



Webinar

Zabbix User Provisioning JIT

all our microphones are muted

ask your questions in Q&A, not in the Chat

use Chat for discussion, networking or applause

1

What is JIT (Just In Time)



What is JIT (Just In Time)

- › Automatically create and update your Zabbix users with the new Just-in-time user provisioning feature for LDAP and SAML
 - › Simplified user management - map LDAP and SAML user groups to Zabbix user groups
 - › Enterprise-grade security - automatically assign user groups and user roles to LDAP and SAML users
 - › Automatically assign media types to Zabbix users based on their LDAP/SAML attributes
 - › SAML authentication supports both JIT and SCIM user provisioning
- › LDAP
 - › The **L**ightweight **D**irectory **A**ccess **P**rotocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol
- › SAML
 - › **S**ecurity **A**ssertion **M**arkup **L**anguage is an open standard for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider
- › SCIM
 - › **S**ystem for **C**ross-domain **I**ntity **M**anagement is a standard for automating the exchange of user identity information between identity domains, or IT systems

2

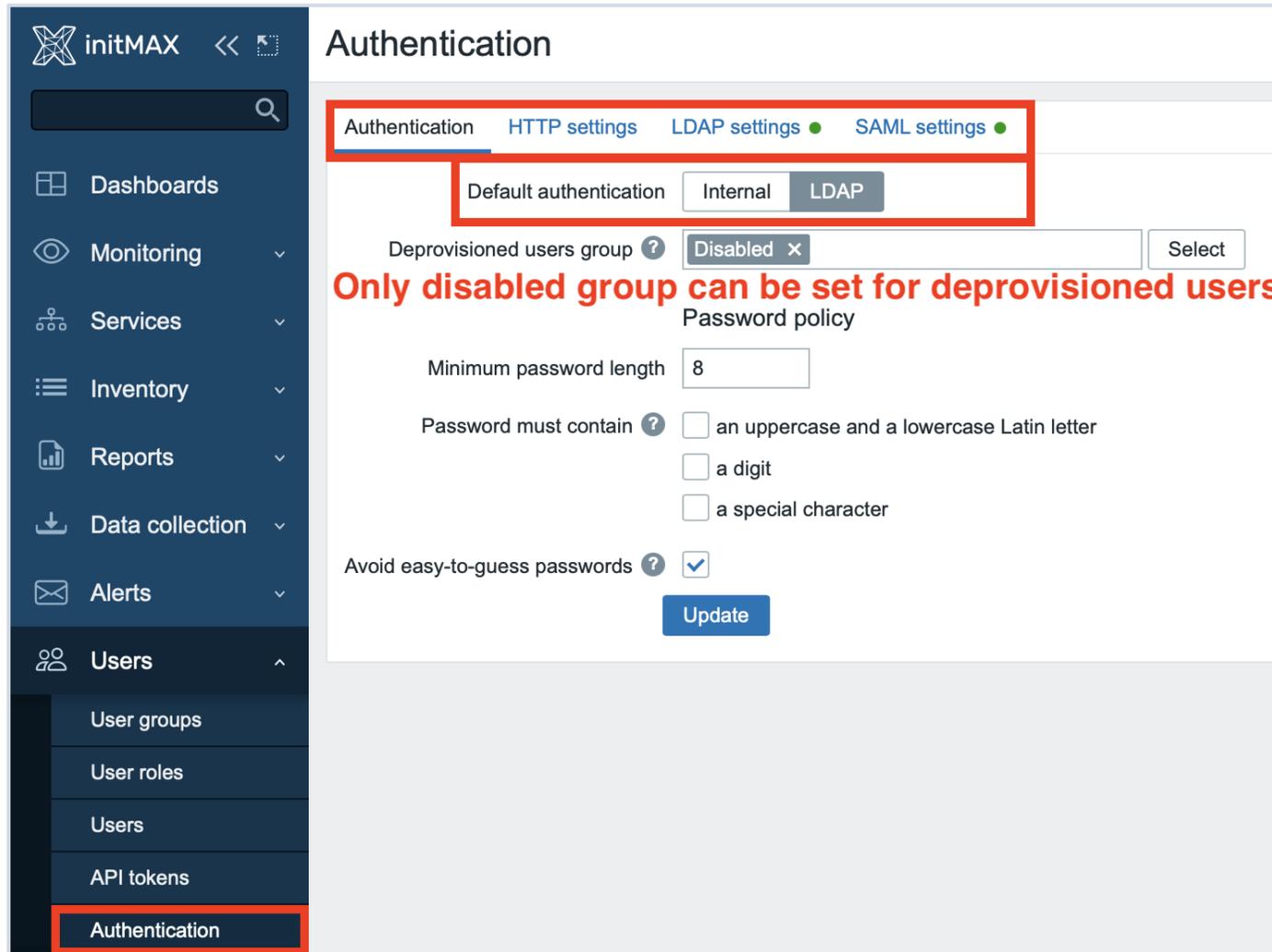
Available authentication options in
ZABBIX



Available authentication options in ZABBIX

- › By default, Zabbix uses **internal Zabbix authentication** for all users
 - › You can use combination internal and LDAP or SAML accounts
- › **HTTP or web server-based authentication** (for example: Basic Authentication, NTLM/Kerberos) can be used to check user names and passwords
 - › We are not be able to use JIT in this authentication
- › **External LDAP authentication** can be used to check user names and passwords
 - › Zabbix LDAP authentication works at least with **Microsoft Active Directory** and **OpenLDAP**
 - › **It is possible to configure JIT** (just-in-time) user provisioning for LDAP users. In this case, it is not required that a user already exists in Zabbix. The user account can be created when the user logs into Zabbix for the first time
- › **SAML 2.0 authentication** can be used to sign in to Zabbix
 - › **Our recommendation** is use this authentication with combination of internal user for fallback
 - › **It is possible to configure JIT** (just-in-time) user provisioning for SAML users. In this case, it is not required that a user already exists in Zabbix. The user account can be created when the user logs into Zabbix for the first time

Available authentication options in ZABBIX



The screenshot shows the Zabbix web interface for the Authentication settings page. The left sidebar contains a navigation menu with the following items: Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, and Users. The Users menu is expanded, showing sub-items: User groups, User roles, Users, API tokens, and Authentication. The Authentication sub-item is highlighted with a red box. The main content area is titled 'Authentication' and has a breadcrumb trail: Authentication > HTTP settings > LDAP settings > SAML settings. The 'Authentication' tab is active. Below the breadcrumb, there are two tabs for 'Default authentication': 'Internal' and 'LDAP'. The 'LDAP' tab is selected. Below the tabs, there is a dropdown menu for 'Deprovisioned users group' with 'Disabled' selected and a 'Select' button. A red text overlay reads: 'Only disabled group can be set for deprovisioned users'. Below this, there is a 'Password policy' section with the following settings: 'Minimum password length' is 8; 'Password must contain' has three unchecked options: 'an uppercase and a lowercase Latin letter', 'a digit', and 'a special character'; 'Avoid easy-to-guess passwords' is checked. An 'Update' button is at the bottom of the form.

initMAX << 🔍

Authentication HTTP settings LDAP settings ● SAML settings ●

Default authentication Internal LDAP

Deprovisioned users group ? Disabled × Select

Only disabled group can be set for deprovisioned users

Password policy

Minimum password length 8

Password must contain ? an uppercase and a lowercase Latin letter
 a digit
 a special character

Avoid easy-to-guess passwords ?

Update

Users

- User groups
- User roles
- Users
- API tokens
- Authentication

3

LDAP



Zabbix User Provisioning JIT

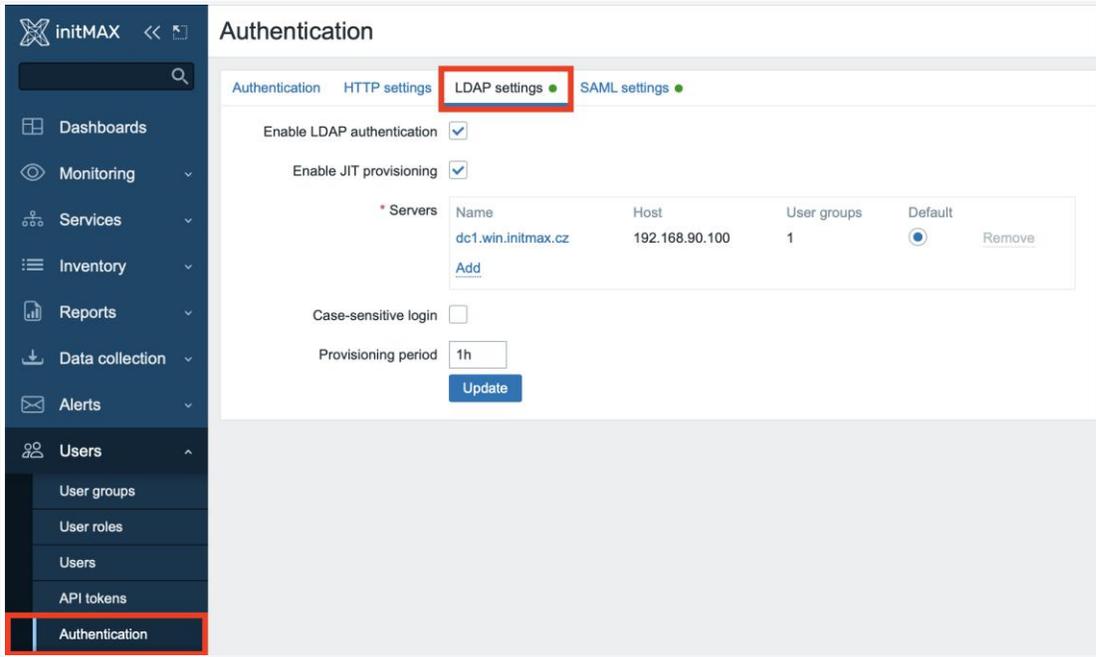
LDAP

- ▶ External LDAP authentication can be used to check user names and passwords
- ▶ Zabbix LDAP authentication works at least with Microsoft Active Directory and OpenLDAP
- ▶ If only LDAP sign-in is configured, then the user **must also exist** in Zabbix, however, its Zabbix password will not be used. If authentication is successful, then Zabbix will match a local username with the **Search attribute** returned by LDAP
 - ▶ It is possible to configure JIT (just-in-time) user provisioning for LDAP users. **In this case, it is not required that a user already exists in Zabbix.** The user account can be created when the user logs into Zabbix for the first time
 - ▶ When an LDAP user enters their LDAP login and password, Zabbix checks the default LDAP server if this user exists. If the user exists and does not have an account in Zabbix yet, a **new user is created in Zabbix and the user is able to log in**
- ▶ LDAP JIT provisioning is **available only** when LDAP is configured to use "anonymous" or "special user" for binding. For direct user binding, provisioning will be made only for user login action, because logging in user password is used for such type of binding
- ▶ Several LDAP servers can be defined, if it necessary

Zabbix User Provisioning JIT

LDAP – Active Directory

- › Enable LDAP authentication
 - › Mark the checkbox to enable LDAP authentication
- › Enable JIT provisioning
 - › Mark the checkbox to enable JIT provisioning
- › Servers
 - › Click on Add to configure an LDAP server
- › Case-sensitive login
 - › Unmark the checkbox to disable case-sensitive login (enabled by default) for usernames
- › Note that with case-sensitive login disabled the login will be denied if multiple users exist in Zabbix database with similar usernames (e.g. Admin, admin).
- › Provisioning period
 - › Set the provisioning period, i.e. how often user provisioning is performed.



The screenshot shows the 'Authentication' settings page in the Zabbix initMAX interface. The 'LDAP settings' tab is selected and highlighted with a red box. The page contains the following configuration options:

- Enable LDAP authentication:
- Enable JIT provisioning:
- Servers table:

Name	Host	User groups	Default	
dc1.win.initmax.cz	192.168.90.100	1	<input checked="" type="radio"/>	Remove

[Add](#)
- Case-sensitive login:
- Provisioning period:
- [Update](#) button

The left sidebar shows the navigation menu with 'Authentication' highlighted at the bottom.

LDAP – Active Directory

- ▶ **Name (dc1.win.initmax.cz)**
 - ▶ Name of the LDAP source in Zabbix configuration
- ▶ **Host (192.168.90.100)**
 - ▶ Host of the LDAP server
 - ▶ **ldap://ldap.initmax.com**
 - ▶ For secure LDAP server use ldaps protocol
 - ▶ **ldaps://ldap.initmax.com**
- ▶ **Port (389, 636) Default is 389 (389)**
 - ▶ Port of the LDAP server
 - ▶ For secure LDAP connection port number is 636.
 - ▶ Not used when using full LDAP URIs
- ▶ **Base DN (OU=initmax,DC=win,DC=initmax,DC=cz)**
 - ▶ Base path to user accounts in LDAP server
 - ▶ **DC=initmax,DC=com**

LDAP Server

* Name

* Host

* Port

* Base DN

* Search attribute

Bind DN

Bind password

Description

Configure JIT provisioning

Group configuration

Group name attribute

User group membership attribute

User name attribute

User last name attribute

* User group mapping

LDAP group pattern	User groups	User role	Action
Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	Remove

[Add](#)

Media type mapping

Name	Media type	Attribute	Action
Email	Email	mail	Remove
Mobile	SMS	mobile	Remove
Pushover	Pushover	msDS-cloudExtensionAttribute1	Remove

[Add](#)

Advanced configuration

LDAP – Active Directory

- › **Search attribute (sAMAccountName)**
 - › LDAP account attribute used for search
- › **Bind DN**
(**CN=search,OU=Service Accounts,OU=initmax,DC=win,DC=initmax,DC=cz**)
 - › LDAP account for binding and searching over the LDAP server
 - › Anonymous binding is also supported. Note that anonymous binding potentially opens up domain configuration to unauthorized users. For security reasons, **disable anonymous binds on LDAP hosts** and use authenticated access instead.
- › **Bind password**
 - › LDAP password of the account for binding and searching over the LDAP server.
- › **Description**
 - › Description of the LDAP server

LDAP Server

* Name

* Host

* Port

* Base DN

* Search attribute

Bind DN

Bind password

Description

Configure JIT provisioning

Group configuration

Group name attribute

User group membership attribute

User name attribute

User last name attribute

* User group mapping

LDAP group pattern	User groups	User role	Action
Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	Remove
Add			

Media type mapping

Name	Media type	Attribute	Action
Email	Email	mail	Remove
Mobile	SMS	mobile	Remove
Pushover	Pushover	msDS-cloudExtensionAttribute1	Remove
Add			

Advanced configuration

LDAP – Active Directory JIT Provisioning

› Configure JIT provisioning (Enable)

- › Mark this checkbox to show options related to JIT provisioning

› Group configuration (memberOf)

- › memberOf - by searching users and their group membership attribute
- › groupOfNames - by searching groups through the member attribute

› Group name attribute (CN)

- › Specify the attribute to get the group name from all objects in the memberOf attribute

› User group membership attribute !!! (memberof) !!!

- › Specify the attribute that contains information about the groups that the user belongs to

LDAP Server

* Name

* Host

* Port

* Base DN

* Search attribute

Bind DN

Bind password

Description

Configure JIT provisioning

Group configuration

Group name attribute

User group membership attribute

User name attribute

User last name attribute

* User group mapping

LDAP group pattern	User groups	User role	Action
Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	Remove
Add			

Media type mapping

Name	Media type	Attribute	Action
Email	Email	mail	Remove
Mobile	SMS	mobile	Remove
Pushover	Pushover	msDS-cloudExtensionAttribute1	Remove
Add			

Advanced configuration

LDAP – Active Directory JIT Provisioning

› User name attribute (givenName)

- › Specify the attribute that contains the user's first name

› User last name attribute (sn)

- › Specify the attribute that contains the user's last name

› User group mapping (Zabbix_Super_Admins)

- › Map an LDAP user group pattern to Zabbix user group and user role.
- › This is required to determine what user group/role the provisioned user will get in Zabbix.
- › The LDAP group pattern field supports wildcards. The group name must match an existing group.
- › If an LDAP user matches several Zabbix user groups, the user becomes a **member of all of them**.
- › If a user matches several Zabbix user roles, the user will get the one with the **highest permission** level among them.

LDAP Server

* Name

* Host

* Port

* Base DN

* Search attribute

Bind DN

Bind password

Description

Configure JIT provisioning

Group configuration

Group name attribute

User group membership attribute

User name attribute

User last name attribute

* User group mapping

LDAP group pattern	User groups	User role	Action
Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	Remove

[Add](#)

Media type mapping

Name	Media type	Attribute	Action
Email	Email	mail	Remove
Mobile	SMS	mobile	Remove
Pushover	Pushover	msDS-cloudExtensionAttribute1	Remove

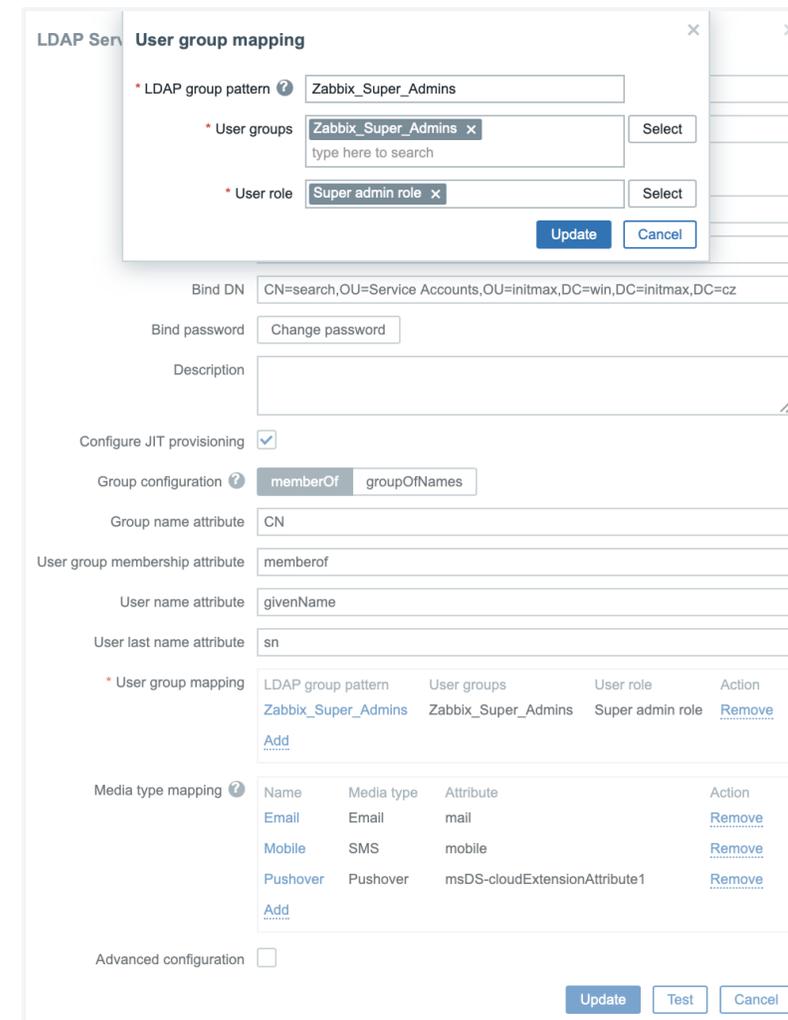
[Add](#)

Advanced configuration

LDAP – Active Directory JIT Provisioning

› User group mapping (Zabbix_Super_Admins)

- › Map an LDAP user group pattern to Zabbix user group and user role.
 - › This is required to determine what user group/role the provisioned user will get in Zabbix.
 - › The LDAP group pattern field supports wildcards. The group name must match an existing group.
 - › If an LDAP user matches several Zabbix user groups, the user becomes a **member of all of them**.
 - › If a user matches several Zabbix user roles, the user will get the one with the **highest permission level** among them.
-
- › Notes - Naming requirements
 - › group name must match LDAP group name
 - › wildcard patterns with '*' may be used



The screenshot shows the 'User group mapping' dialog box in the Zabbix LDAP configuration interface. The dialog is titled 'LDAP Service User group mapping'. It contains the following fields and options:

- LDAP group pattern:** Zabbix_Super_Admins
- User groups:** Zabbix_Super_Admins (selected), with a search input field below it.
- User role:** Super admin role (selected), with a search input field below it.
- Bind DN:** CN=search,OU=Service Accounts,OU=initmax,DC=win,DC=initmax,DC=cz
- Bind password:** Change password
- Description:** (empty text area)
- Configure JIT provisioning:**
- Group configuration:** memberOf (selected), groupOfNames
- Group name attribute:** CN
- User group membership attribute:** memberof
- User name attribute:** givenName
- User last name attribute:** sn
- User group mapping table:**

LDAP group pattern	User groups	User role	Action
Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	Remove

[Add](#)
- Media type mapping table:**

Name	Media type	Attribute	Action
Email	Email	mail	Remove
Mobile	SMS	mobile	Remove
Pushover	Pushover	msDS-cloudExtensionAttribute1	Remove

[Add](#)
- Advanced configuration:**

Buttons: Update, Cancel (in the dialog), Update, Test, Cancel (at the bottom).

