

The ZABBIX logo consists of the word "ZABBIX" in a bold, white, sans-serif font, centered within a solid red rectangular background. The background of the entire slide is a dark blue gradient with a faint, glowing network of white lines and dots, and a subtle world map outline in the background.

**ZABBIX**

# Enterprise User Management and Provisioning in Zabbix

---

**Kaspars Mednis**

Training project manager

# Enterprise requirements



Security - authenticate in a safe way

Granularity - assign different access rights and roles

Automation - use only a single system for authentication



User



User role



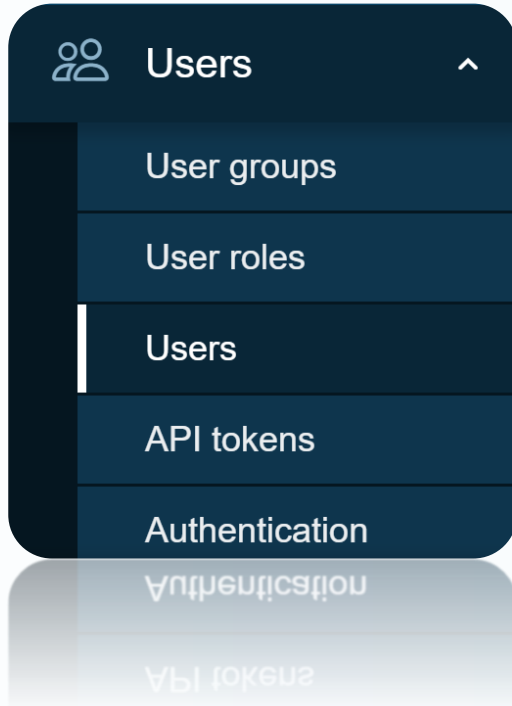
User group



# User permissions



# User management is accessible through the "Users" menu



User groups



User roles



Users






API tokens



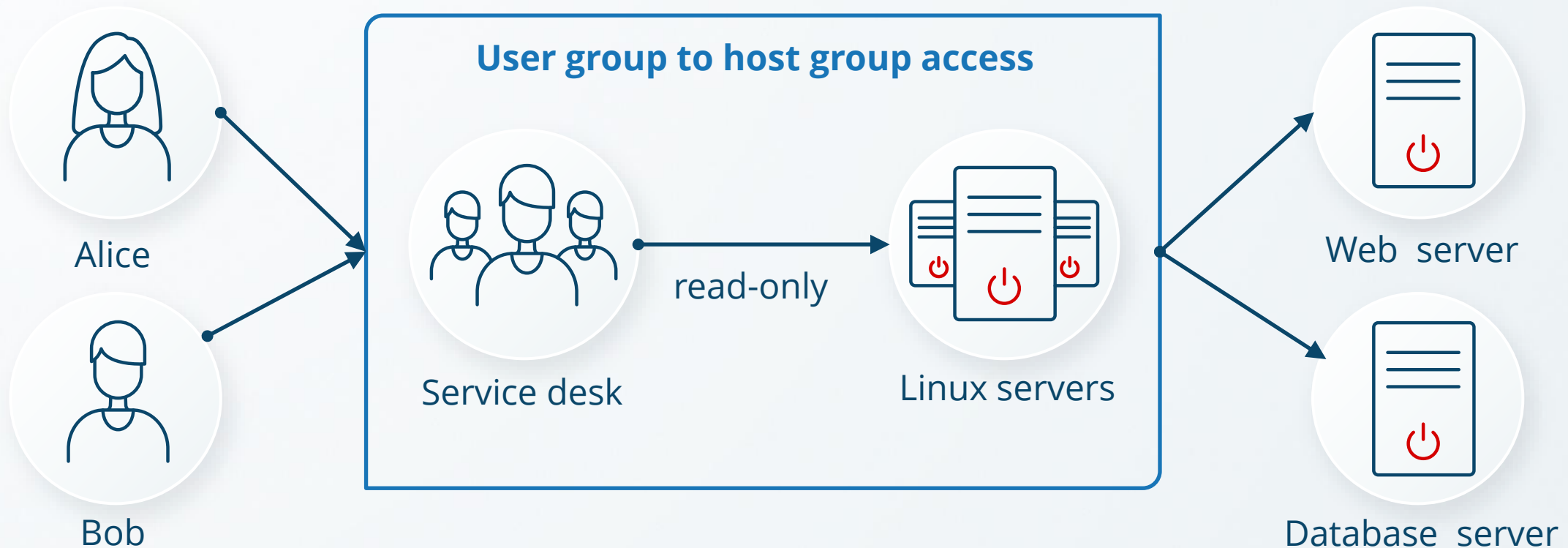
Authentication

Zabbix has three hardcoded types of users:

