



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

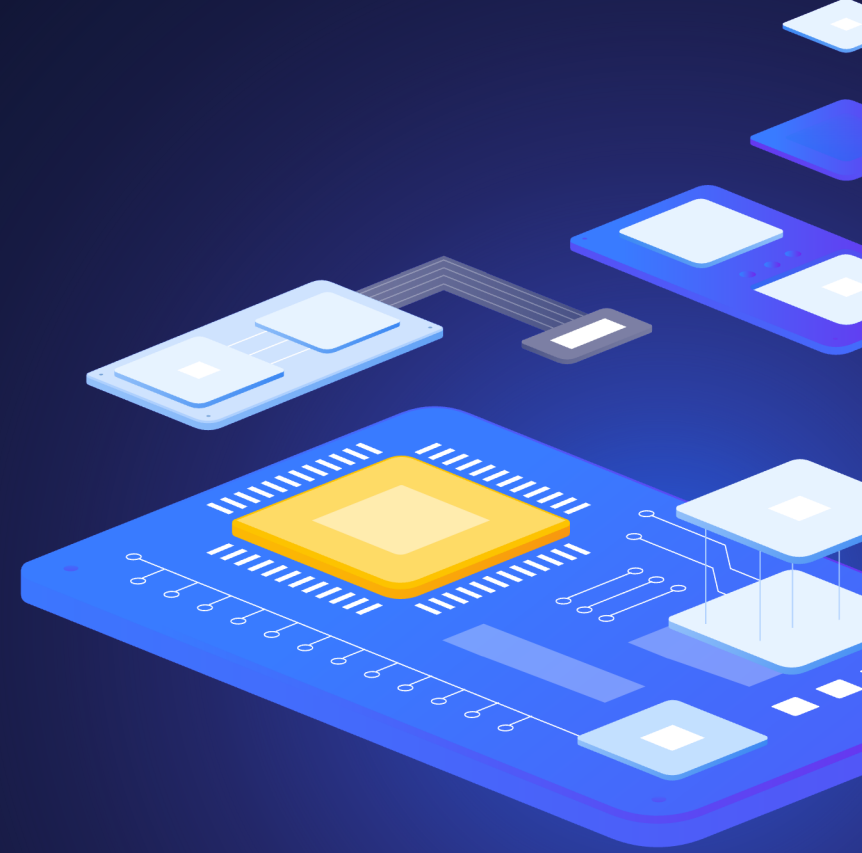
What is JIT (Just In Time)

# 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

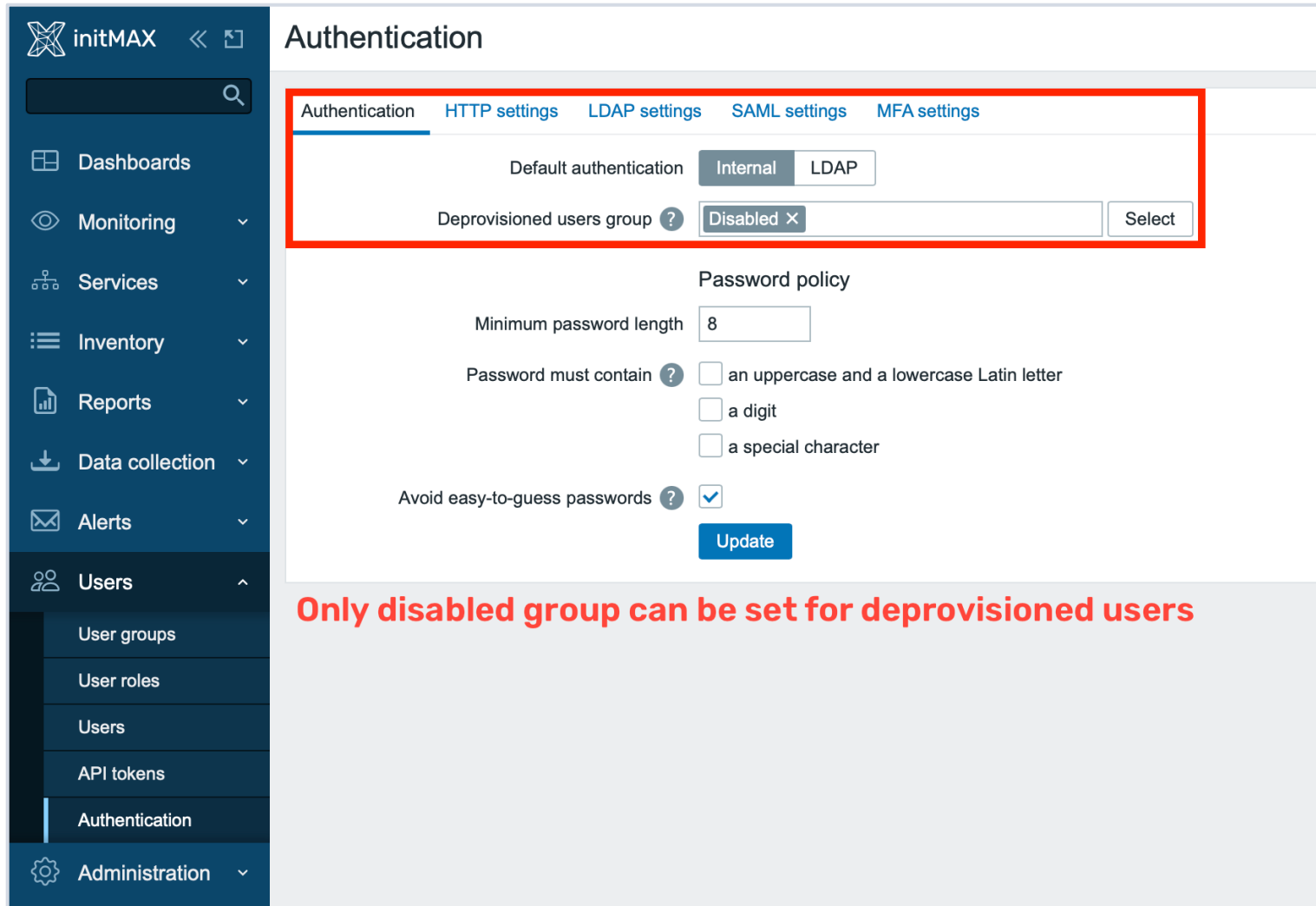




# Available authentication options in ZABBIX

- › 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
- › **Multi-Factor Authentication (MFA)**

# Available authentication options in ZABBIX



The screenshot shows the Zabbix web interface for the Authentication settings page. The left sidebar contains navigation options: Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, Users, and Administration. The main content area is titled 'Authentication' and has tabs for Authentication, HTTP settings, LDAP settings, SAML settings, and MFA settings. The 'Authentication' tab is active. Below the tabs, there are two main sections: 'Default authentication' and 'Password policy'. The 'Default authentication' section has a dropdown menu with 'Internal' selected and 'LDAP' as an alternative. Below this is a 'Deprovisioned users group' dropdown menu with 'Disabled' selected and a 'Select' button. The 'Password policy' section includes a 'Minimum password length' field set to '8', three checkboxes for password requirements (uppercase and lowercase Latin letter, a digit, and a special character), and a checked checkbox for 'Avoid easy-to-guess passwords'. An 'Update' button is located at the bottom of the password policy section. A red box highlights the 'Default authentication' and 'Deprovisioned users group' sections. A red text overlay at the bottom of the screenshot states: 'Only disabled group can be set for deprovisioned users'.

initMAX Authentication

Authentication HTTP settings LDAP settings SAML settings MFA settings

Default authentication Internal LDAP

Deprovisioned users group Disabled Select

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

**Only disabled group can be set for deprovisioned users**

3

LDAP



## Zabbix User Provisioning JIT

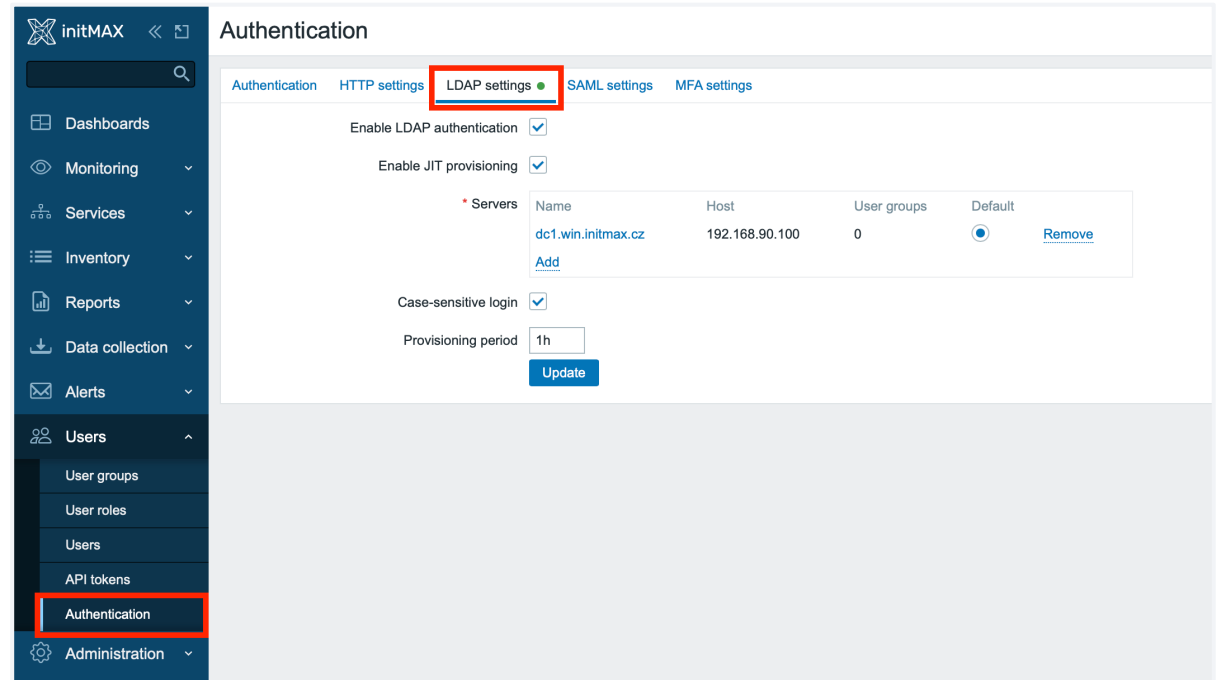
# LDAP

- ▶ 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	
dct1.win.initmax.cz	192.168.90.100	0	<input checked="" type="radio"/>	<a href="#">Remove</a>

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

The left sidebar shows the navigation menu with 'Authentication' highlighted in a red box.

# 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	<a href="#">Remove</a>
<a href="#">Add</a>			

Media type mapping

Name	Media type	Attribute	Action
Email	Email (HTML)	mail	<a href="#">Remove</a>
Pushover	Pushover	msDS-cloudExtensionAttribute1	<a href="#">Remove</a>
Mobile	SMS	mobile	<a href="#">Remove</a>
<a href="#">Add</a>			

Advanced configuration

## Zabbix User Provisioning JIT

# 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	<a href="#">Remove</a>
<a href="#">Add</a>			

Media type mapping

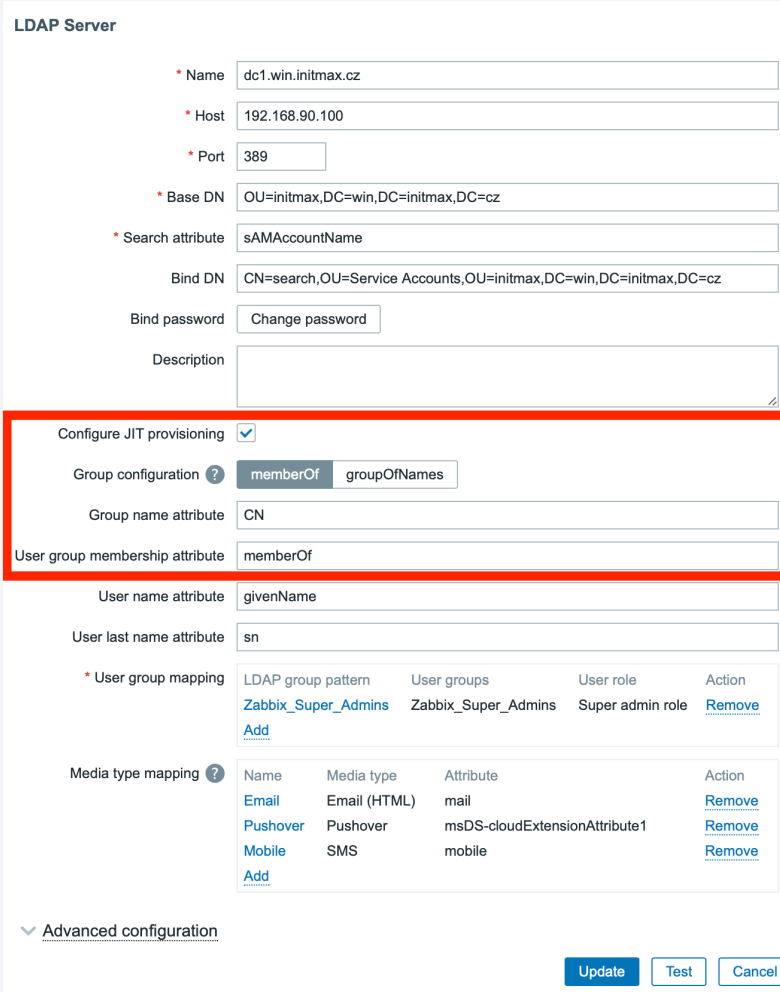
Name	Media type	Attribute	Action
Email	Email (HTML)	mail	<a href="#">Remove</a>
Pushover	Pushover	msDS-cloudExtensionAttribute1	<a href="#">Remove</a>
Mobile	SMS	mobile	<a href="#">Remove</a>
<a href="#">Add</a>			

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: dc1.win.initmax.cz  
\* Host: 192.168.90.100  
\* Port: 389  
\* Base DN: OU=initmax,DC=win,DC=initmax,DC=cz  
\* Search attribute: sAMAccountName  
Bind DN: CN=search,OU=Service Accounts,OU=initmax,DC=win,DC=initmax,DC=cz  
Bind password: Change password  
Description:

Configure JIT provisioning

Group configuration: **memberOf** groupOfNames

Group name attribute: CN

User group membership attribute: memberOf

User name attribute: givenName  
User last name attribute: sn

\* User group mapping

LDAP group pattern	User groups	User role	Action
Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	<a href="#">Remove</a>
<a href="#">Add</a>			

Media type mapping

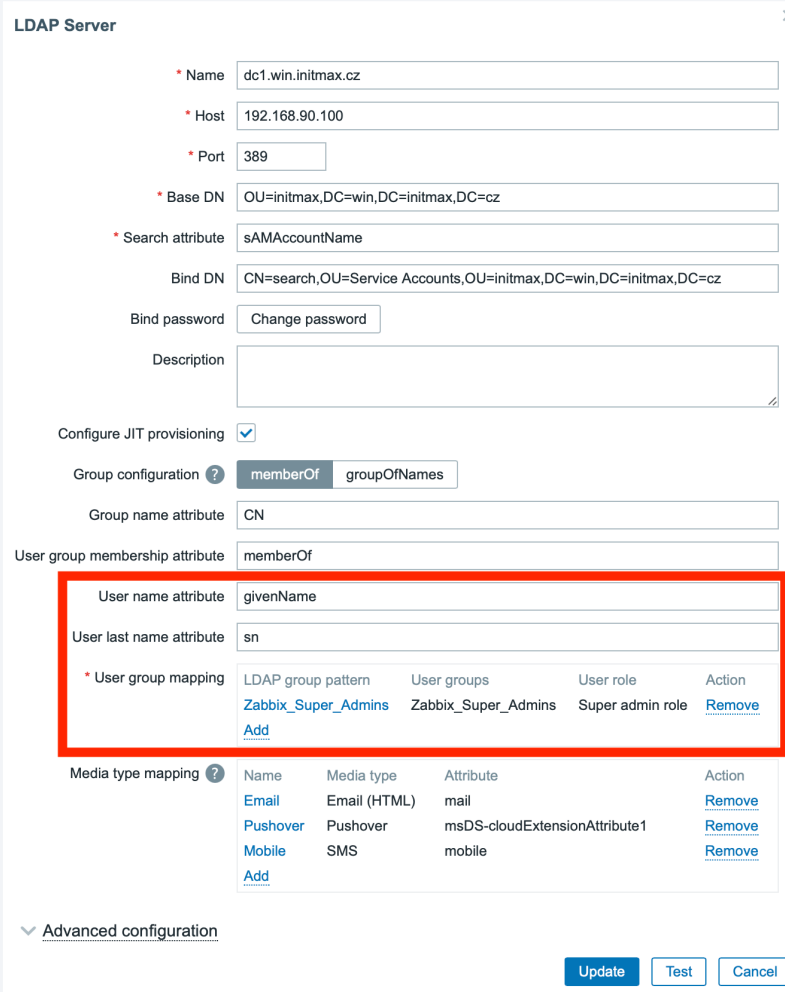
Name	Media type	Attribute	Action
Email	Email (HTML)	mail	<a href="#">Remove</a>
Pushover	Pushover	msDS-cloudExtensionAttribute1	<a href="#">Remove</a>
Mobile	SMS	mobile	<a href="#">Remove</a>
<a href="#">Add</a>			

Advanced configuration

Update Test Cancel

# 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: dc1.win.initmax.cz

\* Host: 192.168.90.100

\* Port: 389

\* Base DN: OU=initmax,DC=win,DC=initmax,DC=cz

\* Search attribute: sAMAccountName

Bind DN: CN=search,OU=Service Accounts,OU=initmax,DC=win,DC=initmax,DC=cz

Bind password: Change password

Description:

Configure JIT provisioning:

Group configuration: memberOf groupOfNames

Group name attribute: CN

User group membership attribute: memberOf

User name attribute: givenName

User last name attribute: sn

\* User group mapping

LDAP group pattern	User groups	User role	Action
Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	<a href="#">Remove</a> <a href="#">Add</a>

Media type mapping

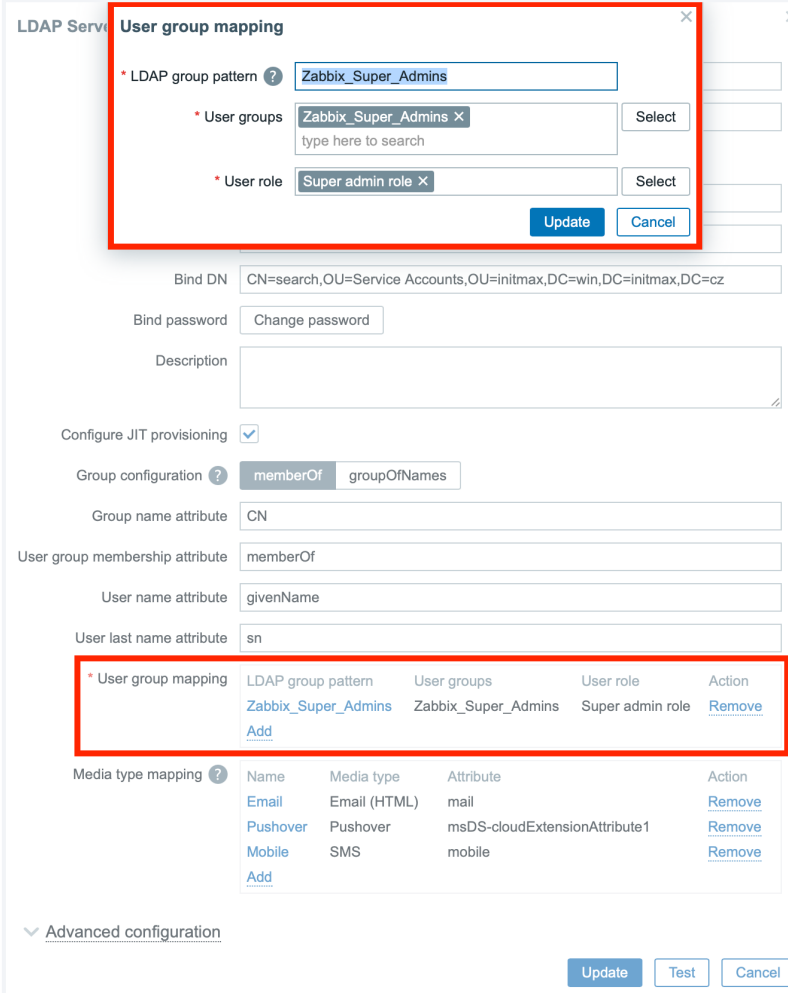
Name	Media type	Attribute	Action
Email	Email (HTML)	mail	<a href="#">Remove</a>
Pushover	Pushover	msDS-cloudExtensionAttribute1	<a href="#">Remove</a>
Mobile	SMS	mobile	<a href="#">Remove</a>

Advanced configuration

Update Test Cancel

# 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 displays the 'LDAP Service' configuration window, specifically the 'User group mapping' section. This section is highlighted with a red border and contains the following fields:

- \* LDAP group pattern**: Zabbix\_Super\_Admins
- \* User groups**: Zabbix\_Super\_Admins (with a 'Select' button and a search input 'type here to search')
- \* User role**: Super admin role (with a 'Select' button)

Below these fields are buttons for 'Update' and 'Cancel'. The rest of the configuration window includes:

- 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

At the bottom, there is a table for 'User group mapping' (highlighted with a red border) and a table for 'Media type mapping'.

