it still does not work, you can reset the user's two-factor secret via the *Administration - Users* view:

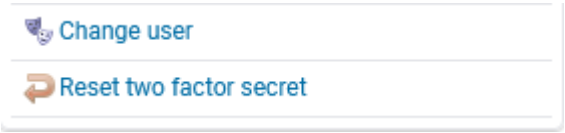


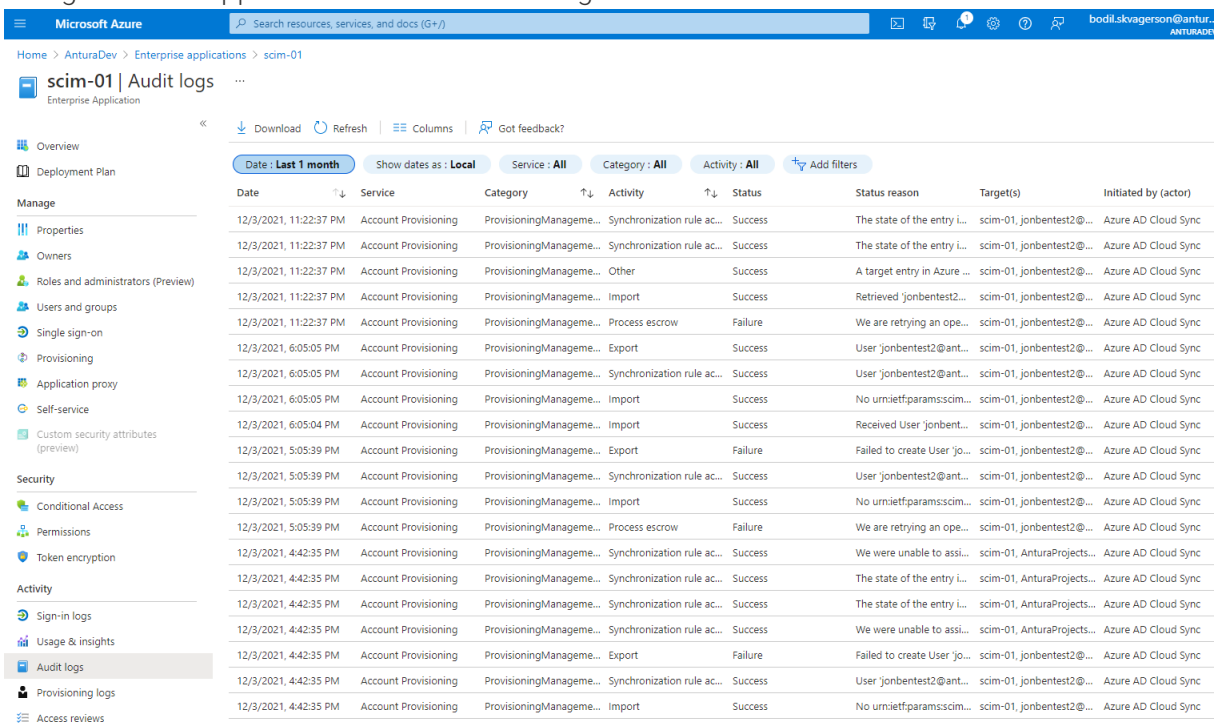
Figure 5 – Reset secret

SCIM troubleshooting

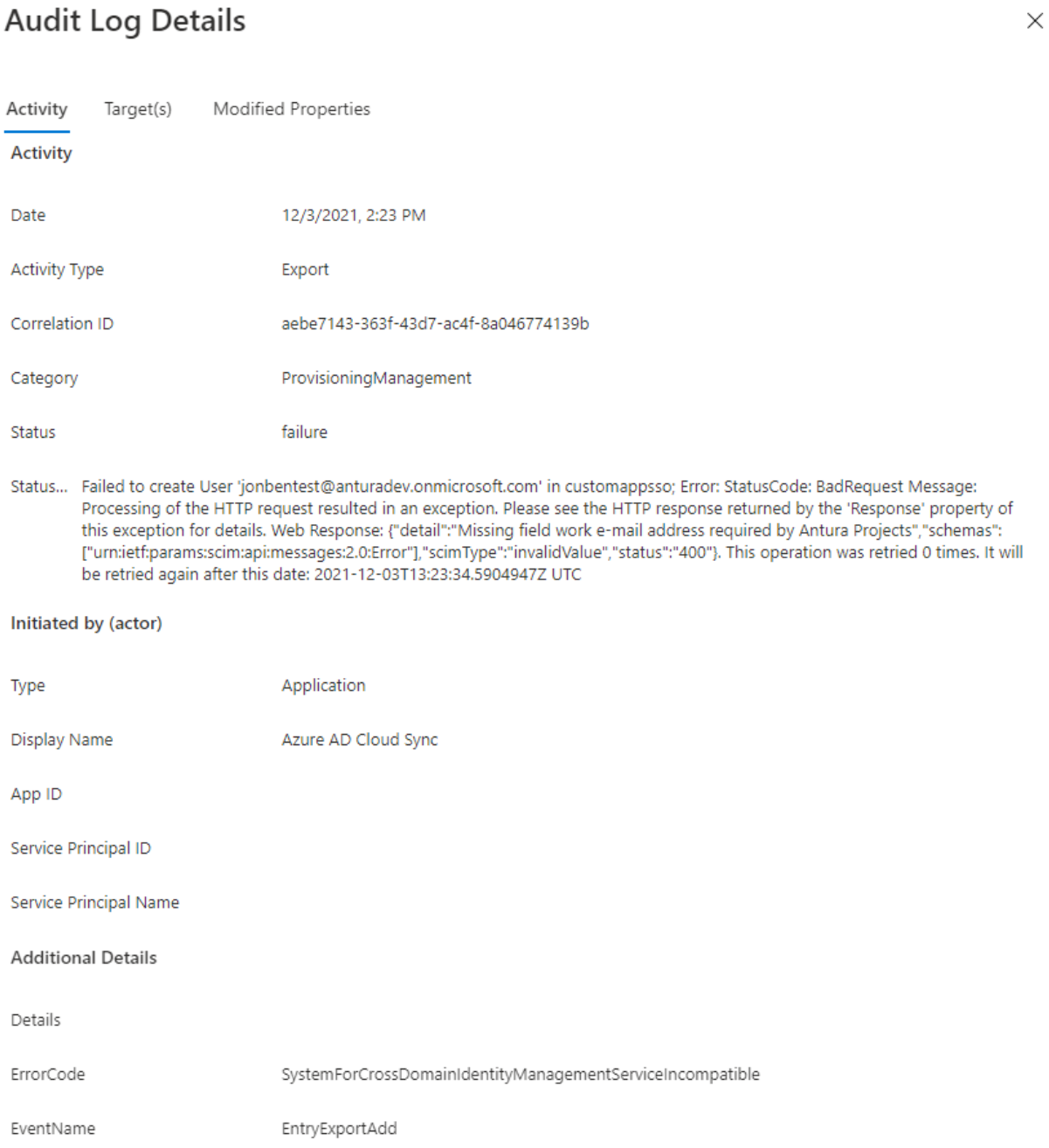
If something goes wrong during provisioning in Microsoft Entra ID, an e-mail will be sent to the e-mail address specified for notifications, provided that the checkbox "Send an email notification when a failure occurs" has been checked (see section "Register Antura as a client application in Microsoft Entra ID").

You can also view provisioning logs in Microsoft Entra ID for more information.

1. Navigate to the application and click “Audit logs”. >



2. Click the row that has Failure as status to see the cause of the error.



SCIM attribute mapping

User attributes

This table describes how user information in Microsoft Entra ID is mapped to user information in Antura (AP) via SCIM (see https://tools.ietf.org/html/rfc7643#section-4.1 and https://tools.ietf.org/html/rfc7643#section-4.3).

Note that mapping of fields other than those mentioned below is not recognized by Antura and will therefore generate errors during provisioning.