LDAP – Active Directory JIT Provisioning

› Media type mapping

- › Map the user's LDAP media attributes to Zabbix user media for sending notifications

› Advanced configuration

- › Mark this checkbox to show advanced configuration options

› StartTLS

- › Mark the checkbox to use the StartTLS operation when connecting to LDAP server. The connection will fall if the server doesn't support StartTLS.
- › StartTLS cannot be used with servers that use the ldaps protocol.

› Search filter

- › Define a custom string when authenticating user in LDAP. The following placeholders are supported:
- › `%{attr}` - search attribute name (uid, sAMAccountName)
- › `%{user}` - user username value to authenticate.
- › If omitted then LDAP will use the default filter: `(%{attr}=%{user})`.

LDAP Server

* Name

* Host

* Port

* Base DN

* Search attribute

Bind DN

Bind password

Description

Configure JIT provisioning

Group configuration

Group name attribute

User group membership attribute

User name attribute

User last name attribute

* User group mapping

LDAP group pattern	User groups	User role	Action
Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	Remove
Add			

Media type mapping

Name	Media type	Attribute	Action
Email	Email	mail	Remove
Mobile	SMS	mobile	Remove
Pushover	Pushover	msDS-cloudExtensionAttribute1	Remove
Add			

Advanced configuration

LDAP – Notes

- ▶ The Test button allows to test user access

Test authentication ✕

✓ Login successful

* Login

* User password

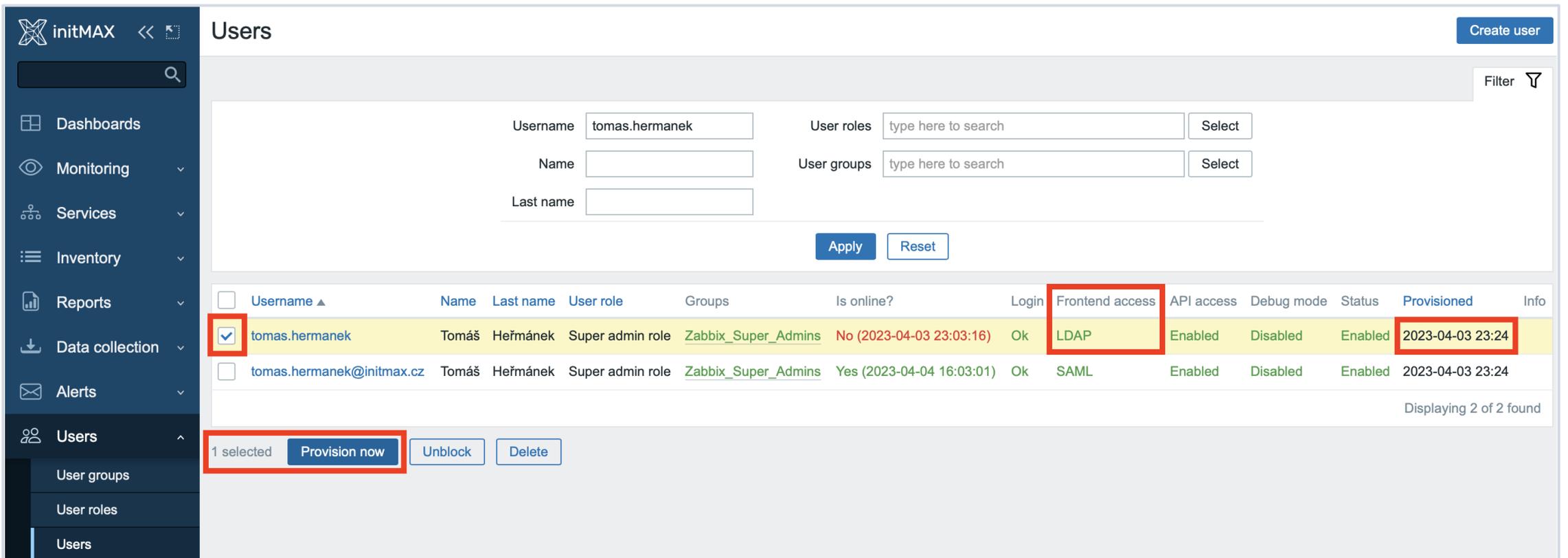
User role

User groups

Media type

LDAP – Notes

- ▶ If you are using binding user, you can use “Provision now” button on LDAP users (Default authentication need to be set up as LDAP)



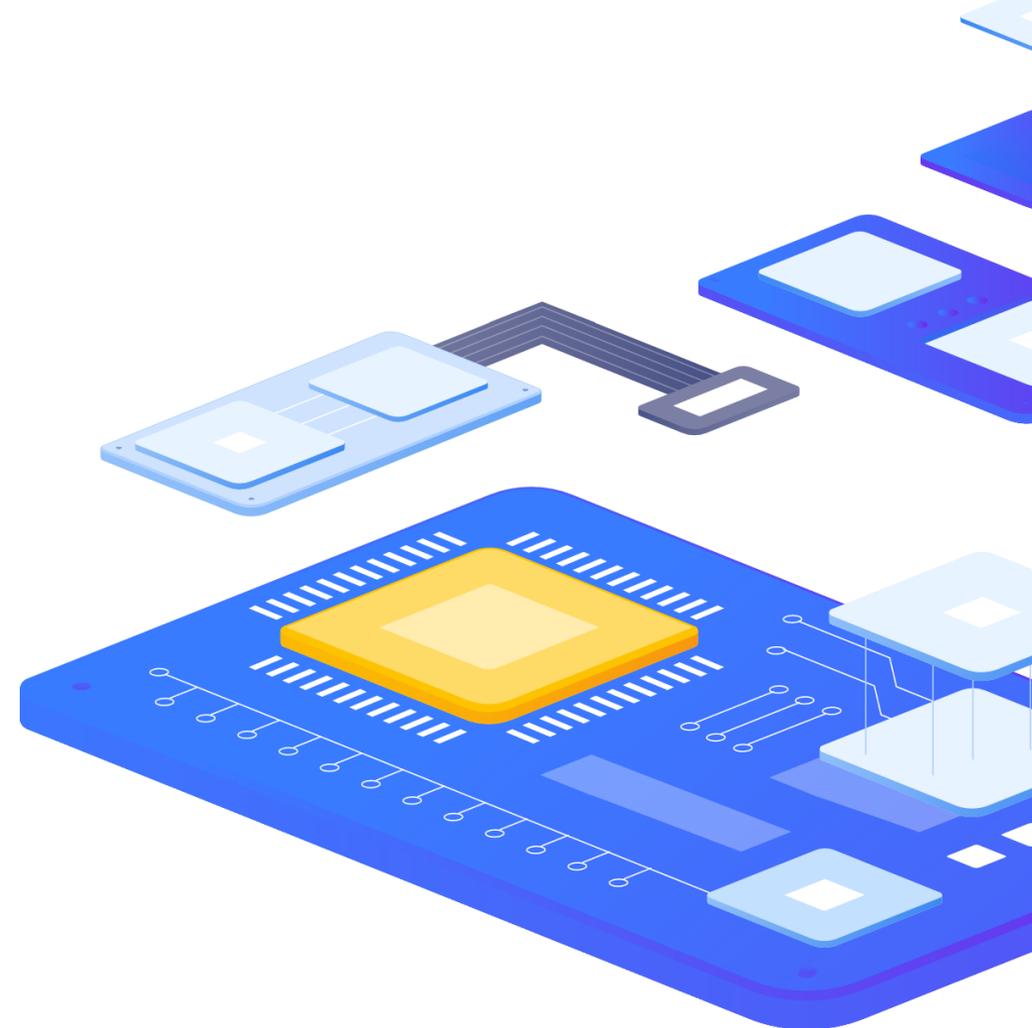
The screenshot shows the Zabbix Users management interface. On the left is a dark sidebar with navigation items: Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, and Users. The main area is titled "Users" and contains a search bar, a "Filter" icon, and a "Create user" button. Below these are input fields for Username (tomas.hermanek), Name, Last name, User roles, and User groups, with "Apply" and "Reset" buttons. A table lists two users:

<input type="checkbox"/>	Username ▲	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	Provisioned	Info
<input checked="" type="checkbox"/>	tomas.hermanek	Tomáš	Heřmánek	Super admin role	Zabbix_Super_Admins	No (2023-04-03 23:03:16)	Ok	LDAP	Enabled	Disabled	Enabled	2023-04-03 23:24	
<input type="checkbox"/>	tomas.hermanek@initmax.cz	Tomáš	Heřmánek	Super admin role	Zabbix_Super_Admins	Yes (2023-04-04 16:03:01)	Ok	SAML	Enabled	Disabled	Enabled	2023-04-03 23:24	

At the bottom, a summary bar shows "1 selected" and buttons for "Provision now", "Unblock", and "Delete".

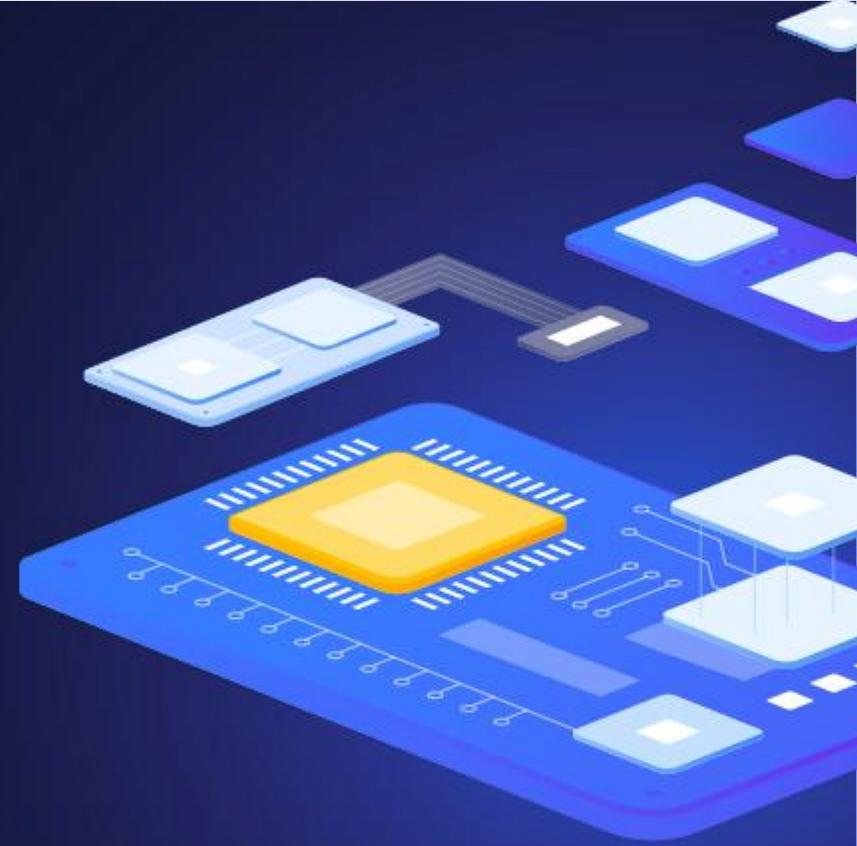
LDAP – Notes

- › If JIT provisioning is enabled, a user group for deprovisioned users must be specified in the Authentication tab.
- › You can use combination internal and LDAP authentication. But you need to use separate user.
- › Authentication setting for user can be found on user group level
 - › For example Admin (internal) and tomas.hermanek (LDAP)
- › Manually created user cannot be provisioned (workaround is use alter table for this specific user)



4

SAML

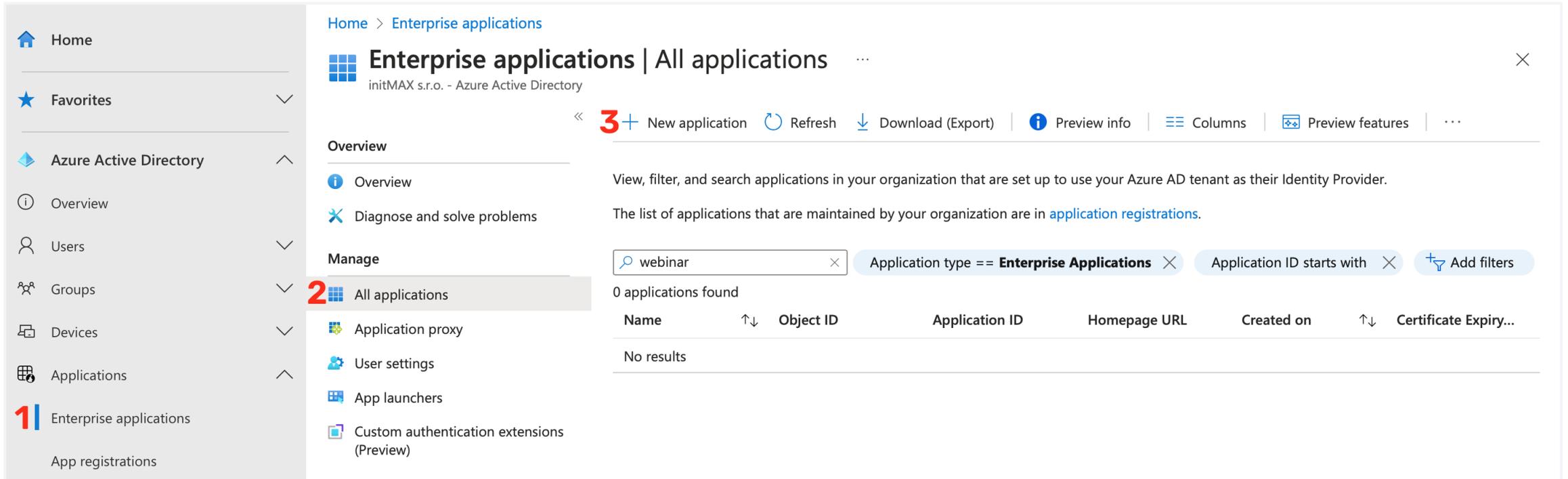


SAML

- › SAML authentication can be used for Single Sign On authentication
- › If only SAML sign-in is configured, then the user must also exist in Zabbix, however, its Zabbix password will not be used. If authentication is successful, then Zabbix will match a local username with the username attribute returned by SAML
- › You can define only one SAML authentication provider
- › You can use Azure Guest accounts from another tenants
 - › You need to setup this manually, (invite external users)
 - › Setup for this case is little bit complicated but it can be done
- › **User provisioning**
 - › It is possible to configure JIT (just-in-time) user provisioning for SAML users. In this case, it is not required that a user already exists in Zabbix. The user account can be created when the user logs into Zabbix for the first time.
- › Secure way for user authentication (recommended)

SAML – Zabbix – Azure

- ▶ Create your new Enterprise application
 - ▶ We need this application for our SAML setting



The screenshot shows the Azure Active Directory portal interface. On the left is a navigation sidebar with options: Home, Favorites, Azure Active Directory, Overview, Users, Groups, Devices, Applications, Enterprise applications (highlighted with a red '1'), and App registrations. The main content area is titled 'Enterprise applications | All applications' for 'initMAX s.r.o. - Azure Active Directory'. It features a search bar with 'webinar' and filters for 'Application type == Enterprise Applications' and 'Application ID starts with'. Below the search, it states '0 applications found' and displays a table with columns: Name, Object ID, Application ID, Homepage URL, Created on, and Certificate Expiry... The table currently shows 'No results'. A red '2' is placed over the 'All applications' menu item in the sidebar.

Home > Enterprise applications

Enterprise applications | All applications

initMAX s.r.o. - Azure Active Directory

« **3+** New application Refresh Download (Export) Preview info Columns Preview features ...

Overview

- Overview
- Diagnose and solve problems

Manage

- 2** All applications
- Application proxy
- User settings
- App launchers
- Custom authentication extensions (Preview)

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

The list of applications that are maintained by your organization are in [application registrations](#).

