

Start: Launching the Test Drive and Accessing EJBCA and Keyfactor Command

Launching the Keyfactor Test Drive Instance

A Test Drive can be started from the Azure Marketplace: [Keyfactor Command](#). After Test Drive provisioning has started, the screen will display the Test Drive instance URL, username, and password used to access all Keyfactor resources on the instance. (Figure 1) Please note this login information securely, as it will be needed later. The values are generated specifically for your Test Drive instance and will expire in 30 days.

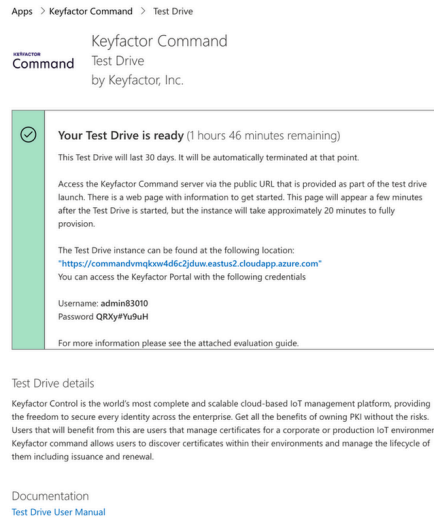


Figure 1. Keyfactor Command Test Drive Information

The instance will take approximately 30 minutes to complete deployment. Early in the provisioning process, a temporary provisioning information page with links to Keyfactor Command, EJBCA, and documentation will be available (Figure 2). This page can be accessed over HTTP or HTTPS. Please use this link to reference the various parts of the Keyfactor Test Drive instance. The values here will be specific to the Test Drive launched for you.

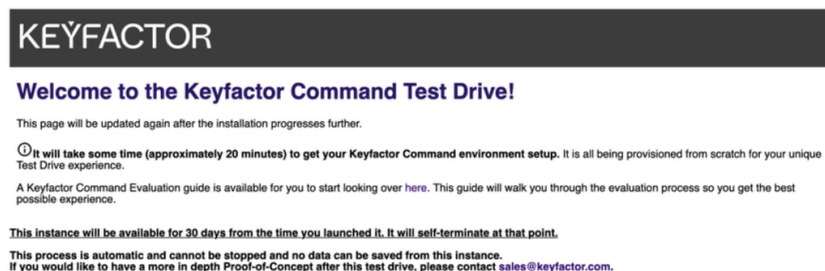


Figure 2. Test Drive start page while deploying

A new and final start page will appear once the provisioning process is complete, notifying you the process is finished with more information such as a documentation download link, Keyfactor Test Drive component URLs, and Test Drive Universal Orchestrator bundle (Figure 3).

Note: The Start Page runs on port 80 and 443. Keyfactor Command for IoT portal is running at /KeyfactorPortal on port 443. EJBCA is running on HTTP 8080 and HTTPS 8443.

KEYFACTOR

Welcome to the Keyfactor Command Test Drive!

This page will guide you through some configuration to get you started.

🕒 Your Keyfactor Command environment setup is complete!

A Keyfactor Command Evaluation guide is available for you to start looking over here. This guide will walk you through the evaluation process so you get the best possible experience.

The following is an overview of the components on this Test Drive:

- Keyfactor EJBCA: Spin up new certificate authorities (CAs) and enable fast certificate enrollment and issuance to authenticate connected devices, workloads, and users.
- Keyfactor Command: This platform provides initial device vetting, registration automation, and device provisioning. Once a device identity certificate is under management, it can be set to automatically reenroll based on customizable criteria.
- Keycloak: Open Source Identity and Access Management. Keycloak provides user federation, strong authentication, user management, fine-grained authorization, and more.

Each of the items above are available on the following URLs/ports:

Figure 3. Example of a completed Test Drive Start Page

Once the Test Drive instance configures itself, click the EJBCA link on the start page. You will be taken to the **EJBCA Web** page (Figure 4). A warning page will appear. To continue in Firefox, click on **Advanced**. This will trigger the display of additional information about the certificate, including the error code SEC_ERROR_UNKNOWN_ISSUER. The error code will resolve after you install the Management CA from EJBCA. Click **Accept the Risk and Continue**.

Click the link on the web page for the **EJBCA Registration Authority Web**.

KEYFACTOR

EJBCA Administration Web
EJBCA Administration Web Interface of this node allowing for configuration of the PKI and its users.

EJBCA Registration Authority Web
Registration Authority (RA) interface for administrative functions that register entities in the PKI. The RA is trusted to identify and authenticate entities according to the CAs policy.

EJBCA Documentation Site
EJBCA Enterprise Documentation site containing detailed information on all aspects of EJBCA

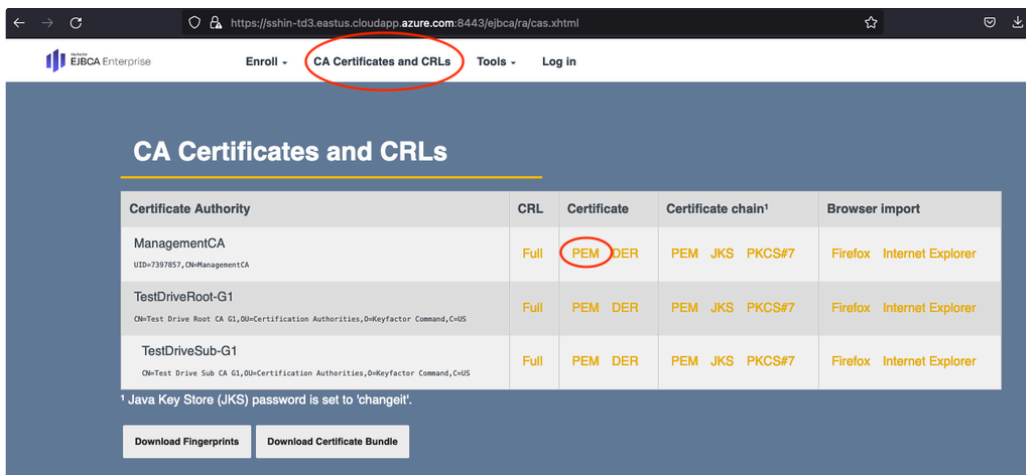
Keyfactor Website
Keyfactor Website for additional information on Keyfactor, its people and its products.

Keyfactor EJBCA Enterprise

Figure 4. EJBCA Landing Page

Adding the ManagementCA Certificate

Proceed to the **EJBCA Registration Authority Web** to add the ManagementCA certificate to your browser. Ignore the Enrollment with Enrollment code page and click the **CA Certificates and CRLs** tab at the top of the page (Figure 5).



Click the **PEM** link for the ManagementCA certificate under the Certificate column and save it to your computer. Access the browser's certificate store and add the ManagementCA certificate to it. In Firefox, you can type `about:preferences` in the address bar, select the Preferences Menu, and go to **Settings**. Click the **Privacy and Security** menu option on the left and then scroll down to the **View Certificates** button. *If using a browser other than Firefox, you must import the CA certificate into your local systems keystore and restart your browser. Firefox is recommended to keep things simple since it has its own keystore.*

In the View Certificates dialog, click the **Authorities** tab and click **Import**. Navigate to the location where the downloaded ManagementCA PEM file was saved and click Open. This will import the ManagementCA cert into the Firefox trust store. A dialog box will appear; select options to trust this CA to identify websites and then click **OK** (Figure 6). You can now view the ManagementCA certificate under **Authorities** (Figure 7).