	 <b>User</b>	 <b>Admin</b>	 <b>Super Admin</b>
Collected data	✓	✓	✓
Monitoring configuration	—	✓	✓
Administrative settings	—	—	✓

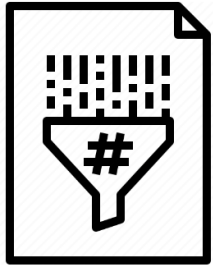
All permissions in Zabbix are based on host and user groups

- ▶ Each host must belong to at least single host group
- ▶ Each user must belong to at least single user group
- ▶ All access permissions can be assigned between host and user groups only





# Permission calculation improvements



Zabbix 7.0 has much faster permission calculation

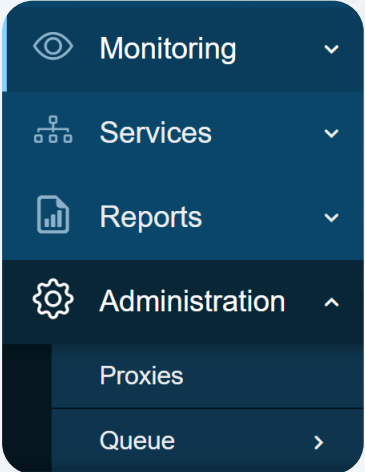
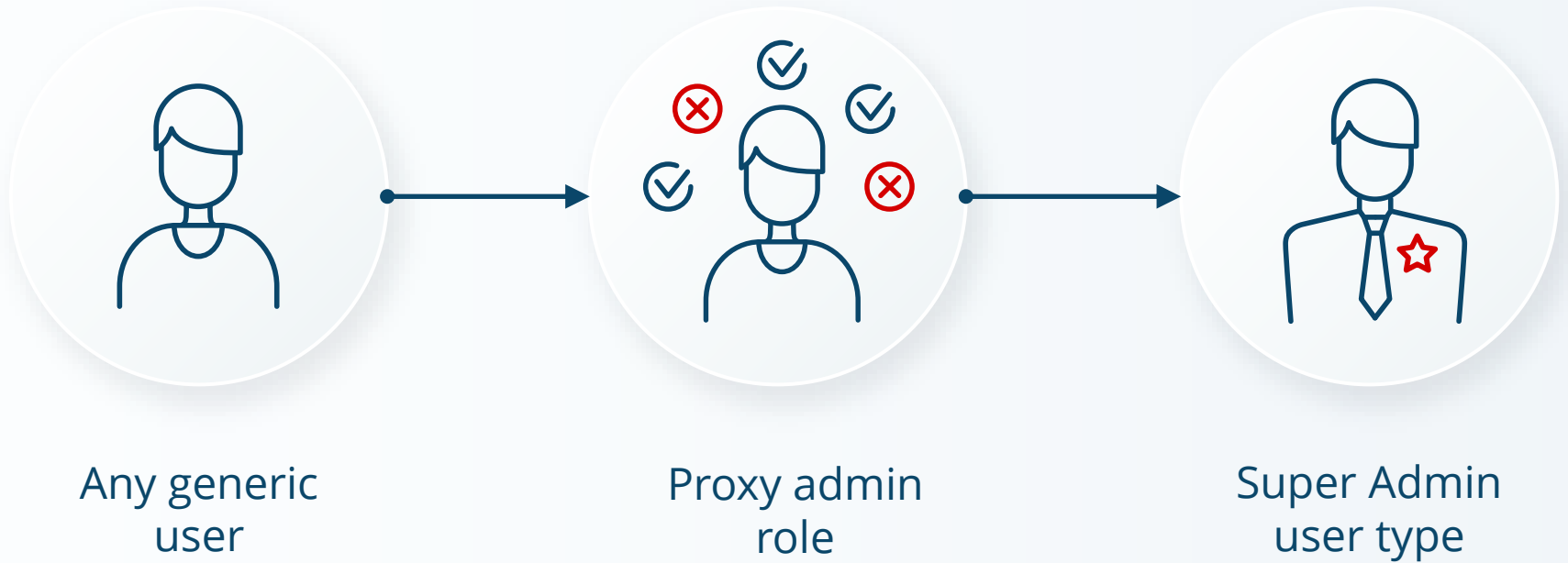
Permissions are pre-hashed

- ▶ Several intermediary tables were introduced for checking non-privileged user permissions.
- ▶ These tables keep hashes (SHA-256) of user group sets and host group sets for each user/host respectively.
- ▶ Additionally, there is a permission table storing only the accessible combinations of users and hosts, specified by the hash IDs.

