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)

initMAX

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

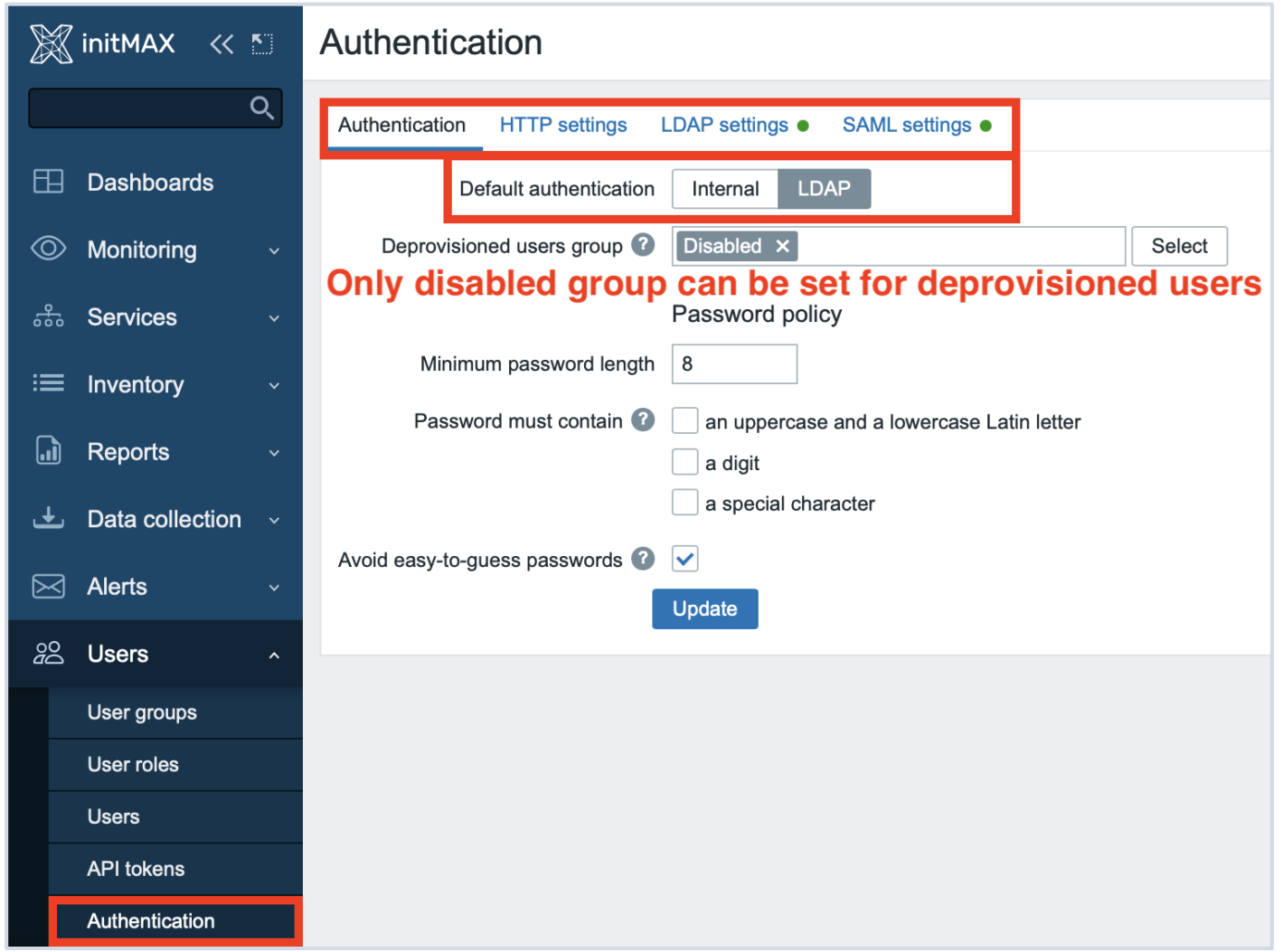
initMAX

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

initMAX

Available authentication options in ZABBIX



3

LDAP

initMAX

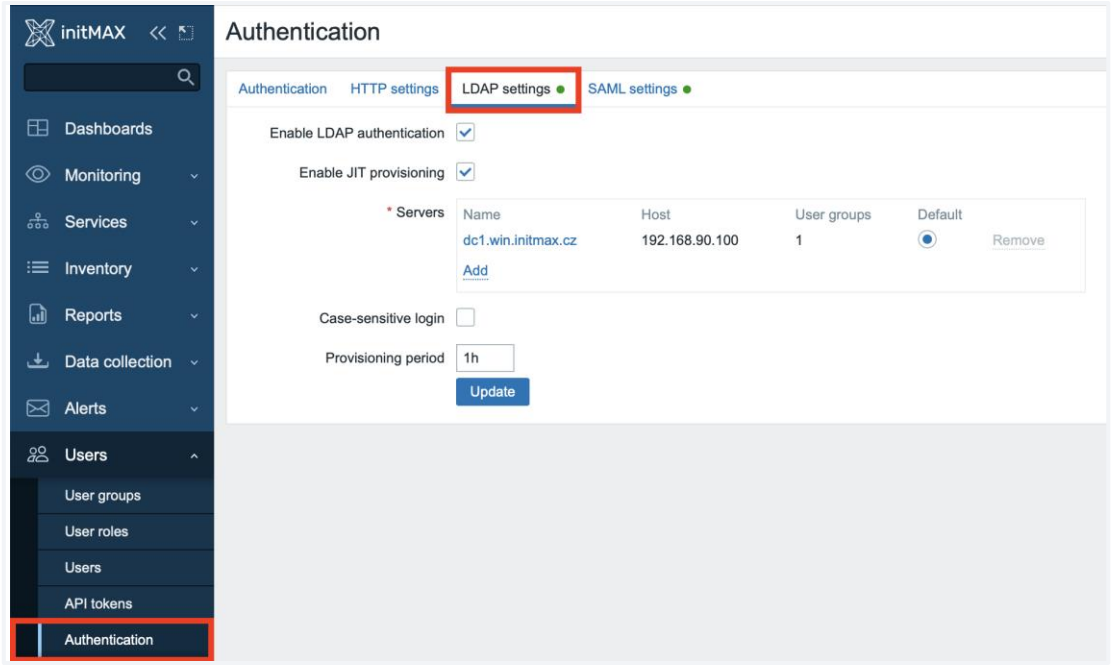
LDAP

- 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

initMAX

LDAP – Active Directory

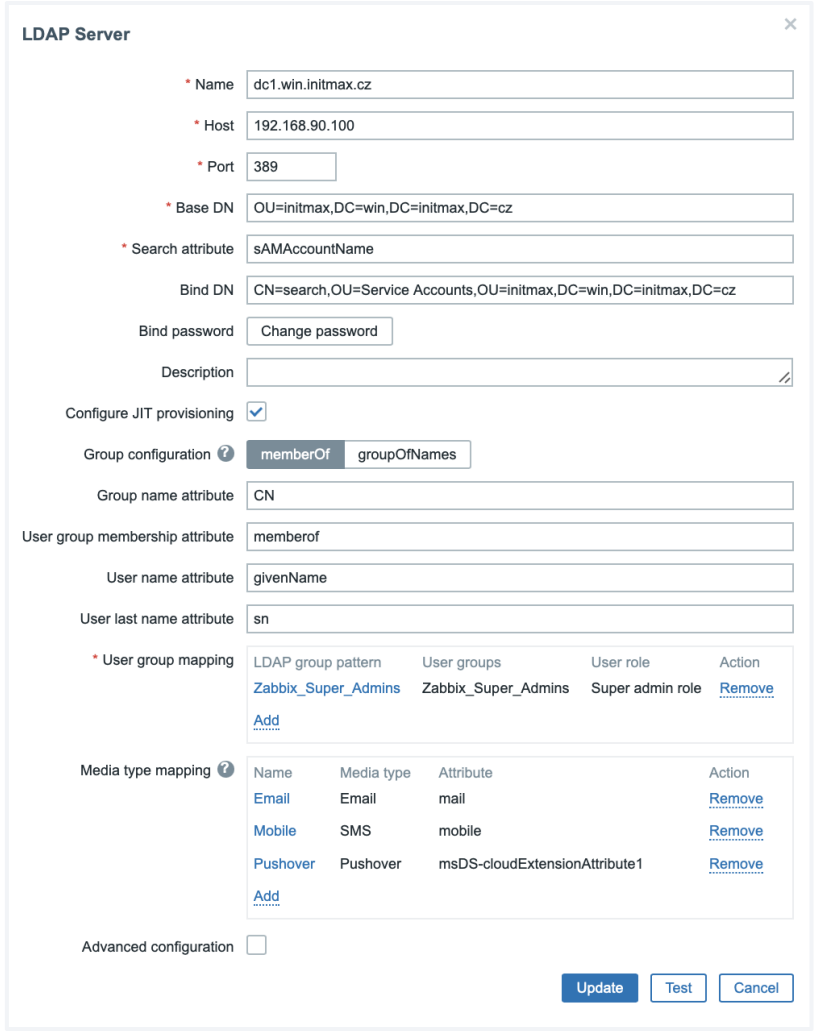
- Enable LDAP authentication
  - Mark the checkbox to enable LDAP authentication
- Enable JIT provisioning
  - Mark the checkbox to enable JIT provisioning
- Servers
  - Click on Add to configure an LDAP server
- Case-sensitive login
  - Unmark the checkbox to disable case-sensitive login (enabled by 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.



initMAX

LDAP – Active Directory

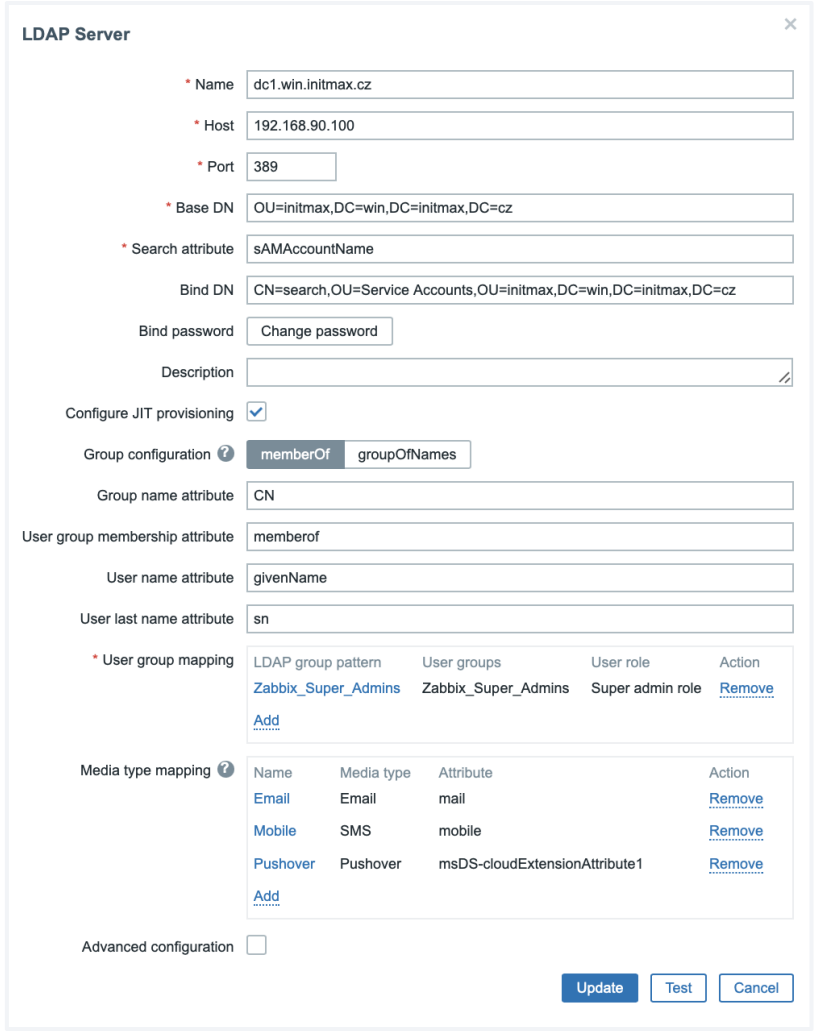
- **Name (dc1.win.initmax.cz)**
  - Name of the LDAP source in Zabbix configuration
- **Host (192.168.90.100)**
  - Host of the LDAP server
  - **ldap**://ldap.initmax.com
  - For secure LDAP server use ldaps protocol
  - **ldaps**://ldap.initmax.com
- **Port** (389, 636) Default is **389 (389)**
  - 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**



initMAX

LDAP – Active Directory

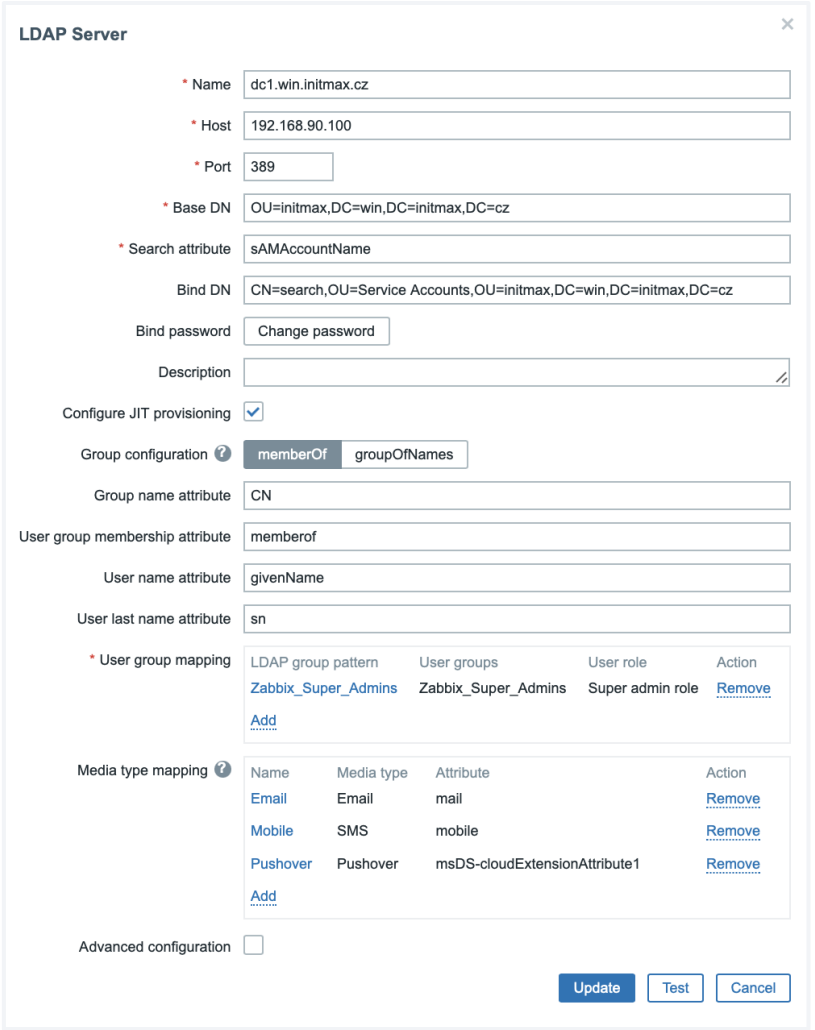
- **Search attribute (sAMAccountName)**
  - LDAP account attribute used for search
- **Bind DN**
  (CN=search,OU=Service Accounts,OU=initmax,DC=win,DC=initmax,DC=cz)
  - LDAP account for binding and searching over the LDAP server
  - Anonymous binding is also supported. Note that anonymous binding potentially 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



initMAX

LDAP – Active Directory JIT Provisioning

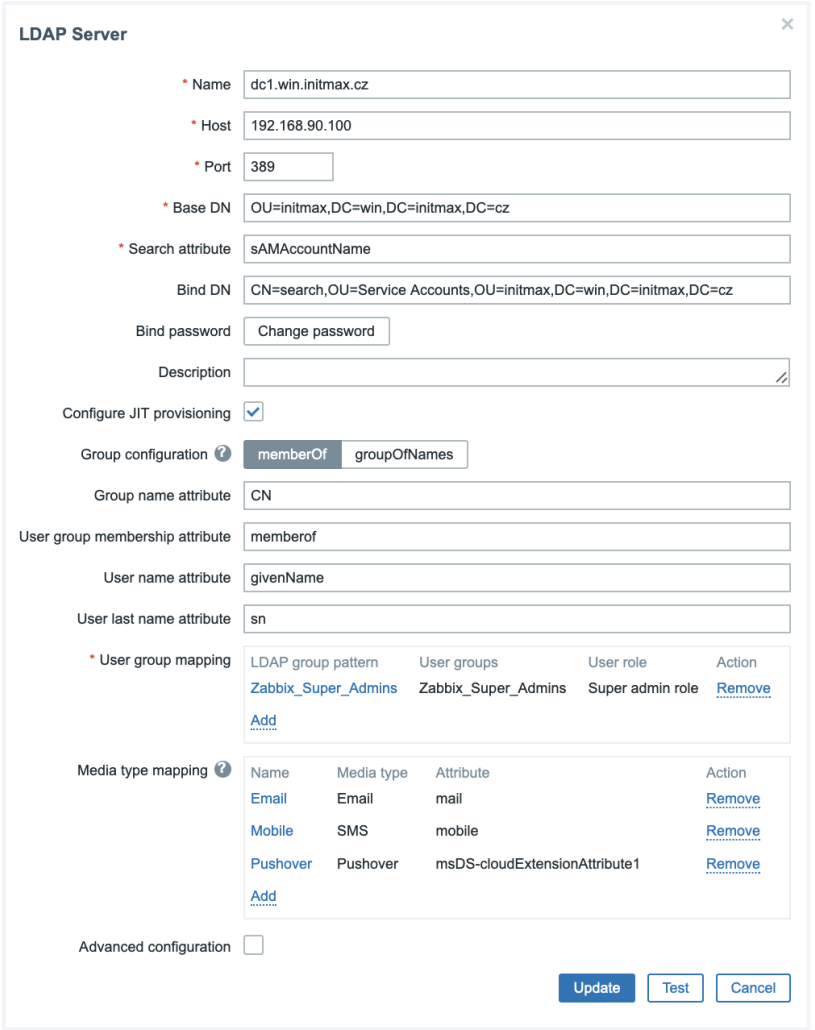
- **Configure JIT provisioning (Enable)**
  - Mark this checkbox to show options related to JIT provisioning
- **Group configuration (memberOf)**
  - memberOf - by searching users and their group membership attribute
  - groupOfNames - by searching groups through the member attribute
- **Group name attribute (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



initMAX

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.

