

BreakingPoint

KCOS Administration

Release 9.30

User Guide

Notices

Copyright Notice

© Keysight Technologies 2022

No part of this document may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Keysight Technologies, Inc. as governed by United States and international copyright laws.

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly,

Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at <http://www.keysight.com/find/sweula>. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Contacting Us

Keysight headquarters

1400 Fountaingrove Parkway
 Santa Rosa, CA 95403-1738
www.ixiacom.com/contact/info

Support

Global Support	+1 818 595 2599	support@ixiacom.com
<i>Regional and local support contacts:</i>		
APAC Support	+91 80 4939 6410	support@ixiacom.com
Australia	+61-742434942	support@ixiacom.com
EMEA Support	+40 21 301 5699	support-emea@ixiacom.com
Greater China Region	+400 898 0598	support-china@ixiacom.com
Hong Kong	+852-30084465	support@ixiacom.com
India Office	+91 80 4939 6410	support-india@ixiacom.com
Japan Head Office	+81 3 5326 1980	support-japan@ixiacom.com
Korea Office	+82 2 3461 0095	support-korea@ixiacom.com
Singapore Office	+65-6215-7700	support@ixiacom.com
Taiwan (local toll-free number)	00801856991	support@ixiacom.com

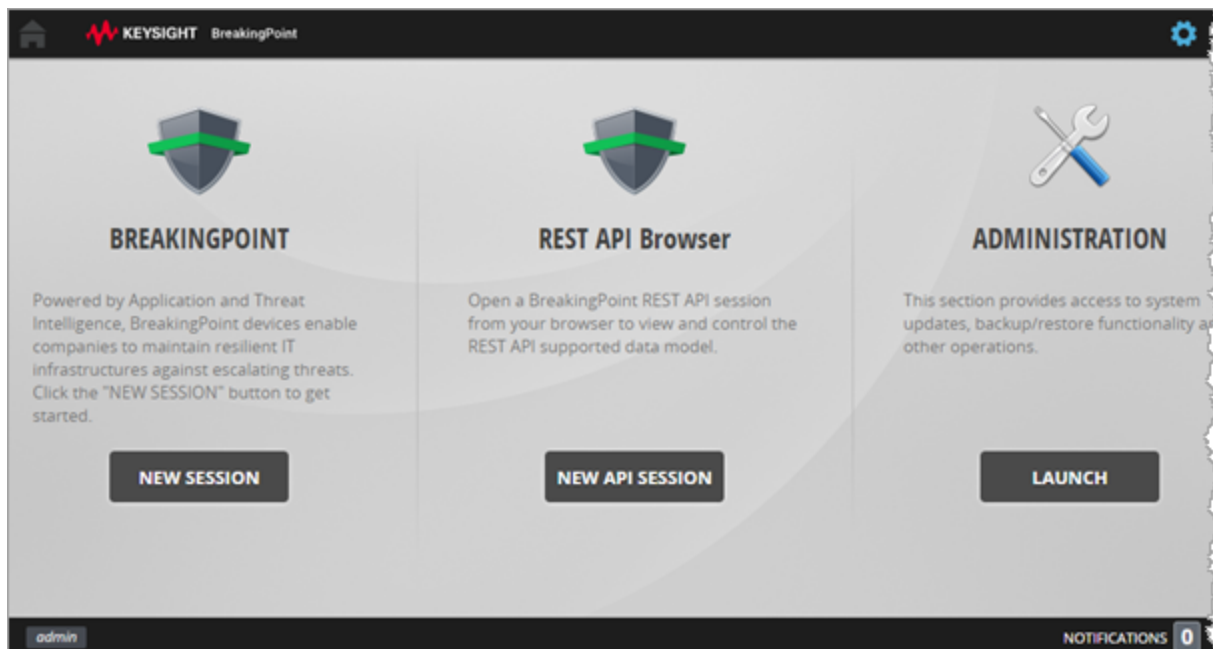
Table of Contents

Contacting Us	3
Chapter 1 KCOS Admin Dashboard	5
Chapter 2 Certificate	8
Chapter 3 Date & Time	10
Chapter 4 Diagnostics	11
Chapter 5 Maintenance	12
Chapter 6 Network	13
Chapter 7 Services	14
Chapter 8 Snapshot	15
Chapter 9 Terminal	17
Chapter 10 Updates	18
Chapter 11 Users	20
Index	23

CHAPTER 1

KCOS Admin Dashboard

When you log in from your browser, BreakPoint opens the landing page.

