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.

KEÝFACTOR

Welcome to the Keyfactor Command Test Drive!

This page will be updated again after the installation progresses further

Ott will take some time (approximately 20 minutes) to get your Keyfactor Command environment setup. It is all being provisioned from scratch for your unique Test Drive experience.

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

This instance will be available for 30 days from the time you launched it. It will self-terminate at that point. This process is automatic and cannot be stopped and no data can be saved from this instance. If you would like to have a more in depth Proco-of-Concept after this text drive, please contact sales®keyfactor.com.

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.

KEÝFACTOR

Welcome to the Keyfactor Command Test Drive!

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

O 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:



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.



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).

$\leftarrow \ \rightarrow \ {\tt G}$	O 🔒 https://sshin-td3.eastus.cloudapp.azure.com:8443/ejbc	a/ra/cas.>	html		☆	
EJBCA En	terprise Enroll - CA Certificates and CRLs Tools	- Lo	g in			
	CA Certificates and CRLs					
	Certificate Authority	CRL	Certificate	Certificate chain ¹	Browser import	
	ManagementCA UI0=7397857, Oli-ManagementCA	Full	PEMDER	PEM JKS PKCS#7	Firefox Internet Explo	rer
	TestDriveRoot-G1 CN=Test Drive Root CA G1,00=Certification Authorities,0=Keyfactor Command,C=US	Full	PEM DER	PEM JKS PKCS#7	Firefox Internet Explo	rer
	TestDriveSub-G1 ON=Test Drive Sub CA G1,0U=Certification Authorities,O=Keyfactor Command,C=US	Full	PEM DER	PEM JKS PKCS#7	Firefox Internet Explo	rer
	¹ Java Key Store (JKS) password is set to 'changeit'.					
	Download Fingerprints Download Certificate Bundle					

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 the 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).

🍪 Firefox	about:prefere	nces#searchResults				
			Certificate Mana	iger		
		Your Certificates You have been asked to tr	Authentication Decisions ust a new Certificate Authority (CA).			
	You hav	Do you want to trust "Mar Trust this CA to identif Trust this CA to identif	lagementCA" for the following purpose 'y websites. 'y email users.	s?		
	LA ∽ Micrı Mi e-	Before trusting this CA for View Examine	any purpose, you should examine its c CA certificate	ertificate and its p	olicy and procedure: Cancel	s (if available).

Figure 6. Dialog box for Importing ManagementCA certificate to Firefox

	🝅 Firefox	about:preferenc	ces#searchResults						☆
						cert	8		
						Cort			
	Sear	ch Results							
	Certif	icates					cert		
	Qí			C	ertificate Mana	ager			×
curity	AI	Yo	our Certificates	Authenticatio	n Decisions	People	Servers	Authorities	
lozilla		You have <mark>cer</mark>	<mark>t</mark> ificates on file tha	it identify thes	e <mark>cert</mark> ificate au	thorities			
021114		Certificate	Name				Security	/ Device	E
		LAWtru	ist Root CA2 (409	6)			Builtin Ol	oject Token	
		✓ Managem	entCA						
		Manage	ementCA				Software	Security Device	
		~ Microsec	Ltd.						
		Microse	ec e-Szigno Root (CA 2009			Builtin Ol	oject Token	
		e-Szigr	no Root CA 2017				Builtin Ol	oject Token	
		View	Edit Trust	Import	Export	Delete or I	Distrust		
									ок

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.

	Certificate Ma	anager			×
Your Certificates	Authentication Decisions	People	Servers	Authorities	
These entries identify s	server <mark>cert</mark> ificate error exc	ceptions			
Server		SHA-256 Finger	rprint		
command114-5.east	us2.cloudapp.azure.c	E3:12:6E:F1:0C	:2C:07:72:54:9	1:1C:A2:DC:	
command114-5.east	us2.cloudapp.azure.c	E3:12:6E:F1:0C	:2C:07:72:54:9	1:1C:A2:DC:	
command114-5.east	us2.cloudapp.azure.c	E3:12:6E:F1:0C	:2C:07:72:54:9	1:1C:A2:DC:	