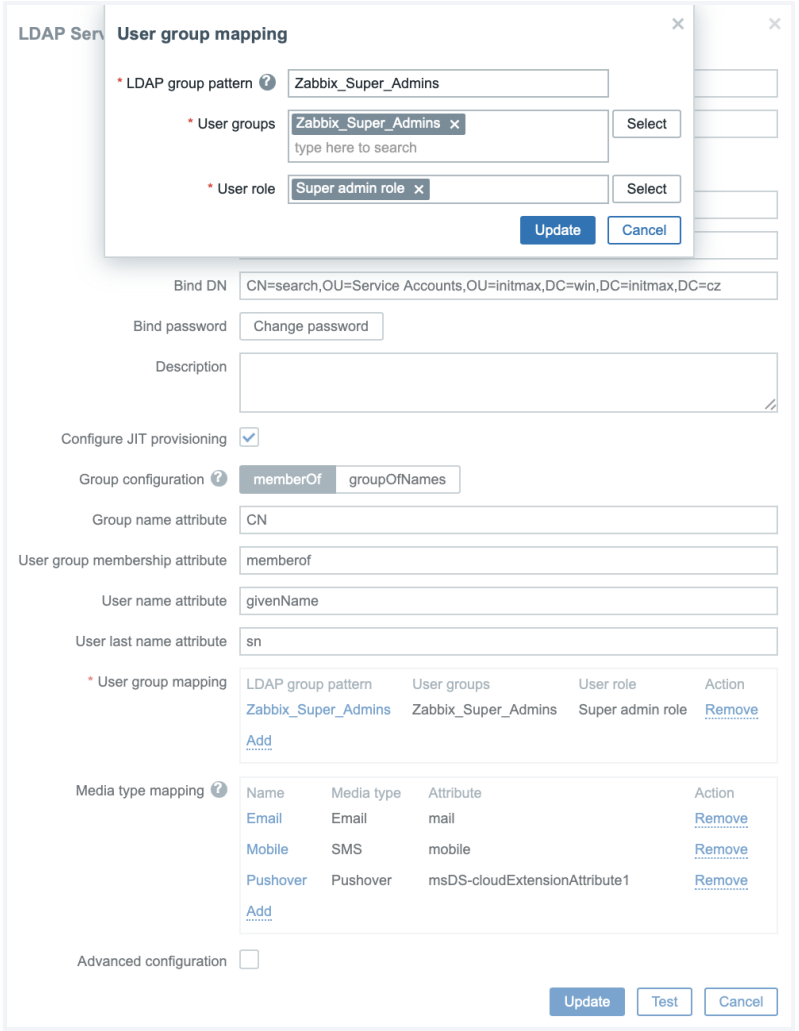


initMAX

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.

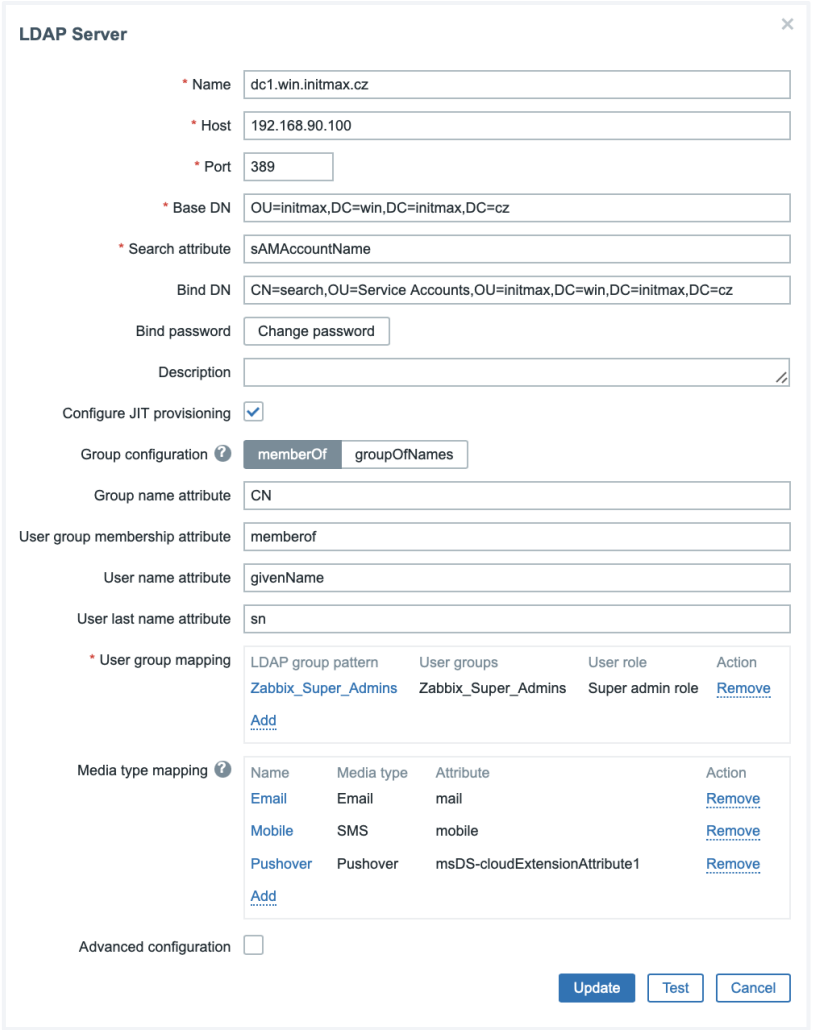
- Notes - Naming requirements
  - group name must match LDAP group name
  - wildcard patterns with '*' may be used



initMAX

LDAP – Active Directory JIT Provisioning

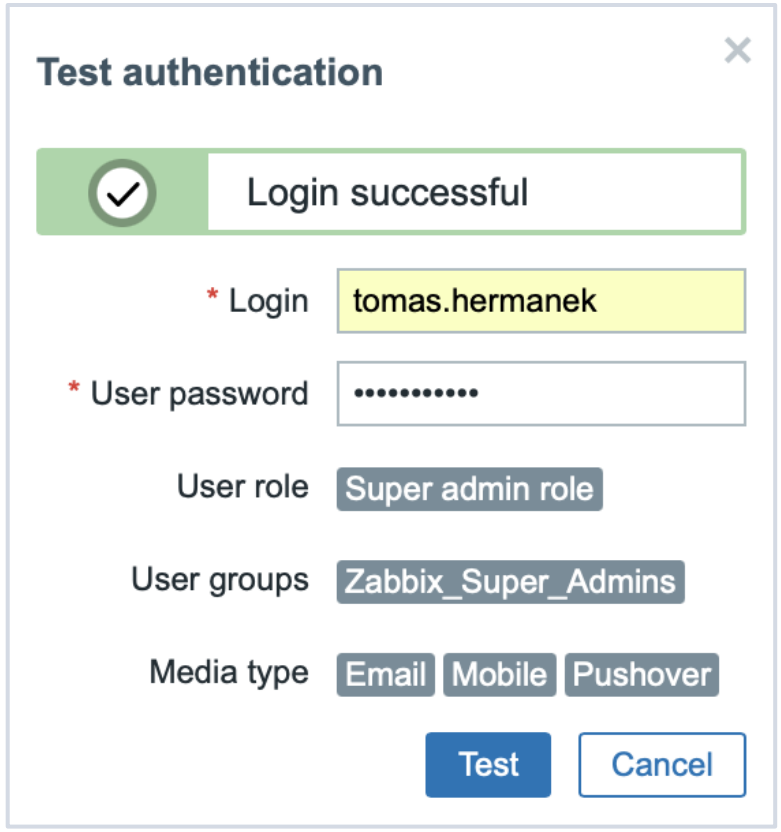
- **Media type mapping**
  - Map the user's LDAP media attributes to Zabbix user media for sending notifications
- **Advanced configuration**
  - Mark this checkbox to show advanced configuration options
- **StartTLS**
  - Mark the checkbox to use the StartTLS operation when connecting to LDAP server. 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}).



initMAX

LDAP – Notes

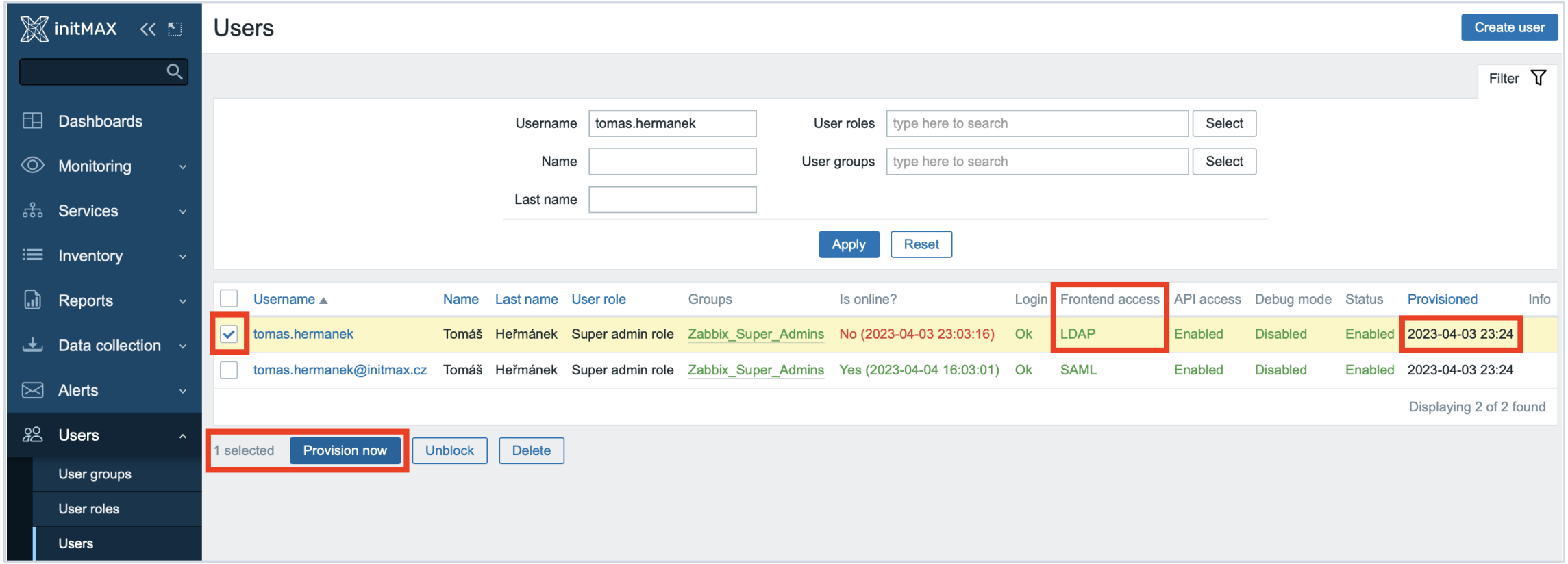
- The Test button allows to test user access



initMAX

LDAP – Notes

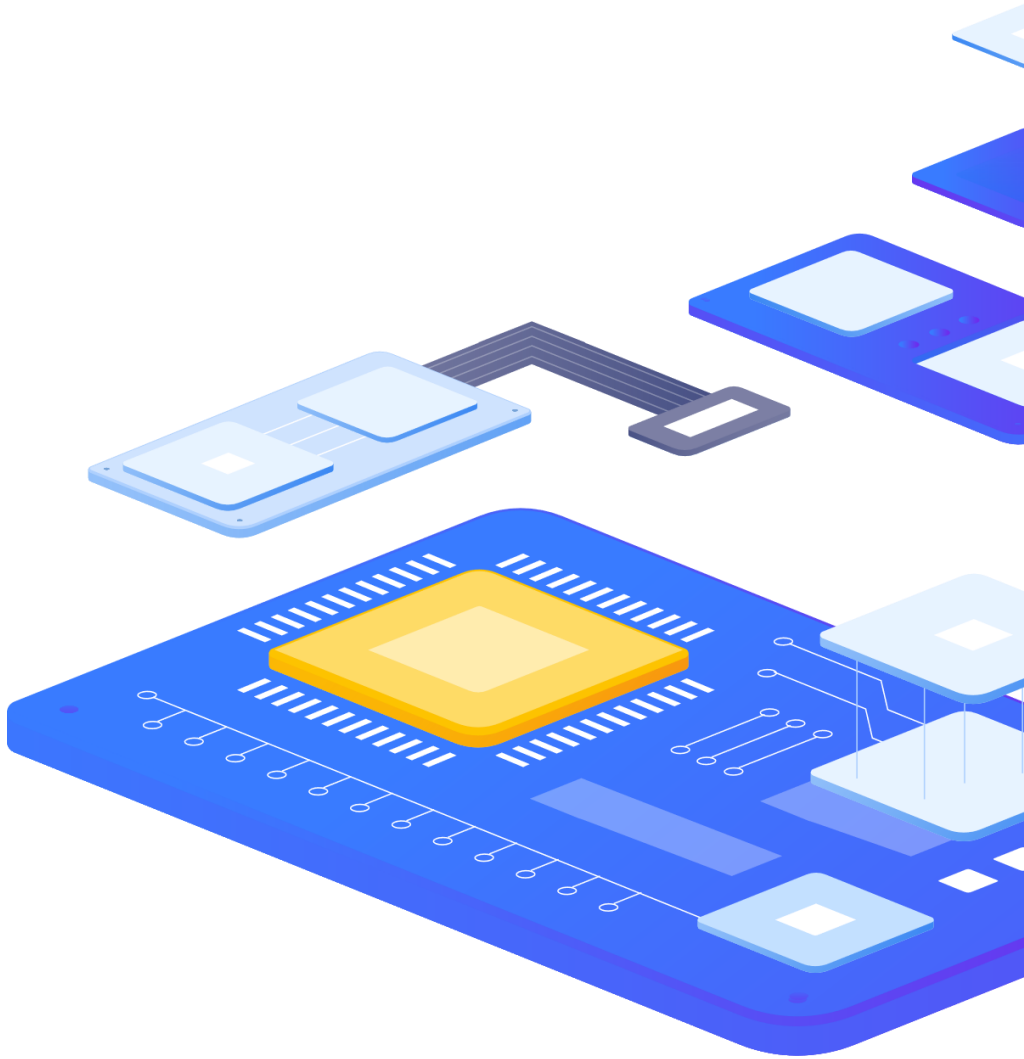
- If you are using binding user, you can use “Provision now” button on LDAP users (Default authentication need to be set up as LDAP)



initMAX

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.
- Authentification 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

initMAX

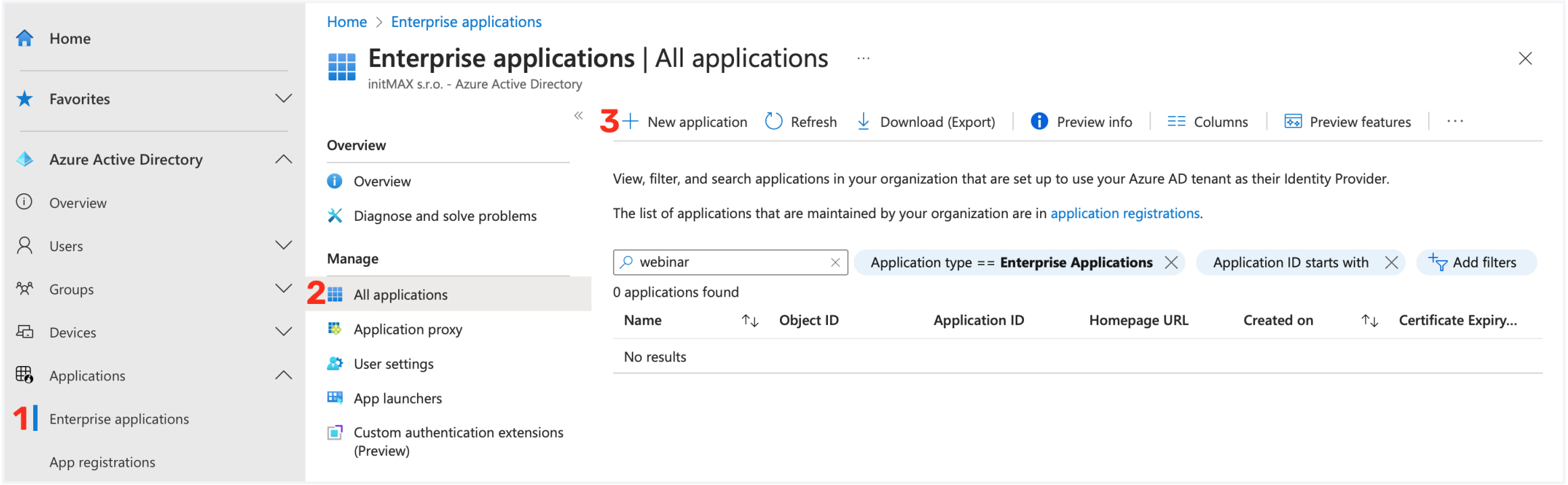
SAML

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

Zabbix User Provisioning JIT

SAML – Zabbix - Azure

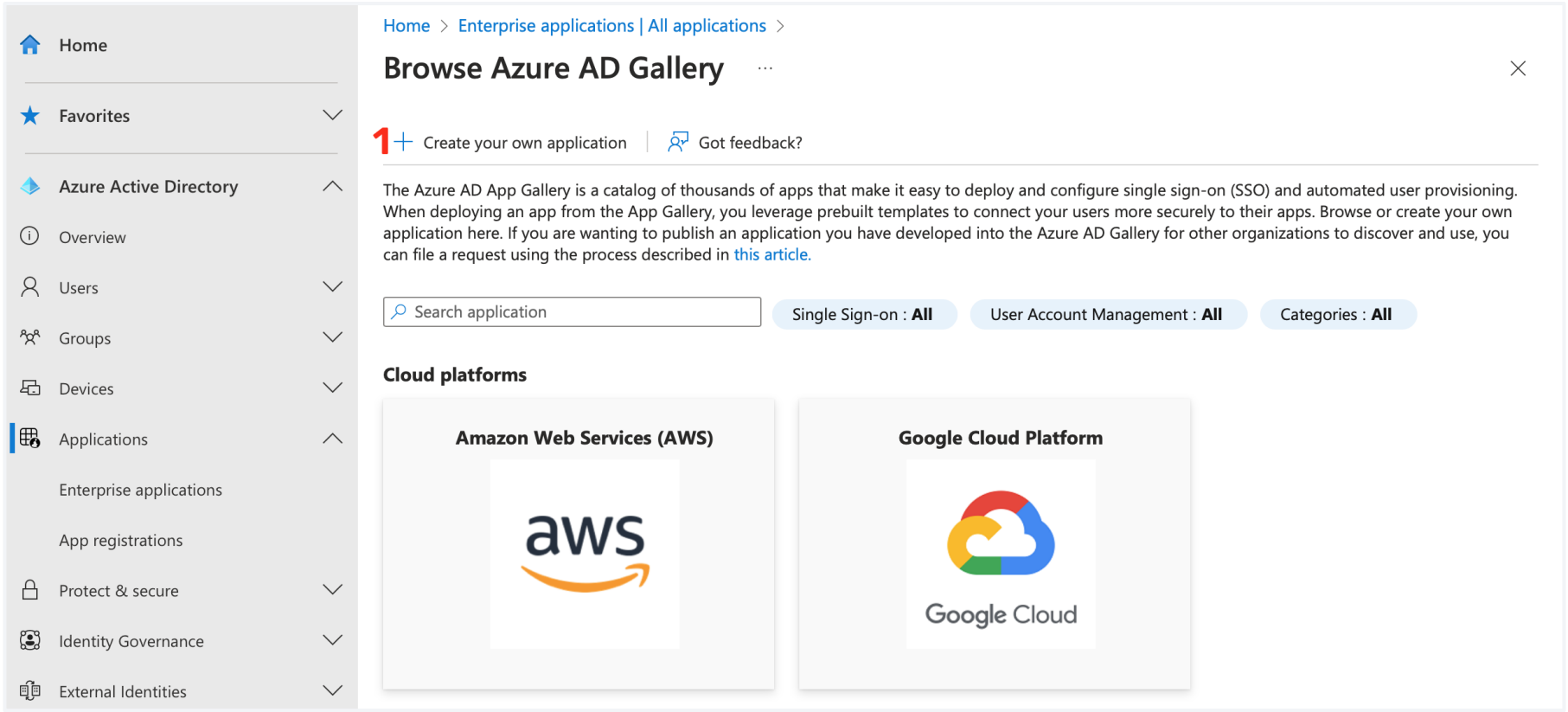
- Create your new Enterprise application
  - We need this application for our SAML setting



