Forcepoint

Forcepoint Data Classification

Powered by Getvisibility

[22.0.4+] Keycloak User Federation Configuration (LDAP/AD)

Forcepoint

Report

Forcepoint
15 July, 2024
Forcepoint Proprietary

forcepoint.com

Table of Contents

Introduction

The authentication protocol that the customer decides to use is different per use case. Below is some guidance on how to configure a User Federation in Keycloak.

Configuring the User Federation

1. As we are looking to authorize our users for the GetVisiblity dashboard (not Keycloak itself), make sure that it is the **gv** realm selected in the top left, **not** *master* (unless you are looking to authorize LDAP users to use Keycloak):

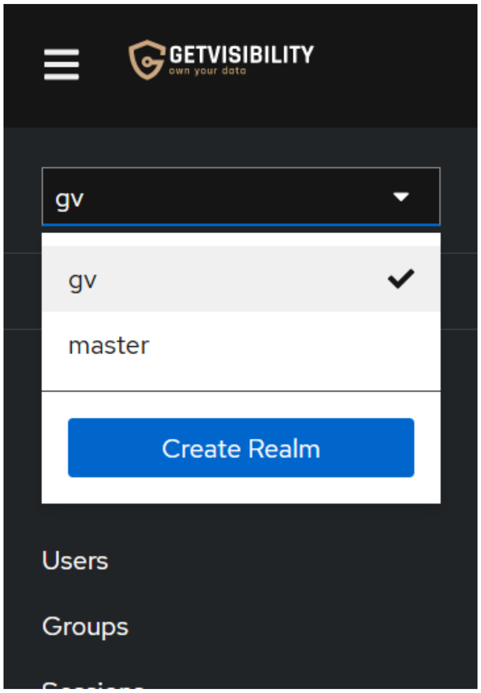
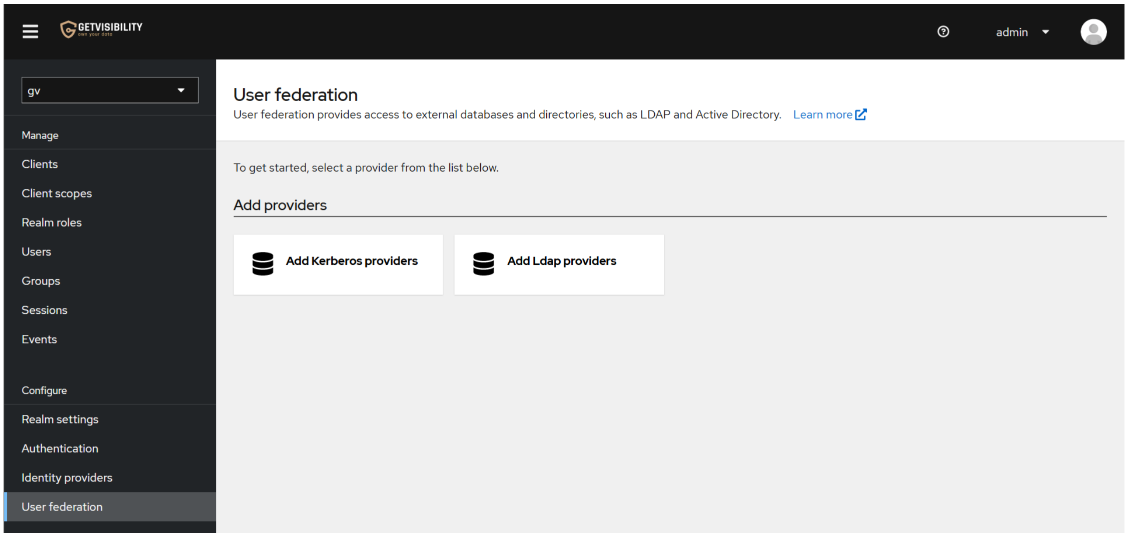


figure 1.

2. Click on the **User Federation** menu item on the left pane. This should load a list of configured user federations (none at first).



User federation

User federation provides access to external databases and directories, such as LDAP and Active Directory.

To get started, select a provider from the list below.

figure 2.

3. Click on **Add Ldap providers** to load the LDAP (Lightweight Directory Access Protocol) configuration.

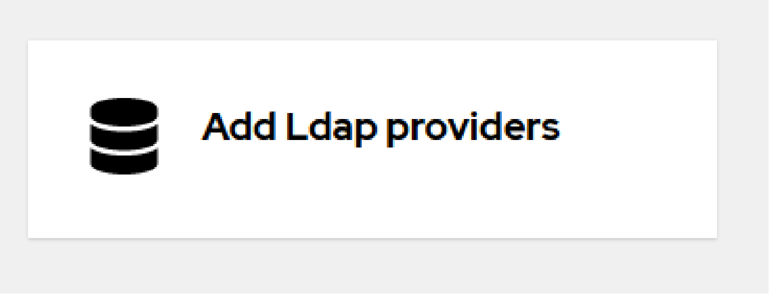
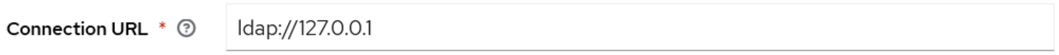


figure 3.

