|  |
| --- |
| IBM Corp. |
| IBM Security Verify |
| Authenticator Extensions for Keycloak |

Table of Contents

[Introduction 2](#_Toc42523975)

[Getting Started 2](#_Toc42523976)

[Software/Hardware Requirements 2](#_Toc42523977)

[Installation 2](#_Toc42523978)

[Server Administration 3](#_Toc42523979)

[Creating an IBM Security Verify API Client 3](#_Toc42523980)

[IBM Verify Mobile Application 5](#_Toc42523981)

[FIDO2 Device Support 5](#_Toc42523982)

[FIDO2 Relying Party Setup 5](#_Toc42523983)

[Authentication Flow Setup 6](#_Toc42523984)

[Creating and Enabling an Authentication Flow in Keycloak/RedHat SSO 7](#_Toc42523985)

[One-time Passcode 10](#_Toc42523986)

[Push Notification 12](#_Toc42523987)

[QR Code 15](#_Toc42523988)

[FIDO2 17](#_Toc42523989)

[Account Management 21](#_Toc42523990)

[IBM Security Verify: Dashboard and Analytics 22](#_Toc42523991)

[Dashboard 22](#_Toc42523992)

[Authentication Activity 22](#_Toc42523993)

[Sample Keycloak Demo Experience 23](#_Toc42523994)

[Known Issues 23](#_Toc42523995)

[FAQ 23](#_Toc42523996)

[Releases 24](#_Toc42523997)

[v1.0 24](#_Toc42523998)

[Supported Versions 24](#_Toc42523999)

# Introduction

Security requirements continue to evolve in response to newly discovered threats and attacks on user data. These security requirements are also driven by business requirements such as enforcing multi-factor authentication (MFA) or enabling MFA for varied types of applications to remain compliant with industry regulations. Organizations are looking for measures to improve their security posture by adopting multiple forms of authentication, including password-less authentication methods which provide an enhanced user experience while being more secure than traditional username/password methods.

[Keycloak](https://www.keycloak.org/) has become a popular open source platform for identity management and securing application access. It provides authentication capabilities and allows for customizations to extend them. IBM Security Verify is a fully enabled Identity as a Service (IDaaS) offering, providing access, governance, analytics, and out of the box support for common identity standards such as SAML, OIDC, and OAuth along with other authentication flows.

To help organizations that are seeking more secure methods of application authentication without compromising user experience, IBM Security Verify can now be extended into Keycloak environments. The IBM Security Verify authenticator extensions for Keycloak are first and second factor authenticators that extend Keycloak’s capabilities without disrupting or changing application code. The authenticator extensions support various methods such as One-time-passcode, QR code, Push notifications, and FIDO2.

IBM Security Verify also allows organizations to gain a deeper understanding of authentication events with analytics, dashboarding, and authentication event details. These data views permit admins and application owners to gain more insights into how applications are being used.

This guide describes in detail all supported usages of the authenticators, including administration, registration, user login procedures, and customizations.

# Getting Started

The IBM Security Verify authenticator extensions consist of a number of plugins that allow the Keycloak administrator to enable authentication methods that leverage an ID-less and password-less experience. The extensions are open source and available on IBM Security’s public [GitHub Repository](https://github.com/IBM-Security/cloud-identity-keycloak-integration). This User Guide outlines the requirements and procedures for customizing and building the extensions, as well as the steps for deploying JAR files to a Keycloak or RedHat SSO instance. Please refer to <Authentication Flow Setup> for the basics on how to create and configure each flow.

## Software/Hardware Requirements

* Keycloak Version 10.0.1 or RedHat SSO Version 7.4
* IBM Security Verify authenticator extensions JAR <LINK TO downloadable JAR files>
* [IBM Security Verify](https://www.ibm.com/account/reg/signup?formid=urx-44536)
* [IBM Verify Mobile Application](#_IBM_Verify_Mobile)
* [FIDO2 device](#_FIDO2_Device_Support)

## Installation

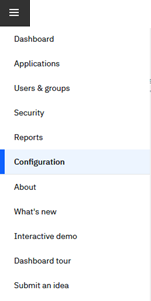
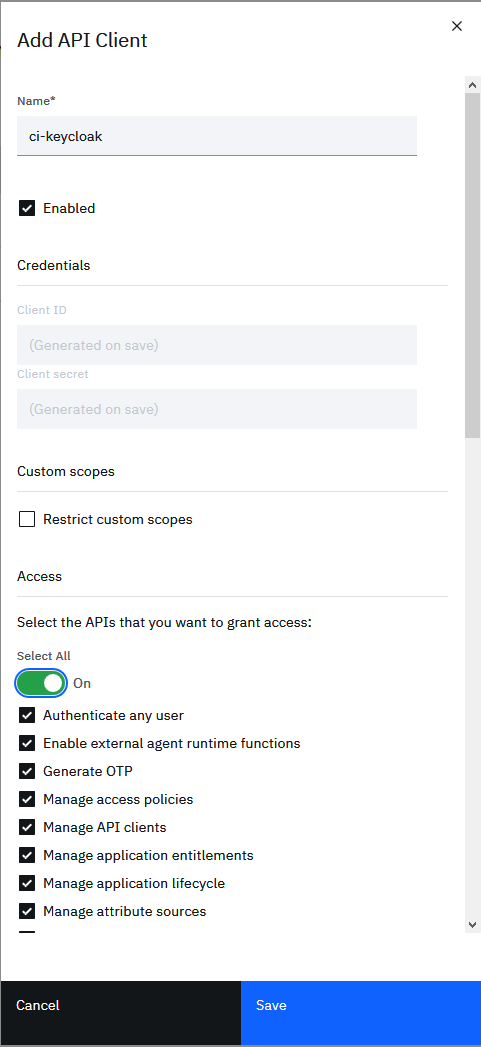
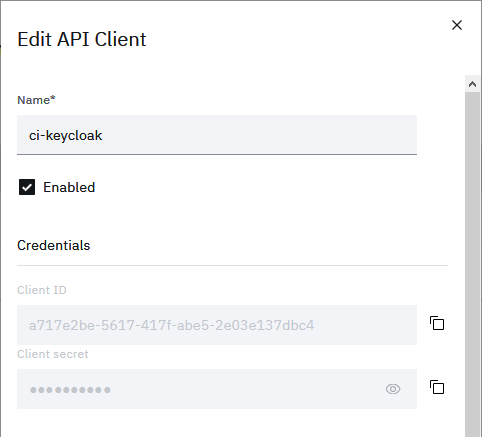
Download and place the IBMSecurityVerifyAuthenticators-1.0.0.jar into the Keycloak or RedHat instance under <installation\_dir>/standalone/deployments. The JAR should be automatically detected and loaded.

