FortiVoice™ 200D/200D-T Security Technical Note

FortiVoice 200D/200D-T Security Technical Note

September 4, 2013

1st Edition

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

PBX security becomes more and more important with the wide adoption of Voice over IP (VoIP) technology. While we enjoy the benefits VoIP has brought us, such as low cost, fast deployment, flexibility, and ease of use, we are facing more and more security threats coming with the new technology. Here are some of the common security threats:

- Denial of Service (DoS) attack against the SIP port to make the PBX unavailable for legitimate users.
- Service fraud that steals user account and registers as an internal extension to make unauthorized long distance or international calls.
- Unauthorized access to PBX administrative interface to modify the configuration or download call recordings.
- Unauthorized access to user voice mailbox to play or download voice messages.
- Unauthorized access to phone directories.

This technical note is a guideline for protecting the FortiVoice (FVC) 200D/200D-T against the most common security threats as mentioned above.

For PBX security, there is no silver bullet where one shot can fix all. Instead, a layered approach is used to prevent any single point of failure. Generally speaking, there are three ways to secure the FVC 200D/200D-T:

1. Protect the system with firewall.
2. Harden the configuration of the system to take advantage of the existing security features and prevent any mis-configuration.
3. Practice your due diligence, monitor the day to day operation of the system and be alert on any anomaly seen on the system.

This technical note assumes that you use the FortiVoice 200D/200D-T 2.2.0 software. Use this note in conjunction with the *FortiVoice 200D/200D-T Administration Guide*.

Protecting the system with firewall

1. Put the FVC 200D/200D-T behind the firewall.

   In addition to the basic network level access control, the so-called Next Generation Firewall (NGFW), such as the FortiGate unit, supports a lot of VoIP related features, like SIP message rate limit, content inspection, and intrusion detection. Deploying the system behind the firewall can take advantage of these security features.

   Note that if you deploy the FVC 200D/200D-T behind a firewall, NAT is usually used. SIP does not work well with NAT by itself. You need to enable NAT Traversal related features on the firewall. For instructions on how to configure the FortiGate unit, see the *FortiVoice 200D/200D-T and FortiGate Network Security Platform Interoperability Technical Note*.

2. Do not open static ports for media on the firewall.

   The FVC 200D/200D-T uses SIP for signalling and RTP for media. The SIP port number is pre-determined (5060 by default), but RTP port numbers are dynamic and negotiated using SIP in each and every SIP conversation. It is desirable for the firewall to have the intelligence to only open those needed ports for each conversation on demand. When the conversation is over, those open ports should be closed. This feature is called "pin-hole". Session Border Controller (SBC) or NGFW such as the FortiGate unit supports this advanced feature. By using pin-hole, only one policy is needed to grant access to SIP port of the FVC 200D/200D-T, all subsequent RTP traffic will be allowed automatically. Once the VoIP call is over, access to those RTP ports would be rejected automatically. Obviously this is more secure than statically opening those RTP ports to the FVC 200D/200D-T on the firewall.

3. Restrict the administrative access to the FVC 200D/200D-T on the firewall.

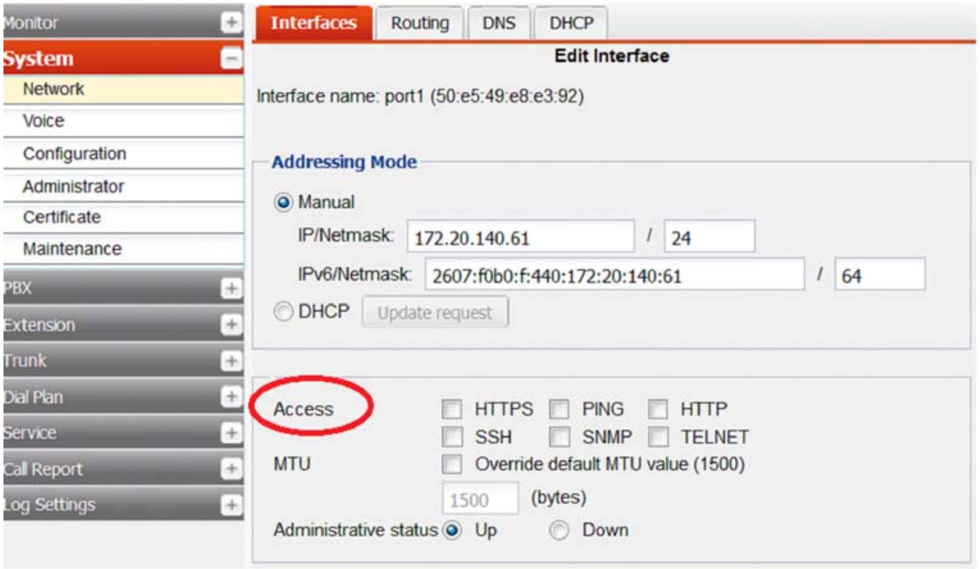
   In addition to SIP and RTP, public administrative accesses to the FVC 200D/200D-T needs to be restricted. All unneeded services such as SSH, HTTP, HTTPS, SNMP, ICMP, and TELNET, should be disabled if possible. The less accesses to expose to the Internet, the less attacking avenues there will be and the more secure the system will be.