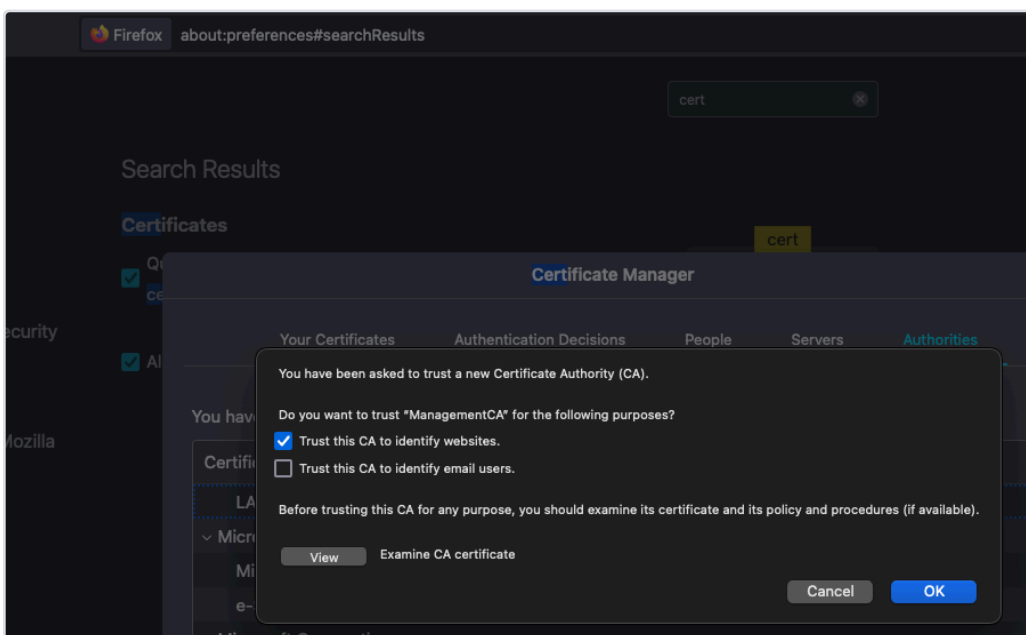


Figure 6. Dialog box for Importing ManagementCA certificate to Firefox

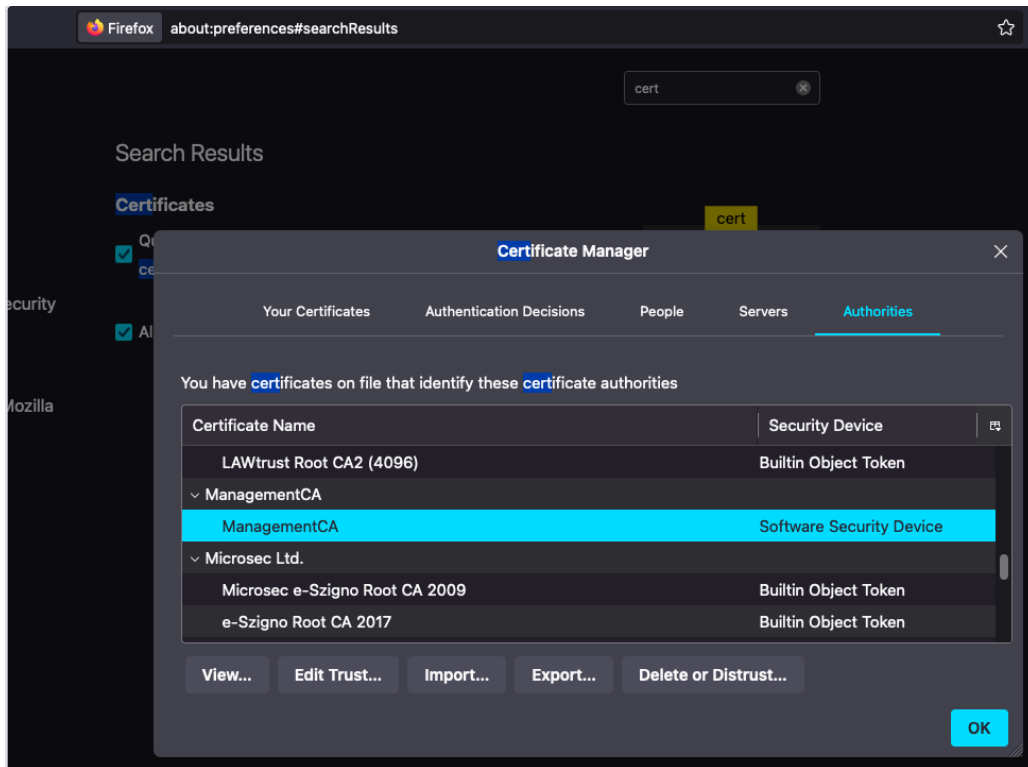


Figure 7. Management CA added as a Certificate Authority

Next, navigate to the Servers tab and look for entries linked to the Test Drive instance (Figure 8). These exceptions were generated by Firefox when 'Accept the Risk and Continue' was selected previously. Delete these entries now that we have the CA certificate of the Trusted Root added.

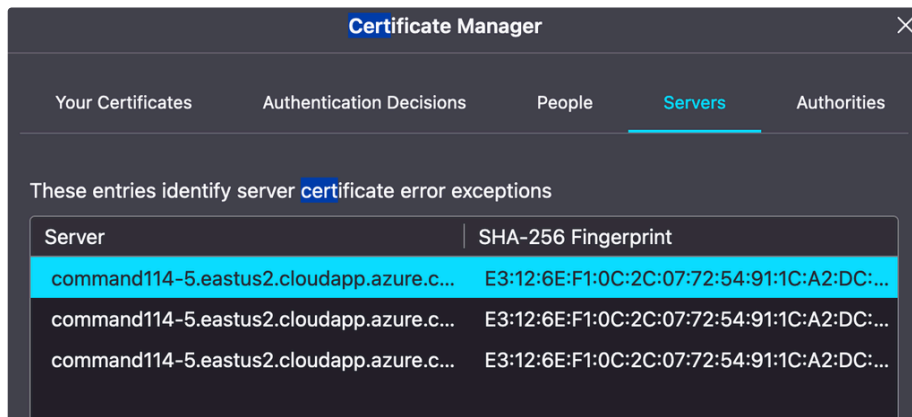


Figure 8. Removing Certificate Exceptions

Refresh the EJBCA page. A verified lock icon will appear in the browser URL bar. If the lock icon does not appear, restart the browser. Try refreshing the page if the lock still does not show correctly after adding the certificates.

Note: Once the Test Drive has ended, you may delete the Test Drive certificates if desired.

Accessing EJBCA

EJBCA can be accessed by two different methods. OAuth (Open Authorization) leveraging Keycloak or Certificate based access. To access EJBCA via OAuth, proceed to the next section. To access it with a superadmin credential, proceed to the section Downloading the EJBCA Superadmin Certificate.