# Server Administration

The following sections describe setting up Authentication Flows for select IBM Security Verify Authenticator extensions.

## Creating an IBM Security Verify API Client

IBM Security Verify authenticator extensions for Keycloak utilize IBM Security Verify’s public APIs to register and authenticate users. They require an API Client to be configured.

1. Log in as the Admin to the IBM Security Verify instance
2. Navigate to the Configuration page using the hamburger menu  
     
   
3. Select Add an API Client  
   
4. Name the API Client, grant access to all APIs, then save  
   
5. Edit the API Client that was created  
   
6. Copy the Client ID and secret for use in Authentication Flow set up in Keycloak/RedHat SSO  
   

## IBM Verify Mobile Application

Push Notification, QR Code, and TOTP authentication require an application to perform device registration and authentication. IBM provides the IBM Verify Mobile Application (iOS & Android) that can be leveraged for these authentication scenarios. Alternatively, users can leverage the [IBM Verify SDK](https://www.ibm.com/blogs/security-identity-access/getting-started-with-the-ibm-verify-sdk/) to integrate these capabilities into an existing application.

The IBM Verify Mobile Application adds an extra layer of security to your online services. Two-step verification helps protect your accounts from the bad guys, even if they steal your password.

With IBM Verify, you can confirm your identity with a simple yes or no, your fingerprint or face, or a secure one-time password right from your registered mobile device.

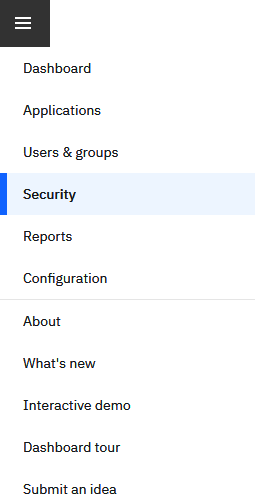
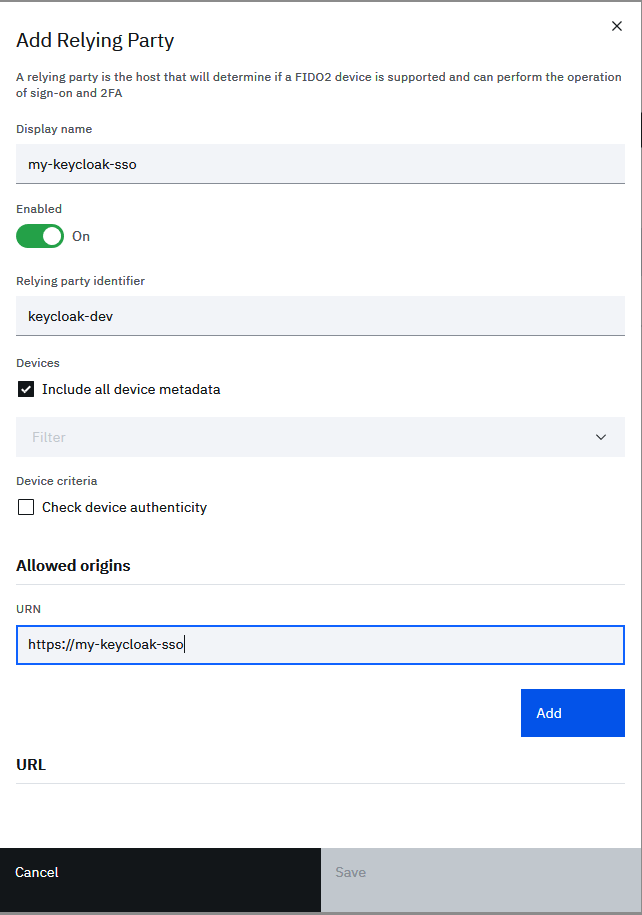
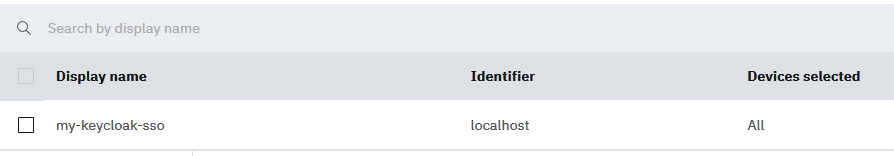
For registering a new device and un-registering an old device for use with Keycloak, please refer to [Account Management](#_Account_Management)

## FIDO2 Device Support

Detailed information on device support and protocols can be found on the [Fido Alliance](https://fidoalliance.org/fido2/) website.

## FIDO2 Relying Party Setup

The relying party uses APIs to authenticate FIDO devices through IBM Security Verify. The following instructions help you set up a whitelist of allowed domains.