* User group mapping	LDAP group pattern	User groups	User role	Action
	Zabbix_Super_Admins	Zabbix_Super_Admins	Super admin role	<a href="#">Remove</a>
	<a href="#">Add</a>			

Media type mapping	Name	Media type	Attribute	Action
	Email	Email (HTML)	mail	<a href="#">Remove</a>
	Pushover	Pushover	msDS-cloudExtensionAttribute1	<a href="#">Remove</a>
	Mobile	SMS	mobile	<a href="#">Remove</a>
	<a href="#">Add</a>			

At the bottom of the window, there is an 'Advanced configuration' section and buttons for 'Update', 'Test', and 'Cancel'.

# 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	<a href="#">Remove</a>
<a href="#">Add</a>			

Media type mapping

Name	Media type	Attribute	Action
Email	Email (HTML)	mail	<a href="#">Remove</a>
Pushover	Pushover	msDS-cloudExtensionAttribute1	<a href="#">Remove</a>
Mobile	SMS	mobile	<a href="#">Remove</a>
<a href="#">Add</a>			

Advanced configuration

# LDAP – Notes

- ▶ The Test button allows to test user access

### Test authentication ✕

✓ Login successful

\* Login

\* User password

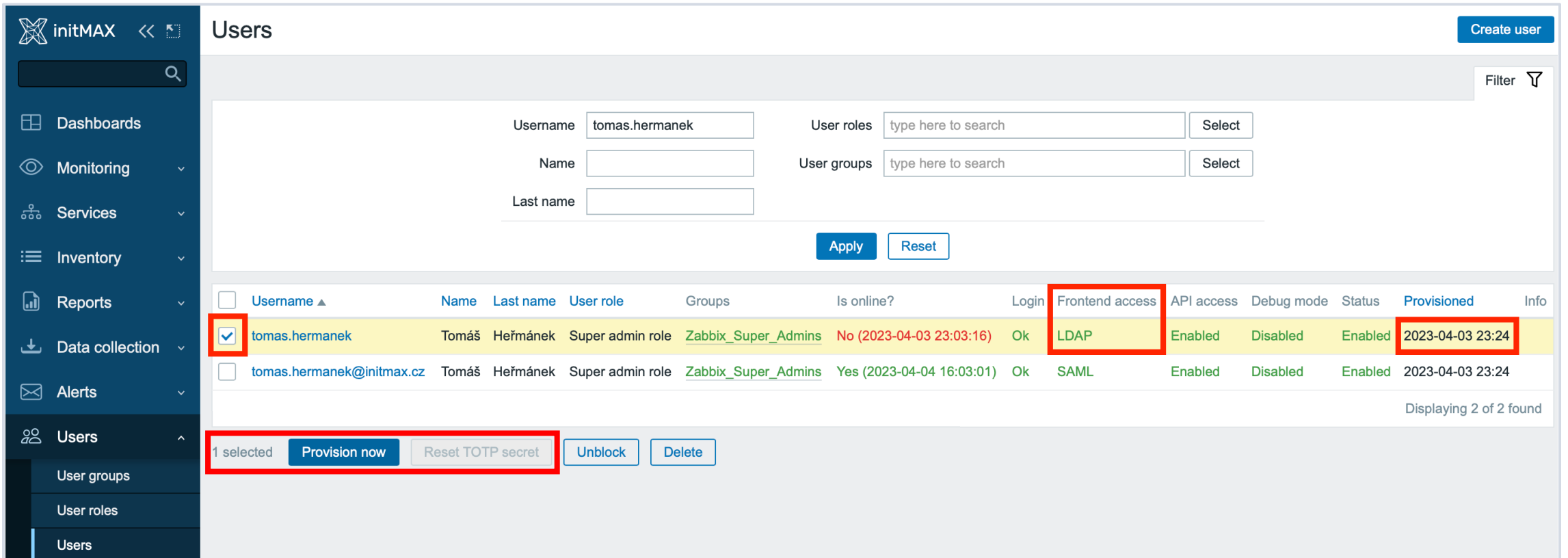
User role

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)



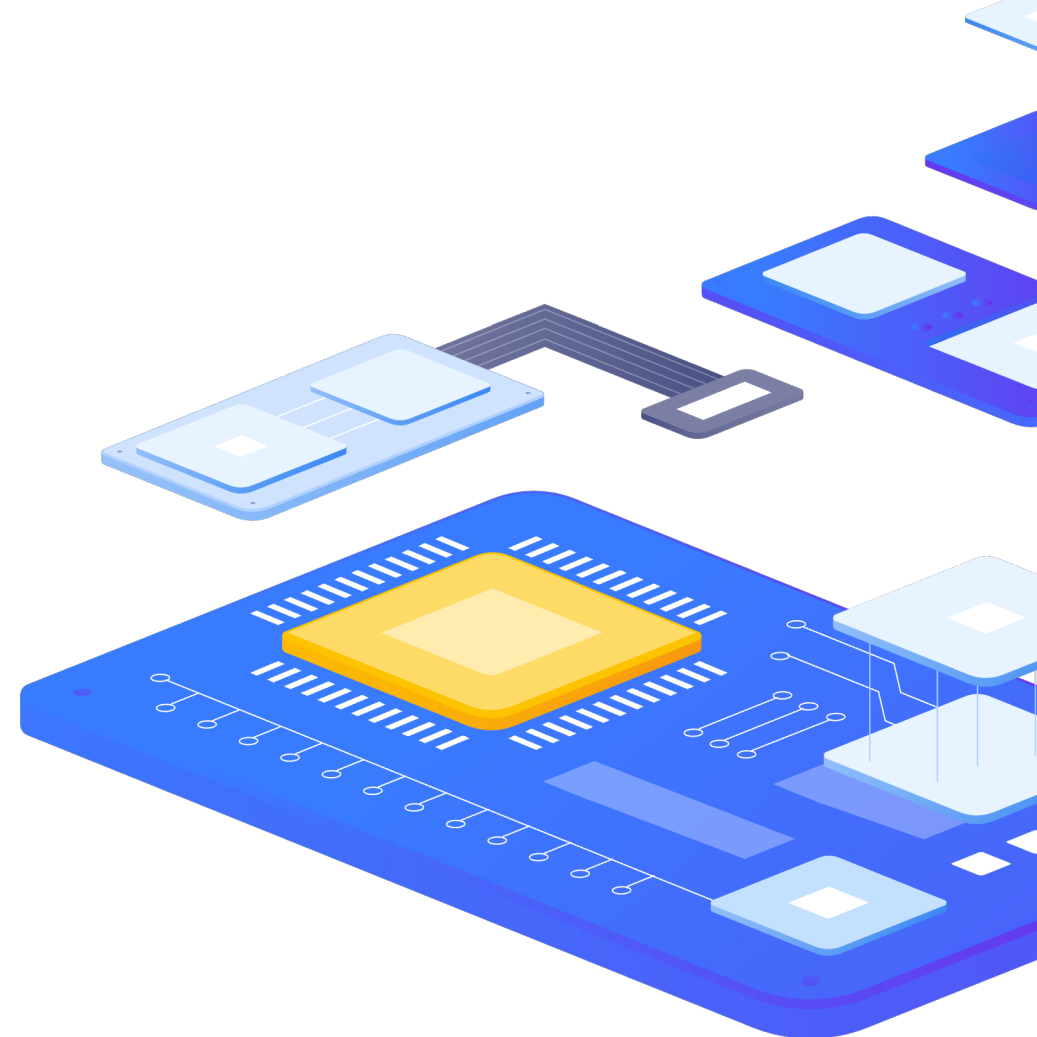
The screenshot shows the Zabbix Users management interface. The left sidebar contains navigation options: Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, and Users. The main content area is titled "Users" and includes a search bar, a "Create user" button, and a filter icon. Below the search bar 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 red box highlights the "1 selected" status and the "Provision now" button. The "Frontend access" column for the first user is also highlighted with a red box.

# LDAP – Notes

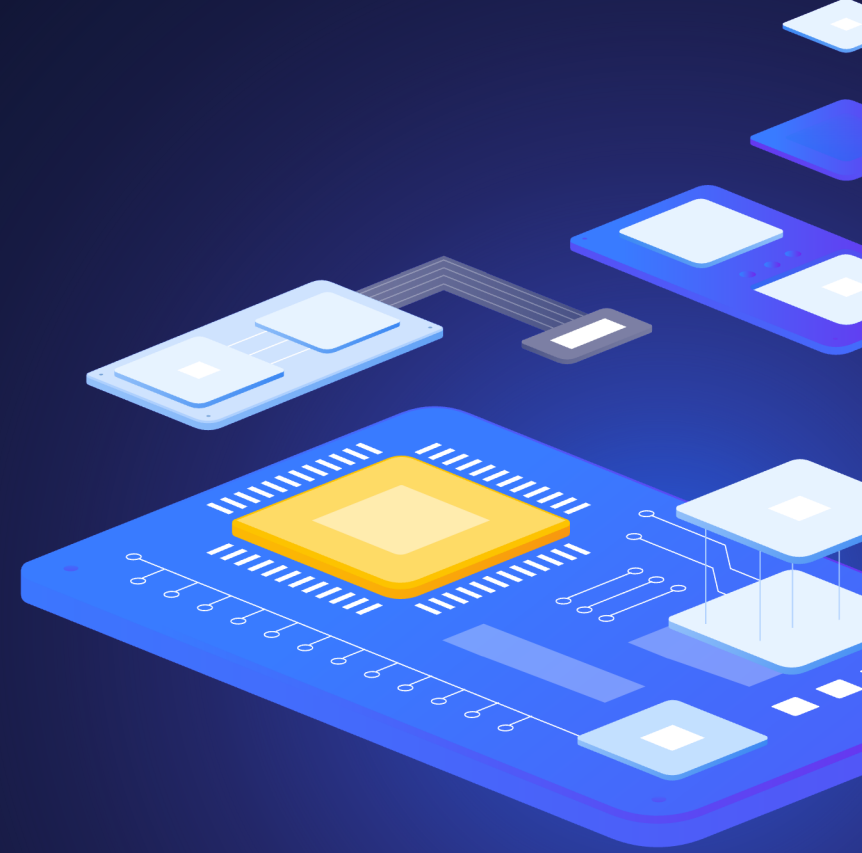
- › If JIT provisioning is enabled, a user group for deprovisioned users must be specified in the Authentication tab.
- › You can use combination internal and LDAP authentication. But you need to use separate user.
- › Authentication setting for user can be found on user group level
  - › For example,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





4

SAML



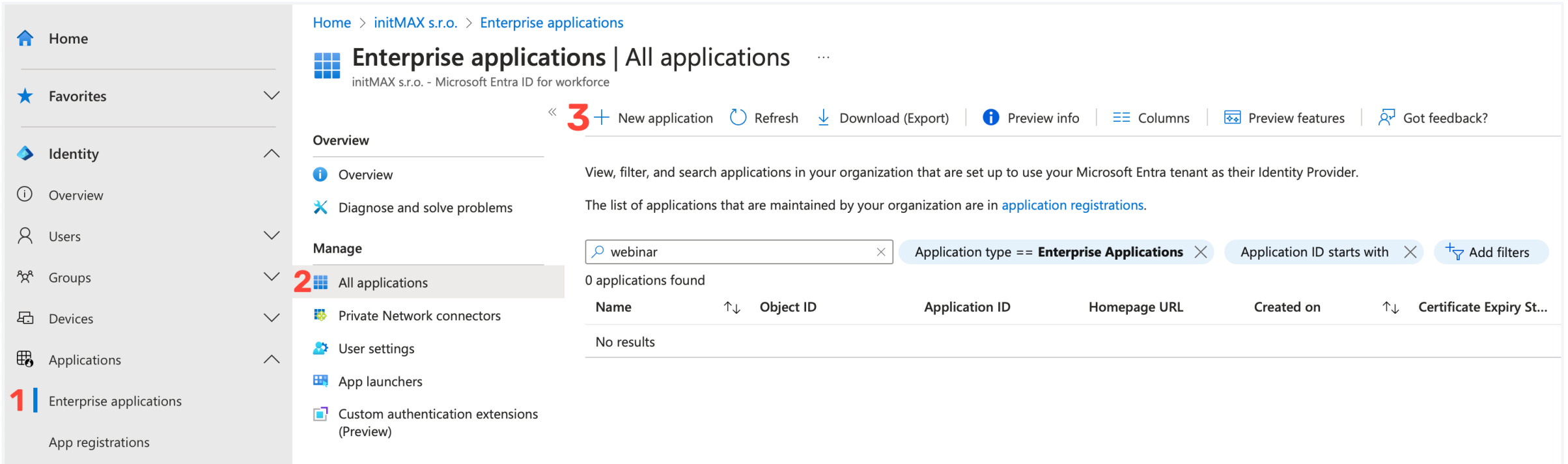
## Zabbix User Provisioning JIT

# 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 Microsoft Entra 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 – Microsoft Entra

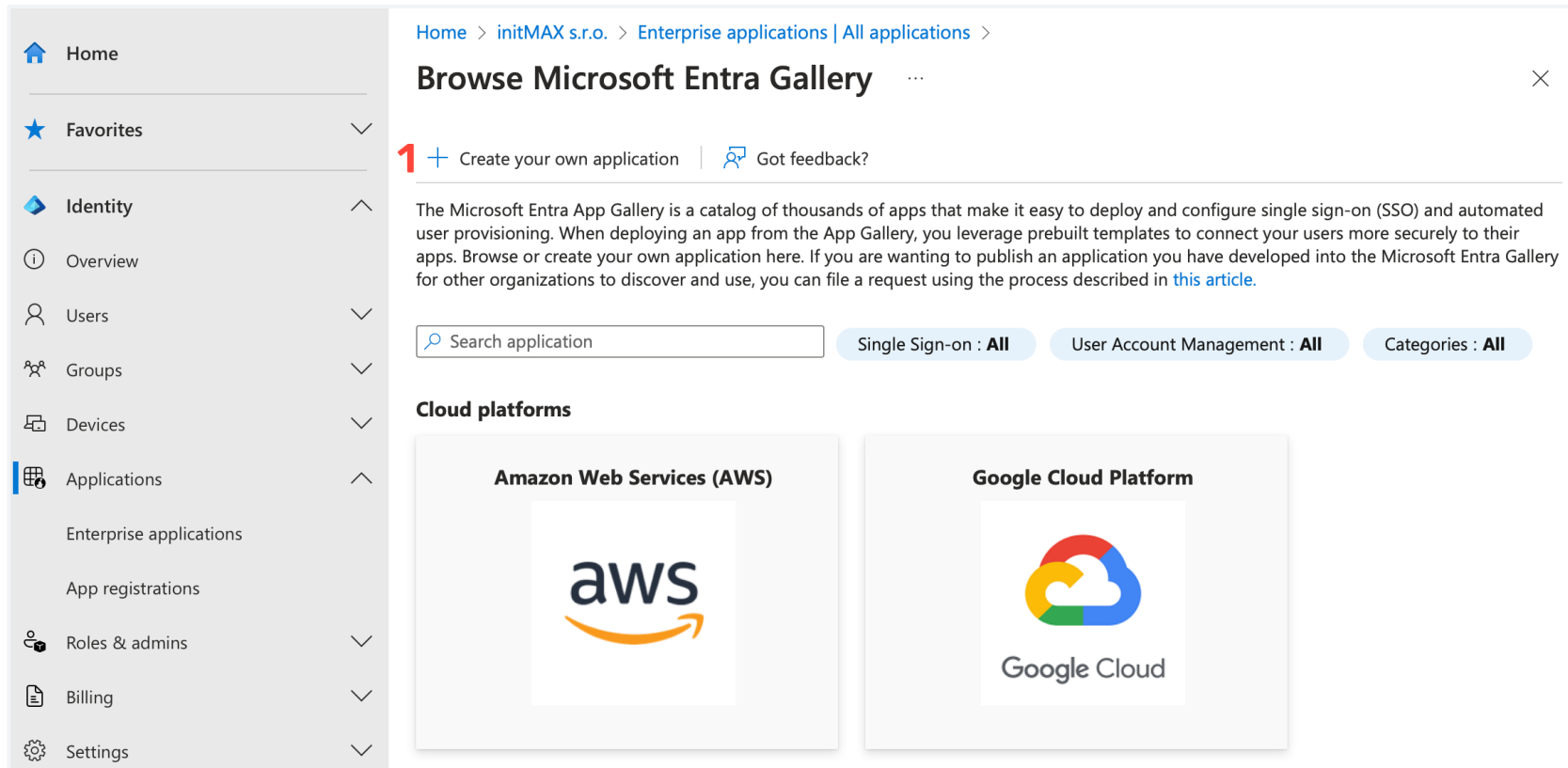
- › Create your new Enterprise application
  - › We need this application for our SAML setting



The screenshot shows the Microsoft Entra 'Enterprise applications' page. The left sidebar contains navigation options: Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, and Enterprise applications (highlighted with a red '1'). The main content area shows the breadcrumb 'Home > initMAX s.r.o. > Enterprise applications' and the title 'Enterprise applications | All applications'. Below the title, there are action buttons: 'New application' (with a red '3+' badge), 'Refresh', 'Download (Export)', 'Preview info', 'Columns', 'Preview features', and 'Got feedback?'. The 'Overview' section contains an information icon, 'Overview', and 'Diagnose and solve problems'. The 'Manage' section is expanded to show 'All applications' (with a red '2' badge), 'Private Network connectors', 'User settings', 'App launchers', and 'Custom authentication extensions (Preview)'. The main content area includes a search bar with 'webinar', filter buttons for 'Application type == Enterprise Applications' and 'Application ID starts with', and an 'Add filters' button. Below this, it states '0 applications found' and shows a table header with columns: Name, Object ID, Application ID, Homepage URL, Created on, and Certificate Expiry St... The table currently displays 'No results'.

