initMAX

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**dentity **M**anagement is a standard for automating the exchange of user identity information between identity domains, or IT systems

2

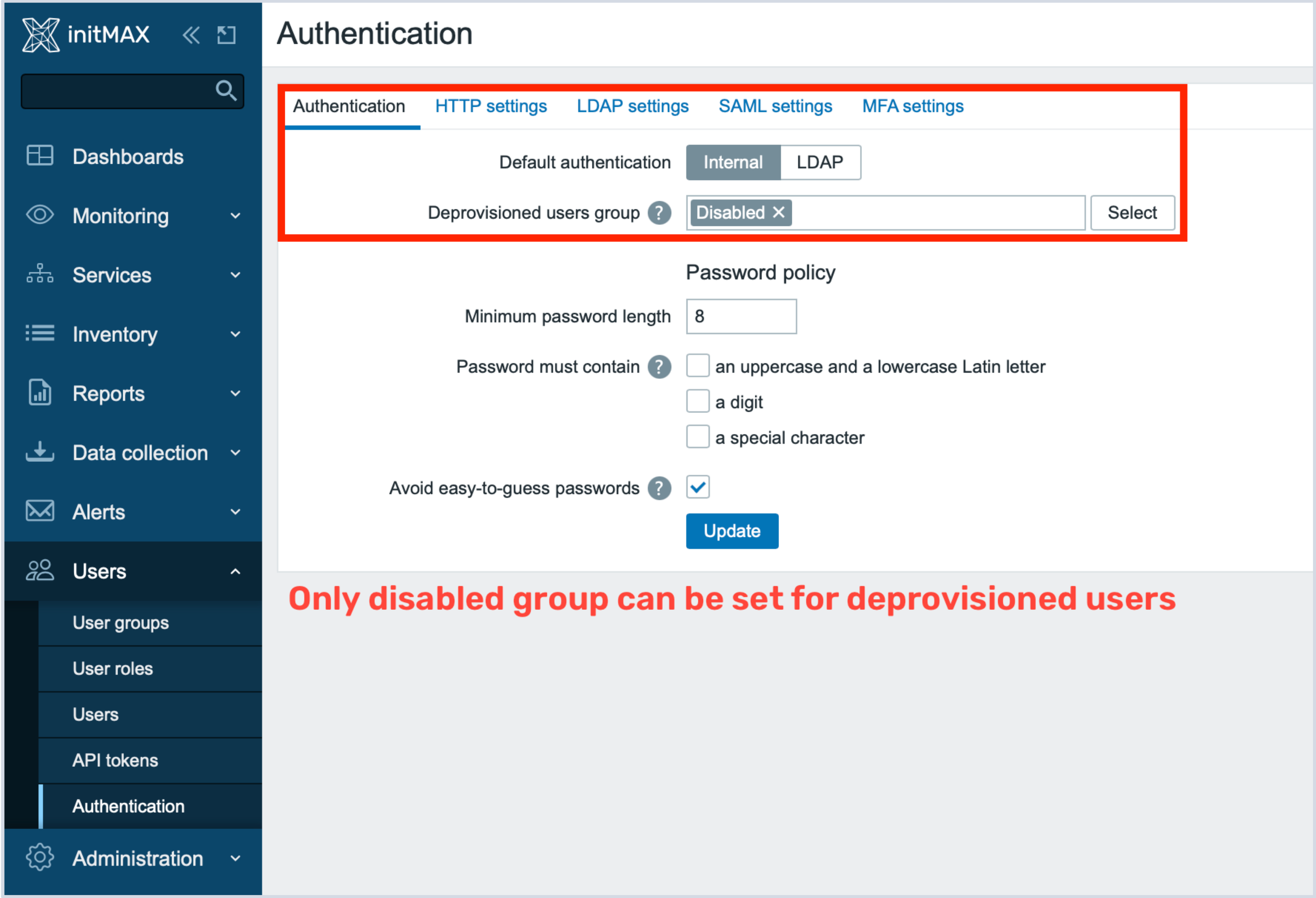
Available authentication options in ZABBIX

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)**

Zabbix User Provisioning JIT

Available authentication options in ZABBIX



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

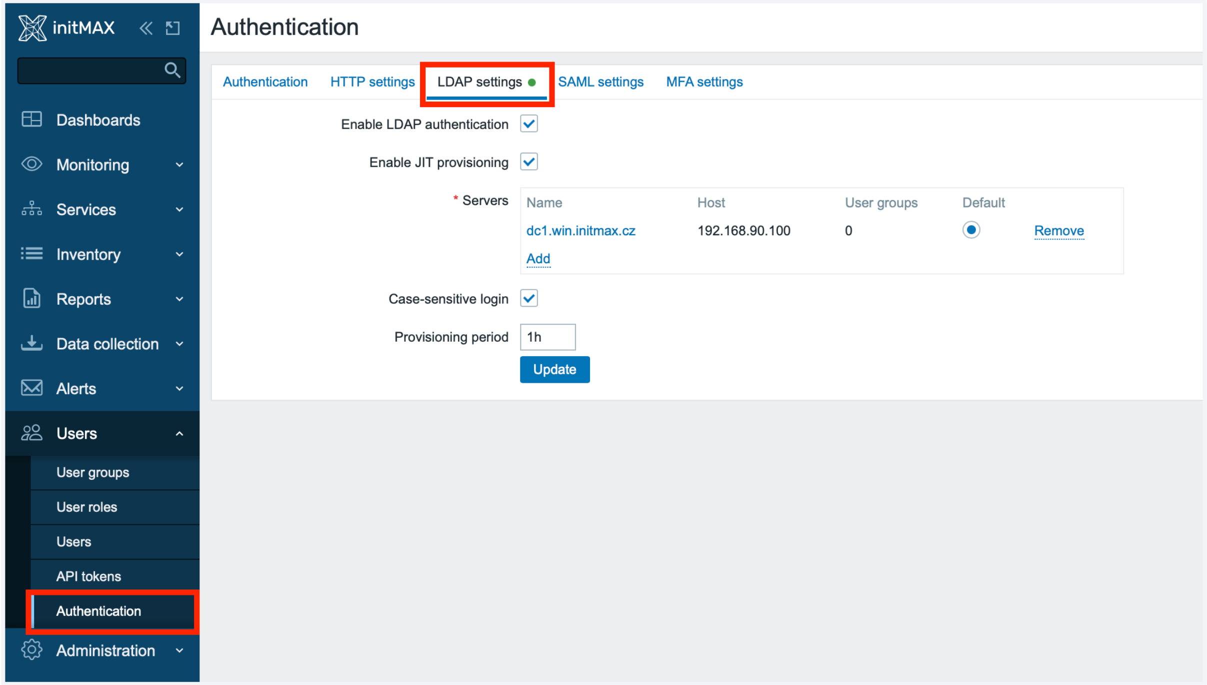
LDAP

- 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.



Authentication

Enable LDAP authentication ☑

Enable JIT provisioning ☑

* Servers

Name	Host	User groups	Default	
dc1.win.initmax.cz	192.168.90.100	0	●	Remove
Add				

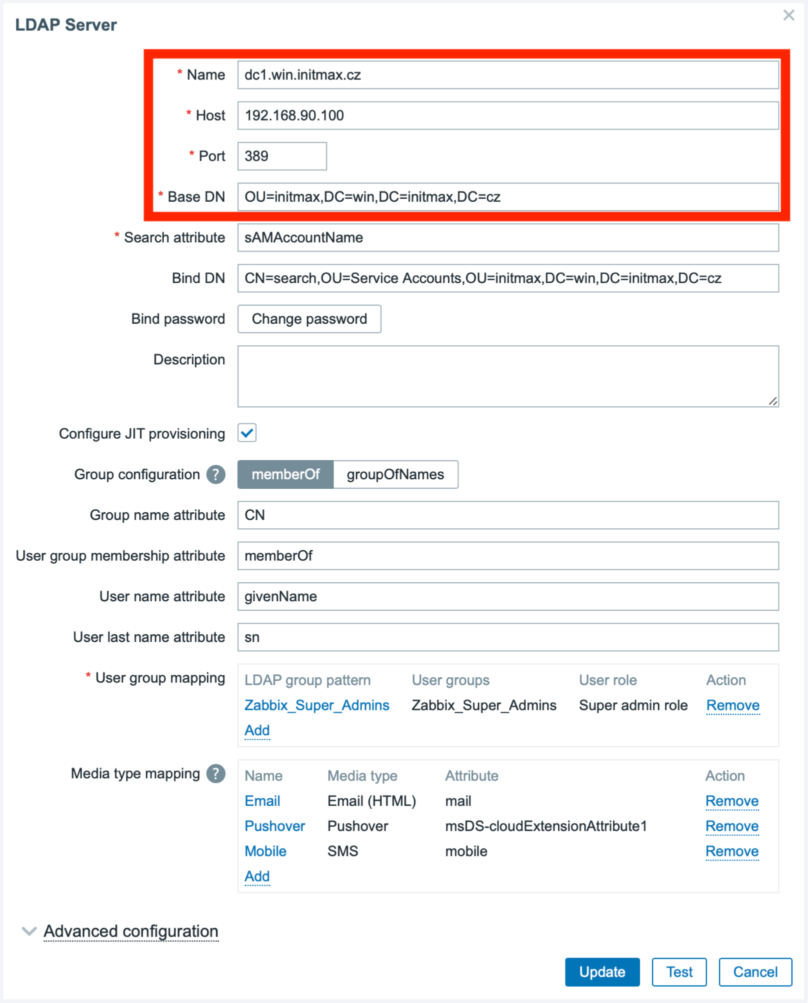
Case-sensitive login ☑

Provisioning period 1h

Zabbix User Provisioning JIT

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	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	Remove
Add			

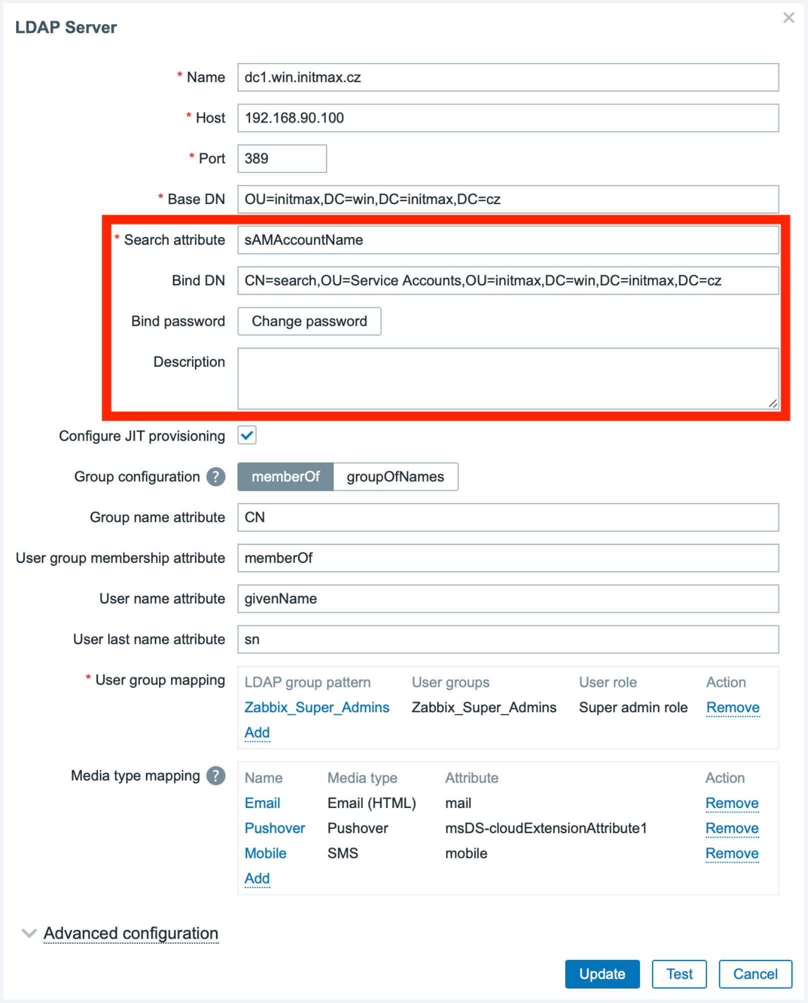
Media type mapping ?

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

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	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	Remove
Add			

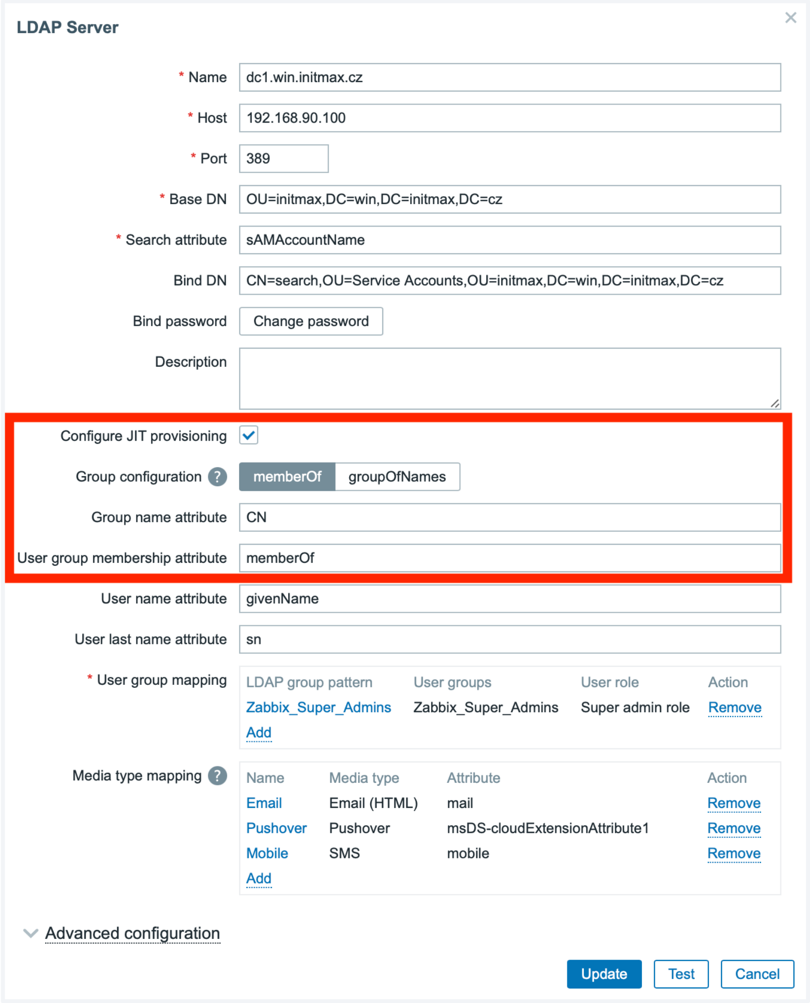
Media type mapping

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

Zabbix User Provisioning JIT

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	Remove
Add			

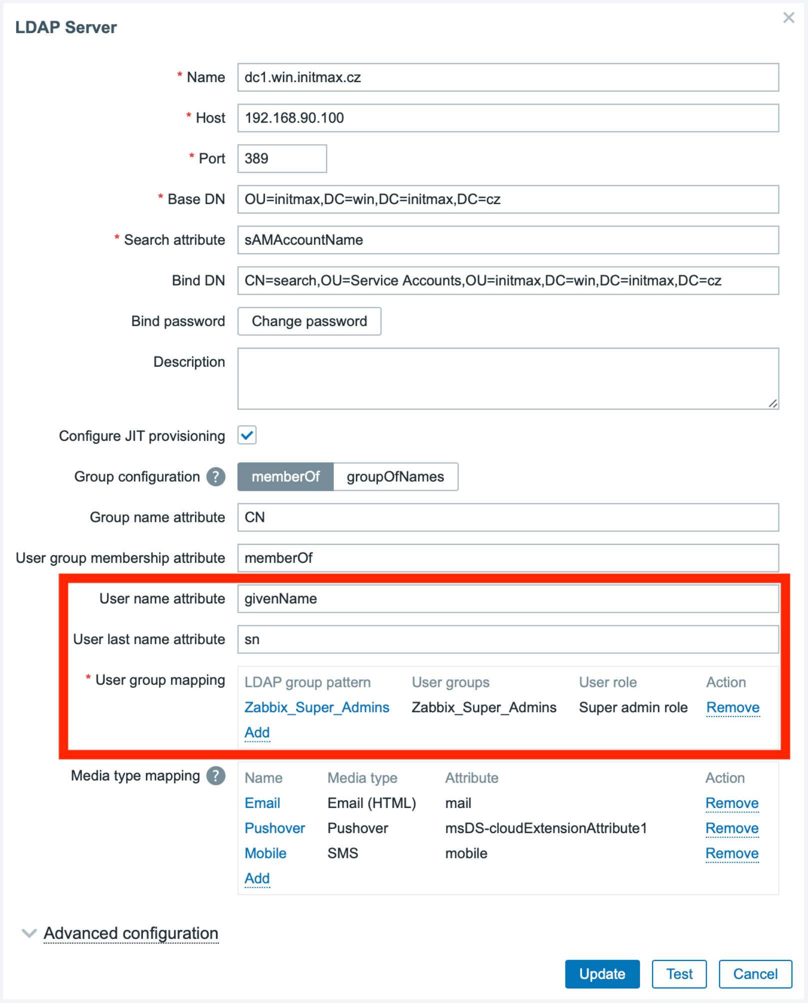
Media type mapping ?

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

Zabbix User Provisioning JIT

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	Remove
Add			

Media type mapping ?

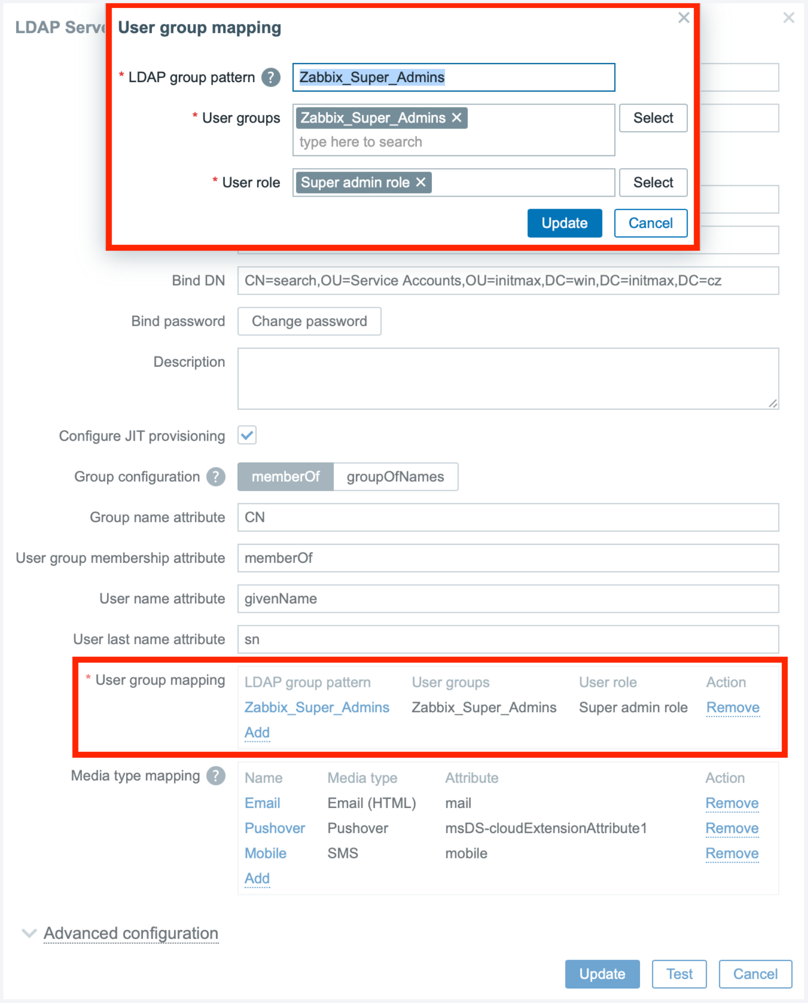
Name	Media type	Attribute	Action
Email	Email (HTML)	mail	Remove
Pushover	Pushover	msDS-cloudExtensionAttribute1	Remove
Mobile	SMS	mobile	Remove
Add			

Zabbix User Provisioning JIT

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



LDAP Serv

User group mapping

* LDAP group pattern: Zabbix_Super_Admins

* User groups: Zabbix_Super_Admins ✕ — type here to search — Select

* User role: Super admin role ✕ — Select

Update | Cancel

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	Remove
Add			

Media type mapping

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

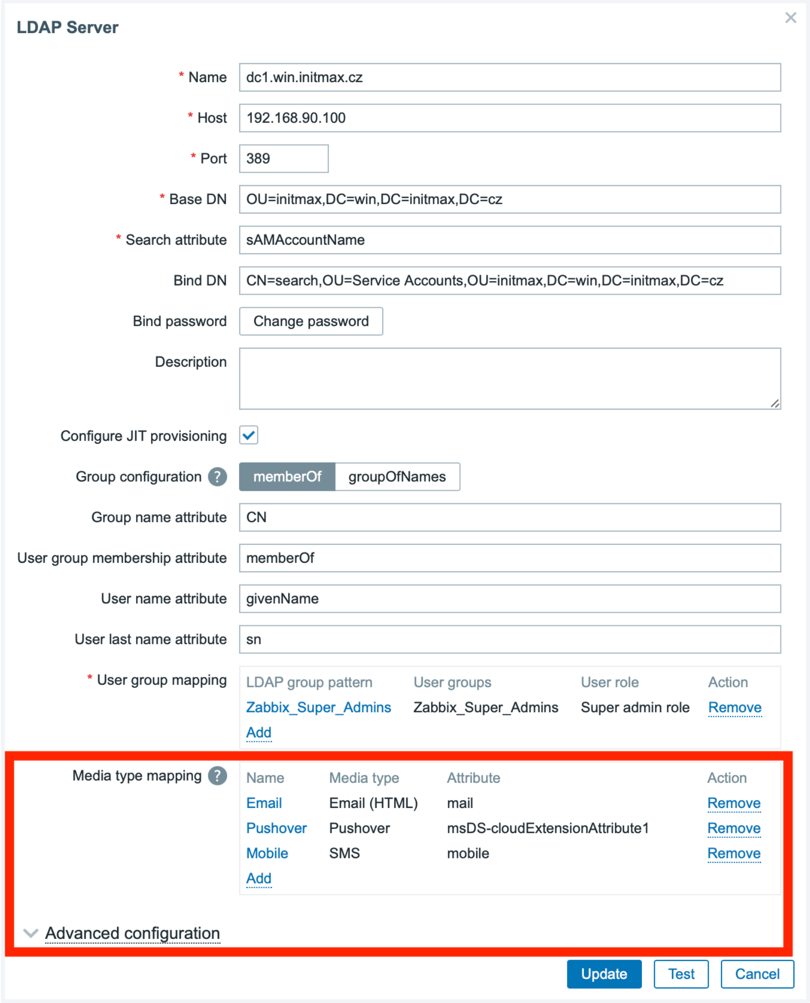
Advanced configuration

Update | Test | Cancel

Zabbix User Provisioning JIT

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	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	Remove
Add			