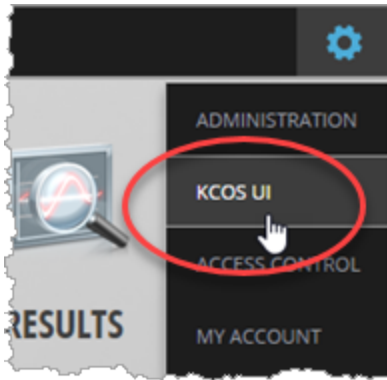


From the landing page you can access BreakingPoint test sessions, the REST API browser, test results, and BreakingPoint administrative functions. In addition, you can access the KCOS Admin Dashboard from a menu selection, as described in [To open the KCOS Admin Dashboard on the next page](#).

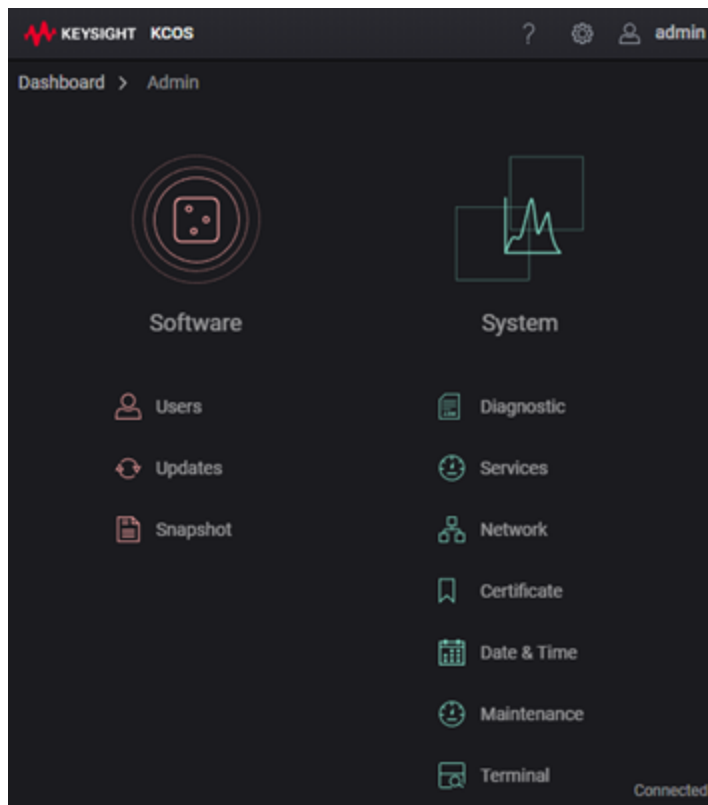
KCOS (Keysight Cluster Operating System) provides system administration services to BreakingPoint and other Keysight software and hardware products.

To open the KCOS Admin Dashboard

1. Click the gear icon (⚙️) to open the system menu.
2. Select **KCOS UI** from the drop-down menu.



The KCOS Admin Dashboard opens:



The KCOS Admin functions

Click the links from the following lists to view detailed instructions for the given KCOS Admin function:

Software

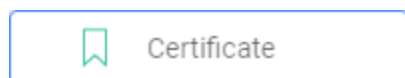
[Users](#)[Updates](#)[Snapshot](#)

System

[Diagnostic](#)[Services](#)[Network](#)[Certificate](#)[Date & Time](#)[Maintenance](#)[Terminal](#)

CHAPTER 2

Certificate



To generate a Certificate Signing Request (CSR) and obtain a signed digital certificate, select **Certificate** from the KCOS **Admin** panel. The signed certificates that you acquire can be used for encryption and authentication in your test network.

There are four steps in the certificate process.

Step 1 – Fill in information

In step 1, enter the values required for the Certificate Signing Request (CSR). A CSR is an encoded message sent to a certificate authority (or other certificate issuing entity) to request the signing of a public key and issuance of a certificate. Be aware that the CSR fields accept only alphanumeric characters.