# SAML – Zabbix – Microsoft Entra

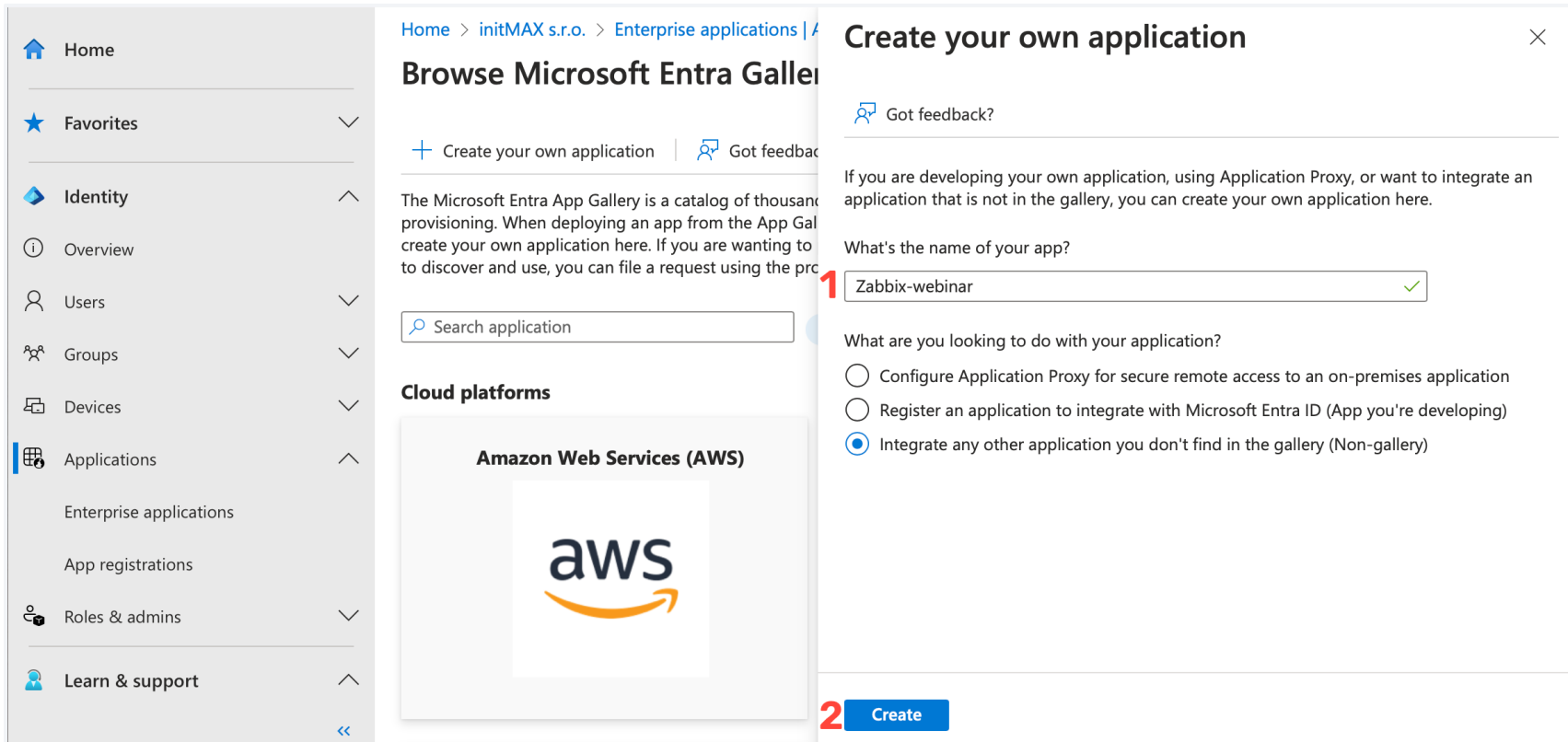
- ▶ Create your new Enterprise application
  - ▶ Hit button “Create your own application”



The screenshot shows the Microsoft Entra App Gallery interface. On the left is a navigation sidebar with options: Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications (selected), Enterprise applications, App registrations, Roles & admins, Billing, and Settings. The main content area has a breadcrumb trail: Home > initMAX s.r.o. > Enterprise applications | All applications >. Below this is a heading "Browse Microsoft Entra Gallery" with a close button. A red notification icon with a plus sign is next to the text "Create your own application" and "Got feedback?". A paragraph of text explains the App Gallery's purpose. 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 – Microsoft Entra

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

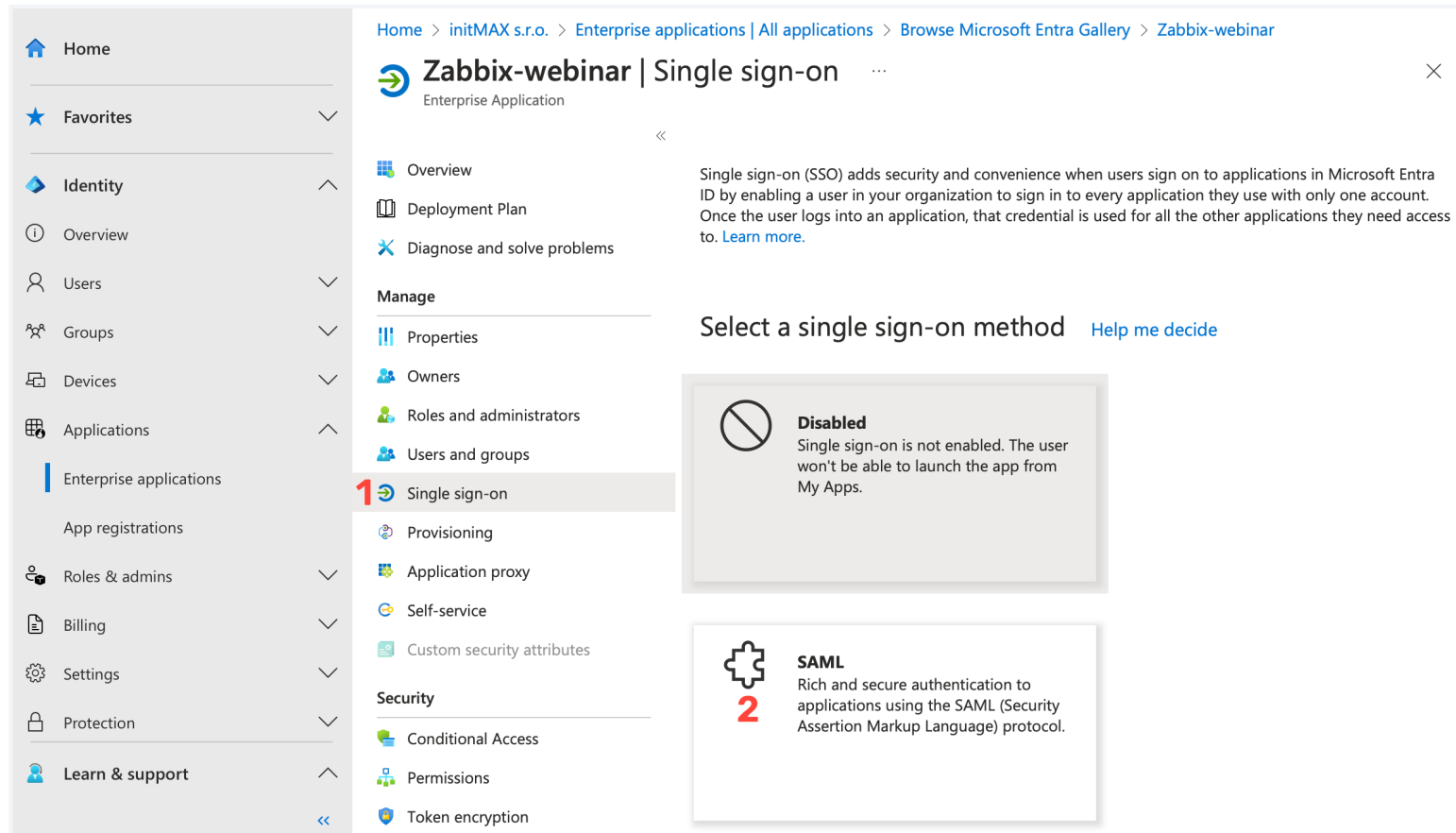


The screenshot shows the Microsoft Entra Admin Center interface. On the left is a navigation sidebar with options: Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Roles & admins, and Learn & support. The main content area displays the 'Browse Microsoft Entra Gallery' page, which includes a search bar and a section for 'Cloud platforms' featuring 'Amazon Web Services (AWS)'. A modal dialog box titled 'Create your own application' is open on the right. It contains the following elements:

- A 'Got feedback?' link.
- Text: 'If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.'
- Text: 'What's the name of your app?' followed by a text input field containing 'Zabbix-webinar' with a green checkmark.
- Text: 'What are you looking to do with your application?' followed by three radio button options:
  - Configure Application Proxy for secure remote access to an on-premises application
  - Register an application to integrate with Microsoft Entra ID (App you're developing)
  - Integrate any other application you don't find in the gallery (Non-gallery)
- A blue 'Create' button at the bottom right, marked with a red '2'.

# SAML – Zabbix – Microsoft Entra

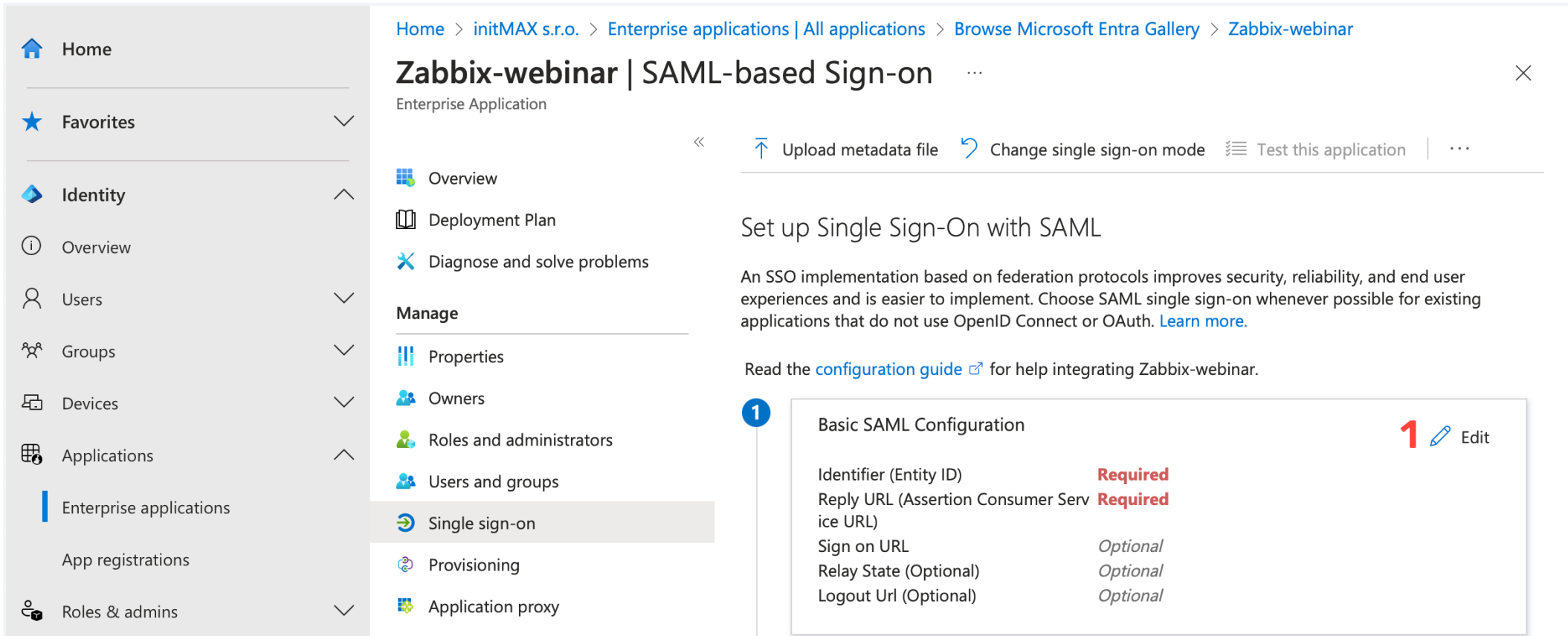
- ▶ Single sign-on setting
  - ▶ Select SAML as a sign-on method



The screenshot shows the Microsoft Entra admin center interface. On the left is a navigation pane with categories like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Roles & admins, Billing, Settings, Protection, and Learn & support. The 'Enterprise applications' section is expanded, showing 'Zabbix-webinar' selected. The main content area displays the 'Single sign-on' configuration page for 'Zabbix-webinar | Single sign-on'. The breadcrumb trail is 'Home > initMAX s.r.o. > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Zabbix-webinar'. The page title is 'Zabbix-webinar | Single sign-on' with a close button. Below the title is a description: 'Single sign-on (SSO) adds security and convenience when users sign on to applications in Microsoft Entra ID 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.](#)' There are three menu items: 'Overview', 'Deployment Plan', and 'Diagnose and solve problems'. Under the 'Manage' section, 'Single sign-on' is highlighted with a red '1'. Below it are 'Provisioning', 'Application proxy', and 'Self-service'. Under the 'Security' section, 'Conditional Access', 'Permissions', and 'Token encryption' are listed. The main content area has a heading 'Select a single sign-on method' with a 'Help me decide' link. There are two options: 'Disabled' (marked with a red '1' and a disabled icon) and 'SAML' (marked with a red '2' and a puzzle piece icon). The 'SAML' option is described as 'Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.'

# SAML – Zabbix – Microsoft Entra

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



The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains navigation options: Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications (selected), App registrations, and Roles & admins. The main content area displays the configuration for the 'Zabbix-webinar' application. The breadcrumb path is: Home > initMAX s.r.o. > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Zabbix-webinar. The page title is 'Zabbix-webinar | SAML-based Sign-on'. Below the title, 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'. A paragraph explains that SAML implementation improves security and user experience. A link to the 'configuration guide' is provided. A 'Basic SAML Configuration' table is shown with a red '1' and an 'Edit' button. The table lists the following fields and their requirements:

Field	Requirement
Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional



## Zabbix User Provisioning JIT

# SAML – Zabbix – Microsoft Entra

- ▶ Single sign-on setting
  - ▶ Fill Entity ID (We are using Zabbix URL)  
<https://student-10.initmax.cz/zabbix>
  - ▶ Reply URL (here is where Zabbix expecting authentication token)  
[https://student-10.initmax.cz/zabbix/index\\_sso.php?acs](https://student-10.initmax.cz/zabbix/index_sso.php?acs)
  - ▶ Logout Url (This is optional)
  - ▶ [https://student-10.initmax.cz/zabbix/index\\_sso.php?sls](https://student-10.initmax.cz/zabbix/index_sso.php?sls)
- ▶ Save our new setting and exit configuration window

### Basic SAML Configuration 5 ×

4 Save | Got feedback?

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

Default

✓ [checkbox] [refresh] [trash]

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

✓ [checkbox] [refresh] [trash]

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) 3  
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 – Microsoft Entra

- › 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?

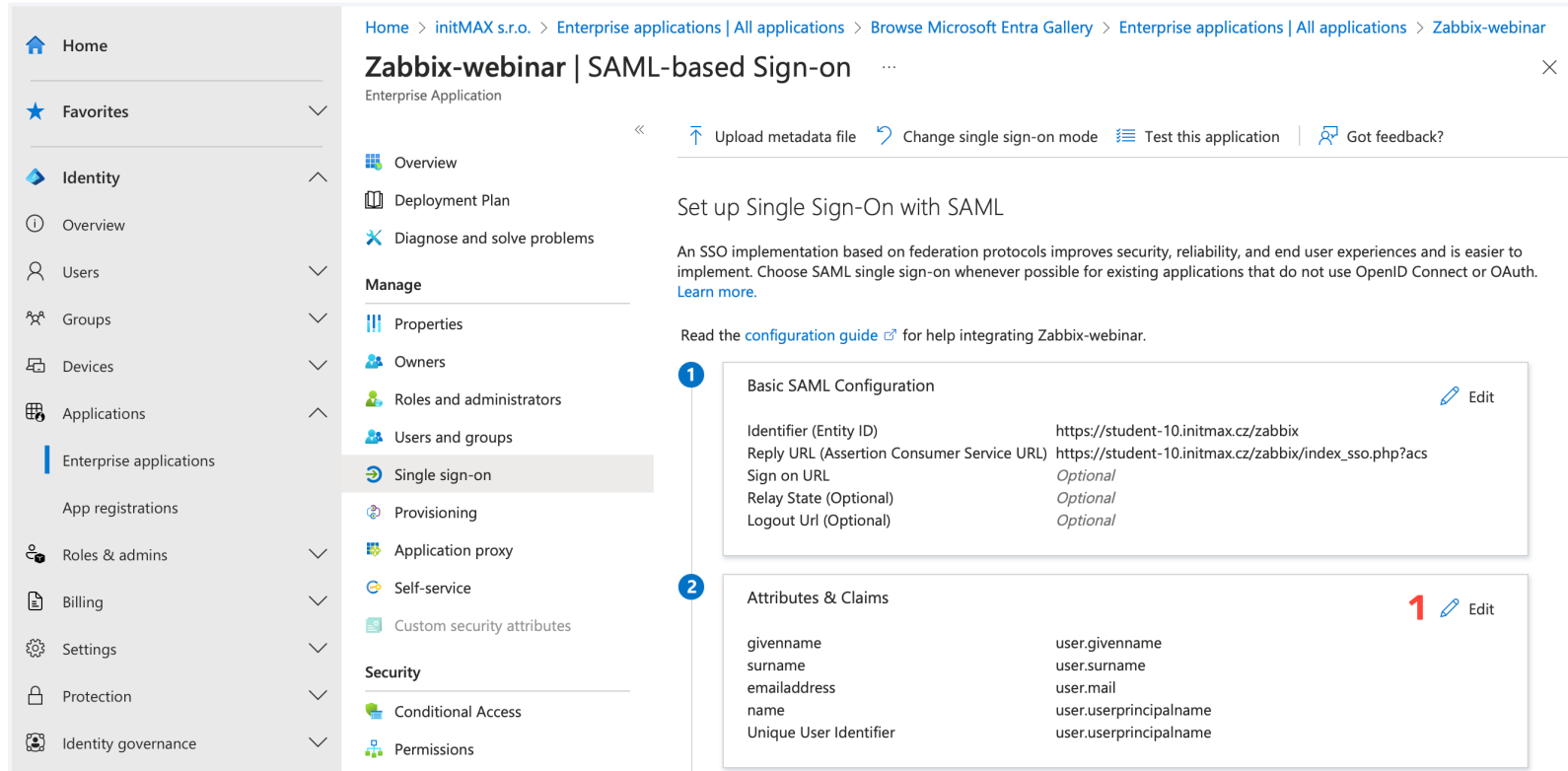
Yes

No, I'll test later

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

# SAML – Zabbix – Microsoft Entra

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



The screenshot displays the Microsoft Entra admin center interface for configuring SAML-based sign-on for the 'Zabbix-webinar' application. The left-hand navigation pane shows the 'Enterprise applications' section expanded, with 'Single sign-on' selected. The main content area is titled 'Zabbix-webinar | SAML-based Sign-on' and includes a breadcrumb trail: Home > initMAX s.r.o. > Enterprise applications | All applications > Browse Microsoft Entra Gallery > Enterprise applications | All applications > Zabbix-webinar. Below the title, there are navigation options: 'Upload metadata file', 'Change single sign-on mode', 'Test this application', and 'Got feedback?'. The page is divided into two main sections: 'Basic SAML Configuration' (step 1) and 'Attributes & Claims' (step 2). The 'Basic SAML Configuration' section contains a table with the following details:

Identifier (Entity ID)	https://student-10.initmax.cz/zabbix
Reply URL (Assertion Consumer Service URL)	https://student-10.initmax.cz/zabbix/index_sso.php?acs
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

