

uniteme 20.04

May 17, 2020

Summary

eZuce is pleased to announce the general availability of **uniteme 20.04**

We're bringing a couple of nice new features to **uniteme**. In previous versions, if somebody dialed a user's name in the dial by name directory the system would read back a mailbox number if the user had not set up their name in voicemail. Now the system will read back the user name.

The second new feature we'll highlight here is a security enhancement. We worked with the guys at <https://apiban.org> to add their automatically created ban list of IP's to **uniteme**. Check out their site, they're offering a great service. All you need to do is request an API key and you can have **uniteme** automatically poll their honeypot created ban list.

Highlights

uniteme New Features

- Read back voice mailbox owner name if the user has not configured their voicemail greeting.
- Support for apiban.org to automatically ban SIP scanners

uniteme Improvements

- Log error messages at Notice level vs. at higher proxy logging levels.
- Firewall blacklist allows entries that are added automatically by fail2ban to be kept in ban list
- Manage the list of banned IP's in Admin GUI
- DID Pools get the ability to transfer to an extension for an unallocated DID.

Notes

1. 19.08 and later are now released on CentOS 7 only. This will require that administrators install CentOS 7 minimal, then install Uniteme with our single line installer and then restore from a previous version backup.
2. AudioCodes and other gateways may need to have their configuration changed if faxing is used. See SIPX-811.
3. For Let's Encrypt certificates to work properly, the server must have a valid outside DNS name and have port 80 and 443 open to LE's servers.

Who Should Install?

New software releases are made at a rate of two to four releases a year. Releases are numbered in the <yy>.<mm>.<uu> format where <yy> and <mm> designate the year and the month, respectively, in which a release is made generally available. Where applicable, <uu> corresponds to an update release relative to a general release on which fixes are made available.

Notes

1. 19.08 and later are now released on CentOS 7 only. This will require that administrators install CentOS 7 minimal, then install Uniteme with our single line installer and then restore from a previous version backup.
2. Customers receiving faxes through AudioCodes devices will need to modify their AudioCodes configurations with the following settings changes:

[Voice Engine Params]

CallerIDType = 0

FaxTransportMode = 0

CNGDetectorMode = 0

[SIP Params]

CHANNELSELECTMODE = 0

ISFAXUSED = 0

SIPTRANSPORTTYPE = 0

[CodersGroup0]

CodersGroup0 0 = "g711Ulaw64k", 20, 0, -1, 0;

1. For Let's Encrypt certificates to work properly, the server must have a valid outside DNS name and have port 80 and 443 open to LE's servers.

Who Should Install?

This release is recommended for all 4.6 and later installations. If you have a patch installed to your system a new patch may be required. Please contact sa@ezuce.com if you think you may have a patch applied as that may be replaced during the update.

eZuce's software products continuously progress through an Agile based development methodology that keeps feature functionality comprehensive and up-to-date in response to evolving market and customer requirements.

New software releases are made at a rate of two to four releases a year. Releases are numbered in the <yy>.<mm>.<uu> format where <yy> and <mm> designate the year and the month, respectively, in which a release is made generally available. Where applicable, <uu> corresponds to an update release relative to a general release on which fixes are made available.

In order to ensure service continuity and stability, customers may keep their production environments unchanged for up to a 6-month period during which release updates or patches are made available. After a release is more than 6-months old, eZuce customers would have to upgrade to the latest generally available release - inclusive of all fixes to date and any new patches.

Questions

If you have questions about updating you can email sa@ezuce.com or if you need assistance with the update please contact your account manager or email sales@ezuce.com.

Software Release History

We're currently running on a 4-month release cycle.

- April release for 2018 is 18.04
- August release for 2018 is 18.08
- ...

