

IPWorks Authentication User Guide

USER GUIDE

Copyright

© Ericsson AB 2017, 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

1	Introduction	1
1.1	Prerequisites	1
1.1.1	Documentation	1
1.2	Related Information	1
2	Default Administrator User in IPWorks	3
3	Remote and Local User Authorization	5
4	Remote User Authentication	7
4.1	Create Emergency User	9
4.1.1	Add User for Standard Linux OS	9
5	Local User Authentication	11
	Reference List	13





1 Introduction

This document describes how to perform the IPWorks authentication procedure after IPWorks installation.

IPWorks provides the following authentication functions:

- Remote user authorization and authentication
- Local user authorization and authentication
- Security log management

The remote/local user access activity is recorded by the IPWorks security log. And the security log for DNS, ENUM, and SS can be generated as a local file or remote server log (with/without TLS). For information on how to configure IPWorks security log, refer to *IPWorks Security Log Management Guide*.

IPWorks supports remote user and local user access respectively through NETCONF, ECLI, and SFTP over SSH.

Note: Operator is free to apply either remote or local authentication method to each of the user account.

1.1 Prerequisites

This section describes the prerequisites which must be fulfilled before starting IPWorks Authentication feature.

1.1.1 Documentation

Before starting the IPWorks Authentication, ensure that the document *Security Management for ECLI, NETCONF, and SFTP Users* is available and understandable.

1.2 Related Information

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

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





2 Default Administrator User in IPWorks

After IPWorks initial installation, a default administrator user (username: `la-admin`, password: `123456`) is available. This user has authorization to create, modify, or delete other users. It is recommended to modify the default administrator password before IPWorks system is in operation. For more information about how to modify password of default administrator, refer to *Reset Password for User Account*.





3 Remote and Local User Authorization

This section describes the default roles of the IPWorks system. These roles are applicable for both remote and local authorization.

Four default roles described in Table 1, are defined to support remote/local user Authorization in IPWorks. Accounts are authorized with specified role. For more information about the default roles, refer to *Security Management for ECLI, NETCONF, and SFTP Users*.

Table 1 Description of default role

Default Role	Description
System Administrator	Responsible for the administration of all non-security-related attributes and capabilities of an ME, including features, configuration parameters, and monitoring
System Security Administrator	Responsible for the administration of all security-related attributes and capabilities of an ME, including user accounts and authorizations
Managed Function Application Administrator	Responsible for the administration of all non-security-related attributes and capabilities of the Managed Function, including features, configuration parameters, and monitoring
Managed Function Application Operator	Can view some non-security-related attributes and capabilities of the Managed Function, including features, configuration parameters, and monitoring





4 Remote User Authentication

The remote user initiates an ECLI, NETCONF, or SFTP session over SSH to the ME and triggers a user LDAP authentication from the ME. To configure remote user authentication, do the following:

1. Create emergency user

See Section 4.1 on page 8

2. Configure remote LDAP server

Refer to *LDAP-Based Authentication and Authorization Interface*

Note: The configuration on the remote LDAP server is out of the scope of this document.

From Step 3 to Step 4, you can see the steps to configure IPWorks.

3. To set LDAP authentication parameters, do the followings:

- a. Log on to the ECLI on the active SC with the user.

```
ssh <user name>@<SC_MIP> -t -s cli
```

- b. Navigate to the LDAP managed object, for example:

```
>dn ManagedElement=<node name>,SystemFunctions=1,SecM=1,UserManagement=1,LdapAuthenticationMethod=1,Ldap=1
```

- c. Enter configuration mode:

```
(Ldap=1)>configure
```

- d. Set the base DN to be used for user authentication to the LDAP target, for example:

```
(config-Ldap=1)>baseDn="dc=my-domain,dc=com"
```

- e. Set the ldapIpAddress for user authentication to the LDAP target, for example:

```
(config-Ldap=1)>ldapIpAddress=192.0.2.10
```