Hardening FVC 200D/200D-T configuration

Security is one of the priorities of the FVC 200D/200D-T. The built-in security features should be turned on to harden the system.

1. Disable the unneeded accesses.

   Accesses such as HTTP, HTTPS, SSH, ICMP, SNMP, and TELNET should be all disabled on public facing interfaces. If a public access like HTTPS is needed, it is better to add a policy on the firewall to restrict the source IP addresses of the access. If a remote address is required, the secure protocols are preferred over those clear text ones, for example, SSH or HTTPS, instead of TELENT or HTTP.



Edit Interface

Interface name: port1 (50:e5:49:e8:e3:92)

Addressing Mode

● Manual

IP/Netmask: 172.20.140.61 / 24

IPv6/Netmask: 2607:f0b0:f:440:172:20:140:61 / 64

○ DHCP Update request

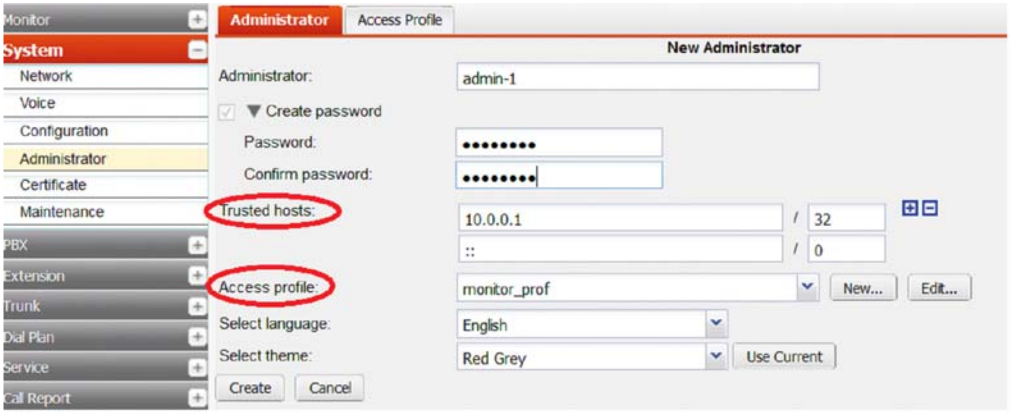
Access □ HTTPS □ PING □ HTTP
□ SSH □ SNMP □ TELNET

MTU □ Override default MTU value (1500)
1500 (bytes)

Administrative status ● Up ○ Down

2. Restrict the administrative access on FVC 200D/200D-T.

   On the FVC 200D/200D-T, you can restrict the sour IP addresses of administrator and limit the type of access. The more specific, the better. A strong password for administrative users is a must.