1. Log in as the Admin to the IBM Security Verify instance
2. Navigate to the Security page using the hamburger menu  
   
3. Add a relying party  
   
4. Enter information about your Keycloak/RedHat SSO instance, then save  
   
5. Your Keycloak/RedHat SSO is now set up as a relying party  
   

## Authentication Flow Setup

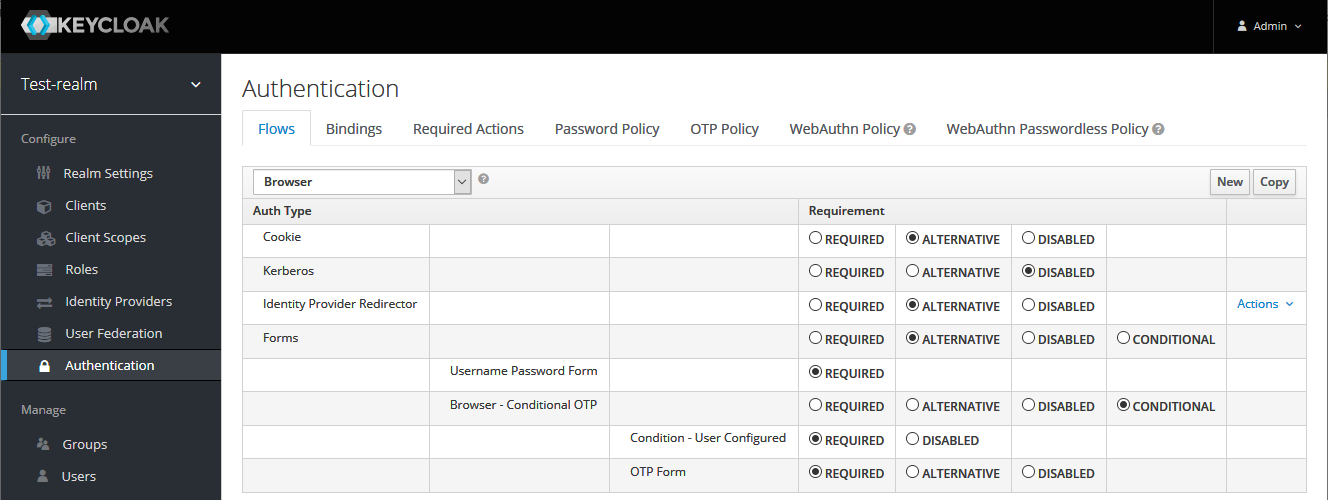
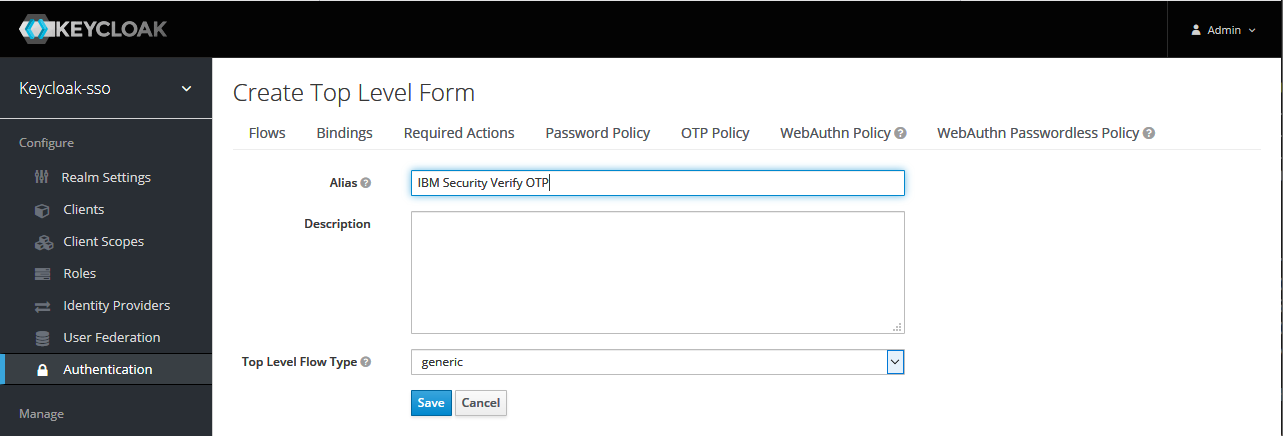
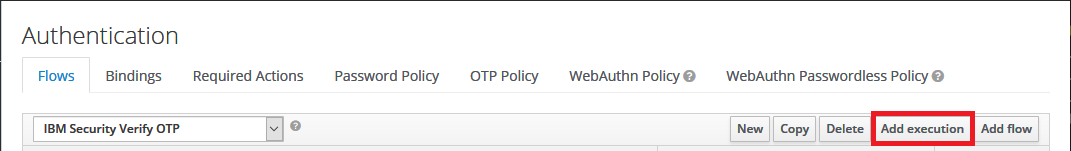
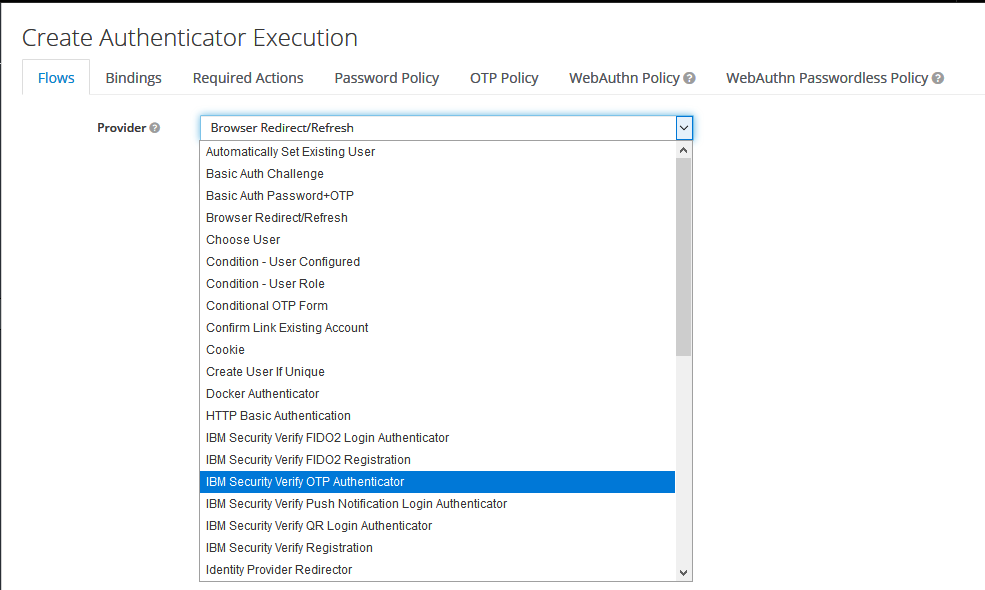
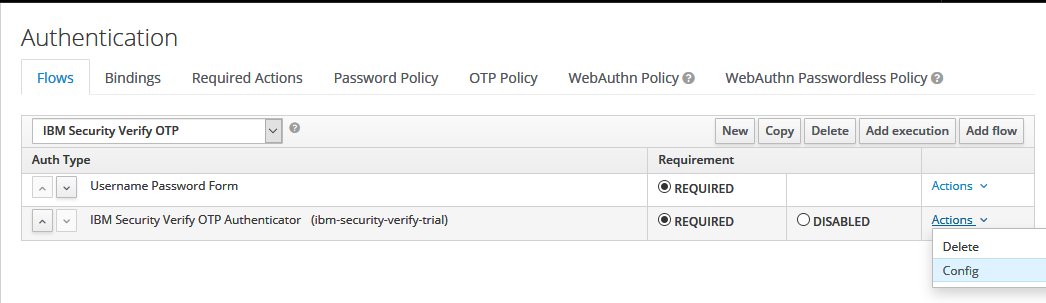