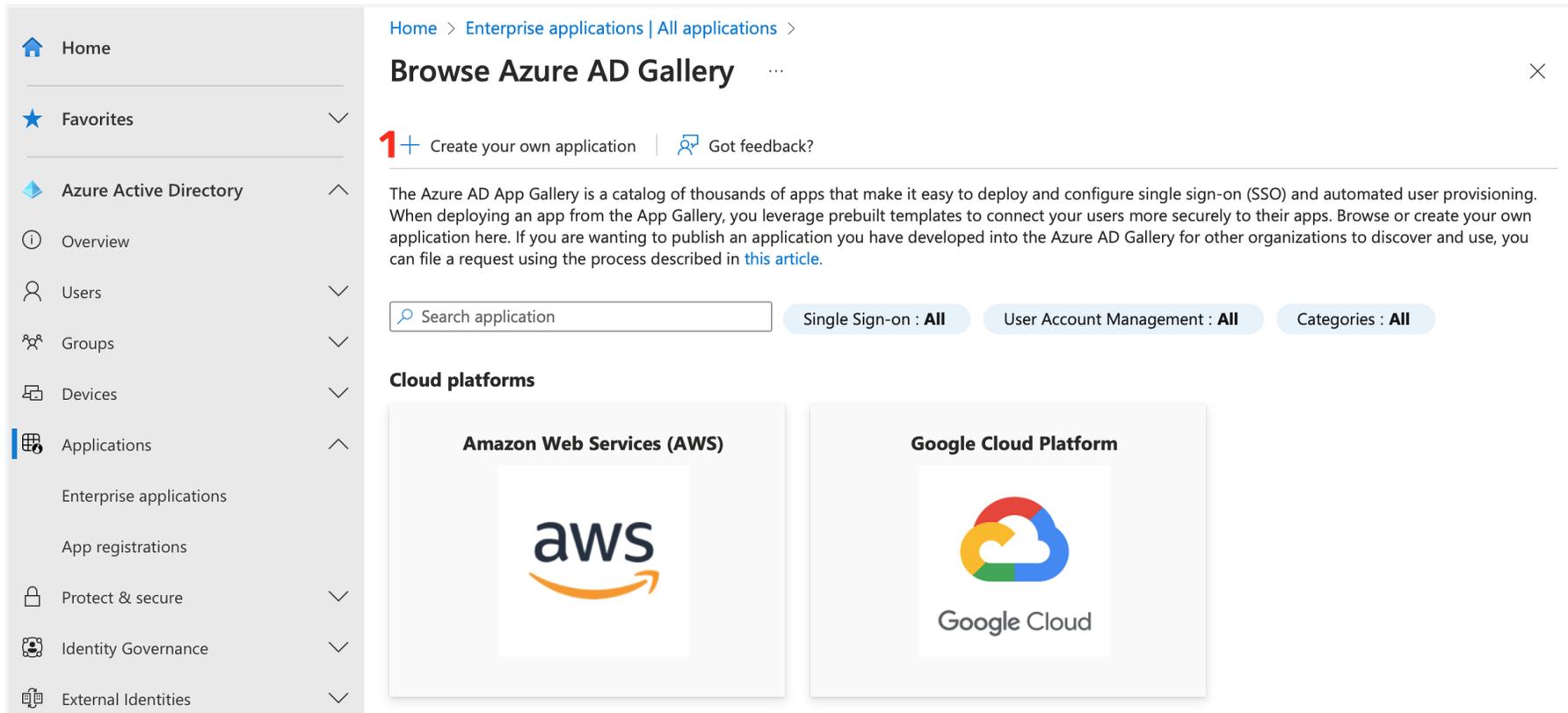
webinar Application type == Enterprise Applications Application ID starts with Add filters

0 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry...
No results					

SAML – Zabbix – Azure

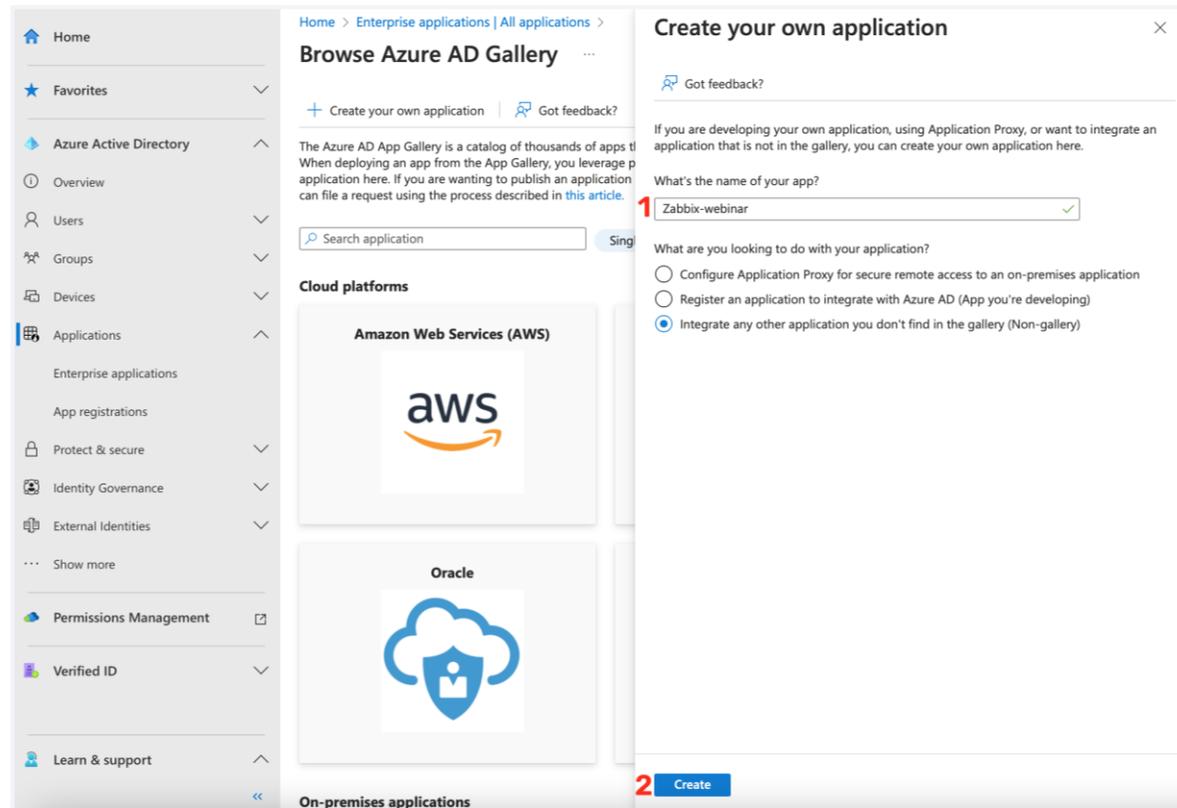
- ▶ Create your new Enterprise application
 - ▶ Hit button “Create your own application”



The screenshot shows the Azure AD App Gallery interface. On the left is a navigation sidebar with the following items: Home, Favorites, Azure Active Directory, Overview, Users, Groups, Devices, Applications (highlighted), Enterprise applications, App registrations, Protect & secure, Identity Governance, and External Identities. The main content area is titled "Browse Azure AD Gallery" and includes a breadcrumb "Home > Enterprise applications | All applications >". Below the title is a button "1+ Create your own application" and a link "Got feedback?". A descriptive paragraph follows: "The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Azure AD Gallery for other organizations to discover and use, you can file a request using the process described in [this article](#)." Below the text is a search bar labeled "Search application" and three filter buttons: "Single Sign-on : All", "User Account Management : All", and "Categories : All". Under the heading "Cloud platforms", there are two cards: "Amazon Web Services (AWS)" with the AWS logo and "Google Cloud Platform" with the Google Cloud logo.

SAML – Zabbix – Azure

- ▶ Create your new Enterprise application
 - ▶ Chose your own application name



The screenshot shows the Azure AD portal interface for creating a new application. The left sidebar contains navigation options: Home, Favorites, Azure Active Directory, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Protect & secure, Identity Governance, External Identities, Show more, Permissions Management, Verified ID, and Learn & support. The main content area is titled 'Browse Azure AD Gallery' and includes a search bar and a 'Create your own application' link. Below this, there are sections for 'Cloud platforms' (Amazon Web Services (AWS) and Oracle) and 'On-premises applications'. A modal window titled 'Create your own application' is open, showing the following steps:

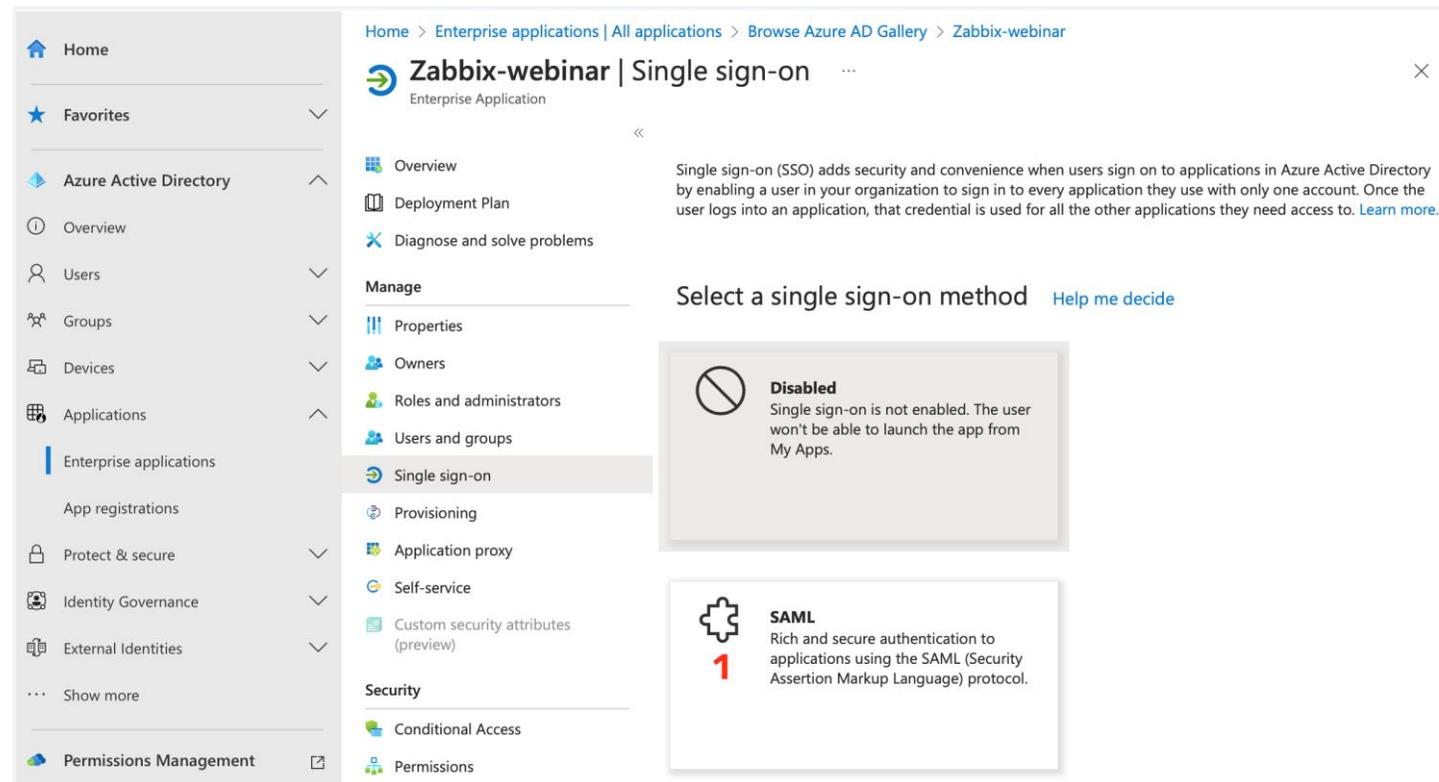
1. What's the name of your app? (Zabbix-webinar)
2. What are you looking to do with your application?
 - Configure Application Proxy for secure remote access to an on-premises application
 - Register an application to integrate with Azure AD (App you're developing)
 - Integrate any other application you don't find in the gallery (Non-gallery)

The 'Create' button is visible at the bottom right of the modal.

Zabbix User Provisioning JIT

SAML – Zabbix – Azure

- ▶ Single sign-on setting
 - ▶ Select SAML as a sign-on method



Home > Enterprise applications | All applications > Browse Azure AD Gallery > Zabbix-webinar

Zabbix-webinar | Single sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes (preview)

Security

Conditional Access

Permissions

Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more.](#)

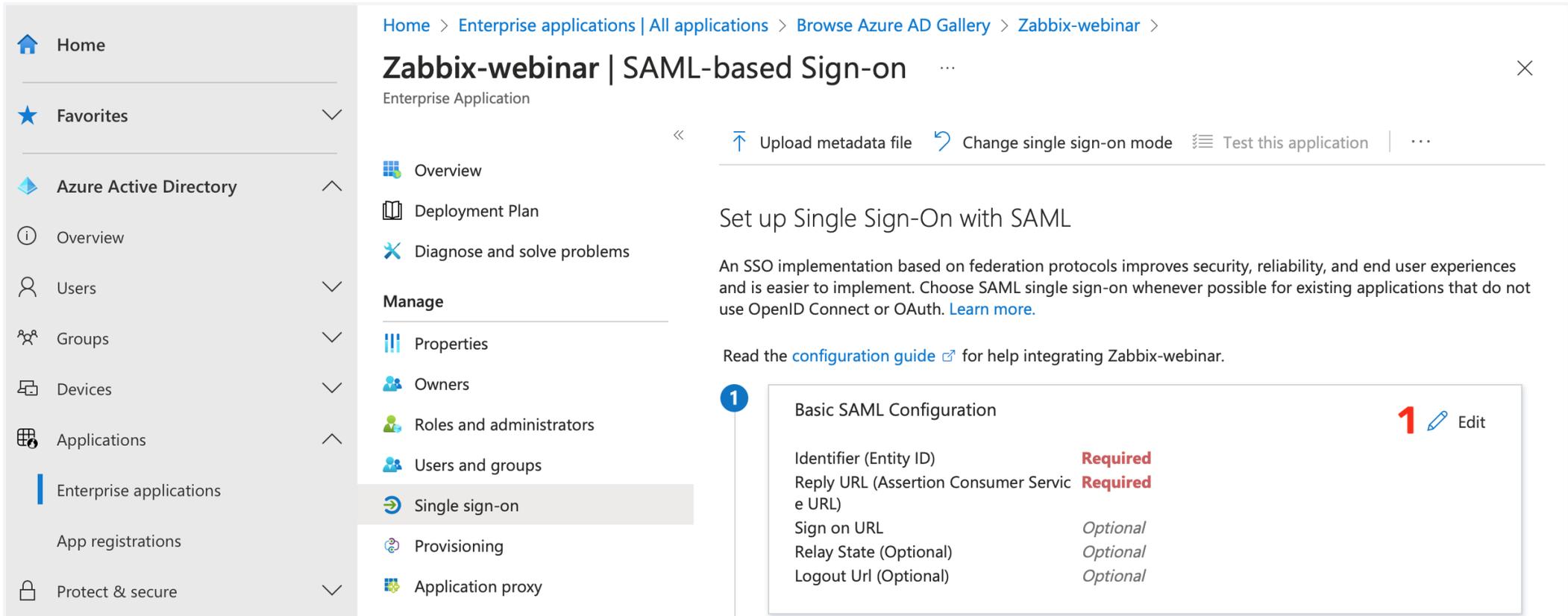
Select a single sign-on method [Help me decide](#)

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

SAML – Zabbix – Azure

- › Single sign-on setting
 - › Edit basic SAML configuration



The screenshot displays the Azure portal interface for configuring SAML-based Sign-on for the 'Zabbix-webinar' application. The left-hand navigation pane includes sections for Home, Favorites, Azure Active Directory, and Enterprise applications. The 'Enterprise applications' section is expanded, showing 'Zabbix-webinar | SAML-based Sign-on' as the selected item. The main content area features a breadcrumb trail: Home > Enterprise applications | All applications > Browse Azure AD Gallery > Zabbix-webinar >. Below the breadcrumb, there are action buttons: 'Upload metadata file', 'Change single sign-on mode', and 'Test this application'. The main heading is 'Set up Single Sign-On with SAML', followed by a descriptive paragraph and a link to the 'configuration guide'. A 'Basic SAML Configuration' table is highlighted with a red '1' and an 'Edit' button.

Basic SAML Configuration		1  Edit
Identifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
Sign on URL	<i>Optional</i>	
Relay State (Optional)	<i>Optional</i>	
Logout Url (Optional)	<i>Optional</i>	

Zabbix User Provisioning JIT

SAML – Zabbix – Azure

- › Single sign-on setting
 - › **Fill Entity ID** (We are using Zabbix URL)
<https://student-01.initmax.cz/zabbix>
 - › **Reply URL** (here is where Zabbix expecting authentication token)
https://student-01.initmax.cz/zabbix/index_sso.php?acs
 - › **Logout URL** (This is optional)
https://student-01.initmax.cz/zabbix/index_sso.php?sls
- › Save our new setting and exit configuration window

Basic SAML Configuration 5x

4 Save | Got feedback?

Identifier (Entity ID) * 1
The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

✓ [] [] []

Add identifier

Reply URL (Assertion Consumer Service URL) * 2
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

✓ [] [] []

Add reply URL

Sign on URL (Optional)
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

✓

Relay State (Optional) ⓘ
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.

Logout Url (Optional) 3
This URL is used to send the SAML logout response back to the application.

✓

SAML – Zabbix – Azure

- › Single sign-on setting
 - › Close test popup

[↑ Upload metadata file](#) [↶ Change single sign-on mode](#) [☰ Test this application](#) | [🗨️ Got feedback?](#)

Test single sign-on with Zabbix-webinar

To ensure that single sign-on works for your application, we recommend using the testing capability (in the last step) to test the changes you recently made. Would you like to test now?

Yes

No, I'll test later

[Read the configuration guide](#) for help integrating Zabbix-webinar.

SAML – Zabbix – Azure

- › Single sign-on setting
 - › Close test pop

[↑ Upload metadata file](#) [↶ Change single sign-on mode](#) [☰ Test this application](#) | [🗨️ Got feedback?](#)

Test single sign-on with Zabbix-webinar

To ensure that single sign-on works for your application, we recommend using the testing capability (in the last step) to test the changes you recently made. Would you like to test now?

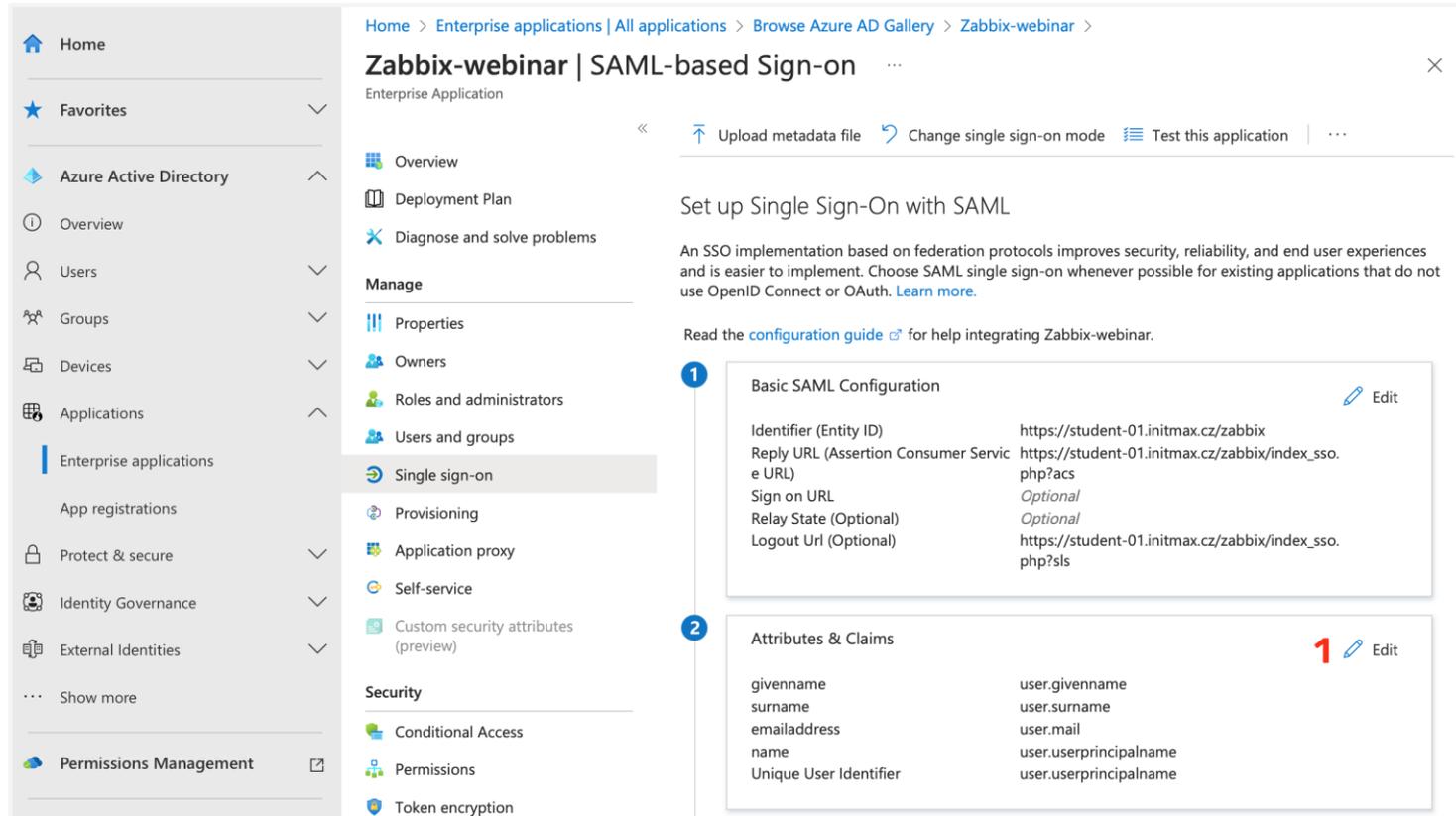
Yes

No, I'll test later

[Read the configuration guide](#) for help integrating Zabbix Webinar.