Accessing EJBCA with OAuth

On the EJBCA start page, click the link to access the EJBCA Administration Web. Once you click that you will be presented with a login page with a link (Figure 9).

Welcome to EJBCA Administration

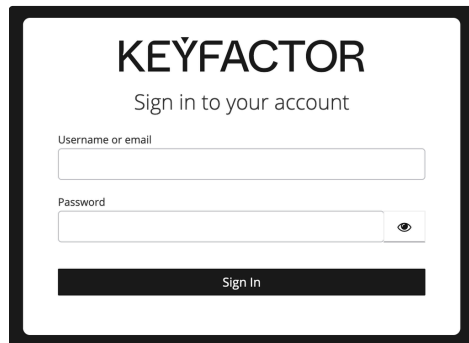
Select a login method to continue

Please select your authentication provider. You may also be able to log in with a client certificate.

[Keycloak](#)

Figure 9. Keycloak OAuth login

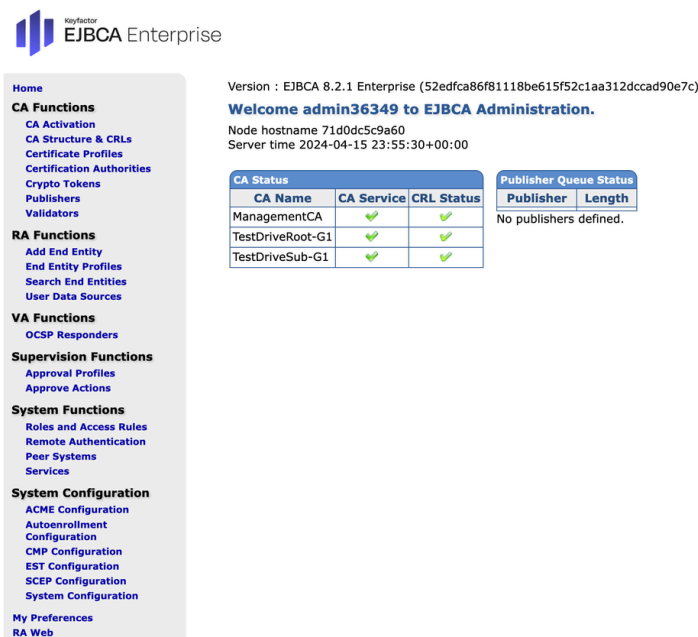
Clicking the Keycloak link will take you to a login screen (Figure 10). Enter the Test Drive credentials on the Azure Test Drive launch page from the Azure Marketplace Test Drive Portal



The image shows a login page for Keyfactor. At the top, it says "KEYFACTOR" in a large, bold font. Below that, it says "Sign in to your account". There are two input fields: "Username or email" and "Password". The password field has a small eye icon to its right. At the bottom of the form, there is a "Sign In" button.

Figure 10. Keycloak login page

Once completed, you will have access to the EJBCA Administration Web interface (Figure 11).



The image shows the EJBCA Administration Web interface. On the left, there is a navigation menu with the following sections:

- Home
- CA Functions
 - CA Activation
 - CA Structure & CRLs
 - Certificate Profiles
 - Certification Authorities
 - Crypto Tokens
 - Publishers
 - Validators
- RA Functions
 - Add End Entity
 - End Entity Profiles
 - Search End Entities
 - User Data Sources
- VA Functions
 - OCSP Responders
- Supervision Functions
 - Approval Profiles
 - Approve Actions
- System Functions
 - Roles and Access Rules
 - Remote Authentication
 - Peer Systems
 - Services
- System Configuration
 - ACME Configuration
 - Autoenrollment Configuration
 - CMF Configuration
 - EST Configuration
 - SCEP Configuration
 - System Configuration
- My Preferences
- RA Web

On the right, the main content area displays the following information:

Version : EJBCA 8.2.1 Enterprise (52edfca86f81118be615f52c1aa312ccad90e7c)
Welcome admin36349 to EJBCA Administration.
Node hostname 71d0dc5c9a60
Server time 2024-04-15 23:55:30+00:00

CA Status			Publisher Queue Status	
CA Name	CA Service	CRL Status	Publisher	Length
ManagementCA	✓	✓	No publishers defined.	
TestDriveRoot-G1	✓	✓		
TestDriveSub-G1	✓	✓		

© 2002–2023. EJBCA® is a registered trademark.

Figure 11. EJBCA Administration Web

Downloading the EJBCA Superadmin Certificate

If you would like to access EJBCA with a the Superadmin credential, return to the **EJBCA Registration Authority Web** page. Here you can download the PKCS12 (P12) file to add to your browser. If you are not directed to the Enrollment with Enrollment code page, click **Enroll** -> **Use Username** to log in and retrieve the **superadmin** credential (Figure 12).

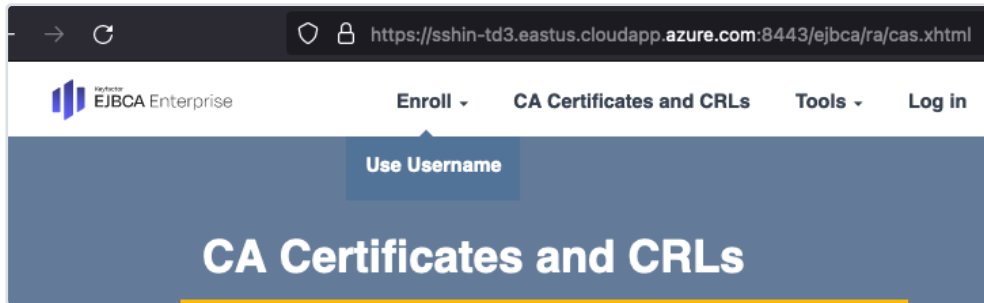


Figure 12. Enroll->Use Username

The username is the Test Drive username and the Enrollment code is the Test Drive password given at provisioning. Click **Check** (Figure 13).

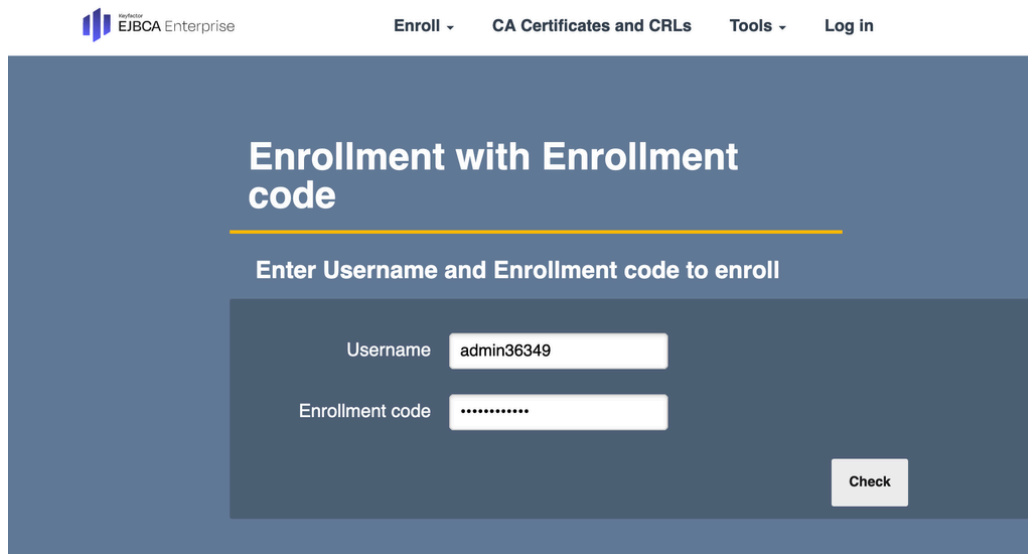
A screenshot of the EJBCA Enterprise web interface showing the 'Enrollment with Enrollment code' page. The page has a dark blue background with white text. The title is 'Enrollment with Enrollment code'. Below the title, it says 'Enter Username and Enrollment code to enroll'. There are two input fields: 'Username' with the value 'admin36349' and 'Enrollment code' with a masked password represented by dots. A 'Check' button is located at the bottom right of the form area.

