Grandstream Security Bulletin
GS20-UCM005 - Important

Security Vulnerability Associated with Unauthenticated Password Retrieval

Revision: 1.2

Published: Tuesday, April 14, 2020
Updated: Thursday, April 23, 2020

Summary

This security bulletin describes a vulnerability in the Grandstream UCM61xx/62xx/6510 series IP PBX appliances that could allow malicious users to obtain user passwords. Solutions and guidelines are also provided with details.

Description

Grandstream received reports of SQL injections that could allow malicious unauthenticated users to retrieve the passwords of created users from the UCM61xx/62xx/6510 series IP PBX appliances with firmware 1.0.20.20 or older for UCM62xx/6510 and firmware 1.0.18.17 or older for UCM61xx. When certain actions are invoked on specific ports, the related modules will be vulnerable to the aforementioned SQL injections and brute force attacks.

Affected Models

The following models have been known to be affected by this issue:

- UCM6102
- UCM6104
- UCM6108
- UCM6116
- UCM6202
- UCM6204
- UCM6208
- UCM6510

Affected Firmware

For UCM6202/6204/6208/6510, firmware 1.0.20.20 or lower versions are affected.

For UCM6102/6104/6108/6116, firmware 1.0.18.17 or lower versions are affected.

* If your UCM is on a test build or a Beta firmware, it is most likely affected as well.

Solution/Recommendation:

For UCM6202/6204/6208/6510, firmware 1.0.20.22 has patched this security vulnerability. The current official firmware 1.0.20.23 contains the security patch and fixes a major crash issue.

Grandstream strongly recommends all UCM62xx/6510 to be upgraded to the current official firmware 1.0.20.23 **IMMEDIATELY**.

For UCM6102/6104/6108/6116, firmware 1.0.18.18 has patched this security vulnerability. Grandstream strongly recommends all UCM61xx to be upgraded to the current official firmware 1.0.18.18 **IMMEDIATELY**.

After upgrading, please read the following security guidelines and take action immediately.

Security Guidelines

Due to the various possible environments UCMs can be deployed in, some UCMs may be less at risk than others. Please see the following recommendations for different types of environments:

- If any of the following are applicable:
  - UCM can only be accessed from internal network.
  - UCM is behind a firewall and can only be accessed via VPN.
  - On UCM web UI->System Settings->HTTP Server, “Enable IP Address Whitelist” is turned on with permitted IP configured to limit web access.

  The UCM is at low risk of being hacked.

  Recommended actions:

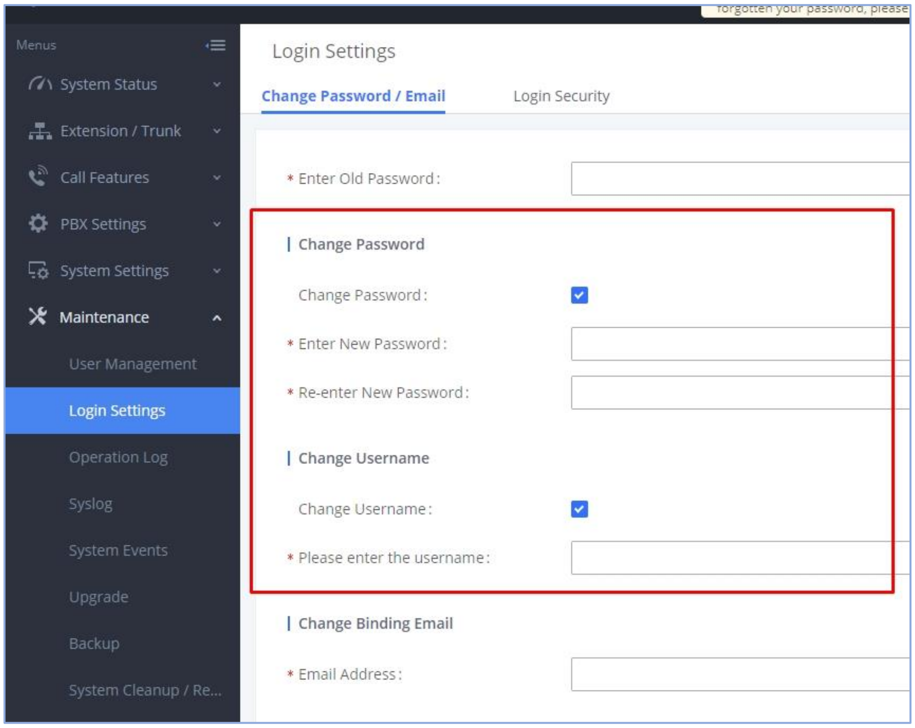
  1. Upgrade UCM62xx/6510 to firmware 1.0.20.23; upgrade UCM61xx to firmware 1.0.18.18.
  2. Change the passwords for super admin and admin users under UCM web UI->Maintenance->User Management page.

- If the UCM can be accessed from external network via port forwarding or is placed directly on a public network without enabling IP address whitelist and configuring permitted IP, the UCM IP address and port information can be discovered easily. The UCM is at high risk of being hacked.

  Recommended actions:

  1. **Upgrade UCM62xx/6510 to firmware 1.0.20.23; upgrade UCM61xx to firmware 1.0.18.18.**

2. **Change the super admin and admin <u>usernames</u> and <u>passwords</u> under UCM web UI->Maintenance->User Management page.** If any unknown users with admin privileges or custom privileges are found in the User Management page, please delete them immediately.



