

iPECS

iPECS UCM

Security Configuration Manual

Please read this manual carefully before operating System.
Retain it for future reference.

iPECS is an Ericsson-LG Brand



Revision History

ISSUE	DATE	DESCRIPTION OF CHANGES
1.0	2017/11/14	Initial Release
1.1	2017/12/08	General Update(SW version 2.0)
1.2	2019/03/11	SW version: 2.5.x. - General Update

Copyright© 2017 Ericsson-LG Enterprise Co., Ltd. All Rights Reserved

This material is copyrighted by Ericsson-LG Enterprise Co. Ltd. Any unauthorized reproductions, use or disclosure of this material, or any part thereof, is strictly prohibited and is a violation of Copyright Laws.

Ericsson-LG Enterprise reserves the right to make changes in specifications at any time without notice.

The information furnished by Ericsson-LG Enterprise in this material is believed to be accurate and reliable, but is not warranted to be true in all cases.

Ericsson-LG Enterprise and iPECS are trademarks of Ericsson-LG Enterprise Co., Ltd.

Table of Contents

1 Introduction	1
2 Security configuration in CentOS	2
2.1 Change root and user password.....	2
2.2 Configuring ACL of SSH.....	3
2.3 Change SAMBA password	4
2.4 Configuring ACL of SAMBA.....	4
3 Change WMS Password	5
4 ACL Settings on WMS.....	6
4.1 Setting ACL lists	6
4.2 Applying ACL rules	7
4.3 Application of WAN/LAN Network.....	8
5 Restriction of SIP Registration	9
5.1 SIP Restriction Management.....	9
5.2 SIP Restriction Information.....	10
5.3 Authentication password setting of SIP phone	11
5.4 407 Authentication setting of SIP phone.....	12
5.5 Access restriction for individual user	13
5.6 Deletion unused SIP account	13
6 HTTPS Setting	14
7 DISA settings.....	14

1 Introduction

When the system is connected to the public network, it's vulnerable to the hacking for the malicious purpose. If the root password is cracked or leaked, the system can be infected by any computer virus or backdoor program . In this case the system can be reset during operation or voice quality may be affected by high traffic of the hidden program.

To protect this malicious access to the system, it's required to change default password and restrict access from unauthorized IP address.

This document explain how to change settings regarding security options such as:

- Security options in CentOS
- Security options in WMS
- Security options for SIP Signaling

It's strongly recommended to change the following passwords and IP filtering rule in the installation stage.

- Root password of shell login
- Samba password
- WMS password
- IP Filtering for ssh, samba service

Even after configuring ACL(Access Control List) in UCM system by WMS & Linux OS Command and changing above Default password with Strong password, UCM system can't protect Flooding & DDoS Attack and UCM System may can't operate properly. So, the installation of Firewall and SBC device is also strongly recommended.

2 Security configuration in CentOS

2.1 Change root and user password

This chapter explains how to change system password for the protection from illegal access. It's very strongly recommended that the new password is set on the condition of the followings.

Recommendations for strong password :

- 1) It should be at least 9 characters.
- 2) It should include 3 or more types of the following categories.
 - uppercase letters, lowercase letters, number, and special character
- 3) It should not contain user name and real name and company name.
- 4) It should not contain a complete word.
- 5) It should not include same or sequential numbers (ex, 123..., 111..., abc....)

Notice)

Please be careful not to forget new password.

To change password

- 1) Connect to the server through SSH as a root
- 2) Change "root" password

root@CentOS58 /root \$ passwd	→ <i>Type This command</i>
Changing password for user root.	
New UNIX password:	→ <i>Type "strong password"</i>
Retype new UNIX password:	→ <i>Confirm the password</i>
passwd: all authentication tokens updated successfully.	

- 3) change "ipeccsm" user password

root@CentOS58 /root \$ passwd ipeccsm	→ <i>Type This command</i>
Changing password for user ipeccsm.	
New UNIX password:	→ <i>Type "strong password"</i>
Retype new UNIX password:	→ <i>Confirm the password</i>
passwd: all authentication tokens updated successfully.	

2.2 Configuring ACL of SSH

Networking **access control list**(ACL) is a list of permission to access to the system. It allows only listed IP address to connect to the system and it can prevent illegal access to the system from any unauthorized IP address.

The **TCP wrapper** is running on the system and it works as a firewall to prevent the malicious access.