Figure 13. Enrollment Code

ECDSA-P256 will be selected by default from the **Key Specification** drop-down; click **Download PKCS#12** (Figure 14).

NOTE: This enrollment can only be done once. Ensure you pick a strong enough Key Specification that modern browsers support.

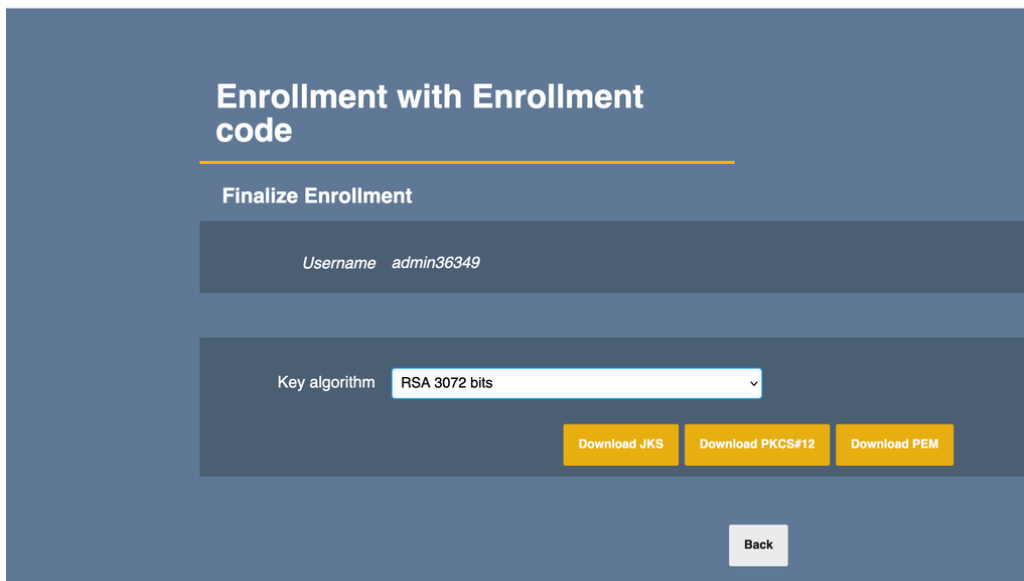


Figure 14. Downloading the superadmin pkcs12 certificate

Save the PKCS#12 (P12) file to your computer. Access the browser's certificate store and add the downloaded P12 keystore. In Firefox, you can type `about:preferences` in the address bar to go to Settings. Click **Privacy and Security**, then scroll down to **View Certificates**. In the dialog that comes up, click the **Your Certificates** tab and click **Import** (Figure 15). Navigate to the location where the SuperAdmin cert downloaded and click **Open**.

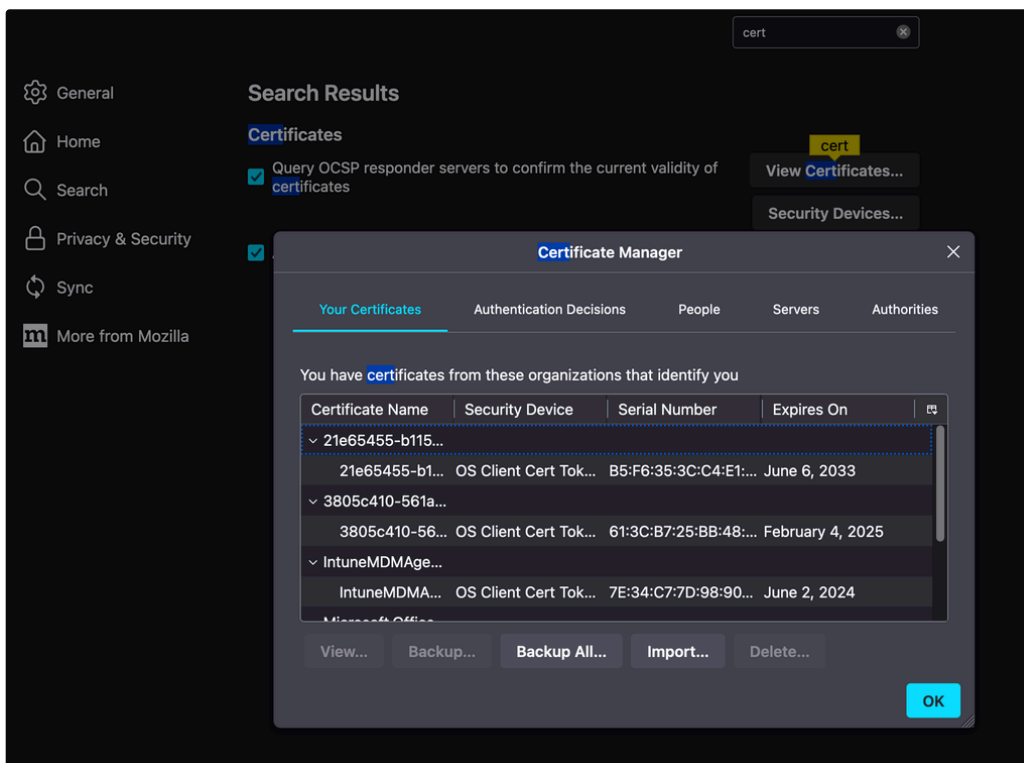


Figure 15. Importing the admin.p12 into FireFox

In the password dialog, type in the same password (enrollment code / Test Drive password), click **Sign in**, then click **OK** (Figure 16).