New Administrator

Administrator: admin-1

☑ ▼ Create password

Password: ••••••••

Confirm password: ••••••••

Trusted hosts: 10.0.0.1 / 32

:: / 0

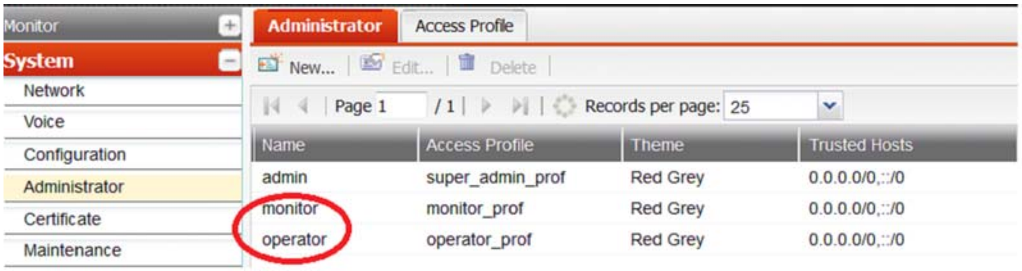
Access profile: monitor_prof

Select language: English

Select theme: Red Grey

3. Remove unused accounts.

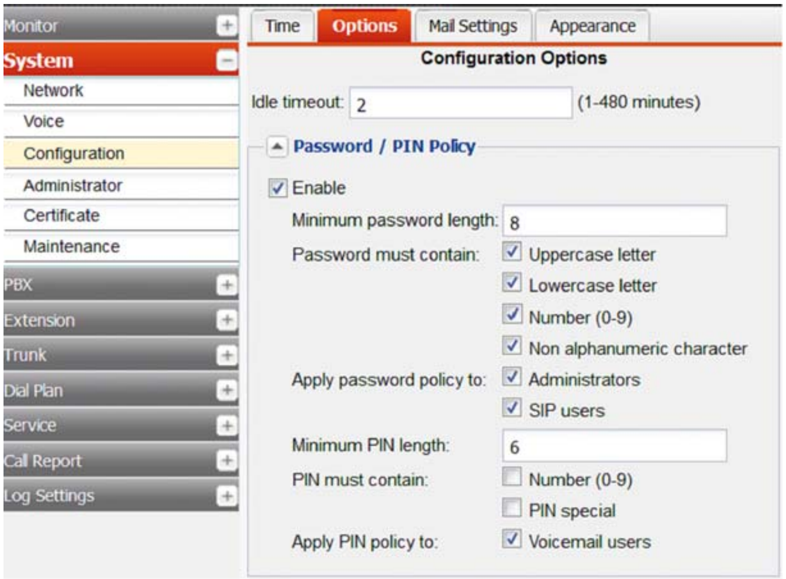
   The FVC 200D/200D-T comes with two additional default accounts "monitor" and "operator" which do not have password preconfigured. Those two default accounts have only limited access to the system. But if you do not need them, it is strongly recommended to remove them.



Name	Access Profile	Theme	Trusted Hosts
admin	super_admin_prof	Red Grey	0.0.0.0/0,::/0
monitor	monitor_prof	Red Grey	0.0.0.0/0,::/0
operator	operator_prof	Red Grey	0.0.0.0/0,::/0

4. Enforce password policy if possible.

   Weak password is the most common vulnerability that malicious people can exploit. The FVC 200D/200D-T supports security policy to enforce the complexity of password.



Configuration Options

Idle timeout: 2 (1-480 minutes)

Password / PIN Policy

☑ Enable

Minimum password length: 8

Password must contain: ☑ Uppercase letter ☑ Lowercase letter ☑ Number (0-9) ☑ Non alphanumeric character

