Deprecated - Upgrade to Latest Stable Version

Legacy Page - For historical reference only. Please see Release Notes and Installing / Upgrading pages.

Notes

- When performing an upgrade is always a good idea to backup your production system. It is also good to perform the update on a test system first in order to mitigate risks in production.
- It is also **NOT** recommended you use the administration web interface to upgrade your system from one version to another. The administration web interface for upgrading is best used for minor bug updates.
- You can upgrade from any version to any version as long as you follow the manual steps both before and after your upgrade.
- If you have multiple systems in a cluster (all managed by one Management server). Complete upgrade process on the slave nodes before proceeding to the master server. Once all the systems have been upgraded, log in to the the management UI, go to `System -> Servers`, select all the servers and press `Send Profiles`. Reboot any services when administration service instructs you to do so.

Upgrade Instructions

Step 1. Check the release notes for the version (and versions between where you are at and the version you are upgrading to). Follow each of the pre-install instructions starting with the version you currently have installed. Then come back to this step and continue. So if you currently have version 4.0.4 installed, you want to start with the instructions for 4.0.4 and then proceed to the end of the pre-install instructions for each version.

- Before upgrading from 3.6 or earlier
- Before upgrading from 3.10.x
- Before upgrading from 4.0.4
- Before upgrading from 4.2.x
- Before upgrading from 4.4.0

Step 2. Visit release download area and decide what version is right for you based on the version numbers. Stage and Beta builds are also available on the ftp server. For a description of builds see the Bug Fix and Release Policy. Find the link to the file that ends in `.repo` and right click in your web browser and copy the link.

Then in a root window on the system you wish to upgrade run

```
wget -O /etc/yum.repos.d/sipxcom.repo  <URL to repo file here>
```

Example:

```
wget -O /etc/yum.repos.d/sipxcom.repo http://download.sipxcom.org/pub/sipXecs/14.10/sipxecs-14.10.0-centos.repo
```

Step 3. Shutdown sipXcom and update your system.

```
service sipxecs stop
yum update -y
```

It's good to let your system update all its packages because

1. The binaries were probably built with the latest packages
2. If ever you needed to update a package for security reasons, you'd want to minimize the changes to your system
3. It's often a requirement for getting assistance on mailing list
4. If you do have any problems, most likely others will see the problem as well and provide a quick solution to your issue.

Step 4. Follow each of the post-install instructions starting with the version you currently have installed. Then come back to this step and continue.

- After upgrading from 3.10.x
- After upgrading from 4.0.4
- After upgrading from 4.2.x
- After upgrading from 4.4.0
- After upgrading from 4.6.0 & Later

Step 5. Reboot the system or start your system services back up. (recommend a reboot to pick up any kernel changes from the yum update).

```
reboot
  or
service sipxecs start
```

Complete. if you are upgrading a clustered system, see the **Notes** section at the top of this document for upgrading each slave node.

Before upgrading from 3.6 or earlier

Consider upgrading to sipXecs 3.10 then following instructions from there.

Before upgrading from 3.10.x

The local domain bind zone is "emptied", if you are using the system as a DNS server, you should copy or backup your zone file before the update. It doesn't effect other zone files on the system, just the one sipx is attached to.

Before upgrading from 4.0.4

If you originally installed your system from the sipfoundry ISO in 4.0.4 and are having issues updating, here's some help:

First you have to determine what your redhat-release is:

```
cat /etc/redhat-release
```

If it doesn't say CentOS but says (sipXecs 4.x), then here's what you need to do, AFTER YOU GET A PROPER BACKUP..

Rename your repo file:

```
ls \-l /etc/yum.repos.d
sipxecs-stable-centos.repo
```

If you do not have a CentOS-Base.repo or other repos in there, it's OK, this will probably fix a lot, just hold on.

```
mv sipxecs-stable-centos.repo CentOS-Base.repo
```

Edit the repo to make it JUST a CentOS repo again - remove these lines and save it:

Remove from CentOS-Base.repo

```
[sipxecs-stable]
name=SIPfoundry sipXecs pbx - latest stable version
baseurl=[http://sipxecs.sipfoundry.org/pub/sipXecs/4.0.4/CentOS/5/i386/RPM/]
gpgcheck=0
gpgkey=[https://secure2.pingtel.com/RPM-GPG-KEY-pingtel]
enabled=1
```

Before upgrading from 4.2.x

Remove the old repo file:
Example:

```
rm /etc/yum.repos.d/sipxecs.repo
```

Before upgrading from 4.4.0

Version 4.4.0 is available on CentOS 5 but not CentOS 6. Version 4.6.0 is available on CentOS 6 but not CentOS 5. Therefore you must make a backup your 4.4.0 system, then install a fresh 4.6.0 system, then restore your 4.4 backups by uploading them from the "Restore" web page. I would strongly suggest you test the this process in a lab to reduce the change you will encounter any problems when upgrading the real system as it will be time consuming to revert back. For example, a VMWare virtual machine would be fine or any virtual environment just to ensure restore goes smoothly. The test machine does not have to have same IP address as the original machine as was the case in prior versions.

Be sure to read "After Upgrading to 4.6.0" in this document for notes about restoring from backups.

After upgrading from 3.10.x

The DHCP 120 test will fail if you are using the on board DHCP server. To correct this you need to add the following to the /etc/dhcpd.conf and restart dhcpd (service dhcpd restart). *This is not required if you aren't using the Counterpath Enterprise Clients.*

```
# header section of dhcpd.conf
option sip-servers-name code 120 = text;

# subnet section of dhcpd.conf
option sip-servers-name      "<hostname>:12000/cmcprov/login";
```

After upgrading from 4.0.4

If you have voicemail messages from the *old* version, let's say <=4.0.X, you might hit the XX-9461
A quick fix for that is:

```
# fix all bad messages
export TZONE=`date +%Z`
find /var/sipxdata/mediaserver/data/ -name '*.xml' -exec sed -i "s|\([AP]M\)\s\+</timestamp>|\1 ${TZONE}
</timestamp>|g" {} \;
```

If you have customized versions of vxml files, you'll lose them starting on 4.2.0 as VXML are no longer used for Voicemail.

After upgrading from 4.2.x

No special instructions

After upgrading from 4.4.0

With 4.6 and above, all services are enabled and disabled individually - you don't have to have everything turned on. However, you must enable them for the item to appear in the menus.

Go to System / Servers /Core Services Enable services you want to run on the server

Go to System / Telephony Services - Enable services you desire

Go to System / Instant Messaging - Enable if you want to use the xmpp server features

Go to System / Device provisioning - Enable services you desire

If you wish to install OpenACD run

```
yum install -y sipxopenacd
chkconfig --add mongod
chkconfig mongod on
service mongod start
```

If you wish to install support for audiocodes HD phones

```
yum install sipxaudiocodes
```

After upgrading from 4.6.0 & Later

It's unlikely you upgraded directly to 4.6.0 because installation on CentOS required a full reinstall. You probably restored from backups.

When restoring from backups, not all settings may have migrated correctly. You will need to reset which services you want enabled on each machine. These were called "roles" in 4.4, and are now simply a list of services. Navigate to menu in administration user interface : System/Servers. There you will see links along the left hand side of the web page such as "Core Services" or "Telephony Services". Go through each link and enable the services you would like to have running. Hover your mouse over each service for more information about the service and what function it provides. Services will automatically start in about 10-30 seconds after you've applied your changed.

If the 'superadmin' password is not correctly decrypted during the restore, you can use 'service sipxconfig reset-admin' to reset it. You can then log in to the Admin GUI with no password and set a new password.