Value	Description
Country	The country or region name, entered as a two-character ISO format country code. Examples: AU, CA, CN, IN, RO.
State	The state or province.
Location	The city or locality.
Organization	The organization name.
Organization Unit	The organizational unit. You can enter NA if this is not relevant to your requirements.
Fully Qualified Name	This is the CSR <i>Common Name</i> field: the fully qualified Domain Name of the private key owner. For example: eagle-ma006.lbj.is.keysight.com.

Step 2 – Generate Certificate Signing Request

Once you have entered the information for the CSR, click **Generate CSR** to generate the signing request. KCOS generates the request and a private key, and stores the private key on your system (the node on which KCOS is running).

The CSR specifies a key type and length of RSA 2048, and certificate file extension of .crt.

Step 3 – Download Certificate Signing Request

Click **Download CSR** to download the generated CSR to your downloads folder.

Step 4 – Upload signed certificate

There are two actions needed for the fourth step:

1. Using your organization's standard practices, submit your downloaded CSR and request a signed certificate.
2. When you receive the signed certificate:
 - a. Click **Upload Certificate**.
 - b. Navigate to the folder in which you stored the certificate, then select it.
KCOS uploads the certificate and displays it.
 - c. Click **Apply**.

KCOS makes the certificate available on the node.

CHAPTER 3

Date & Time

**Date & Time**

You use **Date & Time** to set your system's timezone and to either manually set the system date and time or enable an NTP server to control the date and time.

To configure your system's Date & Time settings:

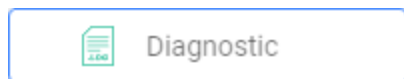
1. Select **Date & Time** from the KCOS **Admin** panel.
2. Enter or select the values, as required for your system.
3. Click **Apply Changes**.

The following table describes the available settings:

Setting	Description
System Time	This field shows the currently-set system date and time.
Timezone	Select the desired UTC (Coordinated Universal Time) timezone from the drop-down list. You can enter a partial value in the field to filter the list.
Date	If you are not using NTP for time management, enable the <i>Date</i> field and then select the date from the pop-up calendar.
Time	If you are not using NTP for time management, enter the system time, using 24-hour notation (hh:mm:ss).
Use NTP	Enable <i>Use NTP</i> if you plan to use NTP servers for date and time management.
NTP Servers	If you have enabled <i>Use NTP</i> , enter a space-separated list of one or more NTP server IP addresses.

CHAPTER 4

Diagnostics



To collect chassis logs, select **Diagnostic** from the KCOS **Admin** panel. The diagnostics are collected for all available components.

You can perform the following actions:

- [Collect diagnostics below](#)
- [Delete a system_logs file below](#)
- [Access a diagnostics file below](#)

Collect diagnostics

To collect chassis logs from the node on which KCOS is running:

- Click **Collect Diagnostics**.

KCOS starts the collection process, and creates a zip file containing the collected logs.

Delete a system_logs file

To delete a system_logs file:

1. In the **Diagnostics** window, hover over the file that you plan to delete.
2. Click the delete icon:



KCOS deletes the file and removes it from the list.

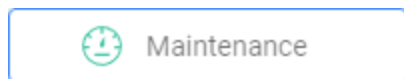
Access a diagnostics file

To access the logs from a zipped system_logs file:

1. SSH to the system with administrator privileges.
2. Locate the zipped file in the **tmp** folder.
3. Unzip the *logs-yyyy-mm-dd-hh-min-sec.zip* file.
4. Unzip the *kcossystemdiagnostics* and the *agentdiagnostics* zip files.
5. Access the log files from the folders that were contained in the zip files.

CHAPTER 5

Maintenance

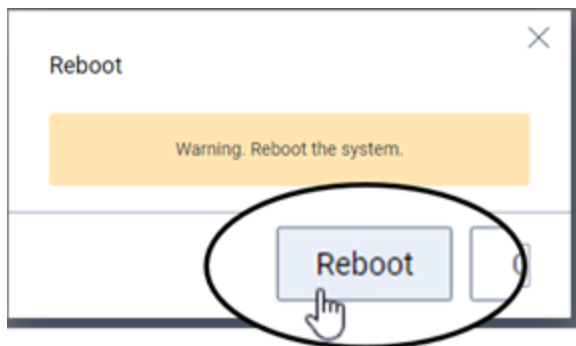


Select **Maintenance** from the KCOS **Admin** panel if you need to perform system maintenance operations.

