

# Configure User Account

IPWorks

OPERATING INSTRUCTIONS

**Copyright**

© Ericsson AB 2017, 2108. 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	Prerequisites	1
1.1.1	Documents	1
1.1.2	Conditions	1
1.2	Relation Information	1
<b>2</b>	<b>User Account Configuration</b>	<b>3</b>
2.1	Configuring Access to CLI	3
2.2	Configuring Open Access	5
2.3	Creating Users in CLI	6
2.4	Showing User Definition	6
2.5	Configuring Profile	7
2.6	Showing Profile Definition	7
2.7	Changing Password	7
2.8	Password Expiration Period	8
2.9	Password Lock after Repeated Login Failure	9
<b>3</b>	<b>Creating A Global User</b>	<b>11</b>
	<b>Reference List</b>	<b>13</b>





# 1 Introduction

This document describes the configuration procedures related to Storage Server user management and access control.

## 1.1 Prerequisites

This section describes the prerequisites, which must be fulfilled before using the procedure.

### 1.1.1 Documents

Before using this document to perform the user account configuration, the users are required to read the Section **User Management** in *IPWorks Configuration Management*.

### 1.1.2 Conditions

Before starting this procedure, the following conditions must apply:

- The IPWorks Storage Server is installed.

## 1.2 Relation Information

Trademark information, typographic conventions, and definition and explanation of abbreviations and terminology can be found in the following documents:

- Trademark Information
- Typographic Conventions
- Glossary of Terms and Acronyms





## 2 User Account Configuration

The user configuration contains the following topics:

- Configuring Access to CLI
- Configuring Open Access
- Creating Users in CLI
- Configuring Profile
- Changing Password
- Password Expiration Period
- Password Lock after Repeated Login Failure

### 2.1 Configuring Access to CLI

Users must log on OS before accessing IPWorks data. By default, only users with root access are allowed to execute IPWorks processes. However, non-root users must be able to run the CLI to manipulate IPWorks configuration objects, either interactively or using automated scripts.

Selected non-root users are given access to the CLI using `sudo` ([SUDO Website](#)), a program that allows a user to run another program with the privileges of a different user, typically the root user.

To give the selected users access to the CLI, do the following:

1. Log on to SC-1 as root.  
  
`# ssh root@<SC-1 Address>`
2. Create a new group. Skip this step if the default group "ipworks" is used.
  - a. Create a new group.  
  
`# groupadd <groupname>`
  - b. Make the new group global to the whole cluster.  
  
`# lde-global-user --group <groupname>`
3. Configure user.

The group name refers to "ipworks" or the new group created in Step 2.



- a. For each existing user that needs to use the CLI, change the user's primary group.

```
# usermod -g <groupname> <username>
```

- b. When adding new users, assign each user to the primary group, which is "ipworks" or the new group created in Step 2.

```
# useradd -g <groupname> <username>
```

```
# passwd <username>
```

```
# lde-global-user --user <username>
```

- c. Create the home directory for the users if it doesn't exist, and set the file owner and group.

```
# mkdir /home/<username>
```

```
# chown <username>:<groupname> /home/<username>
```

4. Configure sudo to allow user to execute ipwcli.

- a. User visudo to edit the secure path.

```
# visudo
```

- b. Modify secure\_path to add path of ipwcli script:

```
Defaults secure_path="/usr/sbin:/usr/bin:/sbin:/bin:/opt/ipworks/cli/scripts"
```

- c. Append the following line to the file if it is not already present.

```
%<groupname> ALL=(root) NOPASSWD: /opt/ipworks/cli/scripts/ipwcli
```

For example, use the default group "ipworks":

```
%ipworks ALL=(root) NOPASSWD: /opt/ipworks/cli/scripts/ipwcli
```

- d. Close the text editor using the following command:

```
:wq
```

5. Add login privilege.

- a. Edit login privilege control file.

```
# vi /cluster/etc/login.allow
```





- b. For each user that needs to use the CLI, append the following line to allow login.

```
<username> control
```

6. Use the selected user to login to SC-1 and run the CLI with the sudo command.

```
# ssh <username>@<SC-1 Address>
```

```
<username>@SC-1:~> sudo ipwcli
```

## 2.2 Configuring Open Access

When a user is required to configure IPWorks to have open access, the user must modify the properties that are used to initialize the IPWorks Storage Server. Access to the `/opt/ipworks/ss/confs/ipworks_ss_defaults.conf` file, on the system where the server is running, or root privileges of the user are required.

The `/opt/ipworks/ss/confs/ipworks_ss_defaults.conf` file is a text file that contains settings. The following content is an example with default settings:

```
##### Authentication Properties #####
#
# These properties are used to configure how the server
# authenticates users that are trying to get access
# to the data.
#----- Auth.AllowAnonymous -----
# Indicates whether anonymous logins are allowed.
# This should be set to either "true" or "false".
# The default value is false.
#
Auth.AllowAnonymous=false
#----- Auth.RequirePasswords -----
# Indicates whether a user's password is required for
# authentication. This should be set to either "true"
# or "false". If set to false, users can omit their
# password when logging in.
# The default is true.
#
Auth.RequirePasswords=true
##### Access Control Properties #####
#
# These properties are used to configure how
# Access Control is enforced.
#----- AccessControl.Default -----
# Indicates the access control level to use if a
# user's ACL does not specify ALLOW or DENY.
# Possible values are:
# allow
# Allow access
# deny
# Do not allow access
```



```
# The default is deny.  
#  
AccessControl.Default=deny
```

To configure for open access, the properties shown in Table 1 must be set to the corresponding value.