Media type mapping

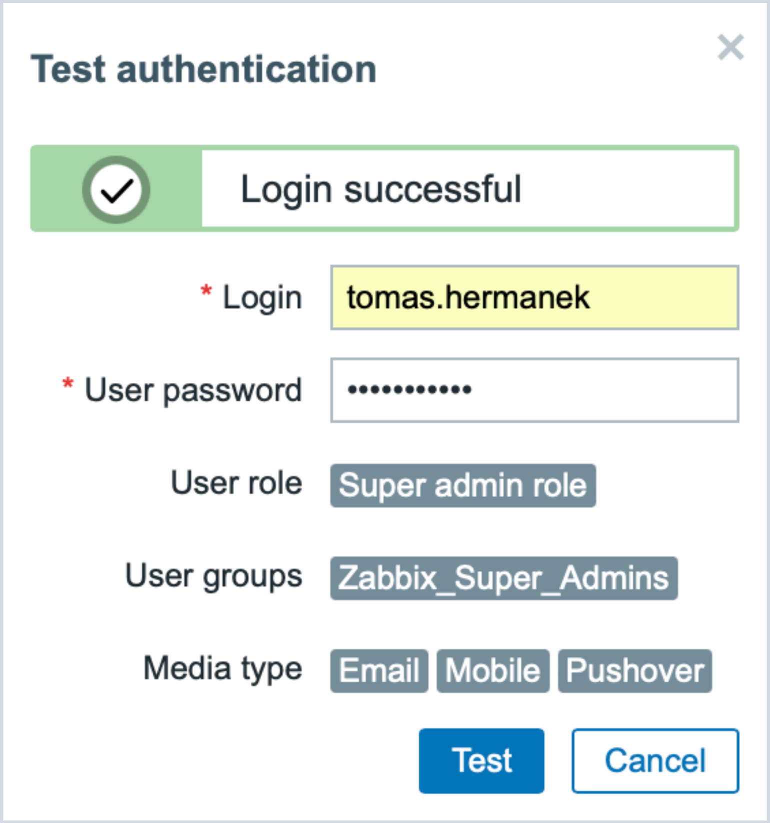
Name	Media type	Attribute	Action
Email	Email (HTML)	mail	Remove
Pushover	Pushover	msDS-cloudExtensionAttribute1	Remove
Mobile	SMS	mobile	Remove
Add			

Advanced configuration

Zabbix User Provisioning JIT

LDAP – Notes

- The Test button allows to test user access



Test authentication

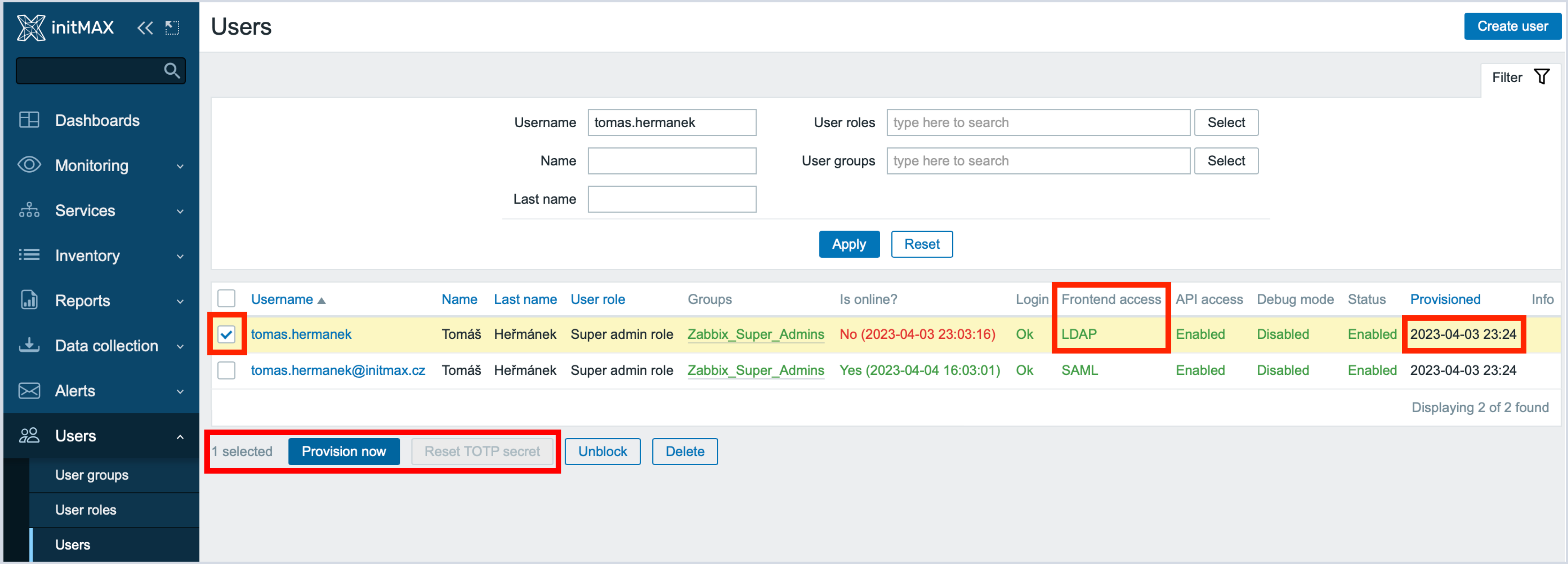
✓ Login successful

* Login	tomas.hermanek
* User password	••••••••••••
User role	Super admin role
User groups	Zabbix_Super_Admins
Media type	Email Mobile Pushover

Zabbix User Provisioning JIT

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)



Users

Username: tomas.hermanek

Name:

Last name:

User roles: type here to search

User groups: type here to search

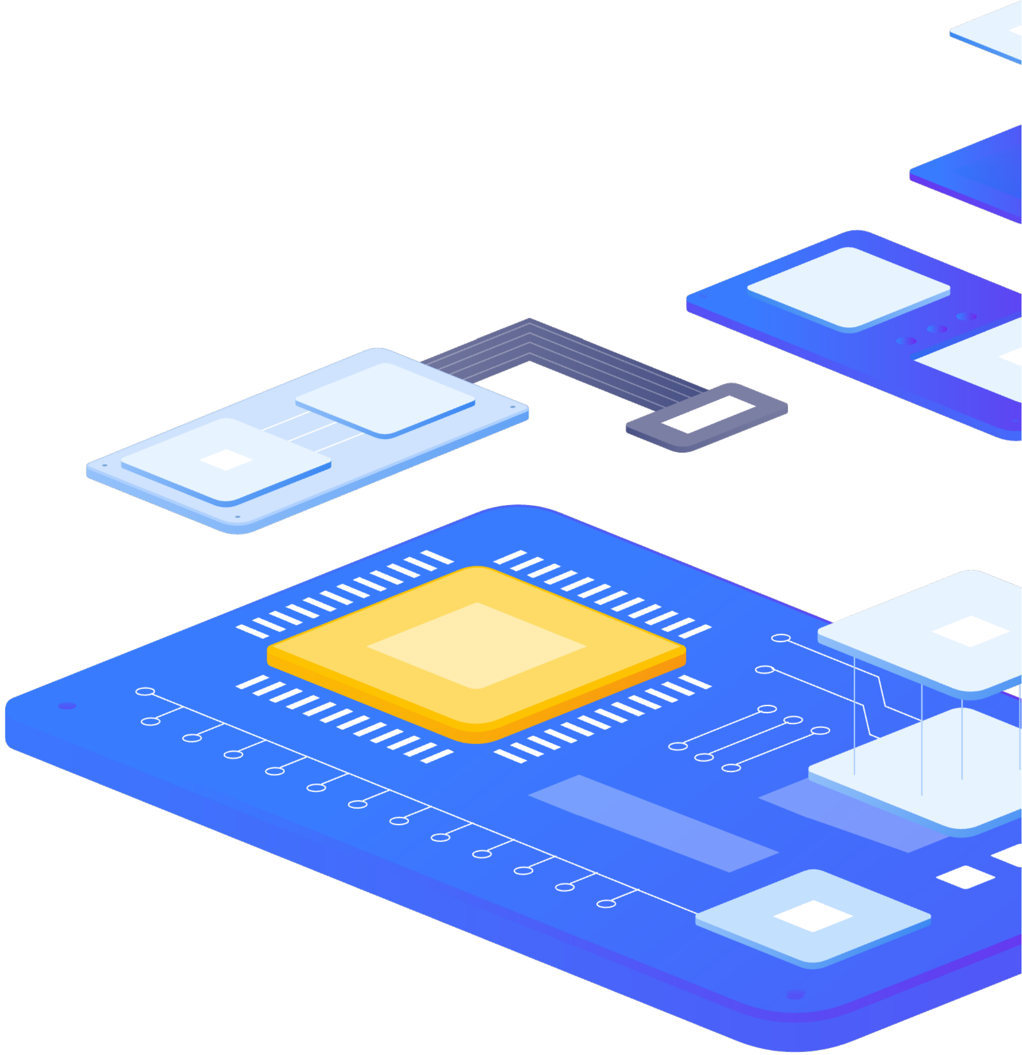
☐	Username ▲	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	Provisioned	Info
☑	tomas.hermanek	Tomáš	Heřmánek	Super admin role	Zabbix_Super_Admins	No (2023-04-03 23:03:16)	Ok	LDAP	Enabled	Disabled	Enabled	2023-04-03 23:24	
☐	tomas.hermanek@initmax.cz	Tomáš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

Displaying 2 of 2 found

Zabbix User Provisioning JIT

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

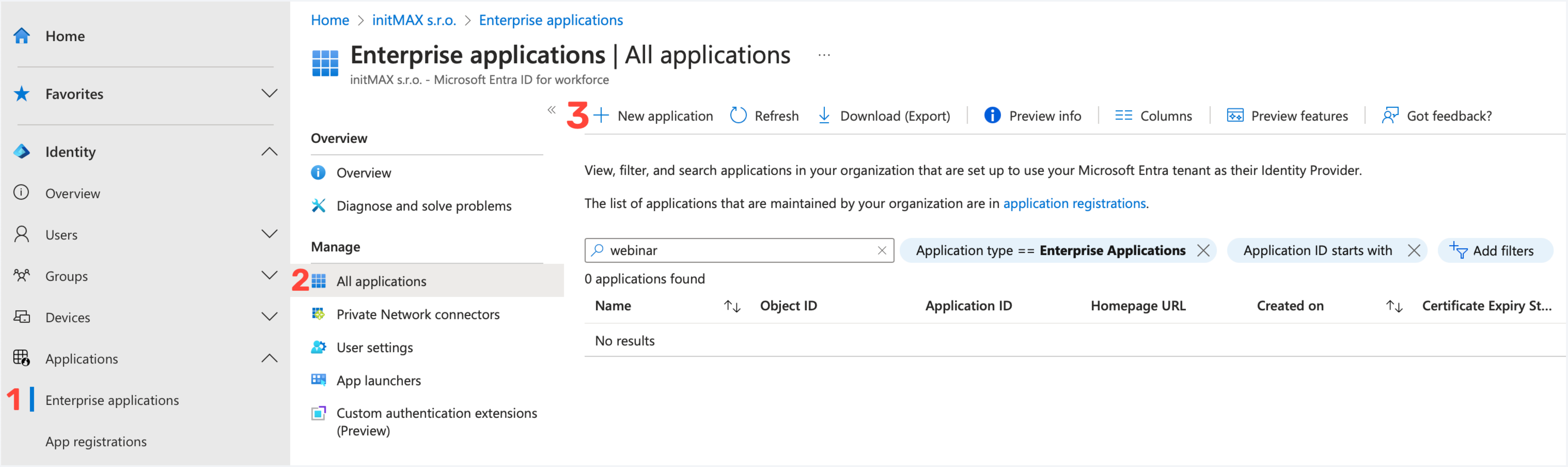
- SAML authentication can be used for Single Sign On authentication
- If only SAML sign-in is configured, then the user must also exist in Zabbix, however, its Zabbix password will not be used. If authentication is successful, then Zabbix will match a local username with the username attribute returned by SAML
- You can define only one SAML authentication provider
- You can use 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)

initMAX

Zabbix User Provisioning JIT

SAML – Zabbix - Microsoft Entra

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



Home > initMAX s.r.o. > Enterprise applications

Enterprise applications | All applications

initMAX s.r.o. - Microsoft Entra ID for workforce

View, filter, and search applications in your organization that are set up to use your Microsoft Entra 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

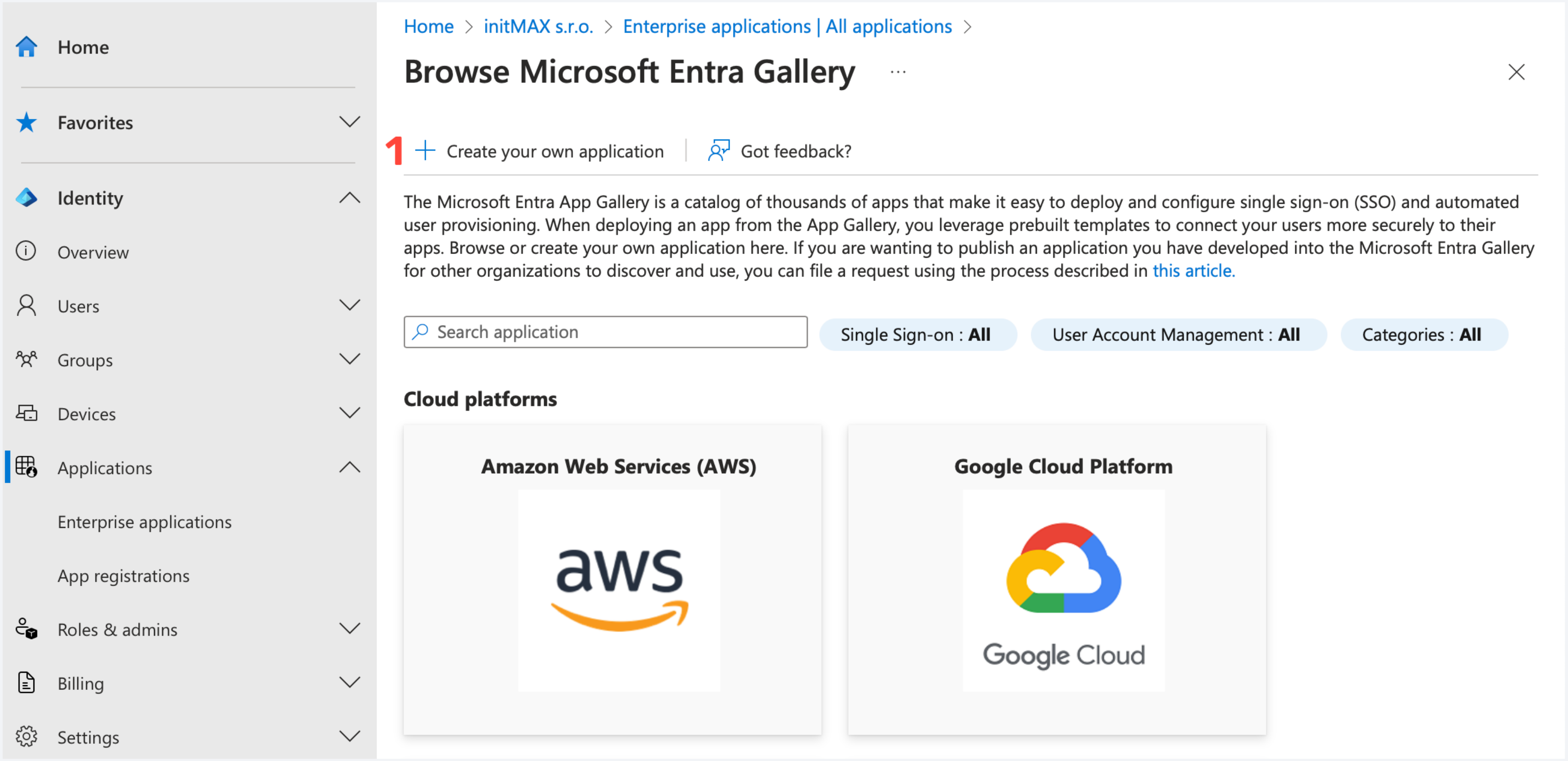
0 applications found

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

Zabbix User Provisioning JIT

SAML – Zabbix – Microsoft Entra

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

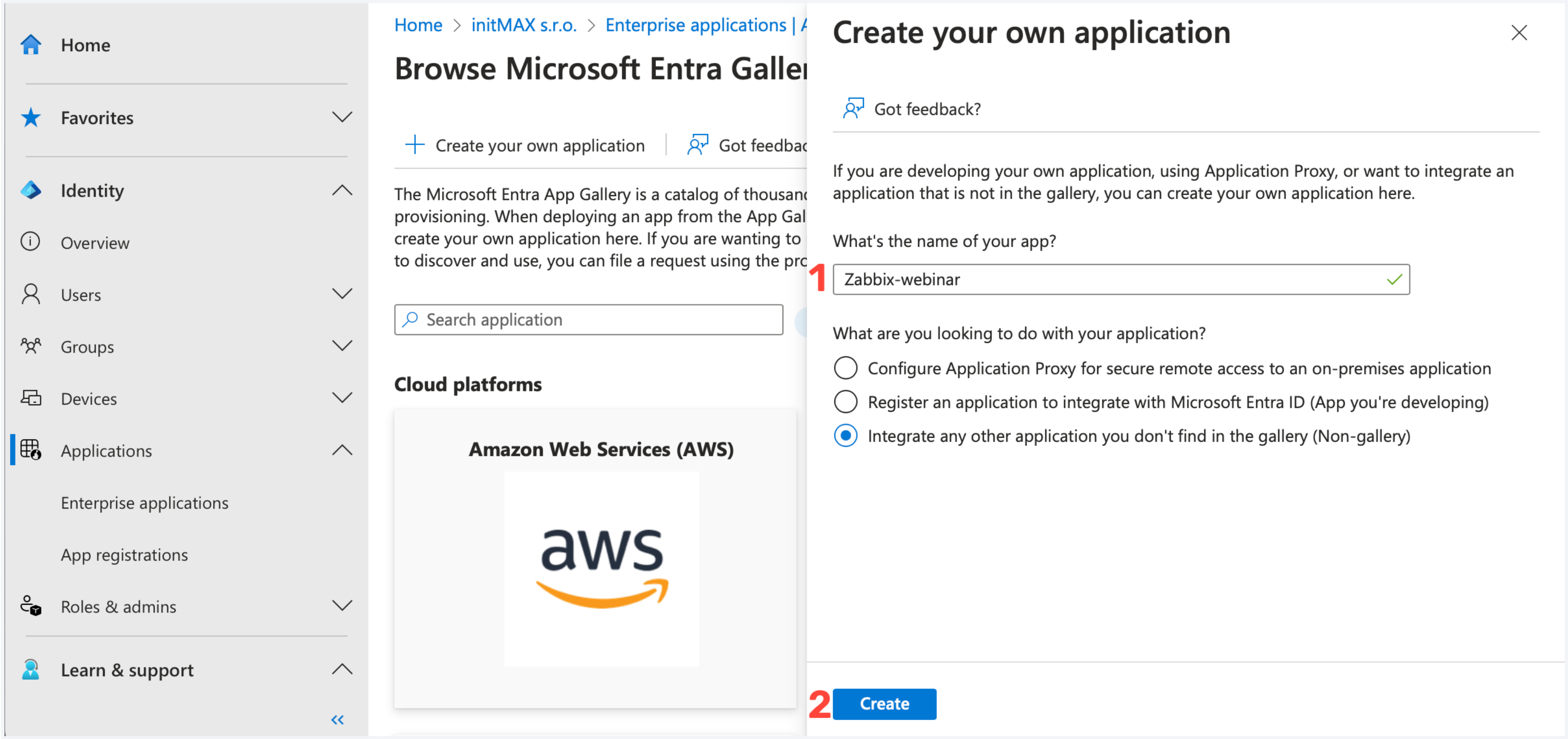


The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, you leverage prebuilt templates to connect your users more securely to their apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Gallery for other organizations to discover and use, you can file a request using the process described in this article.

Zabbix User Provisioning JIT

SAML – Zabbix - Microsoft Entra

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



The Microsoft Entra App Gallery is a catalog of thousanc provisioning. When deploying an app from the App Gal create your own application here. If you are wanting to to discover and use, you can file a request using the prc

Create your own application

Got feedback?