Zabbix User Provisioning JIT

SAML – Zabbix - Azure

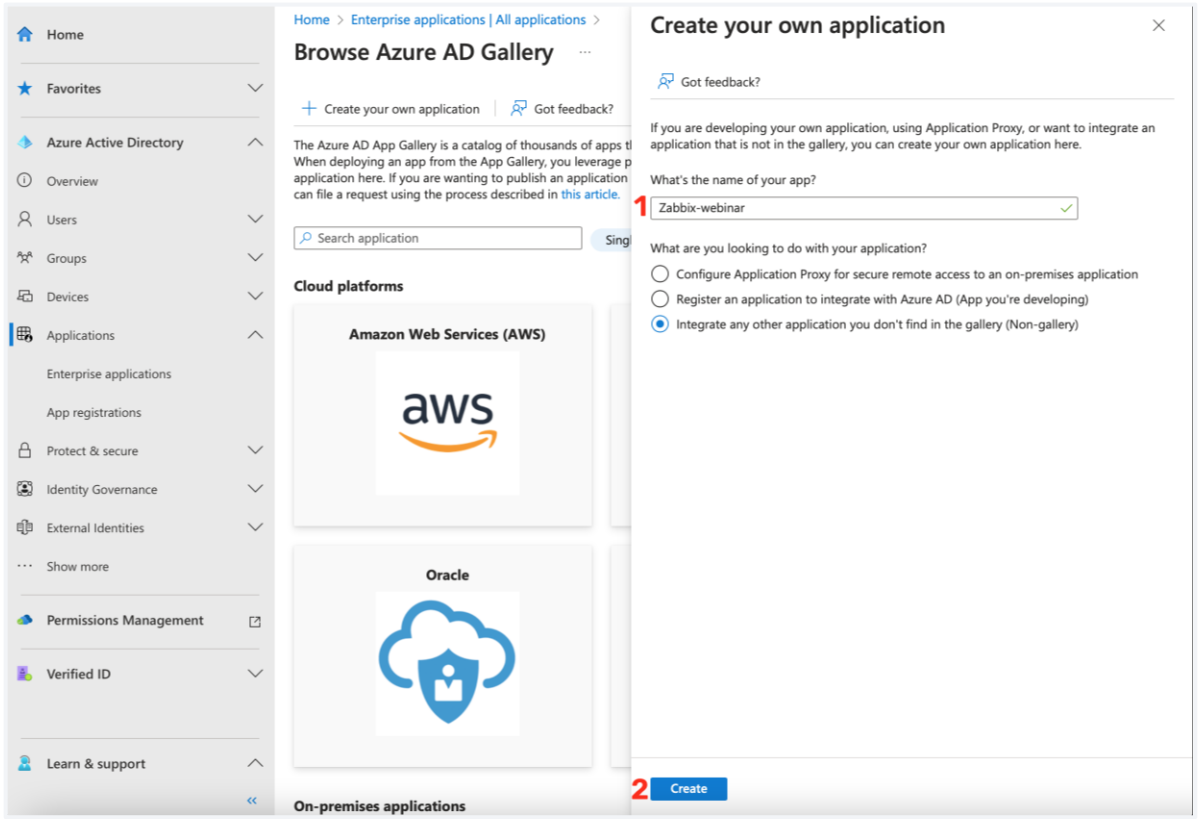
- Create your new Enterprise application
  - Hit button “Create your own application”



initMAX

SAML – Zabbix - Azure

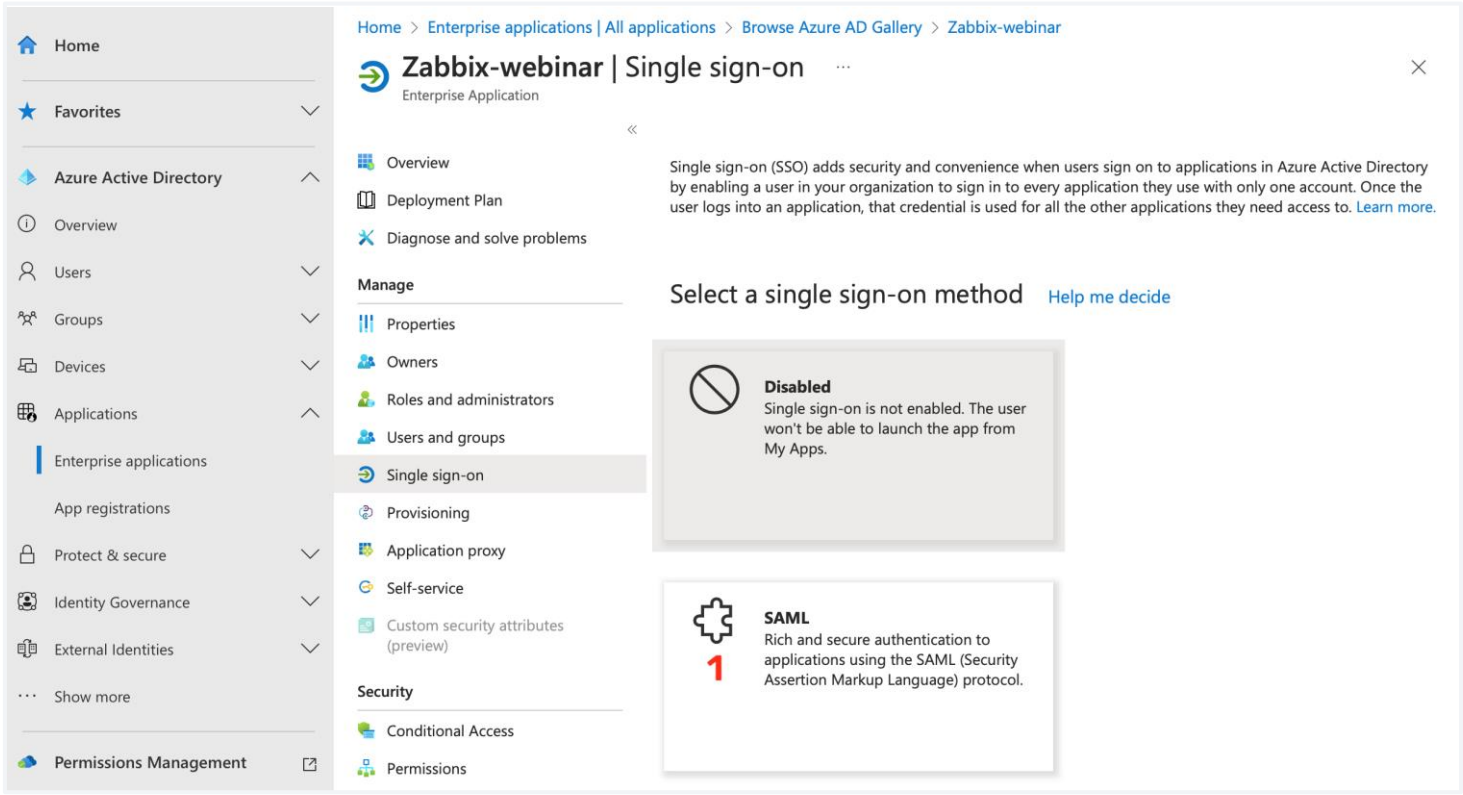
- Create your new Enterprise application
  - Chose your own application name



initMAX

SAML – Zabbix - Azure

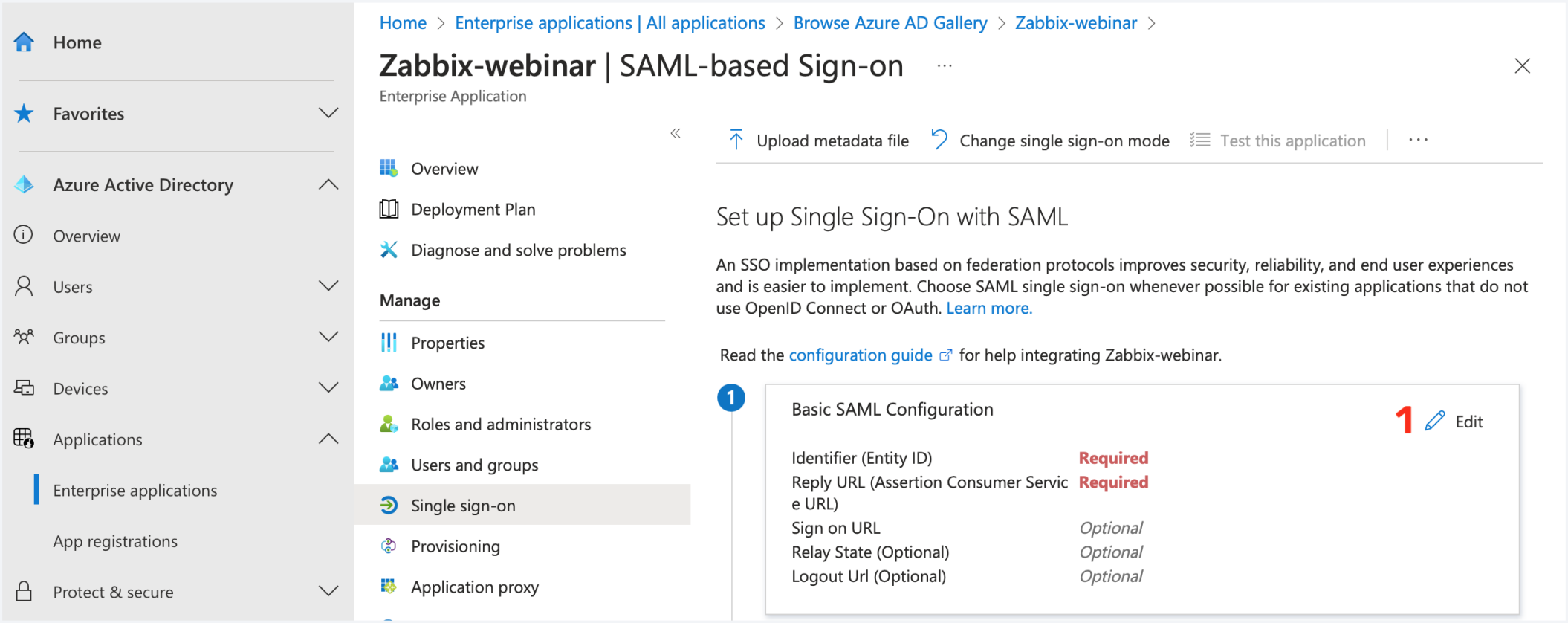
- Single sign-on setting
  - Select SAML as a sign-on metod



Zabbix User Provisioning JIT

SAML – Zabbix - Azure

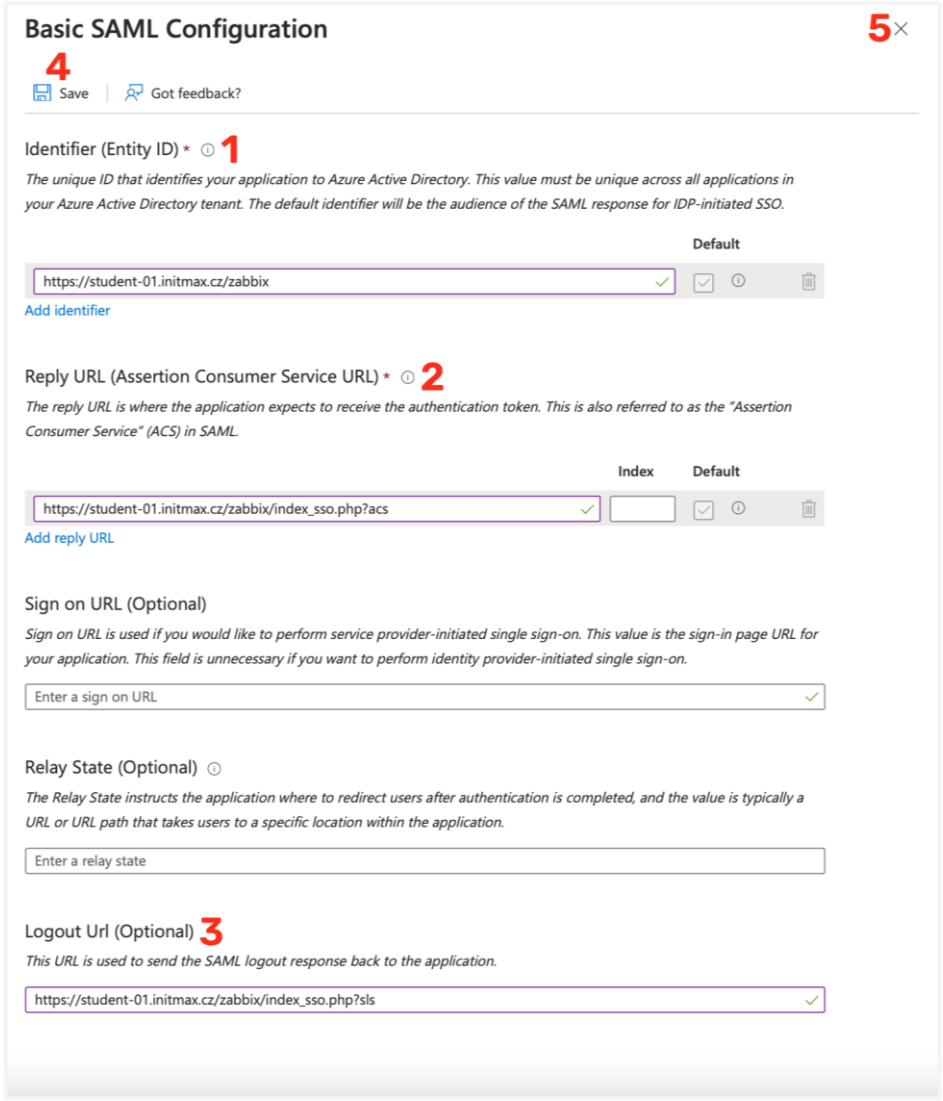
- Single sign-on setting
  - Edit basic SAML configuration



Zabbix User Provisioning JIT

SAML – Zabbix - Azure

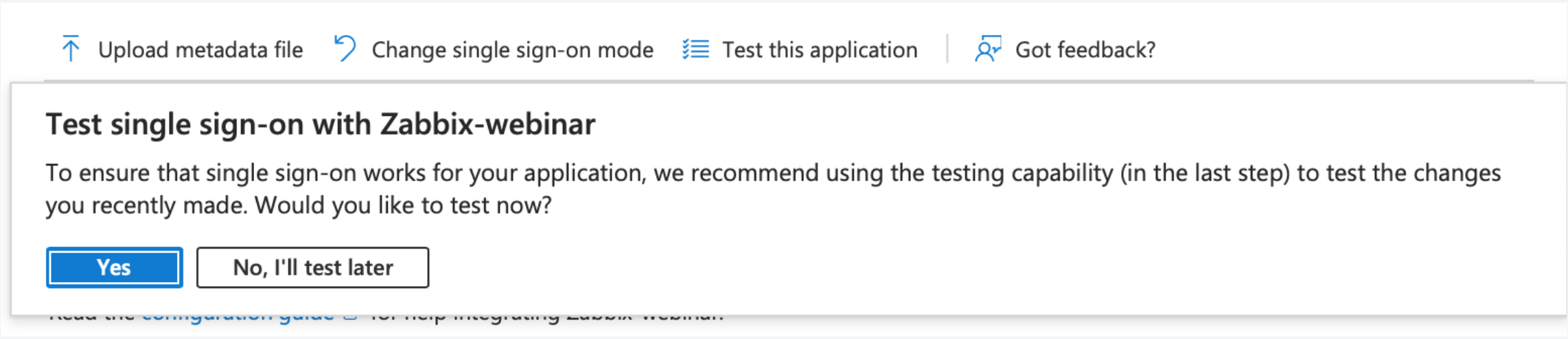
- Single sign-on setting
  - **Fill Entity ID** (We are using Zabbix URL) **https://student-01.initmax.cz/zabbix**
  - **Reply URL** (here is where Zabbix expecting authentication token) **https://student-01.initmax.cz/zabbix/index_sso.php?acs**
  - **Logout URL** (This is optional)
  - https://student-01.initmax.cz/zabbix/index_sso.php?sls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



initMAX

SAML – Zabbix - Azure

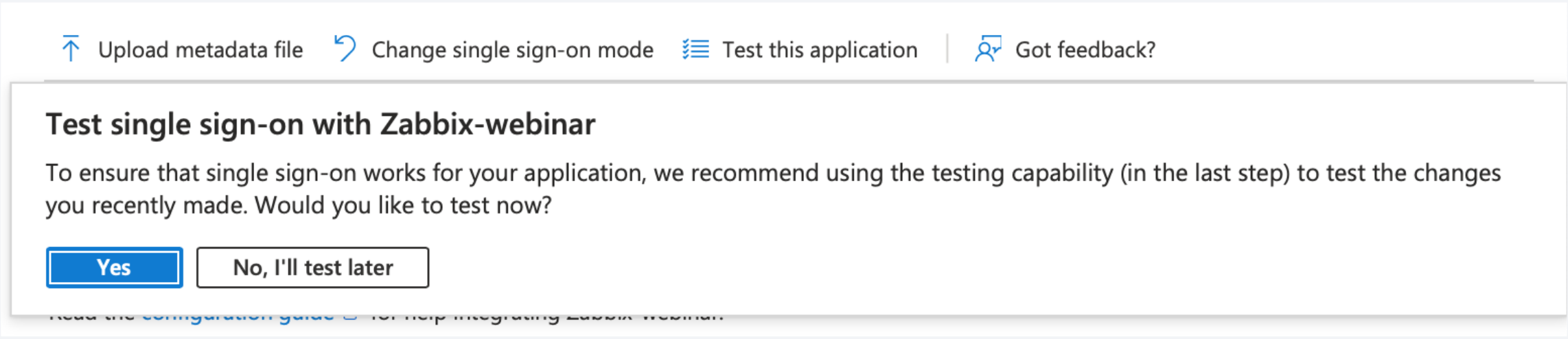
- Single sign-on setting
  - Close test popup



initMAX

SAML – Zabbix - Azure

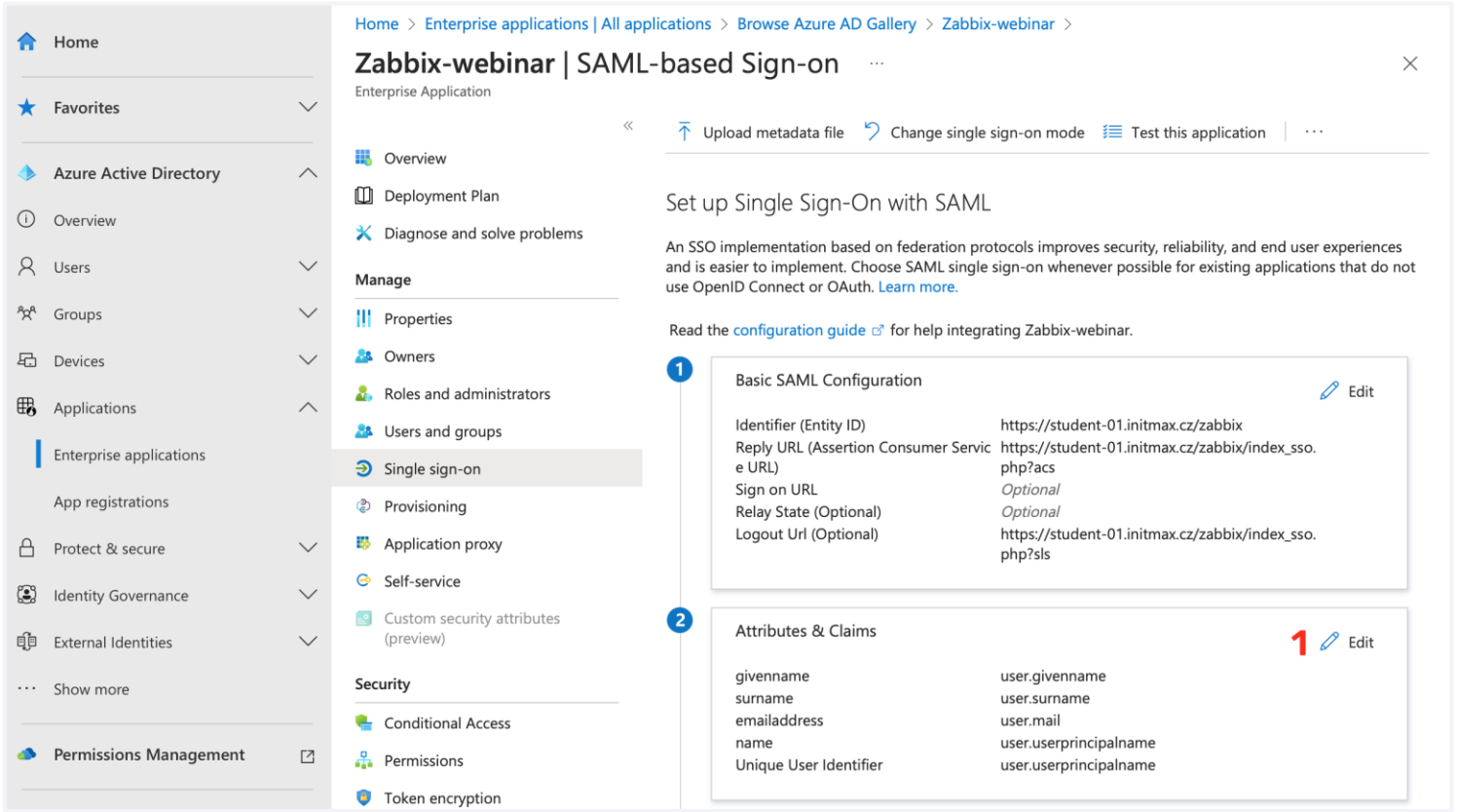
- Single sign-on setting
  - Close test pop