SSH IP Filtering

- 1) Connect to the server through SSH as a root
- 2) Edit deny rules
 - Open deny configuration file (/etc/hosts.deny)
: If it finds a matching rule, it denies the connection
 - Add this line, "sshd:ALL"
: All packet for SSH connection will be dropped.

```
root@CentOS58 ~ $ vim /etc/hosts.deny
sshd:ALL
```

Notice)

Please keep in mind to assign the IP address of management PC to allow list. If any IP is not defined in allow list, all the connection will be rejected. The ACL rule would be applied from new session.

- 3) Edit allow rules
 - Open allow configuration file (/etc/hosts.allow)
: If it finds a matching rule, it accept the connection
 - Add this line, "sshd:<authorized IP>"
: SSH connection will be accepted only from the authorized IP address.

ex1) only 1 IP allow: 192.168.122.190

```
root@CentOS58 ~ $ vim /etc/hosts.allow
sshd:192.168.122.190
```

ex2) Two IP allow: 192.168.122.190, 192.168.122.191

```
root@CentOS58 ~ $ vim /etc/hosts.allow
sshd:192.168.122.190, 192.168.122.191
```

ex3) Local Subnet allow: 192.168.122.0/24

```
root@CentOS58 ~ $ vim /etc/hosts.allow
sshd:192.168.122.
```

← it contains period at the end position.

2.3 Change SAMBA password

This chapter explains how to change password of SAMBA for accessing from Windows PC.

Refer to Chapter 2.1 for the strong password.

To change password

- 1) Connect to the server through SSH as a root
- 2) Change password

root@CentOS58 ~ \$ smbpasswd -a ipecsucm	→ <i>Type this command</i>
New SMB password:	→ <i>Type "strong password"</i>
Retype new SMB password:	→ <i>confirm the password</i>

2.4 Configuring ACL of SAMBA

This chapter explains how to configure authorized IP address of SAMBA for accessing to the system directory from Windows PC.

SAMBA IP Filtering

Edit allow rules are as below

- 1) Open allow configuration file (/etc/samba/smb.conf)
- 2) Find the line "# hosts allow =" in the "[global] section, and edit this line
- 3) Remove #, # means omitting this line when the samba service is initialized.
: The packet for Samba connection from authorized IP will be accepted.

ex1) only 1 IP allow: 192.168.122.190

root@CentOS58 ~ \$ vim /etc/samba/smb.conf
hosts allow = 192.168.122.190

ex2) Two IP allow: 192.168.122.190, 192.168.122.191

root@CentOS58 ~ \$ vim /etc/samba/smb.conf
hosts allow = 192.168.122.190 192.168.122.191

ex3) Local Subnet allow: 192.168.122.0/24

root@CentOS58 ~ \$ vim /etc/samba/smb.conf
hosts allow = 192.168.122. ← <i>it contains period at the end position.</i>

SAMBA Service Restart

For applying these configuration, the samba service should be restarted.

- 1) Connect to the server through SSH as a root
- 2) Type the following command to restart SAMBA service