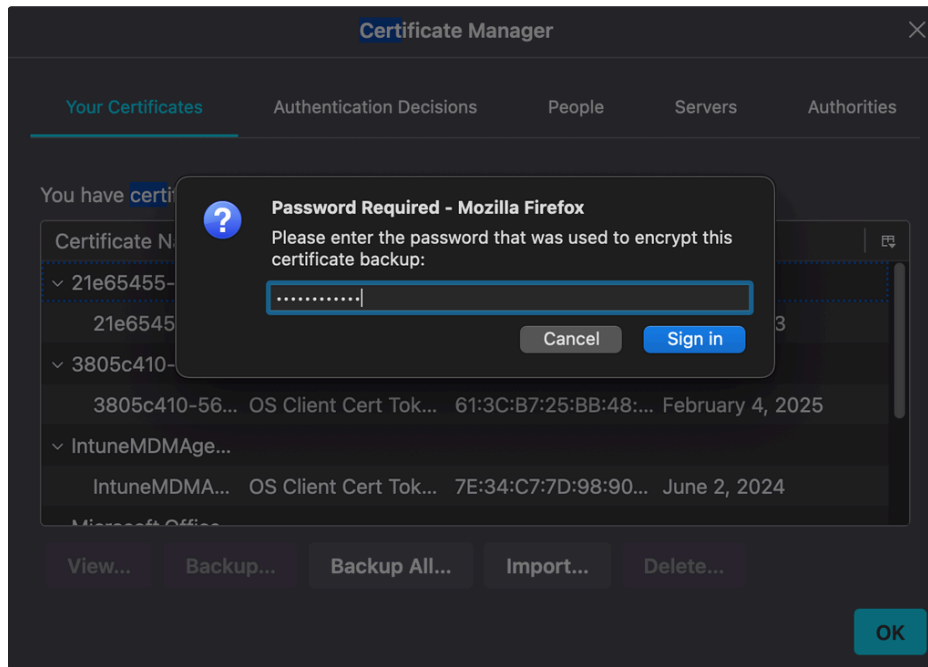


Figure 16. Inputting the admin.p12's password

Return to the EJBCA Enterprise page (Figure 17), **click the EJBCA Administration Web** link to access the EJBCA Administration Web Interface. You should be prompted with a request for your browser to use the imported certificate; click **OK**.

If you are not prompted with the request and instead have an "Authorization Denied" error, please restart your browser or try holding shift while you click refresh.

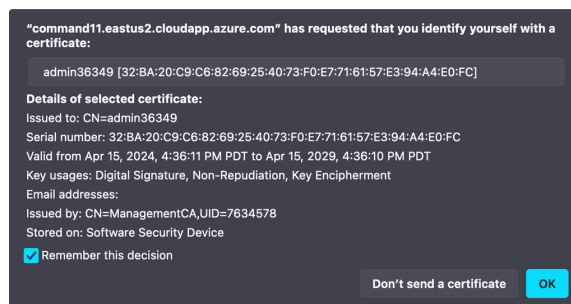


Figure 17. Firefox prompt to login as EJBCA Superadmin

Once completed, you will have access to the EJBCA Administration Web interface (Figure 18).

Home

CA Functions

- CA Activation
- CA Structure & CRLs
- Certificate Profiles
- Certification Authorities
- Crypto Tokens
- Publishers
- Validators

RA Functions

- Add End Entity
- End Entity Profiles
- Search End Entities
- User Data Sources

VA Functions

- OCSP Responders

Supervision Functions

- Approval Profiles
- Approve Actions

System Functions

- Roles and Access Rules
- Remote Authentication
- Peer Systems
- Services

System Configuration

- ACME Configuration
- Autoenrollment Configuration
- CMP Configuration
- EST Configuration
- SCEP Configuration
- System Configuration

My Preferences

RA Web

Version : EJBCA 8.2.1 Enterprise (52edfca86f81118be615f52c1aa312dccad90e7c)

Welcome admin36349 to EJBCA Administration.

Node hostname 71d0dc5c9a60
Server time 2024-04-15 23:55:30+00:00

CA Status		
CA Name	CA Service	CRL Status
ManagementCA	✔	✔
TestDriveRoot-G1	✔	✔
TestDriveSub-G1	✔	✔

Publisher Queue Status	
Publisher	Length
No publishers defined.	

© 2002–2023. EJBCA® is a registered trademark.

Figure 18. EJBCA adminweb

Optional: If you would like more in-depth guidance on configuring EJBCA Enterprise with proper certificate authorities, CRL, OCSP, etc., please refer to this guide: [KF Quick Start Guide](#)

Accessing Keyfactor Command

Click the Keyfactor Portal link on the Test Drive Start Page to log in to the Keyfactor Command Portal (Figure 16). If you did not add the ManagementCA certificate or remove the server exceptions per previous instructions, you will be given two certificate warnings. One of them is for Keycloak and the other will be for Command.

A login dialog will appear. This is the login dialog for Keycloak. Login with the supplied username and password from the Test Drive.

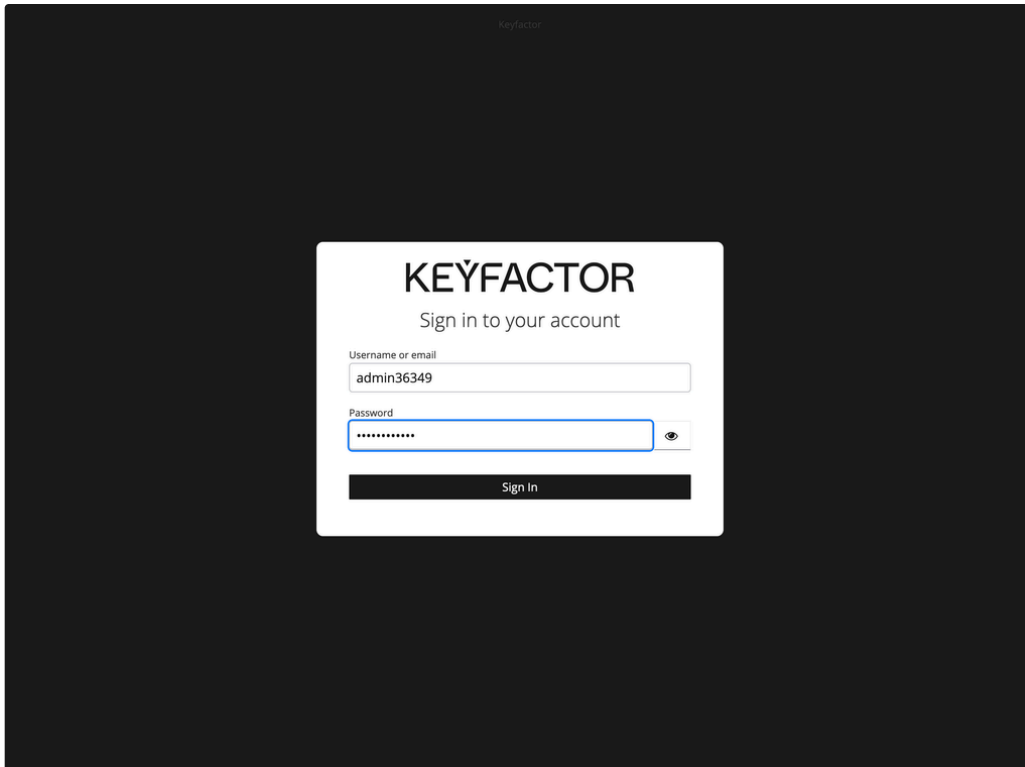


Figure 19. Keycloak Login

Log in using the username and password credentials from the Test Drive provisioning process.

