Zimbra Collaboration 8.8.9 Upgrade Steps

Table of Contents

Before you upgrade . . . 1
- Database Integrity Checking . . . 1
- Preparing your operating system . . . 1
  - Ubuntu OS . . . 1
  - Red Hat Enterprise Linux/CentOS Linux . . . 2
- License Activation . . . 2
- Upgrading LDAP Replica Servers or Multi-Master Server . . . 3
- Disable SSLv3 Support . . . 4
- Update Default Proxy SSL Ciphers Attribute . . . 4
- Customizing ZCO Installations . . . 5

Upgrade Instructions . . . 5
- Download the Software . . . 5
- Single Server Upgrade Steps . . . 6
  - Process . . . 6
- Multi-Server Environment Upgrade Steps . . . 7
  - Process . . . 7
- Using LMDB as the Supported Back-end for On-disk Database Maps . . . 9

After the Upgrade is Complete . . . 9
- Ephemeral Data Migration . . . 12
- IMAPD Service . . . 13

Remove Current Version and Perform Clean Install of ZCS . . . 13

Status of Your Customization after Upgrade . . . 14

Changes to Customized Themes . . . 14

Before you upgrade

The following tasks might need to be performed before you upgrade. After you review the tasks in this section, go to Upgrade Instructions. Be sure to read the release note information before upgrading.

Bug 105056 noted a problem that can occur during a rolling upgrade if two factor authentication (2FA) is enabled before all mailbox servers have been upgraded to 8.7. In particular, pre-8.7 mailbox servers are not compatible with 2FA.

Accordingly, it is recommended that 2FA is not enabled until all mailbox servers have been upgraded to 8.7.

The following new services are available for installation at upgrade time. Please refer to the *Zimbra Collaboration Administration Guide* for more information and to determine if you wish to install them.

- `zimbra-chat`
- `zimbra-drive`
- `zimbra-imapd`

Database Integrity Checking

Some customers have had corrupted databases prior to upgrade, and the upgrade has in some of those cases exacerbated the problem. In order to detect any corrupted databases as early as possible, we have added an optional step to check the MariaDB database with `zmdbintegrityreport` prior to making any system changes. You are prompted to decide if you would like to run the zmdbintegrityreport.

`zmdbintegrityreport` can take minutes to an hour to run, depending on your system size and disk bandwidth.

`zmdbintegrityreport` is run on a weekly basis from cron on all zimbra-store nodes. Large sites can opt to disable this by setting `zmlocalconfig -e zmdbintegrityreport_disabled=TRUE`. If you choose to disable this, it is recommended that the integrity reports be run by hand during the your normal maintenance windows and prior to running any ZCS upgrades.

Preparing your operating system

Before you upgrade ZCS, Zimbra recommends that the operating system is updated with the latest patches that have been tested with ZCS.

Ubuntu OS

- Ubuntu 16.04 LTS Server Edition (64-bit)
- Ubuntu 14.04 LTS Server Edition (64-bit)

- Ubuntu 12.04.4 LTS Server Edition running the saucy (3.11) or later kernel is required.

If the original install was done with Ubuntu 12.04.2 or earlier, manual intervention is required to switch to the saucy (3.11) or later kernel series. See https://wiki.ubuntu.com/Kernel/LTSEnablementStack for further information.

You can find your current kernel version by running:

```
uname -a
```

For example:

```
build@zre-ubuntu12-64:~$ uname -a
Linux zre-ubuntu12-64 3.11.0-17-generic #31~precise1-Ubuntu SMP Tue Feb 4
21:25:43 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
```

Red Hat Enterprise Linux/CentOS Linux

- If running the RHEL linux distribution, you must have a current valid license from RedHat.
- The server must have a valid yum or apt-get configuration so that it can reach the Zimbra package servers.

- RedHat® Enterprise Linux® 7, AS/ES (64-bit)
- CentOS Linux® 7 (64-bit)
- Red Hat Enterprise Linux 6, AS/ES (64-bit), patch level 4 or later is required
- CentOS Linux 6 (64-bit), patch level 4 or later is required

License Activation

- At the beginning of an upgrade installation, the existing license is validated as being current and qualifies for the upgrade. If your license is expired, an error message displays and the upgrade cannot be performed. Contact Zimbra Sales for a license renewal to continue your upgrade.
- An upgrade installation will not proceed without automatic activation or a manually activated license file. License activations are limited to five activations per license file. If you have previously used all activations prior to upgrading your production system, you must contact Zimbra Sales to enable additional license activations.

All Network Edition installations require a valid license and license activation. New installs will have a 10 day grace period from the license issue date before requiring activation.

License activation is automatic during the install with systems that have external access to the Zimbra license servers. A means of creating manual activations will be provided for systems that do not have external access to the Zimbra license servers. See the *Zimbra Collaboration Administration Guide* for more information.