SAML – Zabbix – Azure

- ▶ Single sign-on setting
 - ▶ Edit Attributes & Claims



The screenshot shows the Azure AD portal interface for configuring SAML for the 'Zabbix-webinar' application. The left sidebar contains navigation options like Home, Favorites, Azure Active Directory, and Enterprise applications. The main content area is titled 'Zabbix-webinar | SAML-based Sign-on' and includes a 'Manage' section with options like Properties, Owners, Roles and administrators, and Users and groups. The 'Single sign-on' option is selected, leading to a configuration page with two main sections: 'Basic SAML Configuration' and 'Attributes & Claims'.

Basic SAML Configuration

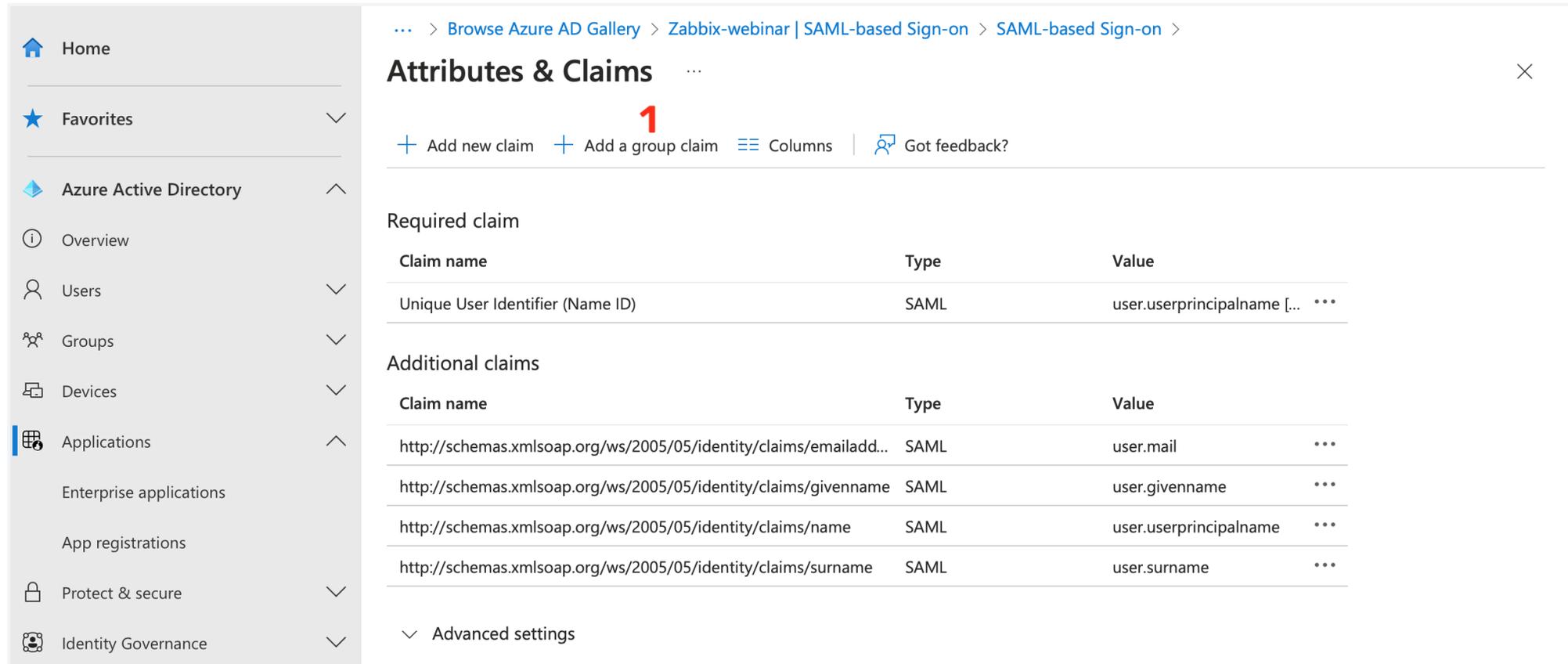
Identifier (Entity ID)	https://student-01.initmax.cz/zabbix
Reply URL (Assertion Consumer Service URL)	https://student-01.initmax.cz/zabbix/index_sso.php?acs
Sign on URL	Optional
Relay State (Optional)	Optional
Logout URL (Optional)	https://student-01.initmax.cz/zabbix/index_sso.php?sls

Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML – Zabbix – Azure

- ▶ Single sign-on setting
 - ▶ We need to add group claim for JIT (We show how this work in Zabbix later)



... > Browse Azure AD Gallery > Zabbix-webinar | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

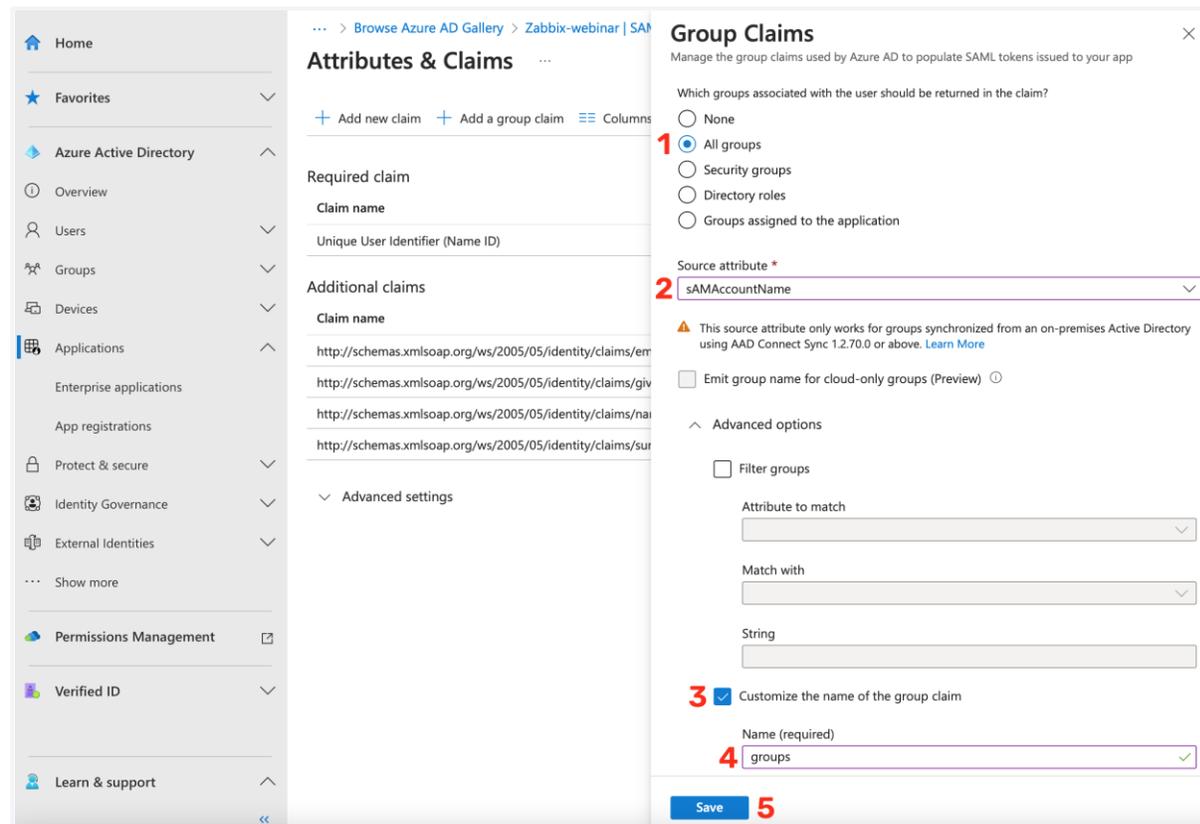
Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

Advanced settings

Zabbix User Provisioning JIT

SAML – Zabbix – Azure

- ▶ Single sign-on setting
 - ▶ Here we are using basic setting for groups claim (We have hybrid environment)
 - ▶ This setting can be tuned!

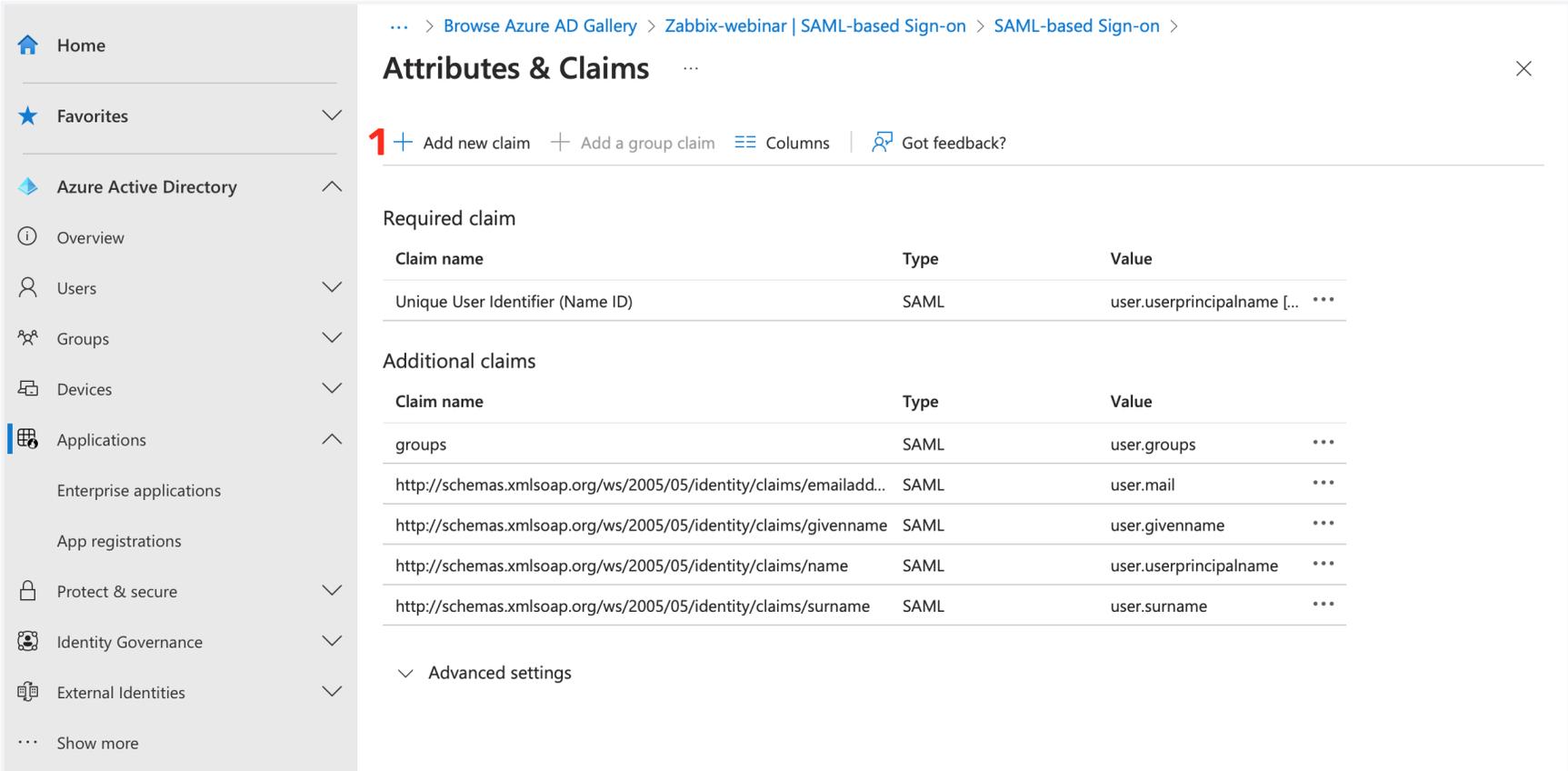


The screenshot displays the Azure AD portal interface for configuring SAML group claims. The left sidebar shows navigation options like Home, Favorites, Azure Active Directory, and Applications. The main content area is titled 'Attributes & Claims' and includes a table of 'Additional claims' with columns for 'Claim name' and 'Source attribute'. The right-hand 'Group Claims' panel is the primary focus, showing the following configuration:

- Group Claims**: Manage the group claims used by Azure AD to populate SAML tokens issued to your app.
- Which groups associated with the user should be returned in the claim?**: Radio buttons for None, **All groups** (selected), Security groups, Directory roles, and Groups assigned to the application.
- Source attribute ***: A dropdown menu set to 'sAMAccountName'.
- Advanced options**:
 - Emit group name for cloud-only groups (Preview)
 - Filter groups
 - Attribute to match: [Dropdown]
 - Match with: [Dropdown]
 - String: [Text input]
 - Customize the name of the group claim
 - Name (required): [Text input set to 'groups']
- Save** button.

SAML – Zabbix – Azure

- ▶ Single sign-on setting
 - ▶ We need to add new claim for username and additionally for first name, last name and medias



The screenshot shows the 'Attributes & Claims' configuration page in the Azure AD portal. The left sidebar contains navigation options: Home, Favorites, Azure Active Directory, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Protect & secure, Identity Governance, External Identities, and Show more. The main content area shows the breadcrumb path: ... > Browse Azure AD Gallery > Zabbix-webinar | SAML-based Sign-on > SAML-based Sign-on >. Below the breadcrumb is the title 'Attributes & Claims' with a close button. A red '1+' icon indicates a new claim. Action buttons include 'Add new claim', 'Add a group claim', 'Columns', and 'Got feedback?'. The page is divided into 'Required claim' and 'Additional claims' sections, each with a table of claim details.

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

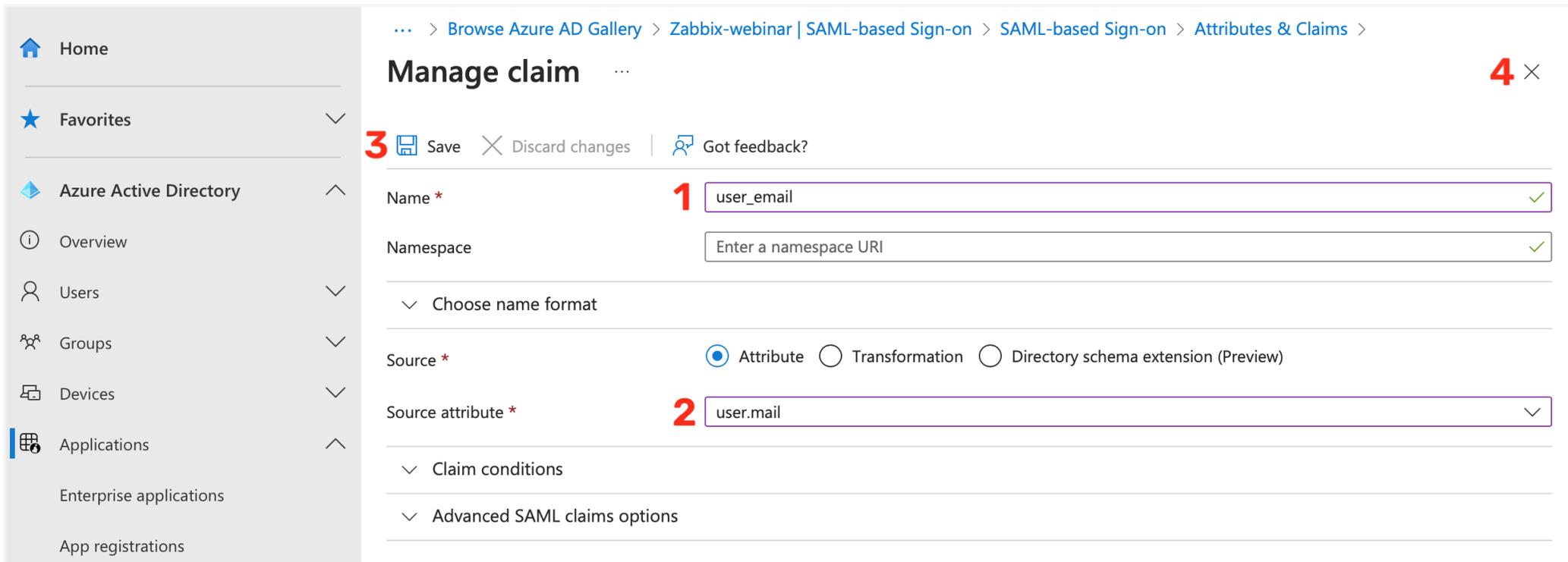
Claim name	Type	Value
groups	SAML	user.groups
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

Advanced settings

SAML – Zabbix – Azure

› Single sign-on setting

- › We need to add new claim for username and additionally for first name, last name and medias



... > [Browse Azure AD Gallery](#) > [Zabbix-webinar | SAML-based Sign-on](#) > [SAML-based Sign-on](#) > [Attributes & Claims](#) >

Manage claim 4 ×

3 Save × Discard changes | [Got feedback?](#)

Name * **1**

Namespace

Choose name format

Source * Attribute Transformation Directory schema extension (Preview)