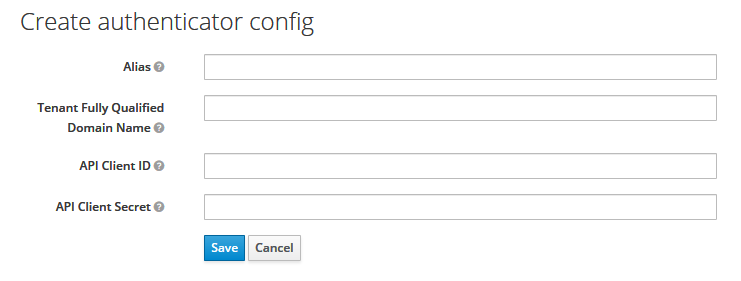
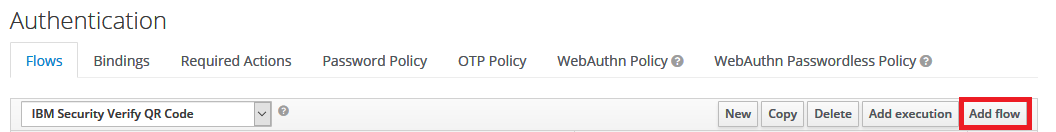
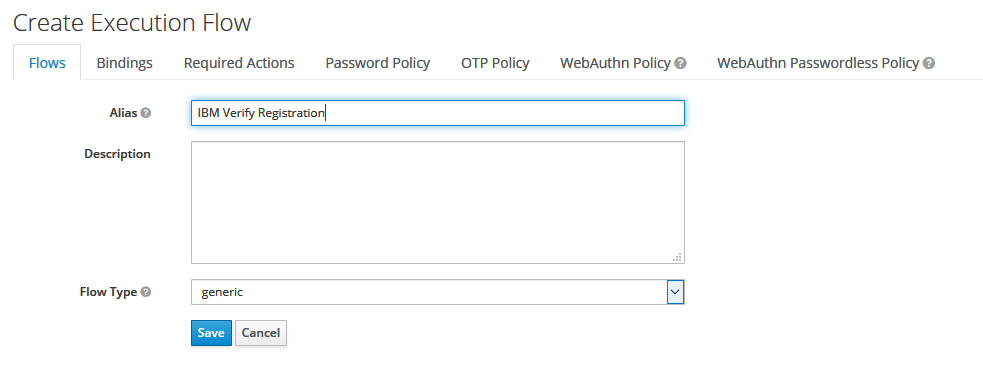
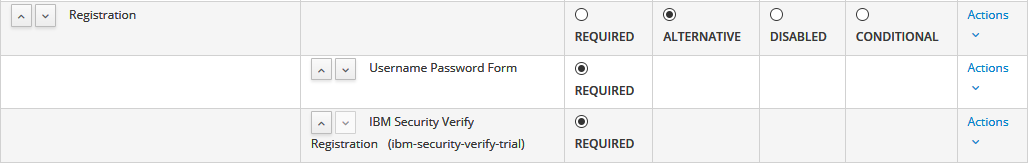
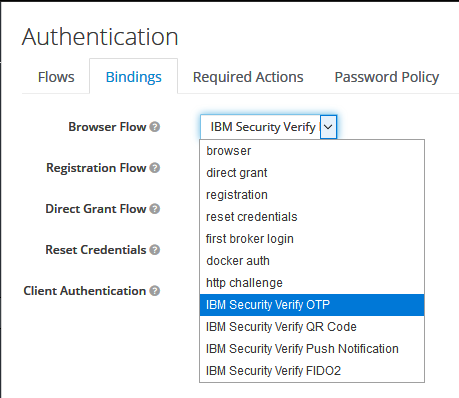
IBM Security Verify authenticator extensions for Keycloak work to extend existing username and password authentication for those looking to add a second factor of authentication. Additionally, they can replace the traditional method with single factor password-less authentication. Both methods can be configured through Keycloak’s Authentication component.