Microsoft Entra ID (default)	SCIM	Antura
userPrincipalName	userName	Username (User.Login)
Switch([IsSoftDeleted], , “False”, “True”, “True”, “False”)	active (User.	Status – Activated/ Deactivated Active)
displayName	displayName	Only used by SCIM (User.ExternalDisplayName)
jobTitle	title	Only used by SCIM (User.ExternalTitle)
mail	emails[type eq “work”].value E-	mail (User.Email1)
preferredLanguage	preferredLanguage	*Ignored*
givenName	name.givenName	First name (User.FirstName)
surname	name.familyName	Last name (User.LastName)
Join(“ “, [givenName], [surname]) na	me.formatted *I	gnored, does not exist in Antura*
physicalDeliveryOfficeName	addresses[type eq “work”].formatted *I	gnored*
streetAddress	addresses[type eq “work”]. St streetAddress	reet address (User.StreetAddress)

Microsoft Entra ID (default)	SCIM	Antura
city	addresses[type eq “work”].locality *S	ee postalCode below*
state	addresses[type eq “work”].region *I	gnored, does not exist in Antura*
postalCode	addresses[type eq “work”]. Po postalCode	stal address (User.Address gets the value “{postalCode}, {locality}[, {country}]”)
country	addresses[type eq “work”].country *S	ee postalCode above*
telephoneNumber	phoneNumbers[type eq “work”].value Ph	one (User.Telephone)
mobile	phoneNumbers[type eq “mobile”]. Mo value	bile (User.MobilePhone)
facsimileTelephoneNumber	phoneNumbers[type eq “fax”].value Fa	x (User.Facsimile)
mailNickname	externalId	Only used by SCIM (User.ExternalId)
employeeId	urn:ietf:params:scim:schemas: extension:enterprise:2.0:User: employeeNumber	*Ignored*
department	urn:ietf:params:scim:schemas: extension:enterprise:2.0:User: department	Department (User.Department)
manager	urn:ietf:params:scim:schemas: extension:enterprise:2.0:User: manager	*Ignored, does not exist in Antura*

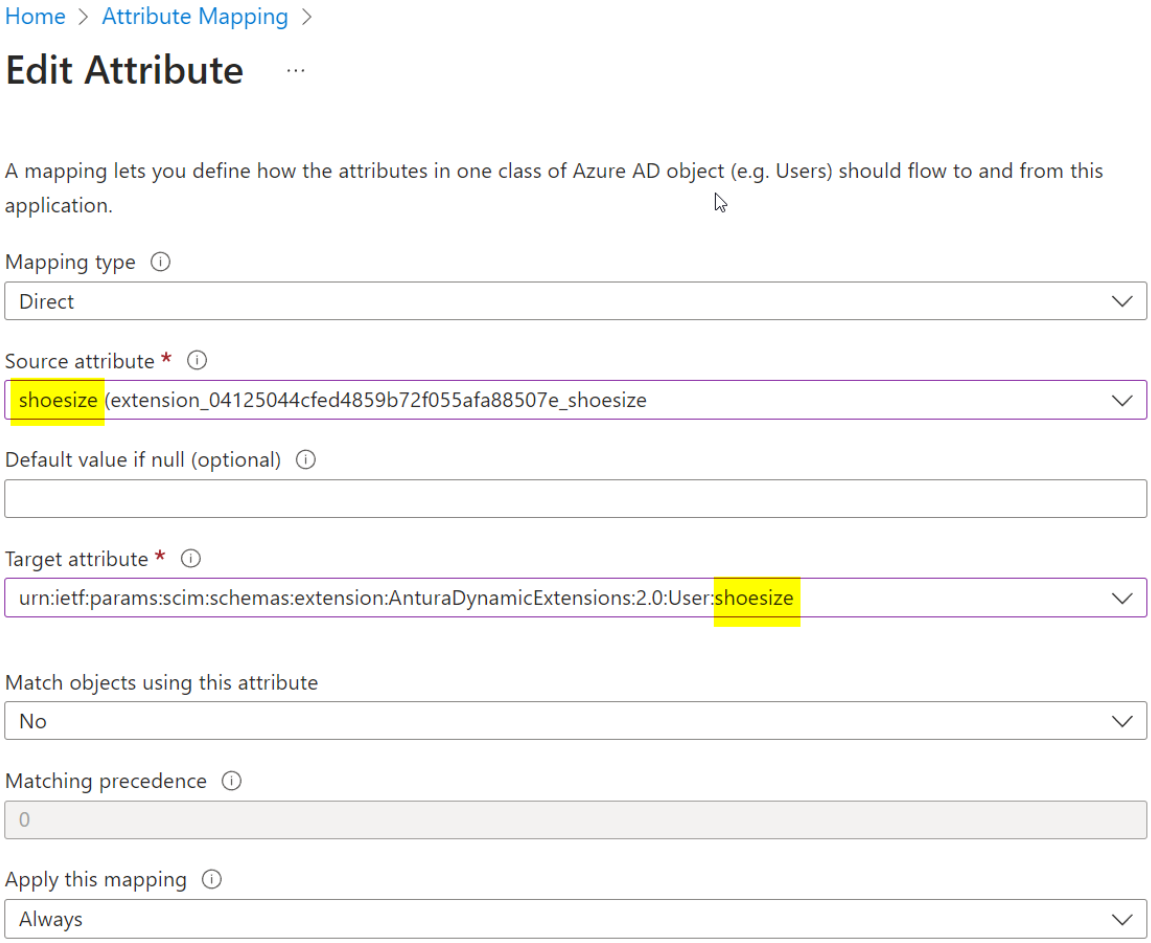
Microsoft Entra ID (default)	SCIM	Antura
companyName	urn:ietf:params:scim:schemas:extension:AnturaFixedExtensions:2.0:User:company. For mapping of companyName to work the companyName needs to be manually mapped to this schema [1].	Company (User.Company)
Note that default is missing in Microsoft Entra ID for organizational unit. For mapping of org unit to work, the org unit needs to be mapped to a field in Microsoft Entra ID such as companyName.[2]	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:organization	Org. unit (mapped through the field "Reference" on organizational unit)
	urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:costCenter	*Ignored*
	nickName	*Ignored, does not exist in Antura*
	profileUrl	*Ignored, does not exist in Antura*
	userType	*Ignored, does not exist in Antura*
	locale	*Ignored*
	timezone	*Ignored, does not exist in Antura*