- f. Set the value of useTls to false.

```
(config-Ldap=1)>useTls=false
```

- g. Commit the settings:



```
(config-Ldap=1)>commit
```

h. Verify the result:

```
(Ldap=1)>show
```

The following is an example output:

```
Ldap=1
  baseDn="dc=my-domain,dc=com"
  bindDn="cn=proxyaccount,dc=ericsson,dc=com"
  bindPassword="1:PLDGCpRMq16BVyHxsZSp4dNvsCA2u6ED"
  fallbackLdapIpAddress=[] <empty>
  filterType=[] <empty> <deprecated>
  ldapId="1"
  ldapIpAddress="192.0.2.10"
  nodeCredential=[] <empty>
  nodeType=[] <empty> <deprecated>
  profileFilter=[] <empty>
  roleAliasesBaseDn=[] <empty> <deprecated>
  serverPort=[] <empty>
  tlsCaCertificate=[] <empty> <deprecated>
  tlsClientCertificate=[] <empty> <deprecated>
  tlsClientKey=[] <empty> <deprecated>
  tlsMode=STARTTLS <default>
  trustCategory=[] <empty>
  useReferrals=false <default>
  userLabel="LDAP based login authentication"
  useTls=false
  useTlsFallback=false <default> <deprecated>
  EricssonFilter=1
  Filter=1
```

Note: This is only a simple configuration. For more parameters that are listed in the above output, can be used according to descriptions in MO *Ldap*.

4. Enable Remote authorization, refer to *Unlock LDAP Authentication Method*.

If password-based simple bind is required for LDAP authentication, refer to *Change Bind Name and Password for LDAP Authentication*.

If TLS is required for LDAP authentication, refer to *Change Certificate Settings for LDAP TLS*.

If Target-Based Access Control is required for LDAP authentication, refer to *Configure Target-Based Access Control*.

Note: Remote authorization can be disabled, refer to *Lock LDAP Authentication Method*.



4.1 Create Emergency User

At least one emergency user must be created. This user is used when access to the system or to the centralized user management database is lost due to a configuration mistake or communication problems. For example, when LDAP server is unreachable or inactive, or connection between IPW and LDAP Server has broken, then operator is able to use emergency group account for operation. In this situation, You can use local Linux users that belong to the `com-emergency` Linux group to establish authentication locally and get complete Management Information Base (MIB) access through the ECLI or NETCONF.

Note: How many emergency users that are created, and for whom, is deployment-specific. For example, one user for operator personnel and one for Ericsson support personnel can be created.

4.1.1 Add User for Standard Linux OS

To add a user to the `com-emergency` group for the standard Linux® Operating System (OS):

1. Log on to one of the SCs as root:

```
ssh -l <user> <address>
```

2. Add a user account.

```
useradd -G com-emergency <account>
```

An account according to the defaults of `/etc/default/useradd` is created. The account is added to the `com-emergency` group.

3. Set password for the user account.

```
passwd <account>
```

The system prompts the user for a password and asks the user to repeat the selected password once more.

4. Log off from the SC.

```
exit
```

5. Log on to the other SC as root.

```
ssh -l <user> <address>
```

6. Add the same user account as in Step 2.

```
useradd -G com-emergency <account>
```

An account according to the defaults of `/etc/default/useradd` is created. The account is added to the `com-emergency` group.



7. Set the same password for the user account as in Step 3.

```
passwd <account>
```

The system prompts the user for a password and ask the user to repeat the selected password once more.

8. Insert *<account> all* into the file `/cluster/etc/login.allow`.
9. Log off from the SC.

```
exit
```



5 Local User Authentication

This section describes the procedures on how to configure local user authentication.

1. Log on to the ECLI on the active SC with the `la-admin`.

```
ssh la-admin@<SC_MIP> -t -s cli
```

2. Create password policy, refer to *Create Password Policy*.
3. Create account policy, refer to *Create Account Policy*.
4. Create user account, refer to *Create User Account*.

The created user account can access to the OS.

5. Enable local authorization, refer to *Unlock Local Authorization Method*.
6. Enable user account, refer to *Unlock Administrative Lock for User Account*.

Note:

- The created user account can access to the OS.
- Local authorization can be disabled, refer to *Lock Local Authorization Method*.





Reference List

- [1] *Reset Password for User Account*
- [2] *Security Management for ECLI, NETCONF, and SFTP Users*
- [3] *LDAP-Based Authentication and Authorization Interface*
- [4] *Change Bind Name and Password for LDAP Authentication*
- [5] *Change Certificate Settings for LDAP TLS*
- [6] *Create Password Policy*
- [7] *Create Account Policy*
- [8] *Create User Account*
- [9] *IPWorks Security Log Management Guide*
- [10] *Unlock Administrative Lock for User Account*
- [11] *class Ldap*
- [12] *Configure Target-Based Access Control*
- [13] *Unlock LDAP Authentication Method*
- [14] *Lock LDAP Authentication Method*
- [15] *Unlock Local Authorization Method*
- [16] *Lock Local Authorization Method*