The authentication flow when enabling IBM Security Verify authenticator extensions can be divided into three components:

* **Authenticator** - The authenticator is the component that authenticates the end user via a given method.
* **Registration** - Some authenticators require a registration step before using the authenticator. The registration step will register the end user’s device with IBM Security Verify and enable it to make use of the provided authentication method.
* **First or Second Factor** - Some authenticators can be used as either first or second factors of authentication while others are strictly for second factor authentication. The authentication flow setup will be different in each case.

### Creating and Enabling an Authentication Flow in Keycloak/RedHat SSO

The Administrator can set up an Authentication Flow for each supported authentication method.

1. In the Administration Console, select Authentication, then the Flow tab  
   
2. Select New to create a new top-level flow  
   
3. Proceed to Add execution  
   
4. Select an Authenticator to add to the flow  
   
5. Configure the Authenticator with the IBM Security Verify API Client information from [Creating a IBM Security Verify API Client](#_Creating_a_Cloud)  
     
     
   
6. For ID-less / Password-less scenarios, it is often required to group flows into a parent flow. To add a parent flow, select Add flow and create a generic flow.  
     
     
   
7. To add Authenticators under this flow, select Actions, then Add execution  
   
8. The authenticators you created can be enabled by selecting one from Browser Flow under the Bindings tab  
   

### One-time Passcode

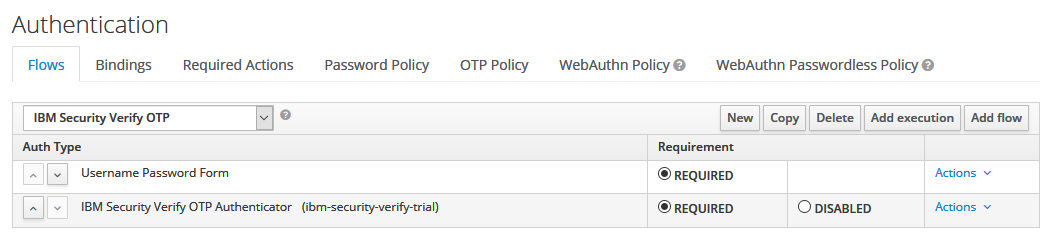
The IBM Security OTP Login Authenticator is a second factor authentication method that sends a one-time passcode to the end user’s email or via SMS. The passcode must be valid for the authentication to succeed.

The user must have a valid email to which the one-time passcode will be sent.

To register a phone number, the attribute “phone.number” must be added to the User’s attribute in the following form including the country code: “+17141234567”

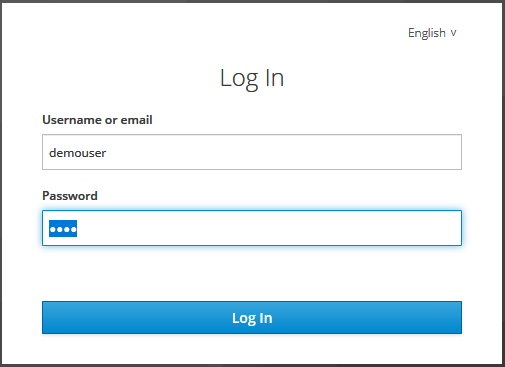
The following Authentication Flow setup is required for One-time Passcode authentication:

* Username Password Form
* IBM Security Verify OTP Authenticator

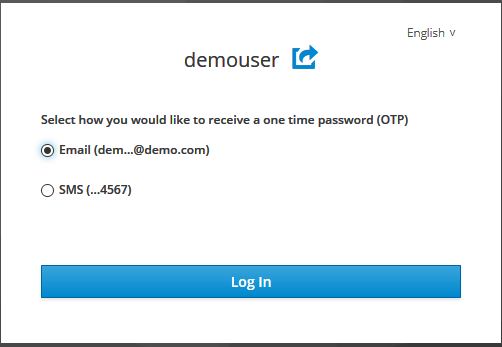


The end user log in experience will include:

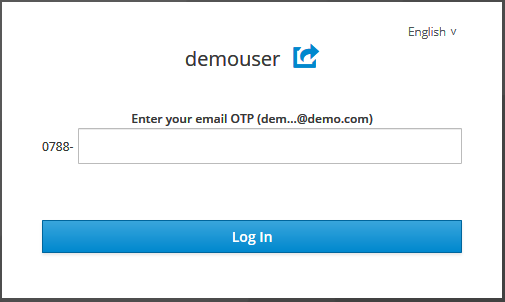
* Username Password authentication to Keycloak system



* OTP delivery method selection (if “phone.number” user attribute is configured)



* OTP validation



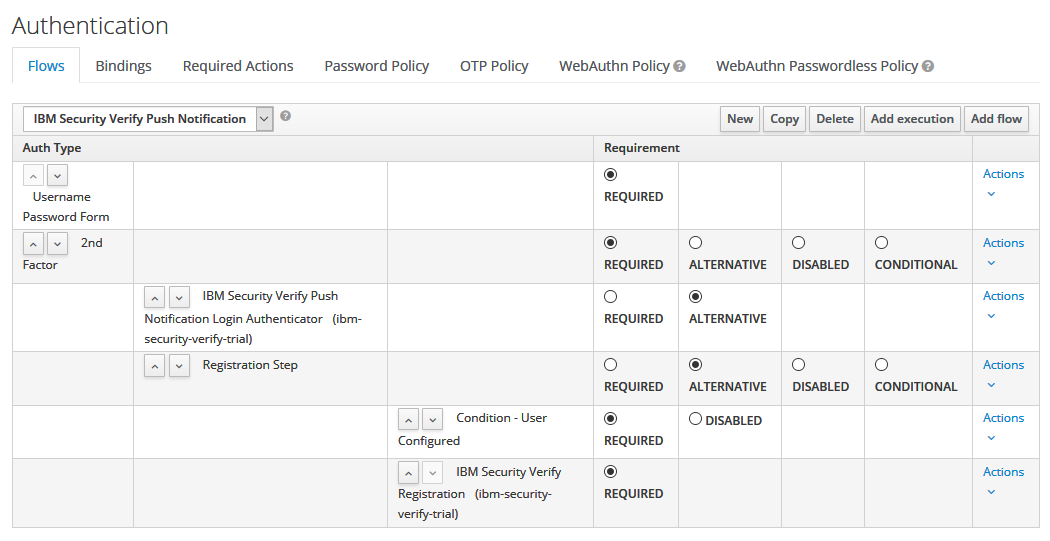
### Push Notification

The IBM Security Verify Push Notification Login Authenticator is a second factor authentication method that sends a push notification to the end user’s [IBM Verify Mobile Application](#_IBM_Verify_Mobile). The push notification must be acknowledged by either user presence or device biometric integration for the user to be authenticated.