User properties

Use the Microsoft Graph PowerShell cmdlet **`New-MgApplicationExtensionProperty`** (in the **`Microsoft.Graph.Applications`** module) to create a new user property in Microsoft Entra ID.

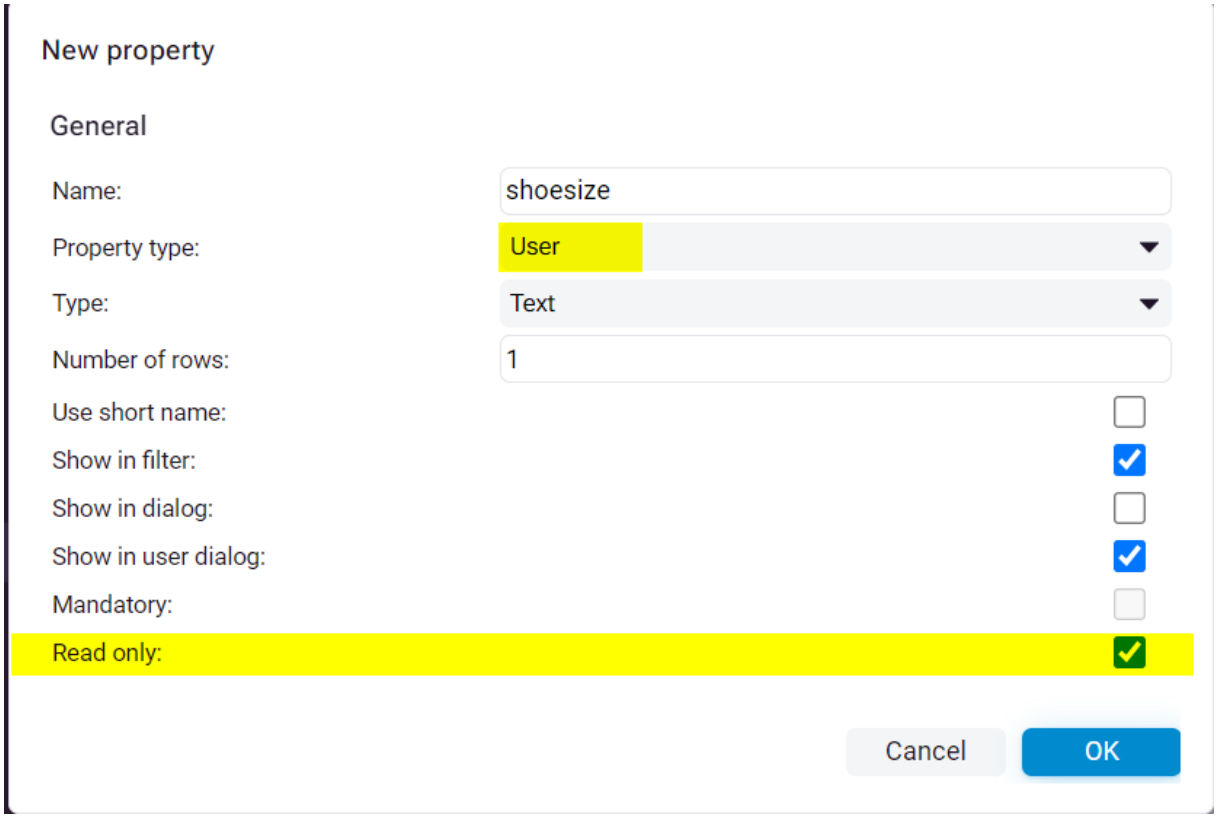
Map the user property to a SCIM attribute in Microsoft Entra ID