The available operations include rebooting the system and directing a specific Baseboard Management Controller (BMC) to perform one of the available maintenance operations.

Reboot System

1. Click **Reboot** to reboot the node on which KCOS is running.
KCOS displays a warning dialog.
2. Click **Reboot** to confirm.



KCOS starts the reboot process, during which time you will lose connection to the system.

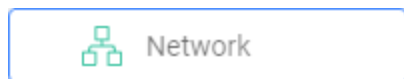
3. After a few minutes, fresh the browser window to see if your connection has been restored.

BMC Nodes

In the current release, the Baseboard Management Controller (BMC) operations are available only from the KCOS CLI (the `kcoc system introspection bmc` commands). You can access the CLI from the [Terminal on page 17](#) window.

CHAPTER 6

Network



To display and configure network settings for the system, select **Network** from the KCOS **Admin** panel.

For each interface on the system, the panel displays the current IP address(es), the gateway, the DNS servers being used by the system, and the MAC address. You can modify these values, as described below.

Modify the Hostname

Enter the desired hostname for the node in the *Hostname* field. The hostname may be a simple name or an FQDN. The semantics are identical to */etc/hostname*.

Configure values for each interface

To configure the network values for an interface:

1. Optionally, modify the interface *Name*.
2. If you are using DHCP, enable either or both of the following:
 - *Use DHCPv4*
 - *Use DHCPv6*
3. If you are using static IP addresses, enter the static IPv4 or IPv6 address and (optionally) the subnet in the *Static IP* field.

Add DNS servers

Add one or more DNS server IP addresses in the *Static DNS Servers* field.

The order in which you enter the DNS server addresses determines their priority. The first server listed has highest priority, with each additional server having a lesser priority.


CHAPTER 7

Services

Services

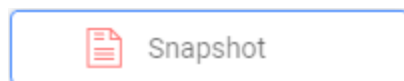
To display information about all Kubernetes pods running on the system, select **Services** from the KCOS **Admin** panel.

KCOS displays the information, as described in this table:

Column	Description
Name	The name that uniquely identifies the pod within a given namespace.
Status	The operational state of the pod.
Pod IP	The IP address that the pod's containers use to communicate with each other.
Host IP	The IP address of the host to which the pod is assigned.
Ready	Displays the number of containers that are currently running, out of the total desired number of containers. For example, "2/3" indicates that the desired number of containers for the pod is three, but only two are running.
	If you want a copy of the table data, click the Copy to Clipboard icon. The data is saved to the clipboard as a semicolon-separated file.

CHAPTER 8

Snapshot



To create and manage system snapshots, select **Snapshot** from the KCOS **Admin** panel. A snapshot captures the state of a system at a particular point in time and enables you to return to that state in the future.

You can perform the following actions:

- [Create a snapshot below](#)
- [Delete a snapshot below](#)
- [Restore a snapshot on the next page](#)

Create a snapshot

IMPORTANT

Creating a snapshot may take up to one hour, and the process automatically triggers a system reboot.

To create a new system snapshot of the node on which KCOS is running:

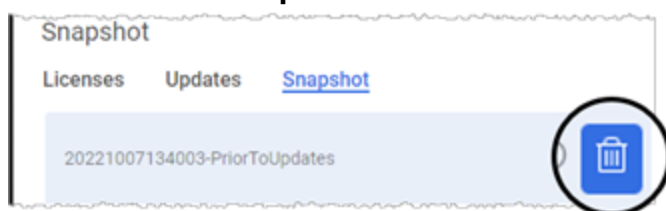
1. Click **New Snapshot**.
KCOS opens the **Create Snapshot** dialog.
2. Enter a name for the snapshot in the *Name* field.
3. Click **Create**.

KCOS starts creating the snapshot and then reboots the system. Once the snapshot creation process is complete, the browser window or tab will refresh to the **Login** page.

Delete a snapshot

The Snapshot panel automatically lists all available snapshots. To delete a snapshot:

1. Point to the **Delete Snapshot** icon for the snapshot that you want to delete.
2. Click the **Delete Snapshot** icon.



KCOS deletes the snapshot and removes it from the list.