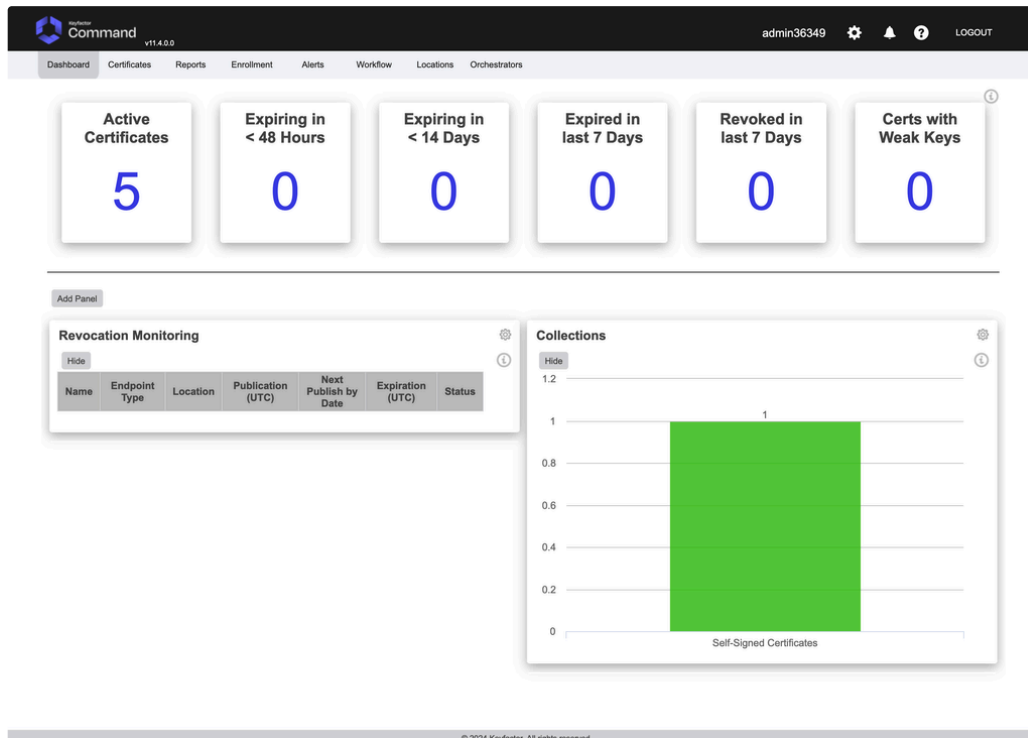


Figure 20. The Keyfactor Command Portal Dashboard

Adding Users to the TestDrive

To add additional users to the Test Drive, start by accessing Keycloak on port 8444 and with the provided Test Drive admin account. Login to the Keycloak admin portal and start by selecting the **Keyfactor Realm** (Figure 21).

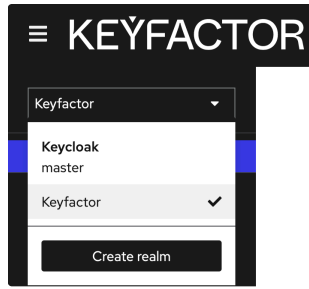


Figure 21. Selecting the Keyfactor Realm

Next select users, then **Add User** (Figure 22).

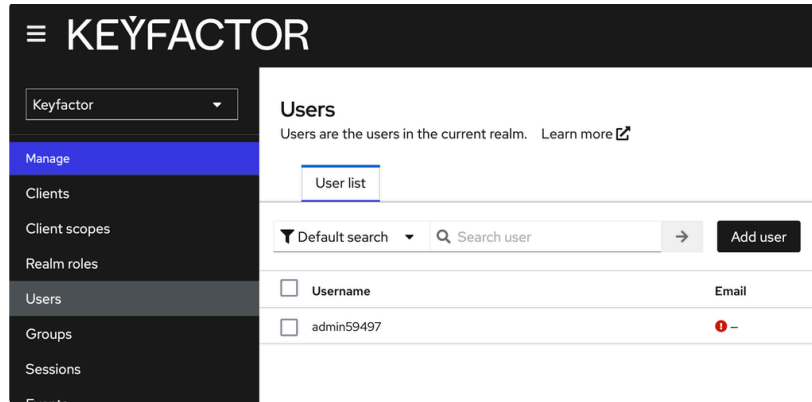


Figure 22. Add User

Enter a username for the new user to access to Test Drive and click **Create** (Figure 23).

General

Username *

Email

First name

Last name

Groups ⓘ

Figure 23. Create User

Make a note of the user ID that is generated. We will use this to create a role in EJBCA (Figure 24) and Command (Figure 30).

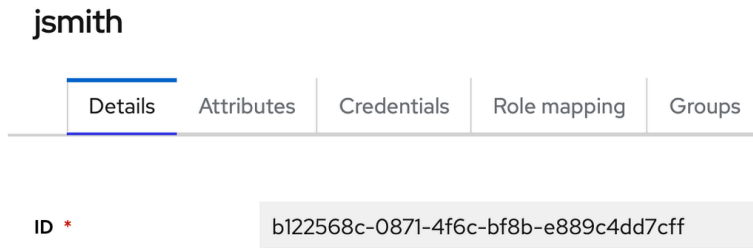


Figure 24. Keycloak User ID

Next, click the **Credentials** tab to set a password. Click Set Password (Figure 25).

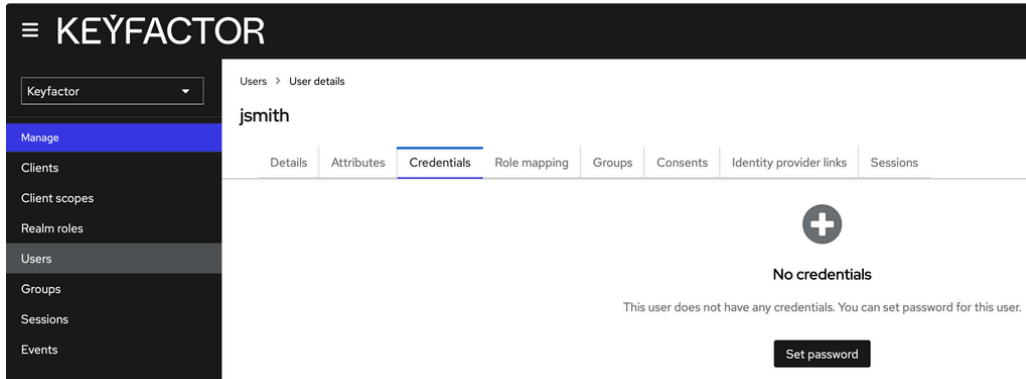


Figure 25. Set Password

Enter the password two times. If you would like the user to set their own password, keep the Temporary password slider on and they will be prompted to change it. Click **Save** (Figure 26) and then **Save Password**.

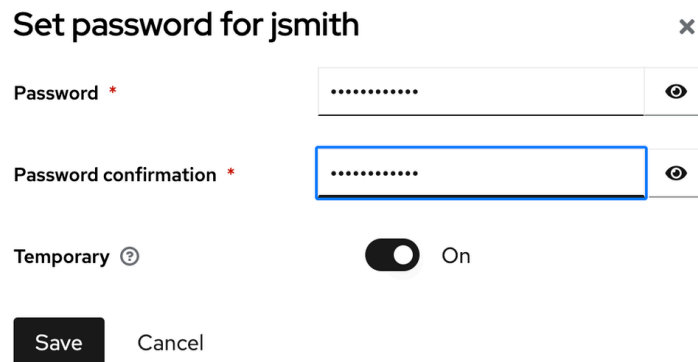


Figure 26. Set Password in Keycloak

Adding Users to EJBCA

With the original TestDrive admin login, access the EJBCA admin screen and select **Roles and Access Rules** (Figure 27).