Login Settings

* Enter Old Password :

| Change Password

Change Password : ☑

* Enter New Password :

* Re-enter New Password :

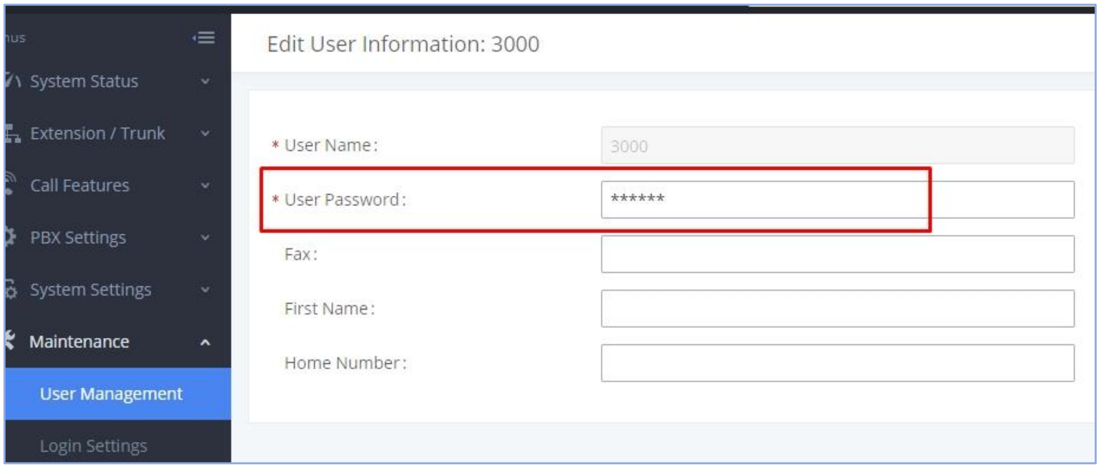
| Change Username

Change Username : ☑

* Please enter the username :

| Change Binding Email

* Email Address :



Edit User Information: 3000

* User Name : 3000

* User Password : ******

Fax :

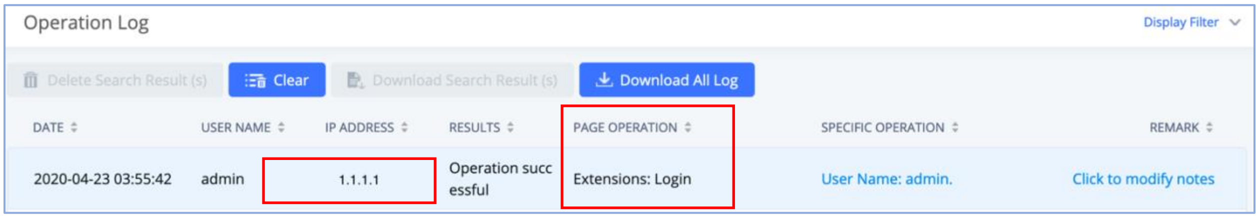
First Name :

Home Number :

3. **Check for suspicious activity in the Operation Log.**

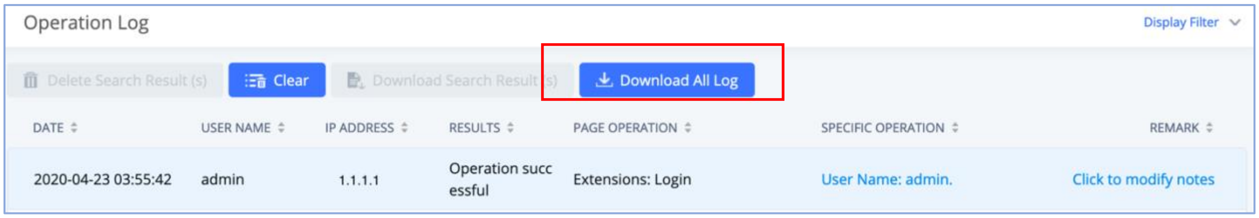
   (1) Navigate to UCM web UI->Maintenance->Operation Log page and look for any activity related to logins by examining the “Page Operation” column information.

- For UCM62xx/6510, please look for “Extensions: Login” actions and check the IP addresses the actions were taken from.



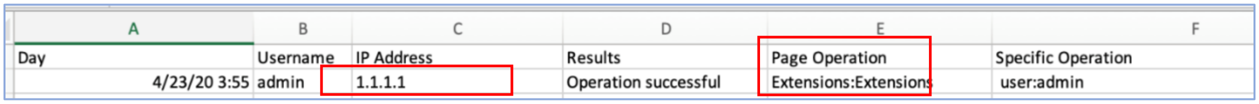
DATE	USER NAME	IP ADDRESS	RESULTS	PAGE OPERATION	SPECIFIC OPERATION	REMARK
2020-04-23 03:55:42	admin	1.1.1.1	Operation successful	Extensions: Login	User Name: admin.	Click to modify notes

Additionally, users can also click on “Download All Log” to get a CSV file. Within the CSV file, search for “Extensions:Extensions” and check the IP addresses the actions were taken from.