root@CentOS58 ~ \$ service smb restart

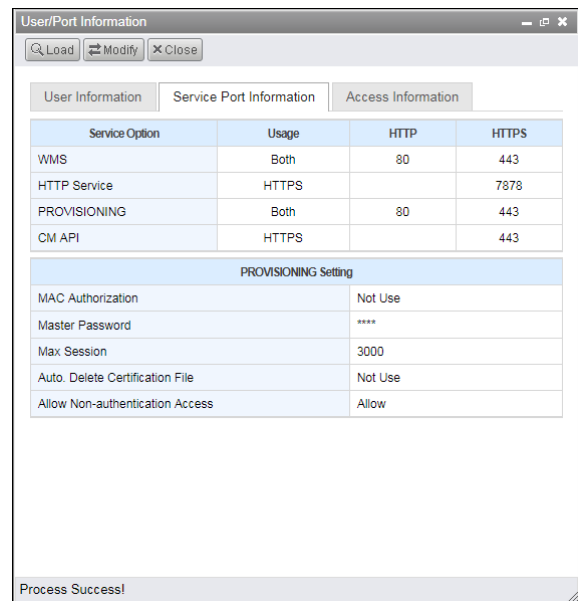
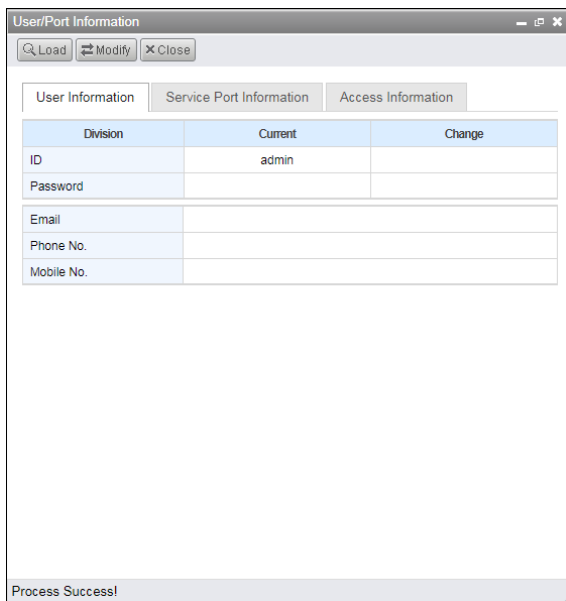
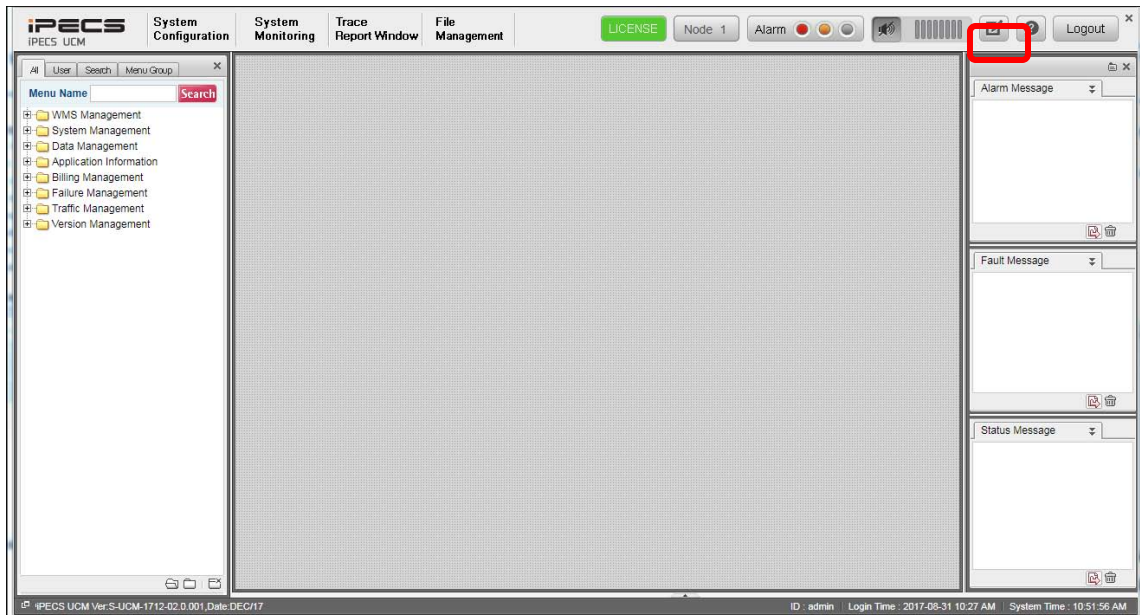
3 Change WMS Password

It's strongly recommended to change default password of WMS to protect the system and user data.

To change password

After login Admin & Maintenance account, you can change the password in User/Port Info menu of the upper right. When you change the password, it requires strong password as follows from version 5.5. When you login at the first time to the WMS, it requires to change password.

- 1) The length should be at least 9 characters.
- 2) It should contains 3 or more types of the categories.(uppercase letters, lowercase letters, number, and special character)
- 3) It should not include 3 serial number of serial same number (ex, 123..., 111..., abc....).



4 ACL Settings on WMS

4.1 Setting ACL lists

It's explained how to configure access restriction of SSH and SAMBA in Chapter 2. This chapter explains how to reject the other protocols in addition.

ACL in WMS works based on white list and all the services are restricted except one defined to use on the menu below.

To Set ACL in WMS

- 1) Login with admin account to WMS to set ACL list, user account can't access to the menu.
: System Management → ACL Information
- 2) Press "Add" button to add new rule.
- 3) Input the following data.
 - Enter individual IP address or IP range.
 - Select coverage. LAN or WAN
 - Select the "Service All" option.