Source attribute * **2**

Claim conditions

Advanced SAML claims options

SAML – Zabbix – Azure

- › Single sign-on setting
 - › Repeat this operation for all your attributes
email is important we are using this claim for “Username attribute” in Zabbix (login)
 - › Pushover in our case is extended attribute from Standalone Active Directory server

user_email

user.mail

Optional claims

user_mobile

user.mobilephone

user_lastname

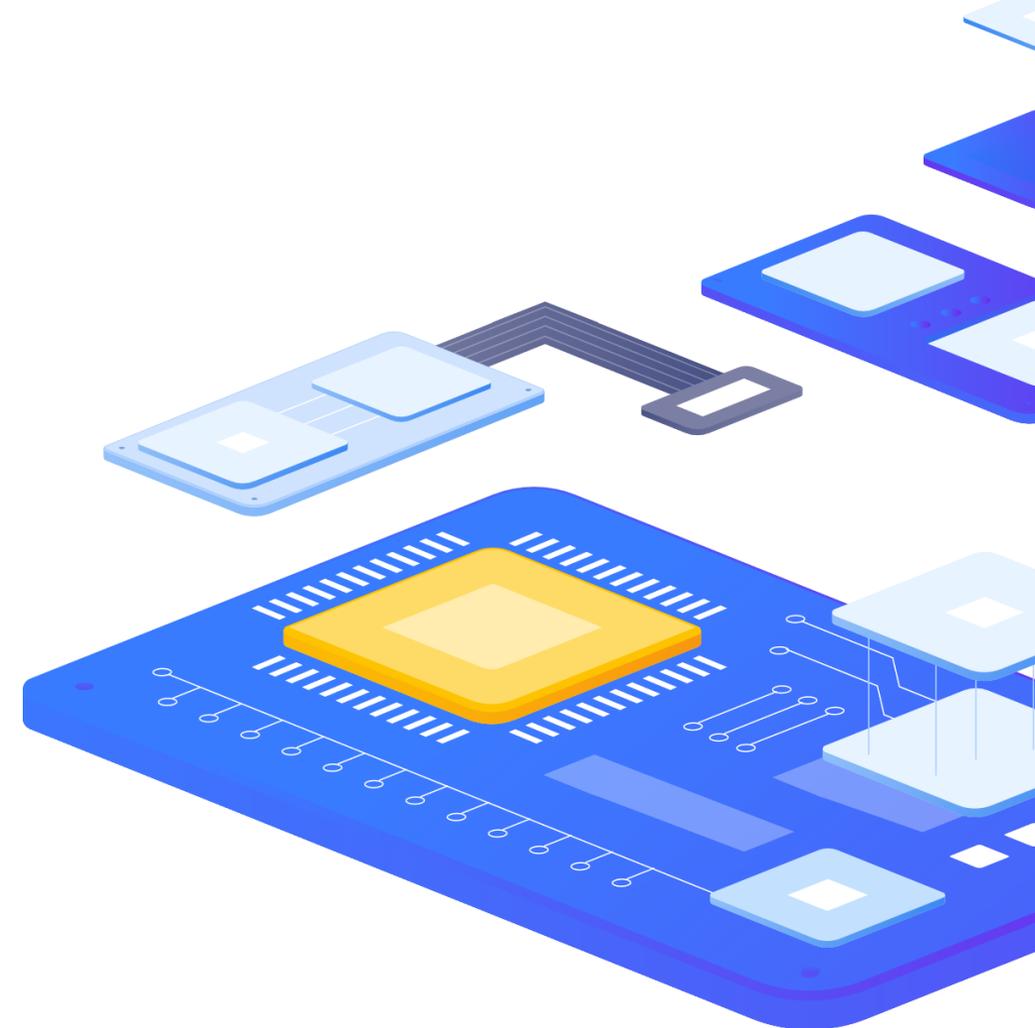
user.surname

user_name

user.givenname

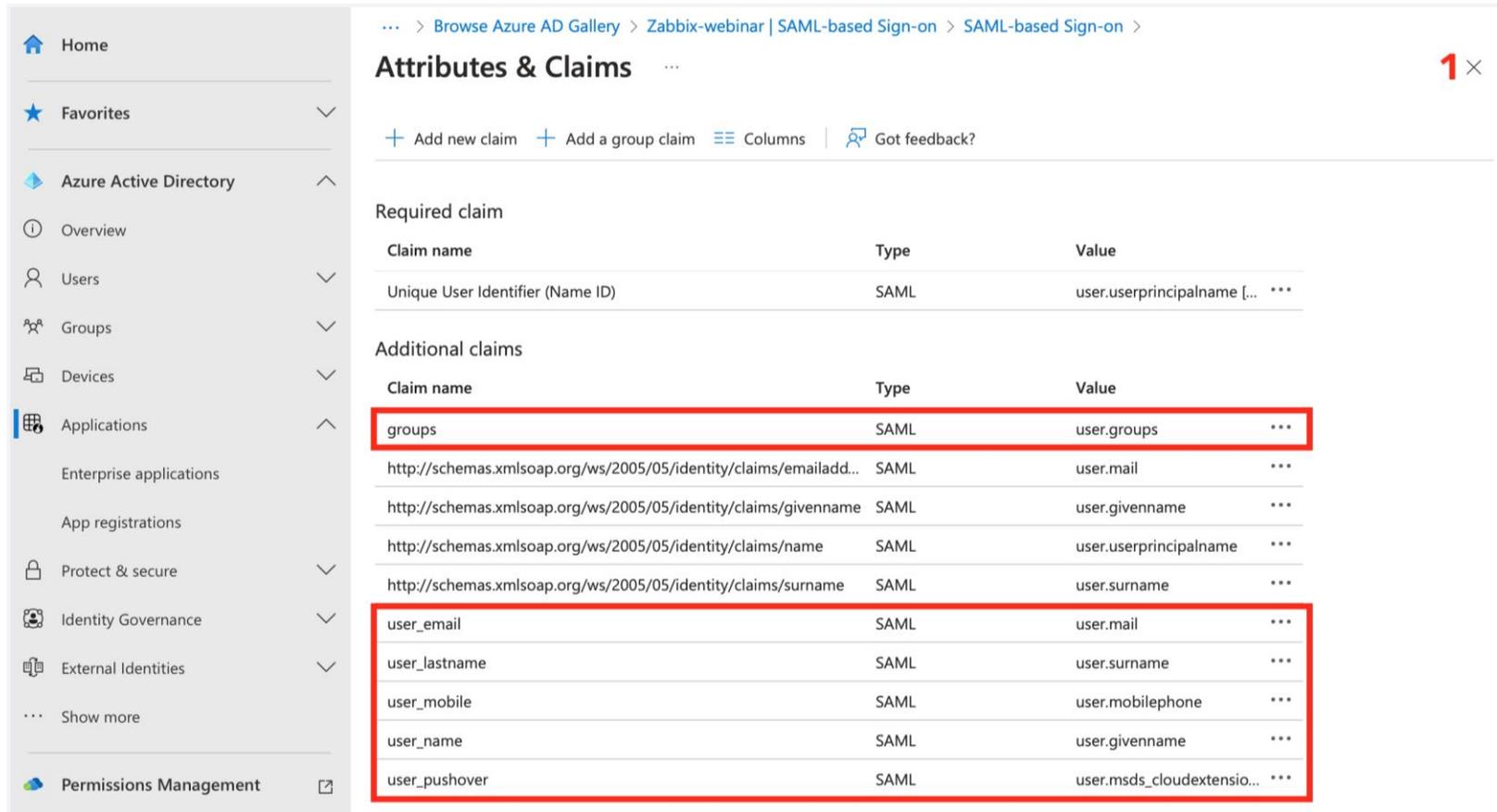
user_pushover

user.msds_cloud...



SAML – Zabbix – Azure

▶ Single sign-on setting



... > Browse Azure AD Gallery > Zabbix-webinar | SAML-based Sign-on > SAML-based Sign-on >

Attributes & Claims

+ Add new claim + Add a group claim Columns | Got feedback?

Required claim

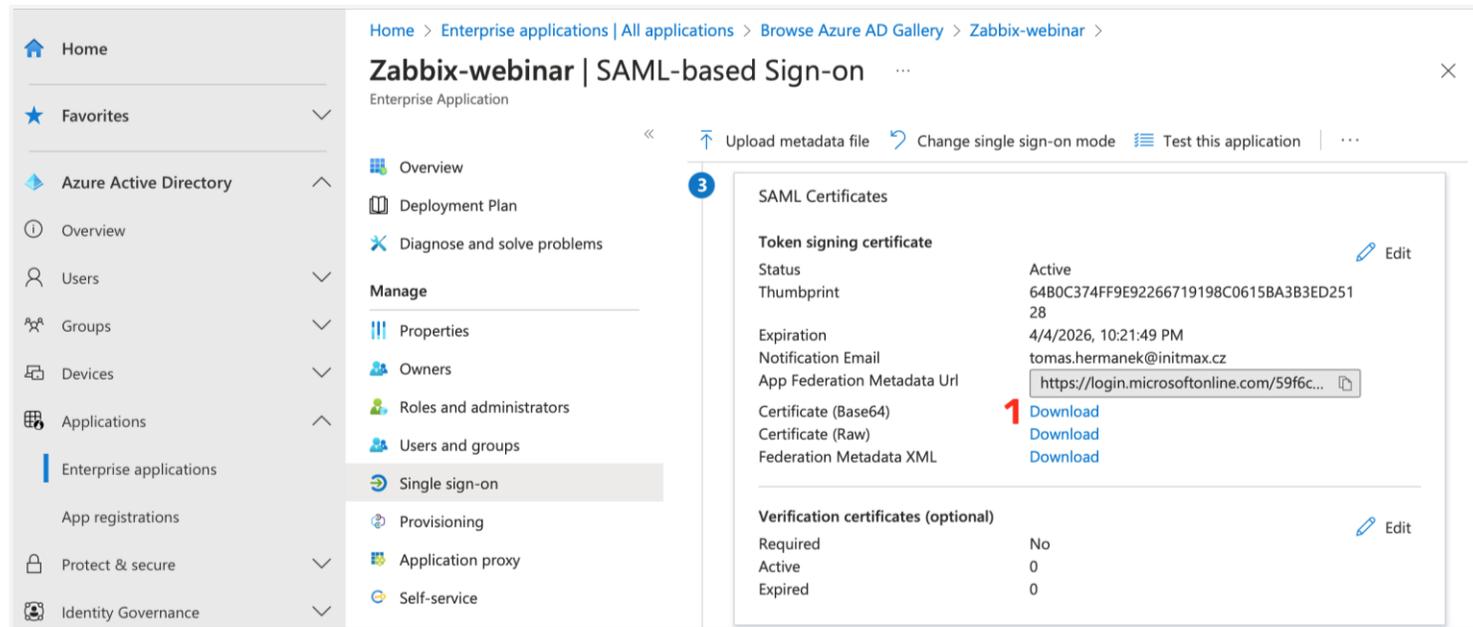
Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
groups	SAML	user.groups
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname
user_email	SAML	user.mail
user_lastname	SAML	user.surname
user_mobile	SAML	user.mobilephone
user_name	SAML	user.givenname
user_pushover	SAML	user.msds_cloudextensio...

SAML – Zabbix – Azure

- ▶ Single sign-on setting
 - ▶ Last part for SAML setting in Azure is export certificate for signed Zabbix tokens (Base64)



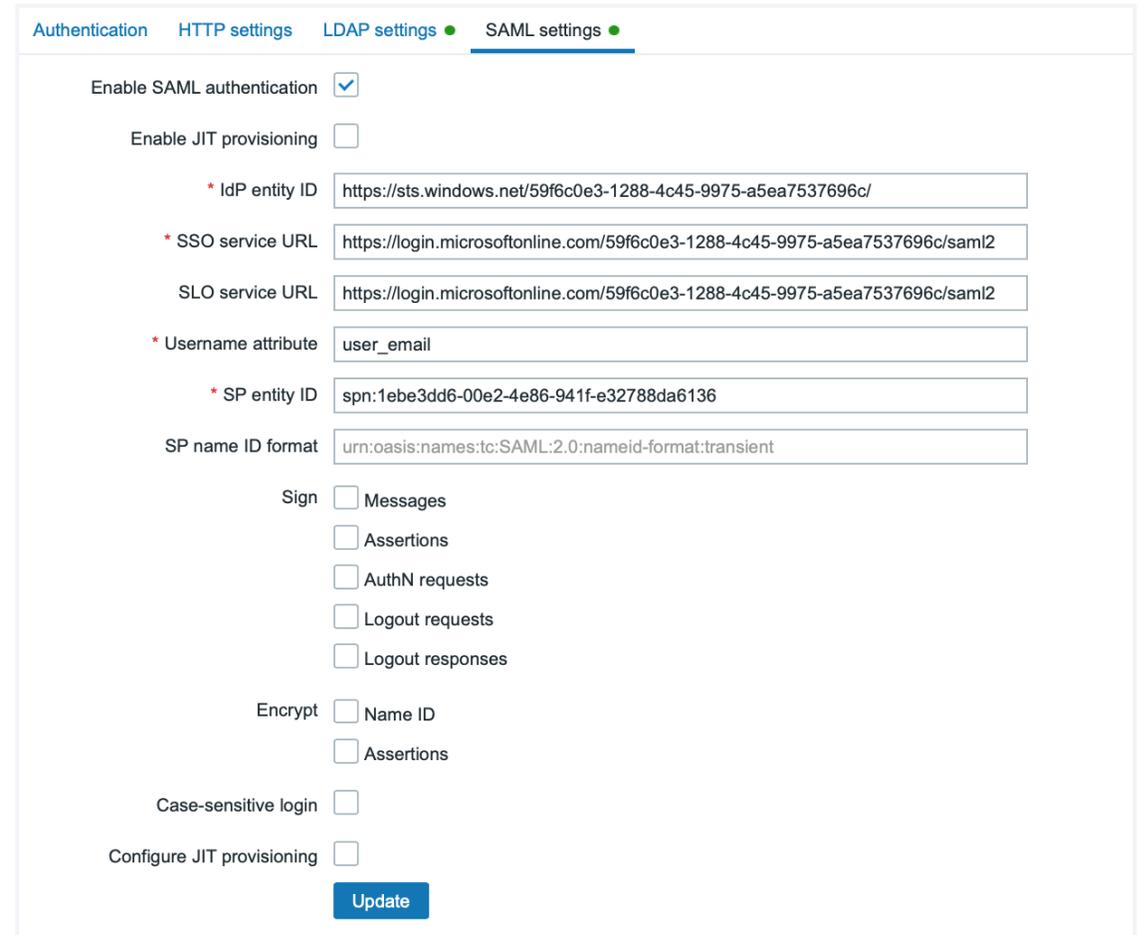
The screenshot shows the Azure portal interface for configuring SAML-based sign-on for an application named "Zabbix-webinar". The left sidebar contains navigation options like Home, Favorites, Azure Active Directory, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Protect & secure, and Identity Governance. The main content area is titled "Zabbix-webinar | SAML-based Sign-on" and includes options to "Upload metadata file", "Change single sign-on mode", and "Test this application". A "SAML Certificates" panel is open, displaying details for a "Token signing certificate".

Token signing certificate		Edit
Status	Active	
Thumbprint	64B0C374FF9E92266719198C0615BA3B3ED25128	
Expiration	4/4/2026, 10:21:49 PM	
Notification Email	tomas.hermanek@initmax.cz	
App Federation Metadata Url	https://login.microsoftonline.com/59f6c...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Verification certificates (optional)		Edit
Required	No	
Active	0	
Expired	0	

SAML – Zabbix

- › Enable SAML authentication
 - › Mark the checkbox to enable SAML authentication
- › Enable JIT provisioning (we discuss this later)
 - › Mark the checkbox to enable JIT provisioning
- › IdP entity ID (In Azure AD is named “**Azure AD Identifier**”)
 - › The unique entity identifier within the SAML identity provider
- › SSO service URL (In Azure AD is named “**Login URL**”)
 - › The URL users will be redirected to when logging in
- › SLO service URL (In Azure AD is named “**Logout URL**”)
 - › The URL users will be redirected to when logging out. If left empty, the SLO service will not be used.
- › Username attribute (Our claim name is “user_email”)
 - › SAML attribute to be used as a username when logging into Zabbix.
- › SP entity ID (In Azure AD is named “**Application ID**”)
 - › The unique service provider identifier
 - › **For Azure you need use prefix “spn:”**

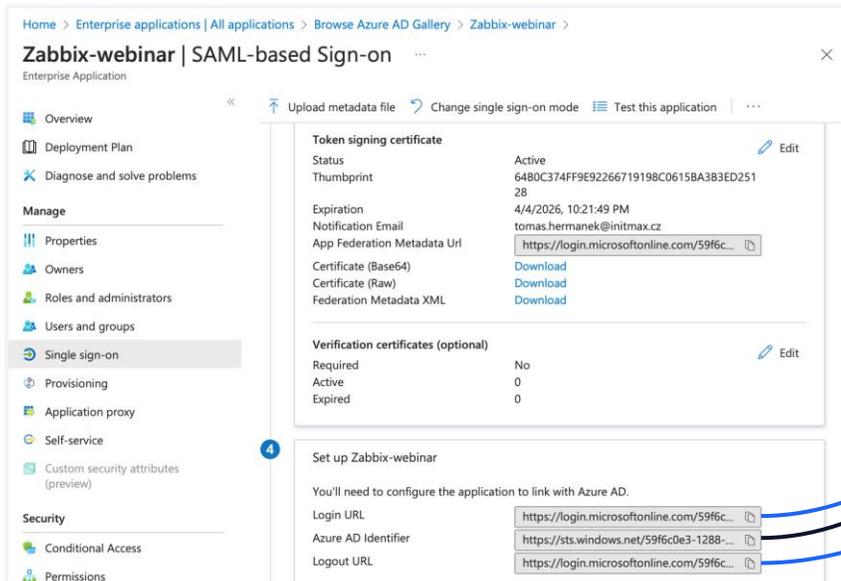


The screenshot shows the Zabbix configuration interface for SAML settings. The 'SAML settings' tab is active. The configuration includes:

- Enable SAML authentication:**
- Enable JIT provisioning:**
- * IdP entity ID:**
- * SSO service URL:**
- SLO service URL:**
- * Username attribute:**
- * SP entity ID:**
- SP name ID format:**
- Sign:** Messages, Assertions, AuthN requests, Logout requests, Logout responses
- Encrypt:** Name ID, Assertions
- Case-sensitive login:**
- Configure JIT provisioning:**
- Update:**

Zabbix User Provisioning JIT

SAML – Zabbix



Home > Enterprise applications | All applications > Browse Azure AD Gallery > Zabbix-webinar > Zabbix-webinar | SAML-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes (preview)

Security

Conditional Access

Permissions

Token signing certificate

Status	Active	Edit
Thumbprint	6480C374FF9E92266719198C0615BA383ED25128	
Expiration	4/4/2026, 10:21:49 PM	
Notification Email	tomas.hermanek@initmax.cz	
App Federation Metadata Url	https://login.microsoftonline.com/59f6c0e3-1288-4c45-9975-a5ea7537696c/	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

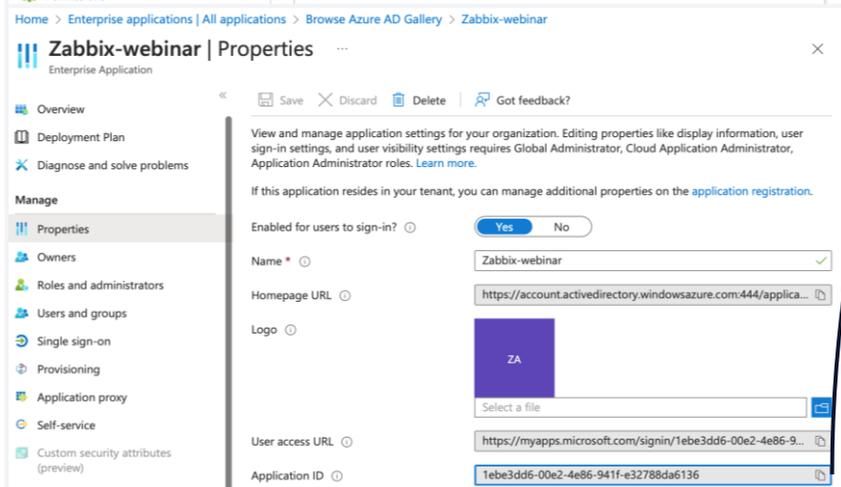
Verification certificates (optional)

Required	No	Edit
Active	0	
Expired	0	

4 Set up Zabbix-webinar

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/59f6c0e3-1288-4c45-9975-a5ea7537696c/
Azure AD Identifier	https://sts.windows.net/59f6c0e3-1288-4c45-9975-a5ea7537696c/
Logout URL	https://login.microsoftonline.com/59f6c0e3-1288-4c45-9975-a5ea7537696c/



Home > Enterprise applications | All applications > Browse Azure AD Gallery > Zabbix-webinar > Zabbix-webinar | Properties

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

Properties

Owners

Roles and administrators

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Custom security attributes (preview)

View and manage application settings for your organization. Editing properties like display information, user sign-in settings, and user visibility settings requires Global Administrator, Cloud Application Administrator, Application Administrator roles. [Learn more.](#)

If this application resides in your tenant, you can manage additional properties on the [application registration](#).

