

# CEE Connectivity User Guide

Cloud Execution Environment

USER GUIDE

**Copyright**

© Ericsson AB 2016–2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

**Disclaimer**

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

**Trademark List**

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Scope	1
1.2	Target Groups	1
1.3	Prerequisites	1
1.3.1	Conditions	1
1.3.2	Tools and Equipment	1
1.3.3	Documents	1
<b>2</b>	<b>Main CEE User Types</b>	<b>2</b>
<b>3</b>	<b>Introduction to the CEE Interfaces</b>	<b>3</b>
3.1	Interfaces for CEE Users	3
3.2	Interfaces for CEE Administrators	4
<b>4</b>	<b>System and Initial User Accounts</b>	<b>6</b>
<b>5</b>	<b>Atlas VM</b>	<b>8</b>
5.1	CLI Logon	8
5.2	GUI Logon	8
<b>6</b>	<b>vCIC</b>	<b>10</b>
<b>7</b>	<b>vFuel</b>	<b>11</b>
<b>8</b>	<b>Compute Host</b>	<b>12</b>
<b>9</b>	<b>Storage Access</b>	<b>13</b>
9.1	EMC ScaleIO Access	13
<b>10</b>	<b>End-User Access</b>	<b>14</b>





# 1 Introduction

This user guide provides an overview of the available interfaces in the Cloud Execution Environment (CEE), and instructions on how to connect to these. The document covers the interfaces from both a CEE user and CEE administrator point of view.

## 1.1 Scope

This user guide provides a basic-level overview of the logon methods available in CEE.

## 1.2 Target Groups

This document is aimed at the following groups:

- Users who want to access a CEE environment
- Administrators who want to configure a CEE environment

## 1.3 Prerequisites

This section describes the prerequisites which have to be fulfilled.

### 1.3.1 Conditions

Ensure that CEE is installed and running.

### 1.3.2 Tools and Equipment

Ensure that a computer with SSH connection to CEE for CLI operations is available.

### 1.3.3 Documents

The site-specific IP and VLAN plan is needed.



## 2 Main CEE User Types

The purpose of CEE Identity and Access Management (IdAM) is to manage identities and credentials for cloud users, and to provide authentication and access control services for user accesses.

The CEE IdAM solution differentiates between the following user types:

- Cloud Infrastructure Administrators
- Local Administrators

OpenStack users are managed by default Keystone and Dashboard operations, not by the CEE IdAM tool. For these operations, refer to [OpenStack Administrator Guide](#).

The following OpenStack user types are defined:

- OpenStack Cloud Administrators
- OpenStack Cloud Users

For detailed information about the user types available in CEE, see the [Security User Guide](#).



## 3 Introduction to the CEE Interfaces

### 3.1 Interfaces for CEE Users

The tasks of a CEE user concern managing the applications (VNFs) running on CEE. Typical tasks include creating and starting VMs, creating or deleting networks, and so on. Such management is done through the CEE Northbound (NB) API, meaning the OpenStack interfaces. These interfaces are provided through the REST API of CEE, and can be accessed by the following:

- Atlas GUI
- OpenStack command line client (OS CLI)
- Other Cloud manager, for example: ECM
- Direct access towards the CEE NB API by means of API calls, for example, using Curl. This option is usually only used for demonstration or development purposes.

The use of the CEE interfaces require user authentication. CEE users are managed in Keystone, and must be defined by the CEE administrator. The administrator creates a CEE project and connects users to it. The CEE user then use the user name and password provided by the CEE administrator to access the CEE NB interfaces.

**Note:** Issuing OpenStack commands from CLI communicating through public URL (if `OS_AUTH_URL='public.fuel.local'`) can result in the following warnings in the printout:

- 318: SNIMissingWarning: An HTTPS request has been made, but the SNI (Subject Name Indication) extension to TLS is not available on this platform.
- 122: InsecurePlatformWarning: A true SSLContext object is not available.

These warnings are issued due to a MOS 9 limitation, and they can be disregarded.

#### Atlas GUI

Atlas runs as a separate VM and provides a management GUI, similar to OpenStack Horizon. The Atlas GUI is provided as a web interface. To log into the Atlas GUI, the Atlas user needs to connect to the interface using a web browser running outside CEE, and uses the credentials defined in Keystone.