If you want to use specific protocol, set "Service All" to "Use Part" and select protocol.

ACL Information > Add			
IP Address	192.168.122.0/24	LAN / WAN	LAN
Service All	Use All	Description	
Service Name	Protocol	Port	Usage
ICMP	ICMP	0	Not Use
TELNET	TCP	23	Not Use
SSH	TCP	22	Not Use
FTP	TCP	1022	Not Use
HTTP	TCP	80	Not Use
SNMP	TCP	161	Not Use
	TCP		Not Use
	TCP		Not Use
	TCP		Not Use
	TCP		Not Use

To check ACL with CLI

- 1) Connect to the server through SSH as a root
- 2) Type command "iptables -L"
- 3) The following line will be added in the location "Chain INPUT"

ACCEPT all -- 192.168.122.0/24 anywhere

```

root@CentOS58 ~ $ iptables -L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 192.168.122.0/24 anywhere
    
```

Cautions)

- If you use ACL settings without any allowed IP address, all the access from any G/W, IP phone, PC is denied.
- When access from OAM PC is restricted, you have to delete ACL list with CLI (console command)

```
root@CentOS58 ~ $ iptables -P INPUT ACCEPT
```

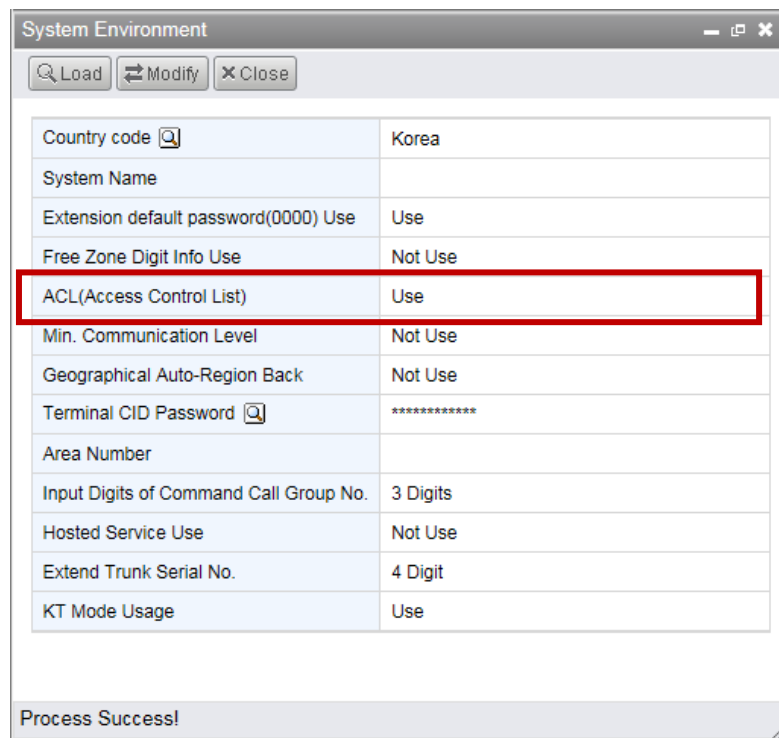
4.2 Applying ACL rules

This chapter explains how to apply ACL rules defined in WMS. If ACL option is set to “Use”, all the services will be rejected except that defined to use in Chapter 4.1.

To Apply ACL in WMS

When you complete to set the ACL list, select ACL option “Use” to apply the ACL rules.

: System Management → System Environment -> ACL(Access Control List)



To check ACL option with CLI

- 1) Connect to the server through SSH as a root
- 2) Type command “iptables -L”

```
root@CentOS58 ~ $ iptables -L
```

```
Chain INPUT (policy DROP)
```

→ If it's “DROP”, it means “Not Use”.

```
root@CentOS58 ~ $ iptables -L
```

```
Chain INPUT (policy ACCEPT)
```

→ If it's “ACCEPT”, it means “Use”.