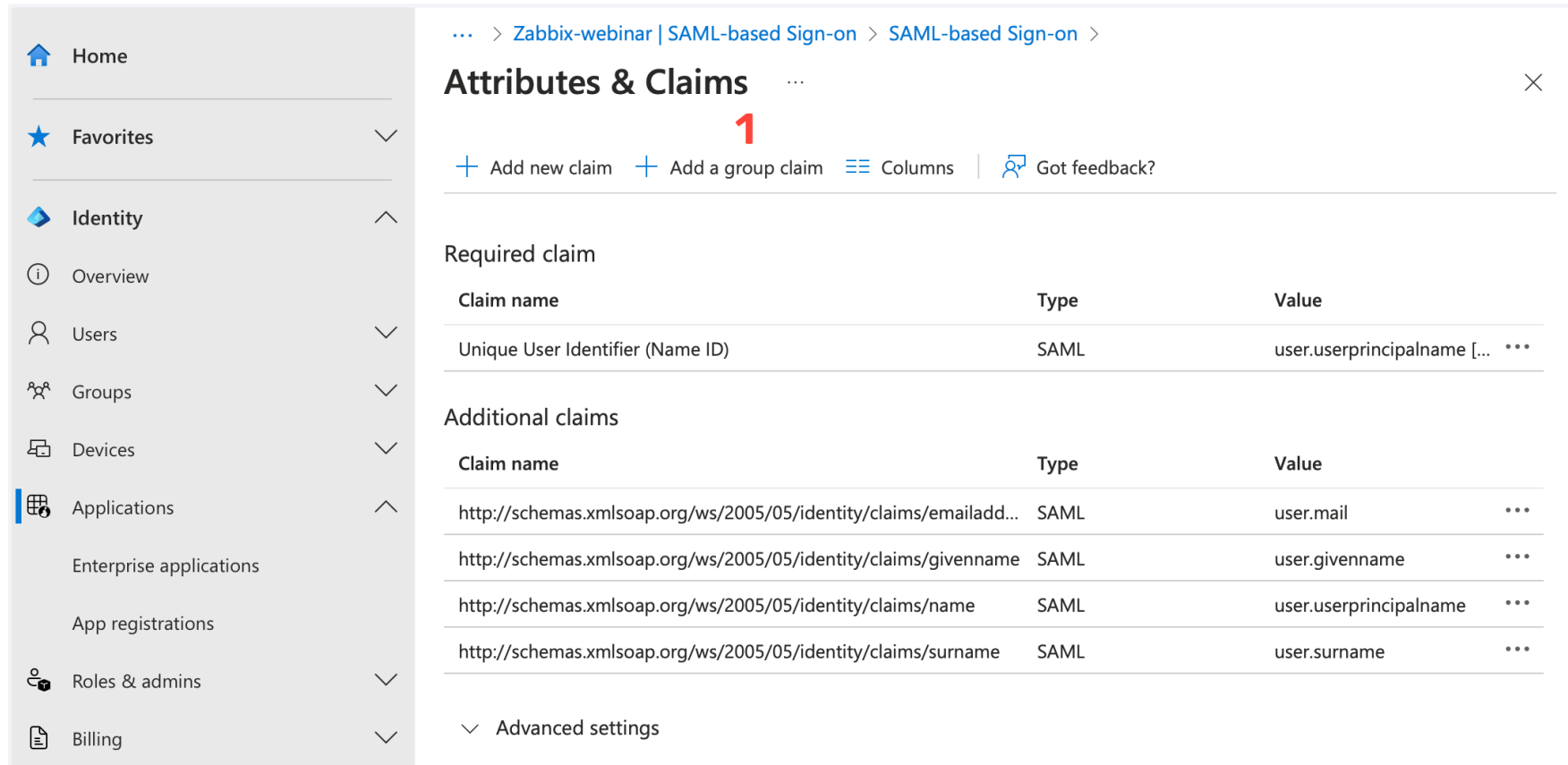
The 'Attributes & Claims' section (step 2) contains a table with the following details:

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

Each configuration section includes an 'Edit' link. The 'Attributes & Claims' section also features a red '1' icon, indicating a required or critical configuration step.

# SAML – Zabbix – Microsoft Entra

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



... > 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

# SAML – Zabbix – Microsoft Entra

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

### Group Claims ✕

Manage the group claims used by Microsoft Entra ID to populate SAML tokens issued to your app

Which groups associated with the user should be returned in the claim?

None

**1**  All groups

Security groups

Directory roles

Groups assigned to the application

Source attribute \*

**2** sAMAccountName

⚠ This source attribute only works for groups synchronized from an on-premises Active Directory using Microsoft Entra Connect Sync 1.2.70.0 or above. [Learn More](#)

Emit group name for cloud-only groups ⓘ

**3** ^ Advanced options

Filter groups

Attribute to match

Match with

String

**4**  Customize the name of the group claim

Name (required)

**5** groups

Namespace (optional)

Emit groups as role claims ⓘ

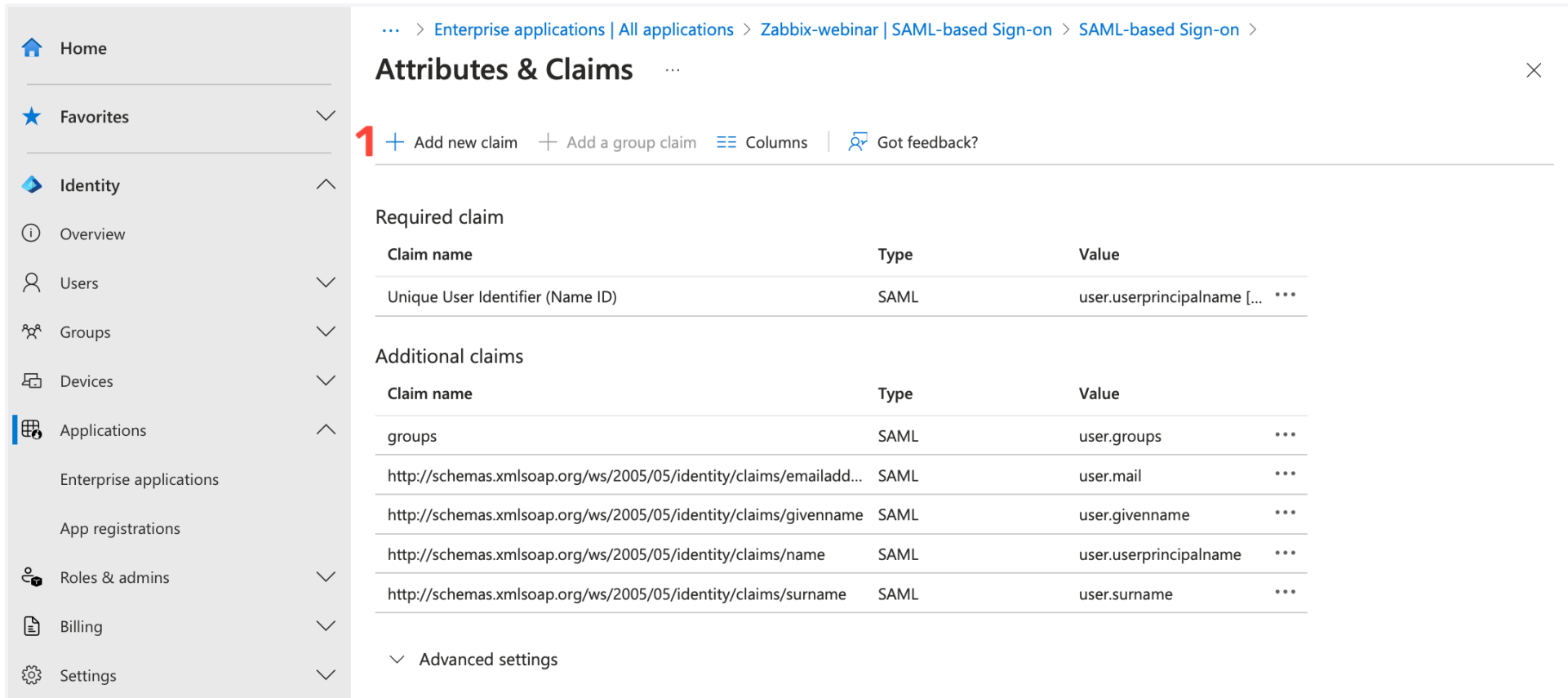
Apply regex replace to groups claim content

Expose claim in JWT tokens in addition to SAML tokens

**Save** **6**

# SAML – Zabbix – Microsoft Entra

- ▶ 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 Zabbix web interface for configuring SAML-based Sign-on. The left sidebar contains navigation options: Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Roles & admins, Billing, and Settings. The main content area is titled 'Attributes & Claims' and includes a breadcrumb trail: Enterprise applications | All applications > Zabbix-webinar | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims. Below the title, there are options to 'Add new claim', 'Add a group claim', 'Columns', and 'Got feedback?'. The configuration is divided into two sections: 'Required claim' and 'Additional claims', each with a table of claim details.

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

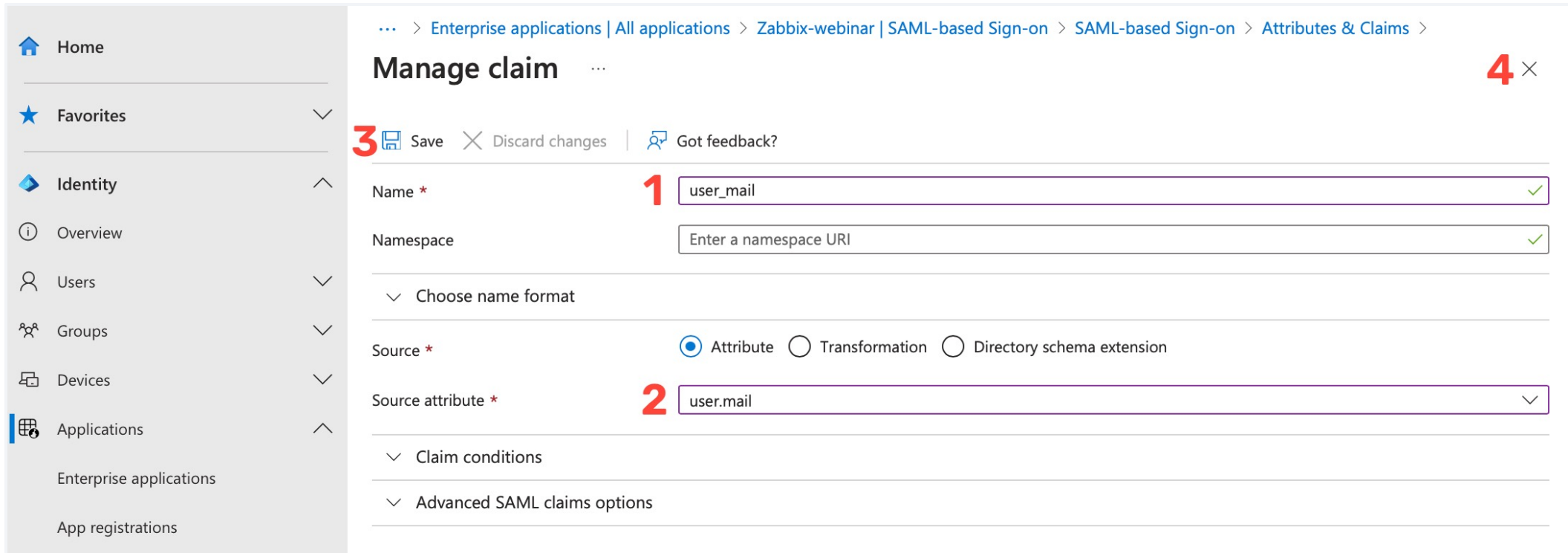
Claim name	Type	Value
groups	SAML	user.groups [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname [...]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname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

Advanced settings

# SAML – Zabbix – Microsoft Entra

## › 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 'Manage claim' configuration page in the Microsoft Entra admin center. The breadcrumb trail is: Enterprise applications | All applications > Zabbix-webinar | SAML-based Sign-on > SAML-based Sign-on > Attributes & Claims >. The page title is 'Manage claim' with a red '4' icon in the top right corner. Below the title, there are three action buttons: '3 Save', 'Discard changes', and 'Got feedback?'. The main configuration area includes:

- Name \***: A text input field containing 'user\_mail' with a green checkmark on the right. A red '1' is positioned to the left of the field.
- Namespace**: A text input field containing 'Enter a namespace URI' with a green checkmark on the right.
- Choose name format**: A dropdown menu.
- Source \***: Radio buttons for 'Attribute' (selected), 'Transformation', and 'Directory schema extension'.
- Source attribute \***: A dropdown menu containing 'user.mail' with a green checkmark on the right. A red '2' is positioned to the left of the field.
- Claim conditions**: A dropdown menu.
- Advanced SAML claims options**: A dropdown menu.



# SAML – Zabbix – Microsoft Entra

- › Single sign-on setting
  - › Repeat this operation for all your attributes  
**mail 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\_mail**

**user.mail**

## Optional claims

user\_mobile

user.mobilephone

user\_lastname

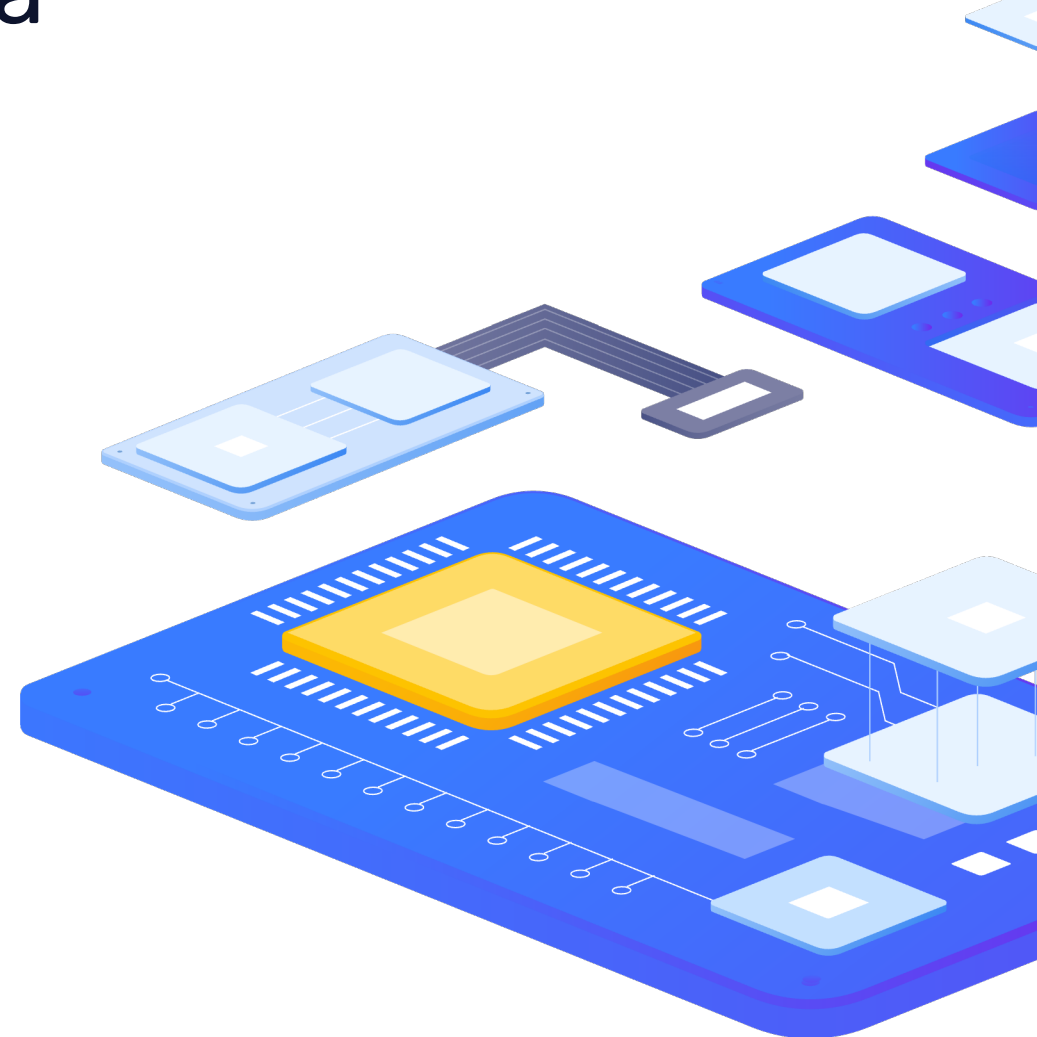
user.surname

user\_name

user.givenname

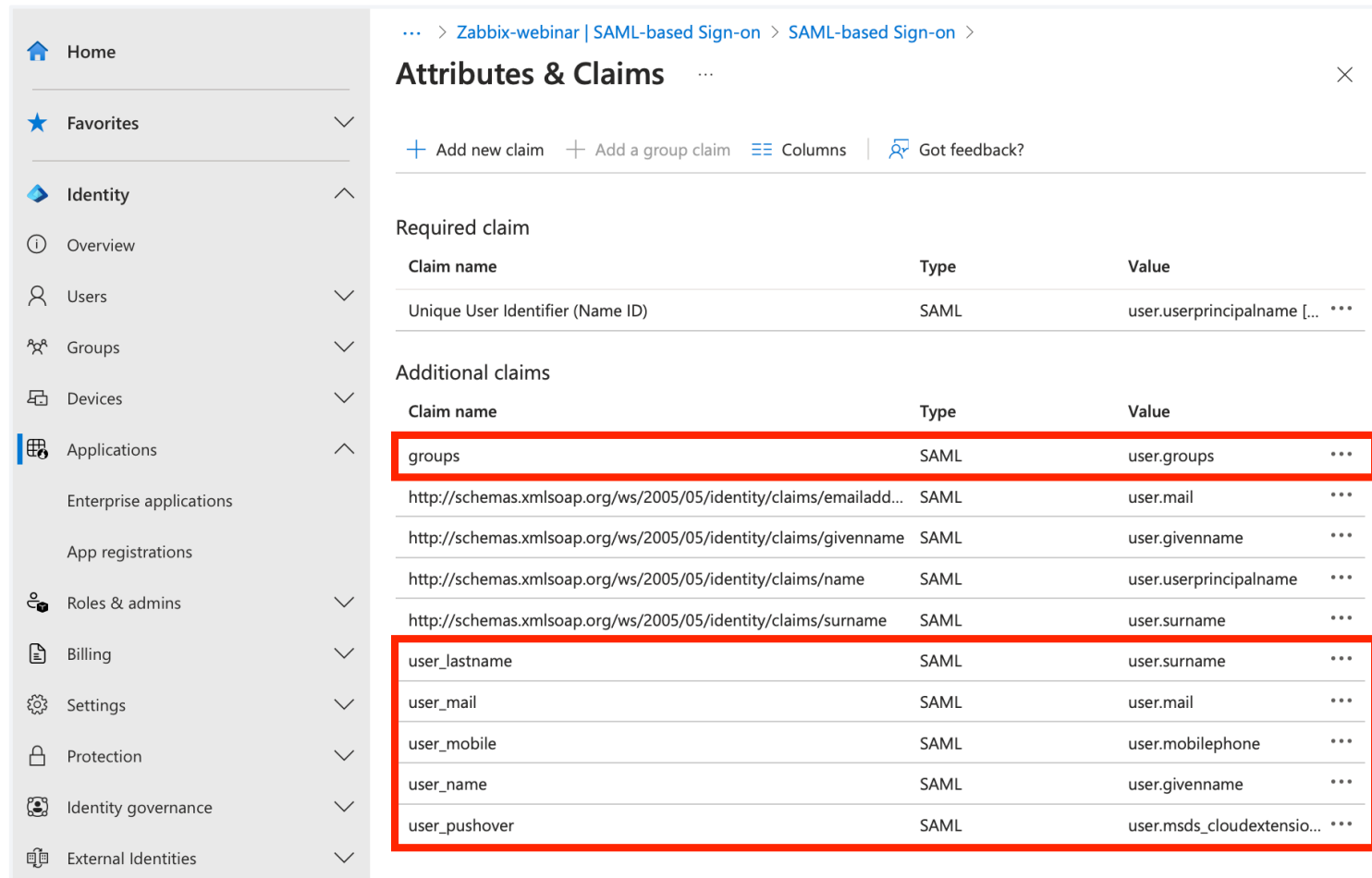
user\_pushover

user.msds\_cloud...