# User roles

Each Zabbix user must have a user role, which:

- ▶ Assigns user type
- ▶ Limits access to different Zabbix frontend sections



Limited frontend access



## Role management has different Access sections:

- ▶ Zabbix Menu elements
- ▶ IT Services
- ▶ Frontend modules (widgets by example)
- ▶ Zabbix API calls
- ▶ Actions (create map, acknowledge problem, etc.)

### Access to actions

- Create and edit dashboards
- Create and edit maps
- Create and edit maintenance
- Add problem comments
- Change severity
- Acknowledge problems
- Suppress problems
- Close problems

### Access to modules

- Action log
- Clock
- Data overview
- Discovery status
- Favorite graphs
- Favorite maps
- Gauge

### Access to API

Enabled

API methods

Allow list

Deny list

host.delete × item.delete × trigger.delete × graph.delete ×

type here to search

Select

If an element is restricted, users will not be able to access it:

- ▶ Restricted elements are hidden in the frontend
- ▶ Even entering a direct URL to this element into the browser will not work

# User role access cannot exceed user type default rights:

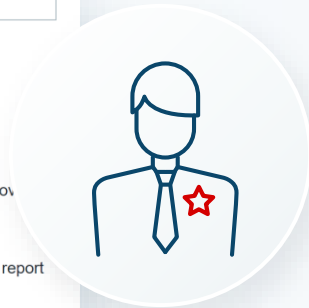
## It is possible to revoke access to any frontend section for Zabbix Super Admin

\* Name

User type

Access to UI elements

Dashboards	<input type="checkbox"/>		
Monitoring	<input type="checkbox"/> Problems	<input type="checkbox"/> Latest data	<input type="checkbox"/> Discov
	<input checked="" type="checkbox"/> Hosts	<input checked="" type="checkbox"/> Maps	
Services	<input type="checkbox"/> Services	<input type="checkbox"/> SLA	<input checked="" type="checkbox"/> SLA report
Inventory	<input type="checkbox"/> Overview	<input type="checkbox"/> Hosts	
Reports	<input checked="" type="checkbox"/> System information	<input type="checkbox"/> Top 100 triggers	<input type="checkbox"/> Notifications
	<input type="checkbox"/> Scheduled reports	<input type="checkbox"/> Audit log	
	<input checked="" type="checkbox"/> Availability report	<input type="checkbox"/> Action log	
Data collection	<input type="checkbox"/> Template groups	<input type="checkbox"/> Hosts	<input type="checkbox"/> Discovery
	<input type="checkbox"/> Host groups	<input type="checkbox"/> Maintenance	
	<input type="checkbox"/> Templates	<input type="checkbox"/> Event correlation	
Alerts	<input type="checkbox"/> Trigger actions	<input type="checkbox"/> Autoregistration actions	<input type="checkbox"/> Scripts
	<input type="checkbox"/> Service actions	<input type="checkbox"/> Internal actions	
	<input type="checkbox"/> Discovery actions	<input type="checkbox"/> Media types	
Users	<input type="checkbox"/> User groups	<input type="checkbox"/> Users	<input type="checkbox"/> Authentication
	<input type="checkbox"/> User roles	<input type="checkbox"/> API tokens	
Administration	<input type="checkbox"/> General	<input type="checkbox"/> Housekeeping	<input type="checkbox"/> Macros
	<input type="checkbox"/> Audit log	<input checked="" type="checkbox"/> Proxies	<input checked="" type="checkbox"/> Queue



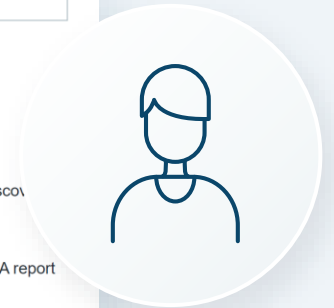
## It is not possible to give some administrative privileges to Zabbix User