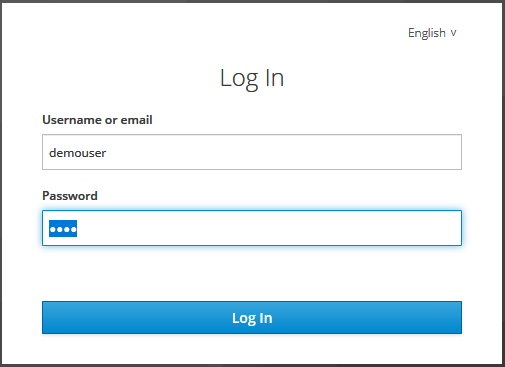
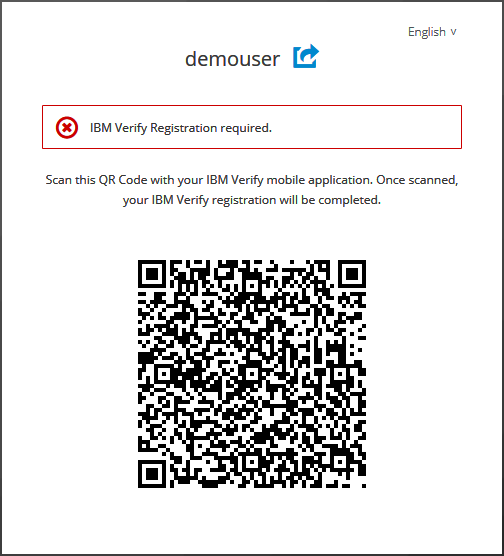
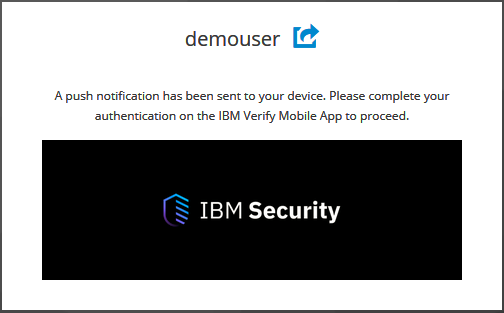
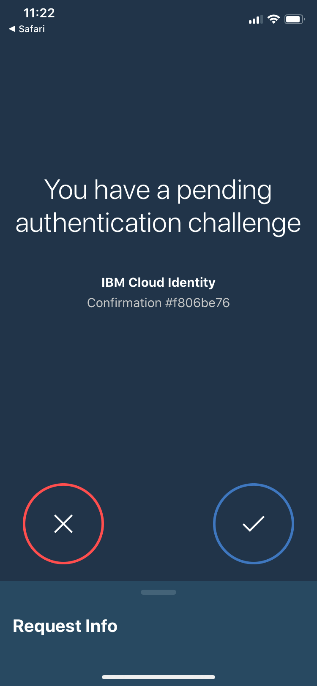
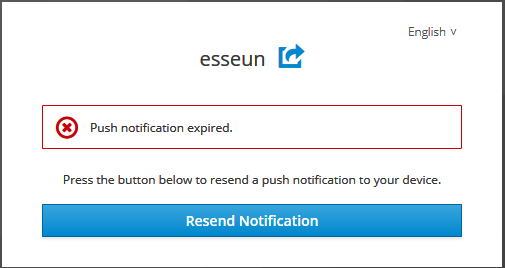
For registering a new device and un-registering an old device, please refer to [Account Management](#_Account_Management).

The following Authentication Flow setup is required for Push Notification authentication:

* Username Password Form
* Generic Flow (2nd Factor)
  + IBM Security Verify Push Notification Login Authenticator
  + Generic Flow (Registration)
    - Condition – User Configured
    - IBM Verify Registration



The end user log in experience will include:

* Username Password Form  
  
* Registration with IBM Verify mobile application (for first time users)  
  
* Push Notification acknowledgement  
    
    
  
* Push Notification expiration with an option to resend (set to 2 minutes by default)  
  

