TOOLS4EVER

HelloID Training

Access Management

Agenda

Day 1 (fundamentals)

- Introduction
- HelloID products & Modules
- Required resources
- Access Management Basics
- The HelloID interface
- Additional configuration options
- Applications
- Security
- Audit logging

Day 2 (implementer)

- Implementation questions
- AD IDP
- Mapping sets
- Identity providers
- Single Sign-on Types
- IDP filtering and settings
- Sign-on policies
- Appearance and CSS
- Custom reports
- Troubleshooting
- HelloID API

Introduction

TOOLS4EVER

Tools4ever

- Dutch origin
- Identity Management
- 7 sites worldwide
- 600 customers in NL
- 5000 customers worldwide
- 140 employees

HelloID Trainers

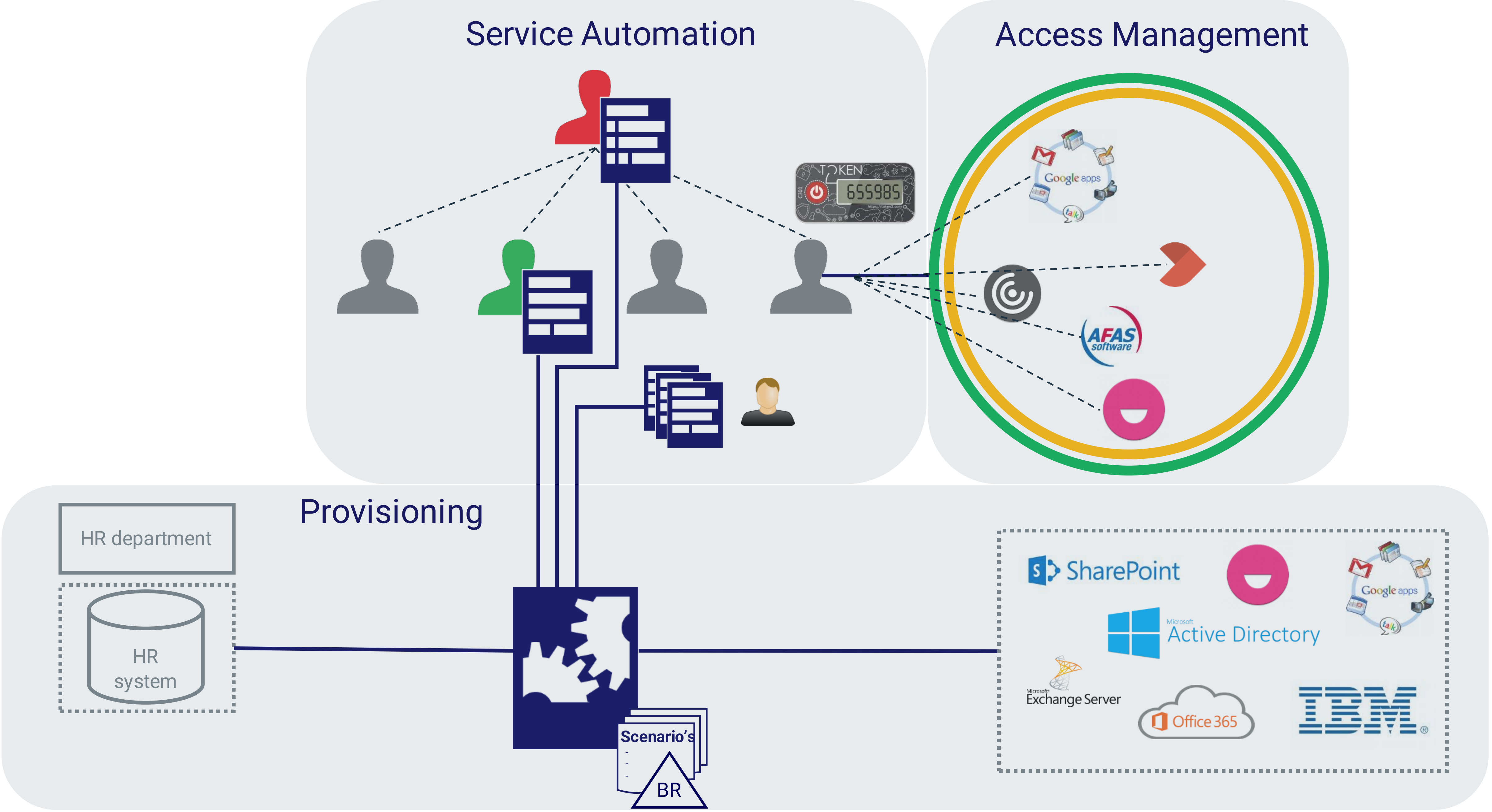
TOOLS4EVER

Audience

- Tools4ever partners
- Tools4ever customers

HelloID Products and Modules

- HelloID Access Management
- HelloID Service Automation
- HelloID Provisioning

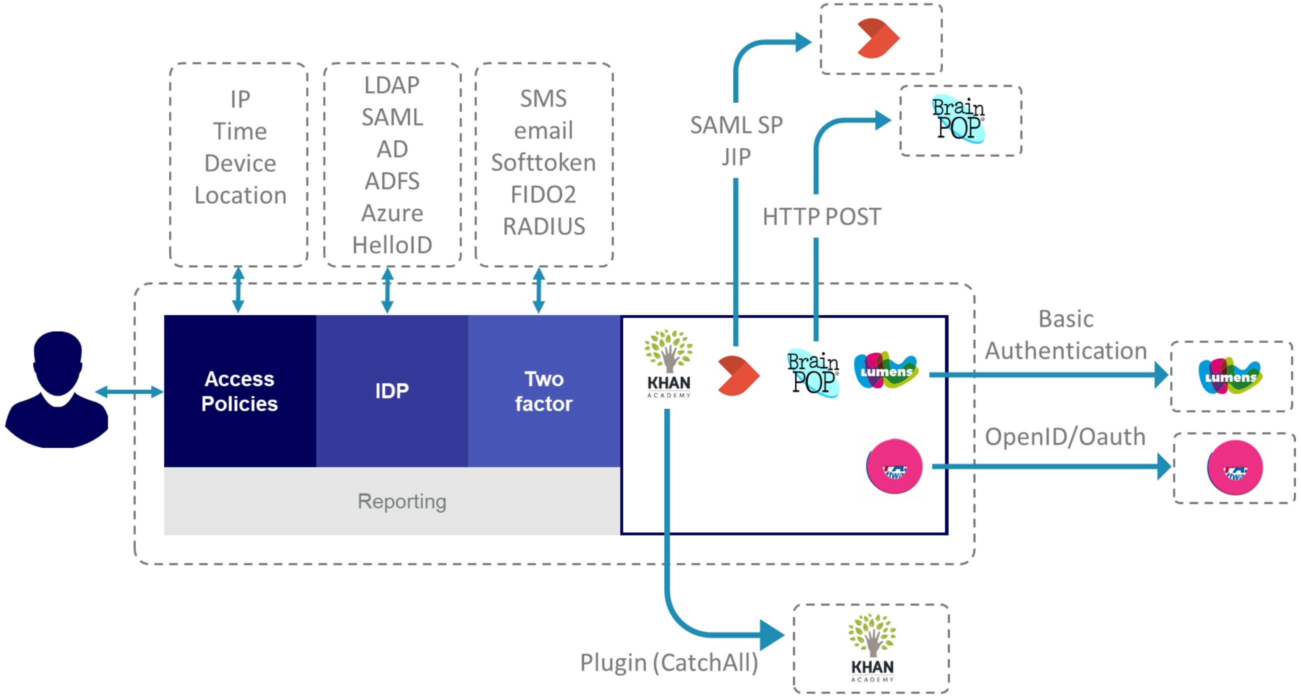

Service Automation
Access Management
TOKEN
655985
Google apps
AFAS software
Provisioning
HR department
HR system
Scenario's
BR
SharePoint
Google apps
Microsoft Active Directory
Microsoft Exchange Server
Office 365
IBM

TOOLS4EVER

HelloID Access Management

HelloID Access Management

- Centralized access management solution
