



RiskTech
100
2018



Gartner 2015
Cool Vendor

NG | Auth

Tonny Kibet

April 2019, Nairobi, Kenya



Summary

- Introduction
- Core Concepts and Terms
- Admin Console
- Configuration

Introduction





NG | Auth - Introduction

- Single Sign On solution (SSO) for NG|Screener suite
- Customizable user interfaces for
 - Login
 - Registration
 - Administration
 - Account management
- Integration with existing LDAP and Active Directory servers

Core Concepts and Terms





Core Concepts and Terms

- Users (entities able to log in the system)
- Authentication (the process of identifying and validating a user)
- Authorization (the process of granting access to a user)
- Credentials
- Roles



Core Concepts and Terms

- User Role Mapping (mapping between a role and a user)
- Groups (management of users)
- Realms (manages a set of users, credentials, roles and groups)

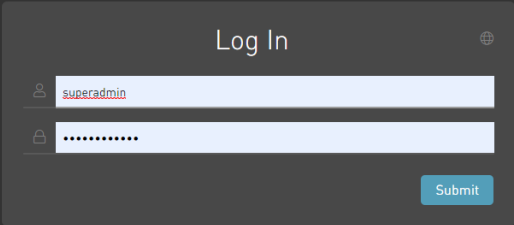


Access NG|Auth

URL: <https://myhost/auth/admin/>

User: superadmin

Password: netguardians



The image shows a dark-themed login interface for NetGuardians. At the top center is the NetGuardians logo, which consists of a blue hexagon with a white 'N' inside, followed by the text 'NetGuardians'. Below the logo is a light gray rectangular box containing the login form. The form has a title 'Log In' at the top right. It features two input fields: the first is for the username, with a user icon on the left and the text 'superadmin' entered; the second is for the password, with a lock icon on the left and masked characters '*****' entered. A blue 'Submit' button is located at the bottom right of the form. At the bottom of the dark background, there is a small copyright notice: '© 2018 - 2022 NetGuardians, Inc. All Rights Reserved.'

Admin Console





Admin Console

Most of the user administration tasks will be done through the Admin Console.

- LEFT MENU

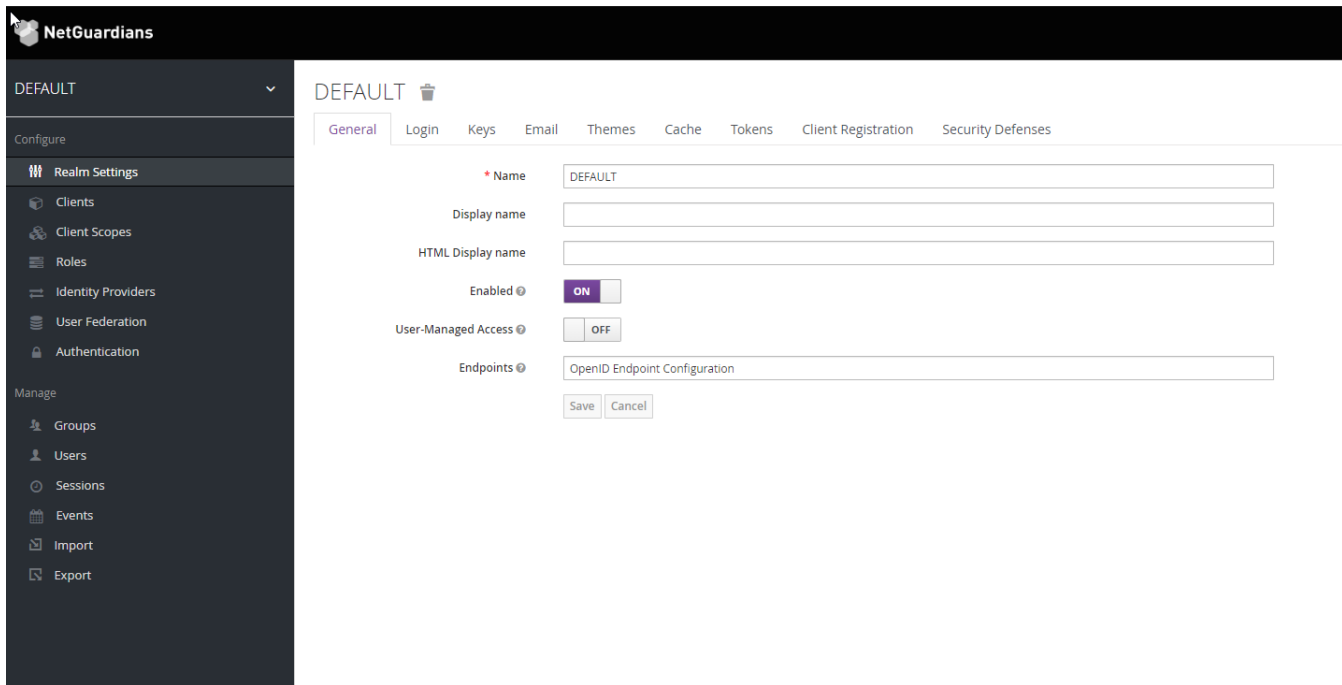
- Pick and manage a realm
- Create a realm