Enabled for users to sign-in? Yes No

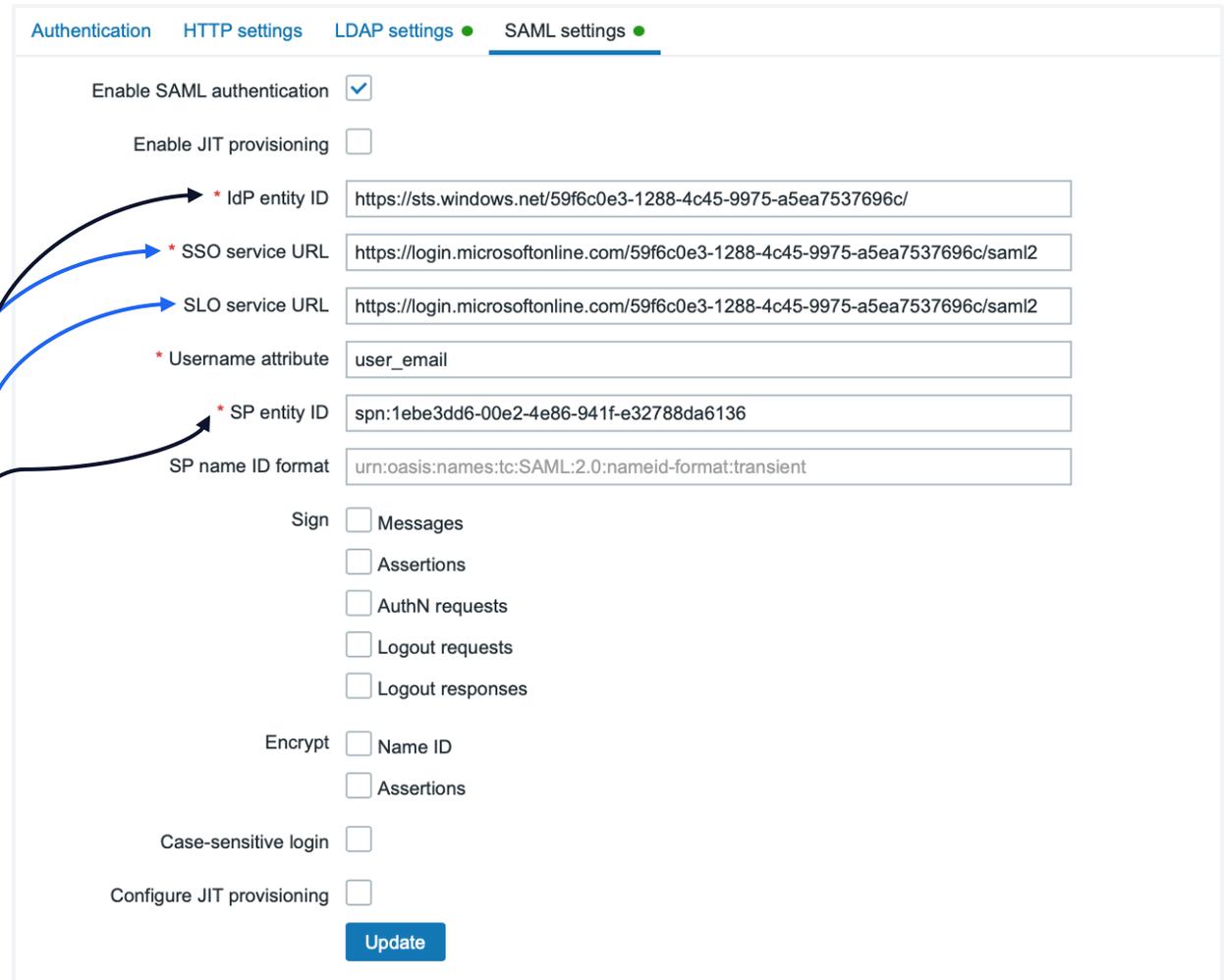
Name *

Homepage URL

Logo

User access URL

Application ID



Authentication HTTP settings LDAP settings SAML settings

Enable SAML authentication

Enable JIT provisioning

* IdP entity ID

* SSO service URL

SLO service URL

* Username attribute

* SP entity ID

SP name ID format

Sign Messages

Assertions

AuthN requests

Logout requests

Logout responses

Encrypt Name ID

Assertions

Case-sensitive login

Configure JIT provisioning

[Update](#)

SAML – Zabbix

- ▶ Download the certificate provided in the Okta SAML setup instructions into ui/conf/certs folder as idp.crt.
 - ▶ Upload already downloaded certificate on Zabbix frontend server (/usr/share/zabbix/conf/certs)
 - ▶ `mkdir /usr/share/zabbix/conf/certs/`
 - ▶ Copy your certificate
 - ▶ `chmod 644 /usr/share/zabbix/conf/certs/AZURE.cer`
- ▶ Change setting in frontend config file
 - ▶ `nano /etc/zabbix/web/zabbix.conf.php`

```
// Used for SAML authentication.  
// Uncomment to override the default paths to SP private key, SP and IdP X.509 certificates, and to set extra settings.  
//$SSO['SP_KEY']           = 'conf/certs/sp.key';  
//$SSO['SP_CERT']         = 'conf/certs/sp.crt';  
$SSO['IDP_CERT']         = 'conf/certs/AZURE.cer';  
//$SSO['SETTINGS']       = [];
```

- ▶ Create your user in Zabbix (tomas.hermanek@initmax.cz) and test SAML configuration

Zabbix User Provisioning JIT

SAML – Zabbix JIT

- › Zabbix SAML JIT provisioning
 - › Enable JIT provisioning
 - › Fill Group name attribute
 - › Fill User user name attribute
 - › Fill User last name attribute
 - › Create correct group mapping for groups
 - › Create correct setting for Media type mapping

Authentication HTTP settings LDAP settings **SAML settings**

Enable SAML authentication

Enable JIT provisioning

* IdP entity ID

* SSO service URL

SLO service URL

* Username attribute

* SP entity ID

SP name ID format

Sign Messages
 Assertions
 AuthN requests
 Logout requests
 Logout responses

Encrypt Name ID
 Assertions

Case-sensitive login

Configure JIT provisioning

* Group name attribute

User name attribute

User last name attribute

* User group mapping

SAML group pattern	User groups	User role	Action
Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	Remove

[Add](#)

Media type mapping ⓘ

Name	Media type	Attribute	Action
mail	Email (HTML)	user_email	Remove
mobile	SMS	user_mobile	Remove
pushover	Pushover	user_pushover	Remove

[Add](#)

Enable SCIM provisioning

[Update](#)

Zabbix User Provisioning JIT

SAML – Zabbix JIT

› Zabbix SAML JIT provisioning

- › Delete your manually created user or use SQL statement for user update where (update users set userdirectoryid =2 where userid=X;) userid is your user ID in Zabbix

Users

? [Create user](#)

Filter 

Username

Name

Last name

User roles [Select](#)

User groups [Select](#)

[Apply](#) [Reset](#)

<input type="checkbox"/>	Username ▲	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	Provisioned	Info
<input type="checkbox"/>	Admin	Zabbix	Administrator	Super admin role	INTERNAL	Yes (2023-04-05 00:57:27)	Ok	Internal	Enabled	Disabled	Enabled		
<input type="checkbox"/>	guest			Guest role	Disabled, Guests	No	Ok	Internal	Disabled	Disabled	Disabled		
<input checked="" type="checkbox"/>	tomas.hermanek@initmax.cz			Super admin role	LDAP	No (2023-04-05 00:57:16)	Ok	LDAP	Enabled	Disabled	Enabled		

1 selected

[Provision now](#) [Unblock](#) [Delete](#) **2**

Displaying 3 of 3 found

Zabbix User Provisioning JIT

SAML – Zabbix JIT

- › Zabbix SAML JIT provisioning
 - › Check your provisioned user

Users

? [Create user](#)

Filter 

Username

Name

Last name

User roles [Select](#)

User groups [Select](#)

[Apply](#) [Reset](#)

<input type="checkbox"/>	Username ▲	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	Provisioned	Info
<input type="checkbox"/>	Admin	Zabbix	Administrator	Super admin role	INTERNAL	No (2023-04-05 00:58:59)	Ok	Internal	Enabled	Disabled	Enabled		
<input type="checkbox"/>	guest			Guest role	Disabled, Guests	No	Ok	Internal	Disabled	Disabled	Disabled		
<input type="checkbox"/>	tomas.hermanek@initmax.cz	Tomáš	Heřmánek	Super admin role	Zabbix_Super_Admins	Yes (2023-04-05 00:59:40)	Ok	SAML	Enabled	Disabled	Enabled	2023-04-05 00:59	

Displaying 3 of 3 found

0 selected [Provision now](#) [Unblock](#) [Delete](#)

Zabbix User Provisioning JIT

SAML – Zabbix JIT

- › Zabbix SAML JIT provisioning
 - › Check your provisioned user

Users ?

 This user is IdP provisioned. Manual changes for provisioned fields are not allowed. ×

User **Media** 3 **Permissions**

* Username

Name

Last name

Groups ×

Password 

Language

Time zone

Theme

Auto-login

Auto-logout

* Refresh

* Rows per page

URL (after login)

Zabbix User Provisioning JIT

SAML – Zabbix JIT

- › Zabbix SAML JIT provisioning
 - › Check your provisioned user

Users ?

 This user is IdP provisioned. Manual changes for provisioned fields are not allowed. ×

[User](#) [Media 3](#) [Permissions](#)

Media	Type	Send to	When active	Use if severity	Status	Action
	Email (HTML)	tomas.hermanek@initmax.cz	1-7,00:00-24:00	N I W A H D	Enabled	Edit Remove
	Pushover	uc4hf8jx1262o3tc2v7qzooeibb1rt	1-7,00:00-24:00	N I W A H D	Enabled	Edit Remove
	SMS	+420 732 447 184	1-7,00:00-24:00	N I W A H D	Enabled	Edit Remove
	Add					

[Update](#) [Delete](#) [Cancel](#)

SAML – Notes

- ▶ You need to use certificates for your webserver/vhost (you can also use self signed certificates)
- ▶ In order to use proxy, you need to define SSO configuration in your zabbix.conf.php
 - ▶ `$SSO['SETTINGS'] = ['use_proxy_headers' => true];`

5

SCIM



Zabbix User Provisioning JIT

SCIM – Zabbix

- › Zabbix SCIM provisioning
 - › Enable SCIM provisioning

Authentication HTTP settings LDAP settings **SAML settings**

Enable SAML authentication

Enable JIT provisioning

* IdP entity ID

* SSO service URL

SLO service URL

* Username attribute

* SP entity ID

SP name ID format

Sign Messages
 Assertions
 AuthN requests
 Logout requests
 Logout responses

Encrypt Name ID
 Assertions

Case-sensitive login

Configure JIT provisioning

* Group name attribute

User name attribute

User last name attribute

* User group mapping

SAML group pattern	User groups	User role	Action
Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	Remove

[Add](#)

Media type mapping ⓘ

Name	Media type	Attribute	Action
mail	Email (HTML)	user_email	Remove
mobile	SMS	user_mobile	Remove
pushover	Pushover	user_pushover	Remove

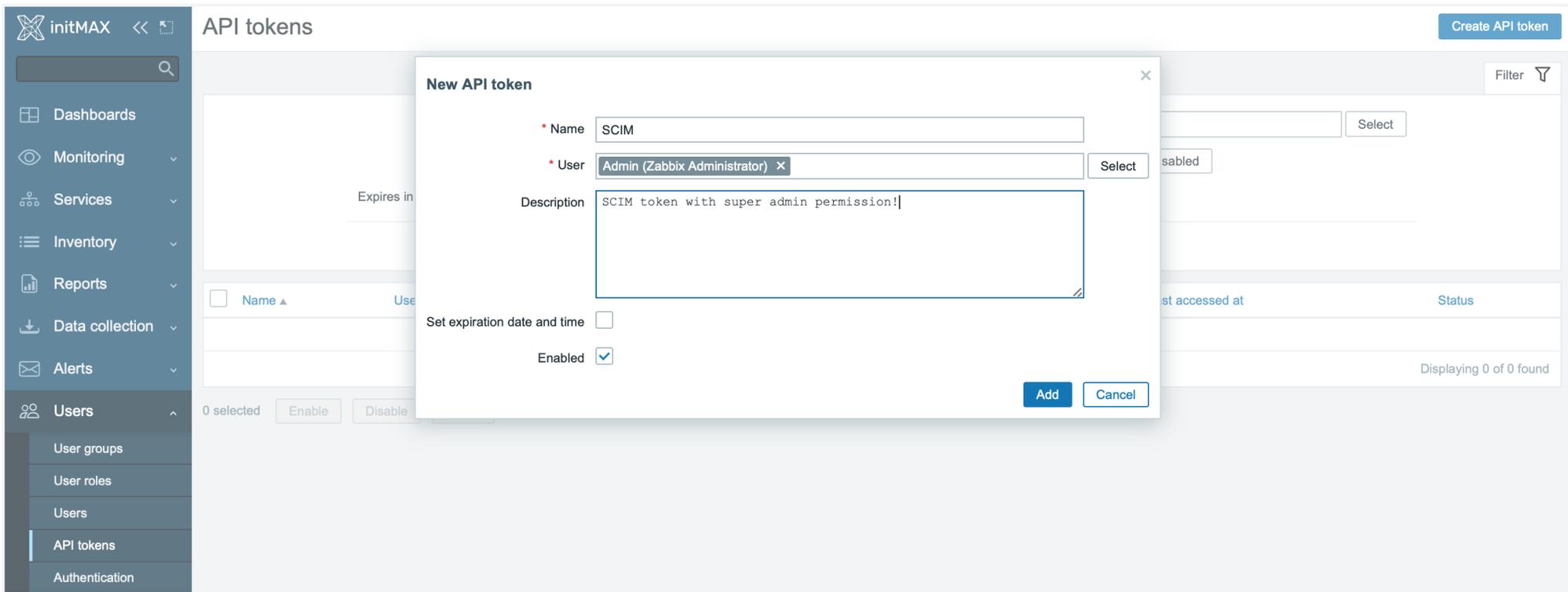
[Add](#)

Enable SCIM provisioning

[Update](#)

SCIM – Zabbix

- ▶ Zabbix SCIM provisioning
 - ▶ Create new API Token with super admin permissions



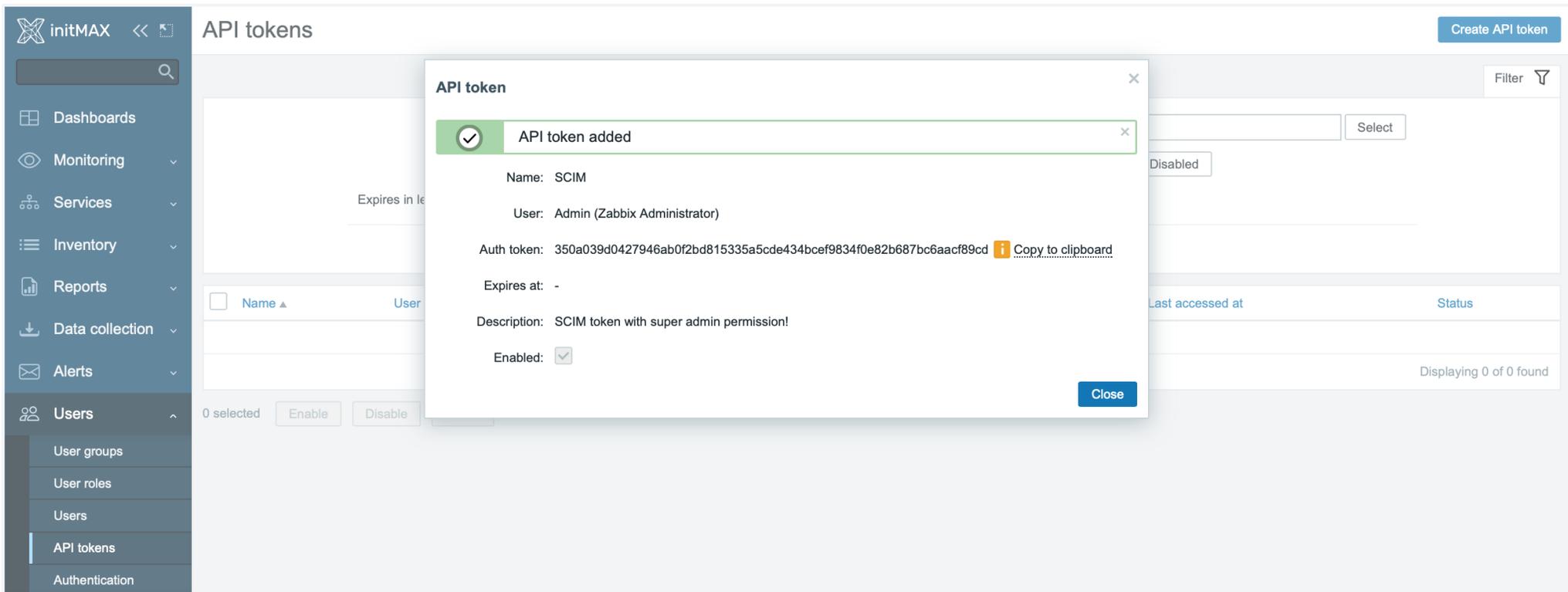
The screenshot displays the Zabbix web interface for managing API tokens. A modal dialog titled "New API token" is open, allowing the creation of a new token. The dialog contains the following fields and options:

- Name:** A text input field containing "SCIM".
- User:** A dropdown menu showing "Admin (Zabbix Administrator)" with a "Select" button to the right.
- Description:** A text area containing "SCIM token with super admin permission!".
- Set expiration date and time:** An unchecked checkbox.
- Enabled:** A checked checkbox.

At the bottom of the dialog are "Add" and "Cancel" buttons. The background interface shows the "API tokens" management page with a sidebar on the left containing navigation options like Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, Users, User groups, User roles, and Authentication. The main content area is currently empty, displaying "0 selected" and "Displaying 0 of 0 found".