\* Name

User type

Access to UI elements

Dashboards	<input checked="" type="checkbox"/>		
Monitoring	<input checked="" type="checkbox"/> Problems	<input checked="" type="checkbox"/> Latest data	<input type="checkbox"/> Discov
	<input type="checkbox"/> Hosts	<input checked="" type="checkbox"/> Maps	
Services	<input type="checkbox"/> Services	<input type="checkbox"/> SLA	<input checked="" type="checkbox"/> SLA report
Inventory	<input type="checkbox"/> Overview	<input checked="" type="checkbox"/> Hosts	
Reports	<input type="checkbox"/> System information	<input type="checkbox"/> Top 100 triggers	<input type="checkbox"/> Notifications
	<input type="checkbox"/> Scheduled reports	<input type="checkbox"/> Audit log	
	<input checked="" type="checkbox"/> Availability report	<input type="checkbox"/> Action log	
Data collection	<input type="checkbox"/> Template groups	<input type="checkbox"/> Hosts	<input type="checkbox"/> Discovery
	<input type="checkbox"/> Host groups	<input type="checkbox"/> Maintenance	
	<input type="checkbox"/> Templates	<input type="checkbox"/> Event correlation	
Alerts	<input type="checkbox"/> Trigger actions	<input type="checkbox"/> Autoregistration actions	<input type="checkbox"/> Scripts
	<input type="checkbox"/> Service actions	<input type="checkbox"/> Internal actions	
	<input type="checkbox"/> Discovery actions	<input type="checkbox"/> Media types	
Users	<input type="checkbox"/> User groups	<input type="checkbox"/> Users	<input type="checkbox"/> Authentication
	<input type="checkbox"/> User roles	<input type="checkbox"/> API tokens	
Administration	<input type="checkbox"/> General	<input type="checkbox"/> Housekeeping	<input type="checkbox"/> Macros
	<input type="checkbox"/> Audit log	<input type="checkbox"/> Proxies	<input type="checkbox"/> Queue



Some parts are greyed out and inaccessible

# Limited Super admin role

Even Zabbix Super Admins can be limited to just some frontend sections:

Access to UI elements

Dashboards	Dashboards
Monitoring	Problems Hosts Latest data Maps Discovery
Services	Services SLA SLA report
Inventory	Overview Hosts
Reports	System information Scheduled reports Availability report Top 100 triggers Audit log Action log Notifications
Data collection	Template groups Host groups Templates Hosts Maintenance Event correlation Discovery
Alerts	Trigger actions Service actions Discovery actions Autoregistration actions Internal actions Media types Scripts
Users	User groups User roles Users API tokens Authentication
Administration	General Audit log Housekeeping Proxy groups Proxies Macros Queue



Proxy admin role

# ServiceDesk role example

\* Name

User type

Access to UI elements

Dashboards <input checked="" type="checkbox"/>			
Monitoring <input checked="" type="checkbox"/> Problems	<input checked="" type="checkbox"/> Latest data	<input type="checkbox"/> Discovery	
<input checked="" type="checkbox"/> Hosts	<input checked="" type="checkbox"/> Maps		
Services <input type="checkbox"/> Services	<input type="checkbox"/> SLA	<input type="checkbox"/> SLA report	
Inventory <input type="checkbox"/> Overview	<input type="checkbox"/> Hosts		
Reports <input type="checkbox"/> System information	<input type="checkbox"/> Top 100 triggers	<input type="checkbox"/> Notifications	
<input type="checkbox"/> Scheduled reports	<input type="checkbox"/> Audit log		
<input checked="" type="checkbox"/> Availability report	<input type="checkbox"/> Action log		
Data collection <input type="checkbox"/> Template groups	<input type="checkbox"/> Hosts	<input type="checkbox"/> Discovery	
<input type="checkbox"/> Host groups	<input type="checkbox"/> Maintenance		
<input type="checkbox"/> Templates	<input type="checkbox"/> Event correlation		

Access to modules

- Action log
- Clock
- Data overview
- Discovery status
- Favorite graphs
- Favorite maps
- Gauge
- Geomap
- Graph
- Graph (classic)
- Graph prototype
- Honeycomb

Access to actions

- Create and edit dashboards
- Create and edit maps
- Create and edit maintenance
- Add problem comments
- Change severity
- Acknowledge problems
- Suppress problems



# API Tokens

API tokens can be created to perform tasks using only Zabbix API

- ▶ It is possible to set the expiration date if required

**New API token** ? X

\* Name

\* User

Description

Set expiration date and time

Enabled

**New API token** ? X

\* Name

\* User

Description

Set expiration date and time

\* Expires at

Enabled

# API Roles

Access to API can be defined by defining using Allow or Deny lists

Access to API

Enabled

API methods **Allow list** Deny list

alert.get × history.get × problem.\* × event.acknowledge × event.get × Select

type here to search

Access to API

Enabled

API methods Allow list **Deny list**

host.delete × item.delete × trigger.delete × host.update × graph.delete ×  
dashboard.delete × sla.\* × service.\* × Select