Apply password policy to: ☑ Administrators ☑ SIP users

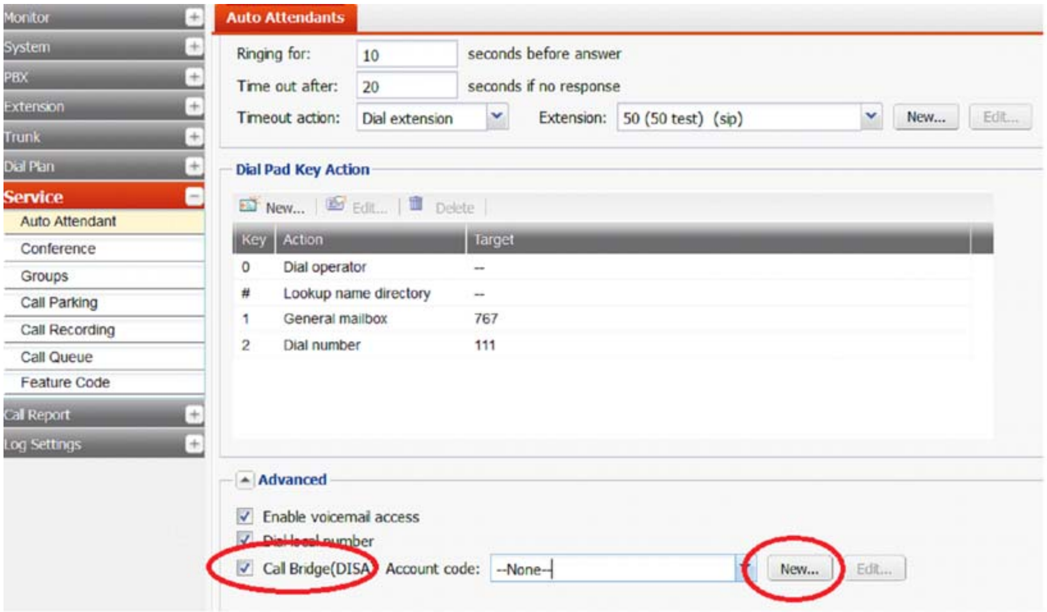
Minimum PIN length: 6

PIN must contain: □ Number (0-9) □ PIN special

Apply PIN policy to: ☑ Voicemail users

5. Configure the passcode for call bridge if enabled.

   Call bridge (DISA) enables callers to make outgoing calls from auto-attendant, which is a very convenient feature. However, if this feature is not password protected, malicious people can take advantage of it and make unauthorized long distance or international calls. Therefore, when you turn on this feature in auto-attendant, remember to configure a passcode.



Ringing for: 10 seconds before answer

Time out after: 20 seconds if no response

Timeout action: Dial extension   Extension: 50 (50 test) (sip)

Dial Pad Key Action

Key	Action	Target
0	Dial operator	--
#	Lookup name directory	--
1	General mailbox	767
2	Dial number	111

Advanced

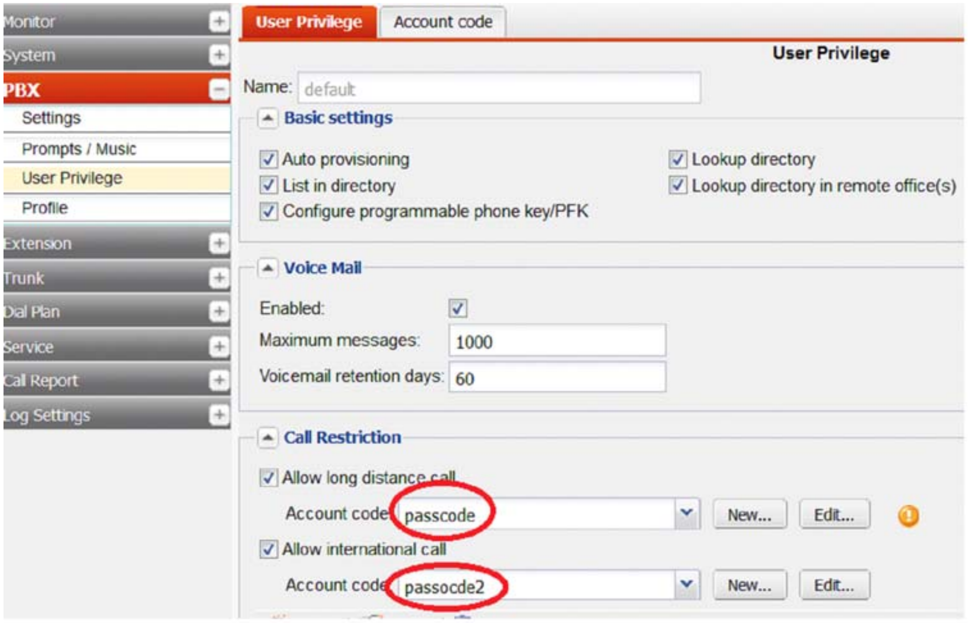
☑ Enable voicemail access

☑ Dial local number

☑ Call Bridge(DISA) Account code: --None--

6. Configure user privilege as needed.

   FVC 200D/200D-T supports very fine-grained user privilege for extensions. Administrators need to configure very specific user privilege based on the business needs and "least privilege" principal. Long distance calls and international calls can be password protected. Without entering the correct passcode, long distance or international calls are rejected. If long distance or international calls are not required, disallow it.