- One, complete, integrated service for every type of user
- 100% single sign-on to connected applications
- Various integrations possible with intranet providers
- Multi-tenant



TOOLS4EVER

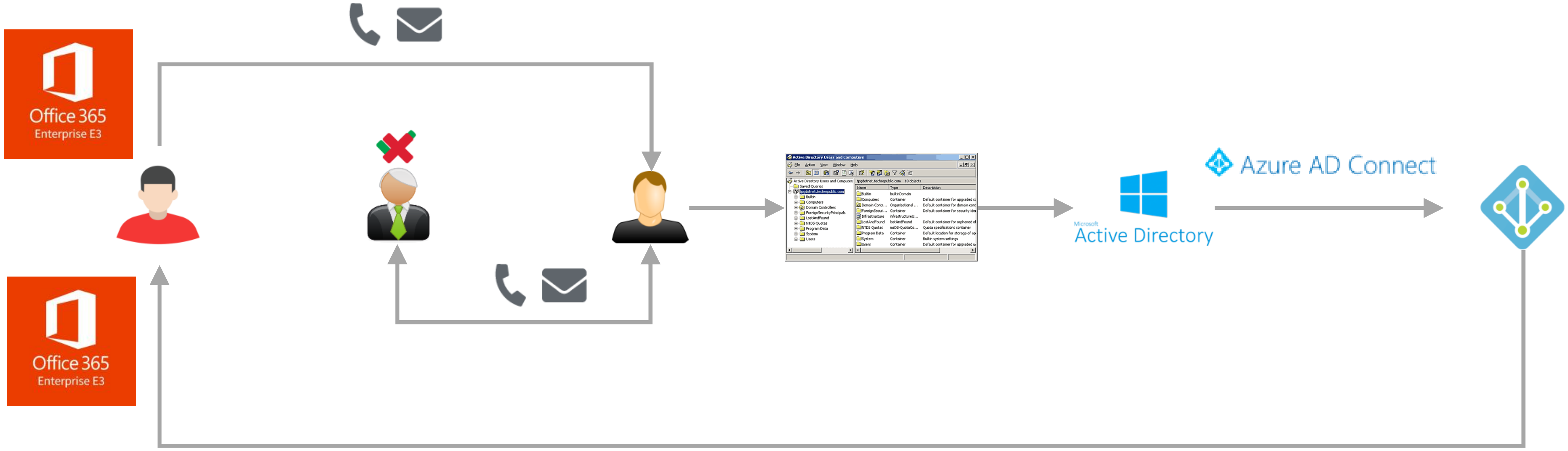
HelloID Service Automation

TOOLS4EVER

HelloID Service Automation

- Less effort from IT department
- Advanced approval workflows available
- Easy to use
- Managers can manage their own users and view reports

Without Service Automation



Active Directory Users and Computers

File Action View Window Help

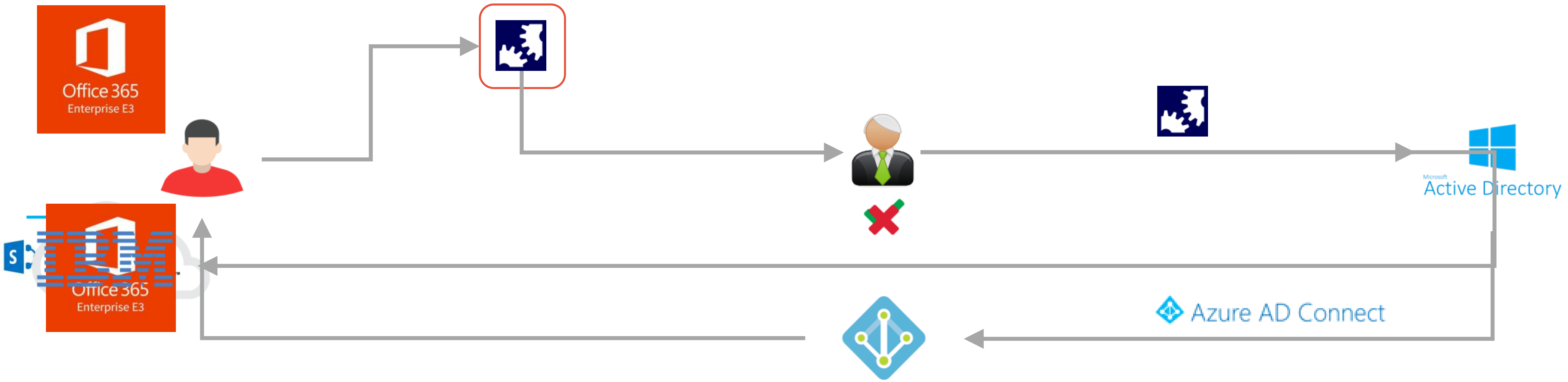
Active Directory Users and Computers
- Saved Queries
- tpgdotnet.techrepublic.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - LostAndFound
  - NTDS Quotas
  - Program Data
  - System
  - Users

tpgdotnet.techrepublic.com 10 objects

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgraded co
Domain Contr...	Organizational ...	Default container for domain cont
ForeignSecuri...	Container	Default container for security ide
Infrastructure	infrastructureU...	
LostAndFound	lostAndFound	Default container for orphaned ol
NTDS Quotas	msDS-QuotaCo...	Quota specifications container
Program Data	Container	Default location for storage of ap
System	Container	Builtin system settings
Users	Container	Default container for upgraded u