- RIGHT drop down menu

- View user account
- Logout

- TIP

- Hover the mouse over any “?” icon to see the description



Configuration





Create a new Realm

- Using the script `/usr/local/ngscreener/tools/multi-tenancy/createTenant.py`.
`./createTenant.py -t MYNEWTENANT -u superadmin -p netguardians -url https://mytenanturl1.mycompany.com/auth/`

NOTE: Using the script is the preferable method to using the UI

- Configuration:

- A Realm corresponds to the Tenant Created in NG|Screener.
- This allows Multi-Tenancy authentication to be done in once instance.
- 1 Tenant in ng|screener = 1 Realm in NG|Auth

The screenshot displays the NetGuardians web interface. On the left is a dark sidebar with a menu. The top of the sidebar shows 'NetGuardians' and a dropdown menu currently set to 'DEFAULT'. Below this is a 'Master' section with an 'Add realm' button. The main menu includes 'Clients', 'Client Scopes', 'Roles', 'Identity Providers', 'User Federation', and 'Authentication'. A 'Manage' section at the bottom contains 'Groups', 'Users', 'Sessions', 'Events', 'Import', and 'Export'. The main content area on the right is titled 'DEFAULT' with a trash icon. It features a tabbed interface with 'General' selected. The 'General' tab contains the following fields and controls: 'Name' (set to 'DEFAULT'), 'Display name' (empty), 'HTML Display name' (empty), 'Enabled' (toggle switch set to 'ON'), 'User-Managed Access' (toggle switch set to 'OFF'), and 'Endpoints' (set to 'OpenID Endpoint Configuration'). 'Save' and 'Cancel' buttons are at the bottom of the form.



Create a new Realm

The screenshot shows the NetGuardians Admin Console interface. On the left is a dark sidebar with the 'NetGuardians' logo at the top. Below the logo, there's a 'DEFAULT' dropdown menu. The sidebar is divided into sections: 'Configure' (with a mouse cursor over it), 'Realm Settings' (containing 'Clients', 'Client Scopes', 'Roles', 'Identity Providers', 'User Federation', and 'Authentication'), and 'Manage' (containing 'Groups'). The main content area has a header with 'DEFAULT' and a trash icon. Below this is a tabbed interface with tabs for 'General', 'Login', 'Keys', 'Email', 'Themes', 'Cache', 'Tokens', 'Client Registration', and 'Security Defenses'. The 'General' tab is active, showing a form with the following fields: 'Name' (with a red asterisk and the value 'DEFAULT'), 'Display name', 'HTML Display name', 'Enabled' (a toggle switch set to 'ON'), 'User-Managed Access' (a toggle switch set to 'OFF'), and 'Endpoints' (with the value 'OpenID Endpoint Configuration'). At the bottom of the form are 'Save' and 'Cancel' buttons.

- After creating the realm you are brought back to the main Admin Console page.
- The current realm will now be set to the realm you just created



Create a new Role (1/2)

- A role in NG|Auth is a global namespace. Functionalities defined in ngBrowser or ngCaseManager

NetGuardians Superadmin

DEFAULT

Configure

Realm Settings

Clients

Client Scopes

Roles

Identity Providers

User Federation

Authentication

Manage

Groups

Users

Roles

Realm Roles Default Roles

Search...