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 lauch page from the Azure Marketplace Test Drive Portal

KEÝFACTOR	
Sign in to your account	
Username or email	
Password	
	۲
Sign In	

Figure 10. Keycloak login page

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

Home	Version : EJBCA 8	2.1 Enterpris	e (52edfca86	f81118be615f52c1aa312dccad90e7c
CA Functions	Welcome adm	in36349 t	O EJBCA A	dministration.
CA Activation CA Structure & CRLs Certificate Profiles	Node hostname 7 Server time 2024-	d0dc5c9a60 04-15 23:55	:30+00:00	
Crypto Tokens	CA Status			Publisher Queue Status
Publishers	CA Name	CA Service	CRL Status	Publisher Length
Validators	ManagementCA	*	 ✓ 	No publishers defined.
RA Functions	TestDriveRoot-G1	*	 V 	
Add End Entity	TestDriveSub-G1	~	v	
Search End Entities				
User Data Sources				
VA Functions				
OCSP Responders				
Supervision Functions				
Approval Profiles				
Approve Actions				
System Functions				
Roles and Access Rules				
Remote Authentication				
Services				
System Configuration				
ACME Configuration				
Autoenrollment				
Configuration				
EST Configuration				
SCEP Configuration				
System Configuration				
My Preferences				
RA Web				

© 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).

EJBCA Enterprise	Enroll	·	CA Certificates and CRL	s Tools -	Log in
	Enrollment code	i wi	th Enrollm	ent	
	Enter Username	and	Enrollment code	to enroll	
	Username	admi	in36349		
	Enrollment code	•••••			
					Check

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.

EJBCA Enterprise	Enroll	 CA Certificate 	es and CRLs	Tools - Lo	og in		
	Enrollment code	with En	rollmen	t			
	Finalize Enrollm	ent					
	Username	admin36349					
	Key algorithm	RSA 3072 bits			×		
			Download	d JKS Down	load PKCS#12	Download PEM	
					Back		

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**.

	се	rt 🛞	
[දියි General	Search Results		
Home	Certificates	cert	
Q Search	Query OCSP responder servers to confirm the current validity of certificates	View Certificates	
		Security Devices	
Privacy & Security	Certificate Manager		×
Sync			
More from Mozilla	Your Certificates Authentication Decisions People	Servers Author	ities
	You have certificates from these organizations that identify you		
	Certificate Name Security Device Serial Number	Expires On	
	~ 21e65455-b115		
	21e65455-b1 OS Client Cert Tok B5:F6:35:3C:C4:E1:	June 6, 2033	
	✓ 3805c410-561a		
	3805c410-56 OS Client Cert Tok 61:3C:B7:25:BB:48:	February 4, 2025	
	✓ IntuneMDMAge		
	IntuneMDMA OS Client Cert Tok 7E:34:C7:7D:98:90	June 2, 2024	
	Mississi Oktion Mississi Deslam All Investig		
	View Backup Backup All Import D		
			ок

Figure 15. Importing the admin.p12 into FireFox

	Certificate Man	ager		×
	Authentication Decisions	People	Servers	
You have certi Certificate N	Password Required - Mozill Please enter the password th certificate backup:	l a Firefox nat was used to e	encrypt this	同一
21e6545 ~ 3805c410-		Cancel	Sign in	3
3805c410-56 ~ IntuneMDMAge	OS Client Cert Tok 61:3C	::B7:25:BB:48:.	February 4, :	2025
View Backu	OS Client Cert Tok 7E:34	:C7:7D:98:90	. June 2, 2024 Delete	
				ОК

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).





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: Ke 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.