4.3 Application of WAN/LAN Network

You can set to not apply the ACL for the device which is connected to LAN port

Access from WAN is restricted but only access from LAN is allowed

ACL Information

Load Modify Add Delete Close

Total Count 8

<input checked="" type="checkbox"/>	Index	IP Address	LAN / WAN	Service All	Description	Service (Service Name / Protocol / Port / Usage)								
<input type="checkbox"/>	1	10.0.0.0/8	LAN	Use All		ICMP	0	Not Use	TELNET	23	Not Use	SSH	22	Not Use
						FTP	1022	Not Use	HTTP	80	Not Use	SNMP	161	Not Use
<input type="checkbox"/>	2	11.150.0.0/16	LAN	Use All		ICMP	0	Not Use	TELNET	23	Not Use	SSH	22	Not Use
						FTP	1022	Not Use	HTTP	80	Not Use	SNMP	161	Not Use

| 01 |

Process Success!

5 Restriction of SIP Registration

5.1 SIP Restriction Management

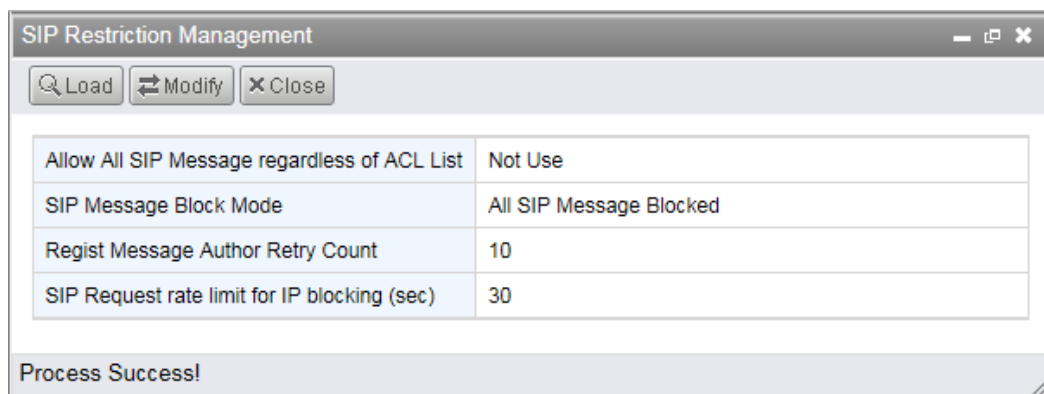
iPECS UCM supports to restrict any illegal access or flooding attack of SIP message.

Blocking based on ACL

SIP signaling is allowed based on ACL configuration, so it require to set ACL options. All the terminal IP address should be contained in ACL allow list. ACL setting is referred in chapter 4.1 and chapter 4.2.

Blocking based on IP address

- 1) SIP Message Block Mode
 - All SIP Message Blocked : If IP address of current message is different with the IP address previously received, the REGISTER message is dropped and any message is not responded.
 - All SIP Message Blocked Except REGISTER : If IP address of current message is different with the IP address previously received, only REGISTER message is allowed and other messages are dropped.
 - All SIP Message Allowed ; Allow all messages to receive.
- 2) Register Message Author Retry Count : 10~100, default value is 30
When Registration Request fail count is over this value with the reason of password mismatch or undefined number, the IP address is restricted. You can check the restricted IP address on the menu "SIP Restriction Information".
- 3) SIP Restriction Count for Registration(sec) : 1~200, default is 10.
This option is for checking REGISTER flooding. If REGISTER message is flooded more than this count in a second, the IP address is added to restriction list. You can check the restricted IP address on the menu "SIP Restriction Information".



5.2 SIP Restriction Information

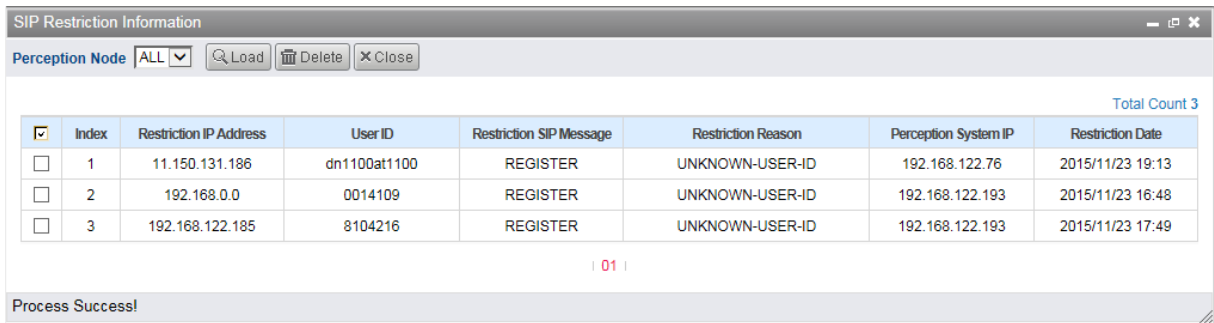
This menu shows the restricted IP addresses with the reason. The administration can release the restricted IP address with deleting from the list.