User Privilege

Name: default

Basic settings

☑ Auto provisioning   ☑ Lookup directory

☑ List in directory   ☑ Lookup directory in remote office(s)

☑ Configure programmable phone key/PFK

Voice Mail

Enabled: ☑

Maximum messages: 1000

Voicemail retention days: 60

Call Restriction

☑ Allow long distance call

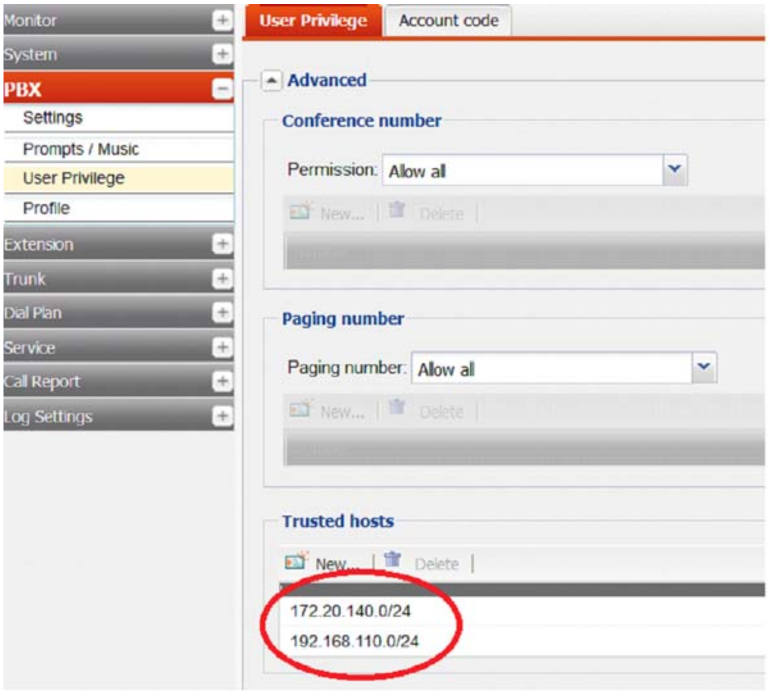
Account code: passcode

☑ Allow international call

Account code: passocde2

7. Configure extension trusted host.

   In user privilege, there is a setting called *Trusted hosts*. Once it is configured, the extension is not allowed to register and make phone calls from hosts not specified in the *Trusted hosts* field. It is recommended to put your internal network there for all internal extensions to prevent malicious people from registering and making phone calls from the Internet with stolen username/password.



Conference number

Permission: Allow all

Paging number

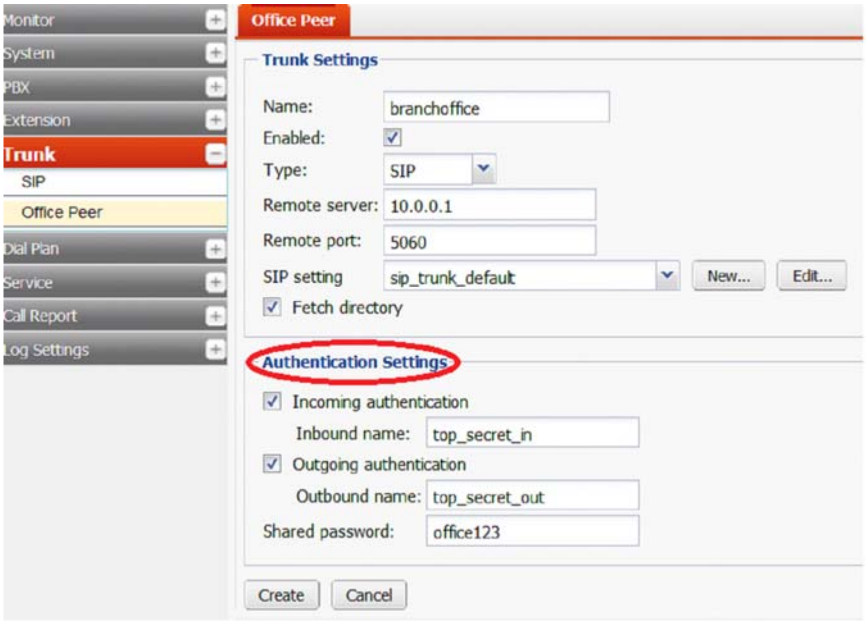
Paging number: Allow all

Trusted hosts

172.20.140.0/24
192.168.110.0/24

8. Enable authentication for peer office.

Authentication can be enabled for both incoming and outgoing directions. It is recommended to enable it on both ends to add one more layer of protection in addition to the IP-based authentication.