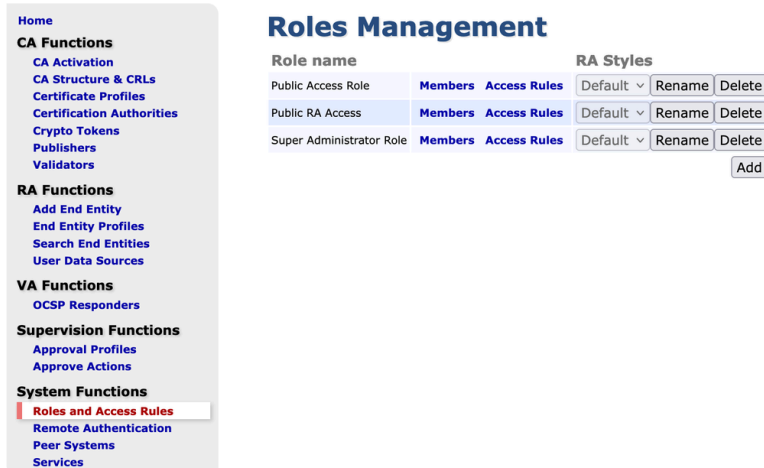


Figure 27. EJBCA Roles and Access Rules

Select the **Members** link of the Super Administrator Role. If desired you can also click **Add** and add a new role for different permissions. For more information on creating EJBCA Roles and Access rules, see the following [EJBCA Tutorials](#) or the [EJBCA Documentation on Roles and Access Rules](#). Select the following criteria for the Role rule:

- **Match With** drop down - Select **“OAuth 2 JWT: Subject (“sub”) claim”**
- **CA** - Leave this set to **“ManagementCA”** (its not used)
- **OAuth Provider** - **“Keycloak”**
- **Match Value** - Paste the User ID from above in Figure 24.
- **Description** - Anything to identify this user. We will use the username in this example **“jsmith”**

Once the user information has been added, click **Add** (Figure 28).

Members [Back to Roles Management](#)
[Edit Access Rules](#)

Role : Super Administrator Role

Match with	CA	OAuth Provider	Match Operator	Match Value	Description	Action
OAuth 2 JWT: Subject ("sub") claim	ManagementCA	Keycloak		71-4f6c-bf8b-e89c4dd7cff	jsmith	Add
CLI: Username	-	-	Equal, case sens.	ejbca		Delete
OAuth 2 JWT: Subject ("sub") claim	-	Keycloak	Equal, case sens.	f1b09d18-89ef-4c9b-92c1-d8e2b902a089	admin12345	Delete
X509: CN, Common name	ManagementCA	-	Equal, case sens.	SuperAdmin		Delete
X509: CN, Common name	ManagementCA	-	Equal, case sens.	admin59497		Delete

Figure 28. Adding role rules to EJBCA

Have the user login with the new username and password at the Test Drive EJBCA URL (for example <https://<TEST DRIVE URL>:8443/ejbca/adminweb>)

⚠ New users should add the Management Certificate as outline above in the section “Adding ManagementCA Certificate” so they don’t get browser warnings.

The user will get the Keyfactor Login screen. Enter the new users username and password. If you left the “Temporary” slider on, they will be prompted to change their password (Figure 29).

Figure 29. Changing Password

Once done, the new user will be logged into the EJBCA Administration web with the new username reflected at the top (Figure 30).

Version : EJBCA 8.2.1 Enterprise (52edfca86f81118be615f52c1aa312dcccad90e7c)

Welcome jsmith to EJBCA Administration.

Node hostname 8d13015396a5
Server time 2024-04-29 23:11:49+00:00

CA Status		
CA Name	CA Service	CRL Status
ManagementCA	✓	✓
TestDriveRoot-G1	✓	✓
TestDriveSub-G1	✓	✓

Publisher Queue Status	
Publisher	Length
No publishers defined.	

Figure 30. New User Logged In

Adding Users to Command

To add a user in Command, add the user via the gear icon near the admin login name (Figure 31) and select **Security Roles and Claims**.

Figure 31. Security Roles & Claims

Select the **Claims** tab and click **ADD**. Fill out the details in the Add Claim dialog (Figure 32). The values that need populating are:

- **Claim Type** - OAuth Subject
- **Claim Value** - User ID that was added as shown in Figure 24 above.
- **Provider** - Command

- **Description** - Value to represent the user. For example "jsmith" in this example.

Click Save.

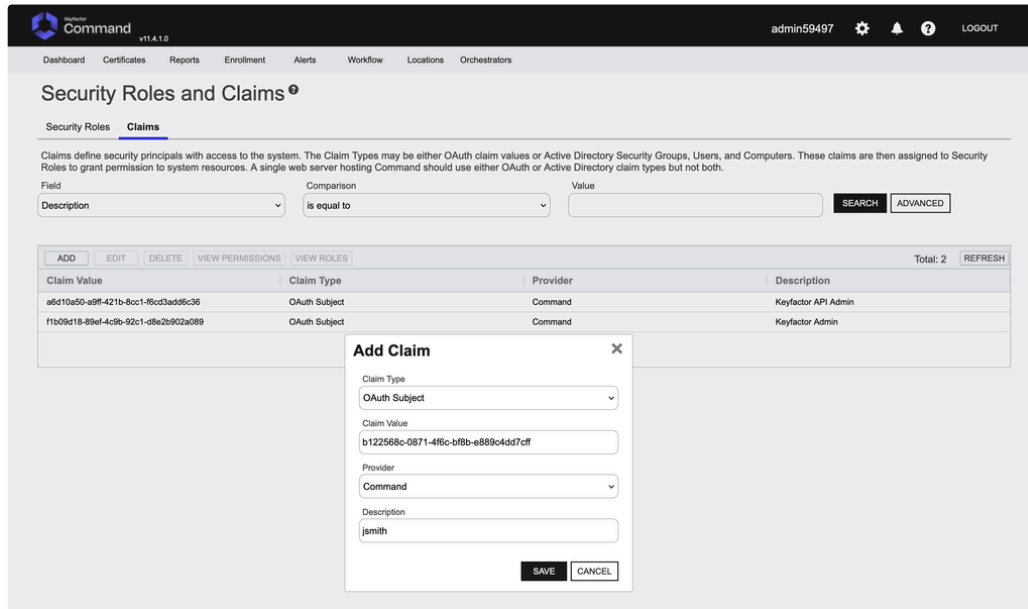


Figure 32. Add Claim

Click the **Security Roles** tab and then click the ADD button (Figure 33).

Security Roles and Claims [?]

Security Roles Claims

Security Roles are used in conjunction with claims to define Containers. Active Directory users, groups, or select OAuth

Field

Name

ADD EDIT DELETE COPY

Figure 33. Add Security Role

Give the new role a name and a description (for example Command Admins). Click the **Global Permissions** tab. Define the role with the permissions you would like to grant. In this example we are going to allow all additional users full access to this test drive for evaluation simplicity. Select the **Select All** option in the drop down and select the **All** checkbox (Figure 34).