Role Name	Composite	Description	Actions	
NG_Admin	False	Full administrator role	Edit	Delete
NG_User	False		Edit	Delete
offline_access	False	\${role_offline-access}	Edit	Delete
TEST_ALL_CONTROLS_NO_MANAGE	False		Edit	Delete
TEST_ALL_CONTROLS_ONLY	False		Edit	Delete
TEST_IB_SCO_MANAGER	False		Edit	Delete
TEST_OWN_CONTROLS_ONLY	False		Edit	Delete
TEST_OWN_PUB_CONTROLS_ONLY	False		Edit	Delete
uma_authorization	False		Edit	Delete

Add Role

- To create a role, click Add Role on this page, enter in the name and description of the role, and Save.



Create a new Role (2/2)

The screenshot shows the NetGuardians web interface. On the left is a dark sidebar with a menu. The top of the sidebar has the 'NetGuardians' logo and a 'DEFAULT' dropdown. Below this are two sections: 'Configure' and 'Manage'. The 'Configure' section includes 'Realm Settings', 'Clients', 'Client Scopes', 'Roles' (which is highlighted with a purple bar), 'Identity Providers', 'User Federation', and 'Authentication'. The 'Manage' section includes 'Groups', 'Users', 'Sessions', and 'Events'. The main content area on the right has a breadcrumb 'Roles > Add Role' and a title 'Add Role' with a mouse cursor pointing at it. Below the title is a form with two fields: 'Role Name' with the value 'NG_Admin' and 'Description' with the value 'Full Administrator Role'. At the bottom of the form are 'Save' and 'Cancel' buttons.

NetGuardians

DEFAULT

Configure

- Realm Settings
- Clients
- Client Scopes
- Roles**
- Identity Providers
- User Federation
- Authentication

Manage

- Groups
- Users
- Sessions
- Events

Roles > Add Role

Add Role

* Role Name NG_Admin

Description Full Administrator Role

Save Cancel

- Roles can also be created using a script

`/usr/local/ngscreener/tools/auth/createRoleKeycloak.py`



Create a new User

- After selecting the right tenant, click on Users in the left menu bar
- Add User

The screenshot displays the NetGuardians web application interface. At the top, a black header bar contains the 'NetGuardians' logo on the left and a user profile 'Superadmin' with a dropdown arrow on the right. Below the header, a dark grey sidebar menu is visible on the left. It has a 'DEFAULT' section with a dropdown arrow, followed by a 'Configure' section containing links for 'Realm Settings', 'Clients', 'Client Scopes', 'Roles', 'Identity Providers', 'User Federation', and 'Authentication'. Below these is a 'Manage' section with links for 'Groups', 'Users' (which is highlighted with a purple bar), 'Sessions', 'Events', 'Import', and 'Export'. The main content area on the right is titled 'Users' and features a 'Lookup' tab. Below the tab is a search bar with a 'Search...' placeholder, a magnifying glass icon, and a 'View all users' button. To the right of the search bar are 'Unlock users' and 'Add user' buttons. At the bottom of the search bar, a message reads: 'Please enter a search, or click on view all users'.



Create a new User

- Input Username then save → management page for your new user

The screenshot displays the NetGuardians web application interface. On the left is a dark sidebar with a menu. The top of the sidebar has the 'NetGuardians' logo and a 'DEFAULT' dropdown. Below this, the menu is divided into 'Configure' (containing Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, and Authentication) and 'Manage' (containing Groups, Users, Sessions, Events, Import, and Export). The 'Users' option is currently selected. The main content area on the right is titled 'Users > Add user' and contains the 'Add user' form. The form includes input fields for ID, Created At, Username (pre-filled with 'demouser'), Email (pre-filled with 'demouser@netguardians.ch'), First Name (pre-filled with 'Demo'), and Last Name (pre-filled with 'User'). There are also toggle switches for 'User Enabled' (set to 'ON') and 'Email Verified' (set to 'OFF'). A dropdown for 'Required User Actions' is set to 'Select an action...', and a 'Locale' dropdown is set to 'Select one...'. At the bottom of the form are 'Save' and 'Cancel' buttons.