Trunk Settings

Name: branchoffice
Enabled: ☑
Type: SIP
Remote server: 10.0.0.1
Remote port: 5060
SIP setting sip_trunk_default
☑ Fetch directory

Authentication Settings

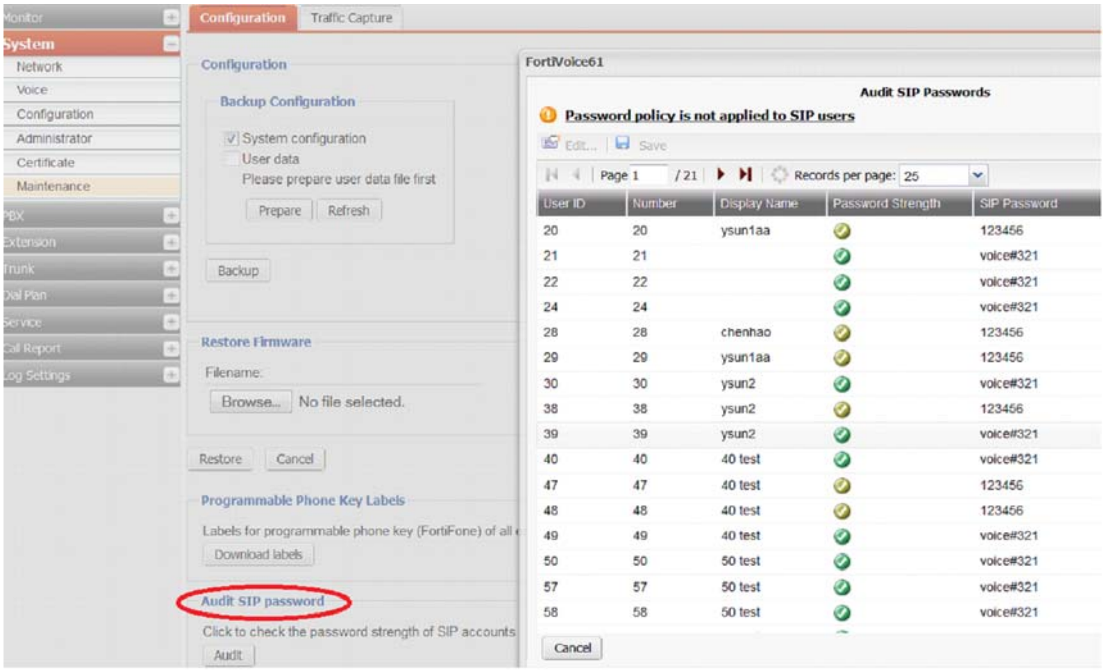
☑ Incoming authentication
Inbound name: top_secret_in
☑ Outgoing authentication
Outbound name: top_secret_out
Shared password: office123

Monitoring the system operation

Security is an ongoing task. You need to practice your due diligence and monitor the system for any anomaly closely.

1. Monitor call records, system, and voice related event logs and pay close attention to the following:
   - CDR and call reports for any over long or spike of long distance/international calls. Usually service fraudulence can be discovered by checking CDR or call report.
   - SIP register attempts in voice logs. Too many register attempts could be explained by a SIP password guessing attack.
   - System login attempts in system event log. If public remote access is disabled, there should be no login attempt from the Internet. If there is any, it may mean that your firewall rules are not properly configured. If public access is required and there is a lot of access attempts, it may mean password guessing attack is undergoing. To address this, you can add a firewall policy to restrict the source IP addresses of the remote administrative access.
2. Audit password strength regularly.

   Weak password is the most common security vulnerability. You should check the password strength on a regular basis to identify any weak ones.



☑ System configuration

□ User data

Please prepare user data file first

Filename:

No file selected.

Labels for programmable phone key (FortiFone) of all

Click to check the password strength of SIP accounts

Audit SIP Passwords

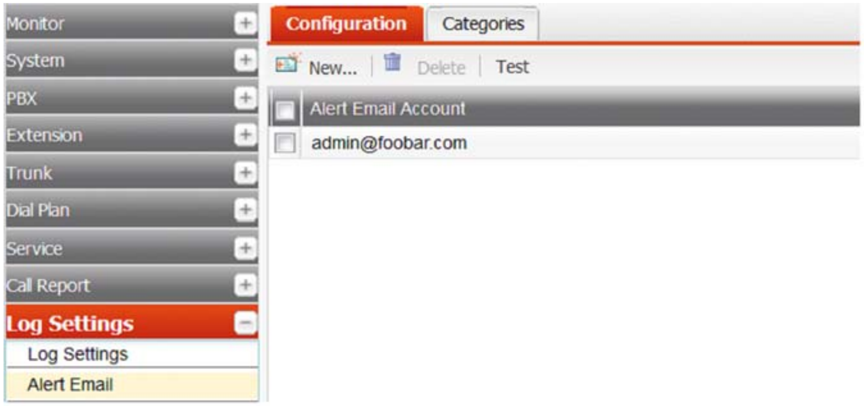
Password policy is not applied to SIP users