SCIM – Zabbix

- ▶ Zabbix SCIM provisioning
 - ▶ Create new API Token with super admin permissions (don't forget to save this token)



The screenshot displays the Zabbix web interface for managing API tokens. A modal dialog titled "API token" is open, showing a success message: "API token added". The dialog details the following information:

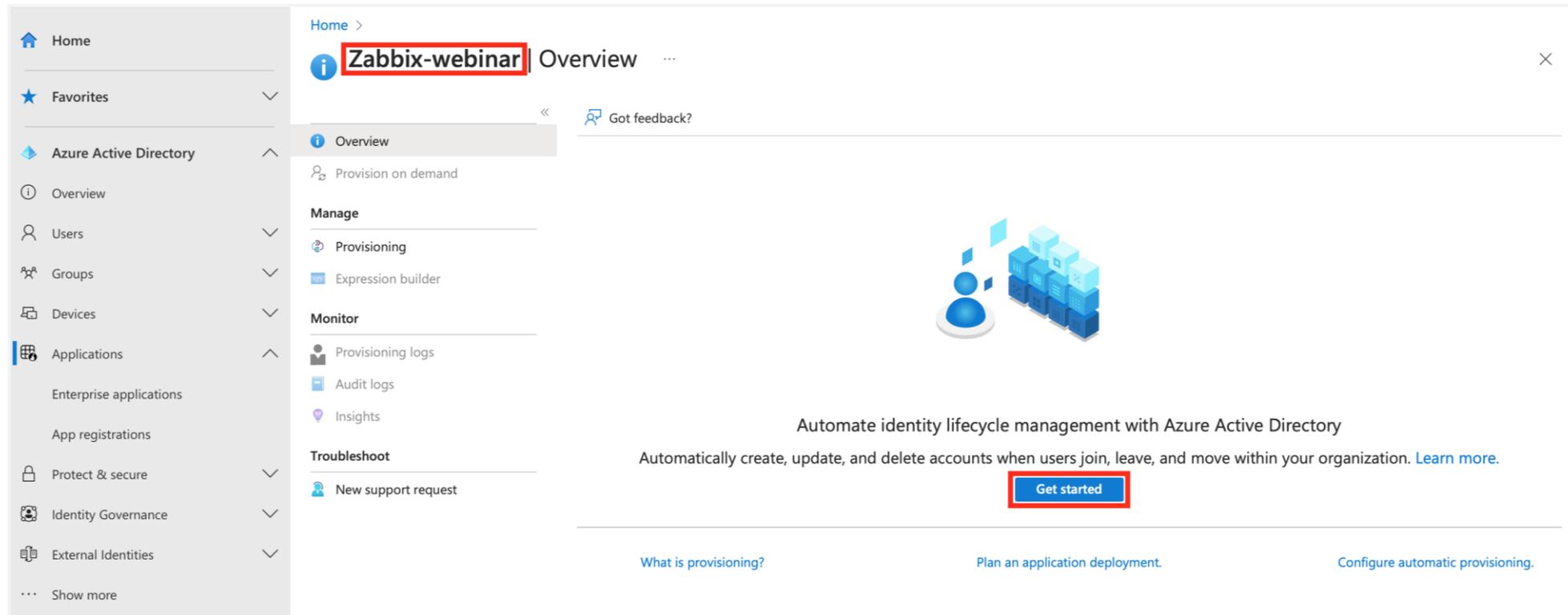
- Name: SCIM
- User: Admin (Zabbix Administrator)
- Auth token: 350a039d0427946ab0f2bd815335a5cde434bcef9834f0e82b687bc6aacf89cd (with a "Copy to clipboard" button)
- Expires at: -
- Description: SCIM token with super admin permission!
- Enabled:

The background interface shows the "API tokens" management page with a sidebar menu on the left containing options like Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, and Users. The "Users" menu is expanded, showing sub-items: User groups, User roles, Users, API tokens, and Authentication. The main content area is currently empty, displaying "0 selected" and "Enable" / "Disable" buttons. A "Create API token" button is visible in the top right corner of the page.

Zabbix User Provisioning JIT

SCIM – Azure

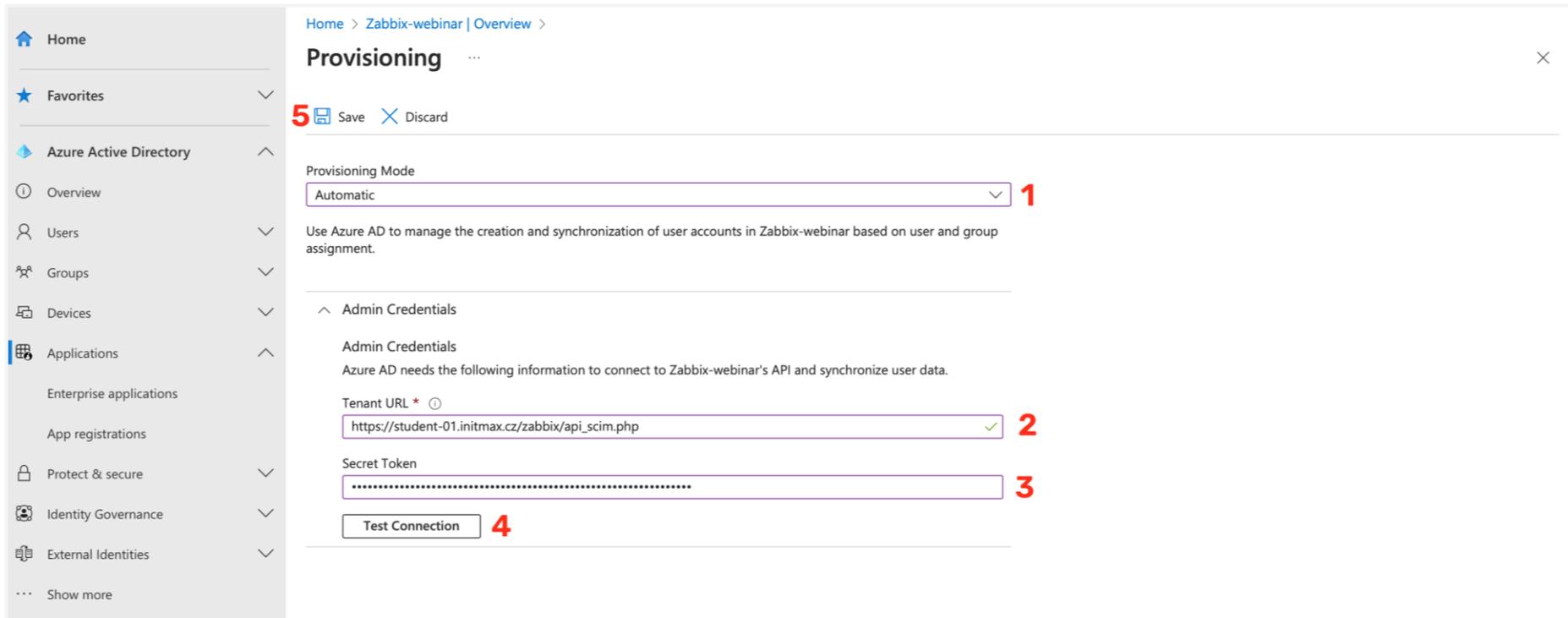
- › Zabbix SCIM provisioning
 - › In Azure application go to section Provisioning and hit button “Get started”



The screenshot shows the Azure Active Directory Provisioning Overview page. The left sidebar contains navigation options: Home, Favorites, Azure Active Directory, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Protect & secure, Identity Governance, External Identities, and Show more. The main content area is titled "Zabbix-webinar | Overview" and includes a "Got feedback?" link. The "Overview" section is expanded, showing "Provision on demand" and a "Manage" section with "Provisioning" and "Expression builder". The "Monitor" section includes "Provisioning logs", "Audit logs", and "Insights". The "Troubleshoot" section has a "New support request" link. The main content area features a 3D graphic of a person and blocks, with the text: "Automate identity lifecycle management with Azure Active Directory. Automatically create, update, and delete accounts when users join, leave, and move within your organization. [Learn more.](#)" A "Get started" button is highlighted in a red box. At the bottom, there are three links: "What is provisioning?", "Plan an application deployment.", and "Configure automatic provisioning."

SCIM – Azure

- › Zabbix SCIM provisioning
 - › Select Automatic Provisioning
 - › Tenant URL - https://student-01.initmax.cz/zabbix/api_scim.php
 - › Fill Secret Token, test connection and save



Home > Zabbix-webinar | Overview >

Provisioning

5 Save Discard

Provisioning Mode
Automatic **1**

Use Azure AD to manage the creation and synchronization of user accounts in Zabbix-webinar based on user and group assignment.

Admin Credentials

Admin Credentials
Azure AD needs the following information to connect to Zabbix-webinar's API and synchronize user data.

Tenant URL * **2**

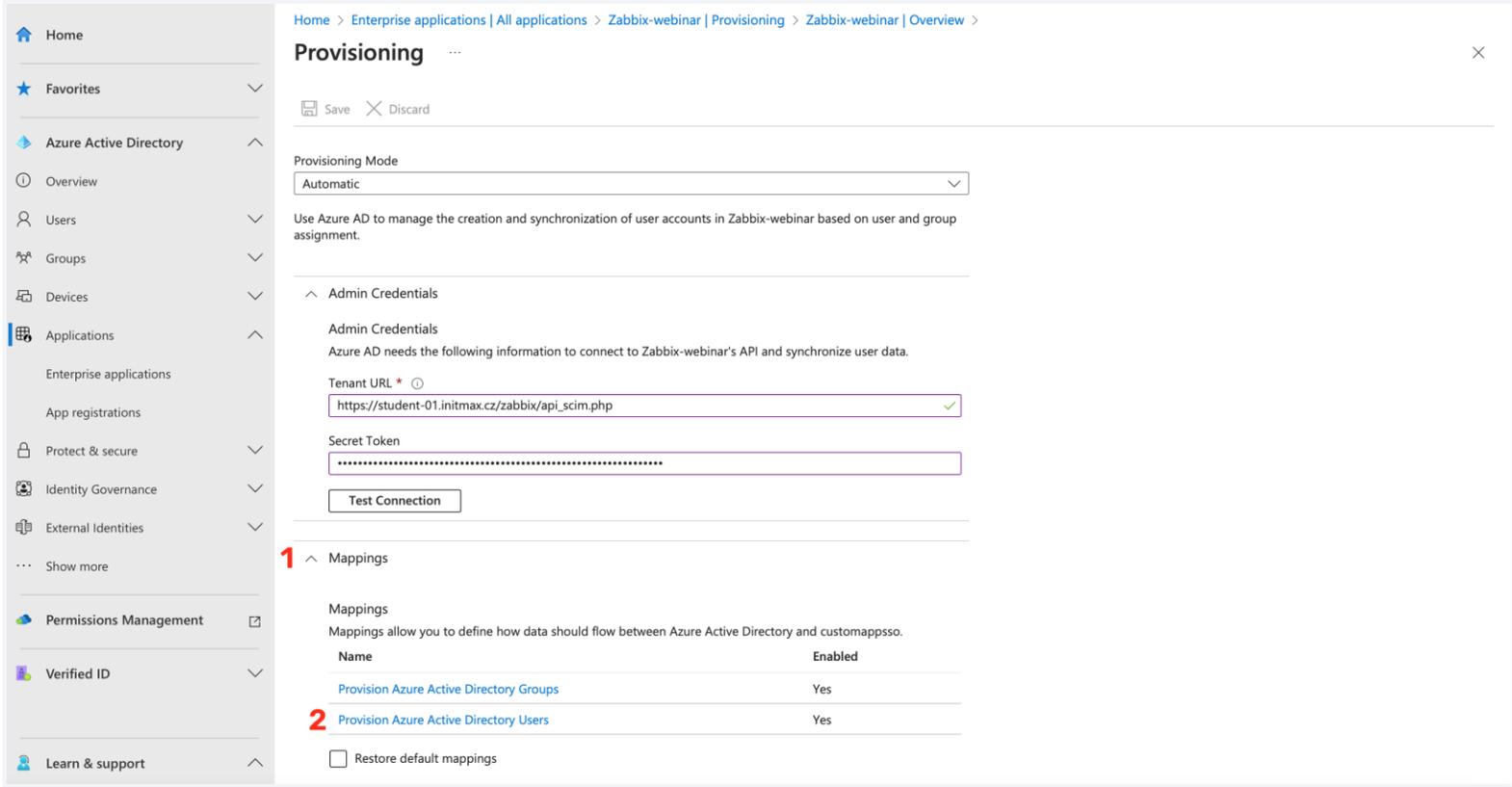
Secret Token **3**

4 Test Connection

Zabbix User Provisioning JIT

SCIM – Azure

- ▶ Zabbix SCIM provisioning
 - ▶ We need to update user mapping



The screenshot shows the Azure Active Directory Provisioning configuration page for the application 'Zabbix-webinar'. The left sidebar contains navigation options like Home, Favorites, Azure Active Directory, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Protect & secure, Identity Governance, External Identities, Permissions Management, Verified ID, and Learn & support.

The main content area is titled 'Provisioning' and includes a breadcrumb trail: Home > Enterprise applications | All applications > Zabbix-webinar | Provisioning > Zabbix-webinar | Overview >. Below the title are 'Save' and 'Discard' buttons.

The 'Provisioning Mode' is set to 'Automatic'. A description states: 'Use Azure AD to manage the creation and synchronization of user accounts in Zabbix-webinar based on user and group assignment.'

The 'Admin Credentials' section is expanded, showing 'Admin Credentials' and a note: 'Azure AD needs the following information to connect to Zabbix-webinar's API and synchronize user data.' The 'Tenant URL' is 'https://student-01.initmax.cz/zabbix/api_scim.php' and the 'Secret Token' is masked with dots. A 'Test Connection' button is present.

The 'Mappings' section is expanded and marked with a red '1'. It contains a table of mappings:

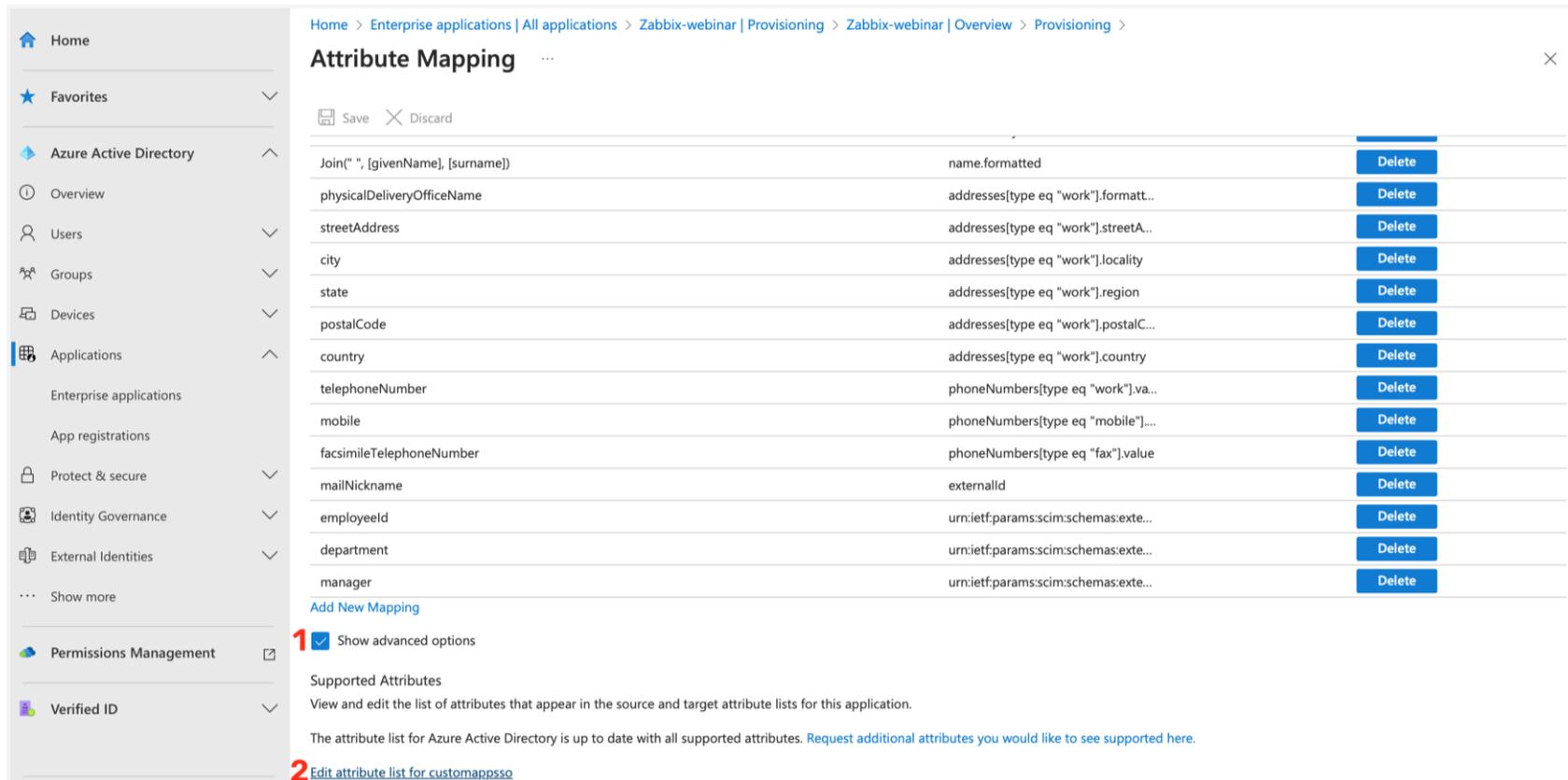
Name	Enabled
Provision Azure Active Directory Groups	Yes
Provision Azure Active Directory Users	Yes

Below the table, there is a checkbox labeled 'Restore default mappings' with a red '2' next to it.

Zabbix User Provisioning JIT

SCIM – Azure

- › Zabbix SCIM provisioning
 - › We need to expand advanced options and edit attribute list



The screenshot shows the Zabbix SCIM provisioning interface. On the left is a navigation sidebar with categories like Home, Favorites, Azure Active Directory, Overview, Users, Groups, Devices, Applications, Permissions Management, and Verified ID. The main content area is titled "Attribute Mapping" and shows a table of mappings between source and target attributes. Below the table, there are options to "Add New Mapping" and "Show advanced options".

Home > Enterprise applications | All applications > Zabbix-webinar | Provisioning > Zabbix-webinar | Overview > Provisioning >

Attribute Mapping

Save Discard

Join(" ", [givenName], [surname])	name.formatted	Delete
physicalDeliveryOfficeName	addresses[type eq "work"].formatt...	Delete
streetAddress	addresses[type eq "work"].streetA...	Delete
city	addresses[type eq "work"].locality	Delete
state	addresses[type eq "work"].region	Delete
postalCode	addresses[type eq "work"].postalC...	Delete
country	addresses[type eq "work"].country	Delete
telephoneNumber	phoneNumbers[type eq "work"].va...	Delete
mobile	phoneNumbers[type eq "mobile"]...	Delete
facsimileTelephoneNumber	phoneNumbers[type eq "fax"].value	Delete
mailNickname	externalId	Delete
employeeId	urn:ietf:params:scim:schemas:exte...	Delete
department	urn:ietf:params:scim:schemas:exte...	Delete
manager	urn:ietf:params:scim:schemas:exte...	Delete

[Add New Mapping](#)

1 Show advanced options

Supported Attributes
View and edit the list of attributes that appear in the source and target attribute lists for this application.