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.

What's the name of your app?

1 Zabbix-webinar ✓

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 Microsoft Entra ID (App you're developing)

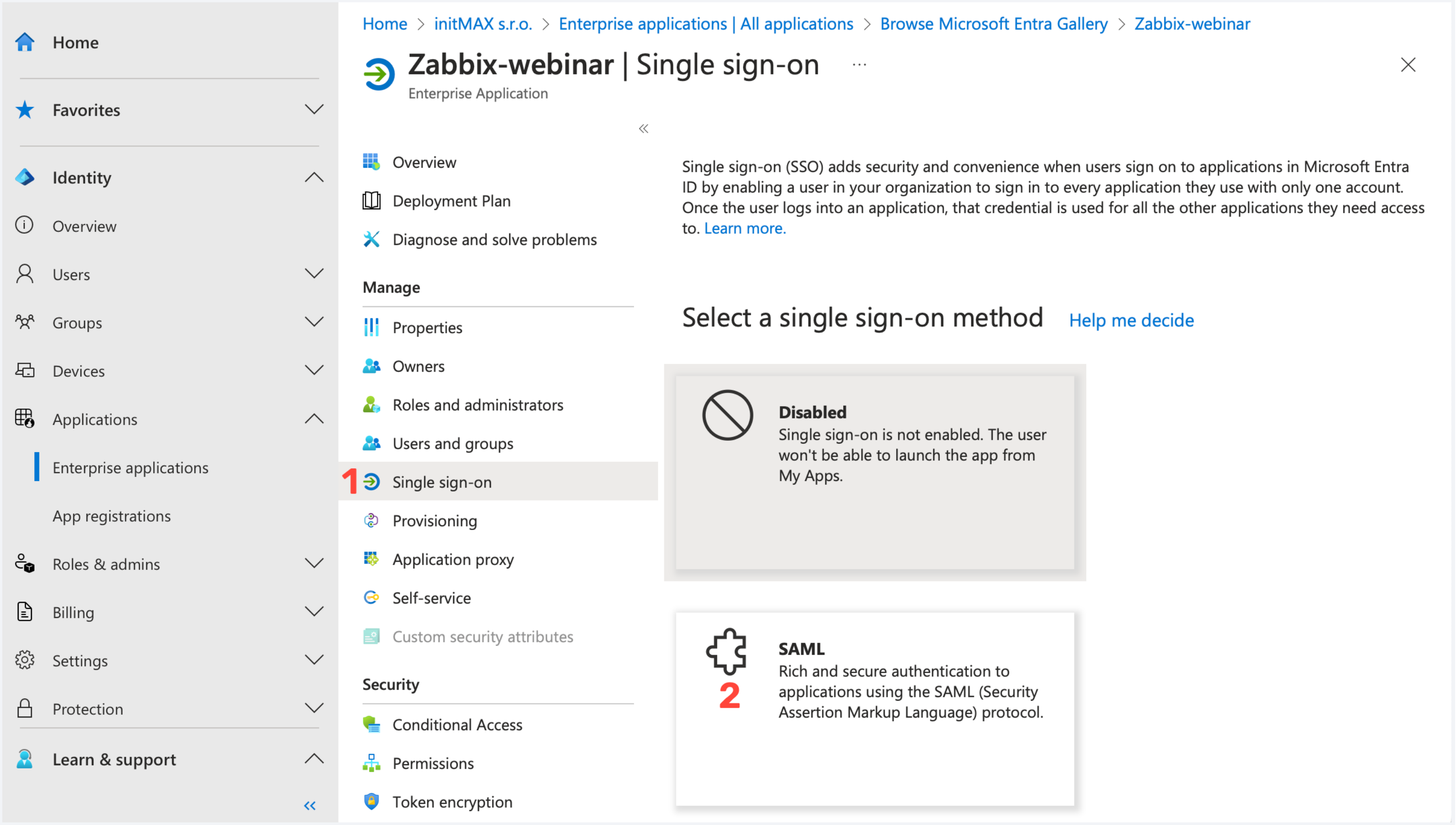
● Integrate any other application you don't find in the gallery (Non-gallery)

2 Create

Zabbix User Provisioning JIT

SAML – Zabbix - Microsoft Entra

- Single sign-on setting
  - Select SAML as a sign-on metod



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.

Select a single sign-on method

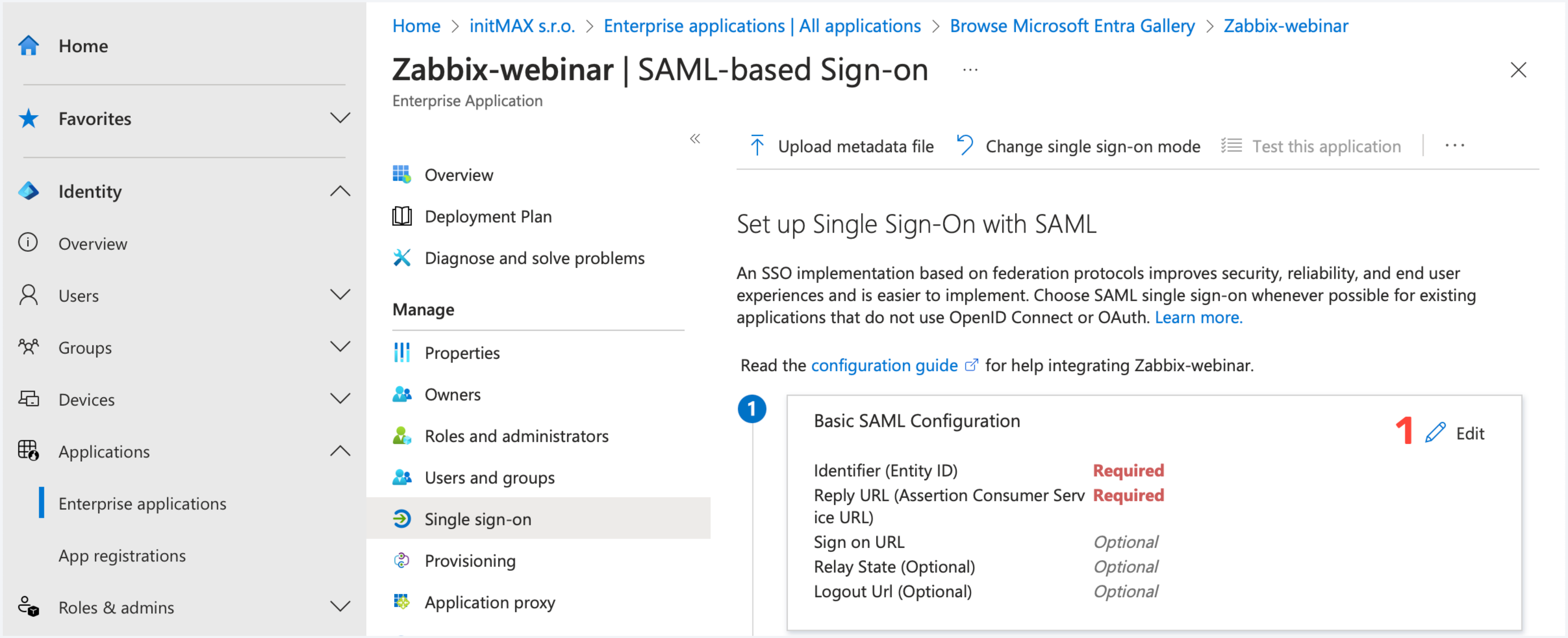
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

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

Zabbix User Provisioning JIT

SAML – Zabbix - Microsoft Entra

- Single sign-on setting
  - Edit basic SAML configuration



Zabbix-webinar | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

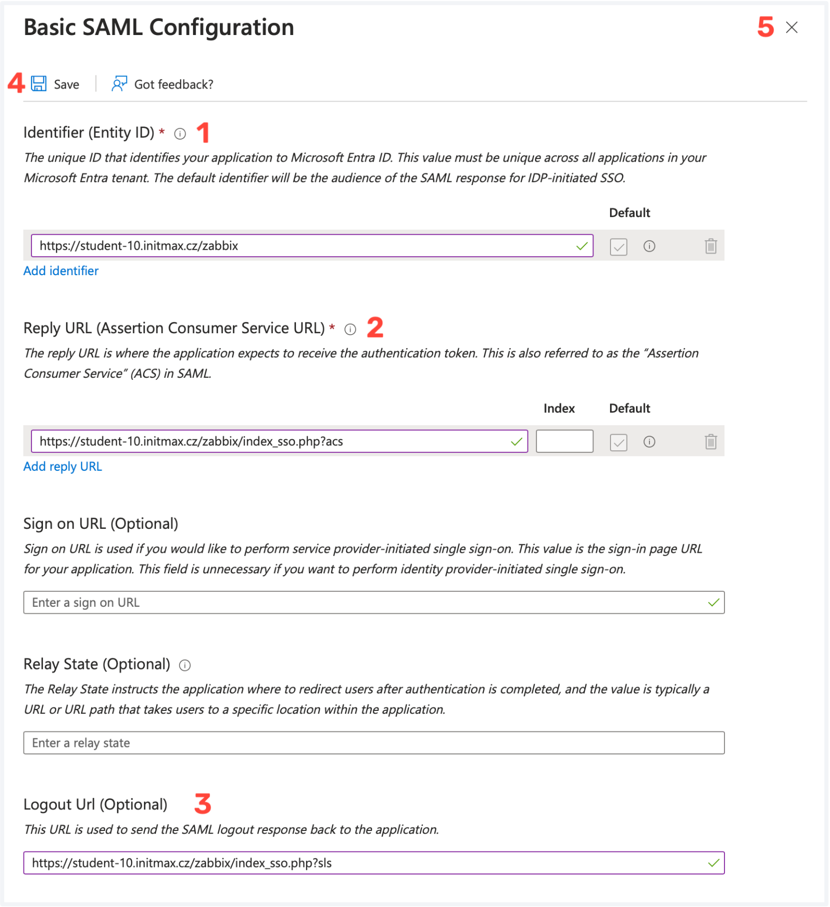
Read the configuration guide for help integrating Zabbix-webinar.

1 Basic SAML Configuration

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

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
  - **Logout UrL** (This is optional)
  - https://student-10.initmax.cz/zabbix/index_sso.php?sls
  - Save our new setting and exit configuration window



Basic SAML Configuration

Identifier (Entity ID) *

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
https://student-10.initmax.cz/zabbix ✓	☑

Reply URL (Assertion Consumer Service URL) *

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
https://student-10.initmax.cz/zabbix/index_sso.php?acs ✓		☑

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.

Enter a sign on URL ✓

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.

Enter a relay state

Logout Url (Optional)

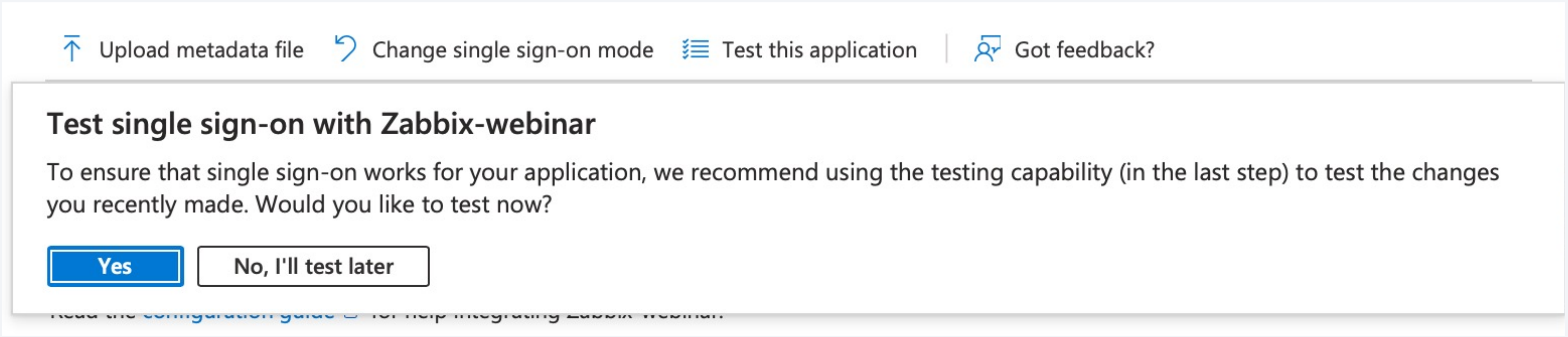
This URL is used to send the SAML logout response back to the application.

https://student-10.initmax.cz/zabbix/index_sso.php?sls ✓

Zabbix User Provisioning JIT

SAML – Zabbix - Microsoft Entra

- Single sign-on setting
  - Close test popup



Test single sign-on with Zabbix-webinar

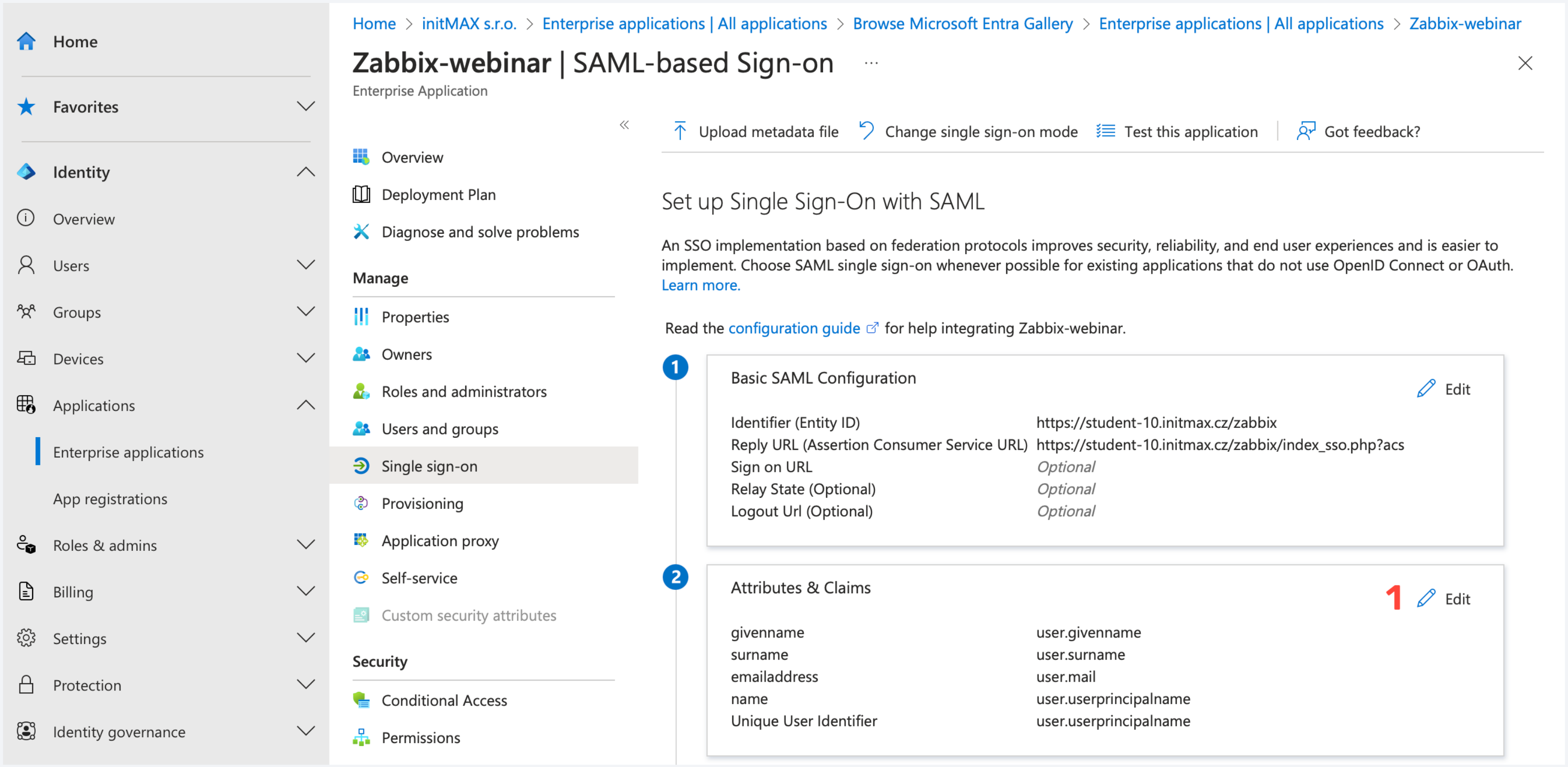
To ensure that single sign-on works for your application, we recommend using the testing capability (in the last step) to test the changes you recently made. Would you like to test now?

Read the configuration guide for help integrating Zabbix-webinar.

Zabbix User Provisioning JIT

SAML – Zabbix - Microsoft Entra

- Single sign-on setting
  - Edit Attributes & Claims



Zabbix-webinar | SAML-based Sign-on

Enterprise Application

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating Zabbix-webinar.