TOOLS4EVER

With Service Automation



TOOLS4EVER

Service Automation “modules”

- Self Service requests
- Helpdesk delegation
- Scheduled automation tasks
- Scheduled reports

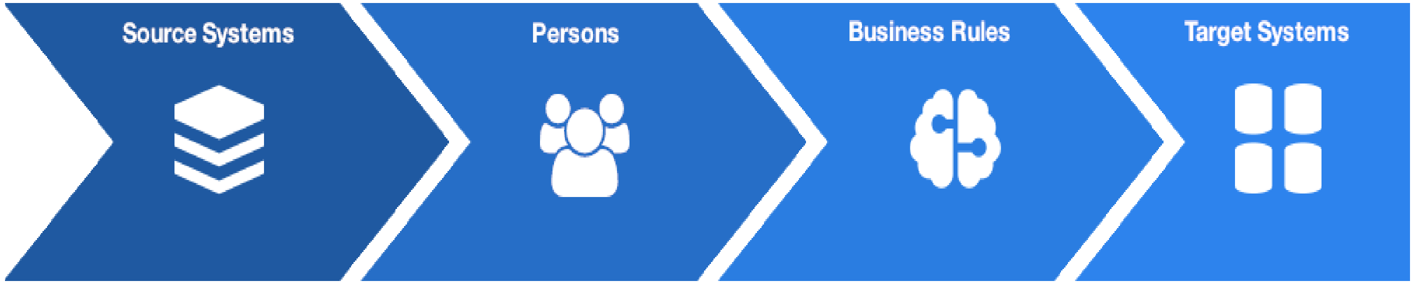
HelloID Provisioning

TOOLS4EVER

HelloID Provisioning

- HelloID provisioning provides a standardized user account management and provisioning system that handles:
  - Automated Account Onboarding
  - Offboarding
  - Re-boarding
  - Rights management
  - & more…

- This solution is fully cloud based, but also interacts with a lot of on-premise applications.



HelloID Provisioning

- HelloID Provisioning can:
  - synchronize user information automatically between the authoritative source system and the target network (cloud/local).
  - use the company HR data to specify a number of roles or function profiles.
  - use this information to manage the assignment of rights, or to withdraw old unnecessary rights when the HR information changes.

Required Resources

TOOLS4EVER

Required Resources

- Documentation: https://docs.helloid.com
- Support: https://servicedesk.tools4ever.com
- Feature requests: https://roadmap.helloid.com
- Forum: https://forum.helloid.com
- Statuspage: https://helloid.statuspage.io

Support account

- When support from Tools4ever is required the technician can request a support account
- The approval of the account will be sent to the administrator emailaddress
- After approval the administrator will receive a email with the option to revoke the account.

HelloID Acces Management

Training day 1

TOOLS4EVER

Training content day 1

- Access Management Basics
- The HelloID interface
- Additional configuration options
- Applications
- Security
- Notifications
- Audit logging

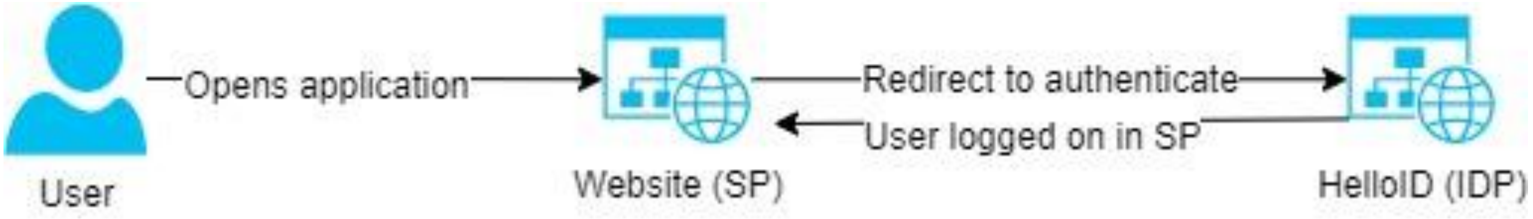
Basic Concepts of HelloID Access Management

- What is an Identity Provider (IDP)?
- What is a Service Provider (SP)?
- Single Sign-on Types
  - SAML
  - OpenID
  - Post
  - Plugin
  - WS-Federation
- HelloID Directory agent

What is an Identity Provider (IDP)

- Within HelloID Access Management an Identity Provider (IdP) can be used to logon to HelloID.

- HelloID can also be configured as an IdP for other applications.
    - An IdP is a federation partner that is configured to authenticate a user. After a successful authentication, it passes the required attributes to the Service Provider (SP).



What is a Service Provider (SP)

- Within HelloID Access Management a Service Provider (SP) can be configured so users authenticated by HelloID (IdP) can access the service provider.

- The authentication for the SP is handled on the IDP.