Restriction Reason

- Unknown IP : The IP of the terminal is different with first registered.
- Unknown user ID : User ID is not defined.
- Unknown auth ID/PW : Password mismatch
- Terminal type mismatch : The User-Agent and terminal type is not matched.
- Heavy Traffic : It's restricted by SIP flooding

Caution)

- If specific SIP phone fails to register to the system, please check the IP is restricted.
- If the terminal is behind NAT or LCM, please use "All SIP Message Blocked Except REGISTER" instead of "All SIP Message Blocked"



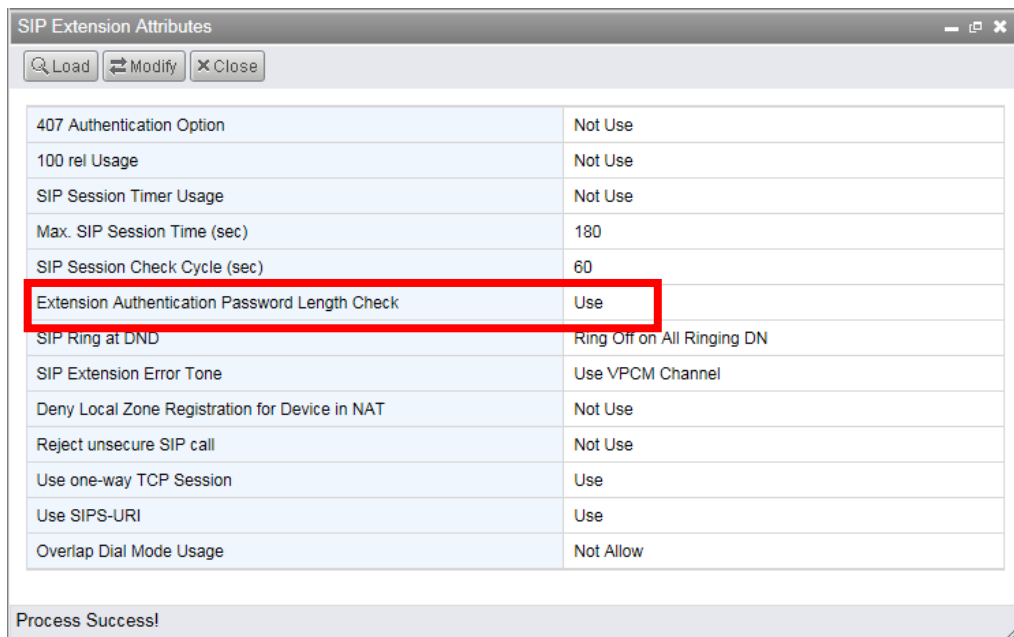
The screenshot shows a window titled "SIP Restriction Information". At the top, there is a "Perception Node" dropdown menu set to "ALL", and buttons for "Load", "Delete", and "Close". Below this is a table with 8 columns: Index, Restriction IP Address, User ID, Restriction SIP Message, Restriction Reason, Perception System IP, and Restriction Date. The table contains 3 rows of data. A "Total Count 3" label is visible in the top right corner of the table area. Below the table, there is a status bar that says "Process Success!".

<input checked="" type="checkbox"/>	Index	Restriction IP Address	User ID	Restriction SIP Message	Restriction Reason	Perception System IP	Restriction Date
<input type="checkbox"/>	1	11.150.131.186	dn1100at1100	REGISTER	UNKNOWN-USER-ID	192.168.122.76	2015/11/23 19:13
<input type="checkbox"/>	2	192.168.0.0	0014109	REGISTER	UNKNOWN-USER-ID	192.168.122.193	2015/11/23 16:48
<input type="checkbox"/>	3	192.168.122.185	8104216	REGISTER	UNKNOWN-USER-ID	192.168.122.193	2015/11/23 17:49