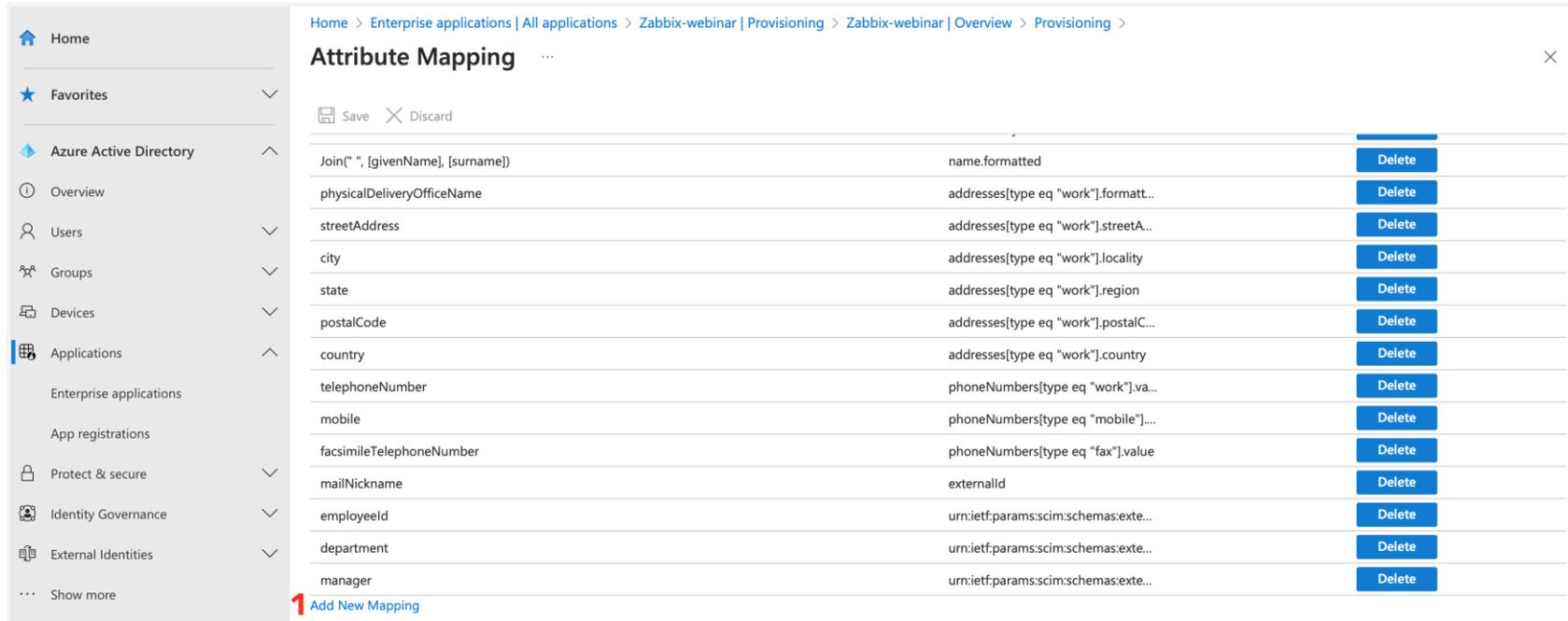
The attribute list for Azure Active Directory is up to date with all supported attributes. [Request additional attributes you would like to see supported here.](#)

2 [Edit attribute list for customappsso](#)

Zabbix User Provisioning JIT

SCIM – Azure

- ▶ Zabbix SCIM provisioning
 - ▶ Here we need to add our custom attributes



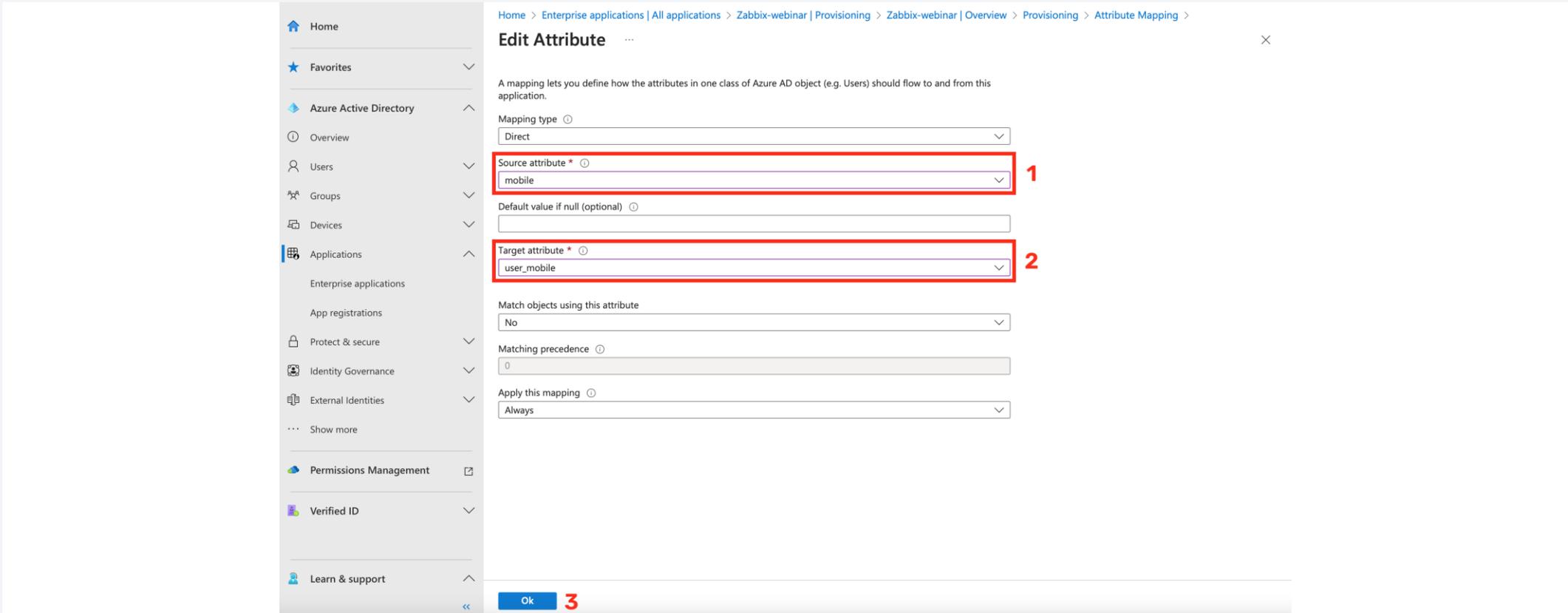
Zabbix Attribute	Azure AD Attribute	Action
Join(" ", [givenName], [surname])	name.formatted	Delete
physicalDeliveryOfficeName	addresses[type eq "work"].formatt...	Delete
streetAddress	addresses[type eq "work"].streetA...	Delete
city	addresses[type eq "work"].locality	Delete
state	addresses[type eq "work"].region	Delete
postalCode	addresses[type eq "work"].postalC...	Delete
country	addresses[type eq "work"].country	Delete
telephoneNumber	phoneNumbers[type eq "work"].va...	Delete
mobile	phoneNumbers[type eq "mobile"]...	Delete
facsimileTelephoneNumber	phoneNumbers[type eq "fax"].value	Delete
mailNickname	externalId	Delete
employeeId	urn:ietf:params:scim:schemas:exte...	Delete
department	urn:ietf:params:scim:schemas:exte...	Delete
manager	urn:ietf:params:scim:schemas:exte...	Delete

1 [Add New Mapping](#)

Zabbix User Provisioning JIT

SCIM – Azure

- ▶ Zabbix SCIM provisioning
 - ▶ Add our custom attributes (user_email, user_mobile, user_name, user_lastname, user_pushover)



Home > Enterprise applications | All applications > Zabbix-webinar | Provisioning > Zabbix-webinar | Overview > Provisioning > Attribute Mapping >

Edit Attribute

A mapping lets you define how the attributes in one class of Azure AD object (e.g. Users) should flow to and from this application.

Mapping type

Source attribute * 1

Default value if null (optional)

Target attribute * 2

Match objects using this attribute

Matching precedence

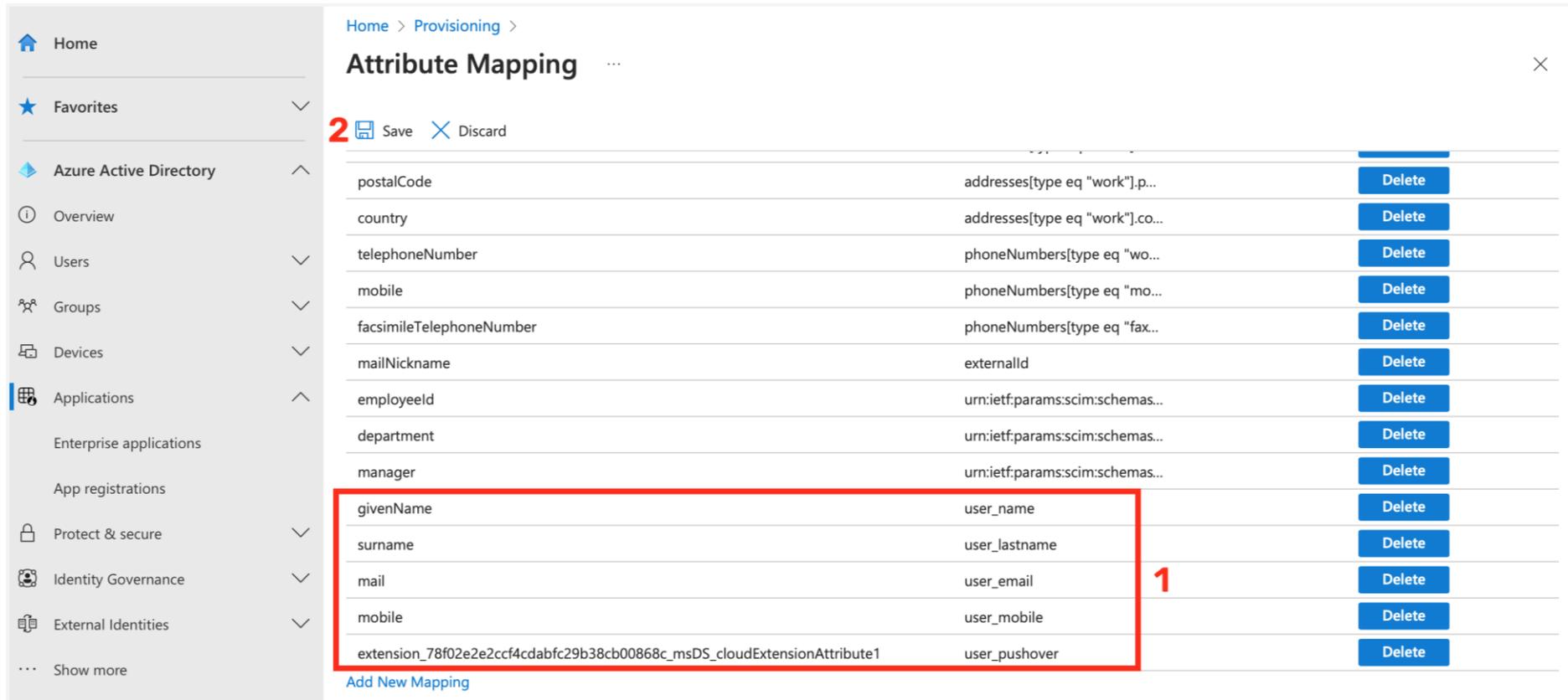
Apply this mapping

Ok 3

SCIM – Azure

› Zabbix SCIM provisioning

- › Add our custom attributes (user_email, user_mobile, user_name, user_lastname, user_pushover) and save



Home > Provisioning > Attribute Mapping

2 Save Discard

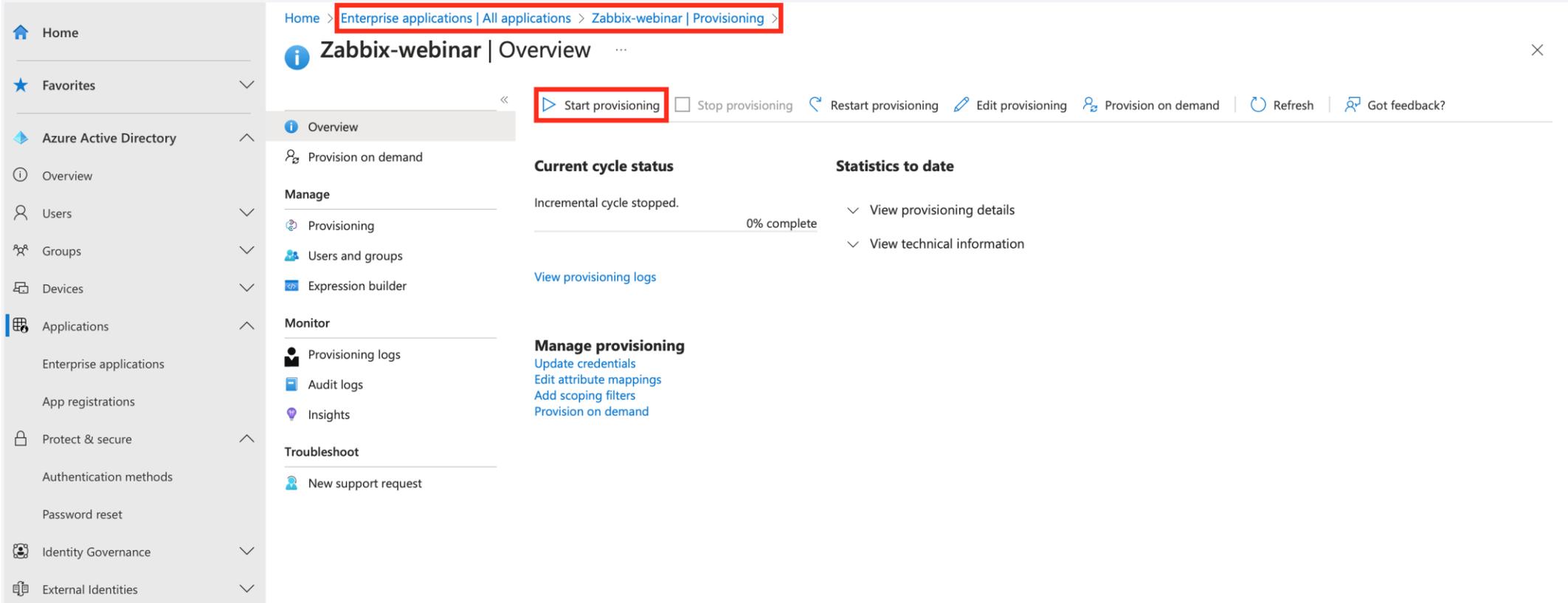
postalCode	addresses[type eq "work"].p...	Delete
country	addresses[type eq "work"].co...	Delete
telephoneNumber	phoneNumbers[type eq "wo...	Delete
mobile	phoneNumbers[type eq "mo...	Delete
facsimileTelephoneNumber	phoneNumbers[type eq "fax...	Delete
mailNickname	externalId	Delete
employeeId	urn:ietf:params:scim:schemas...	Delete
department	urn:ietf:params:scim:schemas...	Delete
manager	urn:ietf:params:scim:schemas...	Delete
givenName	user_name	Delete
surname	user_lastname	Delete
mail	user_email	Delete
mobile	user_mobile	Delete
extension_78f02e2e2ccf4cdabfc29b38cb00868c_msDS_cloudExtensionAttribute1	user_pushover	Delete

Add New Mapping

Zabbix User Provisioning JIT

SCIM – Azure

- › Zabbix SCIM provisioning
 - › Start your provisioning and wait about 1 hour



Home > Enterprise applications | All applications > Zabbix-webinar | Provisioning >

Zabbix-webinar | Overview

[Start provisioning](#) Stop provisioning [Restart provisioning](#) [Edit provisioning](#) [Provision on demand](#) [Refresh](#) [Got feedback?](#)

Overview

- Provision on demand
- Manage**
 - Provisioning
 - Users and groups
 - Expression builder
- Monitor**
 - Provisioning logs
 - Audit logs
 - Insights
- Troubleshoot**
 - New support request

Current cycle status

Incremental cycle stopped. 0% complete

[View provisioning logs](#)

Statistics to date

- [View provisioning details](#)
- [View technical information](#)

Manage provisioning

- [Update credentials](#)
- [Edit attribute mappings](#)
- [Add scoping filters](#)
- [Provision on demand](#)

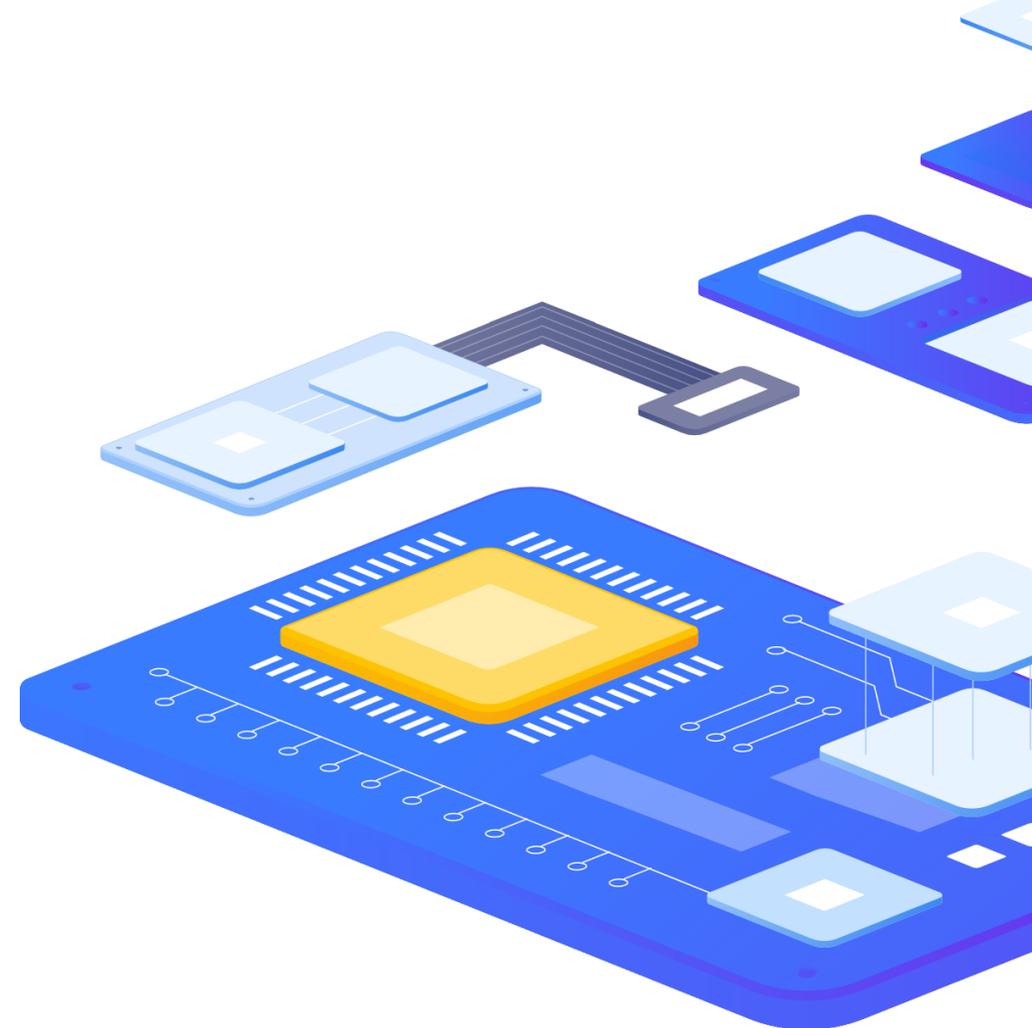
6

Issues and limitations



Issues and limitations

- › Manually created user cannot be provisioned (workaround is use alter table for this specific user)
- › You are not be able to change some user setting after provisioning (media, role, groups)
- › Zabbix have bug with user groups – user groups can be assigned via user groups
- › SCIM have a lot of issues
- › Zabbix have public Security Advisories https://www.zabbix.com/security_advisories



7

DEMO





Questions?



CONTACT US:

Phone:



+420 800 244 442

Web:



<https://www.initmax.cz>

Email:



tomas.hermanek@initmax.cz

LinkedIn:



<https://www.linkedin.com/company/initmax>

Twitter:



<https://twitter.com/initmax>

Tomáš Heřmánek:



+420 732 447 184