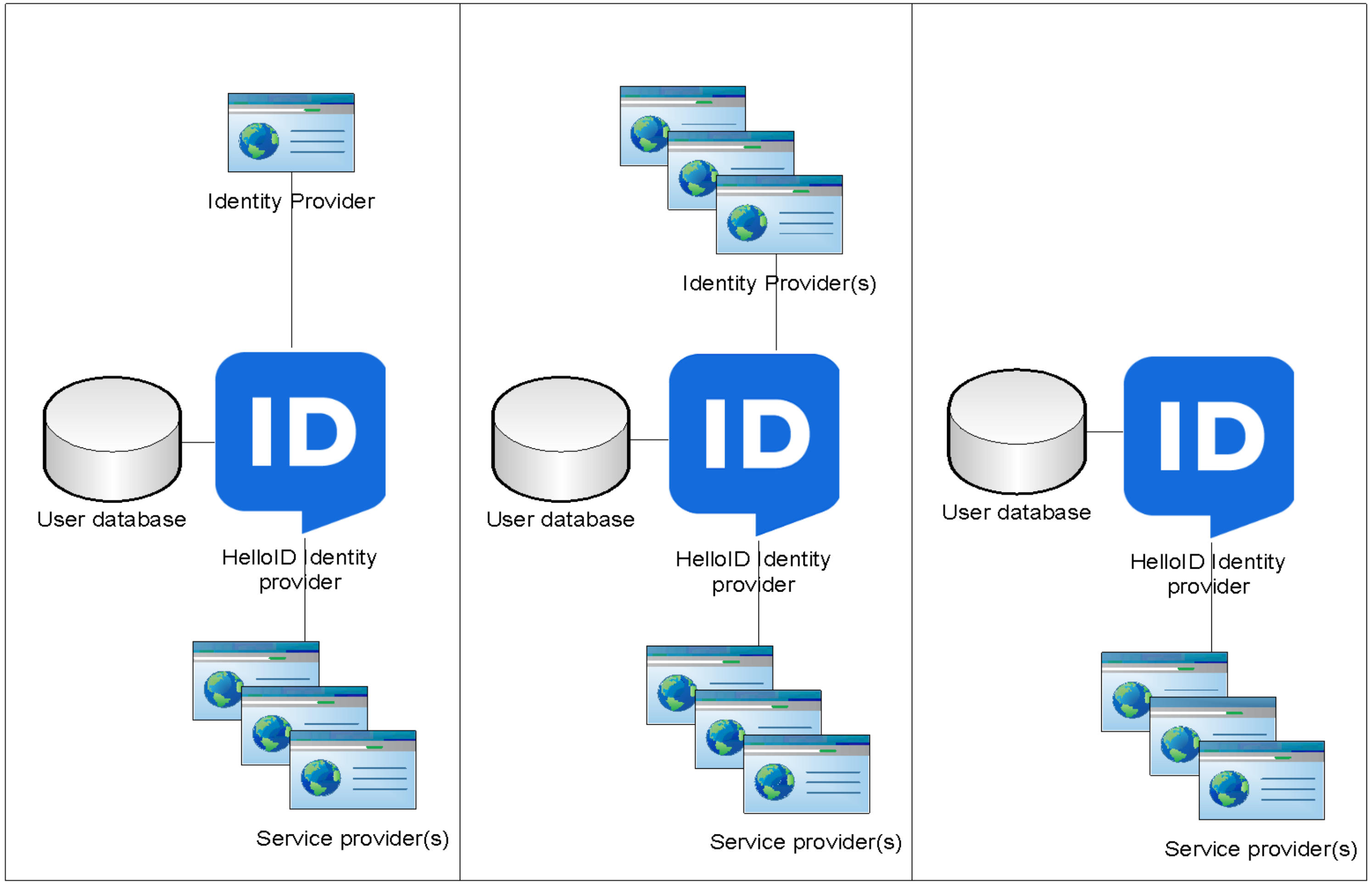
- When the SP supports Just-in-Time provisioning it is possible to create user accounts at the first logon to the SP.

Access Management Basics

- Within HelloID - Identity Providers & Service Providers are supported.
- HelloID supports multiple Identity Providers to support mixed environments.
- In most implementations HelloID serves as Identity provider for the configured service providers while an external identity provider is used to login to HelloID.

- The user is always synced or created by just-in-time provisioning into the local HelloID user database.
- The service provider(s) are authenticating to the local user database.
- This makes it also possible to use accounts without an external source in HelloID which can be cost efficient.

Multiple access scenario’s



Single Sign-on Types

- SAML = **S**ecurity **A**ssertion **M**arkup **L**anguage
  - an open standard which defines the rules and definitions for exchanging authorization and authentication data between identity and service providers.
  - SAML is a web based single sign-on standard.
  - More info: https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

Single Sign-on Types

- OPENID Connect
  - an authentication standard which is controlled by the OpenID Foundation.
  - Based on the OAUTH 2.0. protocol by OpenID
  - Less room for custom implementations like the SAML standard
  - Easier to configure than SAML
  - More info: https://openid.net/

Single Sign-on Types

HelloID Plugin/Post

- Last ditch effort to provide SSO to end-users.
- Possibility for applications that can't be connected with a standard SSO method like SAML or OpenID.
- Using password vault principle.
- Available for:
  - Internet Explorer
  - Google Chrome
  - Firefox (desktop and mobile)
  - Edge (Chromium)

Single Sign-on Types

- Besides SAML, OpenID Connect and HelloID Plugin, HelloID supports the following single sign on methods:
    - FORM Post
    - Basic authentication
    - WS-Federation

- All methods above do not require the HelloID plugin to be installed.

HelloID Plugin Pro’s & Con’s

PROS:

- The end-user can be provided with single sign-on to most of their web applications.
- As an administrator it is possible to pre-define credentials so multiple users can have access to a single account without knowing the password of the account.
- In most cases plugin applications are easy to setup.
- The plugin is client side, so the connected applications do not need to be connected to the internet directly.

CONS:

- The plugin or the mobile application has to be installed on all user devices that are using HelloID. This includes personal devices of the user.
- Group policy management is needed to mass deploy the plugin and enable usage.
- To be able to use the plugin the user always has to visit the HelloID portal first, so the plugin has an active session with the portal.

HelloID Directory Agent

TOOLS4EVER

What is the HelloID Agent

- The HelloID agent is used for synchronizing and authenticating users from the on-premise Active Directory domain.

- This small application service can be installed on any domain joined machine and can be configured in a pool to provide high-availability.

- The HelloID agent is used for the following tasks:
  - Active Directory Authentication
  - Synchronizing from Active Directory
  - Service automation tasks from HelloID
  - Provisioning tasks from HelloID

What is the HelloID Agent

- Please make sure that the machine(s) the agent is installed on meets the requirements as stated on docs.helloid.com

- The HelloID agent only needs a working internet connection. All traffic is Agent initiated and therefore no inbound access rules are needed in the firewall.