Restore a snapshot

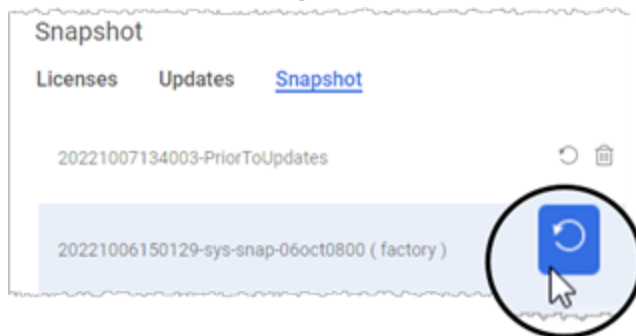
IMPORTANT

Before restoring a snapshot, be aware of the following

- The restored snapshot replaces the current state of your system. Consider creating a snapshot of the current system before restoring it to a prior state.
- APS systems come with a factory image (named *factory*). If necessary, use **Restore Snapshot** to revert to this image.
- In case the KCOS operating system becomes corrupted and inaccessible in the CLI or web-based interface, the system can be restored to *factory* by directly connecting to it (serial or VGA connection) and using the grub factory restore option to restore the factory image. Note that the grub factory restore option is available only on release 9.30 or later KCOS factory images.

To restore the system to the one of your available snapshots:

1. Hover over the snapshot that you want to restore.
2. Click the **Restore Snapshot** icon.



KCOS displays a warning dialog.

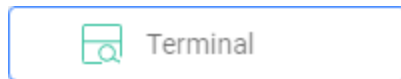
3. Click **Restore** to start the process.



KCOS restores the snapshot, and reboots the system in the process.

CHAPTER 9

Terminal



Select **Terminal** to access the KCOS CLI in a browser tab.

The terminal gives you access to all of the commands that are available in the CLI.

```
Terminal

*** Attempt to connect to KCOS-SSH-Proxy ***
*** Connected to KCOS-SSH-Proxy ***
*** SSH CONNECTION ESTABLISHED ***
Welcome to KCOS shell.
Type 'kcos help' in order to list the available commands.

IP:                                fec0::5054:ff:fe12:3456/64 169.254.170.197/16 10.0.2.15/24
kcos-test-deployment:              2.4.2
kcos-ui-client:                    0.2.29
kcos-ui-service:                   0.2.29

Welcome to KCOS shell. Type 'kcos help' in order to list the available commands.

(kcos)-kcos-525400123456:/home/dev$ kcos shell

Type: "help" for help, "exit" or "CTRL-D" to exit the interactive shell

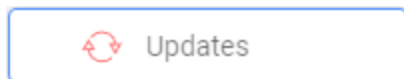
kcos> networking ip show

interface:          mgmt0
ipaddresses:        fec0::5054:ff:fe12:3456/64 169.254.170.197/16 10.0.2.15/24
macaddress:         52:54:00:12:34:56
state:              UP
dhcpv4:             true
dhcpv6:             true
gateways:           []

kcos> |
```

CHAPTER 10

Updates



To install application and system components, select **Updates** from the KCOS **Admin** panel. The specific manner in which you will install the updates depends upon whether or not the node has an Internet connection.

An *update* can be a version upgrade or downgrade.

You can perform system updates using the following methods:

- [Offline installation below](#)
- [Online installation on the next page](#)

Offline installation

Offline installation is required when you do not have an Internet connection from the node on which the updates are being installed:

1. Obtain the packages that you need to install:
 - a. Using a system that has Internet access, download the offline-packages (tar files) from your product's support portal.
 - b. Once downloaded, transfer the packages to the system where the offline installation will be executed.
2. Install the updates:
 - a. From the offline node (the node on which you will install the updates), select **Updates** from the KCOS **Admin** panel.
 - b. Click **Update from File**.
KCOS opens a dialog and selects your standard download directory.
 - c. For each package that you are installing:
 - i. Locate the package, then extract the files.
 - ii. Execute the installer file to start the installation.
3. Click **Apply Changes**.

Online installation

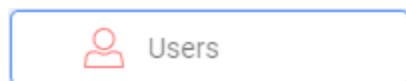
Online installation is available when you have an Internet connection from the node on which the updates are being installed:

1. For each component for which you plan to update, select the desired version from the *Change Version* drop-down list.
2. Click **Apply Changes**.