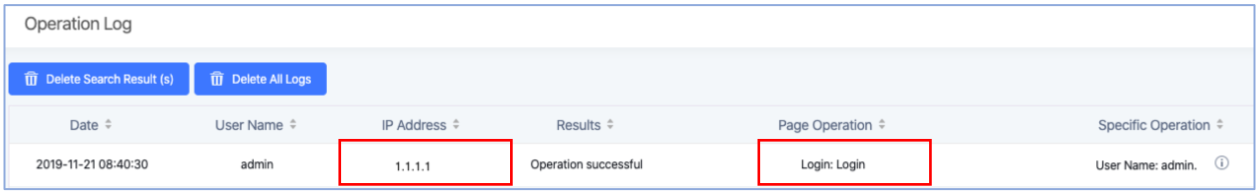
DATE	USER NAME	IP ADDRESS	RESULTS	PAGE OPERATION	SPECIFIC OPERATION	REMARK
2020-04-23 03:55:42	admin	1.1.1.1	Operation successful	Extensions: Login	User Name: admin.	Click to modify notes

In the CSV file:



A	B	C	D	E	F
Day	Username	IP Address	Results	Page Operation	Specific Operation
4/23/20 3:55	admin	1.1.1.1	Operation successful	Extensions:Extensions	user:admin

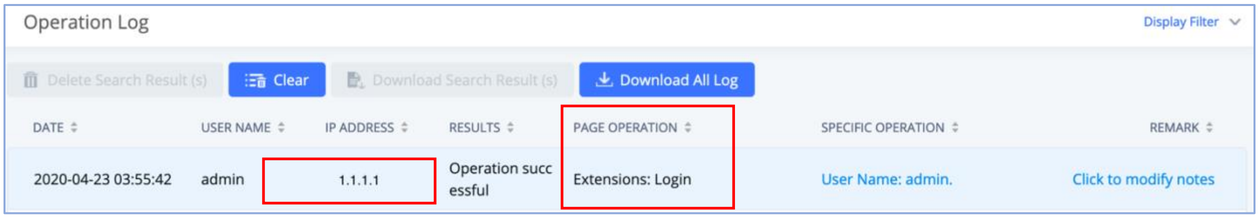
- For UCM61xx, please look for “Login” or “Login: Login” in “Page Operation” column, and check the IP addresses the actions were taken from.



Date	User Name	IP Address	Results	Page Operation	Specific Operation
2019-11-21 08:40:30	admin	1.1.1.1	Operation successful	Login: Login	User Name: admin.

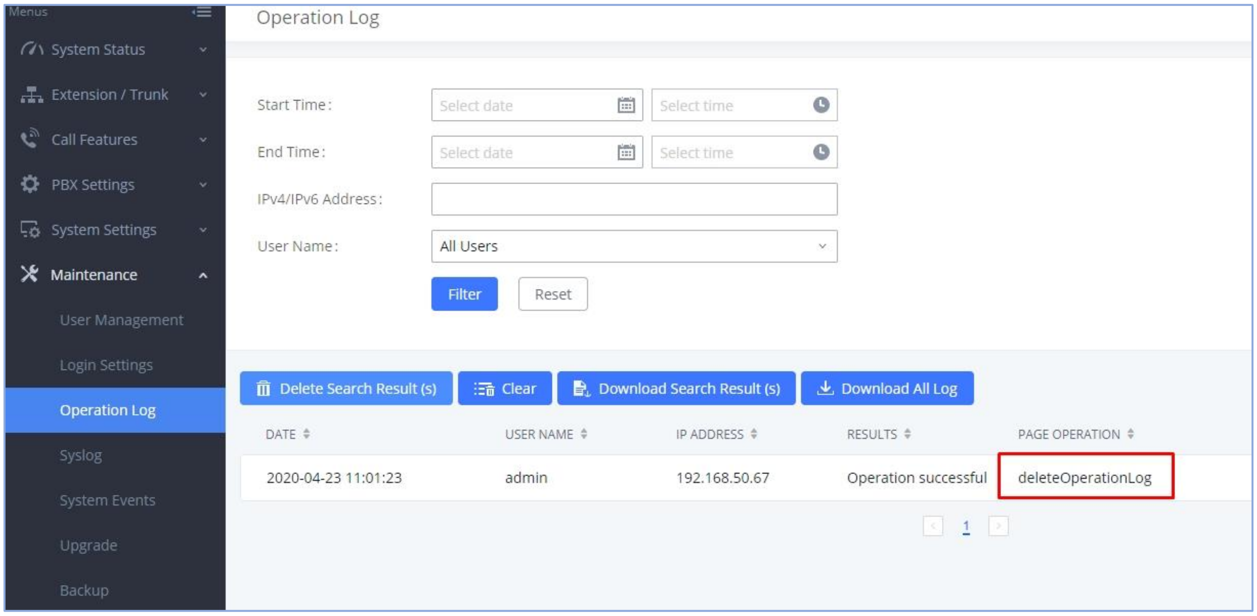
Check if there are unknown IP addresses that have logged in successfully in Operation Log.

For example, if 1.1.1.1 is an unknown IP address, and the Operation Log shows a successful login from it, it is most likely a malicious user who has obtained the password for the username it used. In this case, the password for admin has been compromised.



DATE	USER NAME	IP ADDRESS	RESULTS	PAGE OPERATION	SPECIFIC OPERATION	REMARK
2020-04-23 03:55:42	admin	1.1.1.1	Operation successful	Extensions: Login	User Name: admin.	Click to modify notes

(2) Look for any "deleteOperationLog" activities originating from suspicious IP addresses. This indicates that operation log entries have been deleted by a malicious user with super admin privileges. If this type of entry exists in Operation Log, the UCM is likely compromised.