Zabbix User Provisioning JIT

SAML – Zabbix - Azure

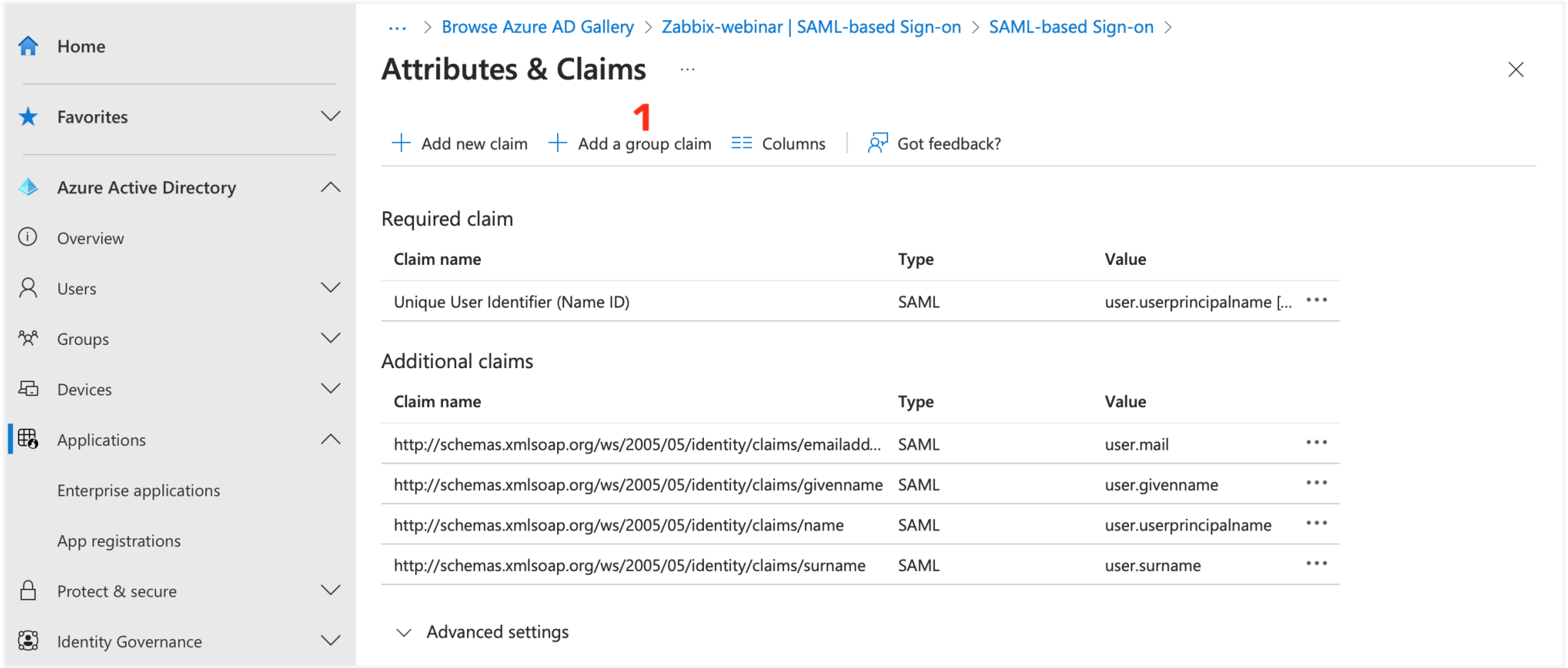
- Single sign-on setting
  - Edit Attributes & Claims



initMAX

SAML – Zabbix - Azure

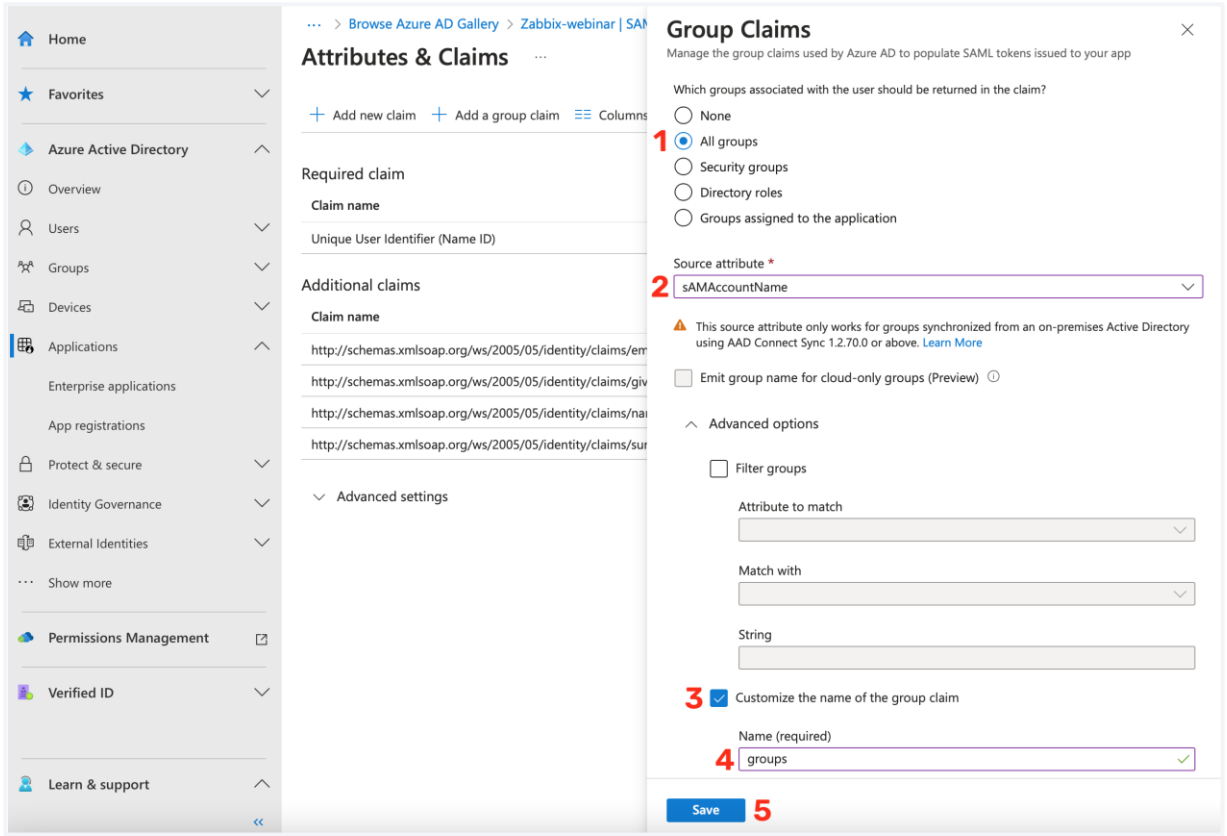
- Single sign-on setting
  - We need to add group claim for JIT (We show how this work in Zabbix later)



Zabbix User Provisioning JIT

SAML – Zabbix - Azure

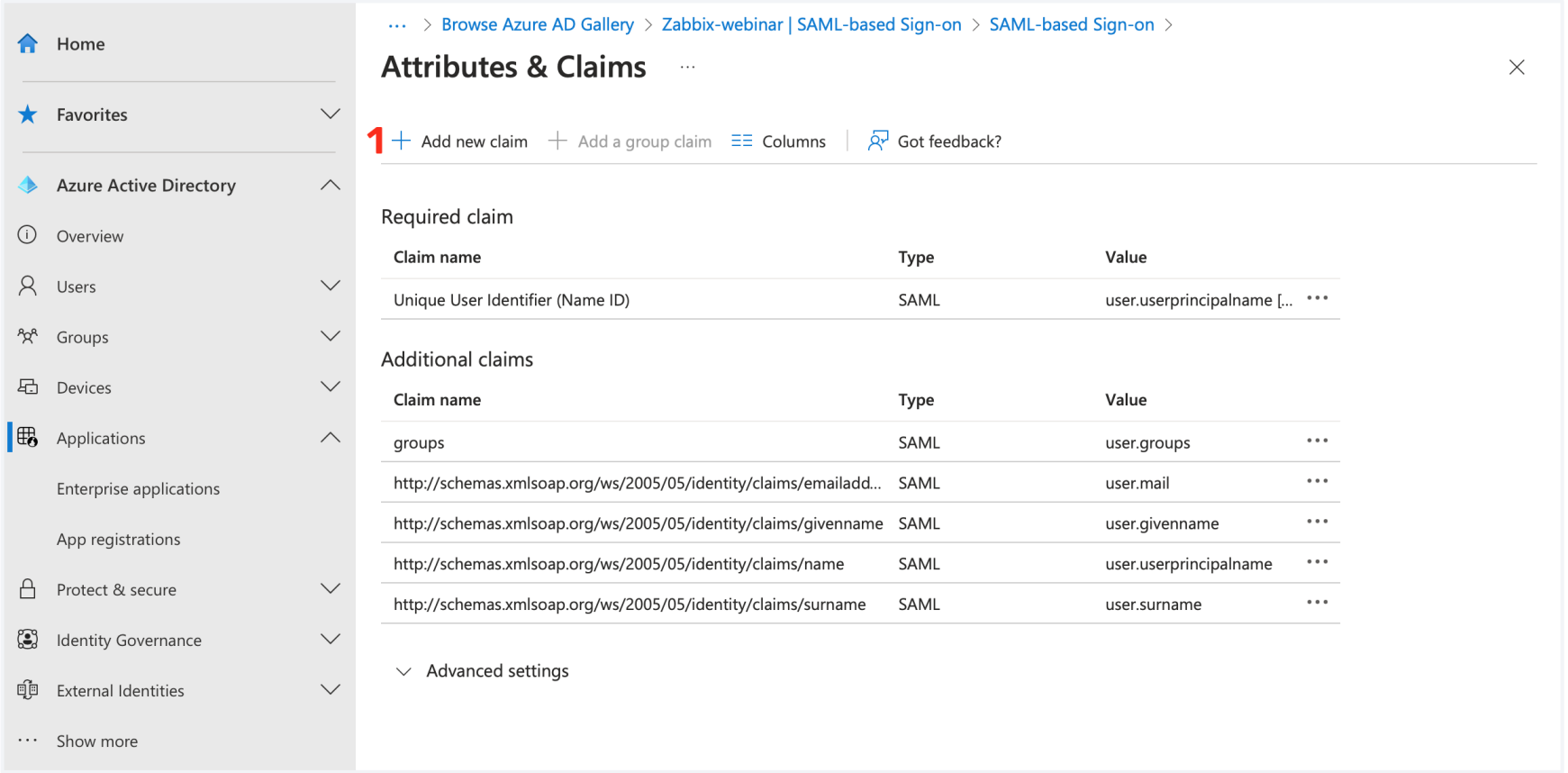
- Single sign-on setting
  - Here we are using basic setting for groups claim (We have hybrid environment)
  - This setting can be tuned!



Zabbix User Provisioning JIT

SAML – Zabbix - Azure

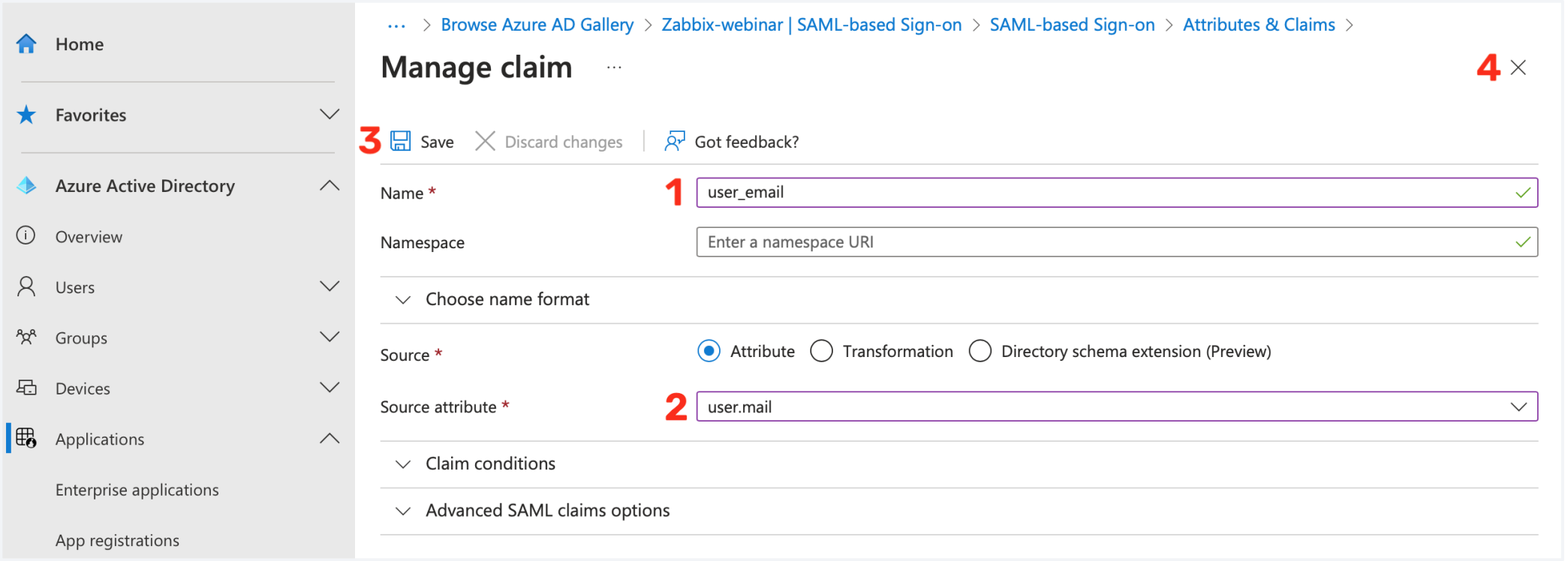
- Single sign-on setting
  - We need to add new claim for username and additionally for first name, last name and medias



Zabbix User Provisioning JIT

SAML – Zabbix - Azure

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



Zabbix User Provisioning JIT

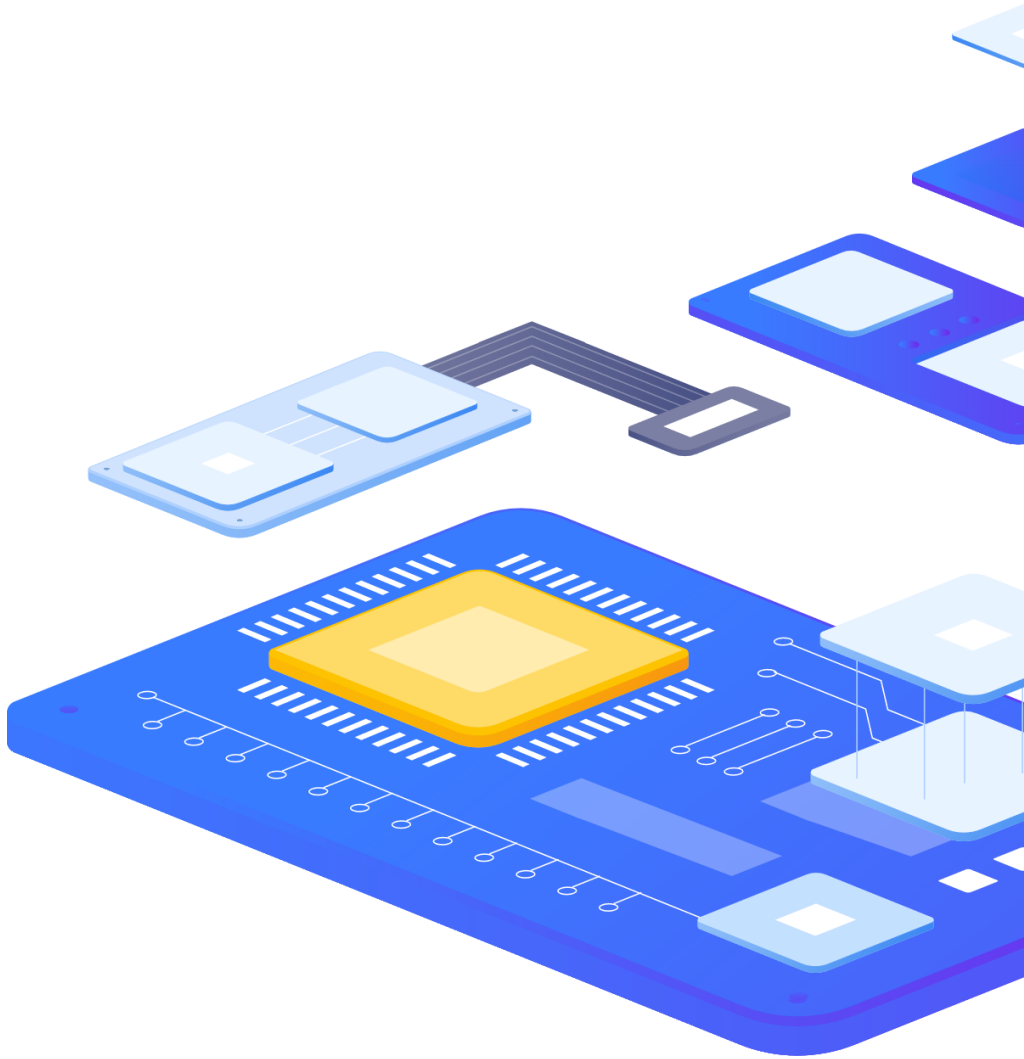
SAML – Zabbix - Azure

- Single sign-on setting
  - Repeat this operation for all your attributes **email 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_email	**user.mail**