## OpenStack Command Line Client

The OS CLI connects to the same REST API as Atlas, and consequently uses the same credentials (users in Keystone). As the name implies, the OS CLI is used from the command line of the user's system. As the CLI uses the REST API of CEE, it can run in various places:

- The OS CLI can be installed and run on the user's computer. CEE users defined in Keystone are provided in the OS CLI, as such, it is not dependent on the local user of the computer.
- The OS CLI is included in Atlas. SSH connectivity to Atlas must be provided for user access. The Atlas administrator needs to create a Linux user in Atlas that can be used for SSH connectivity. The Linux user in Atlas is different from the CEE user in Keystone. Both the Keystone CEE user and the Linux Atlas user are needed to use the OS CLI from Atlas.

**Note:** As the current version of Atlas is based on OpenStack Newton, the following limitations apply to executing commands from Atlas CLI, compared to using OpenStack Client from any vCIC:

- Keystone commands are not available. It is recommended to use OpenStack client commands instead.
- Some OpenStack commands return a notice in the printout on the deprecation of the command.
- OS CLI is included in the CEE infrastructure. A CEE user normally does not have direct access to the CEE infrastructure. This access is reserved for the CEE administrator.

Some use-cases in Atlas require SSH and/or SFTP access to the Atlas VM. In these cases, the Atlas administrator must provide the credentials for Atlas access.

## 3.2 Interfaces for CEE Administrators

The CEE administrator has a number of additional interfaces apart from the interfaces provided for the CEE user.

**Note:** Certain actions require the administrator to use the root account. It is recommended to use sudo to temporarily gain root privileges for such actions.

- Certain CEE management functions (such as debugging, user management, and updates) are done from the Linux CLI in CIC and/or Fuel. There are default users that can be used, however, it is recommended that individual users are created in the CEE infrastructure. These individual CEE administrator user accounts are to be used for SSH connections to the CEE infrastructure.
- The individual CEE administrator accounts can be used to connect to the vCIC node. The CIC can be used to access the individual compute nodes, and to connect to Fuel through SSH.





- The Watchmen alarm service in CEE provides an active alarm list. The service can be accessed from both the CEE infrastructure CLI and the alarm tab in Atlas. The user must be defined as an admin user in Keystone to see the alarms.
- Zabbix is used for infrastructure monitoring, and provides a GUI in the form of a web interface. The credentials for Zabbix are defined during the deployment of CEE.

**Note:** Zabbix is not an official API in CEE, and may be subject to change.



## 4 System and Initial User Accounts

The initial administrator and system account credentials that are created during the system installation are shown in Table 1.

Table 1 Initial Administrator and System Account Credentials

Username	Where	Type	Initial Password and Public Key Set	Password Access Allowed <sup>(1)</sup>	Place of Use	Allowed Human Interface
ceeadm	vCIC, Compute, vFuel	Linux	Initial factory password; initial public key is generated at installation time  Public key access from vCIC to vCICs, compute, and vFuel	Yes	Initial non-root administrator account for example for creating LDAP administrators or accounts. Disable after admin users are created.  Local user in vFuel, LDAP user for vCIC and compute. <sup>(2)</sup>	SSH, console access
ceebackup	vCIC, vFuel	Linux	Initial factory password; initial public key is generated at installation time.  Public key access from vCIC to vCICs, compute, and vFuel.	Yes	Backup and restore processes  Local user in vCIC, vFuel	SSH, console access
root	vFuel	Linux	Initial factory password, password based login must be disabled after install.  Root account public key access from vFuel to vCIC and compute	Yes	In operation system account to manage vCIC, compute, and vFuel	SSH, console access at bootstrap
root	vCIC, Compute	Linux	Initial factory password, public key based login available only from vFuel	Yes, but console only access (no SSH)	Mainly system account for vFuel to manage vCIC and compute  Console access for recovery	Console access for password, no SSH (for recovery)
atlasadm	Atlas VM	Linux	Initial password to log in to Atlas, no public key based authentication by default	Yes	Initial account in Atlas VM.	SSH
admin	OpenStack (vCIC, host, Atlas)	OpenStack	Initial factory passwords, no public keys.	Yes	OpenStack management	Atlas dashboard, OpenStack CLI (RESTful interfaces)