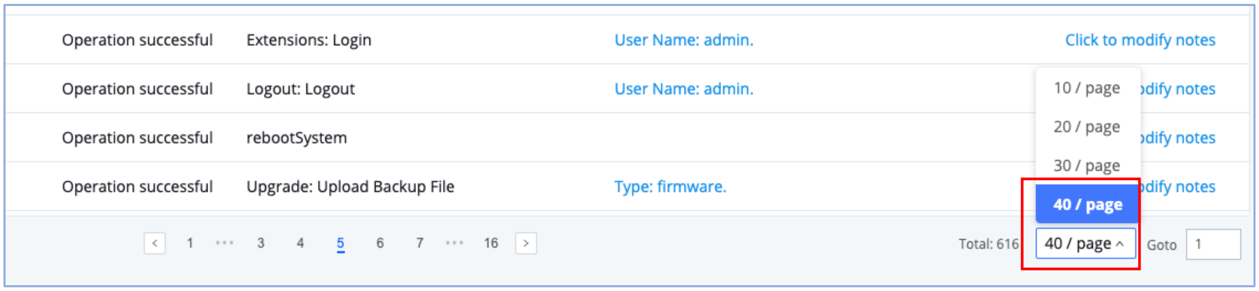


User Name: All Users

DATE	USER NAME	IP ADDRESS	RESULTS	PAGE OPERATION
2020-04-23 11:01:23	admin	192.168.50.67	Operation successful	deleteOperationLog

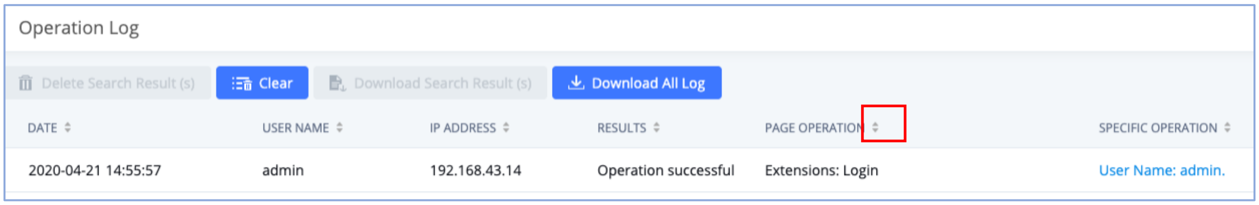
If no suspicious IP addresses or activities are found, skip step 4 and proceed to step 5. Otherwise, continue to step 4.

Note: To view and exam operation logs easier, change the page display to "40 per page" and sort the entries by action by clicking on the "Page Operation" sort buttons.



Operation successful	Extensions: Login	User Name: admin.	Click to modify notes
Operation successful	Logout: Logout	User Name: admin.	odify notes
Operation successful	rebootSystem		odify notes
Operation successful	Upgrade: Upload Backup File	Type: firmware.	odify notes

Sort "Page Operation":

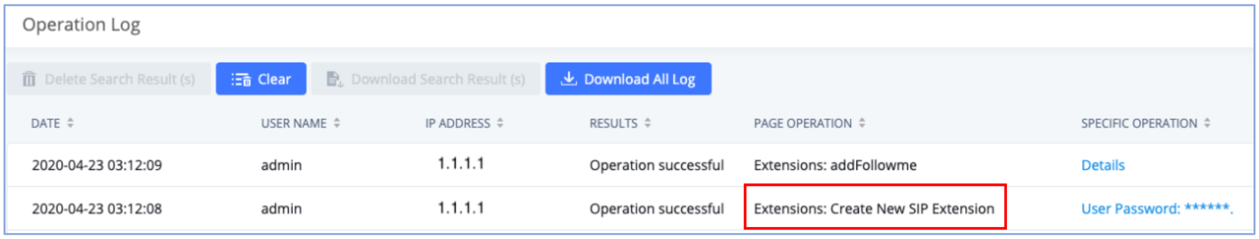


DATE	USER NAME	IP ADDRESS	RESULTS	PAGE OPERATION	SPECIFIC OPERATION
2020-04-21 14:55:57	admin	192.168.43.14	Operation successful	Extensions: Login	User Name: admin.

4. **Delete suspicious users, change passwords, and revert unauthorized changes.**

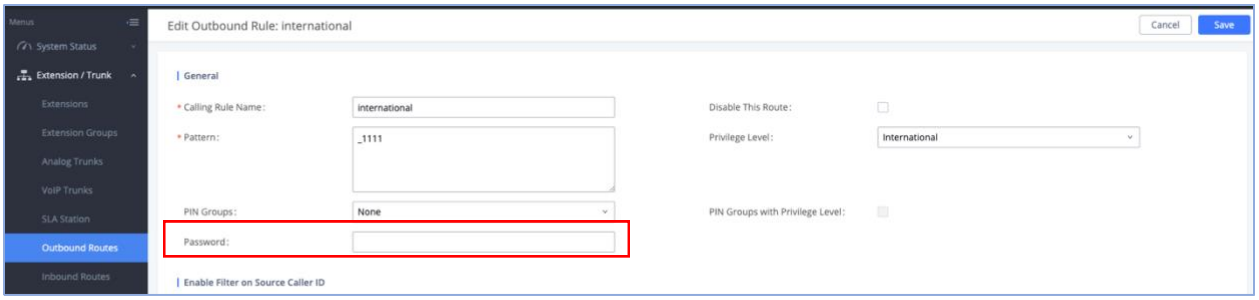
(1) If the suspicious/malicious user logged in successfully as super admin or admin, please change the password for all consumer users under UCM web UI->Maintenance->User Management page.

Check for any additional activities from this unknown IP address in the Operation Log such as newly created extensions and web configuration changes.



DATE	USER NAME	IP ADDRESS	RESULTS	PAGE OPERATION	SPECIFIC OPERATION
2020-04-23 03:12:09	admin	1.1.1.1	Operation successful	Extensions: addFollowme	Details
2020-04-23 03:12:08	admin	1.1.1.1	Operation successful	Extensions: Create New SIP Extension	User Password: ******.