Release Level History

- 14.04 - April 30, 2014
- 14.04.1 - June 01, 2014
- 14.04.2 - July 11, 2014
- 14.04.3 - October 24, 2014
- 14.10 - February 5, 2015
- 15.04 - April 29, 2015
- 15.05 - May 27, 2015
- 15.06 - June 30, 2015
- 15.08 - August 31, 2015
- 15.10.1 - December 9, 2015
- 15.12 - January 6, 2015
- 16.02 - March 14, 2016
- 16.04 - May 31, 2016
- 16.08 - October 6, 2016
- 16.12 - January 17, 2016
- 17.04 - April 18, 2017
- 17.08 - September 7, 2017
- 17.10 - December 7, 2017
- 18.04 - June 5, 2018
- 18.08 - September 7, 2018
- 18.12 - January 15, 2019
- 19.04 - May 28, 2019
- 19.08 - October 10, 2019
- 19.12 - February 13, 2020
- 20.04 - May 17, 2020

System Requirements

For a reasonably performing system, we recommend the following configuration.

Minimum hardware requirements

- Pentium 4 or Xeon processor @ 2.0 GHz 64bit or higher
- Minimum 4 GB of RAM with sufficient swap space
- 40 GB disk (75 users depending on usage patterns, VoiceMail consumes ~ 1 MB per minute so scale appropriately for your user count and anticipated VM retention policy)
- As with anything server wise, more CPU/RAM/DISK = better.

Notes:

- **uniteme** supports an unlimited number of voicemail boxes, the total number of hours of recorded messages is determined by the size of the hard-disk. As a rule, for every minute of recorded messages, you will need 1 MB of disk space (About 3 hours per 10 GB of disk space).

Operating System

CentOS/RHEL 7 x86_64 minimal with latest updates is required (recommended now).

Devices

Phones

- **Polycom VVX Devices** with firmware 5.9.1 (split) are recommended for new installations
- **Polycom SoundPoint IP** Devices should run firmware 4.0.14 (split)

Gateways

- **AudioCodes Gateways** are recommended for PSTN connectivity

SBCs

- **Frafos, Sangoma, Acme Packet and Ingate** SBC's are recommended for SIP Trunking and Remote Worker connectivity (commonly referred to as sipXbridge and MediaRelay services respectively).
- **NOTE:** The eZuce uniteme - "Use built-in SIP Trunk SBC" found in Gateway Details for use with Trunking or Remote Worker solutions should be used only for lab purposes. Additionally, sipXbridge does not work in an HA environment.

Documentation

Technical Reference Manuals, User Guides, and other technical and user information can be found under the following link: [Documentation Page](#)

Installation and Upgrade Notes

Special MongoDB note

Please be aware of these MongoDB requirements <http://docs.mongodb.org/manual/reference/ulimit/> **Note:** Both the "hard" and the "soft" ulimit affect MongoDB's performance. The "hard" ulimit refers to the maximum number of processes that a user can have active at any time. This is the ceiling: no non-root process can increase the "hard" ulimit. In contrast, the "soft" ulimit is the limit that is actually enforced for a session or process, but any process can increase it up to "hard" ulimit maximum. Every deployment may have unique requirements and settings; however, the following thresholds and settings are particularly important for mongod and mongos deployments:

```
ulimit -a
-f (file size): unlimited
-t (cpu time): unlimited
-v (virtual memory): unlimited
-n (open files): 64000
-m (memory size): unlimited
-u (processes/threads): 32000
```

Always remember to restart your mongod and mongos instances after changing the ulimit settings to make sure that the settings change takes effect. If you limit virtual or resident memory size on a system running MongoDB the operating system will refuse to honor additional allocation requests. After every install/upgrade please check that "cat /proc/\$pid_of_mongo/limits" have the recommended value of 655350. To make this value permanent you need to create this file `/etc/security/limits.d/99-mongodb-nproc.conf` and add the following lines:

```
mongodb soft nproc 64000
```

```
mongodb hard nproc 64000
```

```
mongodb soft nofile 64000
```

```
mongodb hard nofile 64000
```

Special Patch Note

If you have a patch installed to your system a new patch may be required. Please contact sa@ezuze.com if think you may have a patch applied as that may be replaced during the update.

Installing from Repository

uniteme can be installed using the following procedure

1. Download CentOS 7 64 bit Minimal ISO from CentOS (<https://www.centos.org/download/>)
2. Install CentOS 7. ([Installing#InstallRedHatEnterpriseLinux7.xorCentOS7.x](#))
3. Install **uniteme**. ([Installing#Installuniteme](#))

Upgrade from previous versions

Warning!