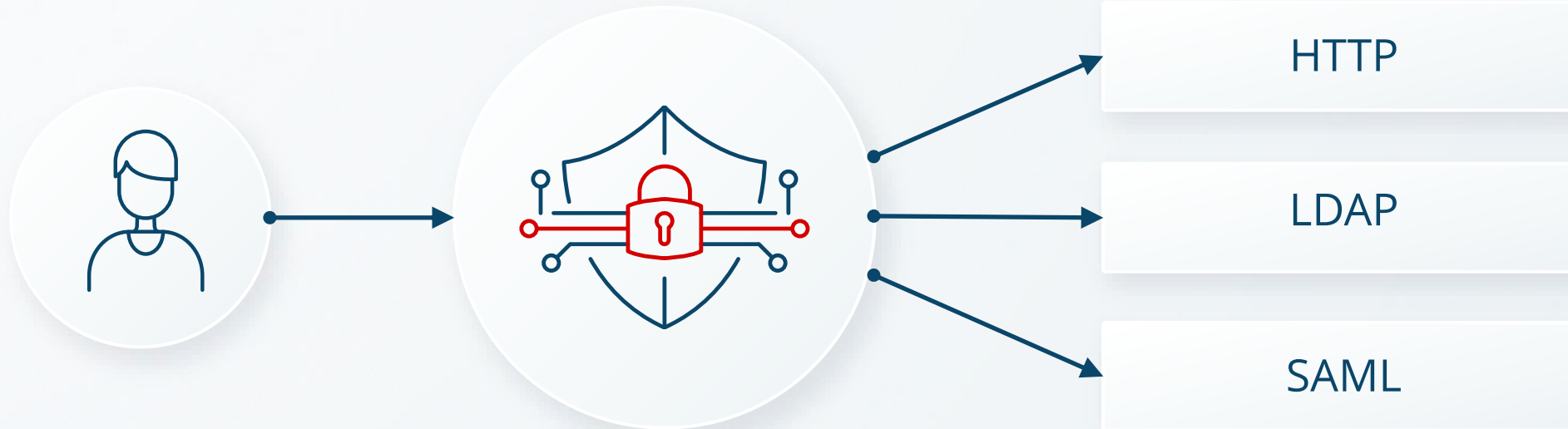
type here to search

# User Provisioning



## External authentication providers are supported:

- ▶ HTTP or web server based (BasicAuthentication, NTLM/Kerberos, etc.)
- ▶ LDAP (OpenLDAP, ActiveDirectory, Apache Directory server, etc.)
- ▶ SAML identity providers (Okta, Microsoft, Google, etc.)



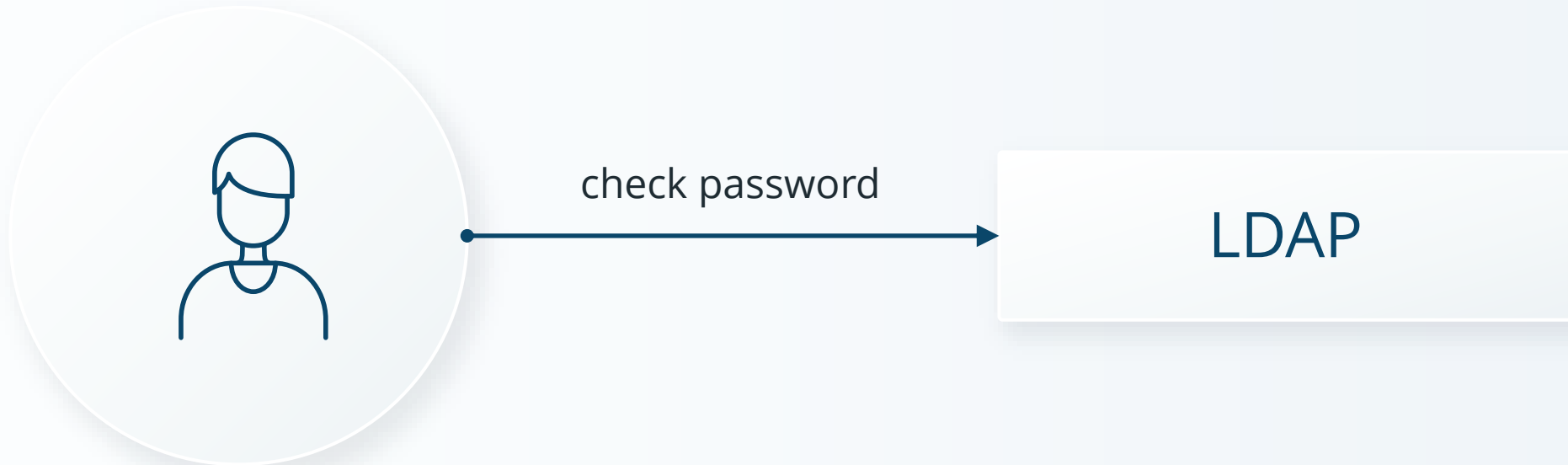


# LDAP

---

LDAP authentication was introduced in Zabbix 1.6

- ▶ It was required to create user manually
- ▶ It was possible to authenticate by using a single LDAP server