Revert all changes made by the suspicious/malicious users and change all passwords for web access, SIP registration, etc. Add a password to outbound routes to prevent unauthorized calls.



Edit Outbound Rule: international

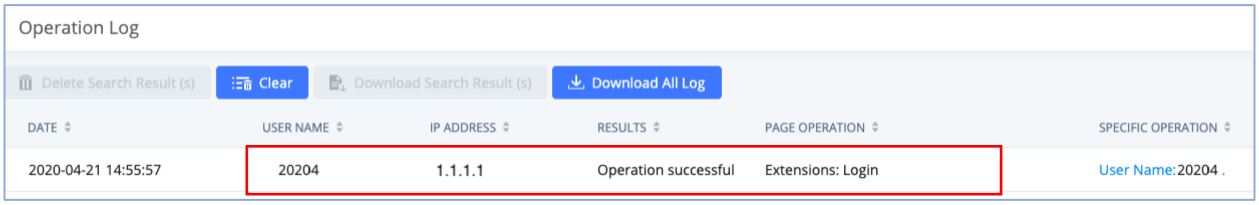
General

* Calling Rule Name: international
* Pattern: _1111
PIN Groups: None
Password:
Disable This Route: □
Privilege Level: International
PIN Groups with Privilege Level: □

Enable Filter on Source Caller ID

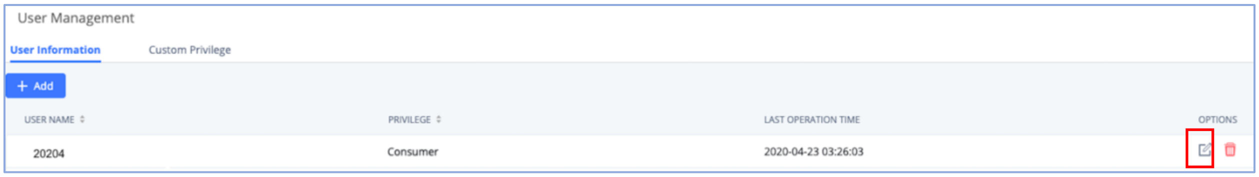
(2) If the suspicious/malicious user only logged in successfully from consumer user and there is no Operation Log showing suspicious/malicious login from admin or super admin, please change the password for such consumer user under UCM web UI->Maintenance->User Management page.

For example, 20204 is a consumer user in the UCM and 1.1.1.1 is an unknown IP address. The login operation is successful from this IP address, which means the malicious user obtained the login password for consumer user 20204 already and the information from 20204 user portal is compromised.



DATE	USER NAME	IP ADDRESS	RESULTS	PAGE OPERATION	SPECIFIC OPERATION
2020-04-21 14:55:57	20204	1.1.1.1	Operation successful	Extensions: Login	User Name:20204 .

Click on “Edit” button for the compromised user and change the password for 20204:

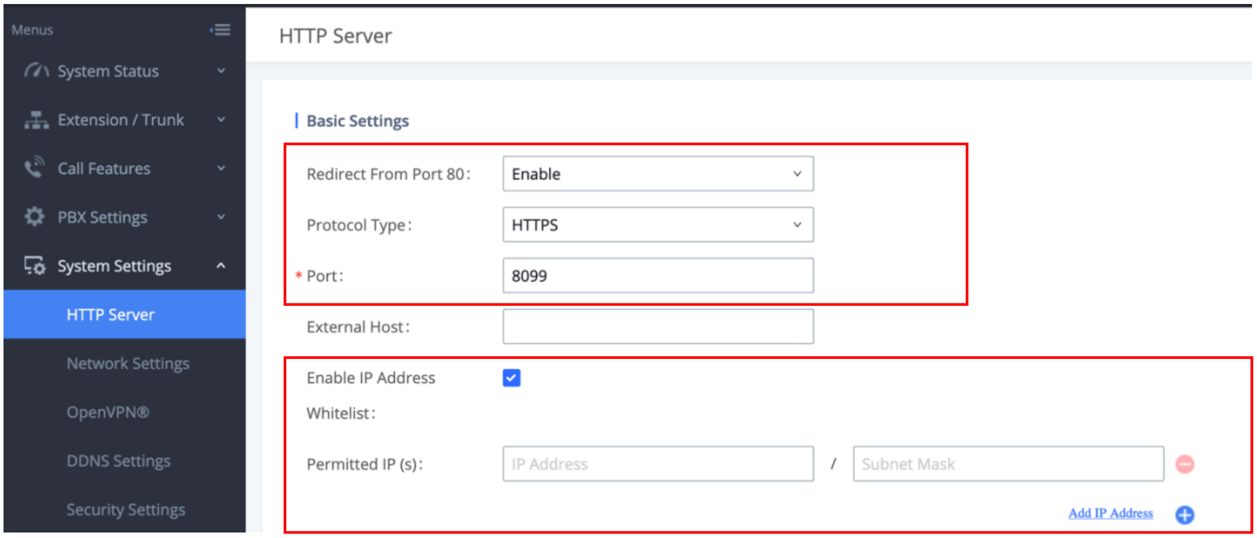


User Management

USER NAME	PRIVILEGE	LAST OPERATION TIME	OPTIONS
20204	Consumer	2020-04-23 03:26:03	

5. On UCM web UI->System Settings->HTTP Server page, turn on “Enable IP Address Whitelist” option and add the IP addresses allowed to access the UCM web portal to “Permitted IP” list.