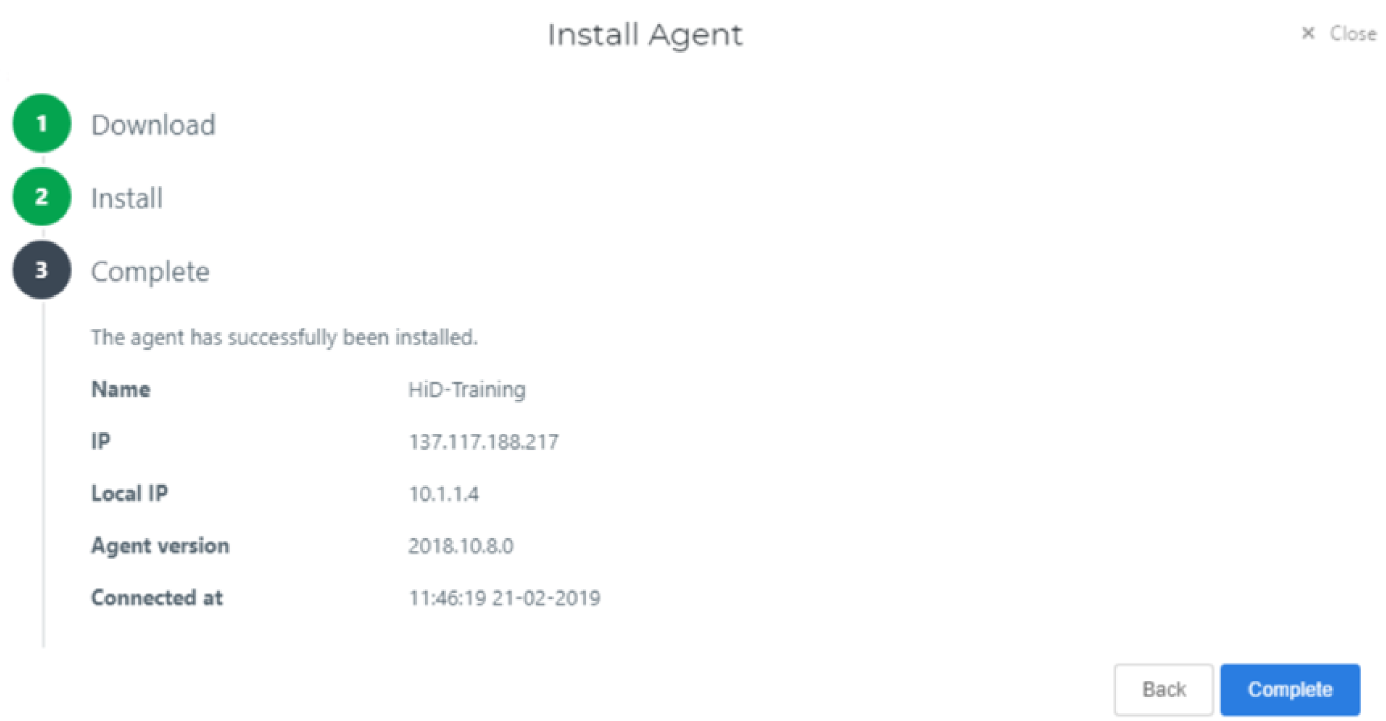
- Running the agent with a service account is required in production environments.

  - Reference: https://docs.helloid.com/hc/en-us/articles/360019130974-HelloID-Requirements

Agent Installation

- Add a new agent pool.

- Install the agent in the created pool by following the installation wizard.



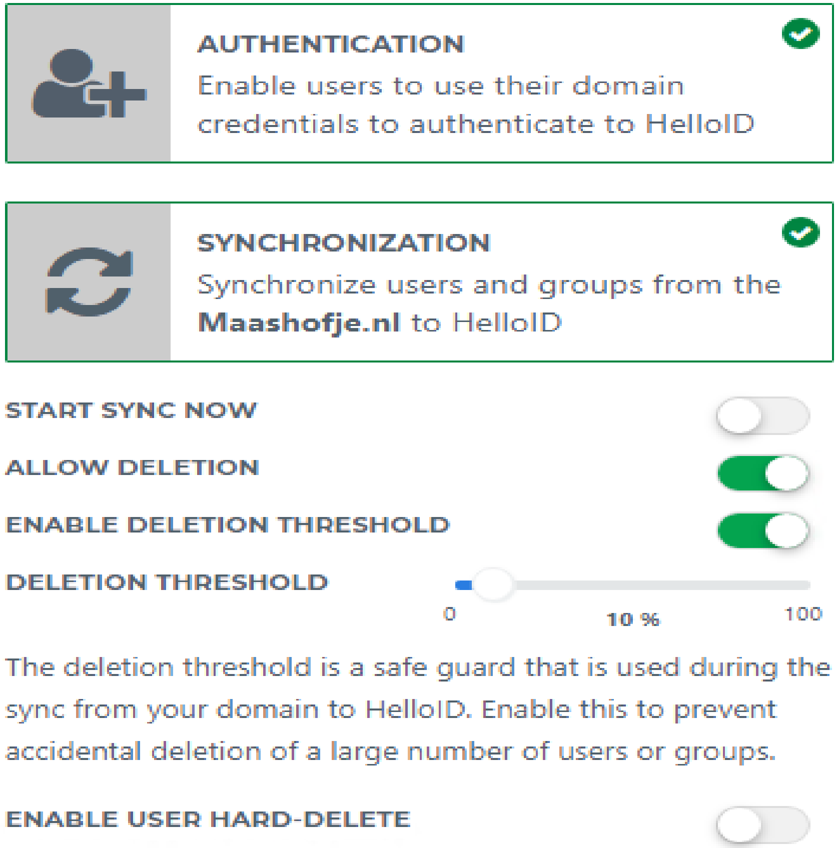
The agent has successfully been installed.

Name	HiD-Training
IP	137.117.188.217
Local IP	10.1.1.4
Agent version	2018.10.8.0
Connected at	11:46:19 21-02-2019

Agent Configuration

- If you do not select authorization since an external IDP like ADFS is used. It is always possible to add this later.

- Sample setup:



AUTHENTICATION ✓
Enable users to use their domain credentials to authenticate to HelloID

SYNCHRONIZATION ✓
Synchronize users and groups from the **Maashofje.nl** to HelloID

START SYNC NOW

ALLOW DELETION

ENABLE DELETION THRESHOLD

DELETION THRESHOLD 0 10 % 100

The deletion threshold is a safe guard that is used during the sync from your domain to HelloID. Enable this to prevent accidental deletion of a large number of users or groups.

ENABLE USER HARD-DELETE

Agent Configuration

- It is recommended to leave the user Hard-Delete option disabled.
  - With this setting disabled, users will be marked as deleted instead of deleting them entirely.
  - When a user is soft-deleted because the account was placed out of scope of the sync he will not lose all his credential sets and history when placed back into sync.

Agent Configuration

- Select the OU which needs to be synced to HelloID.
- Please be aware that it is not possible to exclude one sub OU when the OU in a higher level is selected.
- Select the scope for groups which need to be synced to HelloID.
- Best practice is to sync all groups from the entire domain.
  - This is done to prevent nesting issues that can occur when only specific OU’s are selected.