# LDAP Configuration

---

Setup LDAP based on your environment (OpenLDAP or MS AD)

## LDAP Server

* Name	<input type="text" value="ldap-netherlands.example.com"/>
* Host	<input type="text" value="ldap.example.com"/>
* Port	<input type="text" value="389"/>
* Base DN	<input type="text" value="ou=training,ou=it,dc=example,dc=com"/>
* Search attribute	<input type="text" value="uid"/>
Bind DN	<input type="text" value="uid=bind_user,dc=example,dc=com"/>
Bind password	<input type="button" value="Change password"/>
Description	<input type="text"/>

# MULTIPLE LDAP SERVERS

Zabbix 6.2 introduced multiple LDAP servers

Authentication HTTP settings **LDAP settings** ● SAML settings MFA settings ●

Enable LDAP authentication

Enable JIT provisioning

\* Servers

Name	Host	User groups	Default	
<a href="#">ldap-belgium.example.com</a>	ldap.example.com	0	<input type="radio"/>	<a href="#">Remove</a>
<a href="#">ldap-luxembourg.example.com</a>	ldap.example.com	0	<input type="radio"/>	<a href="#">Remove</a>
<a href="#">ldap-netherlands.example.com</a>	ldap.example.com	0	<input checked="" type="radio"/>	<a href="#">Remove</a>
<a href="#">Add</a>				

Case-sensitive login

# JIT user provisioning

JIT provisioning is supported for both LDAP and SAML since 6.4

- ▶ User accounts are created on demand on the first login
- ▶ Deprovisioned users are automatically disabled

Authentication HTTP settings **LDAP settings** SAML settings MFA settings

Enable LDAP authentication

Enable JIT provisioning

\* Servers

Name	Host	User groups	Default	
ldap-belgium.example.com	ldap.example.com	0	<input type="radio"/>	<a href="#">Remove</a>
ldap-luxembourg.example.com	ldap.example.com	0	<input type="radio"/>	<a href="#">Remove</a>
ldap-netherlands.example.com	ldap.example.com	0	<input checked="" type="radio"/>	<a href="#">Remove</a>

[Add](#)

Case-sensitive login

Provisioning period

[Update](#)

Default authentication

Deprovisioned users group



# User group mapping

- ▶ User groups in Zabbix are assigned automatically based on the LDAP groups

Configure JIT provisioning

Group configuration ? memberOf groupOfNames

Group name attribute

User group membership attribute

User name attribute

User last name attribute

\* User group mapping

LDAP group pattern	User groups
<a href="#">zabbix_super_admins</a>	Zabbix administrat
<a href="#">Add</a>	

**User group mapping** ✕

\* LDAP group pattern ?

\* User groups  Select

\* User role  Select

Update Cancel

# User media provisioning

Media type mapping ?

Name	Media type	Attribute	Action
<a href="#">Email</a>	Email (corporate)	mail	<a href="#">Remove</a>
<a href="#">Add</a>			

**LDAP field name for email**

Media type mapping

\* Name

\* Media type

\* Attribute

User media

\* When active

Use if severity

- Not classified
- Information
- Warning
- Average
- High
- Disaster

Create enabled

# Add media for provisioned users



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

User Media 2 Permissions

**Additional  
email address**

Media

Type	Send to	When active	Use if severity	Status	Action
Email (private)	john.doe@home.org	6-7,00:00-24:00	<input type="checkbox"/> N <input type="checkbox"/> I <input type="checkbox"/> W <input type="checkbox"/> A <input checked="" type="checkbox"/> H <input checked="" type="checkbox"/> D	<a href="#">Enabled</a>	<a href="#">Edit</a> <a href="#">Remove</a>
Email (corporate)	john.doe@example.com	1-7,00:00-24:00	<input type="checkbox"/> N <input checked="" type="checkbox"/> I <input checked="" type="checkbox"/> W <input type="checkbox"/> A <input type="checkbox"/> H <input type="checkbox"/> D	<a href="#">Enabled</a>	<a href="#">Edit</a> <a href="#">Remove</a>
<a href="#">Add</a>					