Optional claims

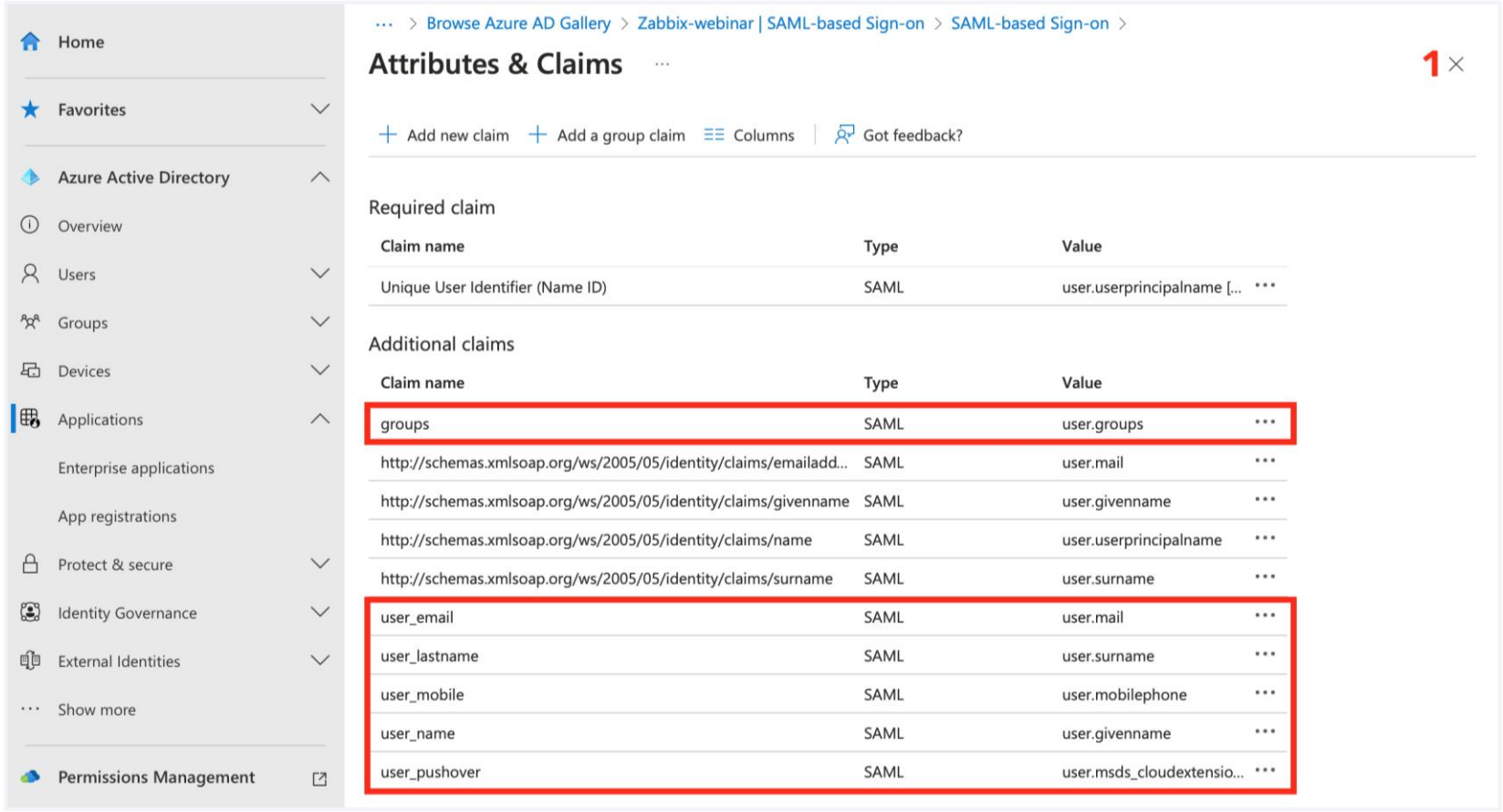
user_mobile	user.mobilephone
user_lastname	user.surname
user_name	user.givenname
user_pushover	user.msds_cloud…



Zabbix User Provisioning JIT

SAML – Zabbix - Azure

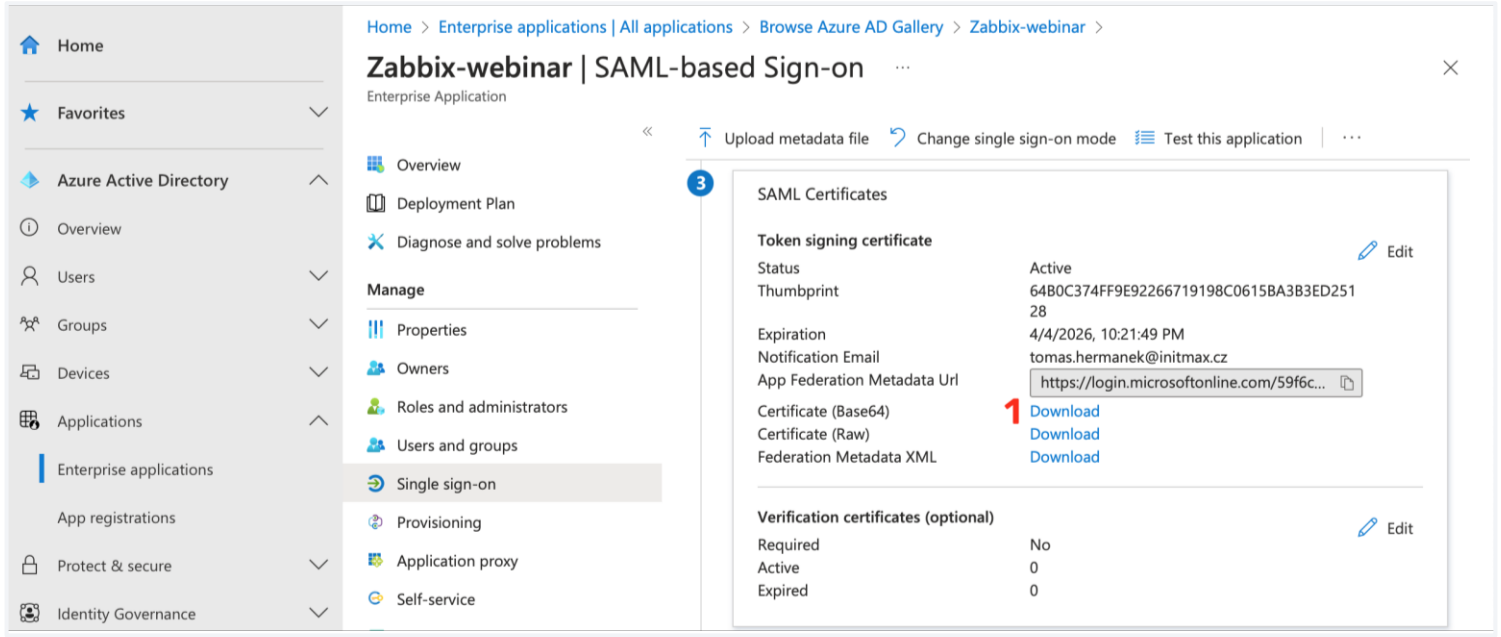
- Single sign-on setting



initMAX

SAML – Zabbix - Azure

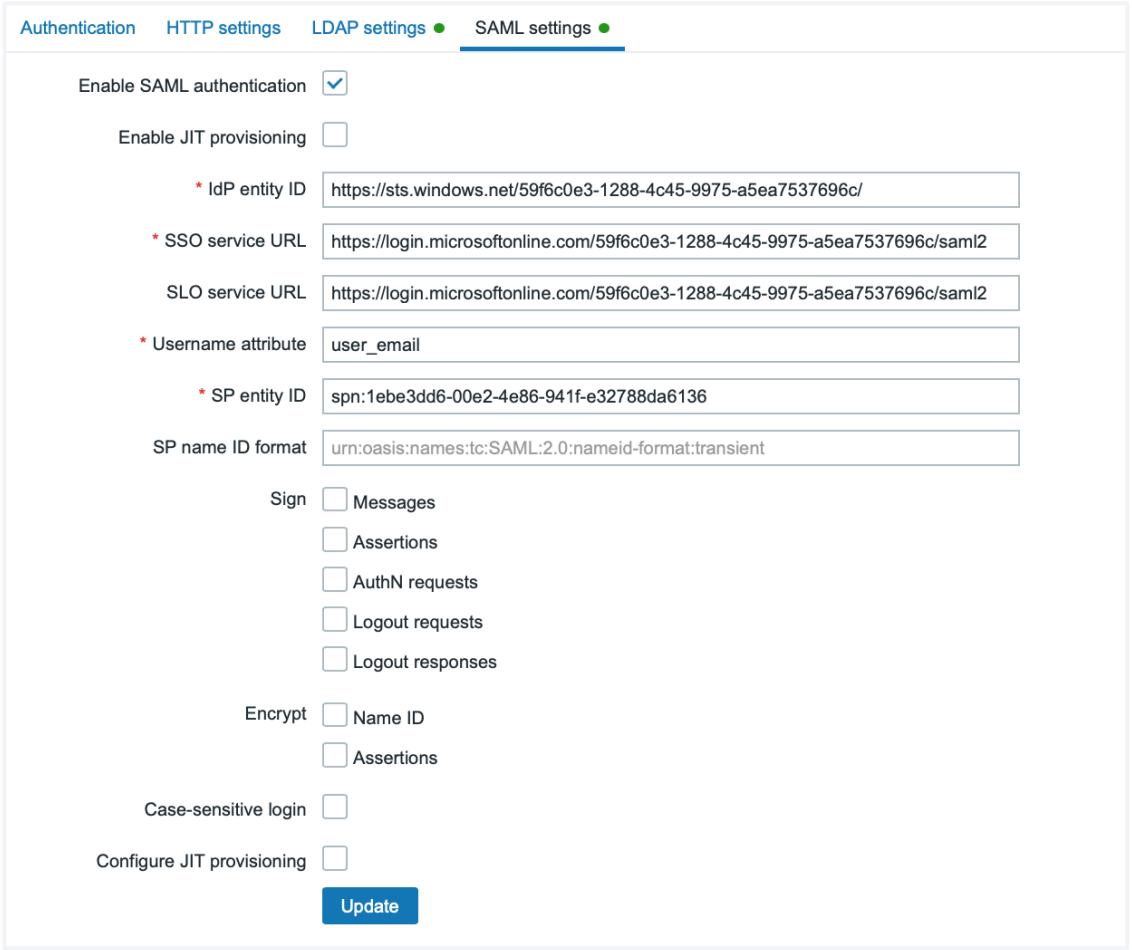
- Single sign-on setting
  - Last part for SAML setting in Azure is export certificate for signed Zabbix tokens (Base64)



initMAX

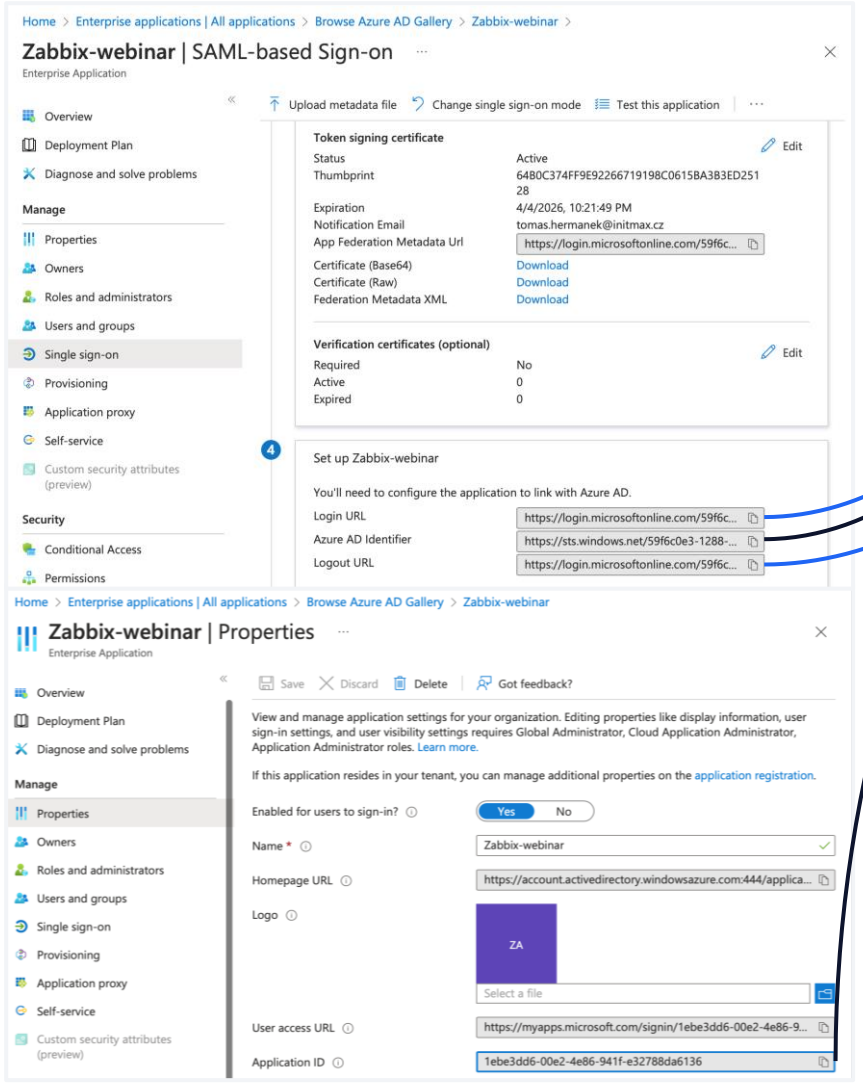
SAML – Zabbix

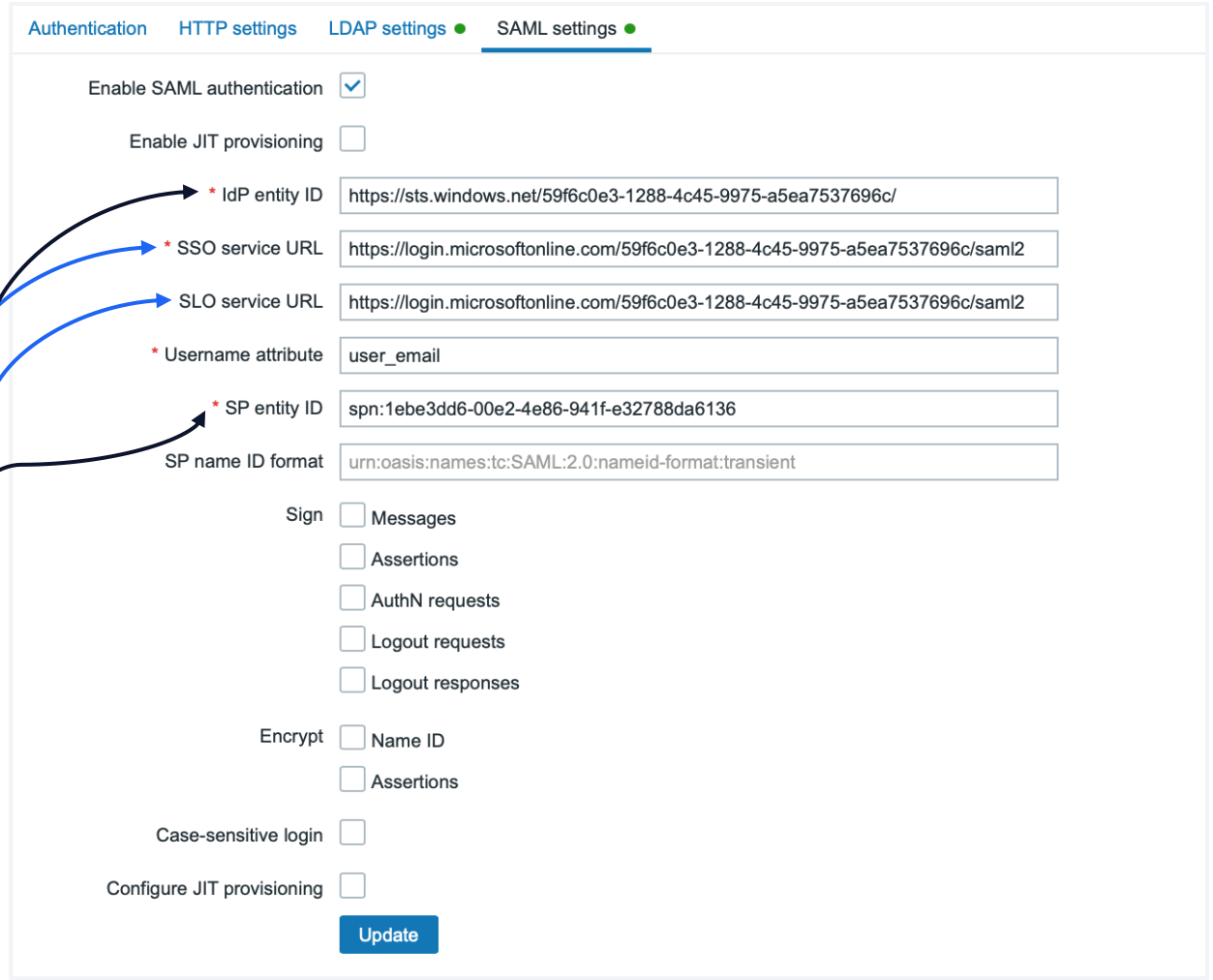
- Enable SAML authentication
  - Mark the checkbox to enable SAML authentication
- Enable JIT provisioning (we discuss this later)
  - Mark the checkbox to enable JIT provisioning
- IdP entity ID (In Azure AD is named "**Azure AD Identifier**")
  - The unique entity identifier within the SAML identity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