# SAML – Zabbix – Microsoft Entra

## ▶ Single sign-on setting



The screenshot shows the Zabbix web interface for configuring SAML-based Sign-on. The left sidebar contains navigation options: Home, Favorites, Identity (selected), Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Roles & admins, Billing, Settings, Protection, Identity governance, and External Identities. The main content area is titled "Attributes & Claims" and displays a table of claims. The "Required claim" section shows a single claim: "Unique User Identifier (Name ID)" with type "SAML" and value "user.userprincipalname [...]". The "Additional claims" section lists several claims, with two rows highlighted by a red box: "groups" and "user\_lastname".

... > 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 [...] ***

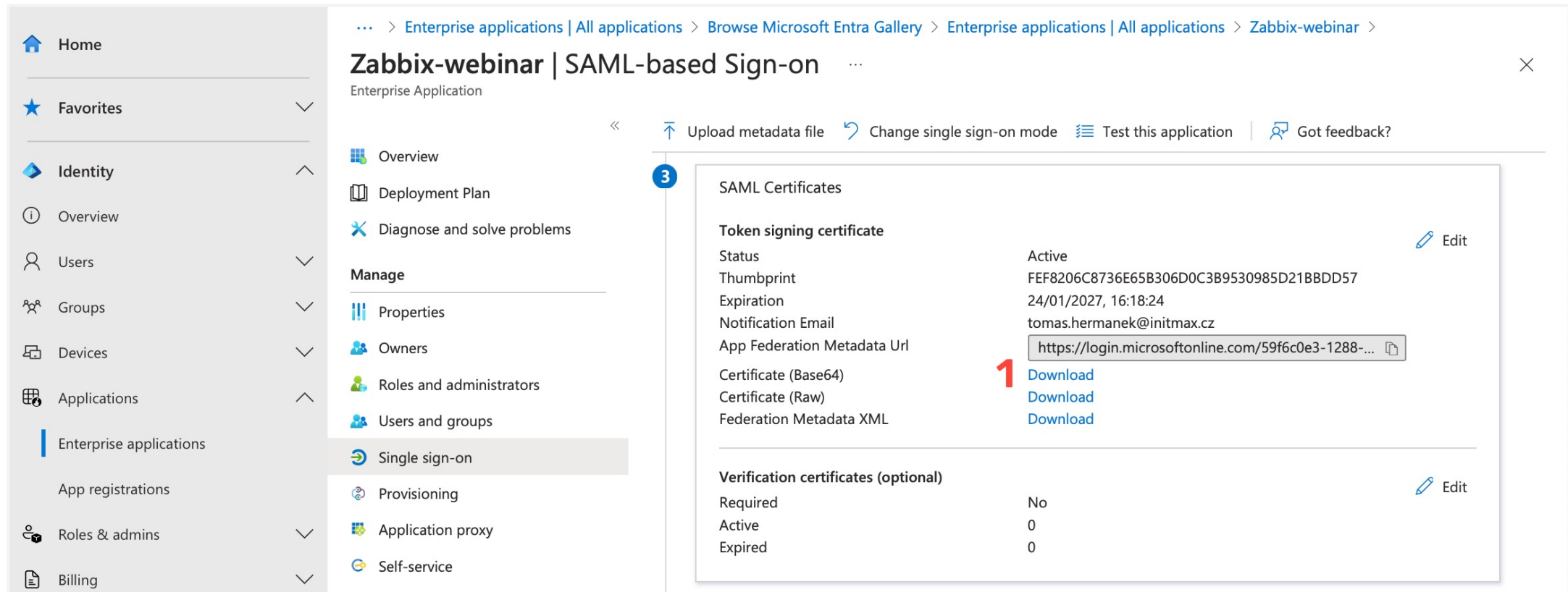
Additional claims

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_lastname	SAML	user.surname ***
user_mail	SAML	user.mail ***
user_mobile	SAML	user.mobilephone ***
user_name	SAML	user.givenname ***
user_pushover	SAML	user.msds_cloudextensio... ***

# SAML – Zabbix – Microsoft Entra

### › Single sign-on setting

- › Last part for SAML setting in Microsoft Entra is export certificate for signed Zabbix tokens (Base64)



Enterprise Application: Zabbix-webinar | SAML-based Sign-on

Overview | Deployment Plan | Diagnose and solve problems

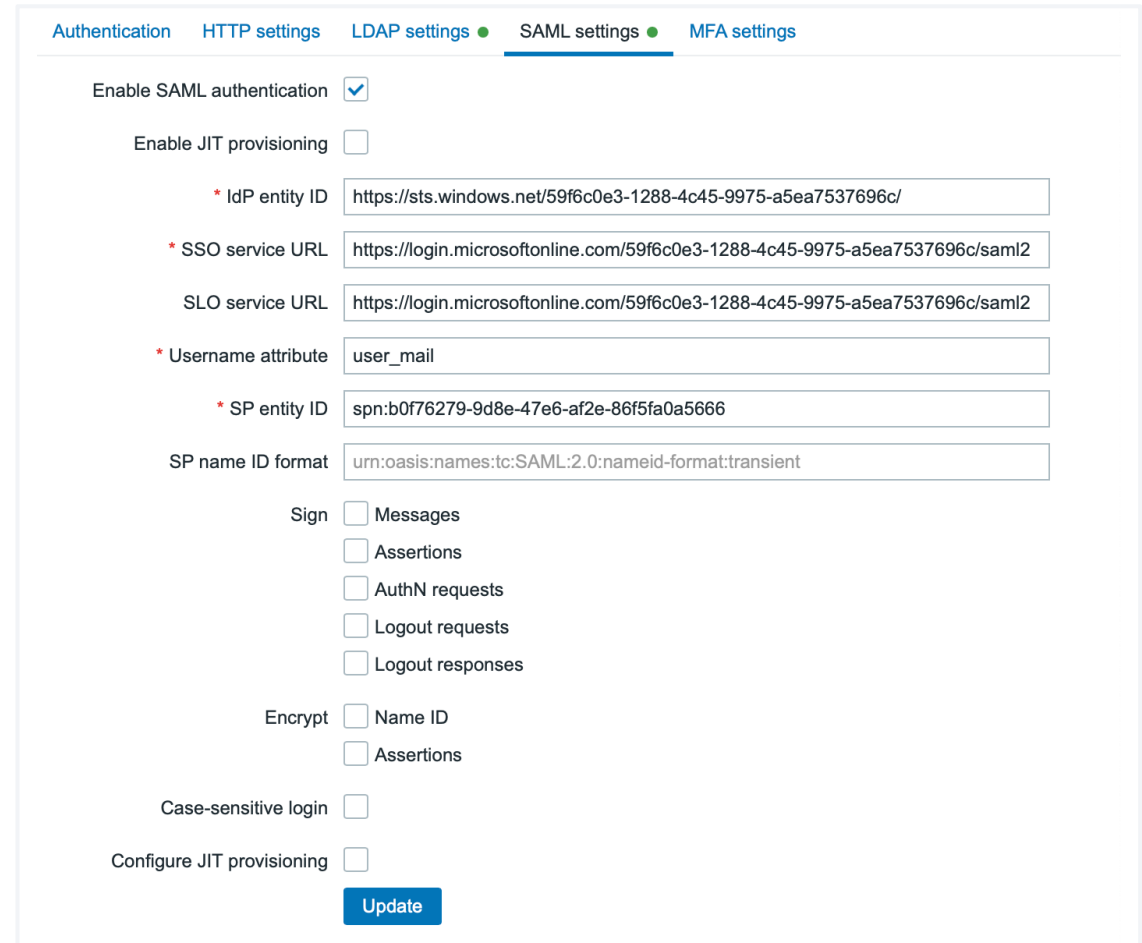
Manage: Properties | Owners | Roles and administrators | Users and groups | **Single sign-on** | Provisioning | Application proxy | Self-service

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

SAML Certificates		Edit
<b>Token signing certificate</b>		
Status	Active	
Thumbprint	FEF8206C8736E65B306D0C3B9530985D21BBDD57	
Expiration	24/01/2027, 16:18:24	
Notification Email	tomas.hermanek@initmax.cz	
App Federation Metadata Url	<a href="https://login.microsoftonline.com/59f6c0e3-1288-...">https://login.microsoftonline.com/59f6c0e3-1288-...</a>	
Certificate (Base64)	<a href="#">Download</a>	
Certificate (Raw)	<a href="#">Download</a>	
Federation Metadata XML	<a href="#">Download</a>	
<b>Verification certificates (optional)</b>		Edit
Required	No	
Active	0	
Expired	0	

# SAML – Zabbix

- › Enable SAML authentication
  - › Mark the checkbox to enable SAML authentication
- › IdP entity ID (In Microsoft Entra is named “**Microsoft Entra Identifier**”)
  - › The unique entity identifier within the SAML identity provider
- › SSO service URL (In Microsoft Entra is named “**Login URL**”)
  - › The URL users will be redirected to when logging in
- › SLO service URL (In Microsoft Entra 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\_mail**”)
  - › SAML attribute to be used as a username when logging into Zabbix.
- › SP entity ID (In Microsoft Entra is named “**Application ID**”)
  - › The unique service provider identifier
  - › For Microsoft Entra you need use prefix “**spn:**”



The screenshot shows the Zabbix SAML settings configuration page. The page has a navigation bar with tabs for Authentication, HTTP settings, LDAP settings, SAML settings (selected), and MFA settings. The main content area contains the following 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 button

## Zabbix User Provisioning JIT

# SAML – Zabbix

Attributes & Claims > Enterprise applications | All applications > App registrations > Enterprise applications | All applications > 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

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

user\_pushover user.msds\_cloudextensionattribute1 (extension\_78f02a2e2cc4f4abfc29b38cb00868c\_msds\_cloudextensionattribute1) user.userprincipalname

Unique User Identifier user.userprincipalname

SAML Certificates

Token signing certificate

Status Active Edit

Thumbprint FEF8206C8736E658306D0C389530985D218BDD57

Expiration 24/01/2027, 16:18:24

Notification Email tomas.hermanek@initmax.cz

App Federation Metadata URL https://login.microsoftonline.com/59f6c0e3-128... Download

Certificate (Base64) Download

Certificate (Raw) Download

Federation Metadata XML Download

Verification certificates (optional) Edit

Required No

Active 0

Expired 0

Set up Zabbix-webinar

You'll need to configure the application to link with Microsoft Entra ID.

Login URL https://login.microsoftonline.com/59f6c0e3-128... Download

Microsoft Entra Identifier https://sts.windows.net/59f6c0e3-1288-4c45-99... Download

Logout URL https://login.microsoftonline.com/59f6c0e3-128... Download

Authentication HTTP settings LDAP settings ● SAML settings ● MFA settings

Enable SAML authentication

Enable JIT provisioning

\* IdP entity ID https://sts.windows.net/59f6c0e3-1288-4c45-9975-a5ea7537696c/

\* SSO service URL https://login.microsoftonline.com/59f6c0e3-1288-4c45-9975-a5ea7537696c/saml2

SLO service URL https://login.microsoftonline.com/59f6c0e3-1288-4c45-9975-a5ea7537696c/saml2

\* Username attribute user\_mail

\* SP entity ID spn:b0f76279-9d8e-47e6-af2e-86f5fa0a5666

SP name ID format urn:oasis:names:tc:SAML:2.0:nameid-format:transient

Sign  Messages

Assertions

AuthN requests

Logout requests

Logout responses

Encrypt  Name ID

Assertions

Case-sensitive login

Configure JIT provisioning

Update

Attributes & Claims > Enterprise applications | All applications > App registrations > Enterprise applications | All applications > 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

Security

- Conditional Access

Save Discard Delete Got feedback?


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 \* Zabbix-webinar

Homepage URL https://account.activedirectory.windowsazure.com/444/applications/de... Download

Logo 

User access URL https://launcher.myapps.microsoft.com/api/signin/b0f76279-9d8e-47e... Download