   Additionally, disable "Redirect from Port 80", set protocol to HTTPS, and change Port to not be 8089.



HTTP Server

Basic Settings

Redirect From Port 80: Enable

Protocol Type: HTTPS

* Port: 8099

External Host:

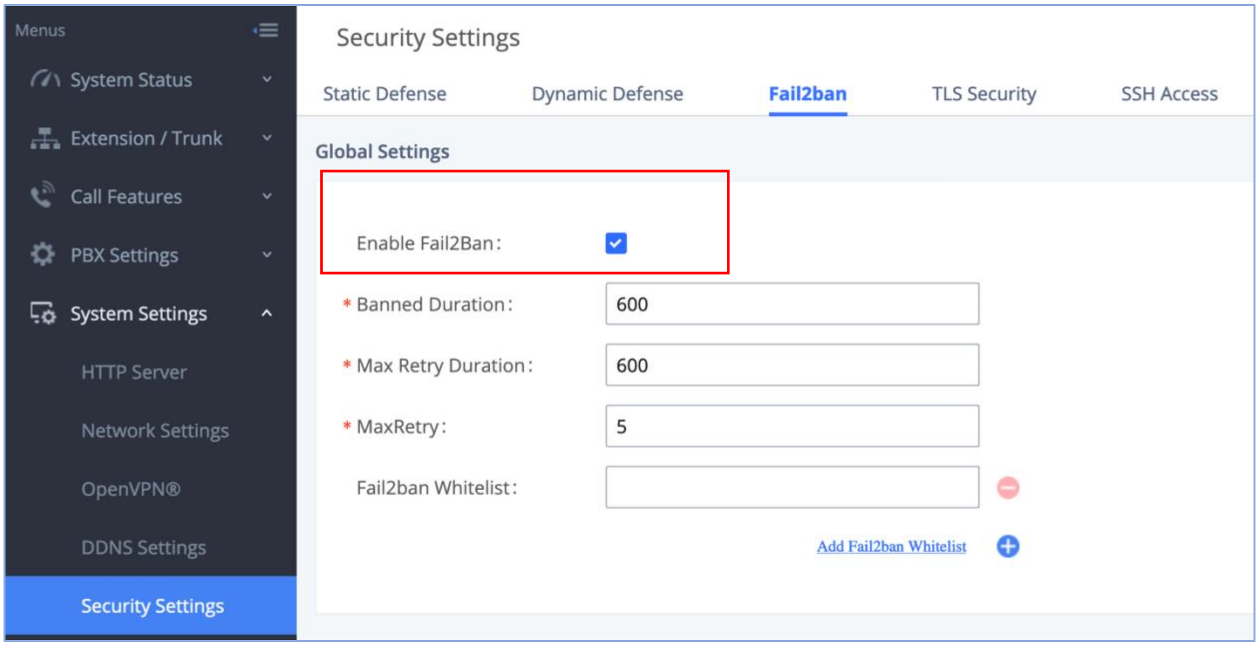
Enable IP Address Whitelist: ☑

Permitted IP (s): IP Address / Subnet Mask

6. **Enable Fail2ban services**.

   On the UCM web UI→System Settings→Security Settings→Fail2ban page, toggle on “Enable Fail2Ban”, “Asterisk Service”, and “Login Attack Defense”.

   If there are repeated unsuccessful login and SIP registration attempts from IP addresses, Fail2ban will blacklist them based on the configured settings.