Make sure you **backup** your system (configuration and voicemail at a minimum) prior to installation.

Upgrade 18.12 or later and already on CentOS 7

Modify your yum repo file for Uniteme (it's in the directory /etc/yum.repos.d) for the release you'd like to use.

Adjust your /etc/yum.repos.d/openuc.repo file to point to the version of openUC you'd like to upgrade to.

For example:

```
baseurl=https://user:password@https://download.ezuze.com/openuc/19.12-centos7/CentOS_${releasever}/${basearch}
to
baseurl=https://user:password@https://download.ezuze.com/openuc/19.12-centos7/CentOS_${releasever}/${basearch}
```

When you are ready to perform the actual upgrade:

```
yum update
or
yum update -y
```

If your system is a highly available cluster of 3 or more servers, update the secondary servers first and the primary server last. Send send all of the server profiles when done update on the primary server.

Upgrade for 18.12 or later CentOS 6 to CentOS 7

Any upgrade to CentOS 7 will require a fresh installation of CentOS 7 and then a restore of **uniteme**.

Backup your System

Login to the Admin GUI and click on System -> Backup and at a minimum backup configuration and voicemail.

Download the configuration and voicemail backup archives.

Build New CentOS 7 Server

Download CentOS 7 64 bit Minimal ISO from CentOS (<https://www.centos.org/download/>)

Install CentOS 7. ([Installing#InstallRedHatEnterpriseLinux7.xorCentOS7.x](#))

Install **uniteme**. ([Installing#Installuniteme](#))

Restore your System

Restore configuration and voicemail.

Remove any secondary servers restored from the Servers page.

Send Server Profile.

Reboot

Add Secondary Servers

Rebuild and re-add any secondary servers.

Modified Files Upgrade Note

If you have manually modified any system related files or some files are not as yum would expect them to be, the yum update process may not overwrite them. It will instead create 'rpmnew' or 'rpmsave' files and not overwrite the files. The administrator may have previously modified the files knowingly or as part of a patch supplied by TAC.

To check your upgrade.log and search for *.rpmnew *.rpmsave on your system check the upgrade log:

You will be responsible for merging any changes from the old file to the new or contacting Technical Support if you require assistance.

Support Tips and Contact Information

Please see the [Getting Support](#) section for support tips and support contact information

Specific Issues Addressed

Jira #	JIRA Name	RN Content	Enhancement/Fix/known Issue	Keywords
SIPX-738	Firewall Blacklist Enhancement	An administrator would like to allow automatically added banned hosts to be remembered and re-loaded when a server is restarted or IPTables is restarted. Each type of system message in System -> Security -> SIP Security should allow for a setting of -1 to add the host to the banned hosts list. Additionally, the administrator would like to be able to see the banned hosts in the admin GUI, why they were banned (sip-dos, invites, registrations, etc.) and be able to remove individual hosts from the list of banned hosts.	Enhancement	Security Firewall
SIPX-740	SIP Proxy should write errors to log file at Notice level	An administrator would like to have certain SIP system errors written to log when at Notice level. Proxy logs are overly verbose at Info or Debug. sipxProxy should write some additional errors to log file at Notice Level. The log file should have the date and time, a description of the error, the offending source IP address and destination IP address. This would be for 4xx, 5xx and 6xx message that sipXproxy can generate.	Enhancement	Logs
SIPX-803	Cleanup Temp Directory on Reset	When the user runs "sipxecs-setup --reset-all" it should cleanup the /var/sipxdata/tmp directory. Some of the files within the directory are used by other services and a cleanup is necessary to do a proper reset.	Fix	Setup
SIPX-804	sipx-backup and postgresql_running	Looks like the /usr/bin/sipx-backup is making a call to postgresql_running that fails even though postgresql is running.	Fix	Backup