# Multi factor authentication



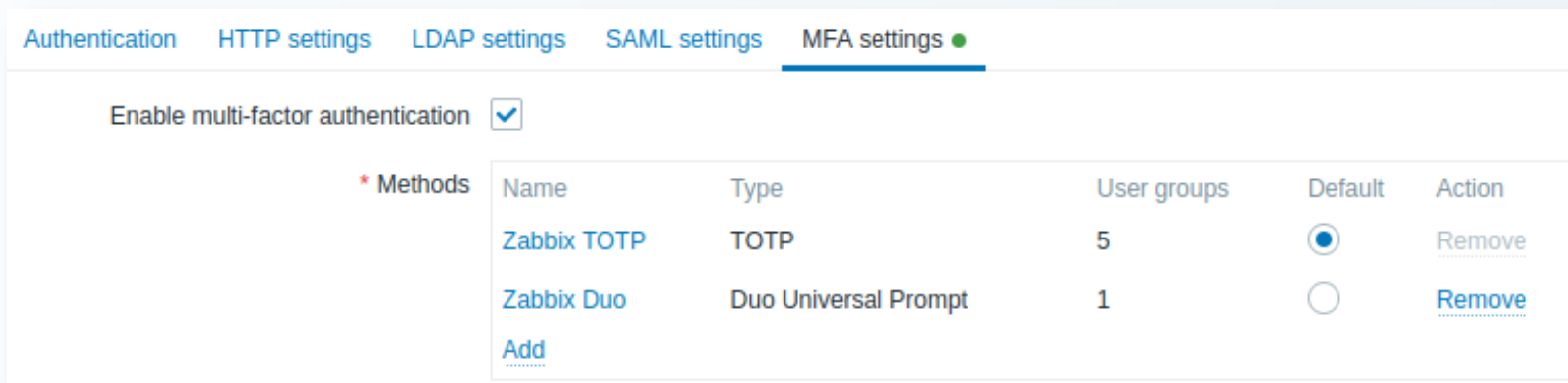
# MFA in Zabbix

---

MFA Provides an additional layer of security beyond just a username and password

Multiple MFA methods are available:

- ▶ Time-Based One-Time Password (TOTP)
- ▶ Duo Universal Prompt



The screenshot shows the Zabbix MFA settings page. At the top, there are navigation tabs: Authentication, HTTP settings, LDAP settings, SAML settings, and MFA settings (which is selected and highlighted with a green dot). Below the tabs, there is a checkbox labeled "Enable multi-factor authentication" which is checked. Underneath, there is a section titled "\* Methods" containing a table with columns: Name, Type, User groups, Default, and Action.

Name	Type	User groups	Default	Action
Zabbix TOTP	TOTP	5	<input checked="" type="radio"/>	<a href="#">Remove</a>
Zabbix Duo	Duo Universal Prompt	1	<input type="radio"/>	<a href="#">Remove</a>
<a href="#">Add</a>				

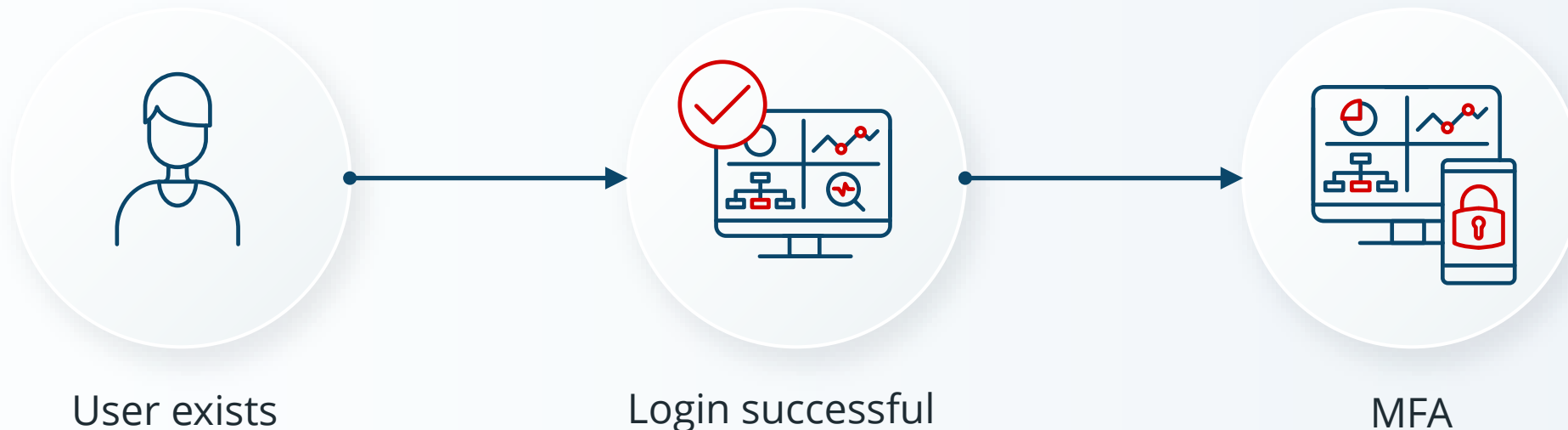


# MFA Authentication

---

If MFA authentication is enabled, the user:

- ▶ Must exist in Zabbix
- ▶ Must provide Zabbix credentials when logging in
- ▶ Must prove their identity by other means, usually, a code generated by an authenticator app on the user's phone

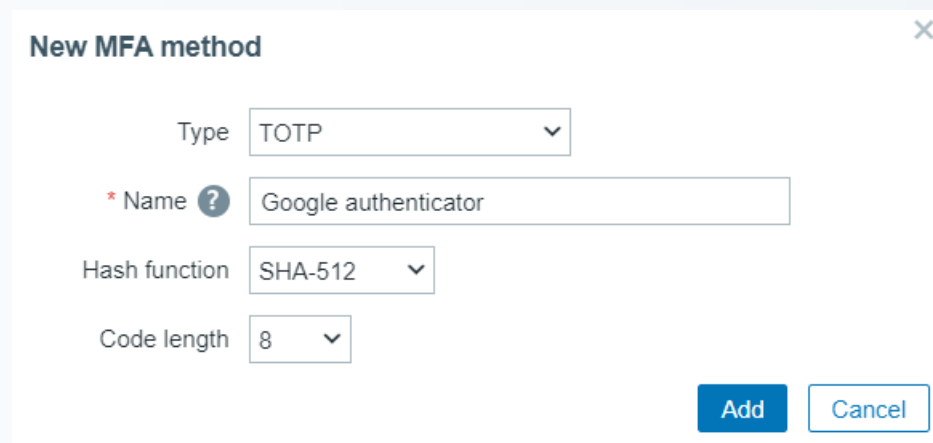


# Time based one - time password

---

Users must verify their identity using an authenticator app

- ▶ Enable multi-factor authentication in Users -> Authentication
- ▶ Add a new TOTP MFA method
- ▶ Assign TOTP authentication to a user group
- ▶ Log out of Zabbix and log back in using your credentials.



**New MFA method** ✕

Type

\* Name ?

Hash function

Code length

# Enroll authentication application

---


Upon successful login, you will be prompted to enroll:

- ▶ Open the authentication app on the phone
- ▶ Scan the QR code
- ▶ Your application generates a new code
- ▶ Enter the code in the Zabbix login form
- ▶ You have enrolled your authentication device

**ZABBIX**

Scan this QR code

Please scan and get your verification code displayed in your authenticator app.



Unable to scan? You can use SHA1 secret key to manually configure your authenticator app:  
NVC4MMZGQHPQMQTDOYBA7BO4B2OXHRUY

Verification code

**Sign in**

# Duo Universal prompt

User management is performed at the DUO web site

- ▶ Create a web SDK application at the Duo web site
- ▶ Copy all attributes to the Zabbix MFA form

The image shows a screenshot of the Duo Web SDK application details page and a 'New MFA method' dialog box. The top bar of the Duo page includes a lock icon, 'Web SDK', '2FA', 'Documentation' with an external link icon, and a 'Protect' button. The 'Details' section on the left lists three attributes: 'Client ID' (redacted), 'Client secret' (SOVU), and 'API hostname' (api-5964fbe1.duosecurity.com), each with a 'Copy' button. A note below the secret field reads: 'Don't write down your client secret or share it with anyone.' The 'New MFA method' dialog box on the right has a close button (X) and contains the following fields: 'Type' (Duo Universal Prompt), '\* Name' (Duo Prompt), '\* API hostname' (api-5964fbe1.duosecurity.com), '\* Client ID' (redacted), and '\* Client secret' (redacted). At the bottom of the dialog are 'Add' and 'Cancel' buttons.

# Create a user group

User group must have either TOTP or Duo authentication specified

User group    Template permissions    Host permissions    Problem tag filter

\* Group name

Users    
type here to search


Frontend access  ▼

LDAP Server  ▼

Multi-factor authentication  ▼

Enabled

Debug mode





# User group membership

---

Users which are created manually are assigned to the MFA group

User Media 4 Permissions

\* Username

Name

Last name

Groups    
type here to search

Password

# MFA and provisioned users

For provisioned users the MFA group is added to the JIT settings:

### User group mapping ×

\* LDAP group pattern ?

\* User groups   
  
type here to search Select

\* User role  Select

Update Cancel

The ZABBIX logo consists of the word "ZABBIX" in a bold, white, sans-serif font, centered within a solid red rectangular background. The background of the entire slide is a dark blue gradient with a faint, glowing network of white lines and dots overlaid on a silhouette of a world map.

**ZABBIX**

Thank you

---

**Kaspars Mednis**

Training Project Manager