Table 1 Open Access Properties

Property	Value
Auth.AllowAnonymous	true
Auth.RequirePasswords	false
AccessControl.Default	allow

The change in the settings takes effect after the IPWorks Storage Server is restarted.

## 2.3 Creating Users in CLI

To create a user in CLI, execute the following commands:

1. Log on the CLI as admin user.

```
IPWorks> Login: admin  
IPWorks> Password: <adminpassword>
```

2. Create a user in the CLI.

```
IPWorks> create user -set UserName=<username  
>;Password=<password>
```

3. Exit the CLI and use the created user to login to the CLI.

```
IPWorks> exit
```

## 2.4 Showing User Definition

The following example shows the definition of an admin user.

```
IPWorks> list user admin  
[User admin]  
  UserName: admin  
  Password: *****  
  Uid: admin  
  Profile: administrator  
  ChangePWFirstLogin: disable  
  ChangePWReset: disable  
  Locked: false
```



## 2.5 Configuring Profile

To create a profile, execute the following command:

```
IPWorks> create profile -set Name=<profilename>;EditRule  
="<permission> <type> [<action>]"
```

To configure an existing user with a profile, execute the following command:

```
IPWorks> mod user <username> -set profile=<profile>
```

## 2.6 Showing Profile Definition

The following example shows the definition of the standard profile for IPWorks.

```
IPWorks> list profile -format=verbose  
Profile: administrator  
Name: administrator  
EditRule: allow all  
Profile: reader  
Name: reader  
EditRule: deny all  
Profile: writer  
Name: writer  
EditRule: deny DnsOption  
EditRule: deny DhcpV4Option  
EditRule: deny User  
EditRule: deny Profile  
EditRule: allow all
```

## 2.7 Changing Password

To change the password, use the `changepassword` command.

After logging on the system for the first time, there is a prompt to have the user change the password.

When logging on IPWorks for the first time, the interaction is as follows:

```
IPWorks> Login:  
IPWorks> Password:  
Login to server successful.
```

Change Password : You are logging in for the first time

```
IPWorks> New Password:  
IPWorks> Confirm New Password:  
Working on 1 object(s).  
1 object(s) were updated.
```



After changing the user password, the password information in ECLI should also be updated accordingly:

```
>dn ManagedElement=1,IpworksFunction.ipworksRootId=1,Ipworks
CommonRoot=1,StorageServer=1,SSInterface=1
(SSInterface=1)>show -v
SSInterface=1
    address="169.254.100.23" <default>
    password="1:0eQ7mxBXFsID3yd+nX53FFBw8z3GaA5u"
    ssInterfaceId="1"
    username="admin" <default>
(SSInterface=1)>configure
(config-SSInterface=1)>password="admin456" cleartext
(config-SSInterface=1)>commit
(SSInterface=1)>
```

**Note:** If DNS is used, ssPassword of MO DnsSm must also be updated accordingly. For more information, refer to the step [Configure the MO of DNS Server Manager by using ECLI in IPWorks Initial Configuration](#).

## 2.8 Password Expiration Period

The password expiration period is 180 days by default. It is adjustable by the administrator in the configuration file `ipworks_ss.conf` file. A valid password expiration period is greater than or equal to 30 days.

The user is also prompted to change the password 7 days before expiration, as shown in the example below.

```
IPWorks> Login:
IPWorks> Password:
Login to server successful.
Your password expires in 7 days.
Use changepassword to change the password
```

If the password is not changed before the stipulated date and time, the account will be locked and only the Administrator can unlock it using the following command:

```
IPWorks>unlock user
Working on 1 object(s).
1 object(s) were updated.
```

To manually lock a user, the administrator has to use the same format as the example, but using the command `lock` instead of `unlock`.



## 2.9 Password Lock after Repeated Login Failure

To prevent password cracking, password locking is implemented in IPWorks. After 3 login failures, the system locks the password.

```
IPWorks> Login:  
IPWorks> Password:
```

```
Access Denied: Invalid username or password Your account  
will be locked after 3 unsuccessful login attempts
```





### 3 Creating A Global User

To create a global user:

- 1 Create a new user.

```
# useradd <username>
```

```
# passwd <username>
```

- 2 Create a new group (optional).

```
# groupadd <groupname>
```

- 3 Add each existing user to the primary group of the user.

```
# usermod -g <groupname> <username>
```

When adding new users, assign each user to the primary group.

```
# useradd -g <groupname> <username>
```

- 4 Make the new group global to the whole cluster.

```
# lde-global-user --user <username>
```

```
# lde-global-user --group <groupname>
```

- 5 Add login privilege.

- a Edit login privilege control file.

```
# vi /cluster/etc/login.allow
```

- b For each user that needs to use the CLI, append the following line to allow login.

```
<username> control
```

- 6 Use below command to check if the global user and group exist:

```
cat /cluster/etc/passwd |grep <user_name>
```

```
cat /cluster/etc/group |grep <group_name>
```







## Reference List

- [1] Trademark Information
- [2] Typographic Conventions
- [3] Glossary of Terms and Acronyms
- [4] [SUDO Website](#)
- [5] [IPWorks Initial Configuration](#), 5/1553-AVA 901 33/3 Uen