Security Settings

Global Settings

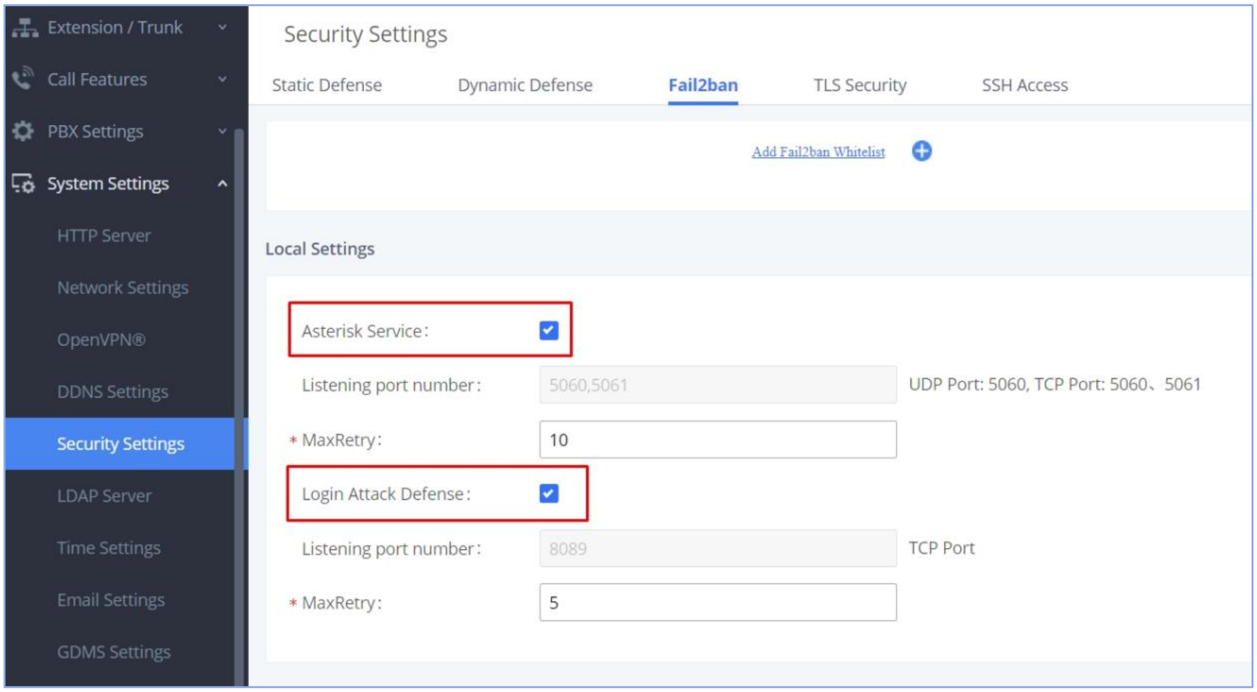
Enable Fail2Ban: ☑

* Banned Duration: 600

* Max Retry Duration: 600

* MaxRetry: 5

Fail2ban Whitelist:



Security Settings

Local Settings

Asterisk Service: ☑

Listening port number: 5060,5061 UDP Port: 5060, TCP Port: 5060、5061

* MaxRetry: 10

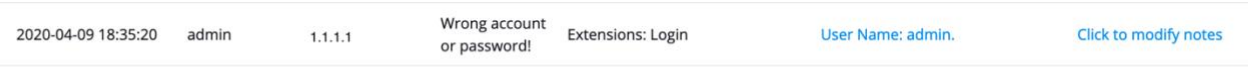
Login Attack Defense: ☑

Listening port number: 8089 TCP Port

* MaxRetry: 5

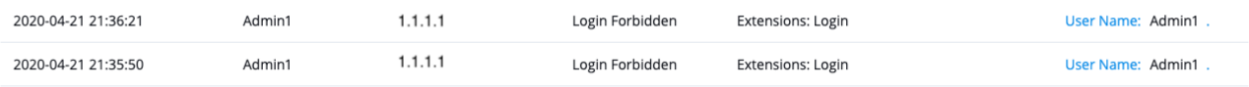
7. During Operation Log check, if you see login attempts or login forbidden attempts like below, it's likely your UCM is exposed to hackers and it's vulnerable to attacks.

   "Wrong account or password!" continuously shows from unknown IP:



2020-04-09 18:35:20	admin	1.1.1.1	Wrong account or password!	Extensions: Login	User Name: admin.	Click to modify notes

"Login Forbidden" frequently shows from unknown IP:



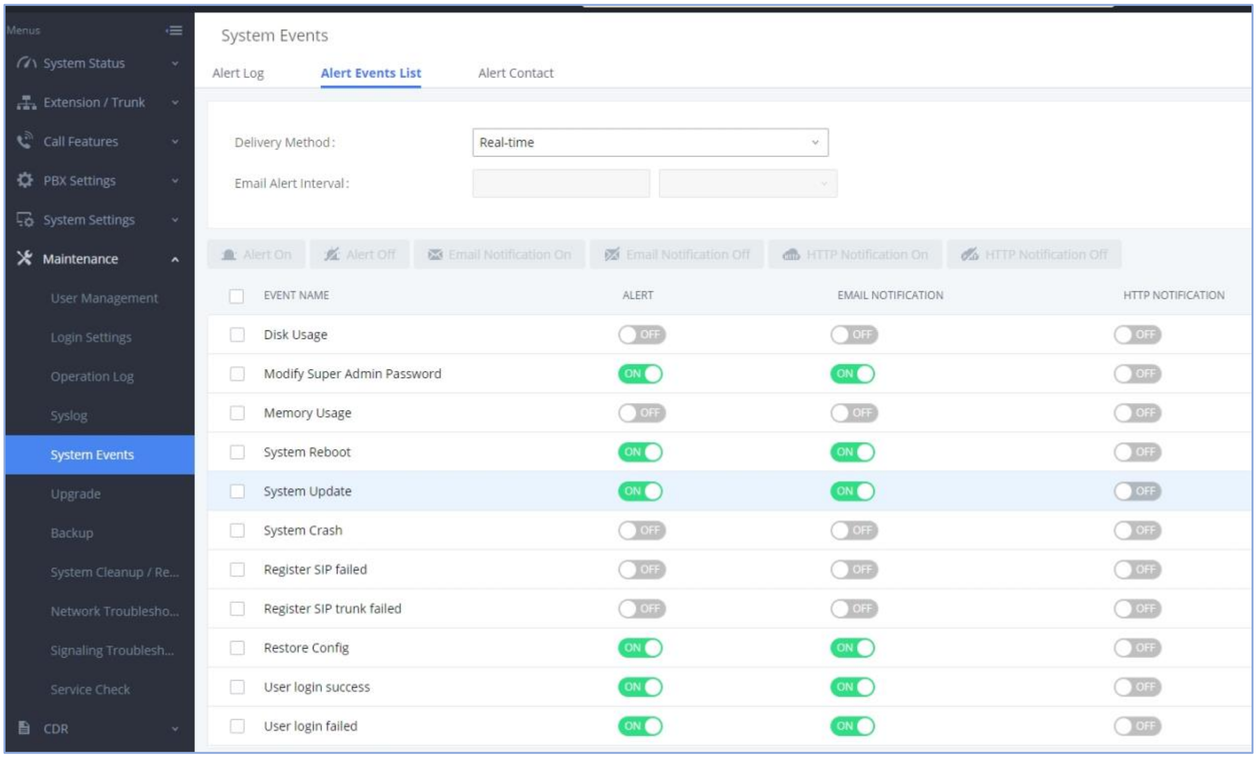
2020-04-21 21:36:21	Admin1	1.1.1.1	Login Forbidden	Extensions: Login	User Name: Admin1 .
2020-04-21 21:35:50	Admin1	1.1.1.1	Login Forbidden	Extensions: Login	User Name: Admin1 .