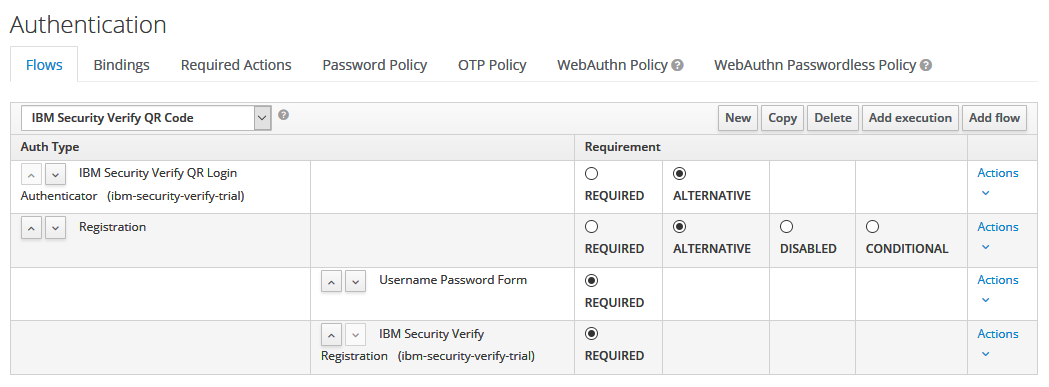
### QR Code

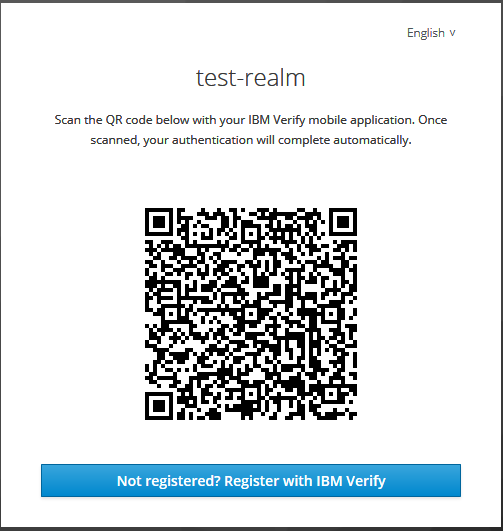
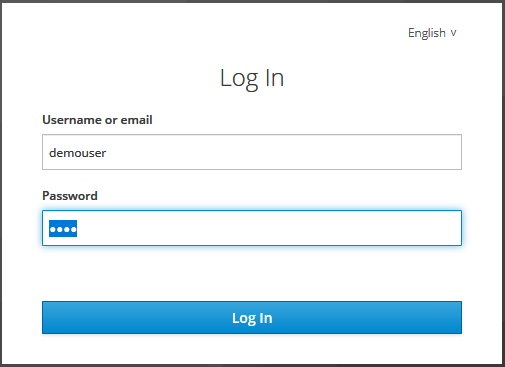
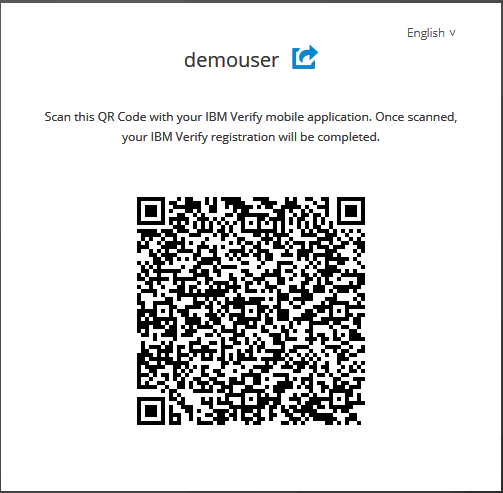
The IBM Security Verify QRCode Login Authenticator is an ID-less authentication method that authenticates the user by scanning a QR Code with the [IBM Verify Mobile Application](#_IBM_Verify_Mobile).

For registering a new device and un-registering an old device for use with Keycloak or RedHat SSO, please refer to [Account Management](#_Account_Management).

The following Authentication Flow setup is required for QR Code authentication:

* IBM Security Verify QR Code Login Authenticator
* Generic Flow (Registration)
  + Username Password Form
  + IBM Verify Registration

The end user log in experience will include:

* ID-less authentication by scanning the QR Code with your *already-registered* IBM Verify mobile application  
  
* OR registration with IBM Verify mobile application for first time users  
    
    
  

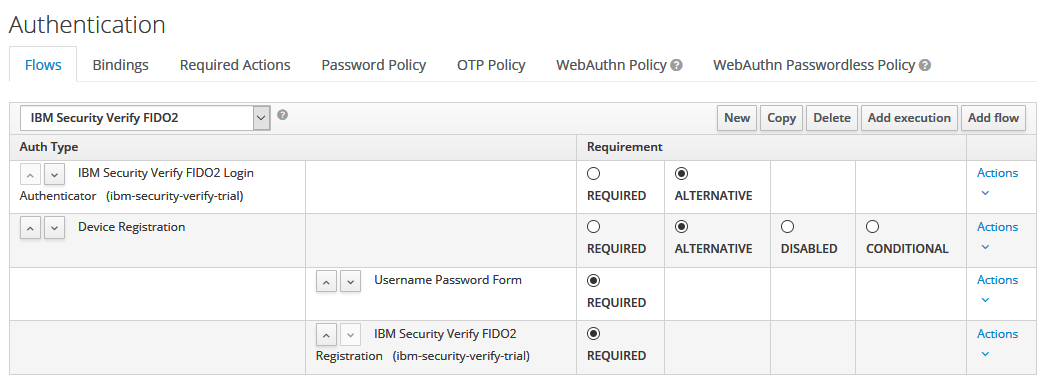
### FIDO2

The IBM Security Verify FIDO2 Login Authenticator is an ID-less, FIDO2 based authentication method that authenticates the using a registered FIDO2 device. Please refer to [FIDO2 Device Support](#_FIDO2_Device_Support) for more details. The user is authenticated entering the FIDO2 device pin and interacting with the device’s capacitive touch.

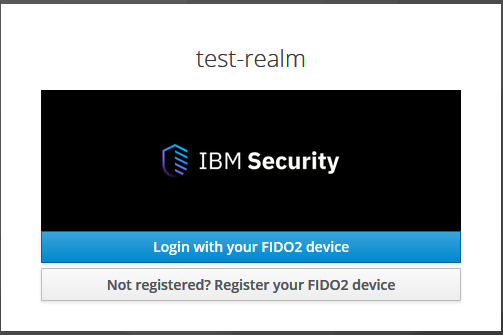
For registering a new device and un-registering an old device for use with Keycloak or RedHat SSO, please refer to [Account Management](#_Account_Management).

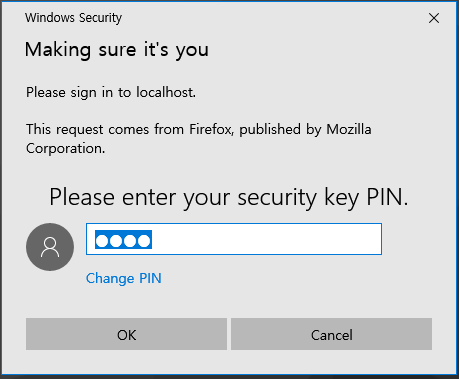
The following Authentication Flow setup is required for FIDO2 authentication:

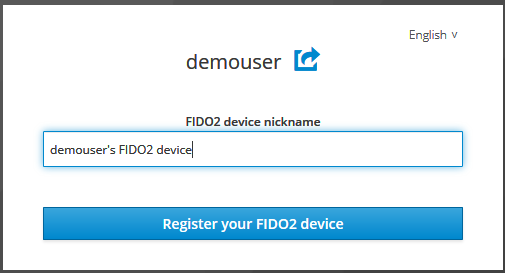
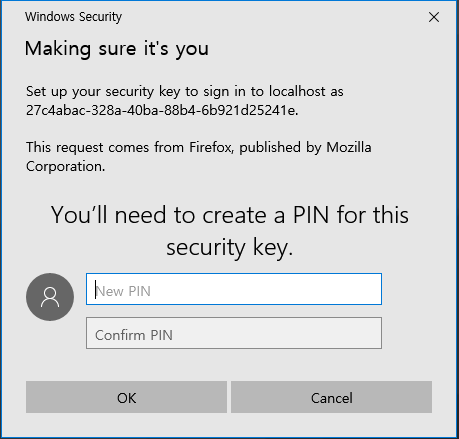
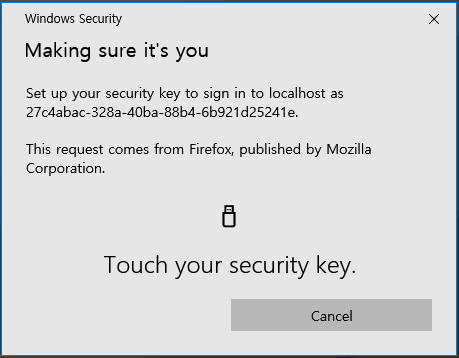
* IBM Security Verify FIDO2 Login Authenticator
* Generic Flow (Registration)
  + Username Password Form
  + FIDO2 Registration