Zabbix User Provisioning JIT

SAML – Zabbix





initMAX

SAML – Zabbix

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

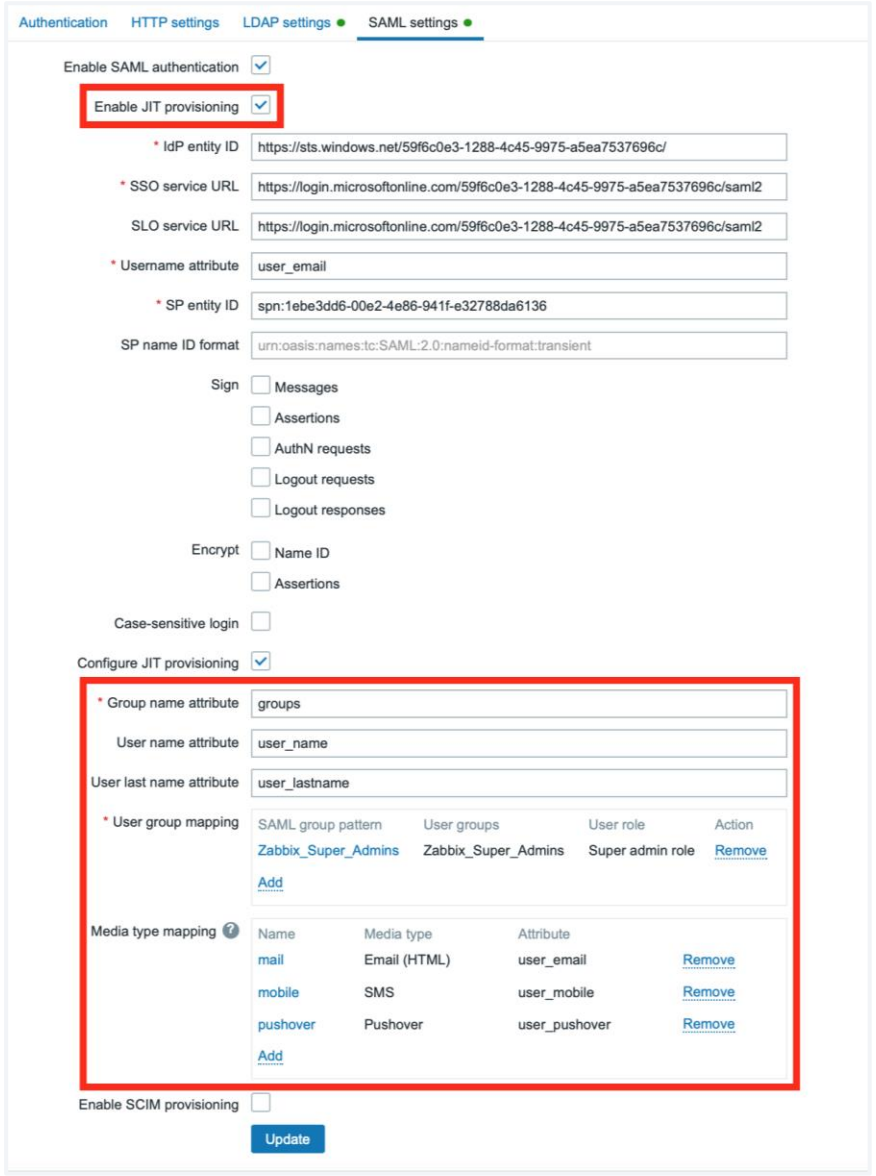
```
// Used for SAML authentication.
// Uncomment to override the default paths to SP private key, SP and IdP X.509 certificates, and to set extra settings.
//$SSO['SP_KEY']                        = 'conf/certs/sp.key';
//$SSO['SP_CERT']                       = 'conf/certs/sp.crt';
$SSO['IDP_CERT'] 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

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

Zabbix User Provisioning JIT

SAML – Zabbix JIT

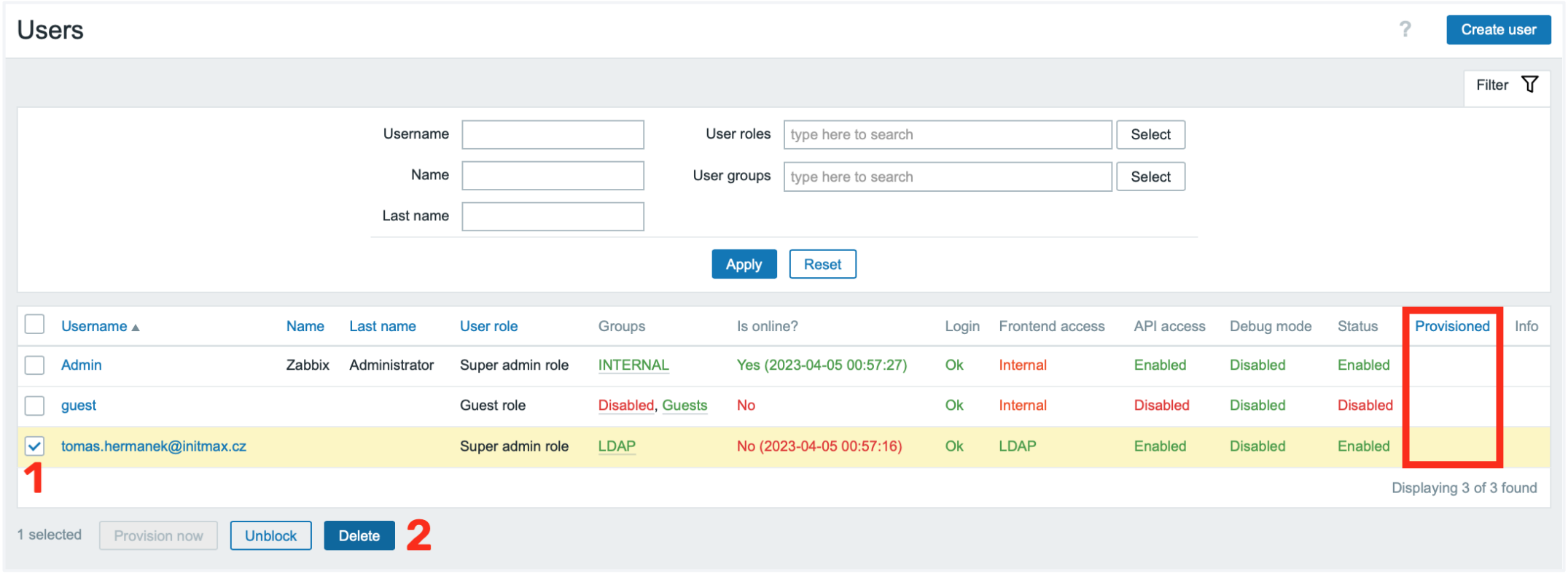
- Zabbix SAML JIT provisioning
  - Enable JIT provisioning
  - Fill Group name attribute
  - Fill User user name attribute
  - Fill User last name attribute
  - Create correct group mapping for groups
  - Create correct setting for Media type mapping



initMAX

SAML – Zabbix JIT

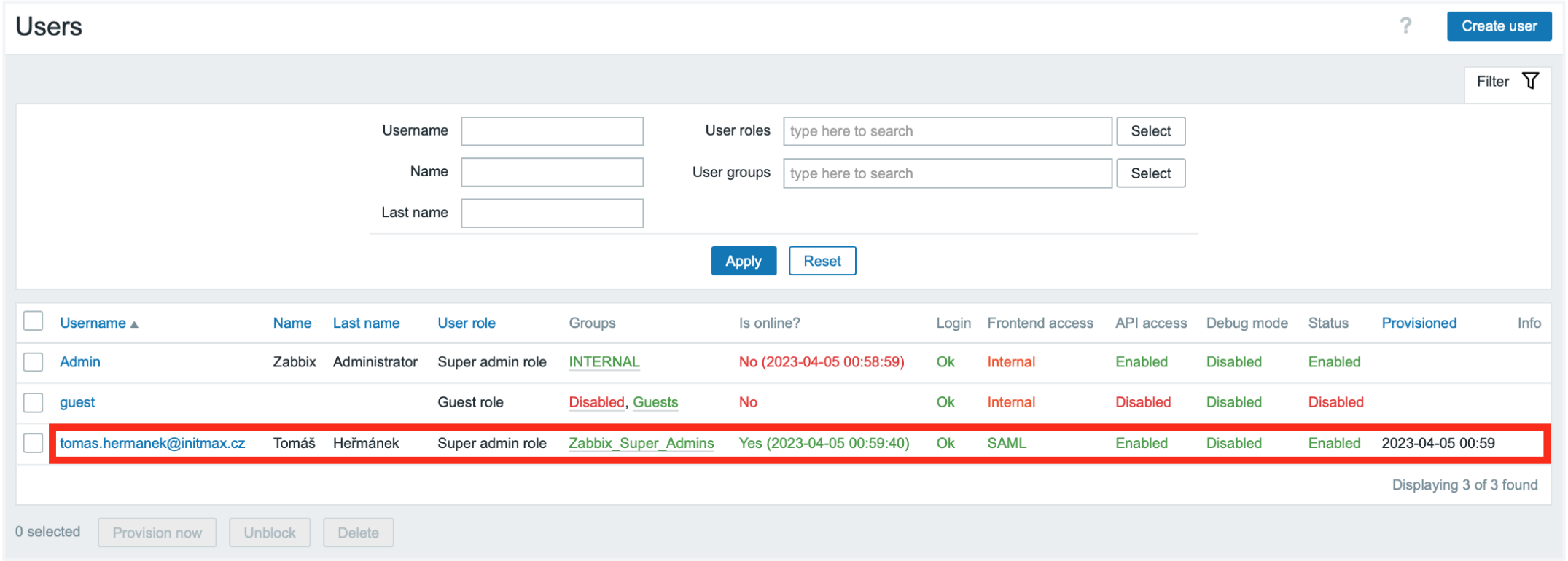
- Zabbix SAML JIT provisioning
  - Delete your manually created user or use SQL statement for user update where (update users set userdirectoryid =2 where userid=X;) userid is your user ID in Zabbix



initMAX

SAML – Zabbix JIT

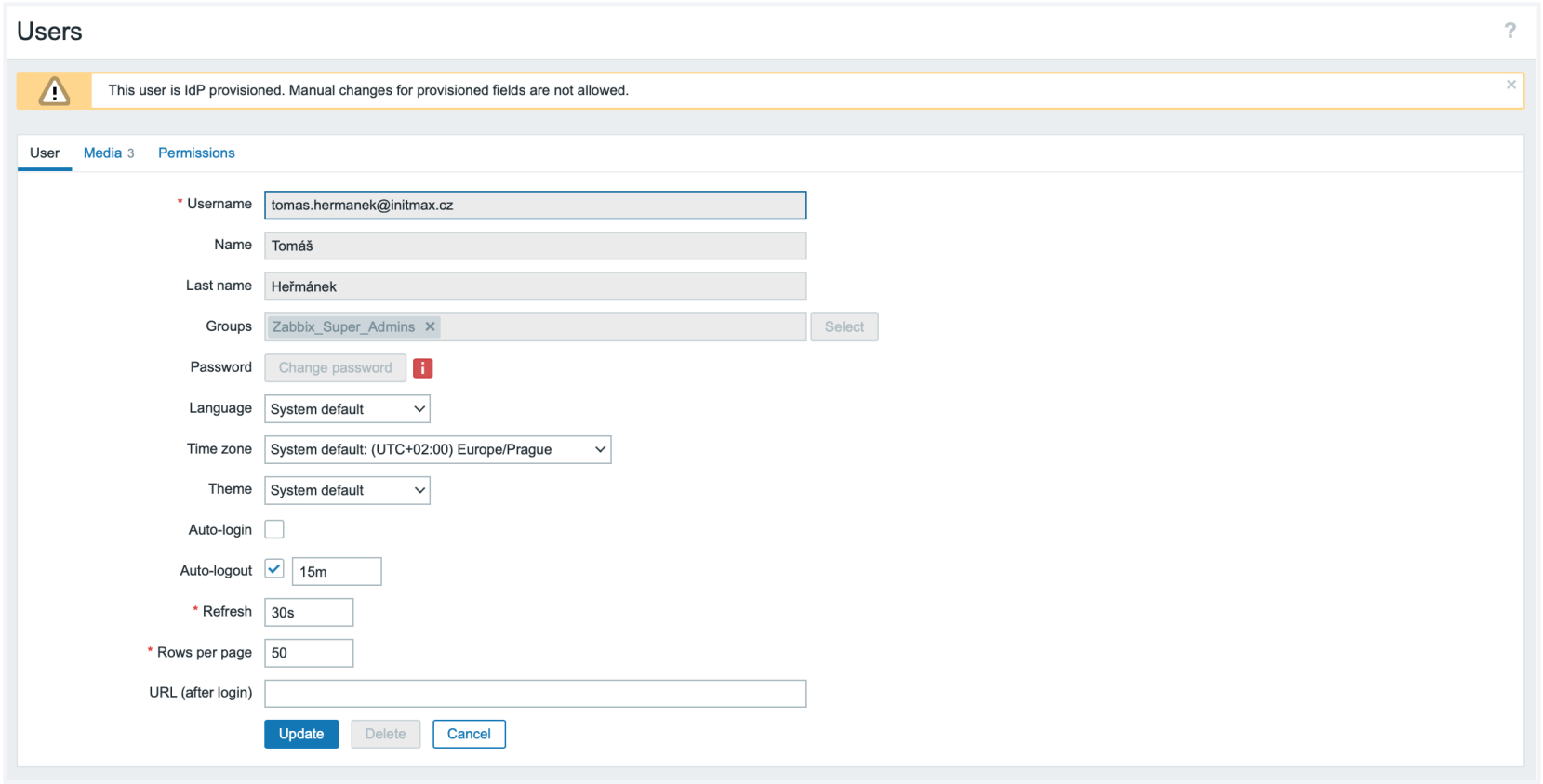
- Zabbix SAML JIT provisioning
  - Check your provisioned user



initMAX

SAML – Zabbix JIT