SIPX-809	Read back voice mailbox owner name	<p>An administrator would like to have the voicemail system play back a user's name if the user has not recorded their name for voicemail.</p> <p>This can be done with mod_flite</p> <p>Speaking the name</p> <p>If the user has recorded their name, then that recording will be used when listing the matches. If they have not, the name will be read one letter at a time by default. If you would like the system to read their name as if it were being spoken, the following two files will have to be edited:</p> <p>[freeswitch_root]/conf/lang/[language]/dir/sounds.xml - Replace the action tag under "directory_result_say_name" with:</p> <pre><action function="speak-text" data="\$1"/></pre> <p>[freeswitch_root]/conf/lang/[language]/[language].xml - Make sure that your tts engine and voice are correct in the line:</p> <pre><language name="[language]" say-module="[language]" sound-prefix="\$\${sounds_dir}/en/us/callee" tts-engine="flite" tts-voice="slt"></pre> <p>If you are using flite, you can find information about it here: mod_flite</p> <p>language is the two character language abbreviation</p> <p>freeswitch_root is the root of your Freeswitch installation</p>	Enhancement	Voicemail
SIPX-820	/var/log/messages spammed by ipv6 messages	<p>The system /var/log/messages log is spammed by these messages:</p> <pre>Oct 24 08:30:37 1912 systemd: Reloading. Oct 24 08:30:37 1912 systemd: Binding to IPv6 address not available since kernel does not support IPv6. Oct 24 08:30:37 1912 systemd: Binding to IPv6 address not available since kernel does not support IPv6.</pre> <p>Looks like a service that keeps trying to start but can't because ipv6 is disabled. This should be found and removed or its ipv6 support disabled</p> <p>UPDATE: This happens in connection to sipxagent runs. Further investigation has found that it is rpcbnd that is misconfigured. On CentOS 7.2 and later it comes with default binding on ipv6 also.</p>	Fix	Logs
SIPX-821	Reverse DNS errors (SERVFAIL) in messages log	<p>named is spamming the messages log with reverse DNS errors from queries coming from cluster members.</p>	Bug	Logs
SIPX-825	Fix CFEngine promises	<p>CFEngine promises don't work with newer versions of CFEngine.</p> <p>The policy file parser is stricter in CFEngine >=3.5.0. The parser is now fully compliant with the CFEngine language syntax reference. The main difference you will encounter is that promiser/promisee no longer allows a comma at the end of the line. This will cause your existing policies to produce errors when they are read by CFEngine 3.5.0.</p>	Bug	Config
SIPX-827	Users report registrations are expiring	<p>Registrations are expiring for a while on different CentOS 7 versions of MongoDB, one had 3.4 and another 3.6. This happens only in clusters.</p> <p>Might or might not be related to</p> <p>http://jira.sipxcom.org/browse/SIPX-745</p> <p>Testing has revealed that expired registrations happen on certain nodes, not related to phone location and/or network. Investigation of registrar logs on DEBUG has seen weird expires values on these servers:</p> <pre>grep RegDB sipregistrar.log</pre> <pre>"2019-12-18T06:56:40.156575Z":150380:SIP:INFO:caracal.iuliu.test::7f7300988700:sipxregistry:"RegDB::getUnexpiredContactsUser Identity: 202@iuliu.test Contact: <sip:202@10.3.0.11;transport=tcp;x-sipX-nonat> Expires: 18446744073709551309 sec Call-Id: 253f71d042b2fac4712c900ccf819fa3"</pre> <p>Registration flow for the call-ids seems ok</p> <p>Changed Registrar to default to 60 minute registration grace period. Set this as the new default in system</p>	Bug	Registrar
SIPX-829	Setting DHCP to "unmanaged" disables it instead of leaving it running	<p>A customer issue has showed us that there is some kind of problem with running DHCP in "unmanaged" mode, with the service unexpectedly dying.</p> <p>Investigation has shown that setting DHCP to "unmanaged" causes cfengine to kill the service instead of leaving it running and just not managing the configuration. Upon manual start of the service, it keeps running until the first cfengine run when it is killed.</p> <p>Seems like /usr/share/sipxecs/cfinputs/plugin.d/dhcpd.cf needs to be modified</p>	Fix	DHCP
SIPX-830	"Identity Validity" setting in Proxy is not documented and doesn't seem to work	<p>"Identity Validity" setting in Proxy is not documented and doesn't seem to work.</p> <p>The value of X-Sipx-Authidentity and P-Asserted-Identity headers are signed using MD5. The signature is calculated over the content of the header value, signature timestamp, data from the SIP message and a unique secret, known only to sipXecs components in a given installation. This should prevent (or minimize) the replay attacks on the system making it relatively difficult to spoof the X-Sipx-Authidentity and P-Asserted-Identity headers. Signature includes a timestamp as epoch seconds indicating when the signature was calculated.</p> <p>- "signature-hash" is MD5(<timestamp><secret><from-tag><call-id><identity>)</p> <p>Signature validation fails if the signature is older then a configurable amount of time (Identity Validity defaulted to 300).</p>	Fix	Config
SIPX-835	Update freeswitch flite RPMs	<p>Flite is broken in our rpms, the module does not load, needs updating:</p> <p>From here</p> <p>https://files.freeswitch.org/repo/yum/centos-release/7/x86_64/</p> <p>Flite must be version 2.0.0-1 not 2.0.0-0</p> <pre>flite-2.0.0-1.el7.centos.x86_64.rpm 2017-01-12 22:27 13M flite-debuginfo-2.0.0-1.el7.centos.x86_64.rpm 2017-01-12 22:27 19M flite-devel-2.0.0-1.el7.centos.x86_64.rpm 2017-01-12 22:27 36K</pre>	Fix	Freeswitch
UC-814	1904.centos7 voicemail and cdr restore prompt config options	<p>When uploading just cdr or just voicemail and clicking restore, the config archive options are prompted next. See attached images.</p>	Fix	Restore