Application ID b0f76279-9d8e-47e6-af2e-86f5fa0a5666

Object ID 080fc38-5568-4d58-ac52-a2c66cd79264

# 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/Zabbix-webinar.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';  
$SSO['IDP_CERT']         = 'conf/certs/Zabbix-webinar.cer';  
//$SSO['SETTINGS']       = [];
```

- ▶ Create your user in Zabbix ([tomas.hermanek@initmax.cz](mailto: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 name attribute
  - › Fill User last name attribute
  - › Create correct group mapping for groups
  - › Create correct setting for Media type mapping

HTTP settings | LDAP settings | **SAML settings** | MFA 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	<a href="#">Remove</a>
<a href="#">Add</a>			

Media type mapping <sup>?</sup>

Name	Media type	Attribute	
Email	Email (HTML)	user_mail	<a href="#">Remove</a>
Pushover	Pushover	user_pushover	<a href="#">Remove</a>
Mobile	SMS	user_mobile	<a href="#">Remove</a>
<a href="#">Add</a>			

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](#) [Reset TOTP secret](#) [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	<a href="#">INTERNAL</a>	No (2023-04-05 00:58:59)	Ok	Internal	Enabled	Disabled	Enabled		
<input type="checkbox"/>	guest			Guest role	<a href="#">Disabled, Guests</a>	No	Ok	Internal	Disabled	Disabled	Disabled		
<input type="checkbox"/>	<a href="#">tomas.hermanek@initmax.cz</a>	Tomáš	Heřmánek	Super admin role	<a href="#">Zabbix_Super_Admins</a>	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](#) [Reset TOTP secret](#) [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	<span>N</span> <span>I</span> <span>W</span> <span>A</span> <span>H</span> <span>D</span>	Enabled	<a href="#">Edit</a> <a href="#">Remove</a>
	Pushover	uc4hf8jx1262o3tc2v7qzooeibb1rt	1-7,00:00-24:00	<span>N</span> <span>I</span> <span>W</span> <span>A</span> <span>H</span> <span>D</span>	Enabled	<a href="#">Edit</a> <a href="#">Remove</a>
	SMS	+420 732 447 184	1-7,00:00-24:00	<span>N</span> <span>I</span> <span>W</span> <span>A</span> <span>H</span> <span>D</span>	Enabled	<a href="#">Edit</a> <a href="#">Remove</a>
	<a href="#">Add</a>					

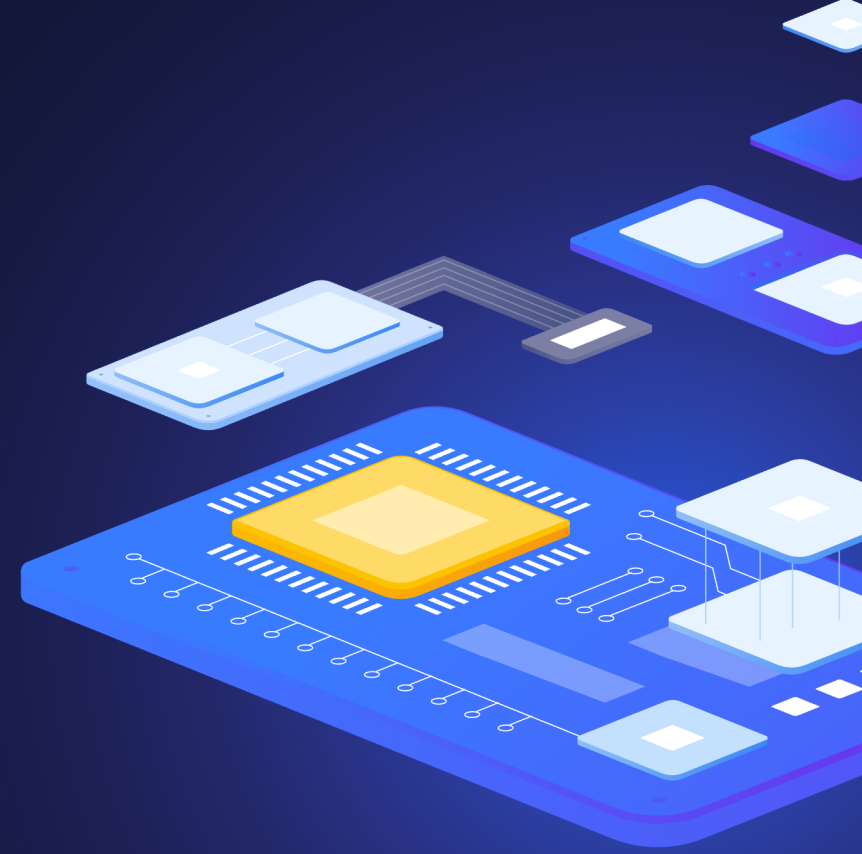
[Update](#) [Delete](#) [Cancel](#)

# 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** MFA 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	<a href="#">Remove</a>
<a href="#">Add</a>			

Media type mapping ?

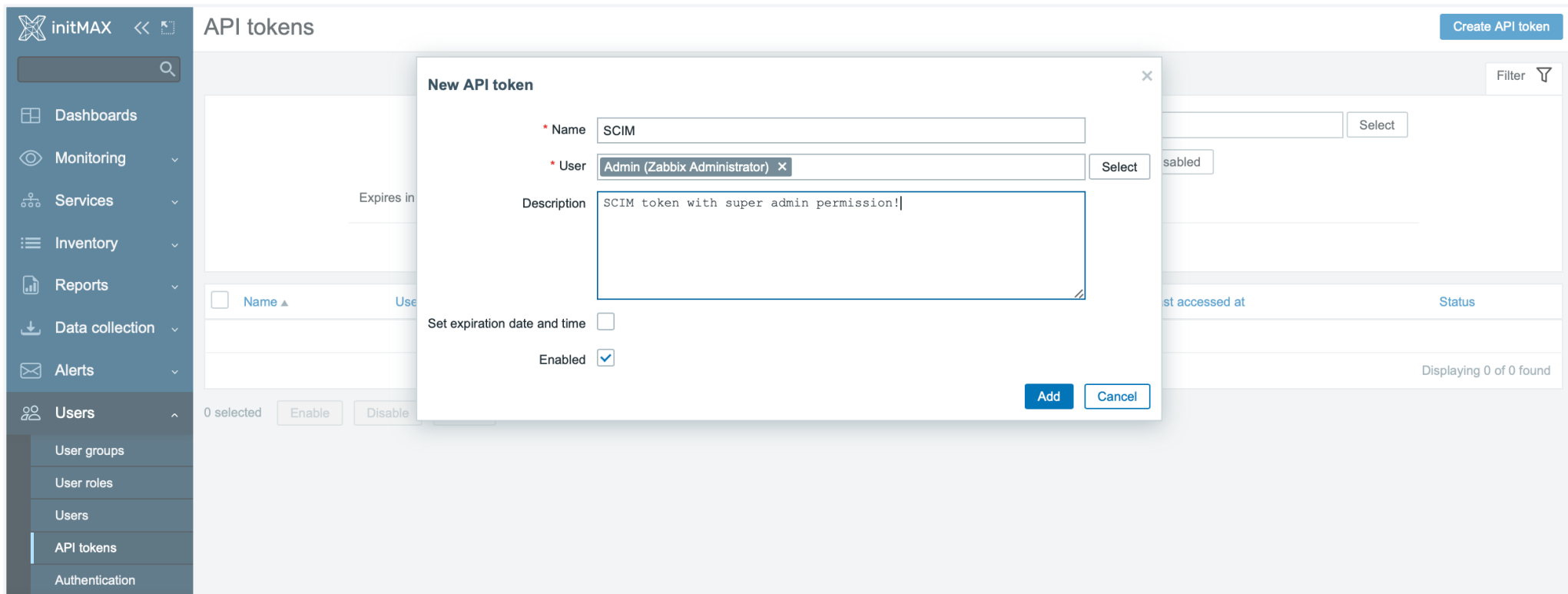
Name	Media type	Attribute	Action
Email	Email (HTML)	user_mail	<a href="#">Remove</a>
Pushover	Pushover	user_pushover	<a href="#">Remove</a>
Mobile	SMS	user_mobile	<a href="#">Remove</a>
<a href="#">Add</a>			

Enable SCIM provisioning

[Update](#)

# SCIM – Zabbix

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



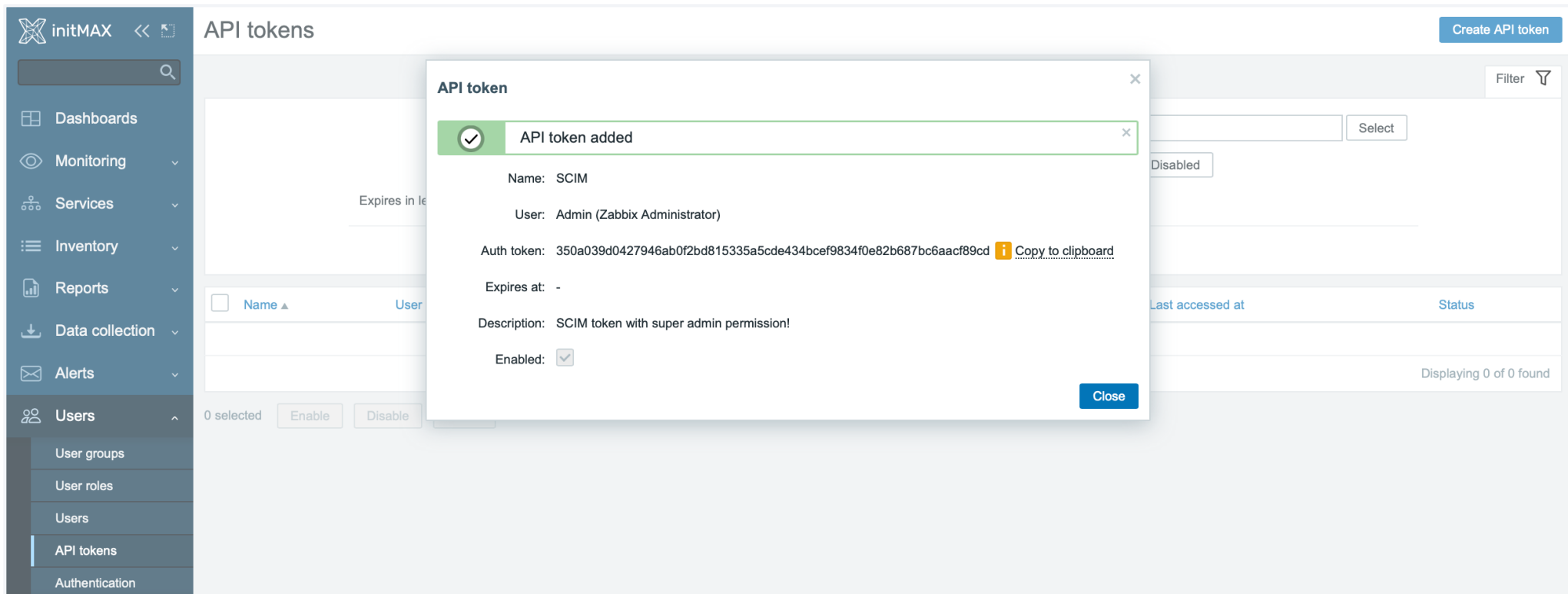
The screenshot displays the Zabbix web interface for managing API tokens. A modal dialog titled "New API token" is open, allowing the creation of a new token. The dialog contains the following fields and options:

- Name:** SCIM
- User:** Admin (Zabbix Administrator) [Select]
- Description:** SCIM token with super admin permission!
- Set expiration date and time:**
- Enabled:**

At the bottom of the dialog are "Add" and "Cancel" buttons. The background interface shows the "API tokens" management page with a search bar, a table of tokens, and a "Create API token" button in the top right corner. The table currently displays 0 tokens.

# 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:

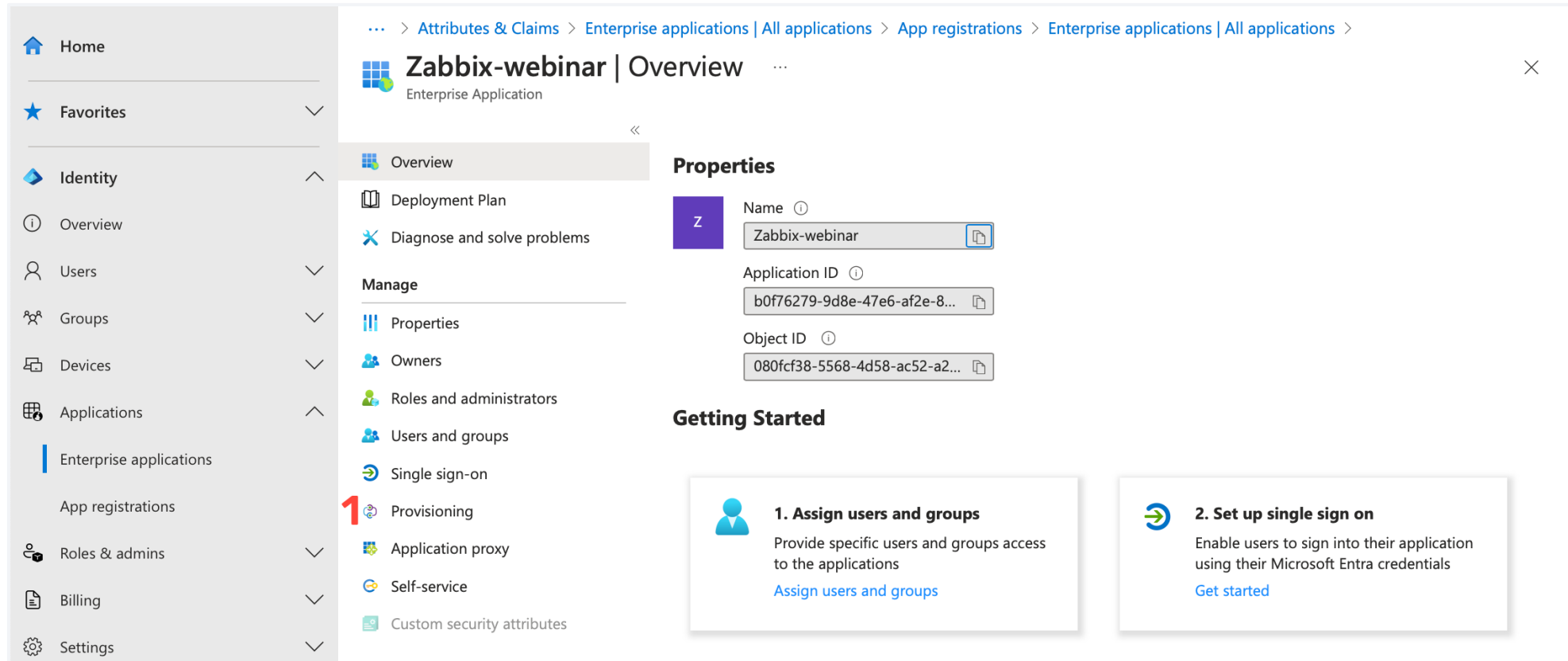
The background interface shows the "API tokens" management page with a sidebar menu on the left containing options like Dashboards, Monitoring, Services, Inventory, Reports, Data collection, Alerts, Users, User groups, User roles, and Authentication. A "Create API token" button is visible in the top right corner of the main content area.



## Zabbix User Provisioning JIT

# SCIM – Microsoft Entra

- › Zabbix SCIM provisioning
  - › In Microsoft Entra application go to section Provisioning



The screenshot shows the Microsoft Entra application configuration interface for 'Zabbix-webinar'. The left sidebar contains navigation options: Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications (highlighted), App registrations, Roles & admins, Billing, and Settings. The main content area shows the 'Zabbix-webinar | Overview' page, which is part of the 'Enterprise Application' section. The breadcrumb trail is: Attributes & Claims > Enterprise applications | All applications > App registrations > Enterprise applications | All applications >. The 'Properties' section displays the following information:

- Name: Zabbix-webinar
- Application ID: b0f76279-9d8e-47e6-af2e-8...
- Object ID: 080fcf38-5568-4d58-ac52-a2...

The 'Getting Started' section provides two main steps:

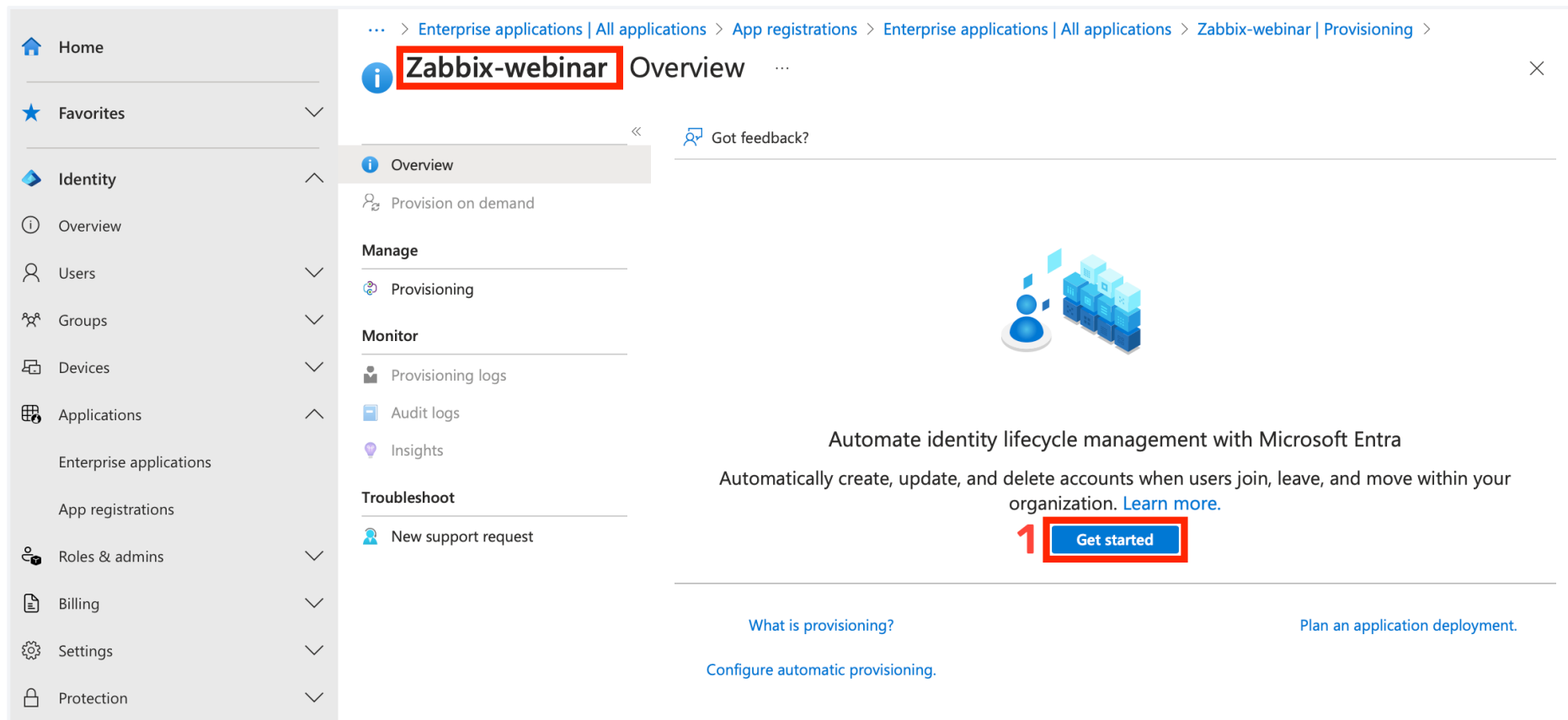
- 1. Assign users and groups**  
Provide specific users and groups access to the applications  
[Assign users and groups](#)
- 2. Set up single sign on**  
Enable users to sign into their application using their Microsoft Entra credentials  
[Get started](#)

A red '1' is placed next to the 'Provisioning' option in the left sidebar, indicating the current step in the process.

# SCIM – Microsoft Entra

### › Zabbix SCIM provisioning

- › In Microsoft Entra application go to section Provisioning and hit button “Get started”



The screenshot shows the Microsoft Entra Provisioning interface. On the left is a navigation sidebar with categories: Home, Favorites, Identity (expanded), Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Roles & admins, Billing, Settings, and Protection. The main content area shows the breadcrumb path: Enterprise applications | All applications > App registrations > Enterprise applications | All applications > Zabbix-webinar | Provisioning. The page title is "Zabbix-webinar Overview". Below the title is a "Got feedback?" link. The main content area features a large blue graphic of a person and blocks, with the text: "Automate identity lifecycle management with Microsoft Entra. Automatically create, update, and delete accounts when users join, leave, and move within your organization. [Learn more.](#)" A red box highlights a "1 Get started" button. At the bottom, there are three links: "What is provisioning?", "Configure automatic provisioning.", and "Plan an application deployment."