Basic SAML Configuration

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*

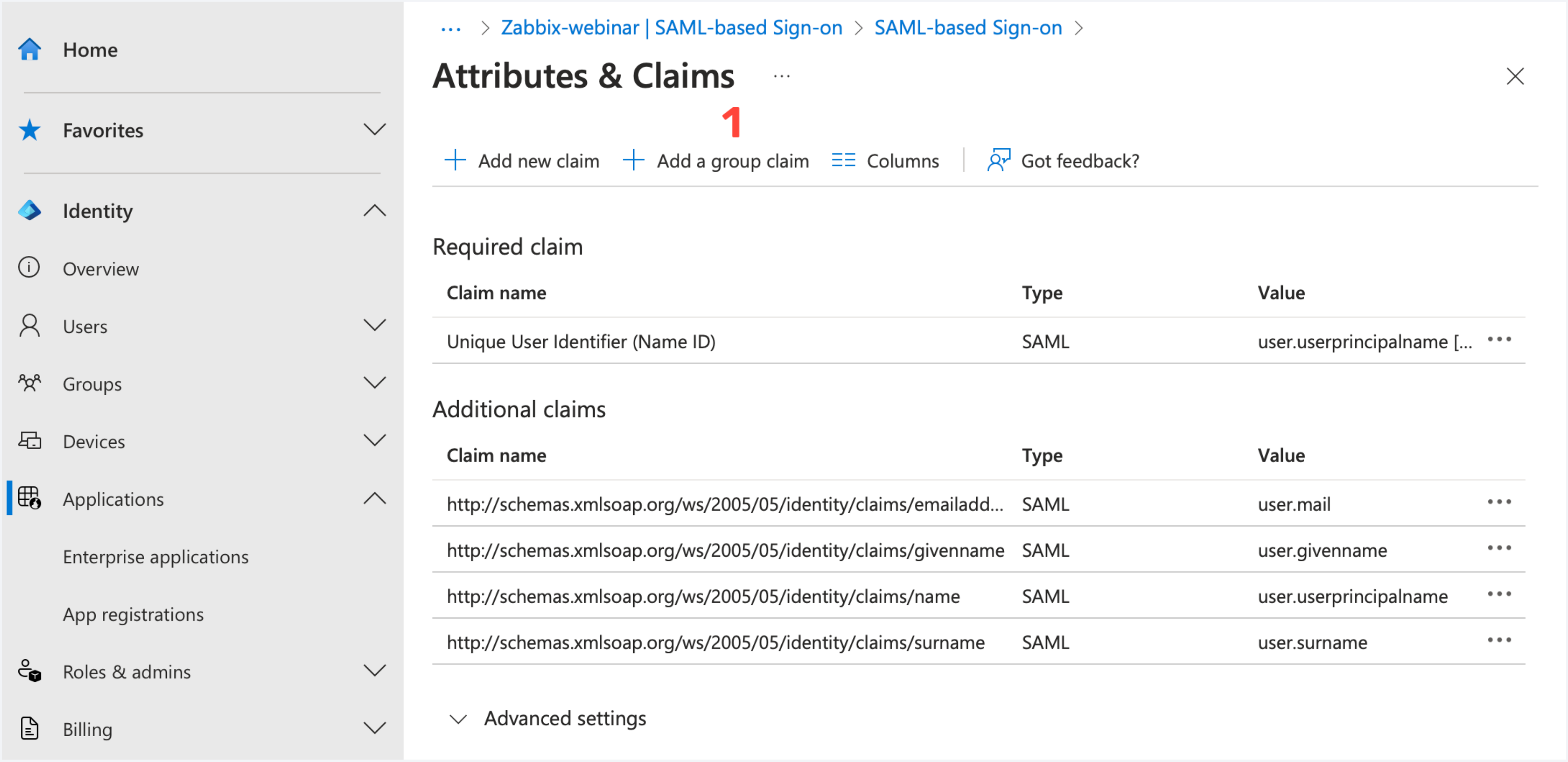
Attributes & Claims

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

Zabbix User Provisioning JIT

SAML – Zabbix - Microsoft Entra

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



Attributes & Claims

Required claim

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

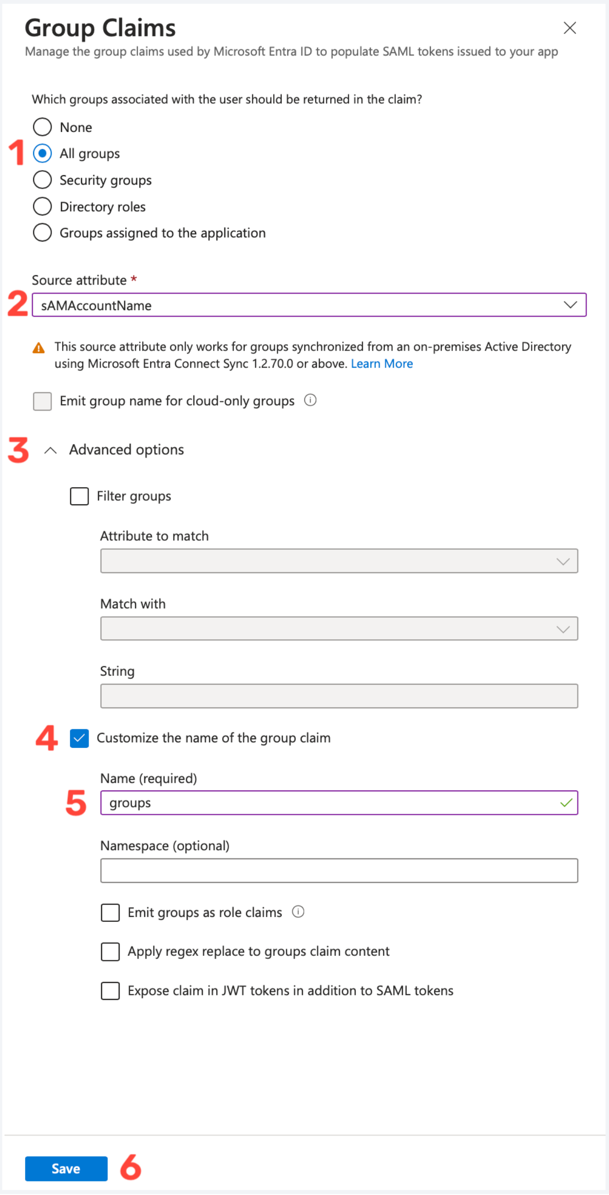
Additional claims

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

Zabbix User Provisioning JIT

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

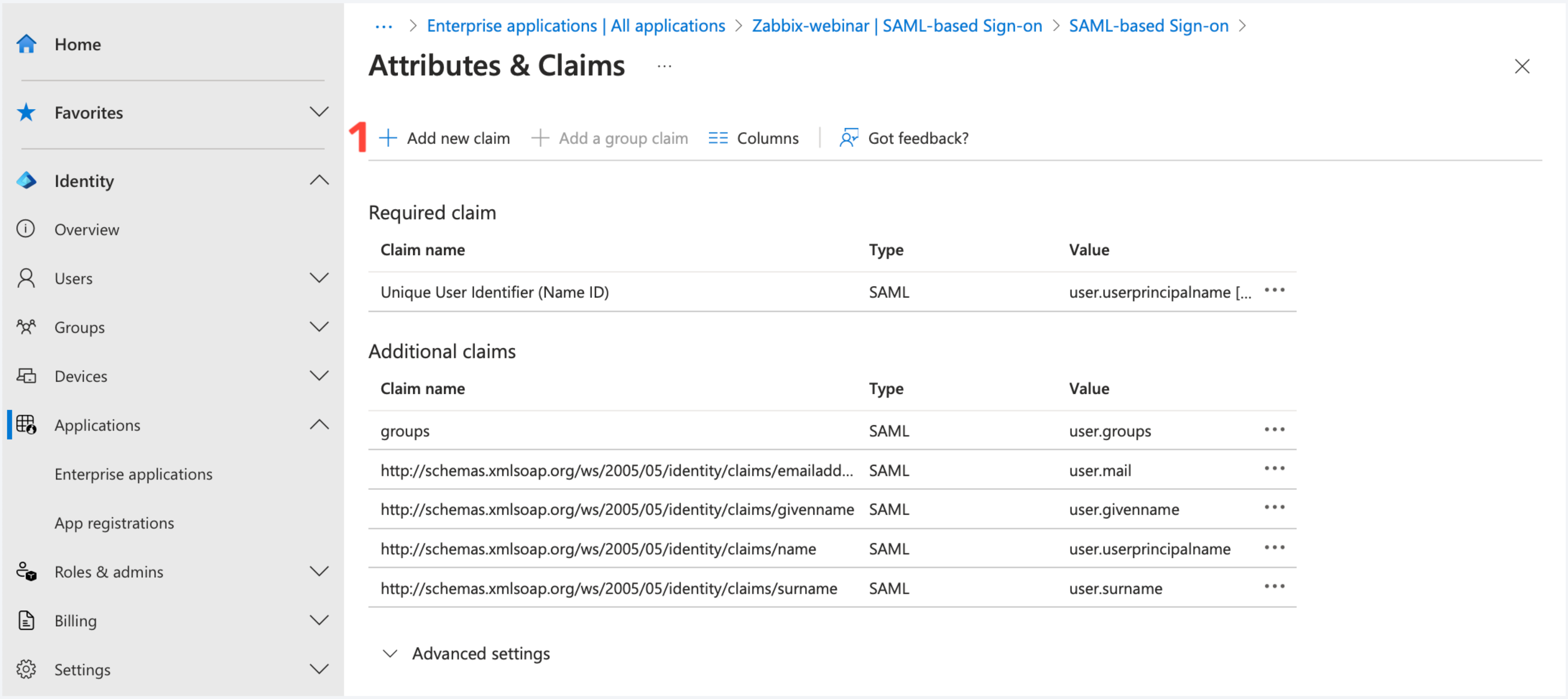
□ Apply regex replace to groups claim content

□ Expose claim in JWT tokens in addition to SAML tokens

Zabbix User Provisioning JIT

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



Attributes & Claims

Required claim

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

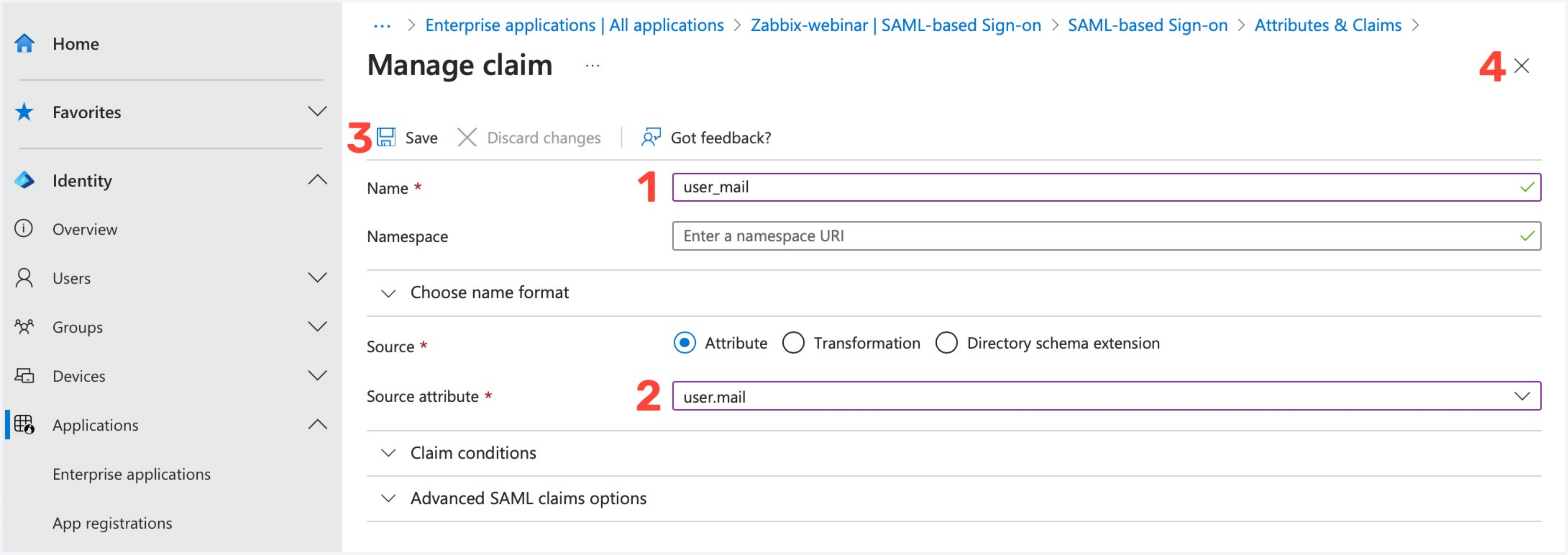
Additional claims

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

Zabbix User Provisioning JIT

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



Manage claim

Name * user_mail

Namespace Enter a namespace URI

Source * ● Attribute ○ Transformation ○ Directory schema extension

Source attribute * user.mail

initMAX

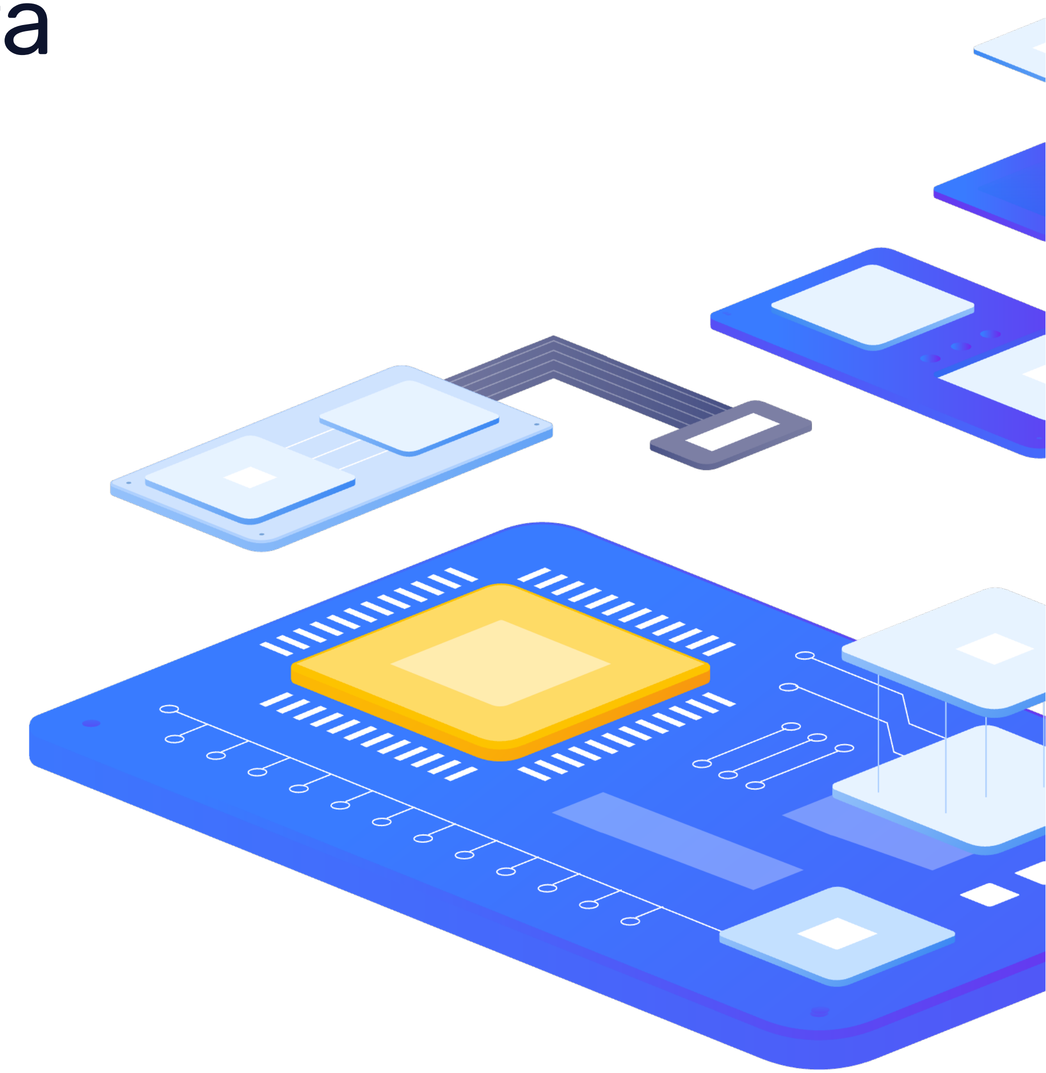
SAML – Zabbix - Microsoft Entra

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

user_mail	**user.mail**

Optional claims

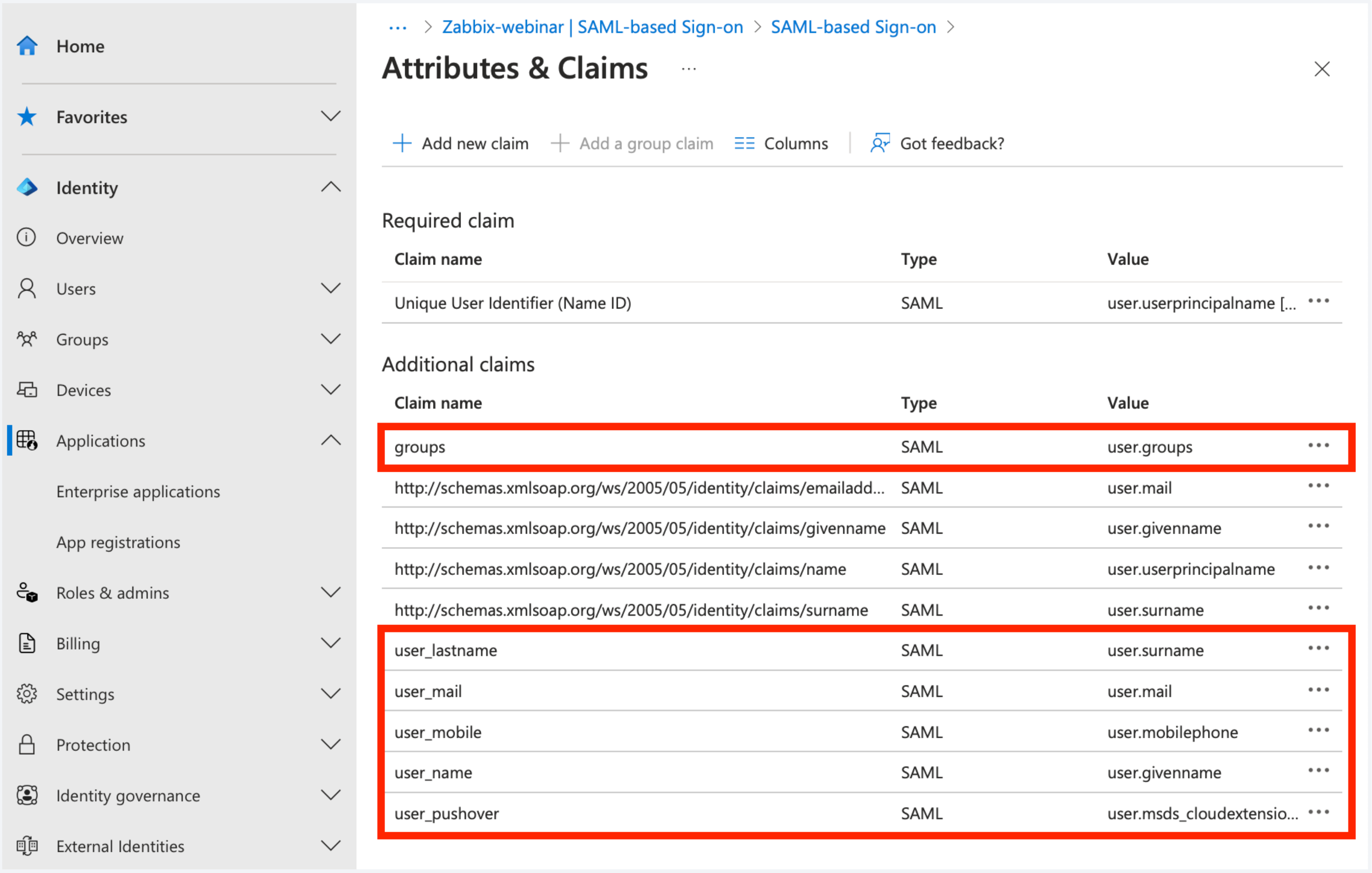
user_mobile	user.mobilephone
user_lastname	user.surname
user_name	user.givenname
user_pushover	user.msds_cloud…



Zabbix User Provisioning JIT

SAML – Zabbix - Microsoft Entra

- Single sign-on setting



Attributes & Claims

Required claim

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

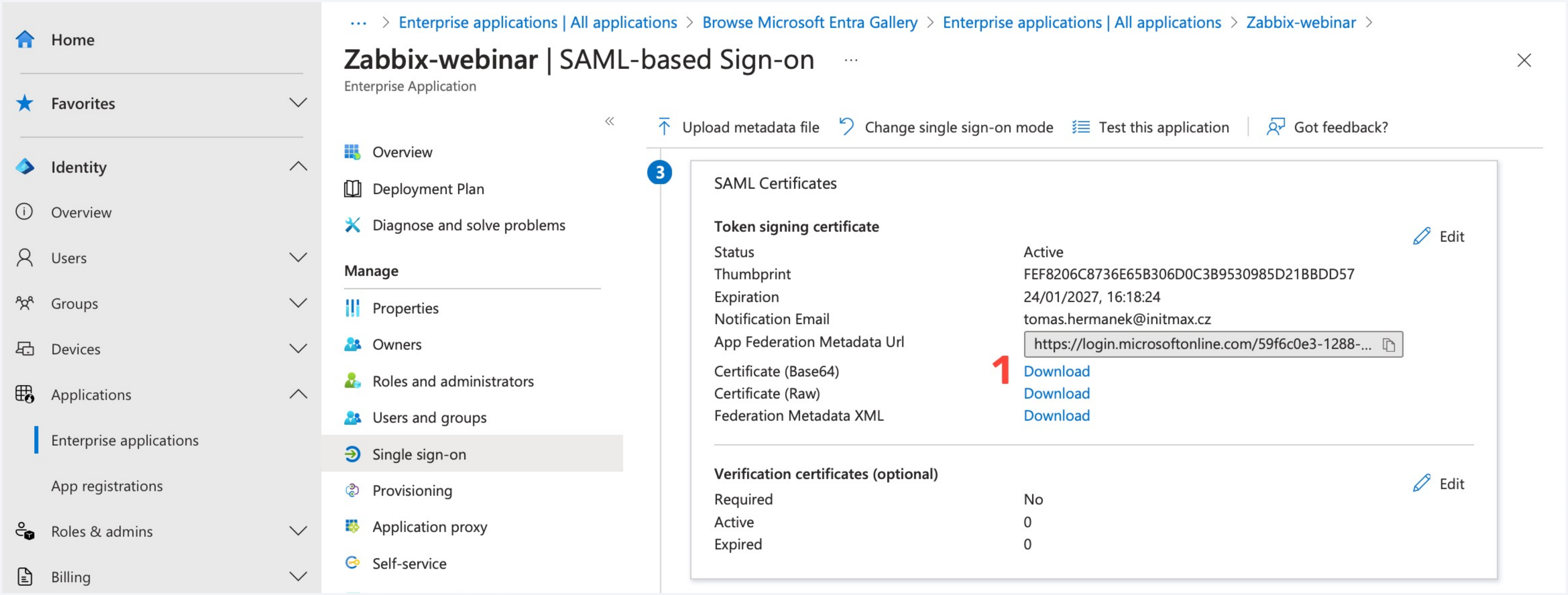
Additional claims

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...