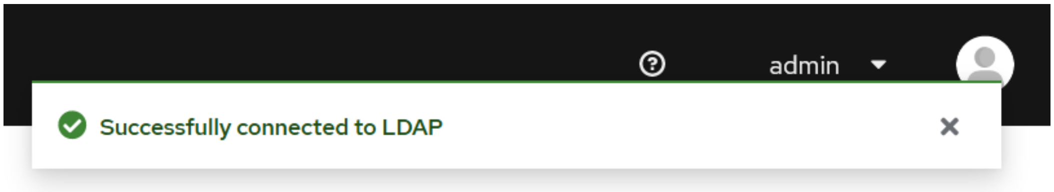
4. Update the **Connection URL** field to reflect the **LDAP server address** where the **Active Directory** is hosted.



Connection URL * ldap://127.0.0.1

figure 4.

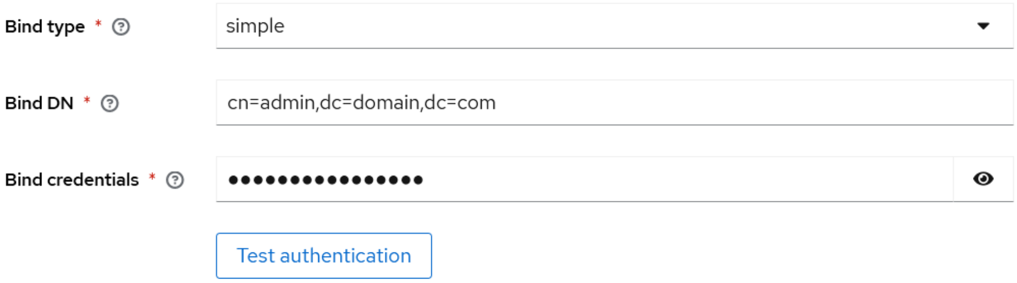
5. Click on the button **Test connection** to test the connection from the Keycloak instance to the LDAP server address. This should succeed quickly. If it hangs, the LDAP server (i.e. a domain controller) may be **blocking connections** from the Keycloak server address (i.e. the IP of the server running the GetVisibility product). You may need to use the Public IP address of the LDAP server.



Successfully connected to LDAP

figure 5.

6. Update the **Bind DN** field to reflect the user used to access the LDAP server. In this case, the user with username “admin” from the domain “domain.com.”



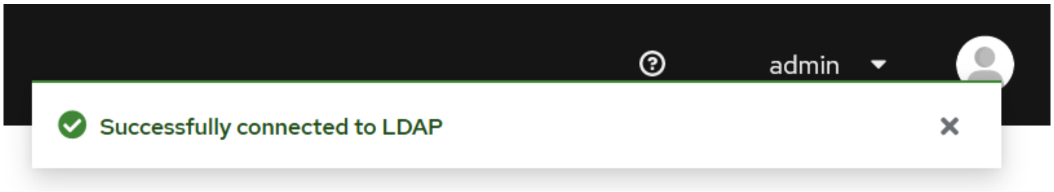
Bind type *	simple
Bind DN *	cn=admin,dc=domain,dc=com
Bind credentials *	●●●●●●●●●●●●●●●●

figure 6.

NOTE: For **Active Directory**, the value for the **Bind DN** field could be `serviceaccount@MY-AD-DC.LOCAL`.

7. Update the **Bind credentials** field (see the above image) to contain the password used to access the LDAP server

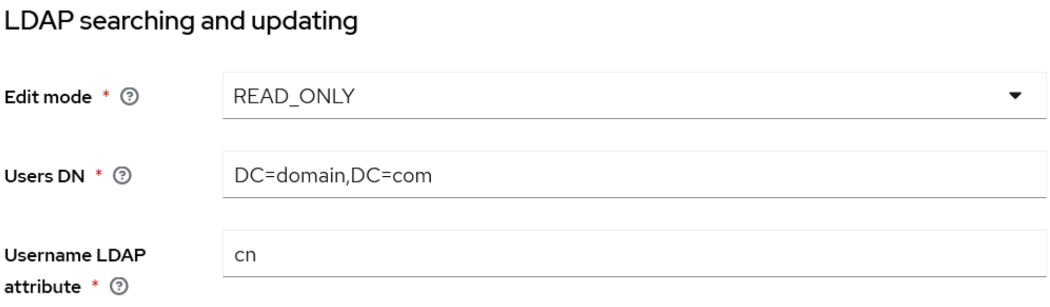
8. Click “**Test authentication**” to confirm that the provided credentials work as expected:



Successfully connected to LDAP

figure 7.