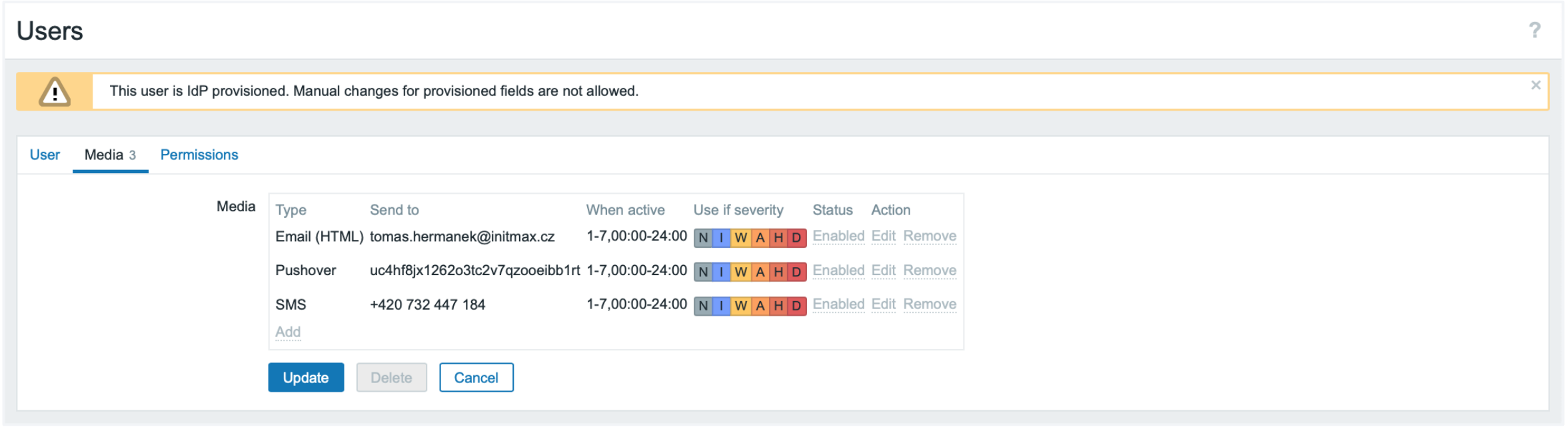
- Zabbix SAML JIT provisioning
  - Check your provisioned user



initMAX

SAML – Zabbix JIT

- Zabbix SAML JIT provisioning
  - Check your provisioned user



initMAX

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];

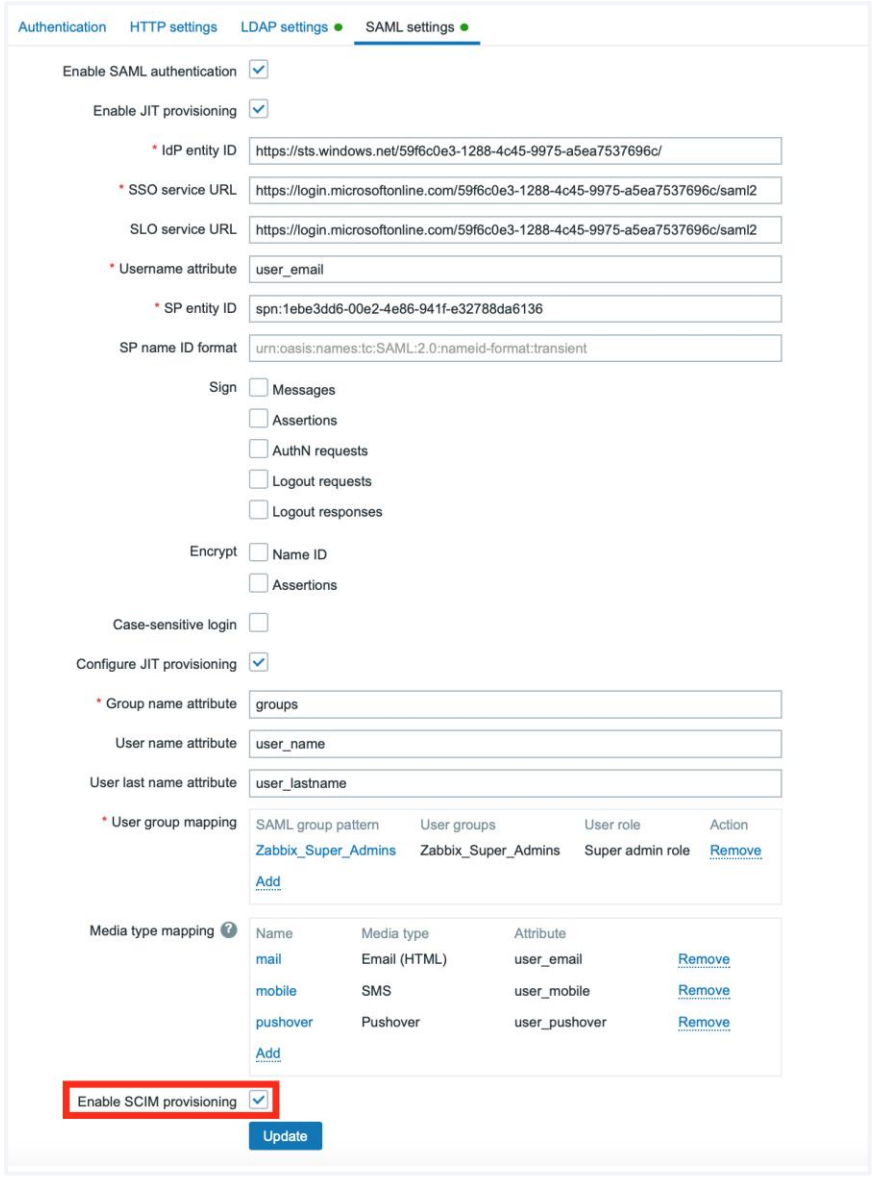
5

SCIM

Zabbix User Provisioning JIT

SCIM – Zabbix

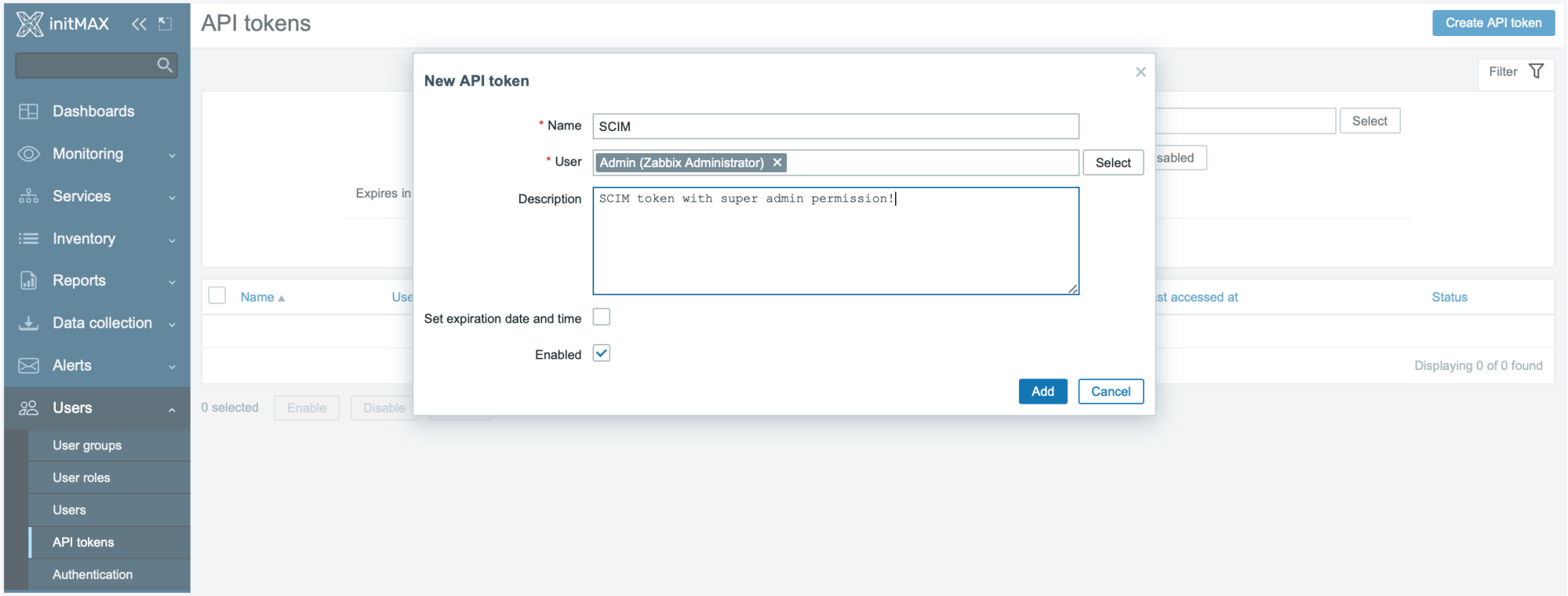
- Zabbix SCIM provisioning
  - Enable SCIM provisioning



Zabbix User Provisioning JIT

SCIM – Zabbix

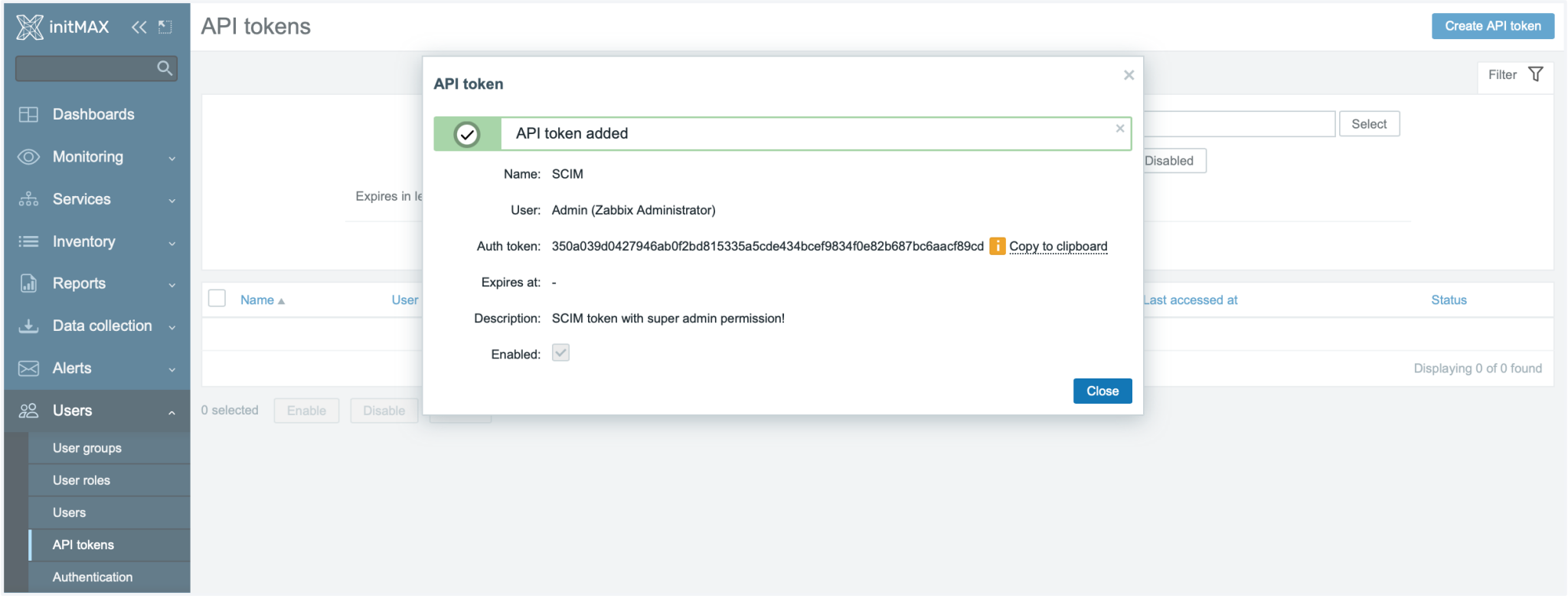
- Zabbix SCIM provisioning
  - Create new API Token with super admin permissions



initMAX

SCIM – Zabbix

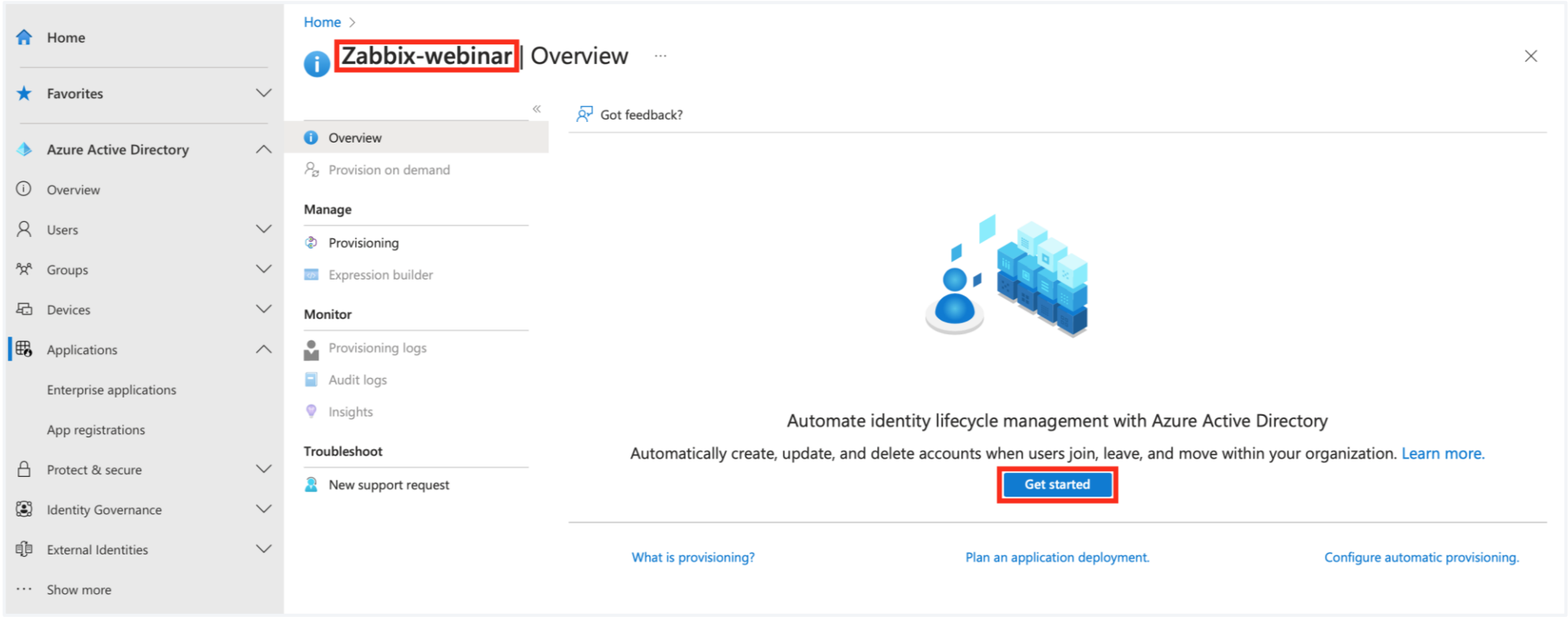
- Zabbix SCIM provisioning
  - Create new API Token with super admin permissions (don’t forget to save this token)



initMAX

SCIM – Azure

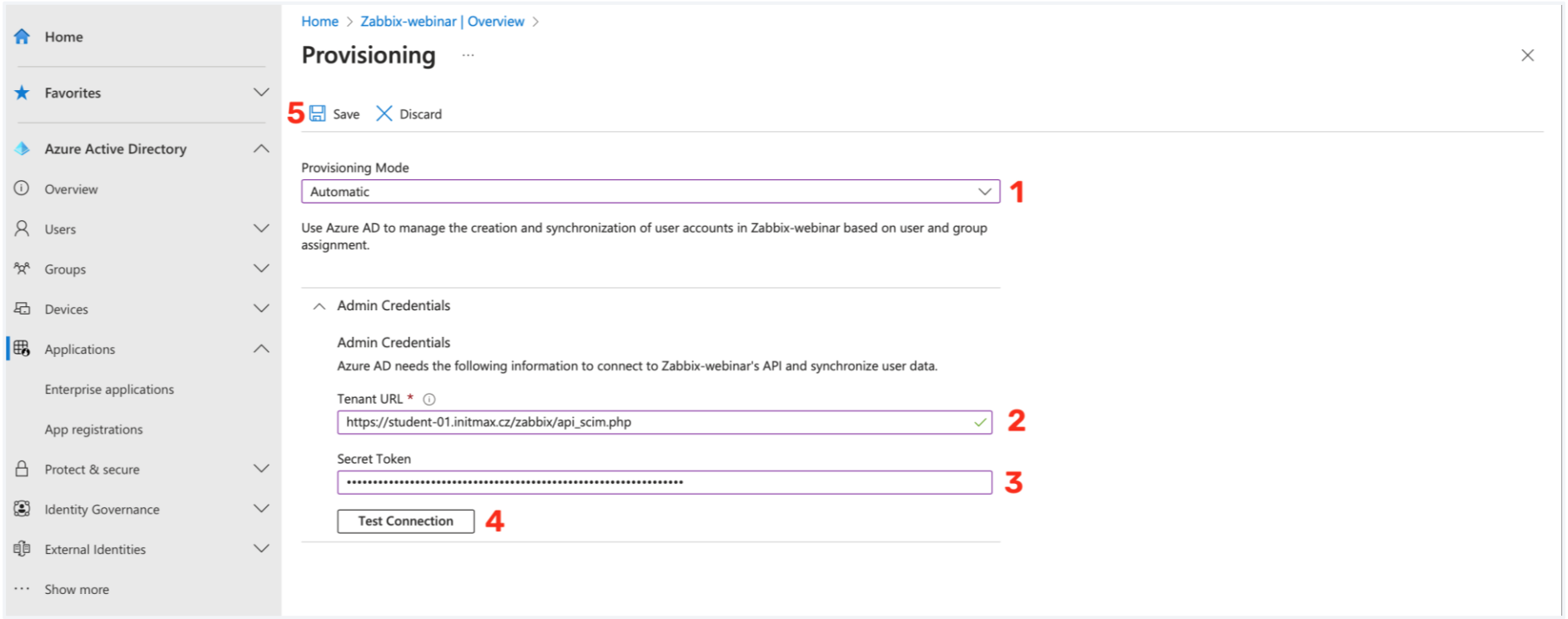
- Zabbix SCIM provisioning
  - In Azure application go to section Provisioning and hit button “Get started”



initMAX

SCIM – Azure

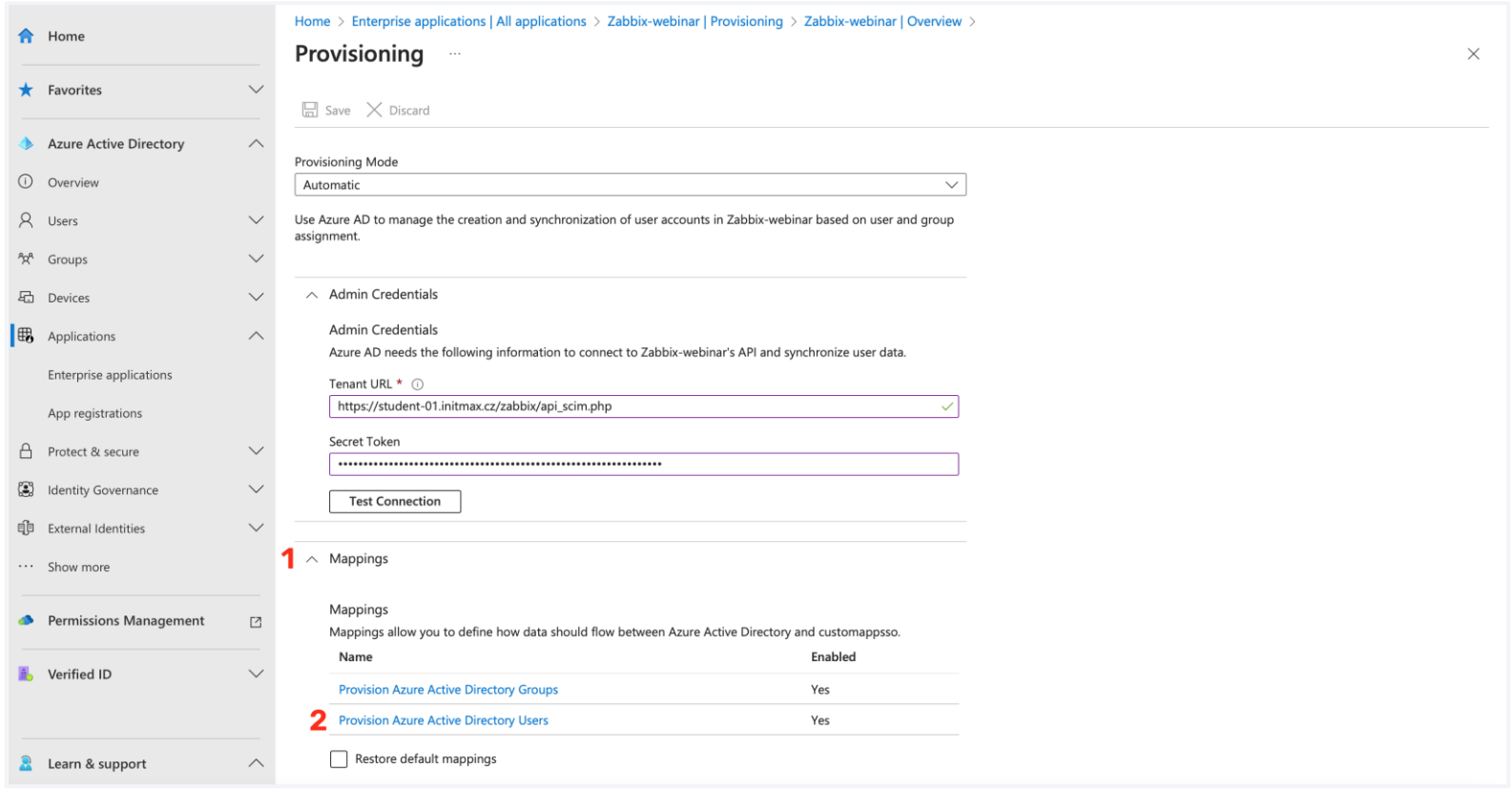
- Zabbix SCIM provisioning
  - Select Automatic Provisioning
  - Tenant URL - https://student-01.initmax.cz/zabbix/api_scim.php
  - Fill Secret Token, test connection and save



Zabbix User Provisioning JIT

SCIM – Azure

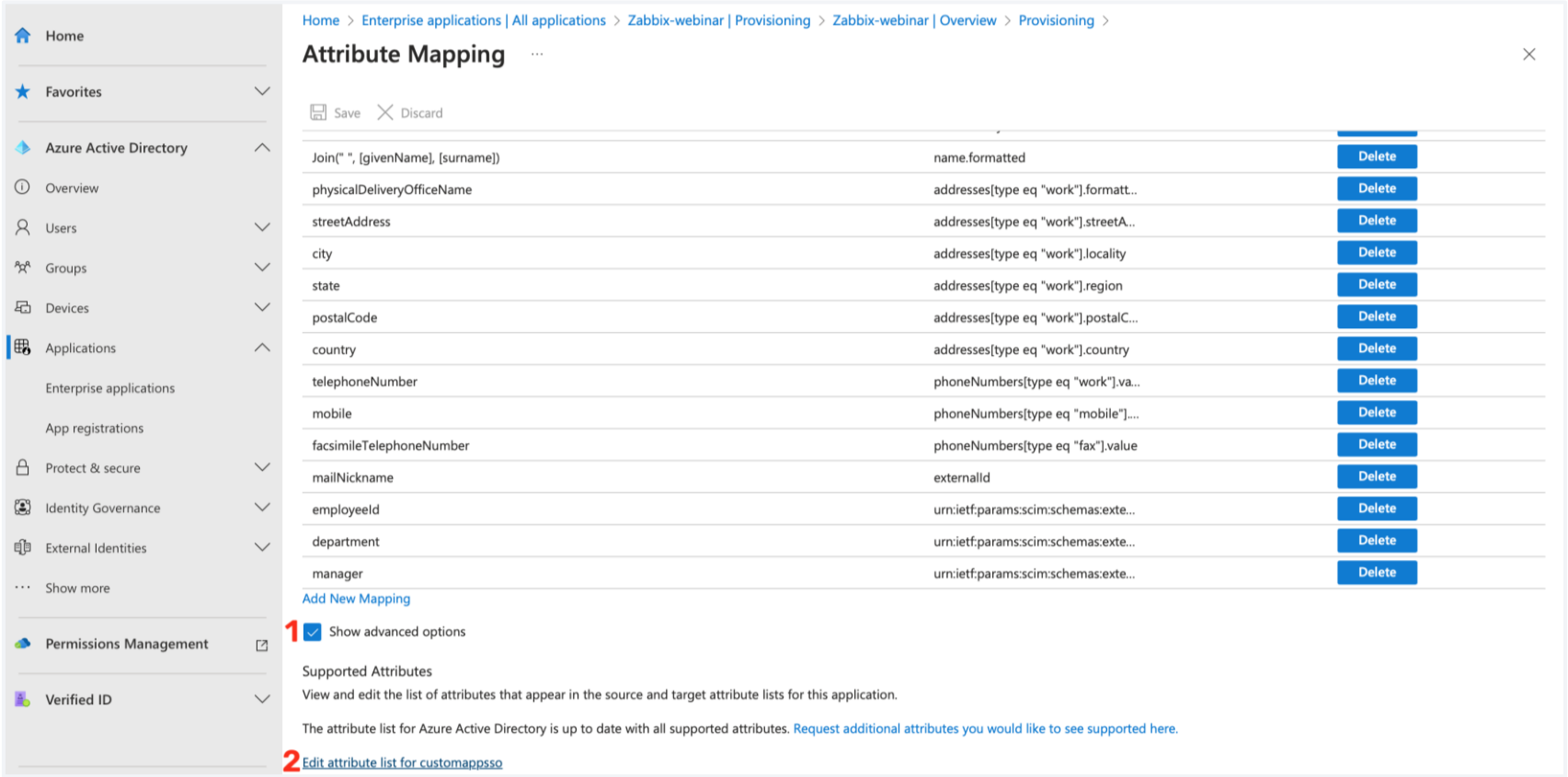
- Zabbix SCIM provisioning
  - We need to update user mapping