# SCIM – Microsoft Entra

- ▶ Zabbix SCIM provisioning
  - ▶ Select Automatic Provisioning mode
  - ▶ Tenant URL - [https://student-10.initmax.cz/zabbix/api\\_scim.php](https://student-10.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 \* ①  
https://student-01.initmax.cz/zabbix/api\_scim.php ✓ 2

Secret Token  
..... 3

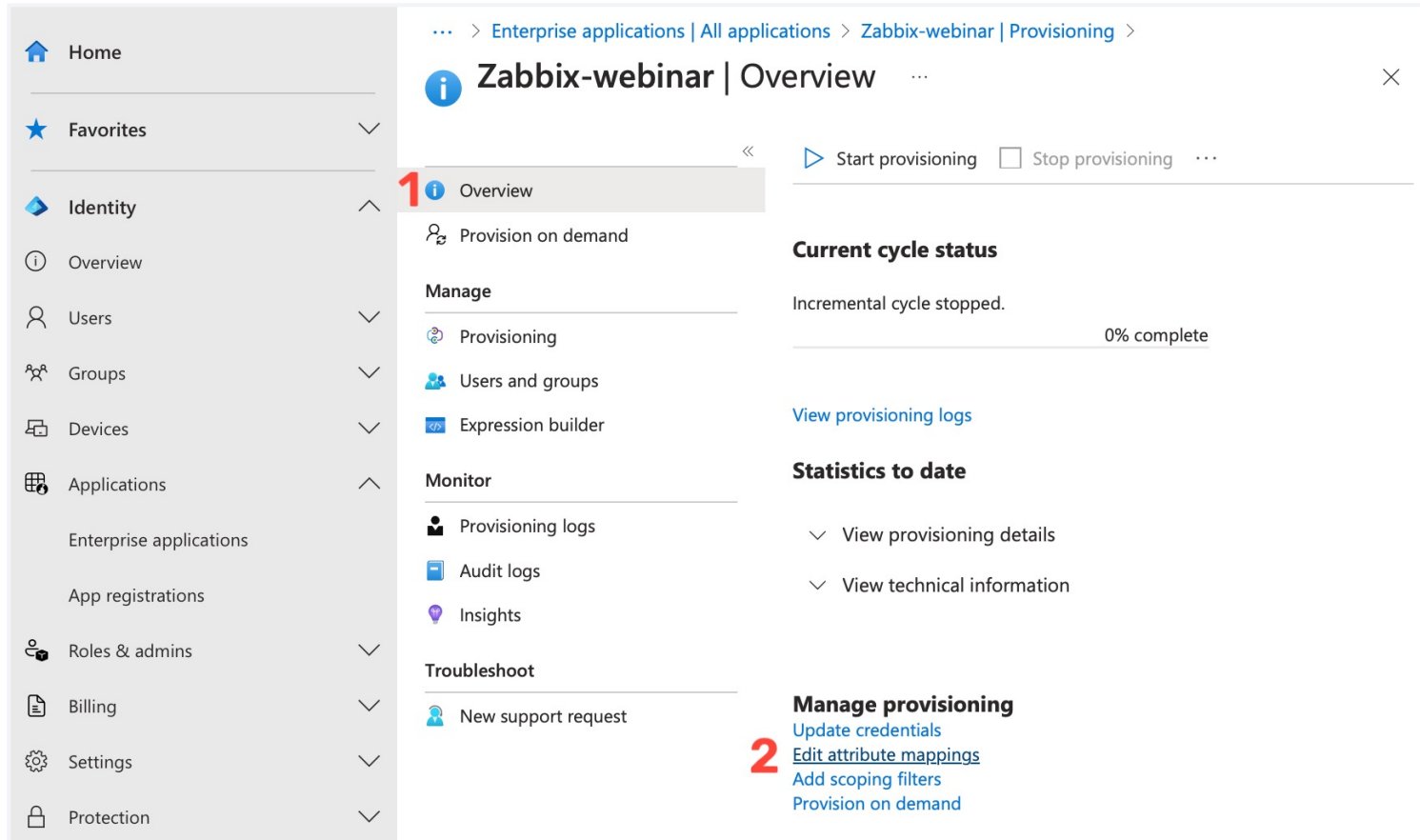
Test Connection 4

## Zabbix User Provisioning JIT

# SCIM – Microsoft Entra

### › Zabbix SCIM provisioning

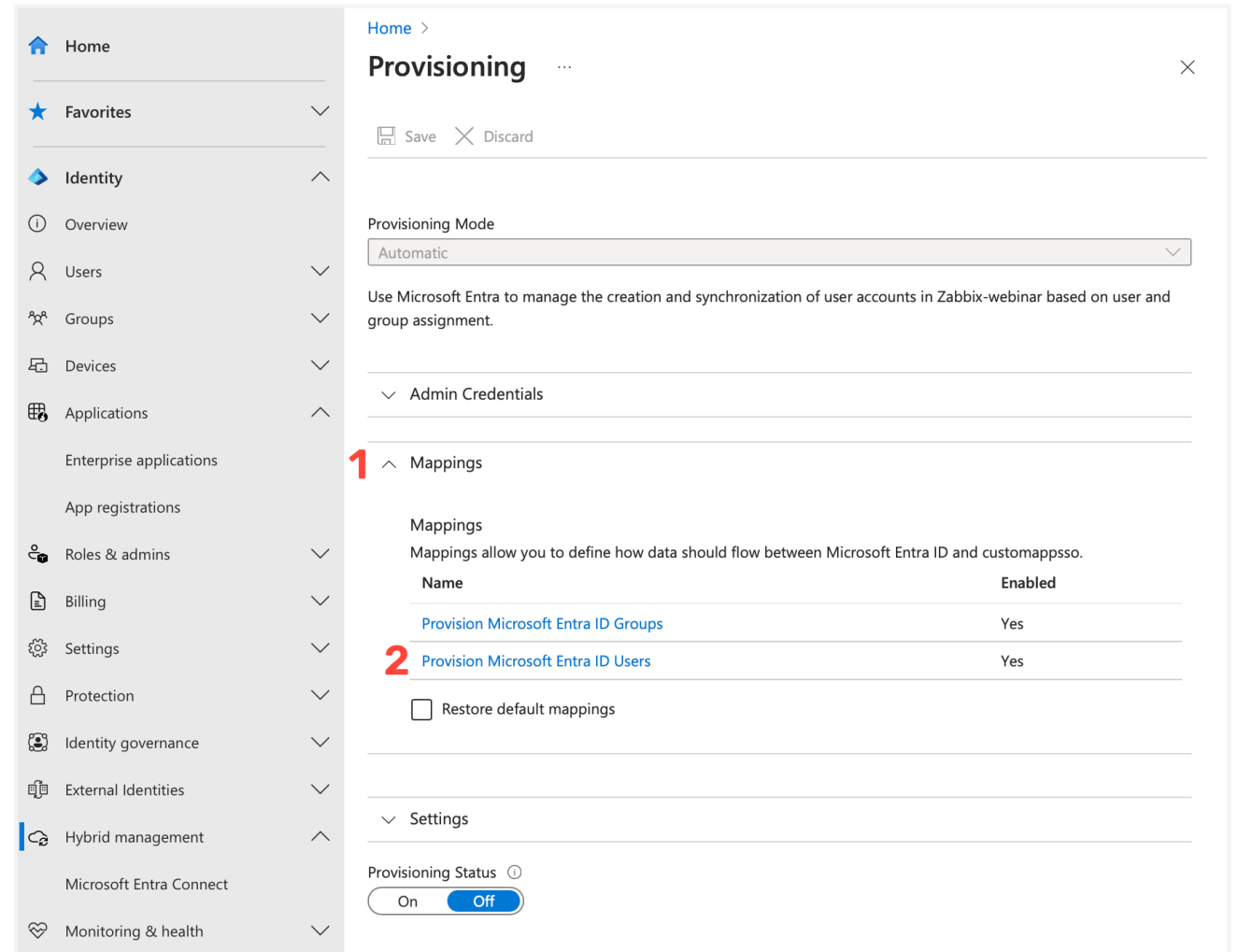
- › From Overview application menu click on “Edit attribute mappings”



The screenshot shows the Zabbix SCIM provisioning interface for the 'Zabbix-webinar' application. The left sidebar contains a navigation menu with items like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Roles & admins, Billing, Settings, and Protection. The main content area is titled 'Zabbix-webinar | Overview' and includes a breadcrumb trail: 'Enterprise applications | All applications > Zabbix-webinar | Provisioning >'. Below the title, there are buttons for 'Start provisioning' and 'Stop provisioning'. The 'Current cycle status' section shows 'Incremental cycle stopped.' and '0% complete'. The 'Statistics to date' section has links for 'View provisioning details' and 'View technical information'. The 'Manage provisioning' section includes links for 'Update credentials', 'Edit attribute mappings', 'Add scoping filters', and 'Provision on demand'. A red '1' highlights the 'Overview' menu item in the sidebar, and a red '2' highlights the 'Edit attribute mappings' link in the 'Manage provisioning' section.

# SCIM – Microsoft Entra

- › Zabbix SCIM provisioning
  - › Expand Mappings
  - › Click on User Mapping



The screenshot shows the Zabbix Provisioning configuration page for Microsoft Entra. The left sidebar contains a navigation menu with items like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, Hybrid management, Microsoft Entra Connect, and Monitoring & health. The main content area is titled 'Provisioning' and includes a 'Provisioning Mode' dropdown set to 'Automatic'. Below this is a description: 'Use Microsoft Entra to manage the creation and synchronization of user accounts in Zabbix-webinar based on user and group assignment.' There is a section for 'Admin Credentials' and a section for 'Mappings' which is expanded. The 'Mappings' section contains a table with two entries: 'Provision Microsoft Entra ID Groups' and 'Provision Microsoft Entra ID Users', both with the 'Enabled' checkbox checked. A red '1' is next to the 'Mappings' section header and a red '2' is next to the 'Provision Microsoft Entra ID Users' row. Below the table is a checkbox for 'Restore default mappings'. At the bottom, there is a 'Provisioning Status' toggle set to 'Off'.

Home >

## Provisioning

Save Discard

Provisioning Mode  
Automatic

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

Admin Credentials

1 Mappings

Mappings allow you to define how data should flow between Microsoft Entra ID and customappsso.

Name	Enabled
<a href="#">Provision Microsoft Entra ID Groups</a>	Yes
2 <a href="#">Provision Microsoft Entra ID Users</a>	Yes

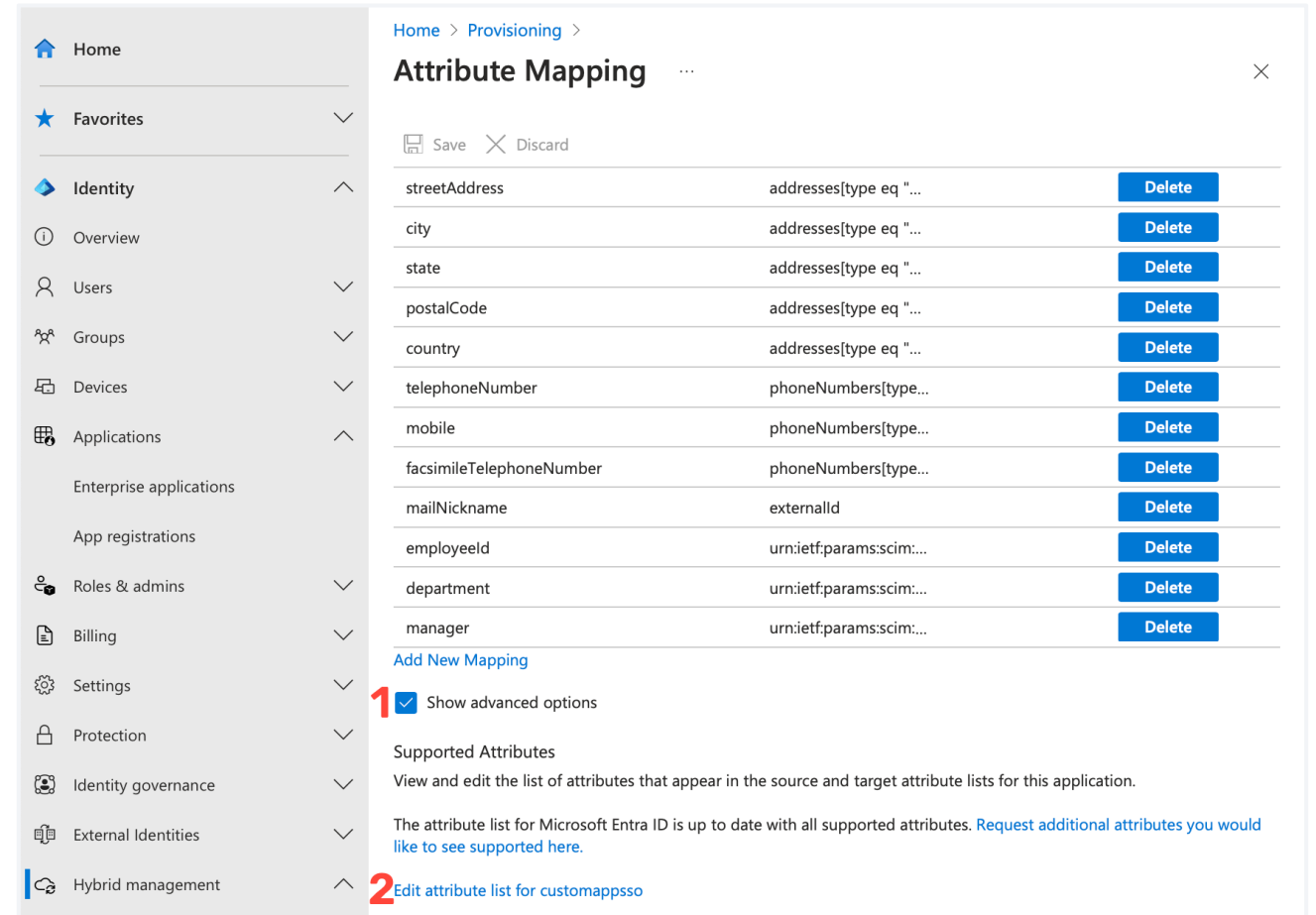
Restore default mappings

Settings

Provisioning Status ⓘ  
On Off

# SCIM – Microsoft Entra

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



The screenshot shows the Zabbix Provisioning interface for Microsoft Entra. The left sidebar contains a navigation menu with items like Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, and Hybrid management. The main content area is titled 'Attribute Mapping' and includes a table of mappings, a 'Show advanced options' checkbox, and a section for 'Supported Attributes'.

Home > Provisioning > Attribute Mapping

Save Discard

streetAddress	addresses[type eq "...	Delete
city	addresses[type eq "...	Delete
state	addresses[type eq "...	Delete
postalCode	addresses[type eq "...	Delete
country	addresses[type eq "...	Delete
telephoneNumber	phoneNumbers[type...	Delete
mobile	phoneNumbers[type...	Delete
facsimileTelephoneNumber	phoneNumbers[type...	Delete
mailNickname	externalId	Delete
employeeId	urn:ietf:params:scim:...	Delete
department	urn:ietf:params:scim:...	Delete
manager	urn:ietf:params:scim:...	Delete

**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 Microsoft Entra ID is up to date with all supported attributes. [Request additional attributes you would like to see supported here.](#)

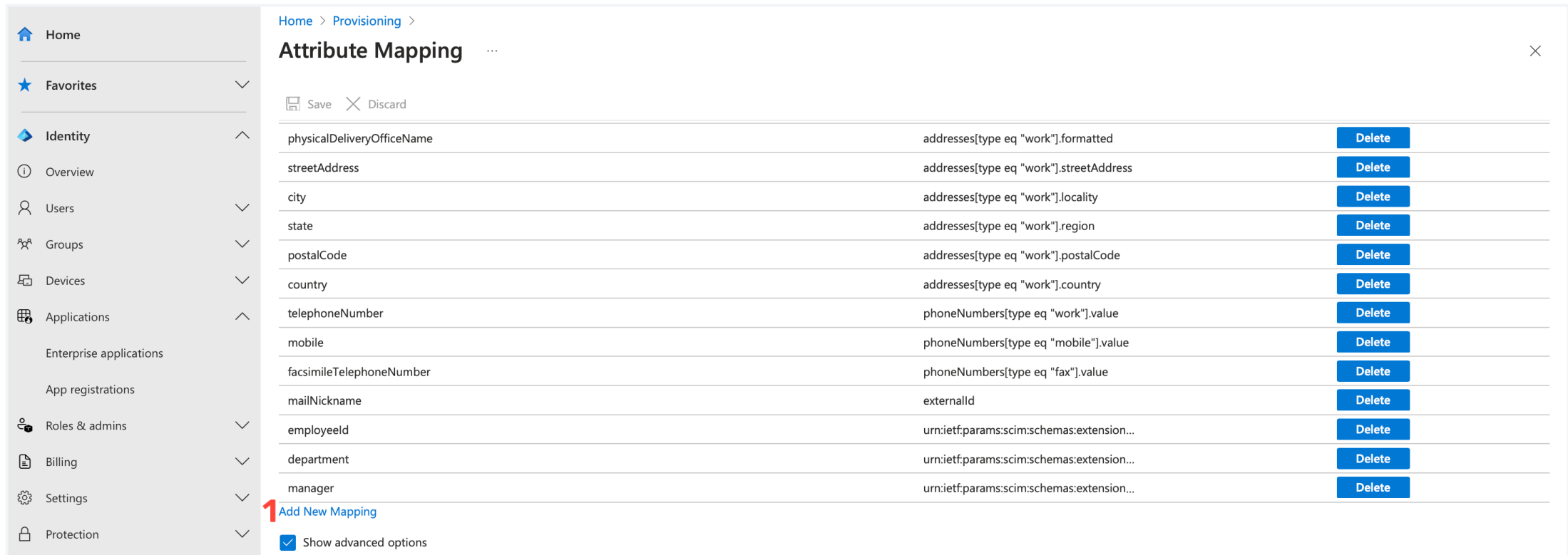
**2** [Edit attribute list for customappsso](#)



## Zabbix User Provisioning JIT

# SCIM – Microsoft Entra

- › Zabbix SCIM provisioning
  - › Next step is to add our custom attributes in Attributes Mapping



The screenshot displays the Zabbix SCIM provisioning interface, specifically the 'Attribute Mapping' configuration page. The left sidebar contains navigation options: Home, Favorites, Identity, Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Roles & admins, Billing, Settings, and Protection. The main content area shows the breadcrumb 'Home > Provisioning > Attribute Mapping' and a close button. Below the breadcrumb are 'Save' and 'Discard' buttons. The main table lists various attributes and their corresponding SCIM paths, with a 'Delete' button for each row. A red '1' icon and the text 'Add New Mapping' are visible at the bottom left of the table area. The 'Show advanced options' checkbox is checked.

Attribute	SCIM Path	Action
physicalDeliveryOfficeName	addresses[type eq "work"].formatted	Delete
streetAddress	addresses[type eq "work"].streetAddress	Delete
city	addresses[type eq "work"].locality	Delete
state	addresses[type eq "work"].region	Delete
postalCode	addresses[type eq "work"].postalCode	Delete