9. Update the Users DN field to contain the **Full DN of the LDAP tree** where your users are.



LDAP searching and updating

Edit mode *	READ_ONLY
Users DN *	DC=domain,DC=com
Username LDAP attribute *	cn

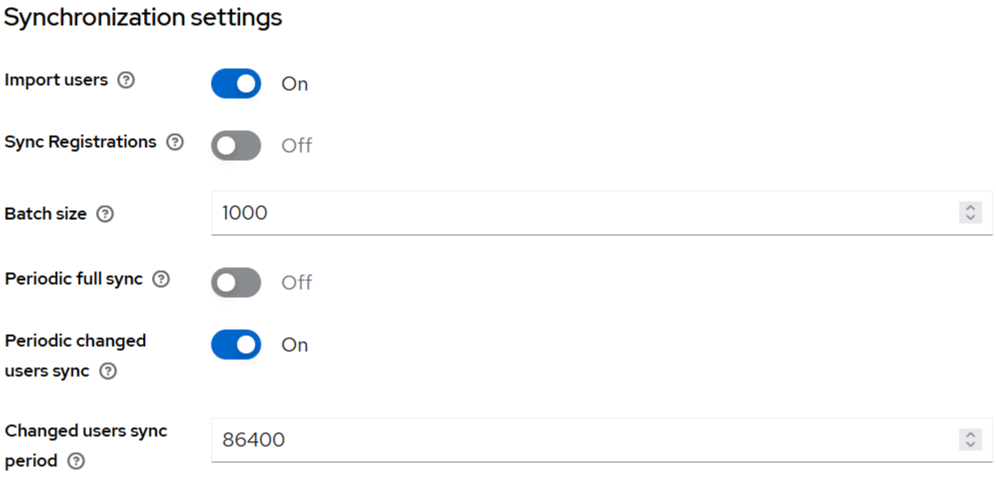
figure 8.

The above value for the “**Users DN**” field will import all users to the **gv** realm. All users within the “domain.com” domain will get full administrative access for the GetVisiblity dashboard.

If this is not desired, make restrictions to which users are imported, e.g. `CN=MyGroup,OU=Users,DC=MyDomain,DC=com`

For AD Server federation, some may prefer to configure the Username LDAP attribute as sAMAccountName or userPrincipalName. See https://learn.microsoft.com/en-ie/windows/win32/ad/naming-properties?redirectedfrom=MSDNand https://activedirectorypro.com/ad-ldap-field-mapping/.

10. (Optional) Within **Synchronization settings**, set up automatic synchronization of users from the LDAP Active Directory to Keycloak.
    You can configure the auto-synchronization settings here if you like.



Synchronization settings

Import users: On

Sync Registrations: Off

Batch size: 1000

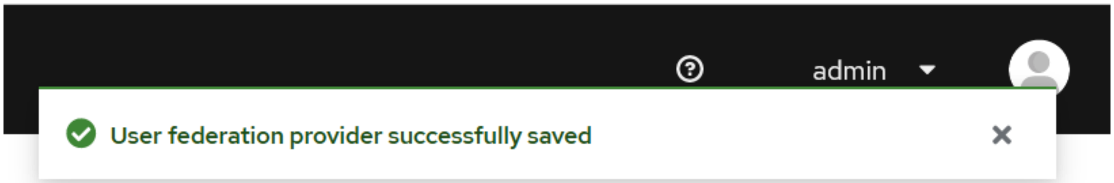
Periodic full sync: Off

Periodic changed users sync: On

Changed users sync period: 86400

figure 9.

11. Click the **Save** button at the bottom of the screen.



User federation provider successfully saved

figure 10.

Synchronizing the Users to Keycloak DB

To get the users into the Keycloak DB, we need to synchronize the users for the first time (before the automatic synchronization happens, if applicable).

This is one simple step:

1. Click the button **Synchronize all users** to immediately fetch all of the LDAP Active Directory users and load them into

the Keycloak instance DB

Synchronizing all users may take some time.

Troubleshooting Keycloak LDAP integration

Usually, any issues that occur during the LDAP Active Directory configuration process above will be related to Network accessibility concerns or authentication credentials being incorrect.

However, if you require any additional support or your problem is not easily resolved by troubleshooting Network communications and authentication details, please reach out to our support at support.forcepoint.com forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's humanly attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.