Lab 1

Installing and configuring the HelloID Agent

TOOLS4EVER

Before we start… make sure your Active Directory contains the following

OU structure

- HelloID Training
  - Users
  - Disabled users
  - Groups

AD user accounts

- 4 employee accounts
  - Configure department and title attributes
- 2 managers accounts
  - Configure department and title attributes
  - Configure manager attribute for user

AD Groups

- 4 AD groups for demo purpose
- Add groups to AD users (random)

Lab 1

30 minutes

Installing and configuring the HelloID Agent

Installing and configuring Active Directory Agent including sync of users and groups.

- Install the Active Directory Agent
- Create Active Directory configuration
  - Synchronize all user accounts from the OU “HelloID Training”
  - Synchronize all groups (because of group nesting)
  - Activate and test Authentication

Please check out the references on https://docs.helloid.com
Manuals for Administrators → Agents

HelloID Interface

HelloID Interface

- User and group management
- License information
- Incidents
- Automation tasks

User and group management

- External source(s)
  - Active Directory
  - Azure Active Directory
  - Google Gsuite
- Editable attributes
- Default group(s)

License information

- License counts are showed on the dashboard
- In case of exceeding subscription you pay the pay as you go rate for the exceeding users.
- Access management: all enabled users that have at least one application assigned.
- NOTE: When adding a new application by default it will be assigned to the default group(s).
- Incidents will be logged when a license is exceeded or license count suddenly rises with more then 10%
- License counts are logged daily to the reporting system

Incidents

- Several incident types available
- New types will be added on a regular base (roadmap.helloid.com)
- Possible to recieve incidents by e-mail or webhook
- Possible to subscribe to specific tags
- If no tags are selected all incidents are sent
- Reminders will be sent if incidents are open for longer time(s)
- Incidents can be manually resolved
- Incidents and incident updates are logged to the reporting system

Automation Tasks

- Option to create, edit and delete automation tasks
- Adjust schedule to fit your needs
- Possible to add your own powershell scripts (Service automation)
- Logging available in the GUI

Lab 2

Setup Incidents

15 minutes

Description

- Add a e-mail address to receive incidents
- Subscribe the added e-mailaddress to the Domain: AM tag

Testing

- Test if the incident is working by stopping the Agent Service on your virtual machine
- If a e-mail is received you can start the service again

Please check out the references on https://docs.helloid.com
Manuals for Administrators → General →Incidents

Additional configuration

Additional configuration

- Custom domain
- Custom e-mail domain
- Certificates
- Application management

Custom domain

- Best practice to add a custom domain before implementation
- Verify ownership by receiving a e-mail with a code
- Add a CNAME DNS record
- Upload SSL Certificate
- Create a ticket at Tools4ever support
- Domain name will be applied within two weeks
- Renewing SSL certificate can be done by uploading the new certificate and creating a support ticket.

Custom e-mail domain

- Mainly used in the Service Automation and Provisioning module
- Verify ownership of the domain by entering the recieved code
- Add the provided DNS records to your domain DNS system
- Verify the DNS Records
- After verification you are able to e-mail from HelloID with your own domain

Certificates

- Within HelloID certificates are used within IDP, SP and custom domain configurations.
- Mostly used for the signing of a SAML message.
- You can create self-signed certificates and import an existing certificate
- When creating self-signed certificates please make sure the common name always contains the HelloID portal domain name. e.g. customer.helloid.com.
- HelloID Self-signed certificates expire in 2 years
- The portal administrator will be warned about expiring certificates
- Incidents according expiring certificates are available
- Administrators can check which certificates are used and their expiration date.

Application management

- Application catalogue available
- Additional information and guides for applications can be found on docs.helloid.com
- Preferred SSO methods are SAML or OpenIDconnect
- Use plugin applications as last resort
- Generic applications available
- SAML Metadata
- OpenIDConnect well known configuration url
- By default, new applications are added to all default groups

Lab 3

30 minutes

Adding application(s)

Description

- Add the RSA SAML Test page application from the catalogue, follow the instructions in the documentation
- Add the C2ID OpenIDConnect Demo application from the catalogue, follow the instructions in the description of the application to add the application.

Testing

- Check if the SAML application is working by clicking on the application tile in your dashboard
- Check if the OpenIDconnect application is working by clicking the “Authenticate with OpenID Connect” button on the website.

TOOLS4EVER

Please check out the references on https://docs.helloid.com
Manuals for Administrators → Application guides → Set Up a demo SSO connection to the RSA SAML Test service provider

Security

TOOLS4EVER

Security

- Roles
- Multi-Factor-Authentication
- Access rules

Roles

- HelloID user access is configured by using roles.
- By default, all users will receive the **user** role.
- Additional roles can be created or setup through the role menu.
- In the role menu you can also add additional administrators to the administrator role or add a group to a role.

Multi-Factor-Authentication

- Push-To-Verify
- SMS
- E-mail
- Hardware Token
- Webauthn (FIDO)
- You can define which types of tokens can be used through the security → 2FA Management menu.
- This menu can also be used to import OATH tokens by CSV.
  - Please provide a comma delimited with the following columns:
    - upn,serial number,secret key,timeinterval,manufacturer,model
- Remember MFA

Access Rules

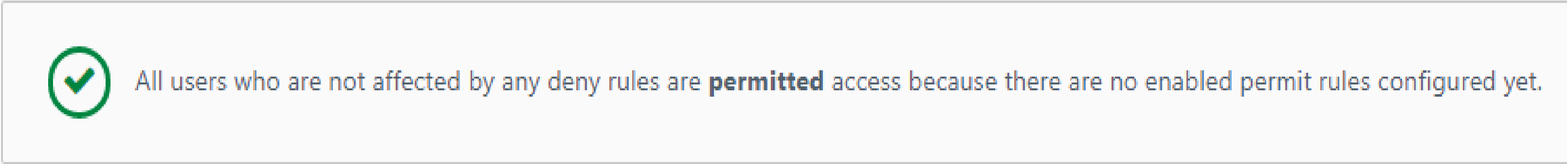
- Within HelloID access to the portal itself and the applications can be controlled by access rules.

- Please keep in mind that with identity provider client restrictions you only control which identity providers are available, with portal access rules you control which identity providers can be used.

- Two types of rules can be made
  - Portal access rules
  - Application access rules

Portal Access Rules

- Possibility to permit or deny portal access based on several options.
- The most commonly used option is the enforcement of MFA.
- Warning:



✓ All users who are not affected by any deny rules are **permitted** access because there are no enabled permit rules configured yet.