- Or by script

`/usr/local/ngscreener/tools/auth/createUserKeycloak.py`



User Role Mappings

- Can be assigned individually to each user through the Role Mappings tab

The screenshot displays the NetGuardians web application interface. On the left is a dark sidebar with a navigation menu. The main content area shows the 'Role Mappings' tab for a user named 'Demouser'.

NetGuardians

DEFAULT ▾

Users » demouser

Demouser 🗑️

Details Attributes Credentials **Role Mappings** Groups Consents Sessions

Realm Roles

Available Roles ⓘ

- NG_Admin
- NG_User
- TEST_ALL_CONTROLS_NO_MANAGE
- TEST_ALL_CONTROLS_ONLY
- TEST_IB_SCO_MANAGER

Add selected >

Assigned Roles ⓘ

- offline_access
- uma_authorization

<< Remove selected

Effective Roles ⓘ

- offline_access
- uma_authorization

Client Roles

Select client to view roles for client

▾



User Federation (Adding a Provider) LDAP

- To add a storage provider go to the User Federation left menu item in the Admin Console
- Add Provider list box. Choose the provider type you want to add and you will be brought to the configuration page of that provider

The screenshot displays the NetGuardians Admin Console interface. On the left is a dark sidebar with a 'NetGuardians' header and a menu. The 'User Federation' item is highlighted under the 'Configure' section. The main content area is titled 'User Federation' and features a database icon. Below the icon, text states: 'Keycloak can federate external user databases. Out of the box we have support for LDAP and Active Directory. To get started select a provider from the dropdown below:'. A dropdown menu is open, showing 'Add provider...' at the top, followed by 'kerberos' and 'ldap'.



How to setup a new LDAP connection

- Click on the "User Federation" left menu to access the Federation part. Then choose Ldap to create a new connection. Then fill the required fields to get the connection working :

The screenshot shows the NetGuardians web interface. On the left is a dark sidebar with a menu. The 'User Federation' section is highlighted. The main content area is titled 'Add user federation provider' and contains a 'Required Settings' form. The form includes various fields for configuring an LDAP connection, with some fields highlighted in yellow. On the right side of the form are two buttons: 'Test connection' and 'Test authentication'.

NetGuardians

DEFAULT

Configure

- RealM Settings
- Clients
- Client Scopes
- Roles
- Identity Providers
- User Federation**
- Authentication

Manage

- Groups
- Users
- Sessions
- Events
- Import
- Export

User Federation > Add user storage provider

Add user federation provider

Required Settings

Enabled ☒

Console Display Name

Priority

Import Users ☒

Edit Mode

Sync Registrations ☐

* Vendor

* Username LDAP attribute

* RDN LDAP attribute

* UUID LDAP attribute

* User Object Classes

* Connection URL

* Users DN

* Authentication Type

* Bind DN

* Bind Credential

Test connection

Test authentication



How to setup a new LDAP connection

- After saving, it's time to configure some mappers to map data from LDAP to the NG|Auth data model
- ROLE_MAPPER to map some ROLE from the LDAP server with LDAP users
- Use Mappers tab → Create

User Federation » Ldap » LDAP Mappers

Ldap 

Settings

Mappers

Search...		Create
Name	Type	
first name	user-attribute-ldap-mapper	
email	user-attribute-ldap-mapper	
modify date	user-attribute-ldap-mapper	
last name	user-attribute-ldap-mapper	
MSAD account controls	msad-user-account-control-mapper	
username	user-attribute-ldap-mapper	
creation date	user-attribute-ldap-mapper	



How to setup a new LDAP connection

- Test connections once you enter both the Connection URL and Users DN, Bind DN and Bind Credential

Import Users ☒ Success! LDAP connection successful. ✕

Edit Mode

Sync Registrations ☐ OFF

* Vendor

* Username LDAP attribute

* RDN LDAP attribute

* UUID LDAP attribute

* User Object Classes

* Connection URL

* Users DN

* Authentication Type

* Bind DN

* Bind Credential

Custom User LDAP Filter

Search Scope

Validate Password Policy ☐ OFF

Use Truststore SPI

Connection Pooling ☒

[Test connection](#)