Zabbix User Provisioning JIT

SAML – Zabbix - Microsoft Entra

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



Zabbix-webinar | SAML-based Sign-on

Enterprise Application

SAML Certificates

Token signing certificate

Status	Active
Thumbprint	FEF8206C8736E65B306D0C3B9530985D21BBDD57
Expiration	24/01/2027, 16:18:24
Notification Email	tomas.hermanek@initmax.cz
App Federation Metadata Url	https://login.microsoftonline.com/59f6c0e3-1288-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

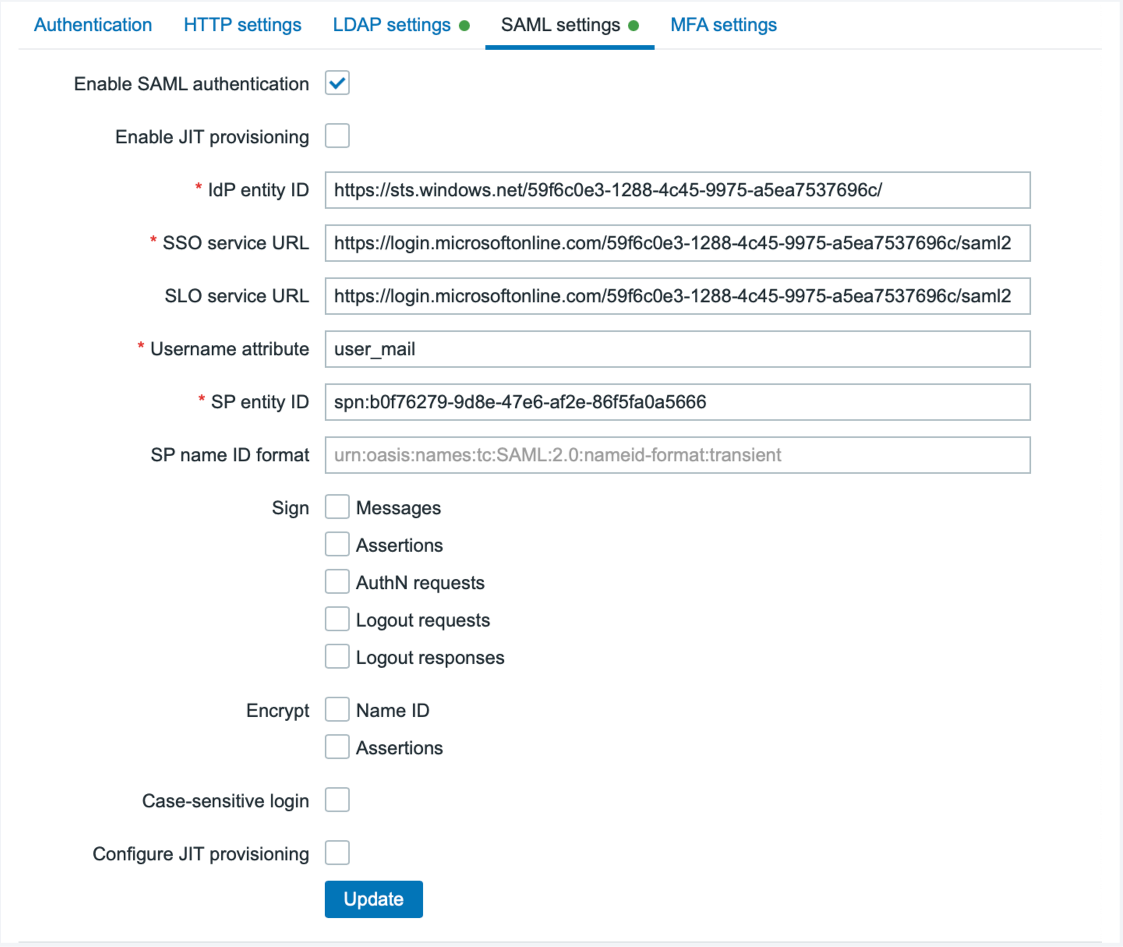
Verification certificates (optional)

Required	No
Active	0
Expired	0

Zabbix User Provisioning JIT

SAML – Zabbix

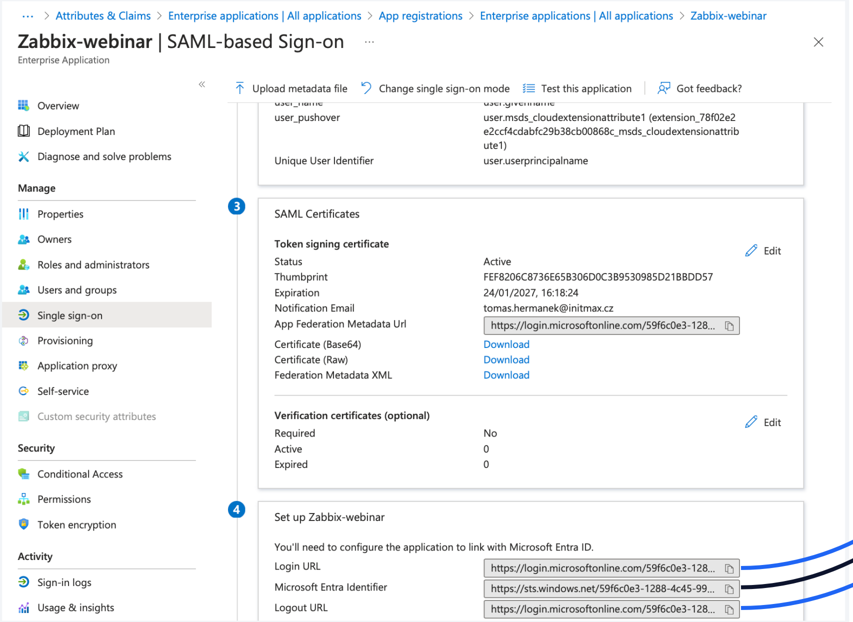
- Enable SAML authentication
  - Mark the checkbox to enable SAML authentication
- IdP entity ID (In Microsoft Entra is named “**Microsoft Entra Identifier**”)
  - The unique entity identifier within the SAML identity provider
- SSO service URL (In Microsoft Entra is named “**Login URL**”)
  - The URL 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:”**



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	□

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

user_name	user.givenname
user_pushover	user.msds_cloudextensionattribute1 (extension_78f02e2e2ccf4cdabfc29b38cb00868c_msds_cloudextensionattribute1)
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate Edit

Status	Active
Thumbprint	FEF8206C8736E65B306D0C3B9530985D21BBDD57
Expiration	24/01/2027, 16:18:24
Notification Email	tomas.hermanek@initmax.cz
App Federation Metadata Url	https://login.microsoftonline.com/59f6c0e3-128...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

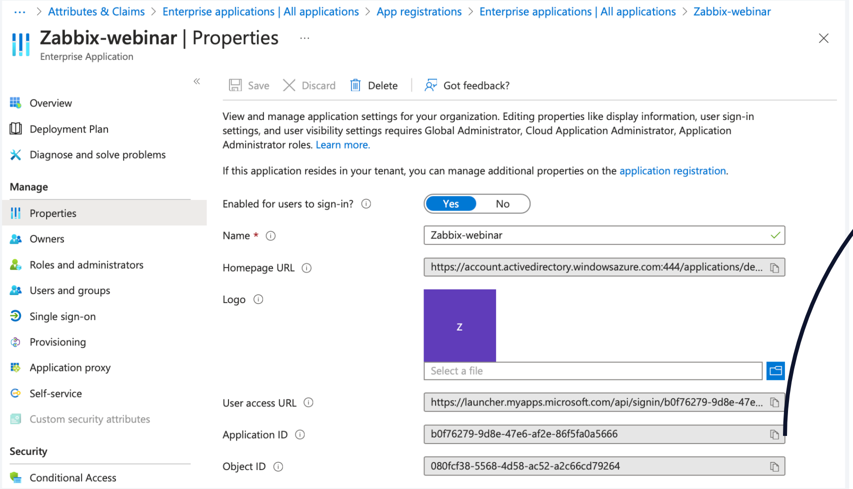
Verification certificates (optional) Edit

Required	No
Active	0
Expired	0

4 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...
Microsoft Entra Identifier	https://sts.windows.net/59f6c0e3-1288-4c45-99...
Logout URL	https://login.microsoftonline.com/59f6c0e3-128...



… > Attributes & Claims > Enterprise applications | All applications > App registrations > Enterprise applications | All applications > Zabbix-webinar

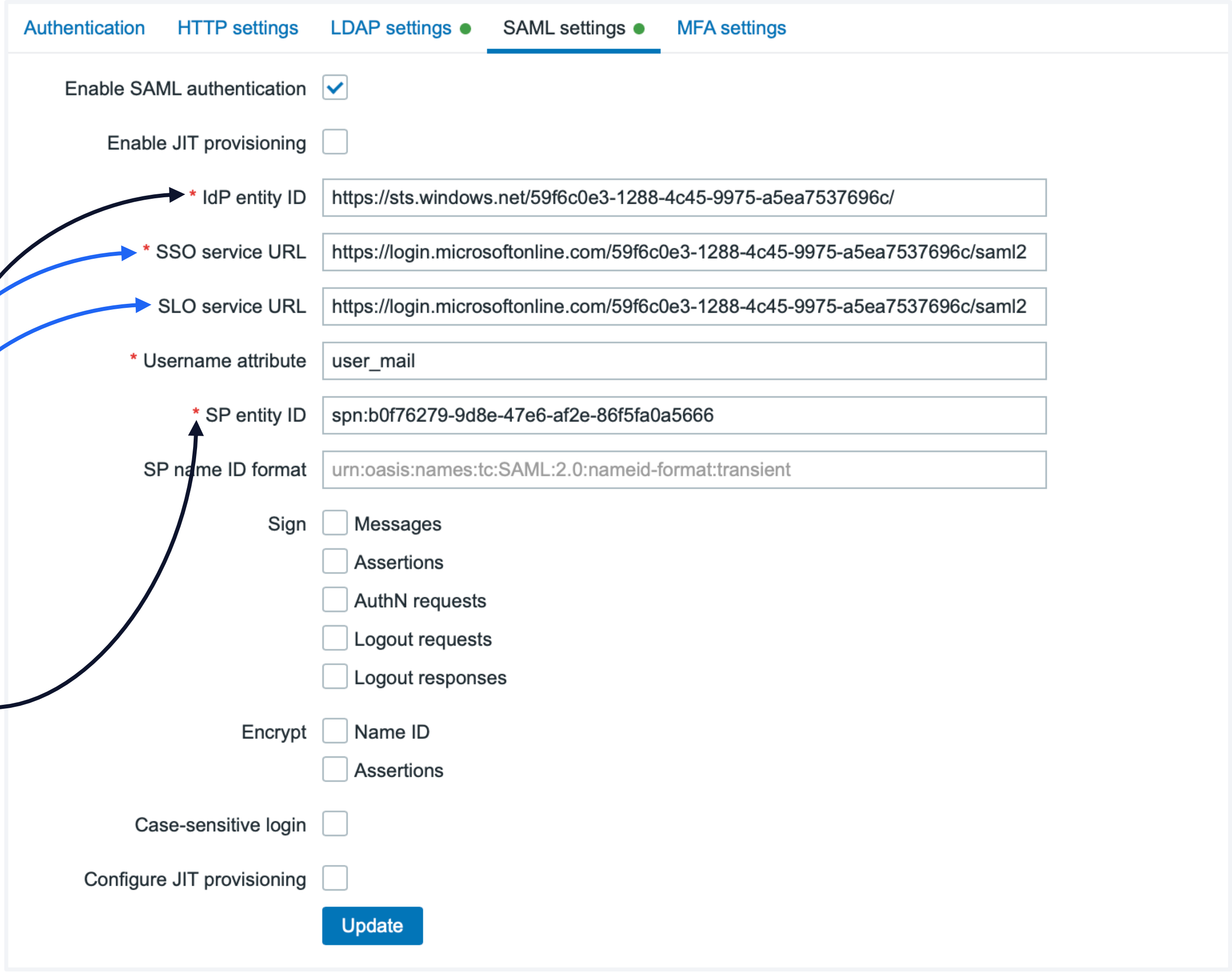
Zabbix-webinar | Properties

Enterprise Application

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...
Logo	Z Select a file
User access URL	https://launcher.myapps.microsoft.com/api/signin/b0f76279-9d8e-47e...
Application ID	b0f76279-9d8e-47e6-af2e-86f5fa0a5666
Object ID	080fcf38-5568-4d58-ac52-a2c66cd79264