Therefore, it's highly recommended to place the UCM behind a firewall, disable port forwarding on the router to avoid external access to the UCM, and make it accessible only through VPN.

8. Check recent billing statement related to UCM calls and UCM CDR entries for suspicious calls. If there are suspicious calls especially unauthorized international calls are found, please locate the SIP extensions that has made unauthorized calls and delete the extension. And then take all actions from above step 1 to step 7 to secure the UCM.

9. **Set up System Event Alerts and Logging.**

   To prevent security breaches in a timely manner, please enable and configure system alerts and logging. System Event Alerts can be configured in the UCM web UI->Maintenance→System Events→Alert Events List page. From here, enable your alerts.



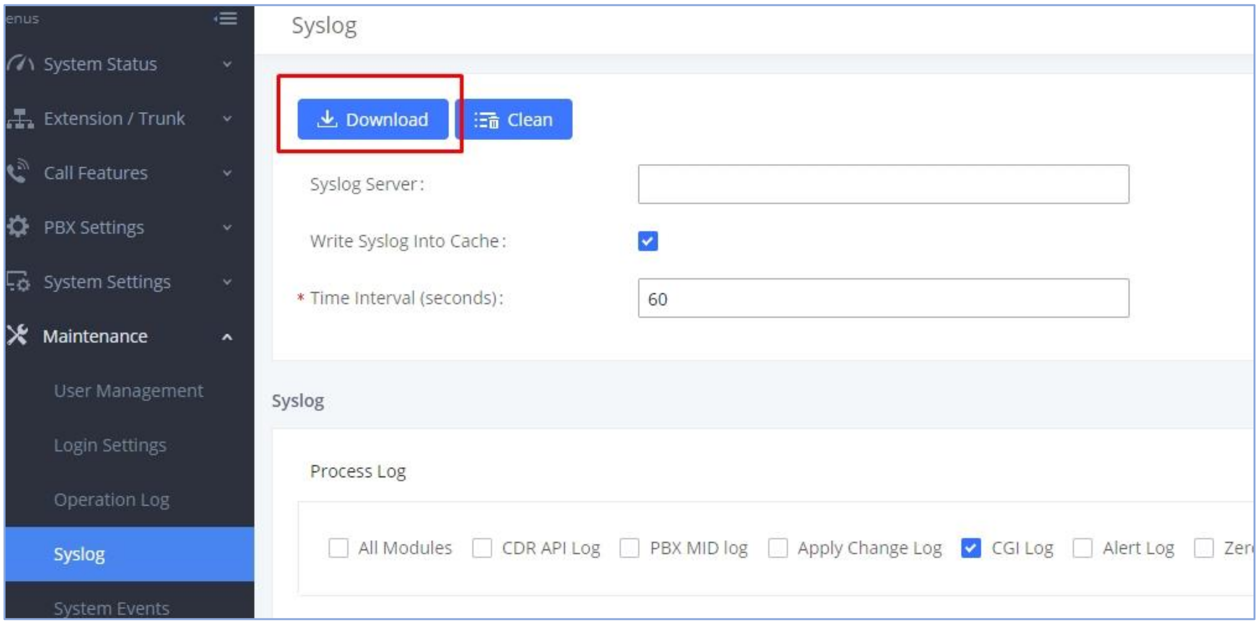
System Events

Delivery Method: Real-time

Email Alert Interval:

□ EVENT NAME	ALERT	EMAIL NOTIFICATION	HTTP NOTIFICATION
□ Disk Usage	OFF	OFF	OFF
□ Modify Super Admin Password	ON	ON	OFF
□ Memory Usage	OFF	OFF	OFF
□ System Reboot	ON	ON	OFF
□ System Update	ON	ON	OFF
□ System Crash	OFF	OFF	OFF
□ Register SIP failed	OFF	OFF	OFF
□ Register SIP trunk failed	OFF	OFF	OFF
□ Restore Config	ON	ON	OFF
□ User login success	ON	ON	OFF
□ User login failed	ON	ON	OFF

For logging, navigate to the **Maintenance→Syslog** page and enable the following syslog modules: CGI Log, SECURITY, HTTP (all levels), PBX (all levels), and pjsip (all levels).



Syslog Server:

Write Syslog Into Cache: ☑

* Time Interval (seconds): 60

Syslog

Process Log

□ All Modules □ CDR API Log □ PBX MID log □ Apply Change Log ☑ CGI Log □ Alert Log □ Zer

If any suspicious or unauthorized activity such as “Modify Super Admin Password” and “User LoginSuccess” have been conducted by a suspicious IP address and reported in alerts, please download the syslog and submit a ticket to Grandstream Technical Support as soon as possible.

Support

To obtain help and support for security update:

- Subscribe for firmware release newsletter for latest firmware update: http://mailinglists.grandstream.com/lists/?p=subscribe&id=1
- Read the UCM Security Manual, which can be downloaded from: http://www.grandstream.com/sites/default/files/Resources/UCM_Security_Manual.pdf
- Explore and use the Grandstream Forums at http://forums.grandstream.com
- Submit a technical support ticket at https://helpdesk.grandstream.com/

Disclaimer

Asterisk, AsteriskGUI, and AsteriskNOW are registered trademarks of Digium, Inc.