1. Navigate to the application in Microsoft Entra ID and click “Provisioning” and then “Edit provisioning”. Click “Mappings” and select “Provision Microsoft Entra ID Users”.
2. Click “Show advanced options” at the bottom of the page and select “Edit attribute list for customappsso”.
3. Add an attribute with the prefix “urn:ietf:params:scim:schemas:extension:AnturaDynamicExtensions:2.0:User:”. *Note that only text and numeric types are supported for user properties. To map numeric types to Antura, the type in Microsoft Entra ID must be “text”. Examples of valid numeric values are “-4”, “42” and “33.5”.*
4. Save the changes and go to the previous page “Attribute mapping”.
5. Click “add new mapping” at the bottom of the page. Example with an attribute called “nickname”.



Create the user property in Antura

1. Navigate to the *System properties* page in Administration - System.
2. Create a new property with the same name and type (text or numeric) as the property in Microsoft Entra ID. Select the property type “User”. The property must be read-only because Microsoft Entra ID overwrites all values in Antura. Example with an attribute called “shoe size”.



Note:

- Mapping of user properties is only supported for properties with a **unique name** in Antura. The comparison is case-insensitive.
- **Deleting a user property value** in Microsoft Entra ID is not provisioned to Antura. This is because Microsoft Entra ID does not provision empty values.
- It is recommended to have the synchronized values as **read-only** in Antura, since changes will be overwritten at the next synchronization.

Group attributes

This table describes how group information in Microsoft Entra ID is mapped to group information in Antura via SCIM (see https://tools.ietf.org/html/rfc7643#section-4.2).

Microsoft Entra ID (default)	SCIM attribute	Antura
displayName	displayName	Group (mapped through the field “Group reference” on the group)
objectId	externalId	Only used by SCIM (Group.ExternalId)
members	members	Members of the group (SystemRoleService.GetMembers)

Synchronization of extension attributes

For users in **on-premises** Active Directory, you must synchronize the users to Microsoft Entra ID. Microsoft Entra ID Connect automatically synchronizes some attributes to Microsoft Entra ID, but not all attributes. In addition, some attributes (such as **`SAMAccountName`**) that are synchronized by default may not be exposed by Graph API. In these cases, you can use a feature in Microsoft Entra ID Connect to synchronize the attribute to Microsoft Entra ID. That way, the attribute becomes visible to Graph API and the Microsoft Entra ID provisioning service. For more information, see use the Microsoft Entra ID Connect directory extension feature to synchronize the attribute to Microsoft Entra ID.

---

1. If no mapping of the attribute is done, the field will not be synchronized.↩
2. If no mapping of the attribute is done, the field will not be synchronized.↩