KEYFACTOR Sign in to your account Username or email admina6349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign in	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password	Keyfactor		
KEYFACTOR Sign in to your account Username or email admin36349 Password 	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign in	KEYFACTOR Sign in to your account Username or email admin36349 Password 			
KEYFACTOR Sign in to your account Username or email admin36349 Pessword 	KEYFACTOR Sign in to your account Username or email admin36349 Password Password	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password 	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In	KEYFACTOR Sign in to your account Username or email admin36349 Password 			
KEYFACTOR Sign in to your account Username or email admin36349 Password	KEŸFACTOR Sign in to your account Username or email admin36349 Password Sign In	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password 	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In			
KEYFACTOR Sign in to your account Username or email admina6349 Password Resourd Resourd	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password Password Sign in	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Passwerd Sign In	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In			
KEYFACTOR Sign in to your account Usemame or email admina6649 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password Instantion	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign in	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In			
KEYFACTOR Sign in to your account Username or email admina6349 Password 	KEYFACTOR Sign in to your account Username or email admin36349 Password 	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign in	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In			
KEYFACTOR Sign in to your account Username or email admina6349 Password 	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In	KEYFACTOR Sign in to your account Username or email admin36349 Password 	KEYFACTOR Sign in to your account Username or email admin36349 Password 	KEYFACTOR Sign in to your account Username or email admin36349 Password Sign In	KEYFACTOR Sign in to your account username or email admin36349 Password Sign In			
Sign in to your account Username or email admin36349 Password Sign In	Sign in to your account Username or email admin36349 Password Sign In	Sign in to your account Username or email admin36349 Password Sign In	Sign in to your account Username or email admin36349 Password Sign In	Sign in to your account Username or email admin36349 Password Sign In	Sign in to your account Username or email admin36349 Password Sign In	Sign in to your account Username or email admin36349 Password Sign In	ΚΕΫΕΔΩΤΟΕ	2	
Sign in to your account Username or email admin36349 Password Sign in	Sign in to your account Username or email admin36349 Password Sign In	Sign in to your account Username or email admin36349 Password Sign In Sign In	Sign in to your account Username or email admin36349 Password Sign In Sign In	Sign in to your account Username or email admin36349 Password Sign In Sign In	Sign in to your account Username or email admin36349 Password Sign in Sign in	Sign in to your account Username or email admin36349 Password Sign In Sign In	REITACIO	•	
Username or email admin36349 Password Sign In	Username or email admin36349 Password Sign In	Username or email admin36349 Password Sign In	Username or email admin36349 Password Sign In	Username or email admin36349 Password Sign In	Username or email admin36349 Password Sign In	Username or email admin36349 Password Sign In	Sign in to your account		
admin36349 Password Sign In	admin36349 Password Sign In	admin36349 Password Sign In	admin36349 Password Sign In	admin36349 Password Sign In	admin36349 Password Sign In	admin36349 Password Sign In	Username or email		
Password Sign In	Password Sign In	Password Sign In	Password Sign In	Password Sign in	Password Sign in	Password Sign in	admin36349		
Sign In	Sign In	Sign In	Sign In	Sign in	Sign in	Sign in	Password		
Sign In	Sign In	Sign In	Sign In	Sign In	Sign In	Sign In		۲	
							Sign In		

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).

≡ KEŸFACT	OR		
Keyfactor 👻	Users Users are the users in the current realm. Learn more P_{i}^{*}		
Manage			
Clients	User list		
Client scopes	▼Default search → Q. Search user	\rightarrow	Add user
Realm roles			
Users	Username		Email
Groups	admin59497		0-
Sessions			
Fuenta			

Figure 22. Add User

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

General	
Username *	jsmith
Email	
First name	
Last name	
Groups 💿	Join Groups
	Create Cancel

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).

jsr	nith				
	Details	Attributes	Credentials	Role mapping	Groups
ID *	ĸ	b122	568c-0871-4f6	c-bf8b-e889c4dd	7cff
		Figure	24. Keycloak Us	ser ID	

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

≡ KEÝFACT(OR							
Keyfactor 👻	Users → User o	details						
Manage								
Clients	Details	Attributes	Credentials	Role mapping	Groups	Consents	Identity provider links	Sessions
Client scopes								
Realm roles							O	
Users							No crodontia	
Groups							Nocredentia	15
Sessions					This	s user does no	t have any credentials. You	can set password for this user.
Events							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).