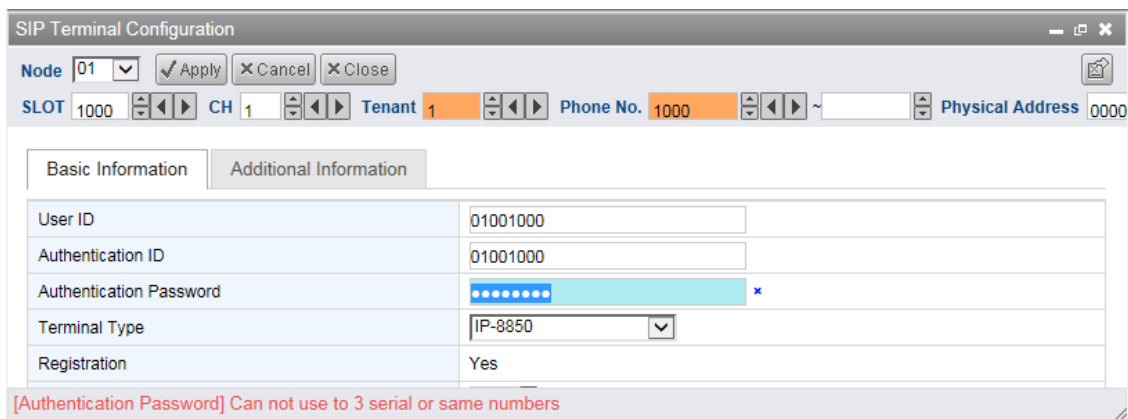
5.3 Authentication password setting of SIP phone

It's recommended to use strong password for SIP authentication password. When the following option is enabled, the system will check if password is valid or not depending on the following conditions.

- 1) The length should be at least 6 characters.
- 2) It should contains 3 or more types of the categories.(uppercase letters, lowercase letters, number, and special character)
- 3) It should not include 3 serial number of serial same number (ex, 123..., 111..., abc....).
- 4) Never use a password same as station number or user id.



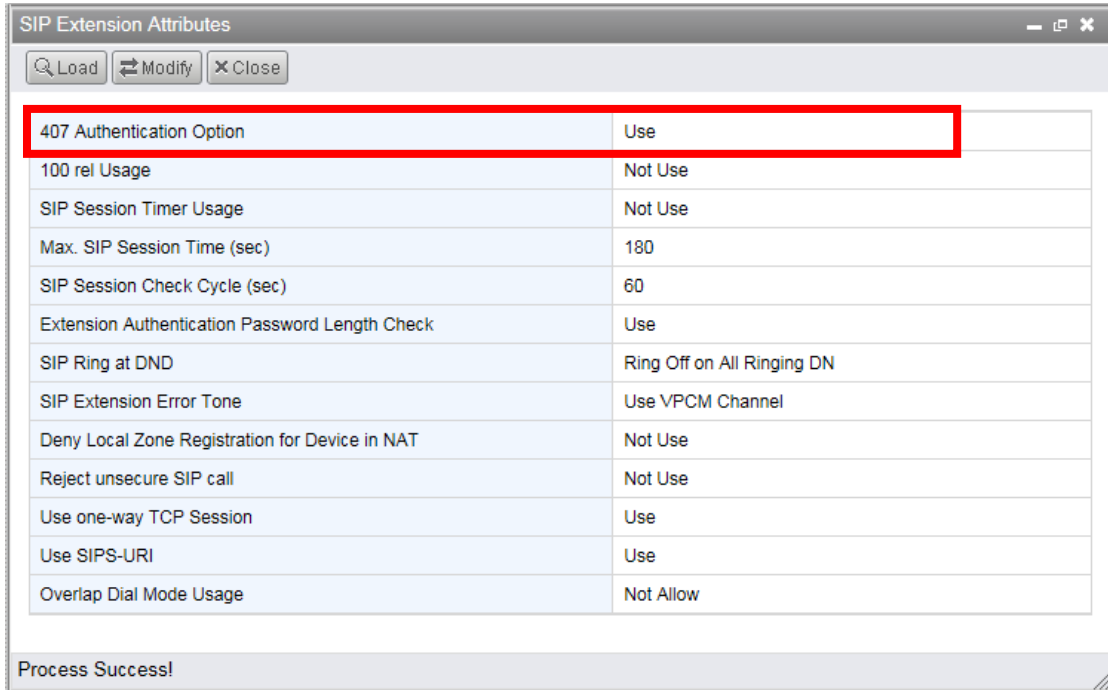
Ex) Sequential number is denied.