Portal Access Rules

- When making rules always make sure that no conflicting rules are made.
  - E.g. one policy that allows login for user group 1 and one policy that denies logon for user group 1.

- If you find yourself in a situation where you are locked out from your own portal please contact Tools4ever immediately.
  - A support technician can disable all rules as emergency procedure.

Portal Access Rules

- The following filter options are available:
  - Identity provider
  - User group(s)
  - Location (by country based on IP address)
  - Network (based on IP address)
  - Time (timeframe)
  - Date
  - Device / Browser type
  - MFA

Application Access Rules

- Application access rules can be created to control access to one or multiple applications Application access rules are commonly used to force users to use a specific browser for specific applications.

- Please keep in mind that application access rules will only work for applications that are using a native single sign on method.

- When using other methods, the user is always to open the target website without going through the HelloID logon process.

- If the site cannot be setup with SSO via a native solution and access rules need to be applied this can be resolved by using the HelloID reverse proxy server.

Lab 4

Access rules

30 minutes

Description

- Configure an application access rule to enforce MFA on the RSA SAML test page application you added earlier

Testing

- Check if you are required to register your MFA when opening the application. Enroll the multifactor and use the push to verify option to login to the application.

TOOLS4EVER

Please check out the references on https://docs.helloid.com
Manuals for Administrators → *Security* → Application Access Rules - Overview

Logging

Logging and Reporting

- HelloID has several reports that are available.
- To enable reports, permissions to the report module, have to be granted.
- Currently permission is arranged with the following groups:
  - Elastic_reports_read
  - Elastic_reports_write
- Currently its not possible to grant permissions to specific reports.
- Some reports might not apply for your environment.
- It is possible to create your own reports

Lab 5

Logging and reporting

15 minutes

Description

- Grant yourself access to the reporting module and view the available reports.

Testing

- After assigning the correct permissions and relogging into the portal the reports should be available.

Please check out the references on https://docs.helloid.com
Manuals for Administrators → Insights

Questions?

TOOLS4EVER

Quick reference guide

- https://docs.helloid.com/
    - Manuals
    - Changelog
    - API docs
- https://feedback.helloid.com/
    - Feature request
- https://forum.helloid.com/
    - Technical Q&A Forum
- https://roadmap.helloid.com/
    - Roadmap overview
- https://github.com/Tools4everBV
    - Connector / Forms repositories
- https://helloid.statuspage.io/
- https://docs.helloid.com/hc/en-us/categories/360002805319-Training
    - HelloID training materials

Access Management

Training day 2

TOOLS4EVER

Training content day 2

- Implementation questions
- AD IDP
- Mapping sets
- Identity providers
- Applications
- IDP Client Restrictions
- Sign-on policies
- Appearance and CSS
- Custom reports
- Troubleshooting
- HelloID API

Recap day 1

- Required resources
- Access Management Basics
- The HelloID interface
- Additional configuration options
- Applications
- Security
- Audit logging

Implementation questions

TOOLS4EVER

Pre-implementation

- During the intake you need to get several questions answered before you can continue with the planning of the actual implementation.

- We strongly suggest to create a list of all applications that should be added before the actual intake

Intake Questions

- Which identity provider(s) will be used to logon to HelloID?
- Is there a synchronization used to retrieve the users from the identity provider(s) or are the users provisioned by using just in time provisioning (JIT) ?
- Do you want to use a custom domain name?
- Is there an intranet integration needed?
- Which kind of devices are being used?

Intake Questions Continued

- Is there already an existing single sign on solution that needs to be migrated?
- If there are applications on the application list that require the use of the HelloID plugin the customer should be made aware of the pros and cons of the plugin.
- Are all requested applications already available in the catalogue or do they need to be developed?
- Are there applications that need to be enclosed by reverse proxy?
- Do you want to use multi factor authentication?

Schedule

- Schedule of implementation depends on various items.
- A basic HelloID access management implementation takes approximately two days. This includes the configuration of an IDP, user sync task and around 4 – 6 applications.
- The actual implementation time also depends very much on the fact if you want a consultant to implement the environment or you will do parts yourself.

AD IDP

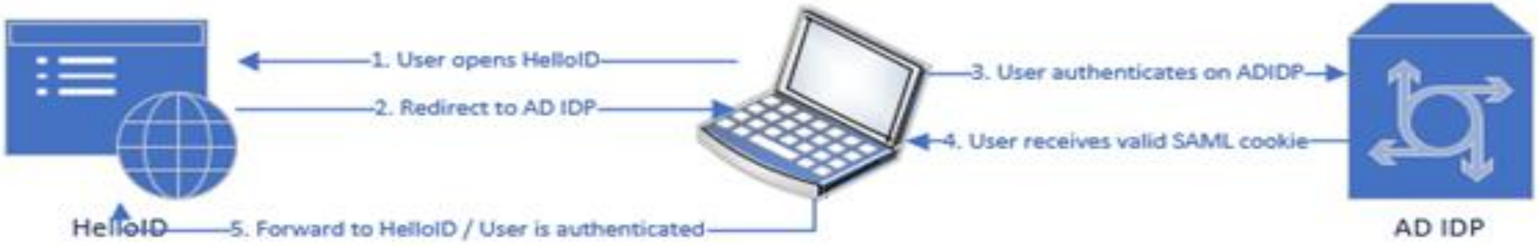
Active Directory Identity Provider

TOOLS4EVER

Active Directory Identity Provider (ADIDP)

- The AD IDP is an IIS website that is hosted on an internal webserver at the customer site.

- This website is used to provide a single sign-on solution for users that are logged on to a domain joined computer.


1. User opens HelloID
2. Redirect to AD IDP
3. User authenticates on ADIDP
4. User receives valid SAML cookie
HelloID
5. Forward to HelloID / User is authenticated
AD IDP

Active Directory Identity Provider (ADIDP)

- The requirements for the AD IDP can be found on out documentations website https://docs.helloid.com

- Please see doc: How-to-Configure-the-HelloID-Active-Directory-Identity-Provider

- To use the AD IDP it might be needed to change some client-side settings.

Lab 6

AD IDP

60 minutes

Description

- Setup the AD IDP on your test environment.
- For testing its not required to create a https binding with a SSL certificate.

Testing

- After installing and configuring the AD IDP all users that are browsing to HelloID from a domain joined machine should be authenticated automatically and not be prompted for a username and password.