[Test authentication](#)

[Connection Pooling Settings](#)



Sync of LDAP users to NG|Auth

- If user import is enabled, the LDAP Provider will automatically take care of synchronization
- Sync all LDAP users into the NG|Auth database → configure and enable the Sync

Settings

Sync Settings

Batch Size ?	<input type="text" value="1000"/>
Periodic Full Sync ?	<input checked="" type="checkbox"/>
Full Sync Period ?	<input type="text" value="604800"/>
Periodic Changed Users Sync ?	<input checked="" type="checkbox"/>
Changed Users Sync Period ?	<input type="text" value="86400"/>

Cache Settings

Cache Policy ?	<input type="text" value="DEFAULT"/>
----------------	--------------------------------------



Sync of LDAP users to NG|Auth

- Once you save all Ldap setting and ensure all connections are tested, synch all users.
- Go to the Users tab and click on View all users you will be able to see all users imported.

Users

Lookup

<input type="text" value="Search..."/>	<input type="button" value="Q"/>	<input type="button" value="View all users"/>						<input type="button" value="Unlock users"/>	<input type="button" value="Add user"/>
ID	Username	Email	Last Name	First Name	Actions				
db607361-2f00-4ef7-9da0-66a62c3b...	admin			Administrator	Edit	Impersonate	Delete		
292efe47-56cb-4980-b422-52a1f7af...	demouser	demouser@netguardians.ch	User	Demo	Edit	Impersonate	Delete		
02f2fdb8-0273-4363-b70e-82de869...	ngscreener			ngscreener	Edit	Impersonate	Delete		
3a2848ef-1863-4f58-809c-d142ab38...	testallcontrols			testallcontrols	Edit	Impersonate	Delete		
c3d5dd98-a244-4aa4-8ac6-3f4f290b...	testallcontrolsmanage			testallcontrolsmanage	Edit	Impersonate	Delete		
f92d709b-3e47-4a76-973d-13cb54c...	testibscomanager			testibscomanager	Edit	Impersonate	Delete		
7dd00d71-62d0-4339-a608-2eb1fc3...	testowncontrols			testowncontrols	Edit	Impersonate	Delete		
72adc73b-2ba3-42da-b646-12c7dc0...	testownpubcontrols			testownpubcontrols	Edit	Impersonate	Delete		
0ace4168-18e2-4288-b3aa-f725f54b...	training1	training1@corp.netguardians.ch	1	training1	Edit	Impersonate	Delete		
031c1d1a-d7bf-45db-969b-c177280...	training2	training2@corp.netguardians.ch	2	training2	Edit	Impersonate	Delete		
6d833144-872a-4942-a257-d2c985e...	training3	training3@corp.netguardians.ch	3	training3	Edit	Impersonate	Delete		
3737ee21-7e03-4a6c-a20e-aa96b8e...	training_admin1	training_admin1@corp.netguardian...	Admin1	training_admin1	Edit	Impersonate	Delete		
f828aaad-2f9b-4e4e-ac1c-900ae7b5...	training_admin2	training_admin2@corp.netguardian...	Admin2	training_admin2	Edit	Impersonate	Delete		
329ced58-3eef-4289-a06d-d659135...	user			user	Edit	Impersonate	Delete		