Table 1 Initial Administrator and System Account Credentials

Username	Where	Type	Initial Password and Public Key Set	Password Access <sup>(1)</sup>	Place of Use	Allowed Human Interface
User accounts in LDAP	Compute	LDAP	No, but can be configured; password complexity can be applied	Yes	Operating system access	SSH
zabbix_ce_user	Zabbix API, OpenStack	OpenStack	User and password can be set		Read-only user in Zabbix to read the GUI	GUI, RO
OpenStack cloud administrators	vCIC	OpenStack	None, no password complexity in OpenStack Mitaka release	Yes, to OpenStack	OpenStack management	OpenStack API
OpenStack cloud users	vCIC	OpenStack	None, no password complexity in OpenStack Mitaka release	Yes, to OpenStack	OpenStack limited management	OpenStack API
BSP users	BSP	HW	Refer to BSP documentation, password	Yes		SSH
HDS users	HDS	HW	Refer to HDS documentation			
admin	Extreme	HW	SSH password, SOAP service	Yes		SSH, SOAP

(1) The value of this field is "Yes" if it is a human access account. The value is "No" if it is a system account.

(2) Fuel commands require root access. Use sudo for running Fuel commands as a personal user.

For more information on initial administrator and system accounts, see the [System Hardening Guideline](#).



## 5 Atlas VM

### 5.1 CLI Logon

To log on to Atlas using the CLI, follow these steps:

1. Open a command line.
2. Type in the following command:  
`ssh <user>@<atlas_ip>`

Replace `<atlas_ip>` with the administrator defined Atlas IP address.

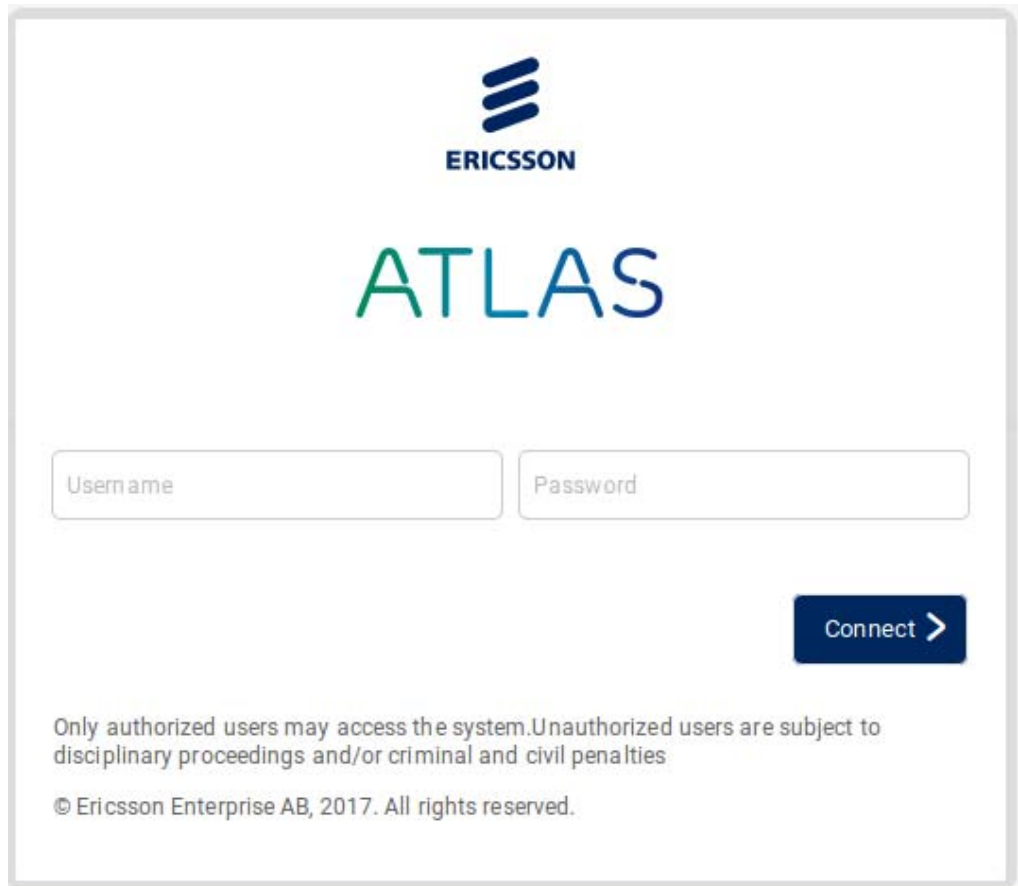
The `<user>` can be a personal user account or `atlasadm` depending on the credentials provided by the Atlas administrator.

### 5.2 GUI Logon

To log on to Atlas using the GUI, follow these steps:

1. Open a web browser.
2. Navigate to `https://<atlas_ip>/` to reach the Atlas GUI logon screen, as shown in Figure 1.

Replace `<atlas_ip>` with the administrator defined Atlas IP address.