Please check out the references on https://docs.helloid.com

Manuals for Administrators → Identity Provider Guides → Configure the HelloID Active Directory SAML Idp

Mapping sets

Mapping sets

- Used in:
  - IDP configurations
  - SAML and OpenID configurations
  - Synchronization configurations
- Used to define which attributes are retrieved from an Identity provider or sent to a service provider
- Hardcoding attribute values is possible
- Newly created userattributes in HelloID cannot be deleted
- HelloID Intellisense

Identity providers

TOOLS4EVER

Other IDP’s

- Within HelloID it is possible to configure as many other identity providers as needed.

- The most commonly used additional identity providers are:
  - Active Directory Federation Services (ADFS)
  - Azure Active Directory
  - Google Gsuite

- You can find the documentation for these additional identity providers on the HelloID documentation website “Identity Provider Guides”

- Configuring multiple identity providers may result in a prompt for end users if no filtering is possible

Single Sign-on Types

TOOLS4EVER

Single Sign-on Types

- SAML = **S**ecurity **A**ssertion **M**arkup **L**anguage
  - an open standard which defines the rules and definitions for exchanging authorization and authentication data between identity and service providers.
  - SAML is a web based single sign-on standard.
  - More info: https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

Single Sign-on Types

- OPENID Connect
  - an authentication standard which is controlled by the OpenID Foundation.
  - Based on the OAUTH 2.0. protocol by OpenID
  - Less room for custom implementations like the SAML standard
  - Easier to configure than SAML
  - More info: https://openid.net/

Single Sign-on Types

HelloID Plugin/Post

- Last ditch effort to provide SSO to end-users.
- Possibility for applications that can’t be connected with a standard SSO method like SAML or OpenID.
- Using password vault principle.
- Available for:
  - Internet Explorer
  - Google Chrome
  - Firefox (desktop and mobile)
  - Edge (Chromium)

Single Sign-on Types

- Besides SAML, OpenID Connect and HelloID Plugin, HelloID supports the following single sign on methods:
  - FORM Post
  - Basic authentication
  - WS-Federation
- All methods above do not require the HelloID plugin to be installed.

IDP Client Restrictions

TOOLS4EVER

IDP Client Restrictions

- Used to show only one IDP based on IP or Source device.
- IP is always the WAN IP of the client
- When only one IDP is available to the end user he will always get automatically redirected unless the always show login selector option is set.
- A hidden IDP will still work by visiting the link directly and is visible when the “Choose other method” button is used.

Lab 7

IDP Client Restrictions

30 minutes

Description

- Make sure that when browsing to HelloID from your test machine you are getting authenticated automatically through the installed AD IDP
- Make sure that when you are browsing to HelloID from any other device the Active Directory logon is shown directly.

Testing

- On your testdevice the user should be automatically logged on through the AD IDP
- On any other machine only the Active directory logon screen should be shown.

TOOLS4EVER

Please check out the references on https://docs.helloid.com
Manuals for Administrators → Security → Configure multiple IDPs with Client restrictions

Sign-On Policies

TOOLS4EVER

Sign-On Policies

- Policy definitions for Signing in to HelloID

- The following options only apply to local accounts:
  - Lock user after number of invalid password entries
  - Lock user after invalid password count
  - Unlock user after specified amount of time
  - Lock Time (minutes)
  - Change password after specified amount of time
  - Change password time (days)

Sign-On Policies

- Use the User session timeout and the fixed session timeout settings to control the user session.

- QR Code login is a login method especially made for primary schools and other low risk environments.

- The allow Self Service Enrollment for MFA via E-Mail option is only used for the forced MFA option on e-mail.

- Remember me: If this option is enabled users can check the remember me option during logon, during the amount of days setup in the policy they are not asked for their username and password but only must enter one of their configured MFA options.

Appearance and CSS

TOOLS4EVER

Appearance and CSS

- You can change the appearance of the end-user portal as well as some default behavior within HelloID.

- It is also possible to provide a custom css to change items which are not configurable within HelloID.

- Please be aware when using custom css settings that you must be as specific as possible when selecting elements.

Create custom reports

TOOLS4EVER

Create custom reports

- Discover
- Index
- Visualizations
- Dashboards

Lab 8

Custom Reports

30 minutes

Description

- Create a new report space
- Add a custom dashboard to your newly created space which shows a graph of all successful login attempts on your portal.

Testing

- After creating your new dashboard, it should be available in the reporting overview

Please check out the references on https://docs.helloid.com
Manuals for Administrators → Insights→ Create a custom Elastic report

Troubleshooting

Troubleshooting

- Almost all authentication traffic is handled by the browser of the end-user. This is also the place where most issues occur with logging into applications.

- When users are having problems logging into applications please first make sure the user has access to the HelloID portal and application.

- If not check if the accounts exist in HelloID and has the application available in the dashboard.

Troubleshooting Plugin

- When end-users report issues with plugin applications please check the following items.
  - Is the plugin installed?
  - Is there an active session with the HelloID portal?
  - In internet explorer is the setting “Enable third-party browser extensions” turned on ?
  - When using internet explorer, is the requested application website in the same zone as the HelloID portal?

Troubleshooting SAML

- Its possible to view the contents of unencrypted SAML message
- Use a plugin like SAML Chrome panel
- If no plugin can be installed the intercepted SAML message can be decoded from the Base64 format

Lab 9

Troubleshoot SAML

15 minutes

Description

- View the contents of the SAML message that is being sent when opening the earlier created SAML test application

Testing

- You should be able to view the contents of the SAML message when opening the SAML test application.

TOOLS4EVER

Please check out the references on https://docs.helloid.com
Manuals for Administrators → Troubleshooting → SAML Troubleshooting Basics

HelloID API

TOOLS4EVER

HelloID API

- Within HelloID an API is available
- Always use skip & take when retrieving datasets
- API documentation is available at docs.helloid.com → API Docs

Lab 10

15 minutes

HelloID API (optional)

Description

- Retrieve a single user through the HelloID API by using powershell
- Update the name of the user through the HelloID API by using powershell

Testing

- After running the update script check the result in the Admin interface.

Please check out the references on https://docs.helloid.com
API Docs → Users

Questions?

TOOLS4EVER

Quick reference guide

- https://docs.helloid.com/
  - Manuals
  - Changelog
  - API docs
- https://feedback.helloid.com/
  - Feature request
- https://forum.helloid.com/
  - Technical Q&A Forum
- https://roadmap.helloid.com/
  - Roadmap overview
- https://github.com/Tools4everBV
  - Connector / Forms repositories
- https://helloid.statuspage.io/
- https://docs.helloid.com/hc/en-us/categories/360002805319-Training
  - HelloID training materials