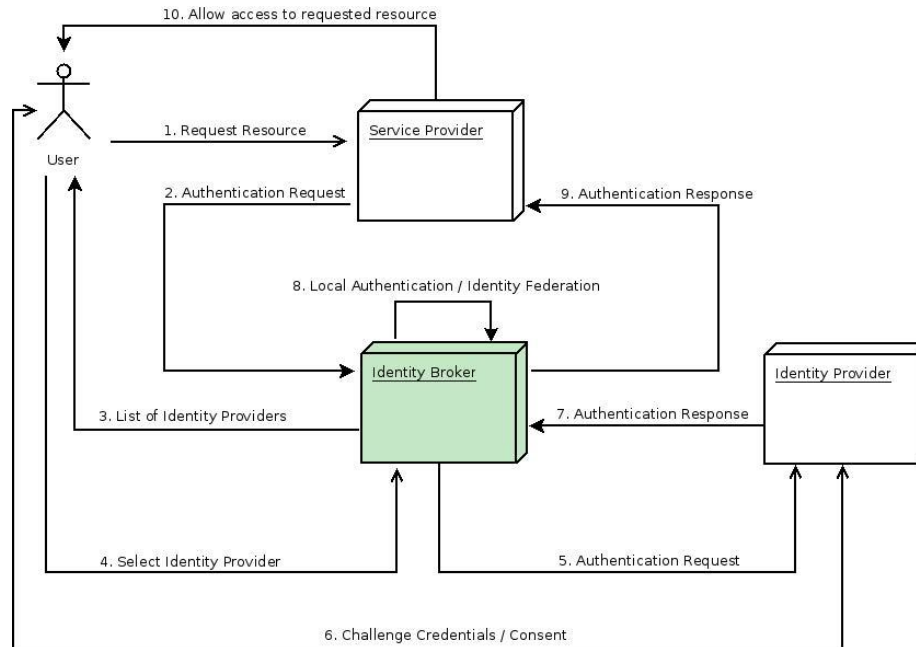
Password Hashing

- When the password of user is updated from NG|Auth and sent to LDAP, it is always sent in plain-text
- In the case of LDAP, the NG|Auth relies on the LDAP server to provide hashing and salting of passwords
- Most of LDAP servers (Microsoft Active Directory, RHDS, FreeIPA) provide this by default.
- Some others (OpenLDAP, ApacheDS) may store the passwords in plain-text by default and one may need to explicitly enable password hashing for them



Identity Brokering

- Identity Broker is an intermediary service that connects multiple service providers with different identity providers creating a trust relationship





User Management

- Role mapping
 - NG|Auth also associates roles to each user.
 - Roles are only plain names at NG|Auth level
 - Default role: NG_Admin.

Roles » NG_Admin



NG_Admin 

Details

Attributes

Users in Role

Username	Last Name	First Name	Email	
ngscreener		ngscreener		Edit
admin		Administrator		Edit



User Management

- Each application using NG|Auth should provide mappings of functionalities with the role names
 - I.e. the names of the roles in NG|screener have to find the corresponding name in NG|Auth
- Scripts for create roles and users (2 scripts in the following folder)
 - /usr/local/ng-screener/tools/auth



User Management

Multi-tenant installation

NG| Screener is always installed in multi-tenant mode, which enables each and every login to be contextual to one tenant (= one of the hosted banks or specific bank internal unit) and, as such, isolated from the other tenants.

This is configured in the `/etc/ng-screener/common/ng-screener.conf` configuration file, through the following property:

```
#-----
```

```
# Multi-Tenancy
```

```
# List of tenants, must be in Upper case. Must not be empty.
```

```
# Example: multiTenancy.tenants = TENANT1,TENANT2,TENANT3
```

```
multiTenancy.tenants = DEFAULT
```



Thank you!

NetGuardians



+41 24 425 97 60



info@netguardians.ch



www.netguardians.ch



[Linkedin.com/company/netguardians](https://www.linkedin.com/company/netguardians)



[Facebook.com/NetGuardians](https://www.facebook.com/NetGuardians)



[@netguardians](https://twitter.com/netguardians)



<https://www.youtube.com/netguardians>

Tonny / Kibet



kibet@netguardians.ch

Contact us

NetGuardians Headquarters

Y-Parc, Av. des Sciences 13
1400 Yverdon-les-Bains
Switzerland

T +41 24 425 97 60

NetGuardians Africa

The Mirage, Tower 2, Pentfloor
Waiyaki Way, Westlands
00101 Nairobi, Kenya

T +254 797735 050

NetGuardians Asia

143 Cecil Street
#09-01 GB Building
069542 Singapore

T +65 6224 0987

NetGuardians Germany

Rhein-Main Gebiet
Germany

T +49 172 3799003

NetGuardians Eastern Europe

WeWork
Krucza 50, 00-025
Warsaw, Poland