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

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

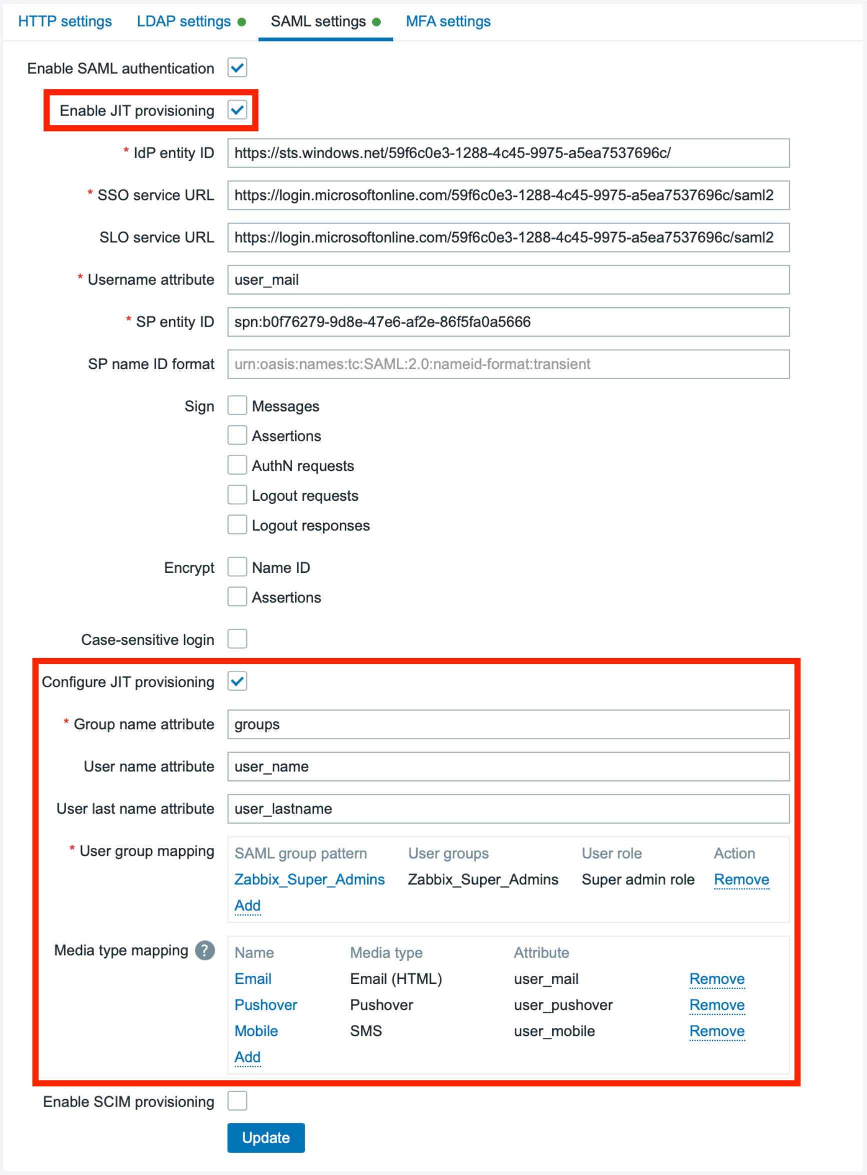
```
// Used for SAML authentication.
// Uncomment to override the default paths to SP private key, SP and IdP X.509 certificates, and to set extra settings.
//$SSO['SP_KEY']                        = 'conf/certs/sp.key';
//$SSO['SP_CERT']                       = 'conf/certs/sp.crt';
$SSO['IDP_CERT'] 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

- Create your user in Zabbix (tomas.hermanek@initmax.cz) 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



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	☑
* Group name attribute	groups
User name attribute	user_name
User last name attribute	user_lastname

* 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 ?

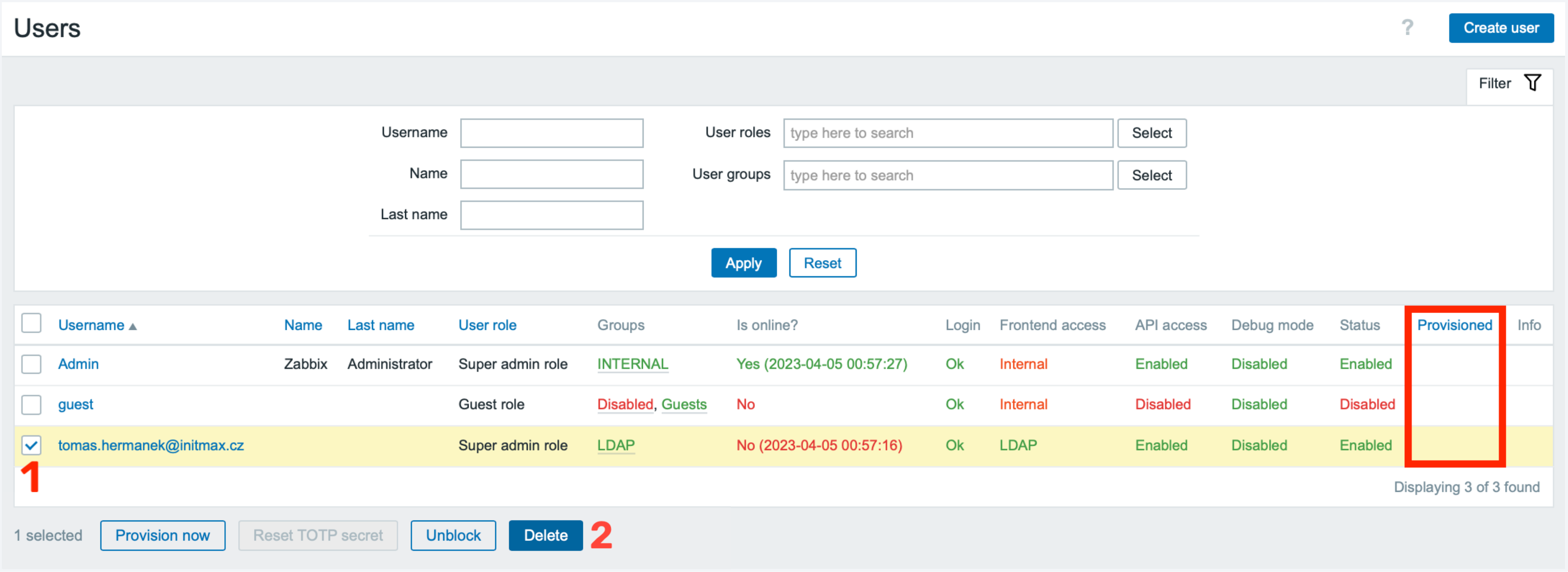
Name	Media type	Attribute	
Email	Email (HTML)	user_mail	Remove
Pushover	Pushover	user_pushover	Remove
Mobile	SMS	user_mobile	Remove
Add			

Enable SCIM provisioning □

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



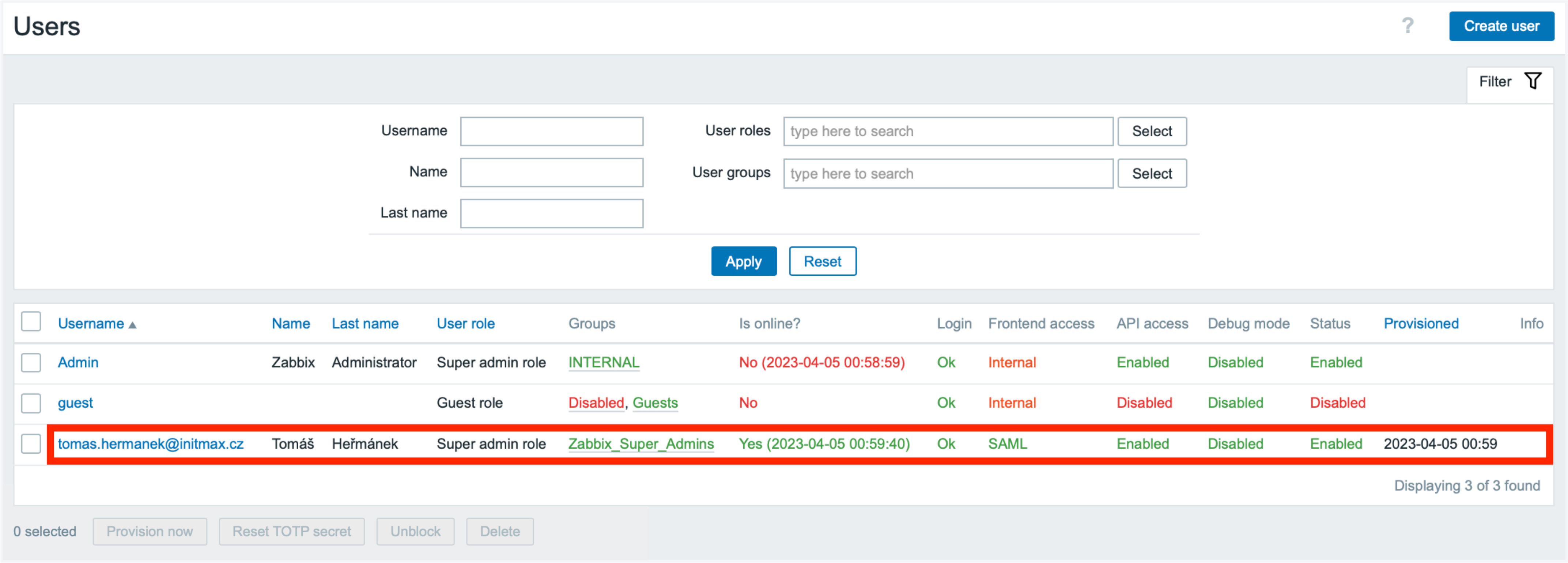
☐	Username ▲	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	Provisioned	Info
☐	Admin	Zabbix	Administrator	Super admin role	INTERNAL	Yes (2023-04-05 00:57:27)	Ok	Internal	Enabled	Disabled	Enabled		
☐	guest			Guest role	Disabled, Guests	No	Ok	Internal	Disabled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

Displaying 3 of 3 found

Zabbix User Provisioning JIT

SAML – Zabbix JIT

- Zabbix SAML JIT provisioning
  - Check your provisioned user



	Username ▲	Name	Last name	User role	Groups	Is online?	Login	Frontend access	API access	Debug mode	Status	Provisioned	Info
□	Admin	Zabbix	Administrator	Super admin role	INTERNAL	No (2023-04-05 00:58:59)	Ok	Internal	Enabled	Disabled	Enabled		
□	guest			Guest role	Disabled, Guests	No	Ok	Internal	Disabled	Disabled	Disabled		
□	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	

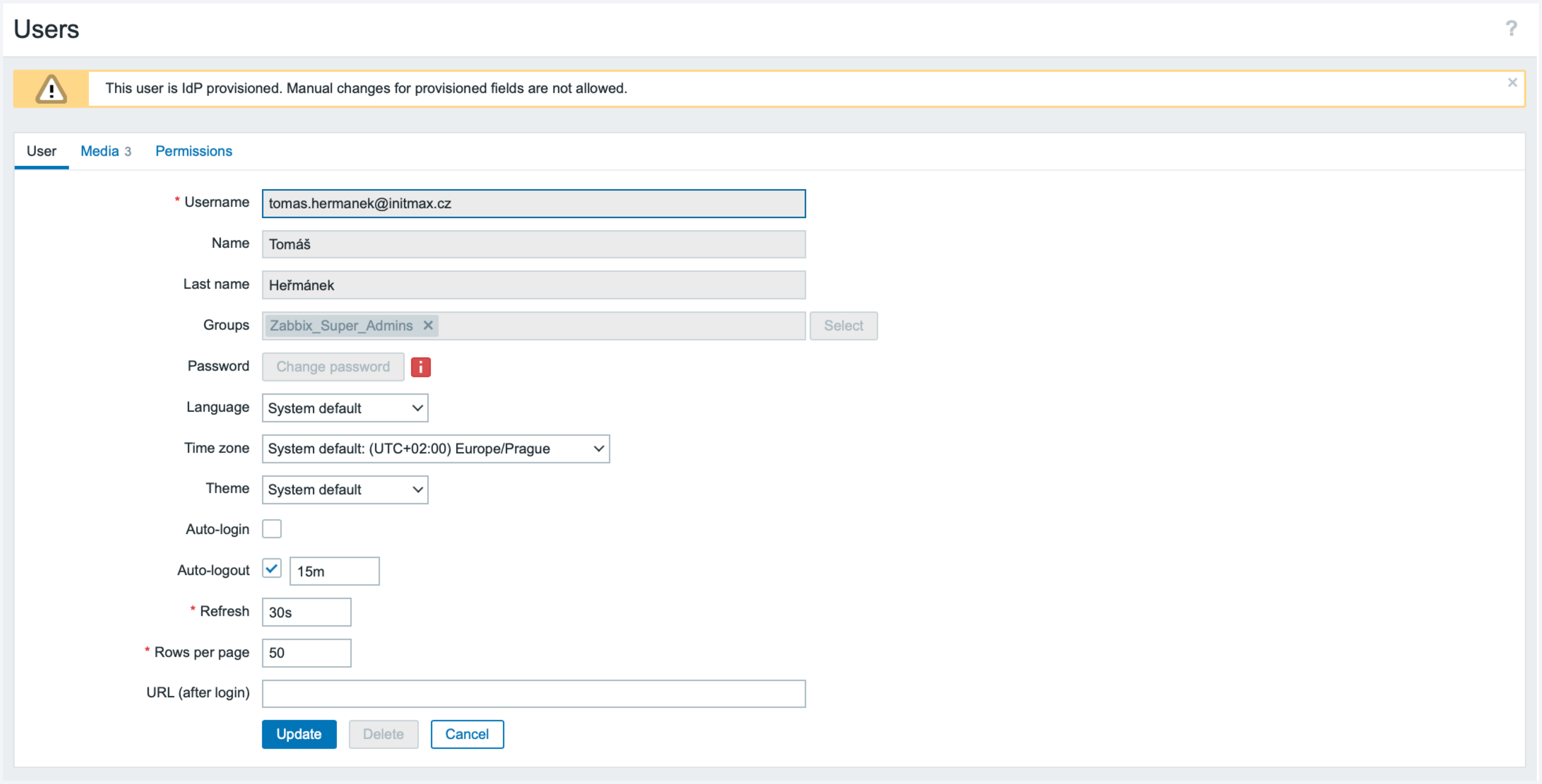
Displaying 3 of 3 found

0 selected

Zabbix User Provisioning JIT

SAML – Zabbix JIT

- Zabbix SAML JIT provisioning
  - Check your provisioned user



Users

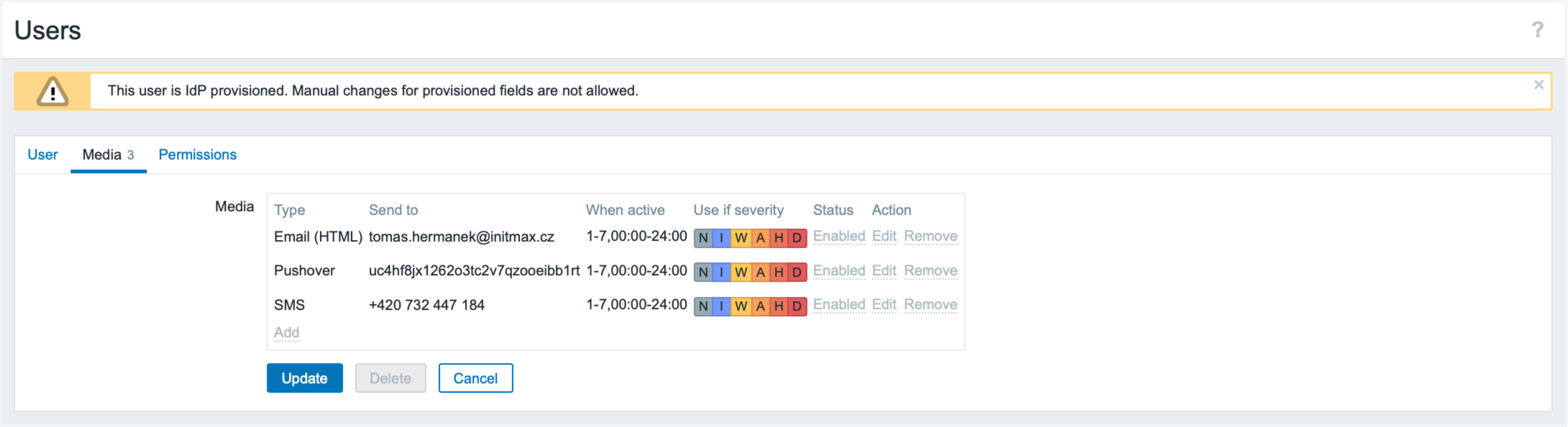
This user is IdP provisioned. Manual changes for provisioned fields are not allowed.

* Username	tomas.hermanek@initmax.cz
Name	Tomáš
Last name	Heřmánek
Groups	Zabbix_Super_Admins ✕
Password	Change password
Language	System default
Time zone	System default: (UTC+02:00) Europe/Prague
Theme	System default
Auto-login	□
Auto-logout	☑ 15m
* Refresh	30s
* Rows per page	50
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.

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

Zabbix User Provisioning JIT

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];

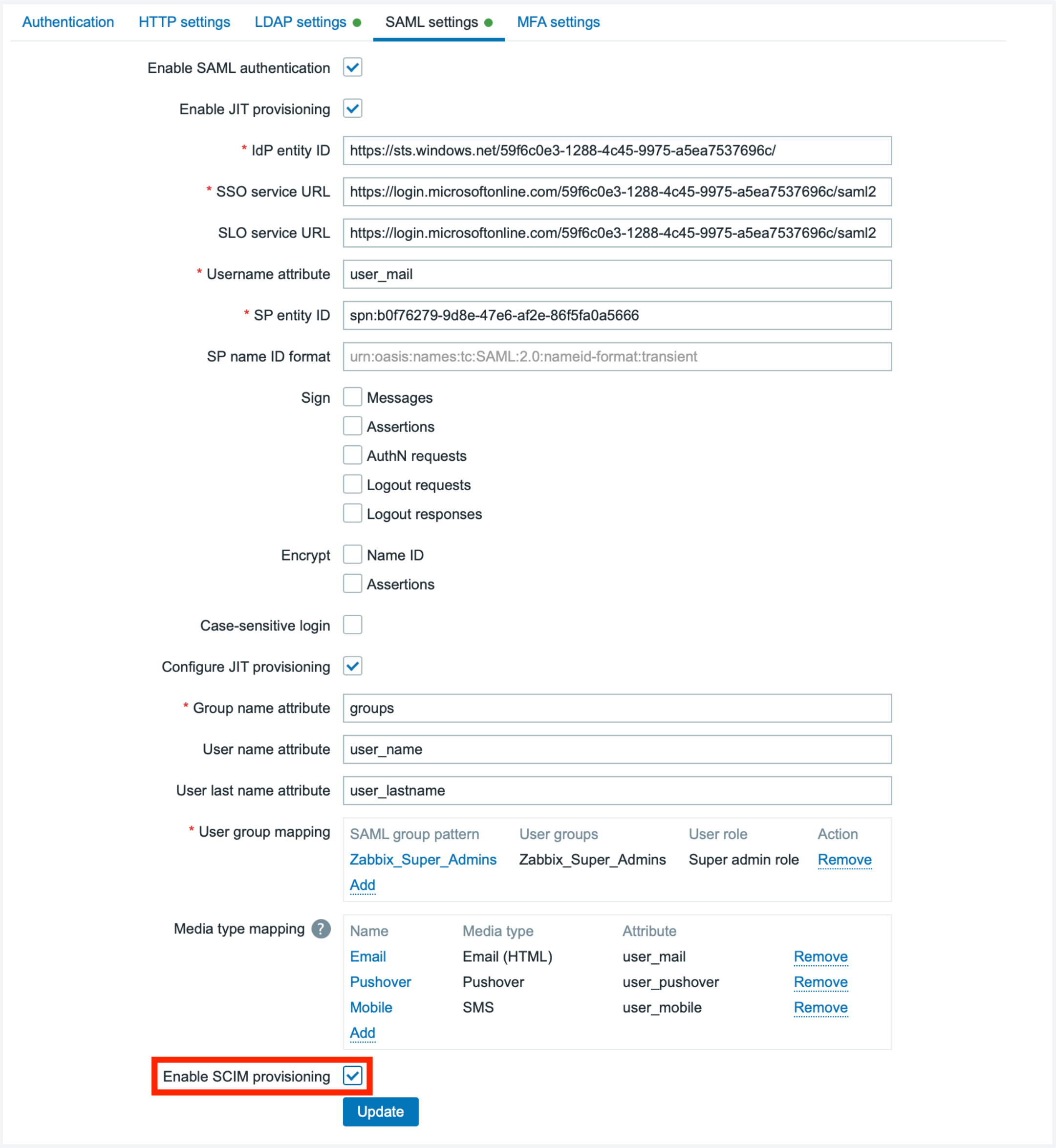
5

SCIM

Zabbix User Provisioning JIT

SCIM – Zabbix

- Zabbix SCIM provisioning
  - Enable SCIM provisioning



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 ☑

* Group name attribute: groups

User name attribute: user_name

User last name attribute: user_lastname

* 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 ?

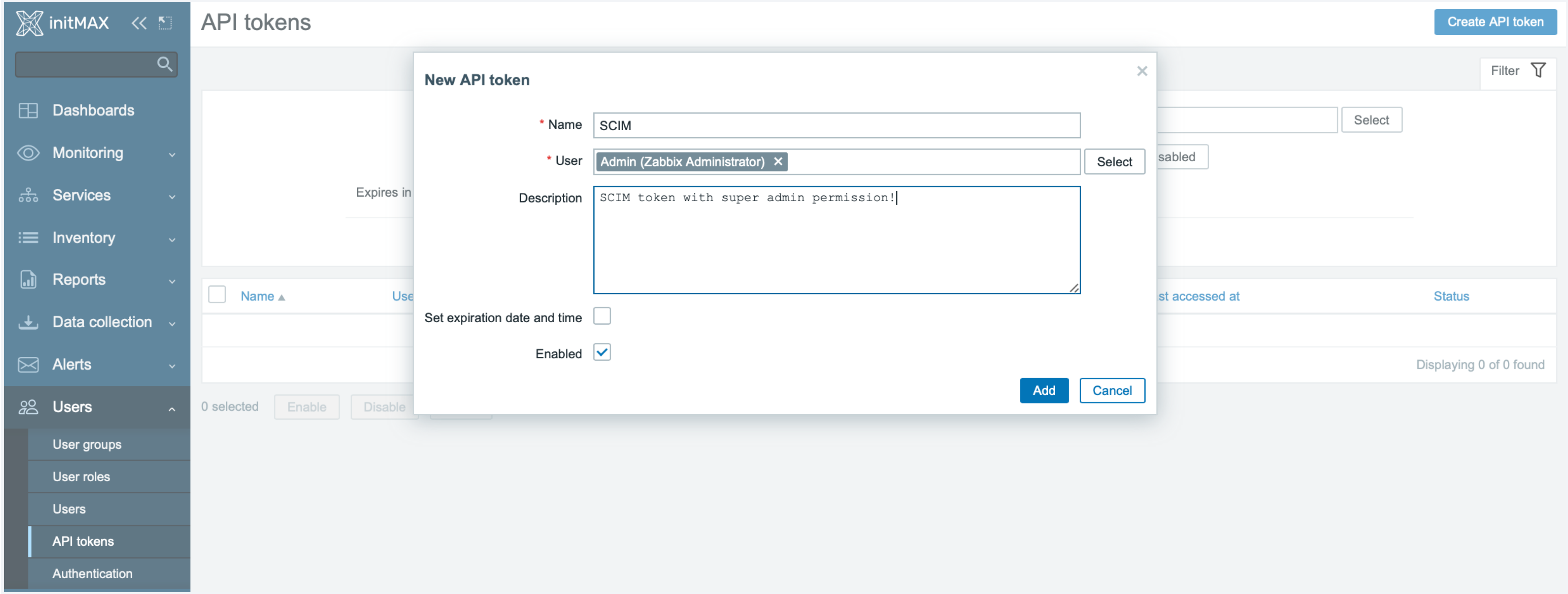
Name	Media type	Attribute	
Email	Email (HTML)	user_mail	Remove
Pushover	Pushover	user_pushover	Remove
Mobile	SMS	user_mobile	Remove