KCOS obtains the updates from the Keysight online portal and initiates the installations.

CHAPTER 11

Users



When you select **Users** from the **Admin** panel, KCOS opens the **Keycloak Admin Console** in a new browser tab. Keycloak is an open source software product used by many Keysight web-based applications for Identity and Access Management.

KCOS uses Keycloak services for managing:

- [Groups below](#)
- [Users on the next page](#)

NOTE

The instructions on this page describe the basic actions needed to define and manage User Groups and Users for your application. Refer to the official Keycloak documentation for detailed instructions for all of the functionality that is available in Keycloak: <https://wjw465150.gitbooks.io/keycloak-documentation/content/index.html>. User management and User Group management are described in the Server Administration section of the document.

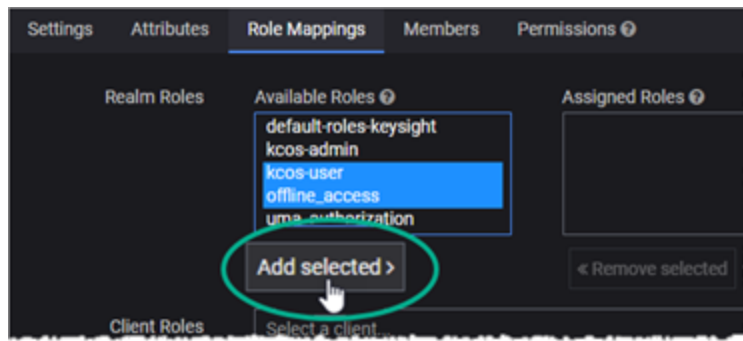
Groups

In Keycloak, *Groups* provides the tools to manage a common set of attributes and role mappings for users. From the **User Groups** page, you add and manage all of the groups for the node on which KCOS is running.

To add a new group:

1. Select **Groups** from the Keycloak navigation pane.
2. Click **New** from the **User Groups** page.
3. Enter a **Name** for the group, then click **Save**.
4. Select the **Role Mappings** tab, select one or more **Available Roles**, then click **Add selected**.

For example:



Keycloak assigns the roles for the new group.

5. Optionally, configure additional attributes and permissions for the group, as required by your organization's Identity and Access Management policies.

To view or modify group details:

1. From the **User Groups** page, select the specific group.
2. Click **Edit**.
3. Make the desired changes.
4. To modify the group name, edit the *Name* field, then click **Save**.

To delete a group:

1. From the **User Groups** page, select the specific group.
2. Click **Delete**.
Keycloak displays a confirmation dialog.
3. Click **Delete** to confirm the group deletion.

Users

From the **Users** page, you add and manage the individual users who need to access the node on which KCOS is running.

To add a new user:

1. Select **Users** from the Keycloak navigation pane.
2. Click **Add user** from the **Users** page.
3. Enter a **Username** for the new user.
Username is the only required field.
4. Optionally, add any desired additional user values (such as email address).
5. Optionally, modify or select these user settings: *User Enabled*, *Email Verified*, *Required User Actions*.
6. Select one or more *Groups* to which the new user will be assigned.
Although optional, this is highly recommended.
7. Click **Save** to complete the addition of a new user.

Keycloak creates the new user and opens the user management page, from which you can modify values and settings for the user as required by your organization's Identity and Access Management policies.

To delete a user:

1. Select **Users** from the Keycloak navigation pane.
2. Enter the *Username* in the **Search** box, then press **Enter**.
Keycloak filters the Users list to show only that user.
3. Click **Delete**.
Keycloak displays a confirmation dialog.
4. Click **Delete** to confirm that you are deleting the user.

Index

A

Admin dashboard 5

C

chassis logs 11

CLI, browser access 17

customer assistance 3

D

date & time settings 10

diagnostics, collecting 11

DNS servers 13

K

KCOS Admin Dashboard 5

Kubernetes pods 14

M

maintenance 12

N

network settings 13

NTP servers 10

P

product support 3

R

reboot the system 12

S

services, show 14

snapshots, create and manage 15

system updates, installing 18

T

technical support 3

U

user management 20



© Keysight Technologies, 2020–2022

This information is subject to change
without notice.

www.keysight.com