UC-817	19.04 sipregistrar webui options	In the 1904 webui the 'log console' option is not defined. It's not defined in the wiki either. I'm not sure what that does? http://wiki.ezuze.com/display/unite/SIP+Registrar Setting does nothing, remove from WebUI	Fix	Config
UC-821	zen 8412: domain alias limitation	Also reported in (4.2, closed) XX-9799 , there is a limitation to the amount of domain aliases you can enter in the webui (varchar 255). Customer workaround was to stand up a second system. Have tested now to 3000 characters	Fix	Config
UC-827	An admin would like to route calls to unassigned DIDs	An administrator would like for calls to unassigned DID on a per-did pool basis should have the option to route to some system extension or reject the call.	Enhancement	DID Pool
UC-837	DID Pool call to unallocated DID	An administrator would like to either play a message that a number is not allocated or re-direct a call to an unallocated number to a particular extension. This should be configurable on a DID pool by DID pool basis.	Enhancement	DID Pool
UC-839	Support APIBAN.org	apiban.org keeps a honeypot generated list of SIP 'bad actors'. An administrator would like to poll apiban.org periodically and update a local list of banned IP's to block with unite / sipxcom's integrated firewall. https://apiban.org/doc.html	Enhancement	Security
UC-841	19.12 sipxecs init script references sipxfreeswitch	The 'sipxecs' service script still references sipxfreeswitch. For example: [root@sipx ~]# service sipxecs status grep freeswitch /etc/init.d/sipxecs: line 21: /etc/init.d/sipxfreeswitch: No such file or directory [root@sipx ~]# ll /etc/init.d/freeswitch -rwxr-xr-x 1 root root 3953 Nov 28 07:24 /etc/init.d/freeswitch [root@sipx ~]# ll /etc/init.d/sipxfreeswitch ls: cannot access /etc/init.d/sipxfreeswitch: No such file or directory [root@sipx init.d]# grep 'freeswitch' /etc/sipxpbx/sipxecs-services.ini sipxfreeswitch	Fix	Config
UC-842	Re-notification on voicemail to flat file migration	When a customer moves to a flat-file storage method for voicemail from mongo the notified flag is not migrated. This causes the system to begin notifying users for all voicemails migrated to file system. The notified flag should be retained when migrating to flat file storage in the xml meta data so that users aren't re-notified of existing voicemails.	Fix	Config