country	addresses[type eq "work"].country	Delete
telephoneNumber	phoneNumbers[type eq "work"].value	Delete
mobile	phoneNumbers[type eq "mobile"].value	Delete
facsimileTelephoneNumber	phoneNumbers[type eq "fax"].value	Delete
mailNickname	externalId	Delete
employeeid	urn:ietf:params:scim:schemas:extension...	Delete
department	urn:ietf:params:scim:schemas:extension...	Delete
manager	urn:ietf:params:scim:schemas:extension...	Delete

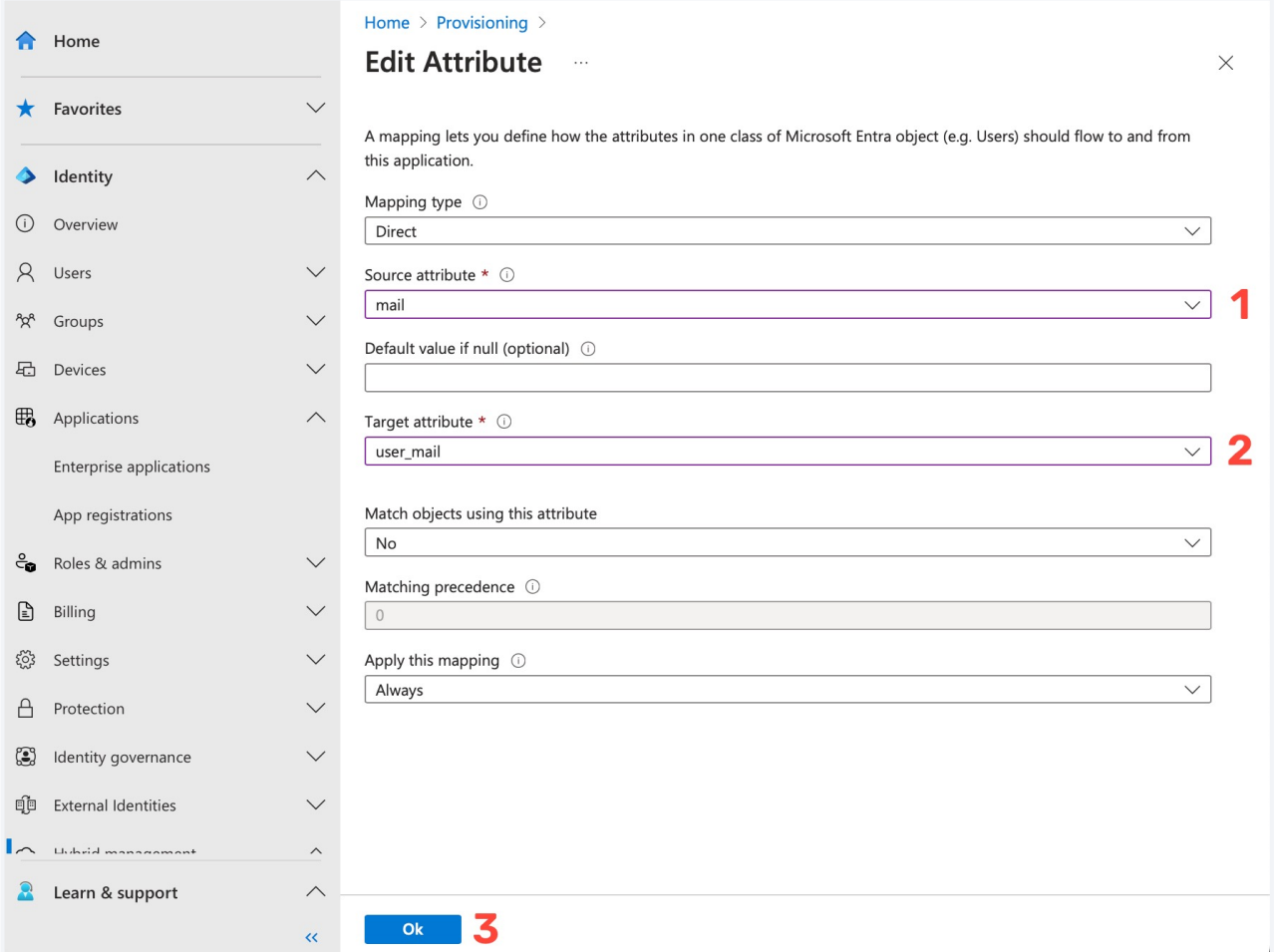
**1** Add New Mapping

Show advanced options



# SCIM – Microsoft Entra

- › Zabbix SCIM provisioning
  - › Add our custom attributes
  - › user\_mail
  - › user\_mobile
  - › user\_name
  - › user\_lastname
  - › user\_pushover



Home > Provisioning >

## Edit Attribute

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

Mapping type <sup>ⓘ</sup>  
Direct

Source attribute \* <sup>ⓘ</sup>  
mail **1**

Default value if null (optional) <sup>ⓘ</sup>

Target attribute \* <sup>ⓘ</sup>  
user\_mail **2**

Match objects using this attribute  
No

Matching precedence <sup>ⓘ</sup>  
0

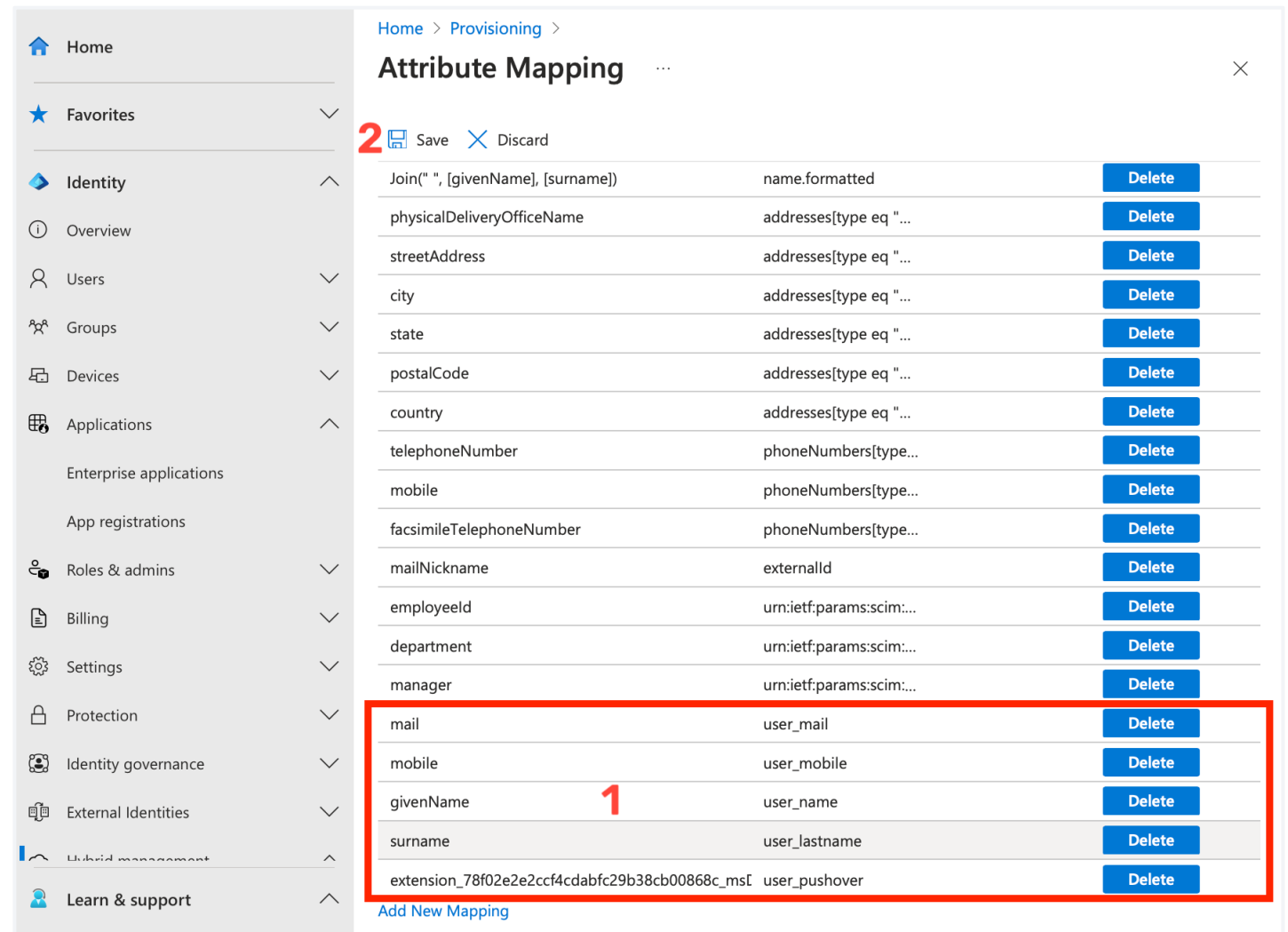
Apply this mapping <sup>ⓘ</sup>  
Always

Ok **3**

## Zabbix User Provisioning JIT

# SCIM – Microsoft Entra

- ▶ Zabbix SCIM provisioning
  - ▶ Add all our custom attributes and save settings



Home > Provisioning > Attribute Mapping

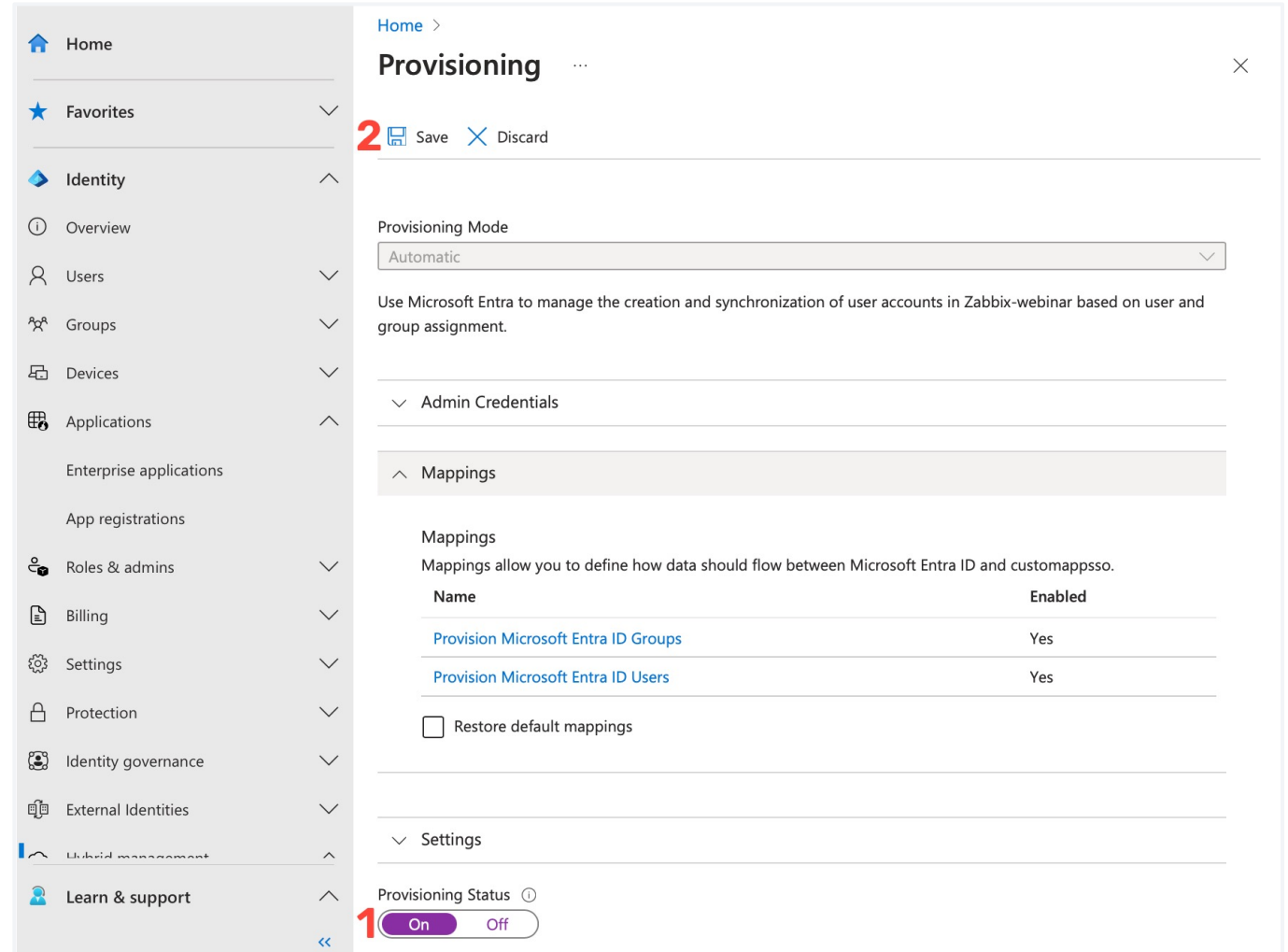
2 Save Discard

Join(" ", [givenName], [surname])	name.formatted	Delete
physicalDeliveryOfficeName	addresses[type eq "...	Delete
streetAddress	addresses[type eq "...	Delete
city	addresses[type eq "...	Delete
state	addresses[type eq "...	Delete
postalCode	addresses[type eq "...	Delete
country	addresses[type eq "...	Delete
telephoneNumber	phoneNumbers[type...	Delete
mobile	phoneNumbers[type...	Delete
facsimileTelephoneNumber	phoneNumbers[type...	Delete
mailNickname	externalId	Delete
employeeId	urn:ietf:params:scim:...	Delete
department	urn:ietf:params:scim:...	Delete
manager	urn:ietf:params:scim:...	Delete
mail	user_mail	Delete
mobile	user_mobile	Delete
givenName	user_name	Delete
surname	user_lastname	Delete
extension_78f02e2e2ccf4cdabfc29b38cb00868c_msI	user_pushover	Delete

Add New Mapping

# SCIM – Microsoft Entra

- ▶ Zabbix SCIM provisioning
  - ▶ Enable provisioning



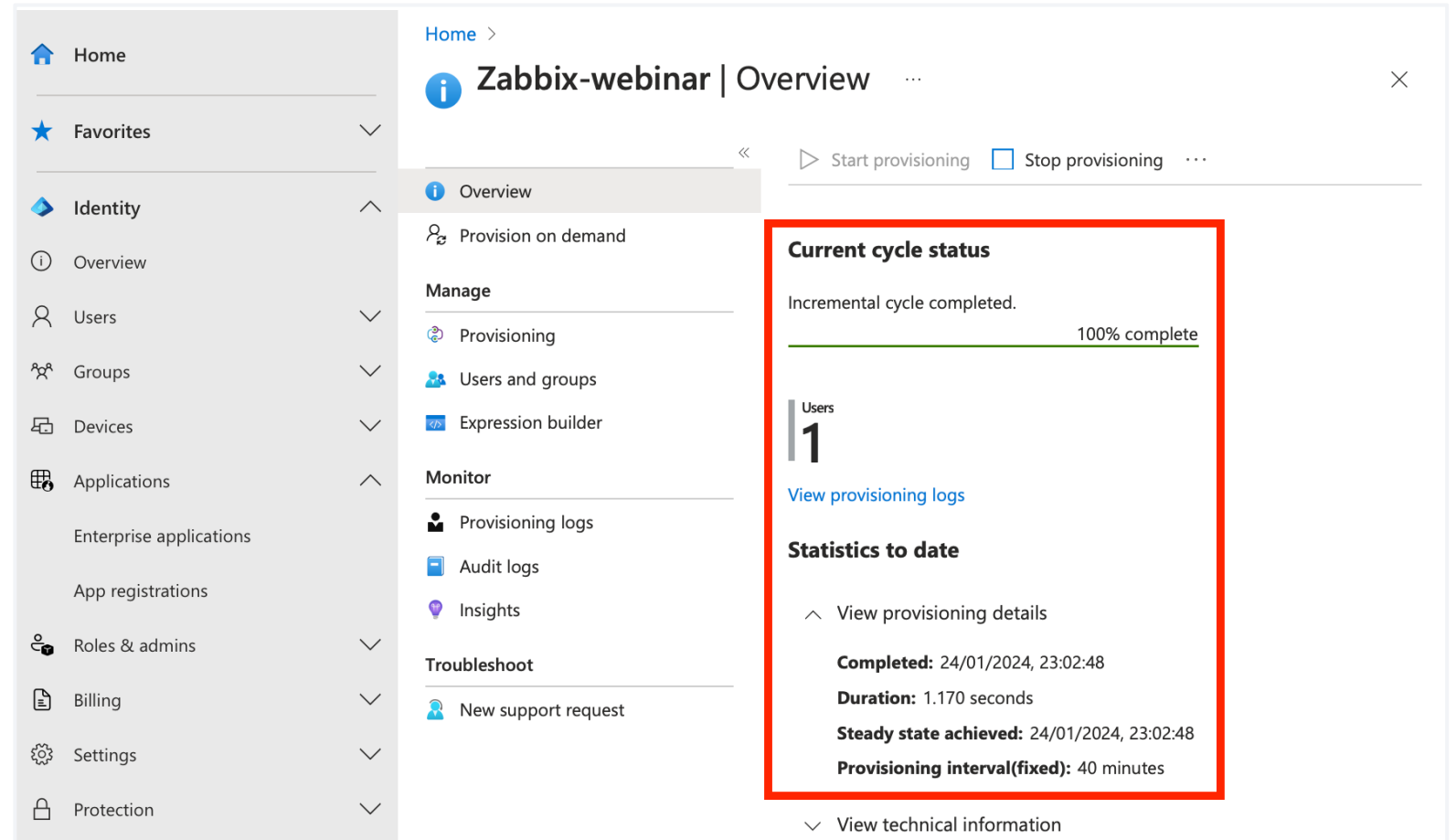
The screenshot shows the Zabbix Provisioning configuration interface for Microsoft Entra. The left sidebar contains navigation options: Home, Favorites, Identity (selected), Overview, Users, Groups, Devices, Applications, Enterprise applications, App registrations, Roles & admins, Billing, Settings, Protection, Identity governance, External Identities, Hybrid management, and Learn & support. The main content area is titled "Provisioning" and includes a "2 Save Discard" button. The "Provisioning Mode" is set to "Automatic". A description states: "Use Microsoft Entra to manage the creation and synchronization of user accounts in Zabbix-webinar based on user and group assignment." Below this, there are sections for "Admin Credentials" and "Mappings". The "Mappings" section contains a table with two entries:

Name	Enabled
<a href="#">Provision Microsoft Entra ID Groups</a>	Yes
<a href="#">Provision Microsoft Entra ID Users</a>	Yes

There is also a checkbox for "Restore default mappings" which is currently unchecked. At the bottom, the "Provisioning Status" is shown as "On" (indicated by a red '1' and a purple toggle switch).

# SCIM – Microsoft Entra

- ▶ Zabbix SCIM provisioning
  - ▶ Status can be found in application Overview



The screenshot shows the Zabbix SCIM provisioning overview page for 'Zabbix-webinar'. The left sidebar contains navigation options: Home, Favorites, Identity (expanded), Overview, Users, Groups, Devices, Applications (Enterprise applications, App registrations), Roles & admins, Billing, Settings, and Protection. The main content area is titled 'Zabbix-webinar | Overview' and includes a 'Start provisioning' button and a 'Stop provisioning' button. The 'Overview' tab is active, showing 'Provision on demand' and 'Manage' sections (Provisioning, Users and groups, Expression builder). The 'Monitor' section includes Provisioning logs, Audit logs, and Insights. The 'Troubleshoot' section includes a 'New support request' button. A red box highlights the 'Current cycle status' section, which displays 'Incremental cycle completed.' with a progress bar at '100% complete'. Below this, a 'Users' counter shows '1' and a 'View provisioning logs' link. The 'Statistics to date' section includes 'View provisioning details' and the following metrics: **Completed:** 24/01/2024, 23:02:48; **Duration:** 1.170 seconds; **Steady state achieved:** 24/01/2024, 23:02:48; **Provisioning interval(fixed):** 40 minutes. A 'View technical information' link is also present at the bottom.

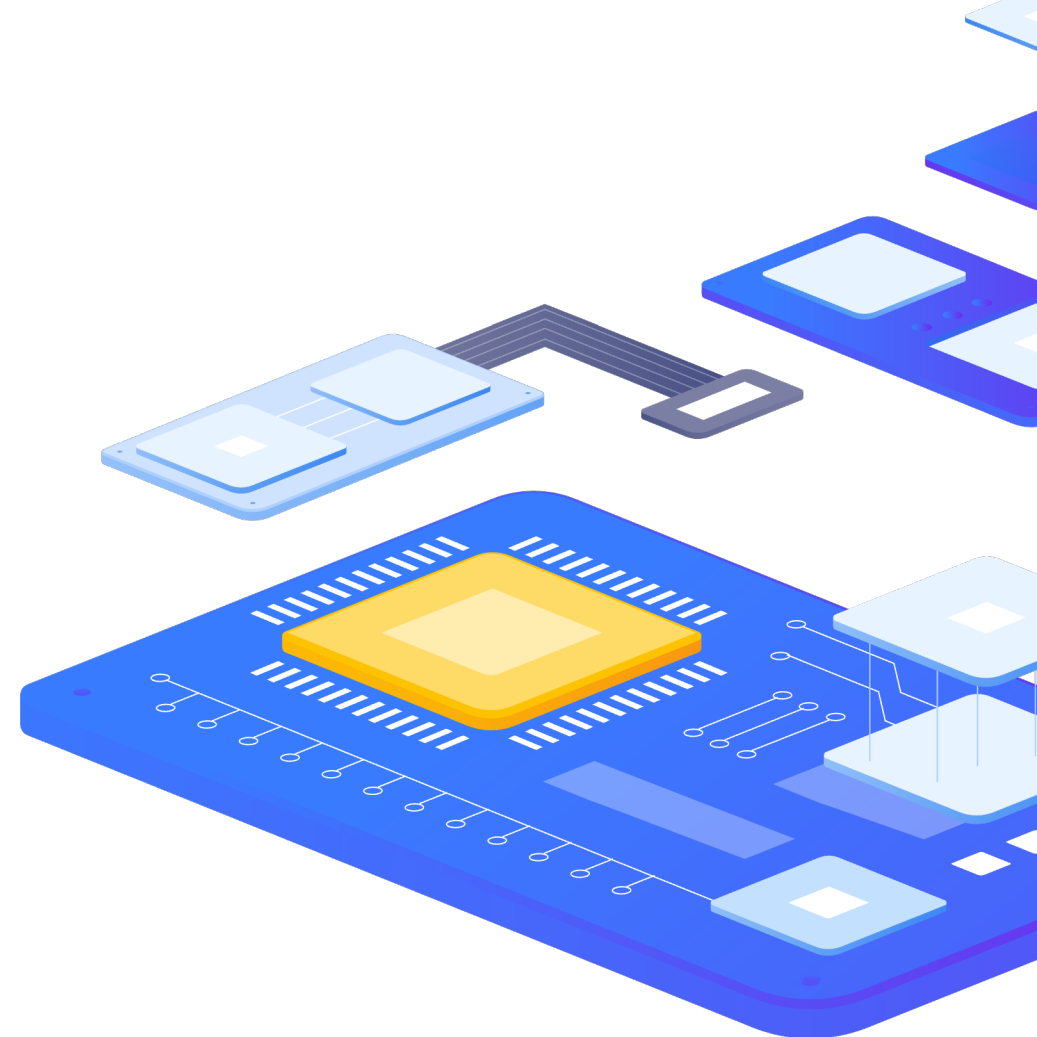
6

Issues and limitations



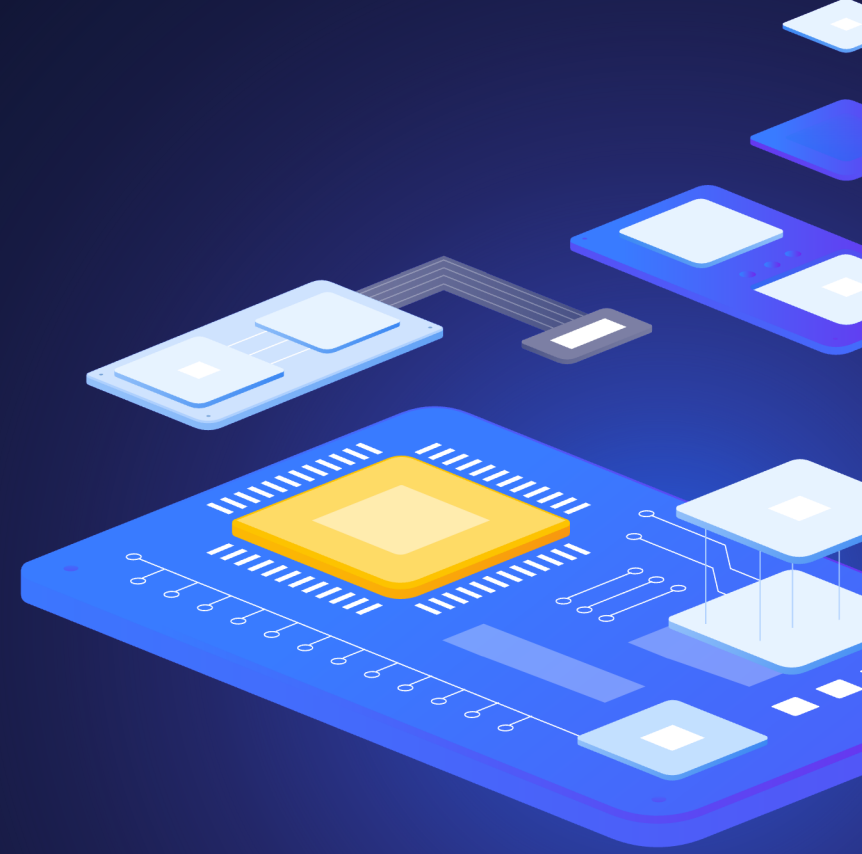
# Issues and limitations

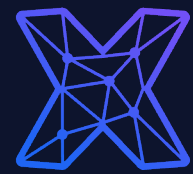
- › Manually created user cannot be provisioned (workaround is use alter table for this specific user)
- › You are not be able to change some user setting after provisioning (media, role, groups)  
<https://support.zabbix.com/browse/ZBXNEXT-8760>  
(it be fixed soon)
- › Zabbix have bug with user groups – user groups can be assigned via user groups  
<https://support.zabbix.com/browse/ZBX-23884>
- › SAML IdP certificate is not accepted, if comments are present  
<https://github.com/SAML-Toolkits/php-saml/issues/572>  
(Not a Zabbix bug)
- › SCIM have a lot of issues
- › Zabbix have public Security Advisories  
[https://www.zabbix.com/security\\_advisories](https://www.zabbix.com/security_advisories)



7

DEMO





initMAX

Questions?





# Contact us:

Phone:



+420 800 244 442

Web:



<https://www.initmax.cz>

Email:



[tomas.hermanek@initmax.cz](mailto:tomas.hermanek@initmax.cz)

LinkedIn:



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

Twitter:



<https://twitter.com/initmax>

Tomáš Heřmánek:



+420 732 447 184