Roles Management

Role name			RA Styles	6	
Public Access Role	Members	Access Rules	Default v	Rename	Delete
Public RA Access	Members	Access Rules	Default ~	Rename	Delete
Super Administrator Role	Members	Access Rules	Default ~	Rename	Delete
					Add

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 Mana	igement
Role : Super Administrator Role						aa Kulea
Match with	CA	OAuth Provider	Match Operator	Match Value	Description	Action
OAuth 2 JWT: Subject ("sub") claim v	ManagementCA v	Keycloak 🗸		71-4f6c-bf8b-e889c4dd7cff	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)

A 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).

KEÝFACTOR Update password		
A You need to change your password to activate your account.		
New Password		
	۲	
Confirm password		
	۲	
Sign out from other devices		
Submit		

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).



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.

shboard Certificates Report	Enrollment Alerts We	orkflow Locations Orchestrators		Security Roles & Claims	
Active Certificates	Expiring in < 48 Hours	Expiring in < 14 Days	Expired in last 7 Days	Certificate Store Types Certificate Metadata Audit Log Event Handler Registration	Certs with Weak Keys
4	0	0	0	Privileged Access Management Identity Providers SMTP Configuration Component Installations	0
4 dd Panel Revocation Monitoring	0	0	Collections	Privileged Access Management Identity Providers SMTP Configuration Component Installations	0



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.

Command vi14.1.9			admin59497 🔅 🌲	COGOUT
Dashboard Certificates Reports Enrollmen	nt Alerts Workflow Locations	Orchestrators		
Security Roles and Clair	ms [₽]			
Claims define security principals with access to the Roles to grant permission to system resources. A Field Description	e system. The Claim Types may be either OAL single web server hosting Command should us Comparison is equal to	th claim values or Active Directory Security Group se either OAuth or Active Directory claim types but Value	is, Users, and Computers. These claims are then ass not both.	Igned to Security
ADD EDIT DELETE VIEW PERMISS	IONS VIEW ROLES			Total: 2 REFRESH
Claim Value	Claim Type	Provider	Description	
a6d10a50-a9ff-421b-8cc1-f6cd3add6c36	OAuth Subject	Command	Keyfactor API Admin	
f1b09d18-89ef-4c9b-92c1-d8e2b902a089	OAuth Subject	Command	Keyfactor Admin	
	Add Claim Claim Type OAuth Subject Claim Value b122686-0871-4160-b1 Provider Command Description jamith	Sb=#889c4dd7cff Sb/#889c4dd7cff		

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.

		admin	59497	¢	٨	0	LOGOUT
Dashboard Certificates Reports Enrollment Alerts W	kflow Locations Orchestrators						
Security Roles and Claims Add Security Role BACK SAVE Details Global Permissions Collection Permissions Con	iner Permissions PAM Provider Permissions Claims						
ADD REMOVE							Total: 0
Claim Value Select Existing	Claims	×	iption				
Field Description ~	Comparison Value SEARCH ADVANCED						
ADD NEW	Total: 3	REFRESH					
Claim Value	Claim Type Provider Description						
a6d10a50-a9ff-421	-8cc1-f OAuth Subject Command Keyfactor API Admir	n					
✓ b122568c-0871-4f	-bf8b OAuth Subject Command jsmith						
[] f1b09d18-89ef-4c9	-92c1 OAuth Subject Command Keyfactor Admin						
		CLOSE					

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)

A 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.

A	
You need to change your password to activate your account.	
New Password	
•••••	۲
Confirm password	
•••••	۲
Sign out from other devices	
Submit	

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).

Active Certificates	Expiring in < 48 Hours	Expiring in < 14 Days	Expired in last 7 Days	Revoked in last 7 Days	Certs with Weak Keys
4	0	0	0	0	0
Panel		0	Collections		
lide	Next	0	Hide		(
ame Type Location	(UTC) Publish by Date	(UTC) Status	1	1	
			0.8		
			0.0		
			0.6		
			0.4		

Figure 37. Newly logged in user