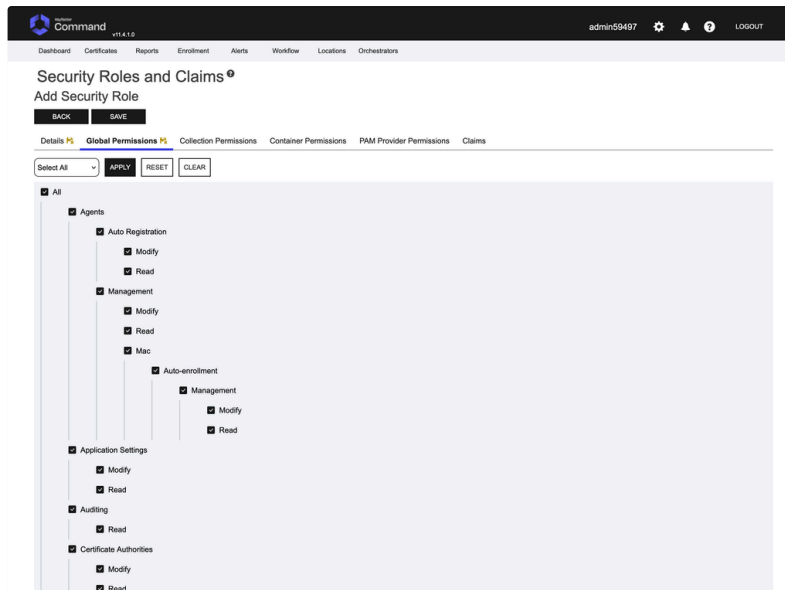


Figure 34. Global Permissions

On the **Claims** tab, select the desired user (jsmith in our example) and click the **Include and Close** button (Figure 35). Click Save.

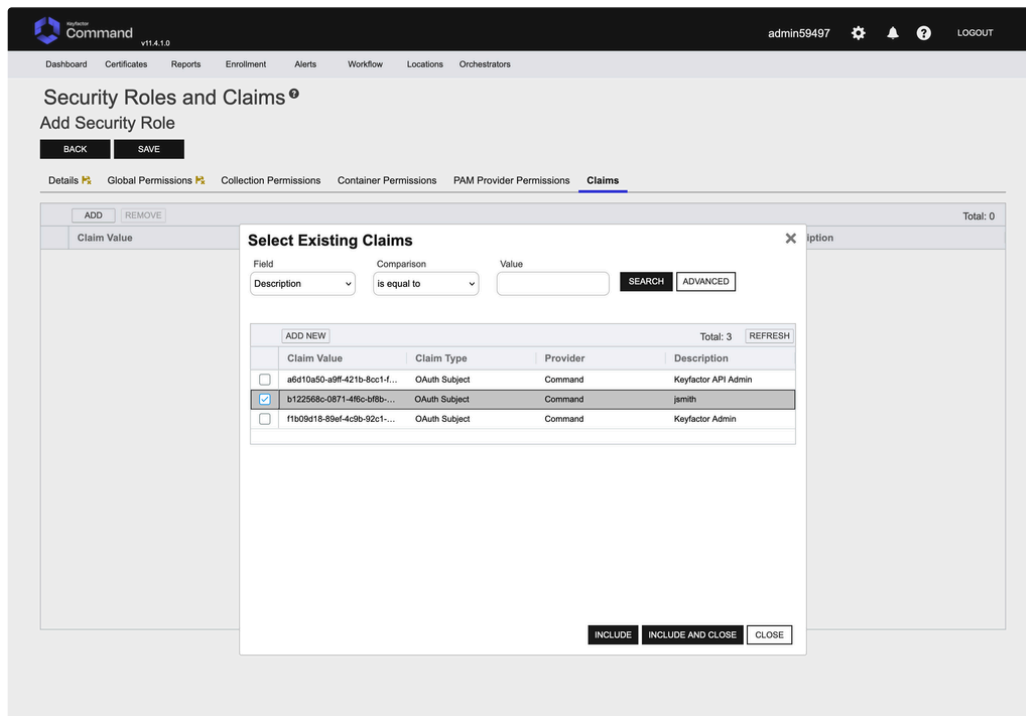


Figure 35. Select Claim

Have the user login with the new username and password at the Test Drive Command URL (for example <https://<TEST DRIVE URL>:/KeyfactorPortal>)

⚠️ New users should add the Management Certificate as outline above in the section “Adding ManagementCA Certificate” so they don’t get browser warnings.

The user will get the Keyfactor Login screen. Enter the new users username and password. If you left the “Temporary” slider on, they will be prompted to change their password (Figure 36) if not already done.

Figure 36. Change Password

Once done, the new user will be logged into the EJBCA Administration web with the new username reflected at the top (Figure 37).

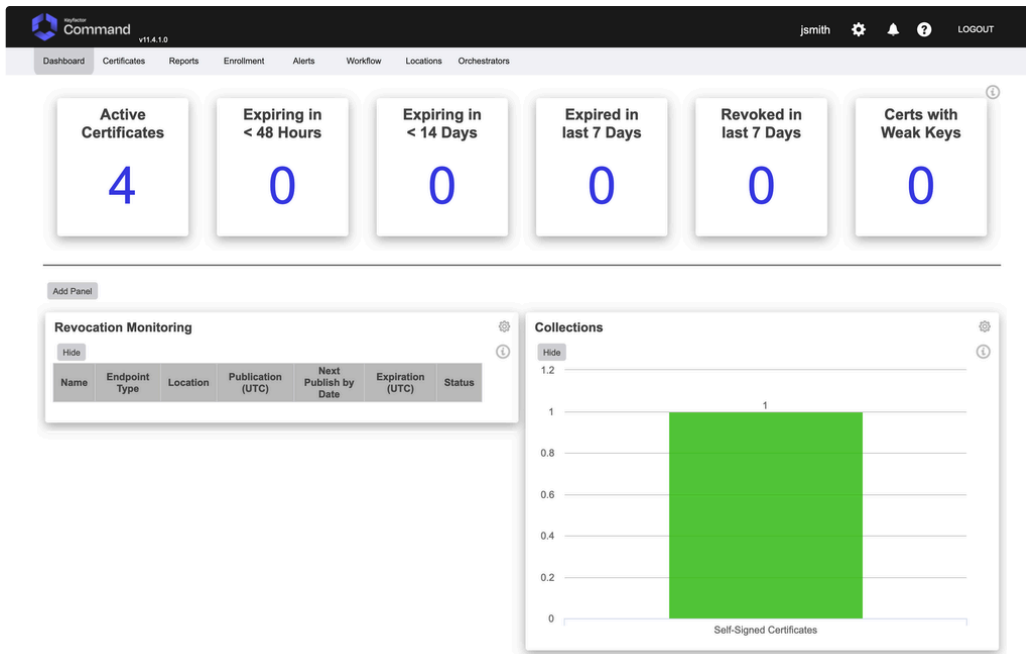


Figure 37. Newly logged in user