Add			

Enable SCIM provisioning ☑

Zabbix User Provisioning JIT

SCIM – Zabbix

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



New API token

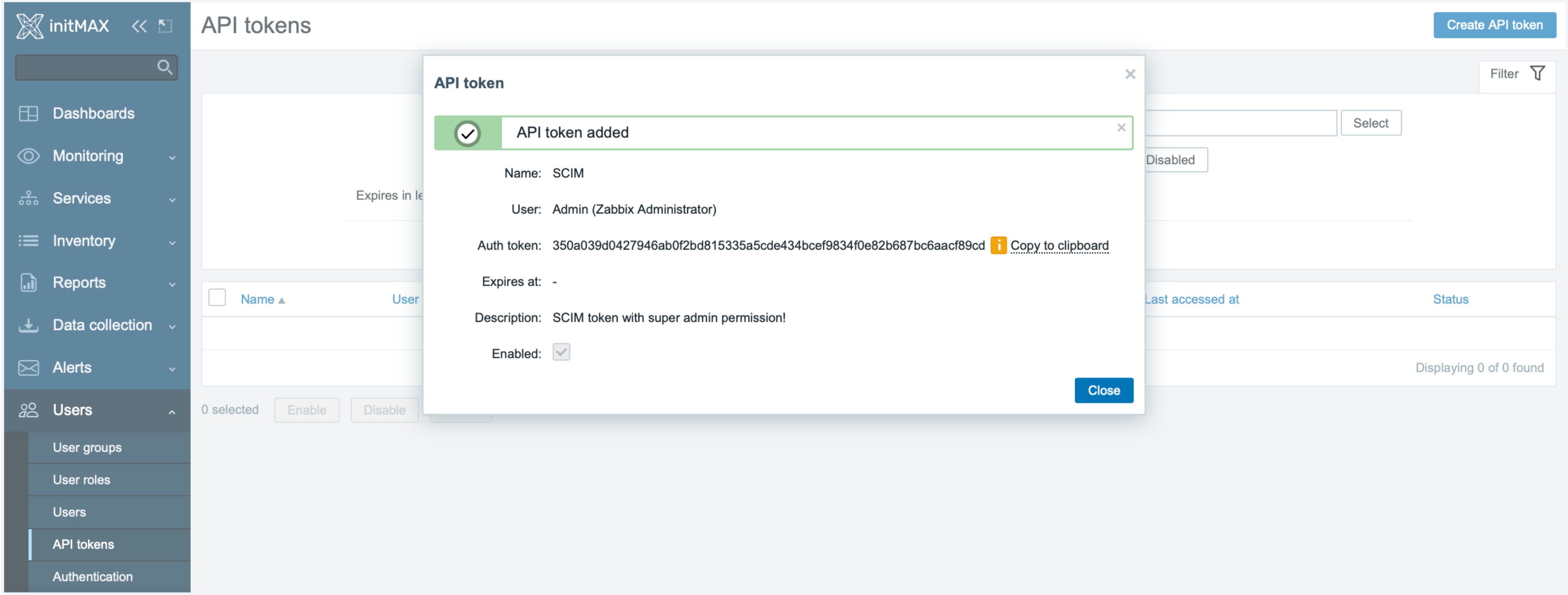
* Name	SCIM
* User	Admin (Zabbix Administrator) ✕ Select
Description	SCIM token with super admin permission!
Set expiration date and time	□
Enabled	☑

Add Cancel

Zabbix User Provisioning JIT

SCIM – Zabbix

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



API token

API token added

Name: SCIM

User: Admin (Zabbix Administrator)

Auth token: 350a039d0427946ab0f2bd815335a5cde434bcef9834f0e82b687bc6aacf89cd Copy to clipboard

Expires at: -

Description: SCIM token with super admin permission!

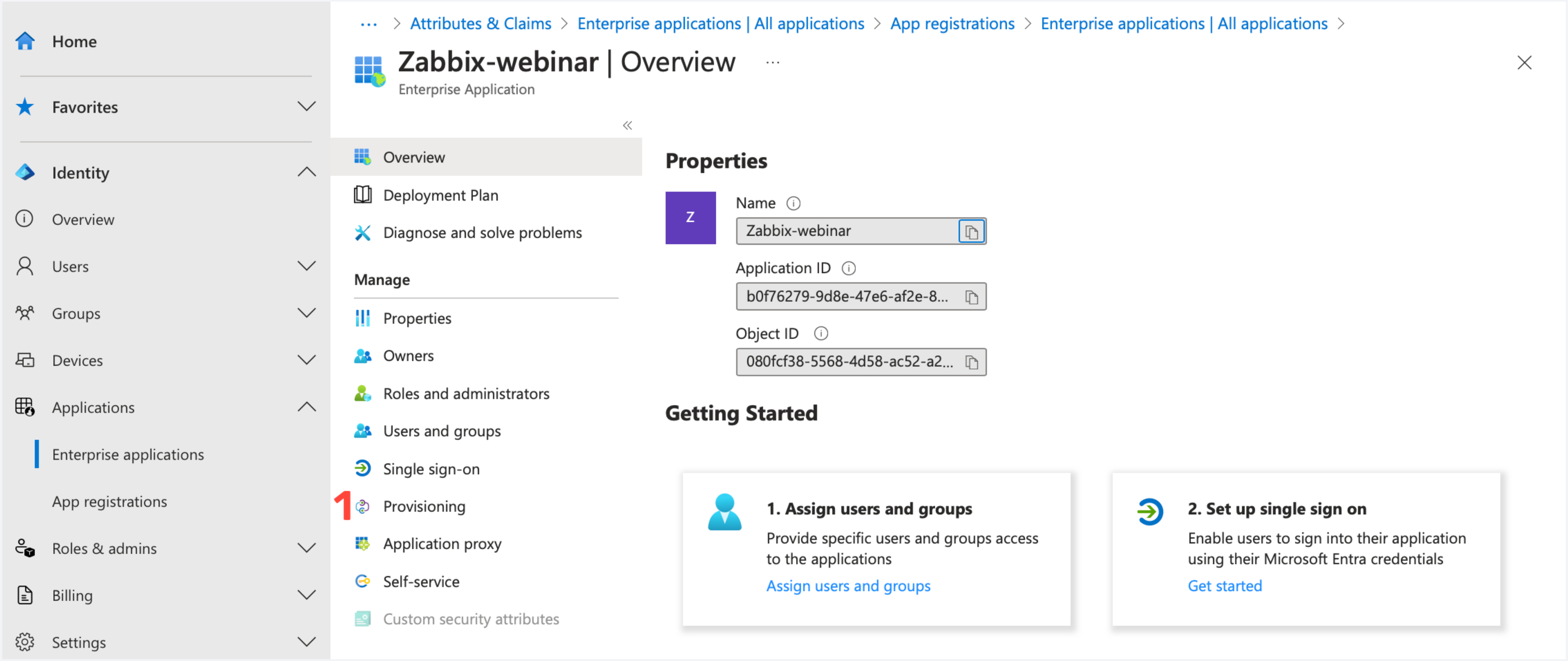
Enabled: ☑

Close

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

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



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

Zabbix-webinar | Overview ...

Enterprise Application

Properties

Name: Zabbix-webinar

Application ID: b0f76279-9d8e-47e6-af2e-8...

Object ID: 080fcf38-5568-4d58-ac52-a2...

Getting Started

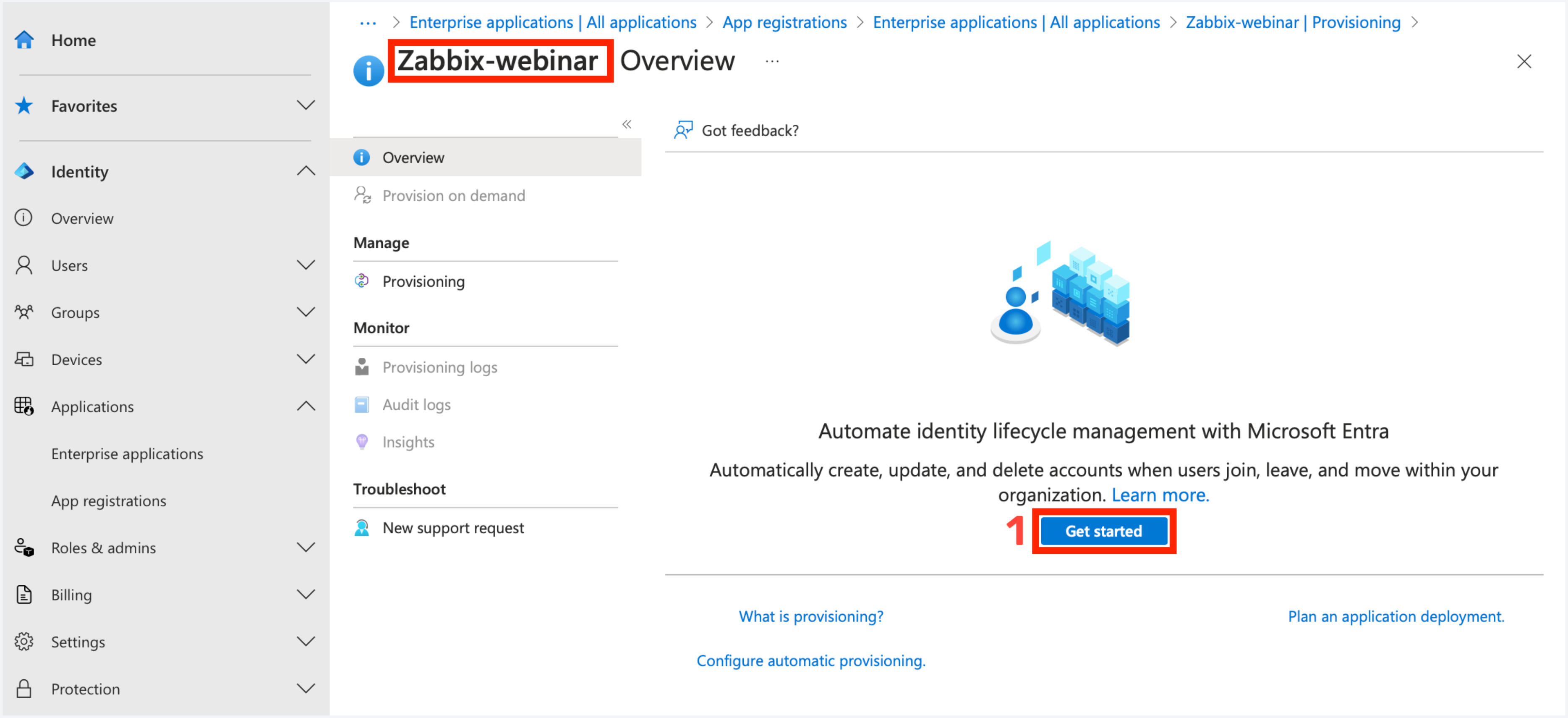
1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
Get started

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

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



... > Enterprise applications | All applications > App registrations > Enterprise applications | All applications > Zabbix-webinar | Provisioning >

Zabbix-webinar Overview ...

Automate identity lifecycle management with Microsoft Entra

Automatically create, update, and delete accounts when users join, leave, and move within your organization. Learn more.

1 Get started

What is provisioning?

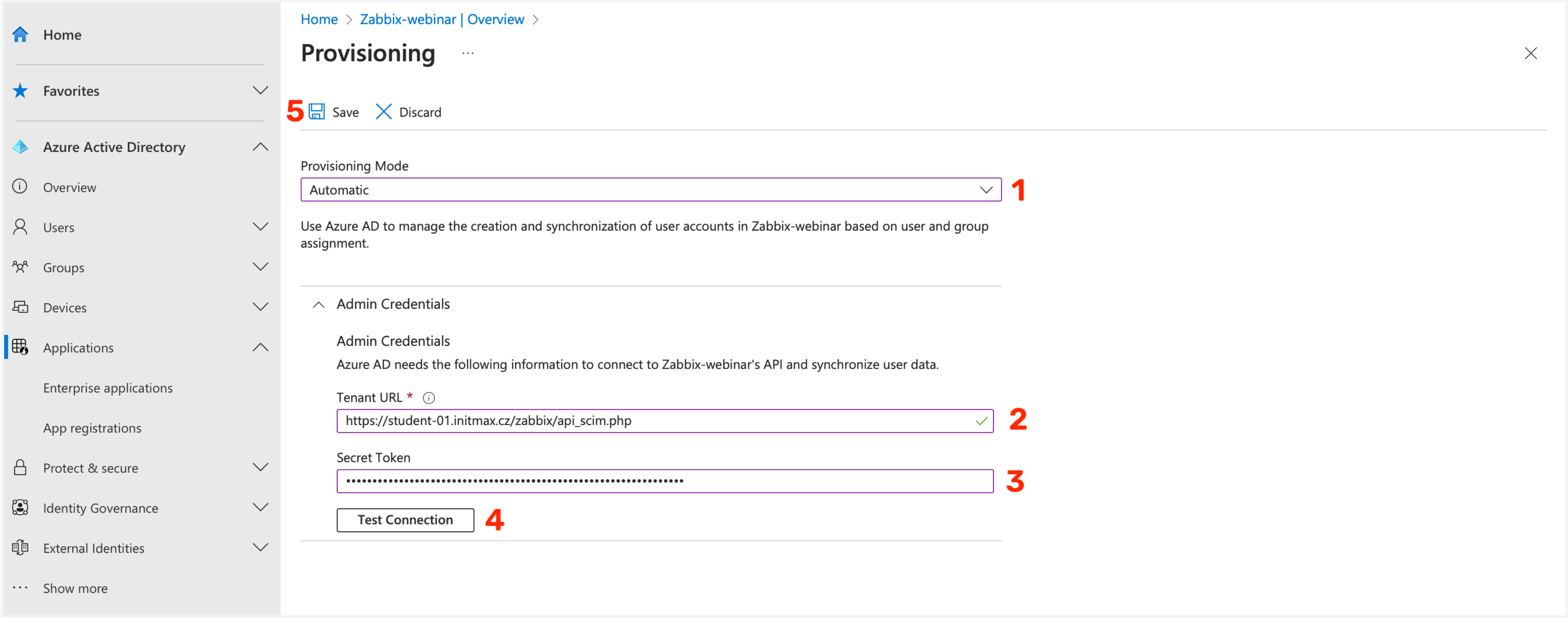
Plan an application deployment.

Configure automatic provisioning.

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

- Zabbix SCIM provisioning
  - Select Automatic Provisioning mode
  - Tenant URL - https://student-10.initmax.cz/zabbix/api_scim.php
  - Fill Secret Token, test connection and save



Provisioning Mode: Automatic

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.

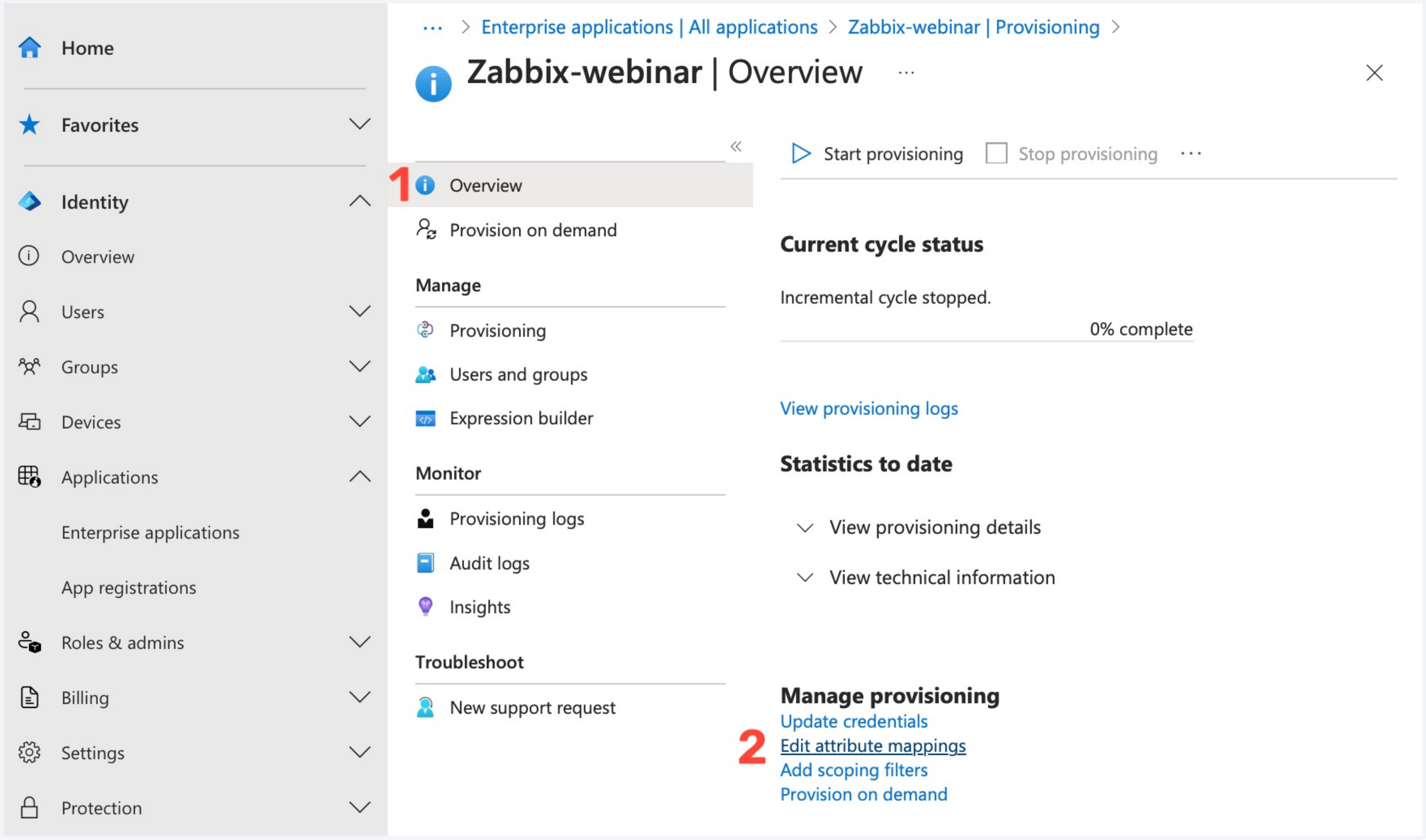
Tenant URL *: https://student-01.initmax.cz/zabbix/api_scim.php

Secret Token: ••

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

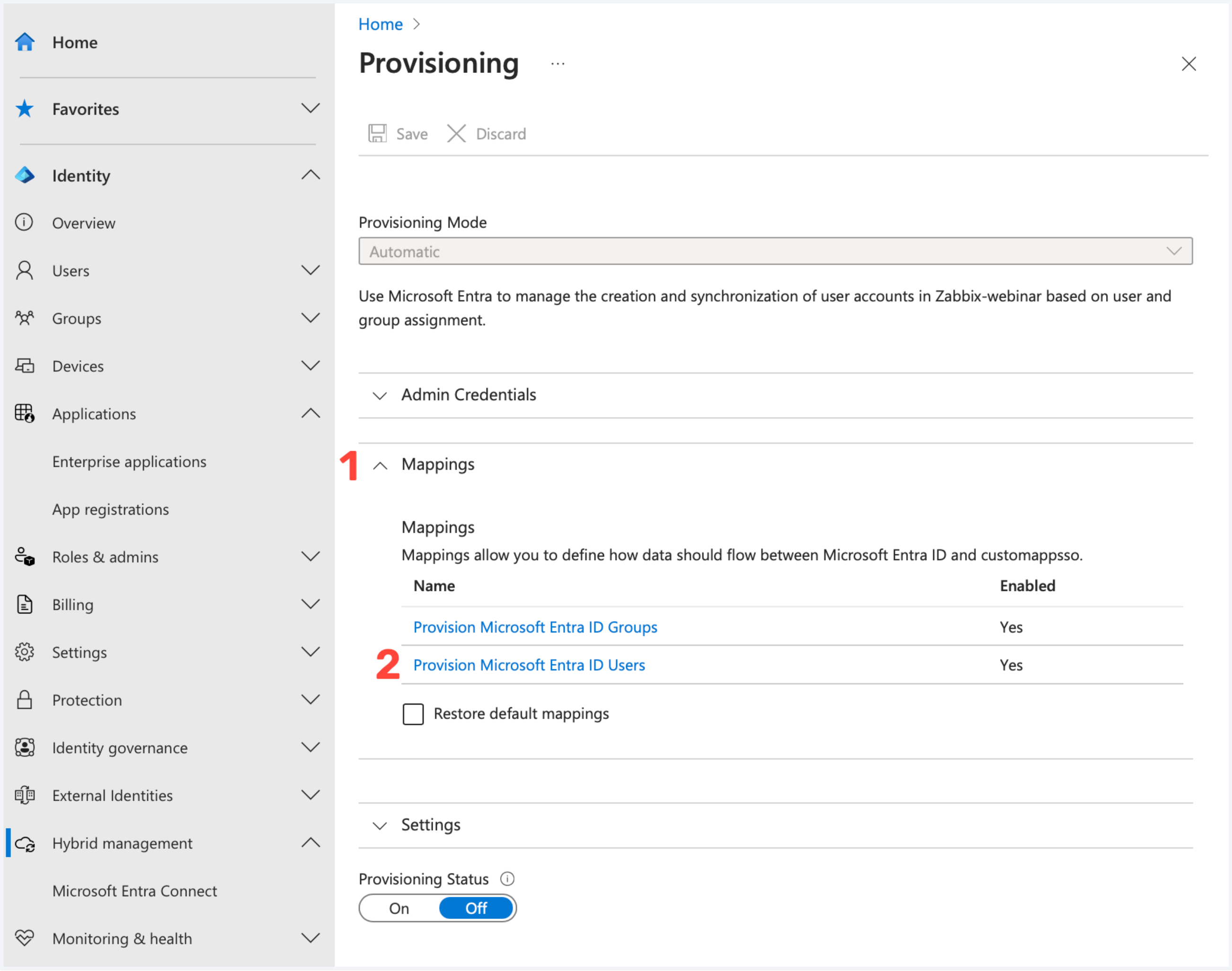
- Zabbix SCIM provisioning
  - From Overview application menu klick on “Edit attribute mappings”



Zabbix User Provisioning JIT

SCIM – Microsoft Entra

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



Provisioning

Provisioning Mode: Automatic

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

Mappings

Mappings

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

Name	Enabled
Provision Microsoft Entra ID Groups	Yes
2 Provision Microsoft Entra ID Users	Yes

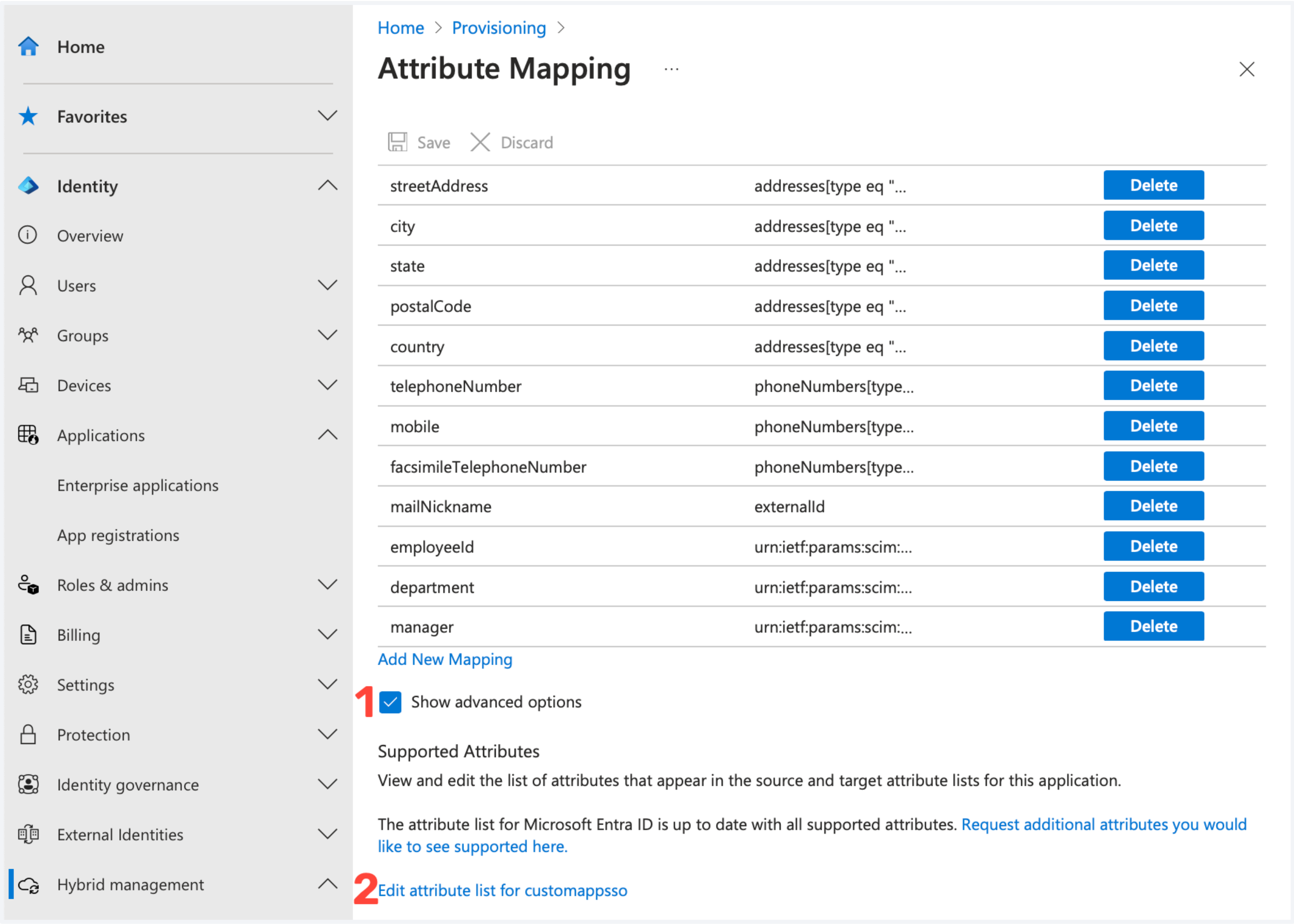
□ Restore default mappings

Provisioning Status: On [✓ Off]

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

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



Attribute Mapping

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

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.

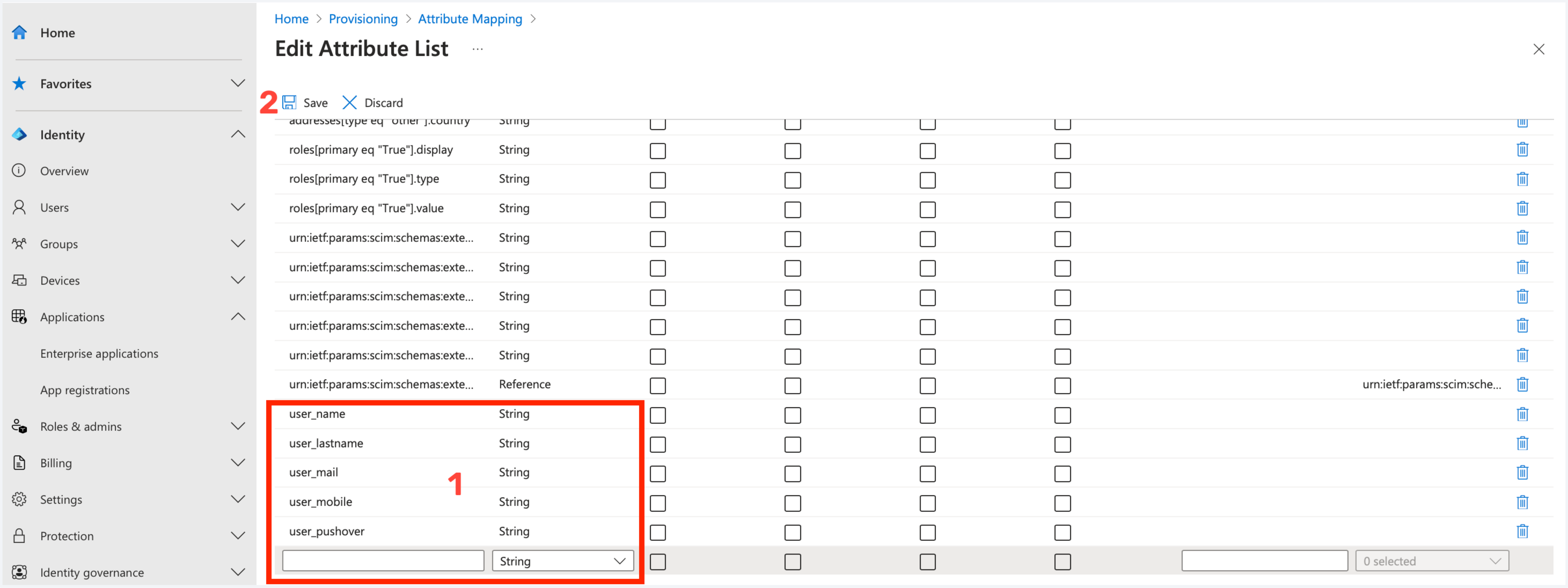