Zabbix User Provisioning JIT

SCIM – Azure

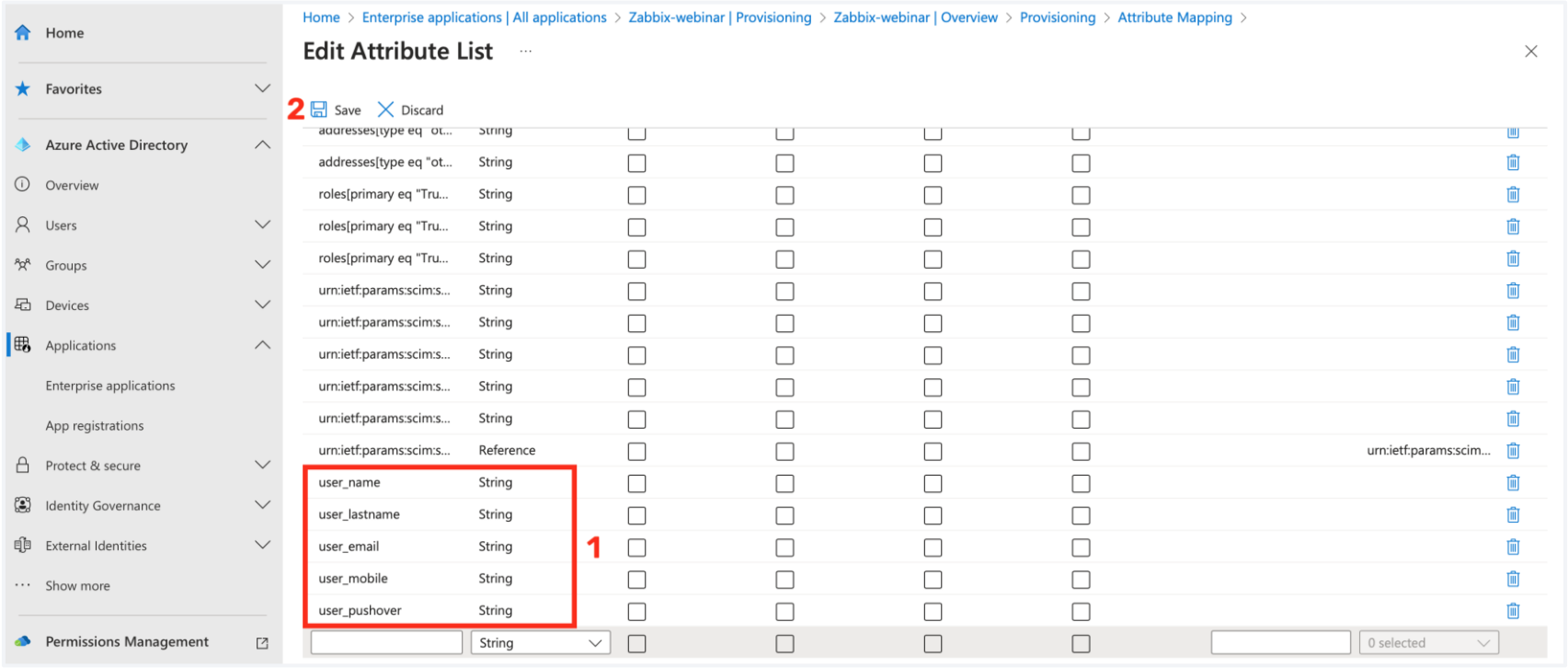
- Zabbix SCIM provisioning
  - We need to expand advanced options and edit attribute list



initMAX

SCIM – Azure

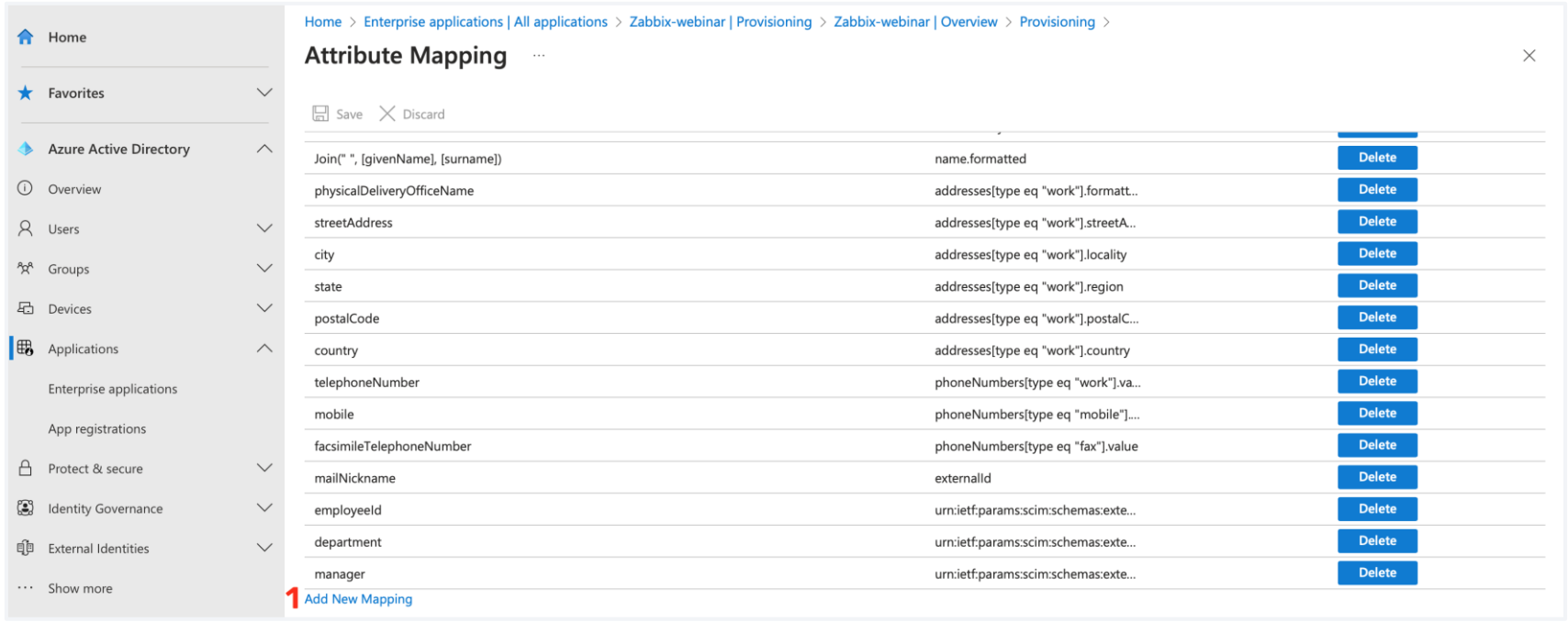
- Zabbix SCIM provisioning
  - Here we need to add our custom attributes



initMAX

SCIM – Azure

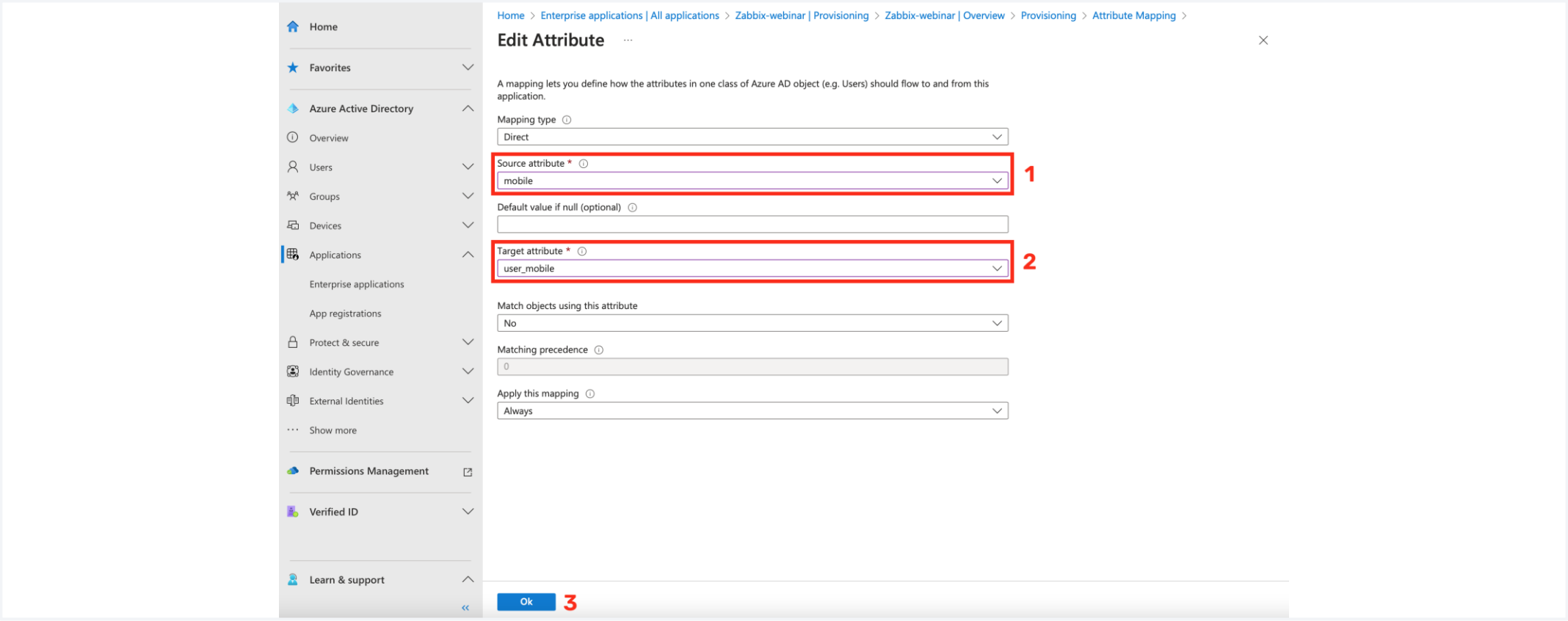
- Zabbix SCIM provisioning
  - Here we need to add our custom attributes



initMAX

SCIM – Azure

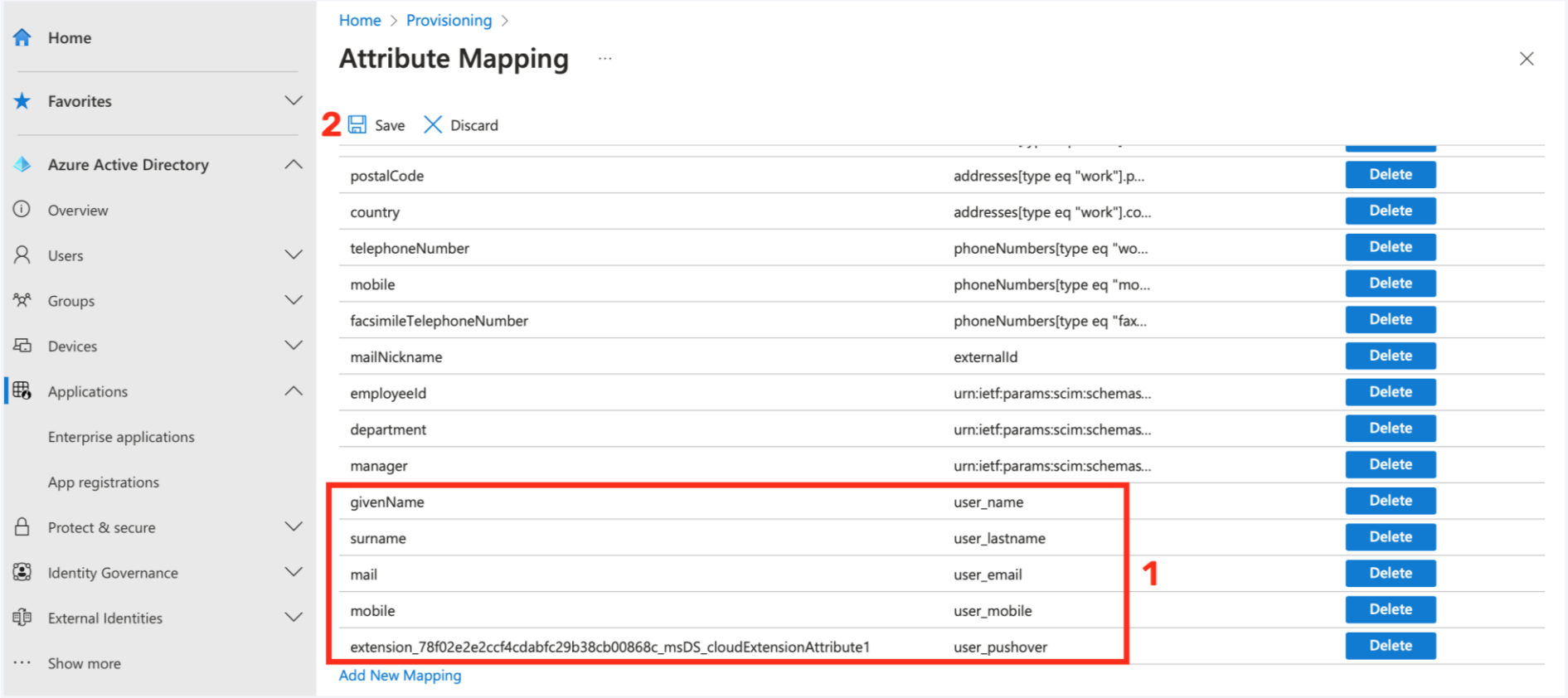
- Zabbix SCIM provisioning
  - Add our custom attributes (user_email, user_mobile, user_name, user_lastname, user_pushover)



initMAX

SCIM – Azure

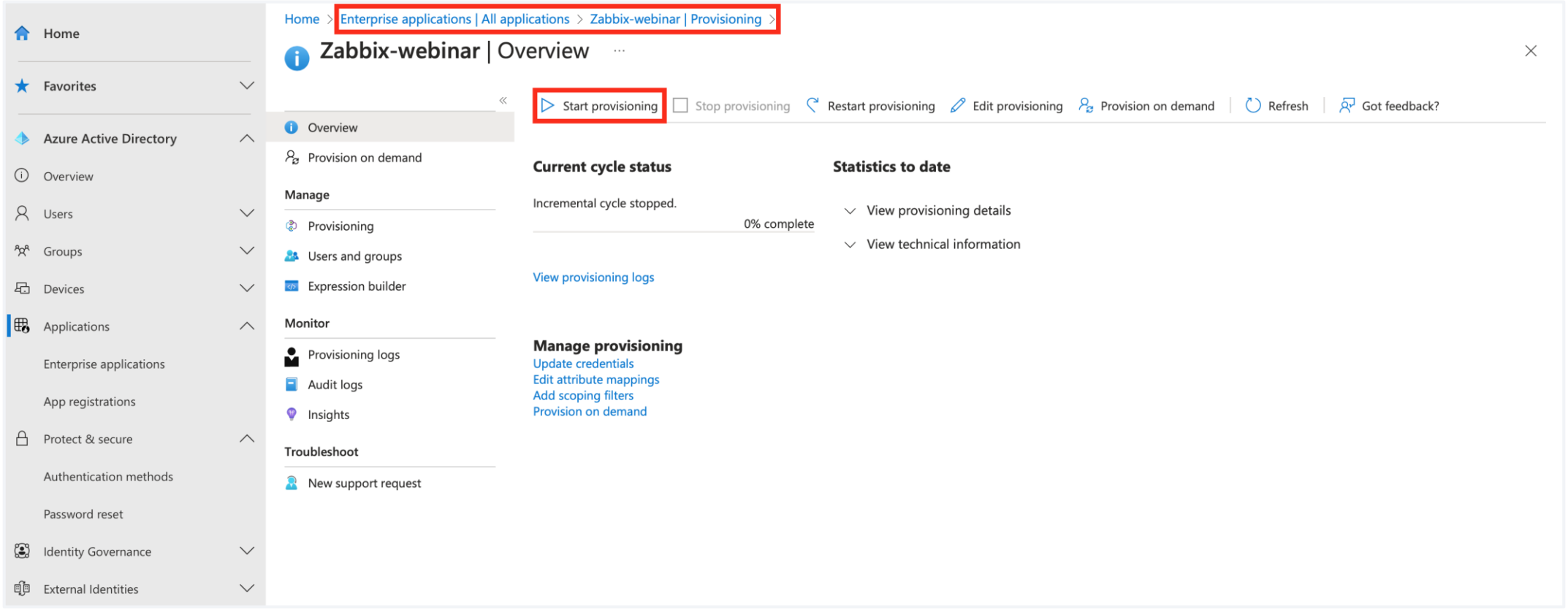
- Zabbix SCIM provisioning
  - Add our custom attributes (user_email, user_mobile, user_name, user_lastname, user_pushover) and save



initMAX

SCIM – Azure

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



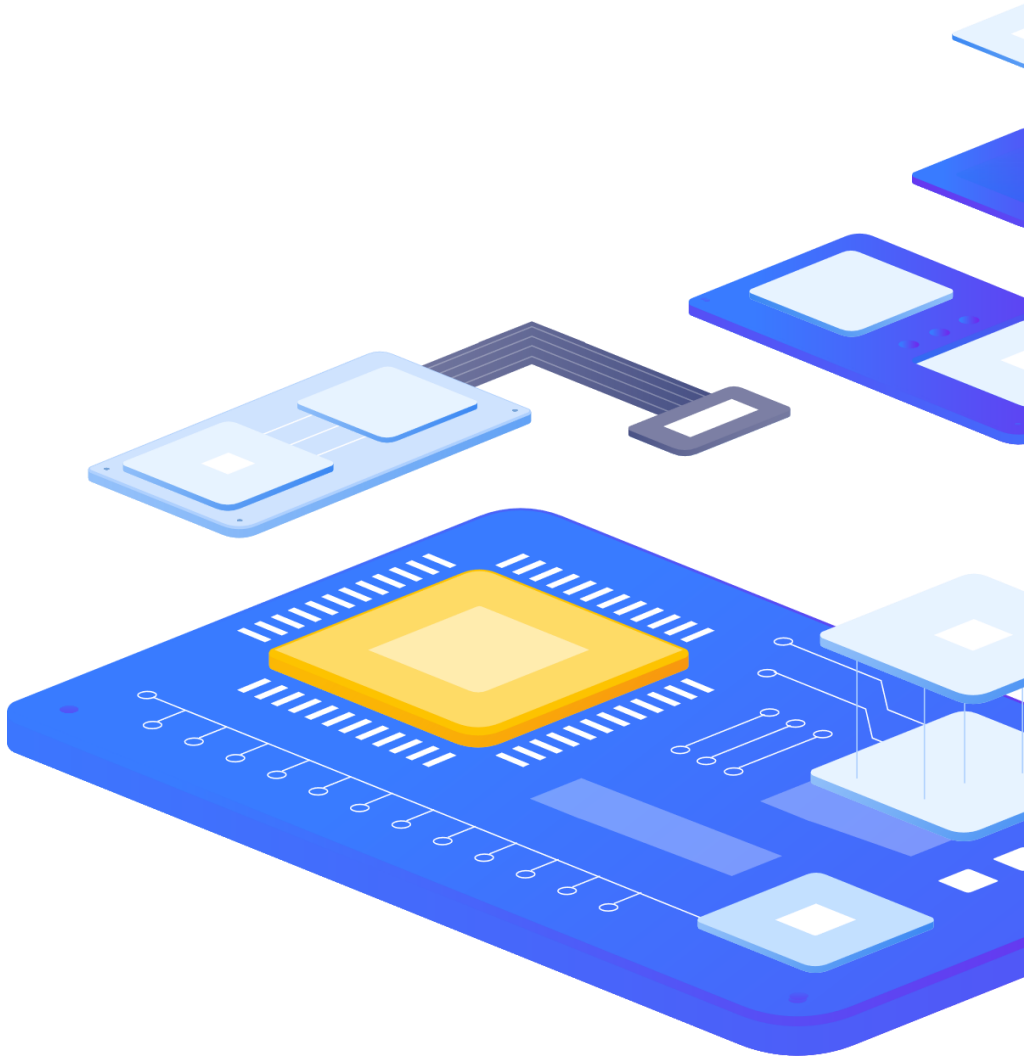
6

Issues and limitations

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)
- Zabbix have bug with user groups – user groups can be assigned via user groups
- SCIM have a lot of issues
- Zabbix have public Security Advisories https://www.zabbix.com/security_advisories



7

DEMO

initMAX

Questions?

Zabbix User Provisioning JIT

initMAX

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