Page 1 / 21 Records per page: 25

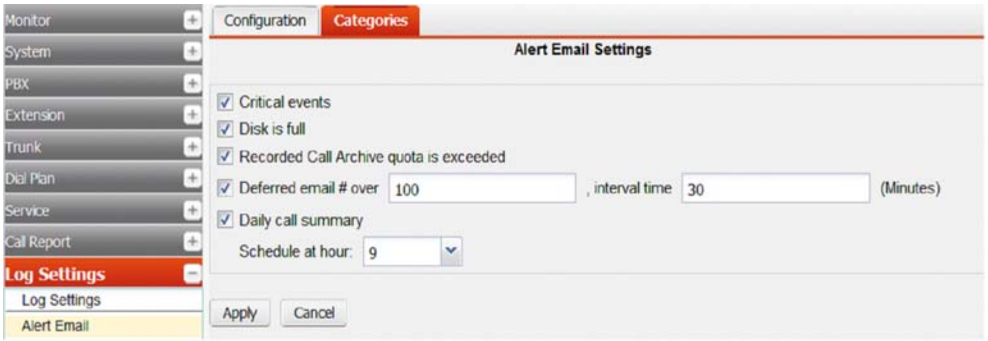
User ID	Number	Display Name	Password Strength	SIP Password
20	20	ysun1aa	✓	123456
21	21		✓	voice#321
22	22		✓	voice#321
24	24		✓	voice#321
28	28	chenhao	✓	123456
29	29	ysun1aa	✓	123456
30	30	ysun2	✓	voice#321
38	38	ysun2	✓	123456
39	39	ysun2	✓	voice#321
40	40	40 test	✓	voice#321
47	47	40 test	✓	123456
48	48	40 test	✓	123456
49	49	40 test	✓	voice#321
50	50	50 test	✓	voice#321
57	57	50 test	✓	voice#321
58	58	50 test	✓	voice#321

3. Enable alert email.

The FVC 200D/200D-T can send notifications to the pre-configured email address for selective critical events so that administrators can take immediate actions as needed.



□ Alert Email Account
□ admin@foobar.com



Alert Email Settings

☑ Critical events

☑ Disk is full

☑ Recorded Call Archive quota is exceeded

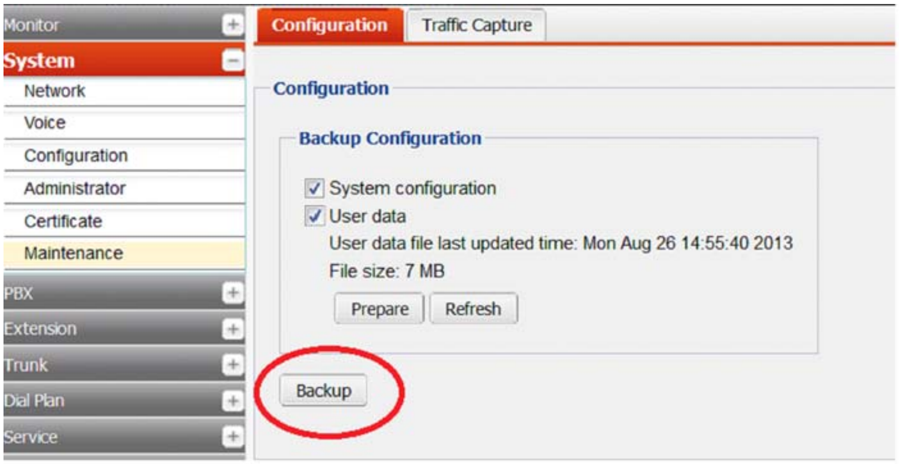
☑ Deferred email # over 100 , interval time 30 (Minutes)

☑ Daily call summary

Schedule at hour: 9

4. Back up configuration regularly.

Back up configuration file regularly and before firmware upgrade or big configuration change. In case there is any system failure, you can restore the previous known-good state.



Configuration

Backup Configuration

☑ System configuration

☑ User data

User data file last updated time: Mon Aug 26 14:55:40 2013

File size: 7 MB