The attribute list for Microsoft Entra ID is up to date with all supported attributes. Request additional attributes you would like to see supported here.

2 Edit attribute list for customappsso

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

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

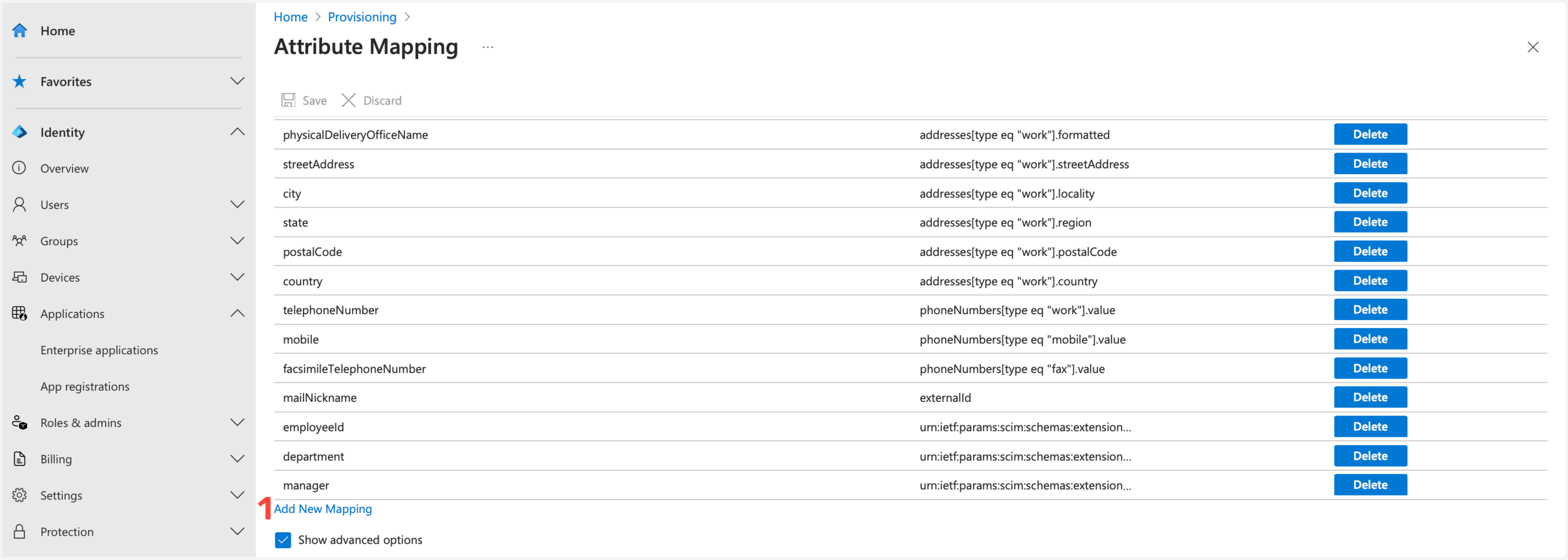


addresses[type eq "other"].country	String	□	□	□	□	
roles[primary eq "True"].display	String	□	□	□	□	
roles[primary eq "True"].type	String	□	□	□	□	
roles[primary eq "True"].value	String	□	□	□	□	
urn:ietf:params:scim:schemas:exte...	String	□	□	□	□	
urn:ietf:params:scim:schemas:exte...	String	□	□	□	□	
urn:ietf:params:scim:schemas:exte...	String	□	□	□	□	
urn:ietf:params:scim:schemas:exte...	String	□	□	□	□	
urn:ietf:params:scim:schemas:exte...	String	□	□	□	□	
urn:ietf:params:scim:schemas:exte...	Reference	□	□	□	□	urn:ietf:params:scim:sche...
user_name	String	□	□	□	□	
user_lastname	String	□	□	□	□	
user_mail	String	□	□	□	□	
user_mobile	String	□	□	□	□	
user_pushover	String	□	□	□	□	
	String	□	□	□	□	0 selected

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

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



Attribute Mapping

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

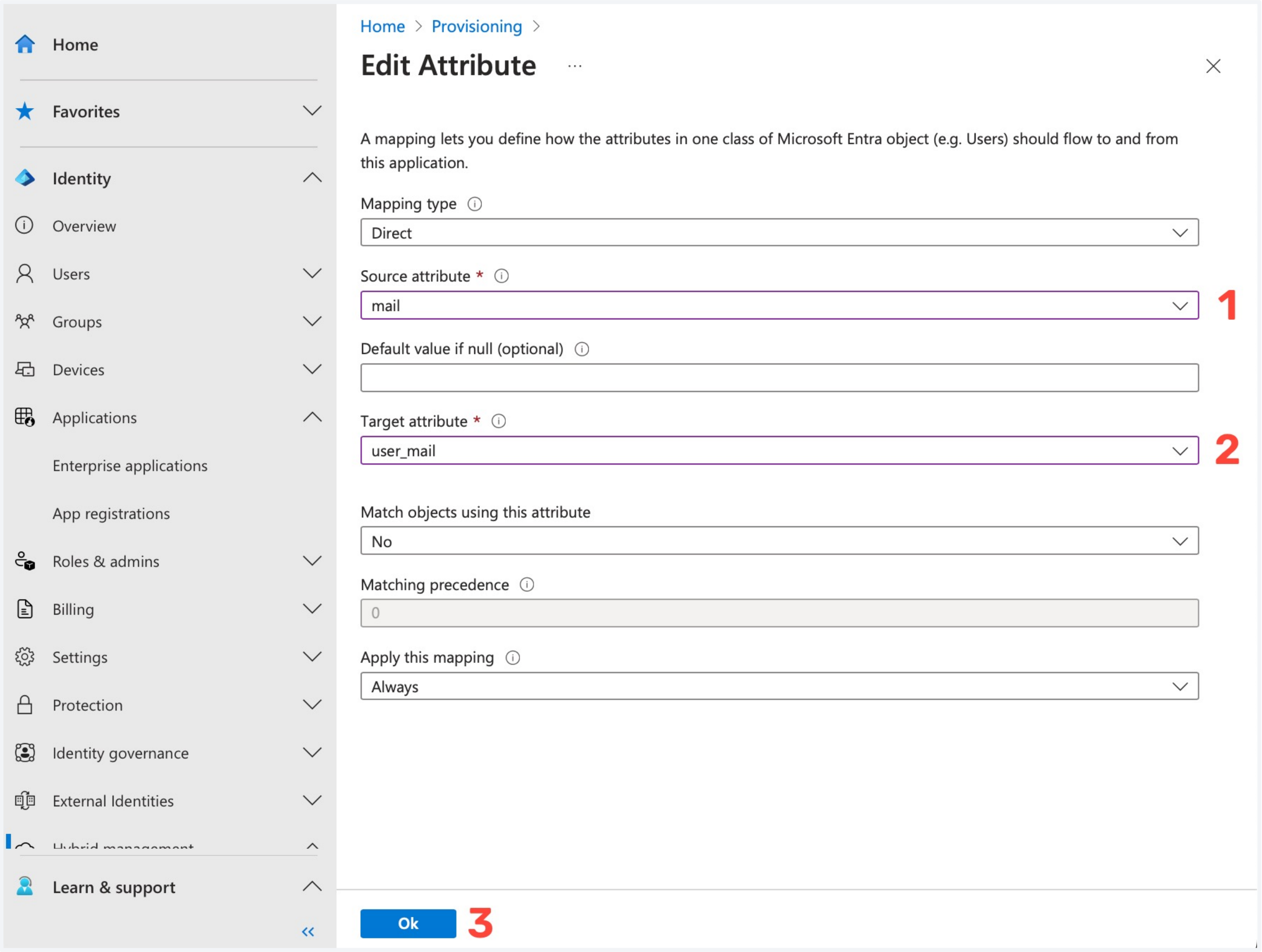
1 Add New Mapping

☑ Show advanced options

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

- Zabbix SCIM provisioning
  - Add our custom attributes
  - user_mail
  - user_mobile
  - user_name
  - user_lastname
  - user_pushover



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: Direct

Source attribute *: mail 1

Default value if null (optional):

Target attribute *: user_mail 2

Match objects using this attribute: No

Matching precedence: 0

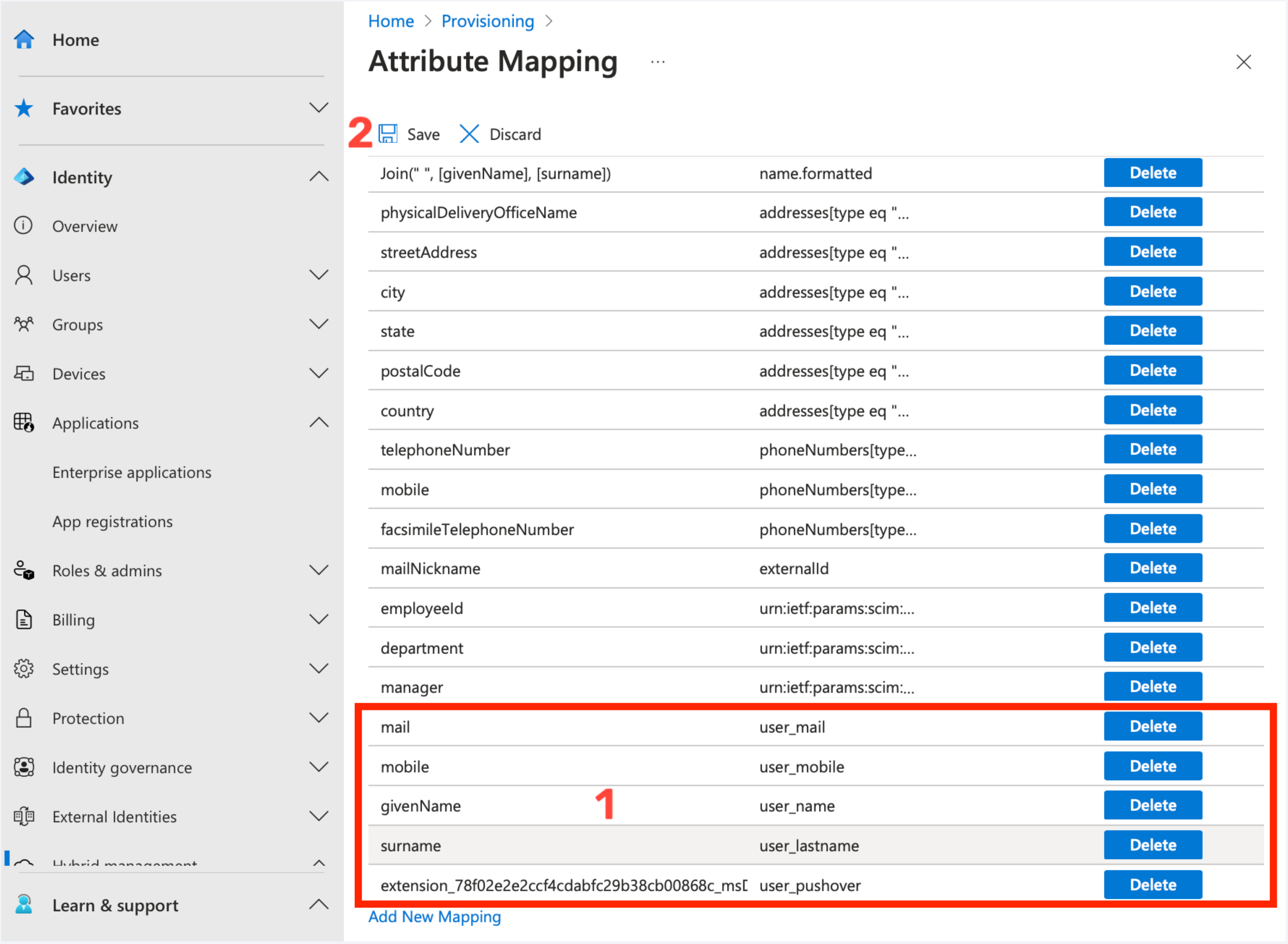
Apply this mapping: Always

Ok 3

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

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



Attribute Mapping

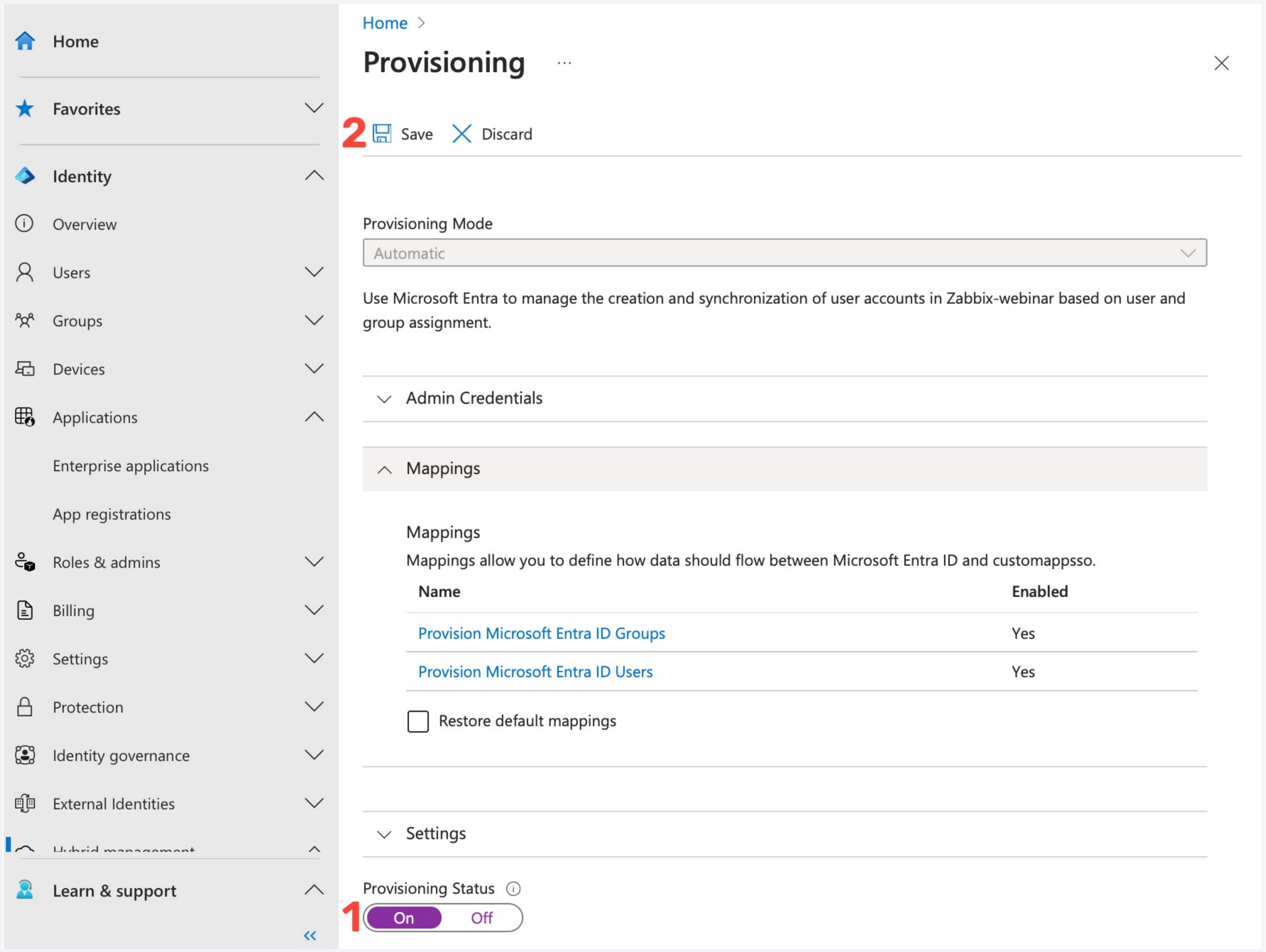
Join(" ", [givenName], [surname])	name.formatted	Delete
physicalDeliveryOfficeName	addresses[type eq "...	Delete
streetAddress	addresses[type eq "...	Delete
city	addresses[type eq "...	Delete
state	addresses[type eq "...	Delete
postalCode	addresses[type eq "...	Delete
country	addresses[type eq "...	Delete
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

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

- Zabbix SCIM provisioning
  - Enable provisioning



Provisioning Mode: Automatic

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

Mappings

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

Name	Enabled
Provision Microsoft Entra ID Groups	Yes
Provision Microsoft Entra ID Users	Yes

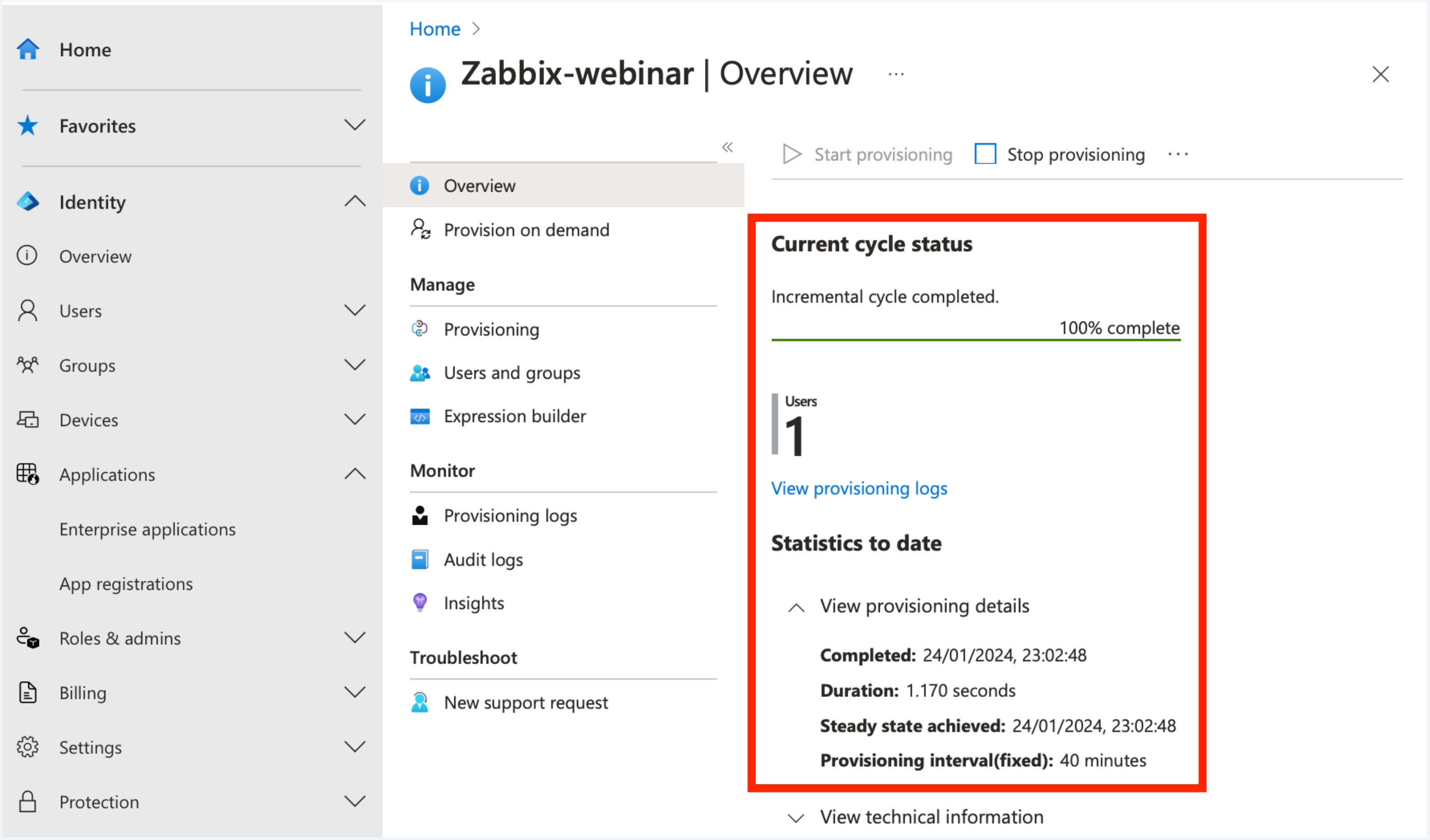
□ Restore default mappings

Provisioning Status: On

Zabbix User Provisioning JIT

SCIM – Microsoft Entra

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



Current cycle status

Incremental cycle completed.

100% complete

Users
1

View provisioning logs

Statistics to date

View provisioning details

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

View technical information

6

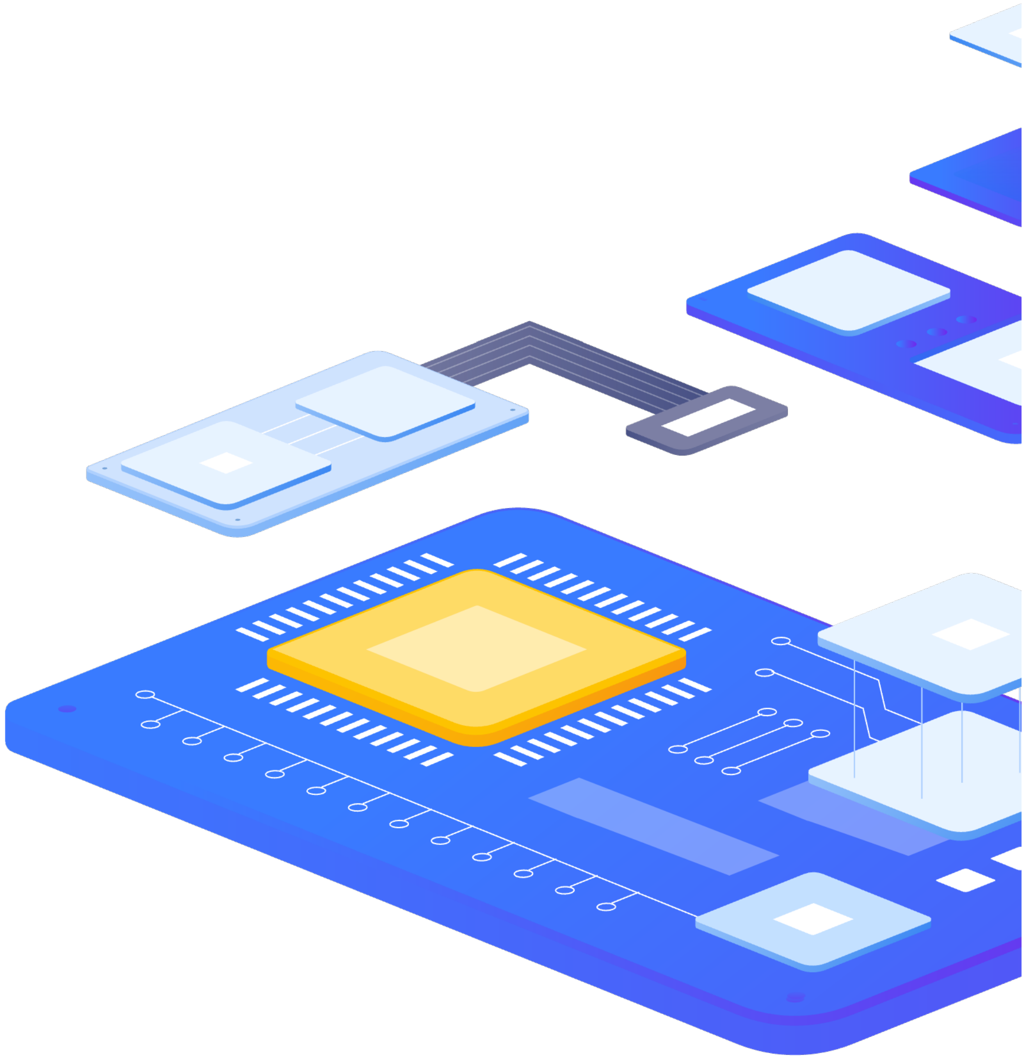
Issues and limitations

Zabbix User Provisioning JIT

initMAX

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



7

DEMO

initMAX

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