The end user log in experience will include:

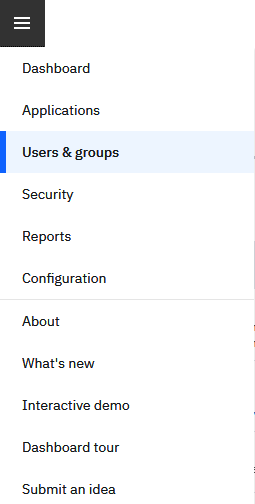
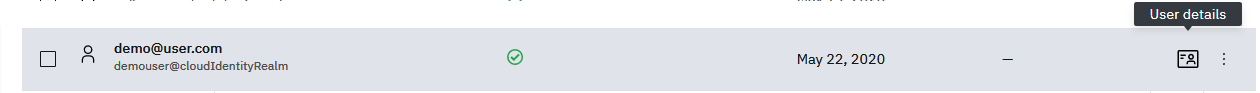
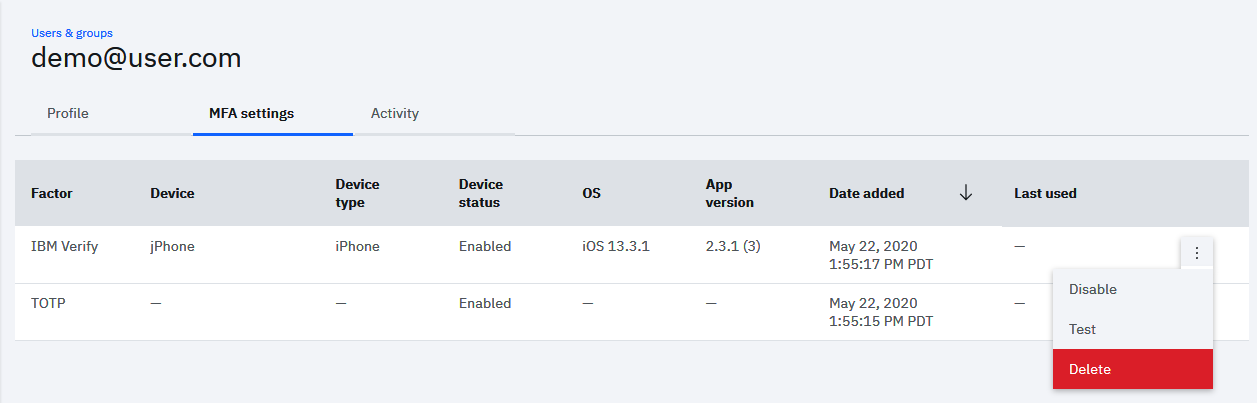
* ID-less authentication by inserting your *already-registered* FIDO2 device  
    
    
    
  Proceed to registering your FIDO2 device if the following message appears  
  

Otherwise, enter your PIN for your registered FIDO2 device to log in  


* OR registration of your FIDO2 device for first time users  
    
    
    
  

## Account Management

A change in a user’s device usually requires a deregistration and reregistration with the user’s IBM Security Verify mobile application or FIDO2 device. The following steps outline how the IBM Security Verify administrator can reset a user’s MFA settings to allow for re-registration.

1. Log in as the Admin to the IBM Security Verify instance
2. Navigate to Users & groups  
   
3. Select the user’s Details  
   
4. Under the MFA Settings tab, delete the authenticator you wish to de-register (either IBM Verify or FIDO)  
   
5. Delete “IBM Verify” or “FIDO” from list
6. FIDO devices can be reset using a FIDO device manager (such as [Yubikey Manager](https://www.yubico.com/products/services-software/download/yubikey-manager/))
7. The user will be prompted to register the new device on the next log in.

# IBM Security Verify: Dashboard and Analytics

Within IBM Security Verify’s administration dashboard organizations can get more visibility into how users are access and interacting with applications.

## Dashboard

Within the admin dashboard, admins get a view into authentication activity that can be filtered by time period, geography, and login type (pass/fail) to gain more insight and take proactive actions. The dashboard also provides a map view to help you see where users are accessing applications from.

A screenshot of a social media post

Description automatically generated

## Authentication Activity

Organizations can also drill down to get authentication activity for an application with detailed granularity by user with corresponding details such as authentication type, location IP, and more.

A screenshot of a social media post

Description automatically generated

These are just a few capabilities that provide organizations visibility into how users are interacting with applications.

# Sample Keycloak Demo Experience

The [IBM-Airways sample application](https://github.com/jason-choi1/ibm-airways-keycloak-sso) demonstrates a consumer log in experience with Keycloak SSO and IBM Security Verify Authenticators. More information on deploying and customizing the application can be found in the public repository.

# Known Issues

Please refer to the [Issues](https://github.com/IBM-Security/verify-keycloak-integration/issues) page on the GitHub repository.

# FAQ

1. javax.net.ssl.SSLException: Received fatal alert: protocol\_version error when executing authenticators

TLS v1.2 is required for Keycloak/RedHat SSO. When running instances with IBM JDK 1.8, set the correct TLS version by passing the following JAVA\_OPTS to your server instance configuration (e.g. standalone.xml):

JAVA\_OPTS="$JAVA\_OPTS -Dcom.ibm.jsse2.overrideDefaultTLS=true -Dcom.ibm.jsse2.overrideDefaultProtocol=TLSv12

# Releases

## v1.0

Initial GA release.

### Supported Versions

Keycloak 10.0.1  
RedHat SSO 7.4