5.4 407 Authentication setting of SIP phone

It's recommended to set "407 Authentication Option" to "Use" for checking authentication for all the outgoing calls.

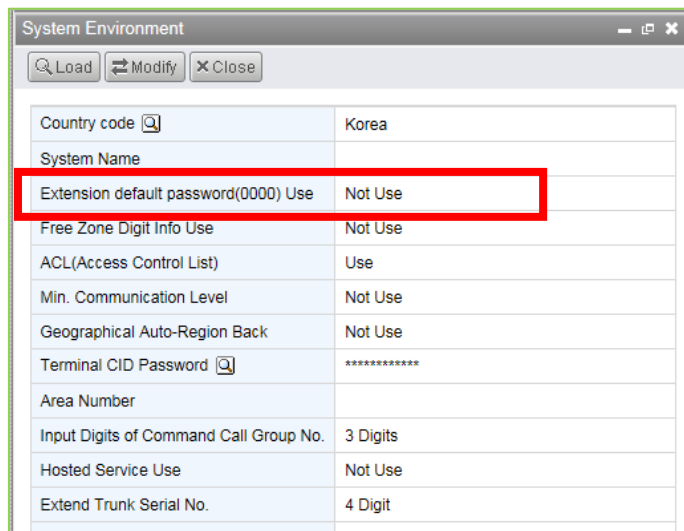
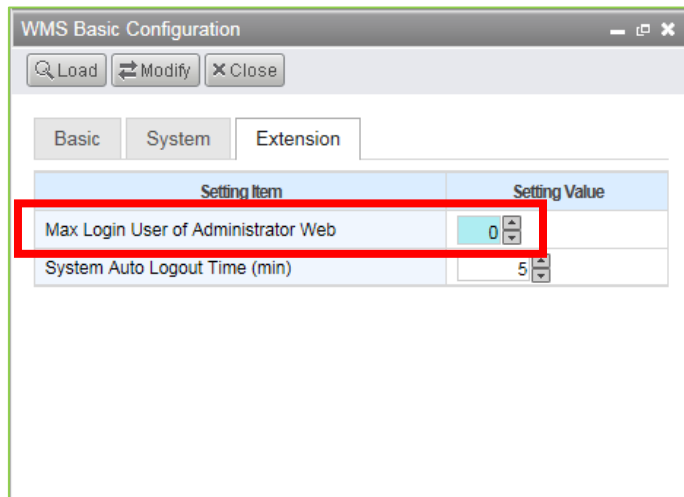
If it's set to "Use", iPECS UCM will send 407 for Invite request.



5.5 Access restriction for individual user

iPECS UCM supports that users change their own data of call features from Web admin. But if it's not necessary, change any individual users not to allow to the Web admin. Or change not to use default password for Web admin.

- Restrict individual user web access
 - Set "Max Login User of Extension User Web" of "WMS Basic Configuration" to "0."
- Don't use default password
 - Set "Extension default password(0000) Use" of "System Environment" to "Not Use"



5.6 Deletion unused SIP account

It's recommended not to create unused SIP account for prevent hacking. If the user id and password is leaked, it can be used maliciously.

6 HTTPS Setting

When system use https, connect to “https://xxx.xxx.xxx.xxx/” to access WMS.

Service Option	Usage	HTTP	HTTPS
WMS	HTTPS		443
HTTP Service	HTTPS		7878
PROVISIONING	HTTPS		443

PROVISIONING Setting

MAC Authorization	Not Use
Master Password*
Max Session	3000
Auto. Delete Certification File	Not Use
Allow non-authentication access	Allow

7 DISA settings

DISA(Direct Inward System Access) is used for external subscriber to use DDD/ISD call through system access, but if not use DISA feature set “DISA Transit” to “Deny” or “Authorization for DISA Transit” to “Use”

	Day	Night	Timed
Trunk Call Routing Table			
DISA Transit	Deny	Deny	Deny
Authorization for DISA Transit	Use	Use	Use
DISA Retry Count	3	3	3
Multi Ring No Answer Time (sec)	0	0	0
Trunk Call Routing Table for Multi Ring No Answer			

Process Success!

Thanks for purchasing iPECS System

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

iPECS is an Ericsson-LG Brand