The screenshot shows the Atlas login interface. At the top center is the Ericsson logo, consisting of three blue slanted bars above the word "ERICSSON" in blue capital letters. Below the logo, the word "ATLAS" is displayed in a large, blue, sans-serif font. Underneath "ATLAS" are two input fields: "Username" on the left and "Password" on the right. To the right of the "Password" field is a dark blue button with the text "Connect" and a white right-pointing chevron. Below the input fields and button, there is a line of small text: "Only authorized users may access the system. Unauthorized users are subject to disciplinary proceedings and/or criminal and civil penalties." At the bottom of the screen is a copyright notice: "© Ericsson Enterprise AB, 2017. All rights reserved."

Figure 1 Atlas Login Screen

3. Type the username and password in the corresponding fields, then click > to log in to Atlas.

**Note:** Atlas is best viewed using Google Chrome™ version 40.0 or later, but it also supports Mozilla Firefox® 40.0+.



## 6 vCIC

The vCICs can be reached from:

- vCIC public IP addresses on VLAN `cee_om_sp`, using the IdAM username and password
- vFuel

The **`fuel node`** command can be used in vFuel to list the available nodes in the system.

The CEE region has one vCIC node (`cic-1`) in case of single server and three vCIC nodes (`cic-1`, `cic-2`, and `cic-3`) in case of multi-server configurations with public IP addresses according to IP addresses allocated for vCIC nodes in `cee_om_sp` network.

The vCIC nodes have hostnames of the format `cic-<id>`, for example: `cic-2`

To log on to any vCIC from outside CEE using the NB IP of the vCIC, follow these steps:

1. Open a command line.
2. Type in the following command:  
**`ssh <personal_user>@<any_cic-ip-address>`**

**Note:** The command line capabilities provided by the vCIC can be used by the CEE administrator for administrative tasks only.

To log on to any vCIC from vFuel, follow these steps:

1. Open a command line.
2. Type in the following command:  
**`ssh cic-<id>`**

**Note:** This method is only applicable if a management network is connected to vFuel with a direct SSH connection to vFuel from outside CEE. The normal procedure is to connect to vCIC and then use SSH to connect to vFuel. In such cases there is no need to make another SSH session to the vCIC from vFuel.



## 7 vFuel

To log on to vFuel, follow these steps:

1. Connect to vCIC as described in Section 6 on page 10.
2. Type in the following command:  
**ssh root@<fuel\_address>**

**<fuel\_address>** is the Fuel static address in the `fuel_ctrl_sp` VLAN. The factory default value is `192.168.0.11`. Refer to the local version of the IP and VLAN plan, updated with site-specific IP addresses.



## 8 Compute Host

Compute hosts can be reached:

- From vCIC
- From vFuel

The **fue1 node** command can be used in vFuel to list the available nodes in the system.

Compute hosts have hostnames of the format `compute-<shelf_id>-<blade_id>`, for example: `compute-0-3`.

More examples are provided in Table 2.

Table 2 Examples of Hostnames

Hostname	Description
compute-0-5	Compute host in shelf 0 (enclosure 0), device bay 5
compute-1-10	Compute host in shelf 1 (enclosure 1), device bay 10
...	Following the same pattern for further shelves
compute-2-16	Compute host in shelf 2 (enclosure 2), device bay 16

To log on to a compute host, follow these steps:

1. Connect to vFuel as described in Section 7 on page 11.
2. Type in the following command:  
**ssh ceeadm@<compute\_address>**

Replace **<compute\_address>** with the relevant IP address or compute node name.





## 9 Storage Access

### 9.1 EMC ScaleIO Access

Refer to the Dell EMC ScaleIO Version 2.x User Guide and Dell EMC ScaleIO Version 2.x CLI Reference Guide documents for ScaleIO CLI and GUI access.



## 10 End-User Access

End users can manage the virtual resources through the following interfaces:

- OpenStack NB APIs
- GUI in Atlas
- OpenStack command line clients, for example, in Atlas

Usage of the OpenStack client requires authentication. The username and password are defined in Keystone and must be provided by the CEE administrator. The username and password can be provided as command line parameters, or configured as environment variables. The procedure for configuring the environment variables are described in [OpenStack Administrator Guide](#).

**Note:** The command line capabilities provided by the vCIC can be used by the CEE administrator for administrative tasks only.