When upgrading, the way in which ZCO and archiving licensing is enforced might have changed on the server if you are using an older version of Zimbra Collaboration. Older licenses might have `MAPIConnectorAccountsLimit` set to `0` or `ArchivingAccountsLimit` missing in the license. Contact Zimbra Sales for an updated license file prior to upgrading if you have licensed either of these features and your current license does not properly reflect the correct number.

Upgrading LDAP Replica Servers or Multi-Master Server

These instructions apply to ZCS 8.0.0, 8.0.1, 8.0.2 to ZCS 8.0.4 and later.

If you have replica servers or are in multi-master mode, you have to install the Zimbra *LDAP* schema specific to the release you are upgrading to onto the replica servers or onto the multi-master server before you upgrade to ZCS 8.0.4 and later. See Bug 81048.

1. On the master *LDAP* server, perform a software installation only of ZCS 8.0.4 and later.

```
./install.sh -s
```

2. On each replica or additional master *LDAP* server in MMR mode, as the `zimbra` user:
   a. Stop the server via one of the following commands:
      i. `ldap stop`
      ii. `zmcontrol stop`
   b. Move the `zimbra` schema out of the way

```
cd /opt/zimbra/data/ldap/config/cn=config/cn=schema
mv cn={4}zimbra.ldif /opt/zimbra/data/ldap/cn={4}zimbra.ldif.dead
```

   c. Copy the schema from the master *LDAP* server.

```
scp root@<master>:/opt/zimbra/openldap/etc/openldap/schema/zimbra.ldif
cn={4}zimbra.ldif
```

   d. Edit cn={4}zimbra.ldif to change the following two lines:

```
dn: cn=zimbra,cn=schema,cn=config     ------->     dn: cn={4}zimbra
cn: zimbra                            ------->     cn: {4}zimbra
```

e. Start the server via one of the following commands:

   i. `ldap start`

   ii. `zmcontrol start`

3. On the master *LDAP* server run:

```
/opt/zimbra/libexec/zmsetup.pl
```

4. On each replica server run:

```
./install.sh
```

   To continue the upgrade, see Multi-Server Environment Upgrade Steps.

Disable SSLv3 Support

If upgrading to ZCS 8.7.0, you need to completely disable SSLv3 support after the upgrade. Disabling SSLv3 is recommended as a result of the SSLv3 vulnerability described in Alert (TA14-290A).

SSLv3 support has been deprecated by default in 8.6.0, although when upgrading from previous versions of ZCS, some protocols might still be enabled.

- New keys created in ZCS 8.7.0 (or later) have SSLv3 disabled by default.
- Pre-existing keys from earlier versions of ZCS will still have SSLv3 enabled.

Follow the steps in the Zimbra wiki article How to Disable SSLv3 to disable SSLv3 after upgrading to ZCS 8.7.0.

Update Default Proxy SSL Ciphers Attribute

Whenever upgrading, it is recommended that you check the values of the following attributes (`zmprov gcf <attr>`) and compare them with the current default values (`zmprov desc -a <attr>`).

```
zimbraReverseProxySSLCiphers
zimbraReverseProxySSLProtocols
zimbraSSLExcludeCipherSuites
zimbraMailboxdSSLProtocols
```

If you have not performed any recent hardening of your settings, your config should already match the ZCS default; and no action would be required.

In addition, it is recommended to make the following changes:

1. Remove the following from `zimbraReverseProxySSLCiphers`:

```
ECDHE-RSA-RC4-SHA
ECDHE-ECDSA-RC4-SHA
RC4-SHA
```

2. Add the following to `zimbraReverseProxySSLCiphers`:

```
!RC4
```

See https://wiki.zimbra.com/wiki/Cipher_suites for the most current information on cipher suite configuration.

Customizing ZCO Installations

Administrators who want to customize the *ZCO* installation MSI should use the unsigned version of the MSI (`ZimbraConnectorOLK_n.n.n.nnnn_xnn-unsigned.msi`), available in the Zimbra download directory. The modified MSI should then replace the standard signed MSI (`ZimbraConnectorOLK_n.n.n.nnnn_xnn.msi`) in order to be available to end users from `/downloads/index.html` and the *ZCO* auto-upgrade process. (Bug 85067).

Upgrade Instructions

Download the Software

For Network Edition, go to http://www.zimbra.com/downloads/zimbra-collaboration to access the software.

- Before you begin the upgrade, make sure you have a good backup for all users!
- Database reloads are performed on 7.x to any 8.x upgrade.

When you run the install script, if ZCS is already installed, you will be asked if you want to upgrade. Follow the instructions in this release note to perform the upgrade. For additional information, refer to the installation guide.

Zimbra recommends that an install or upgrade session be run with a UNIX command such as `screen` to help prevent an install or upgrade session from terminating before it is completed. This is important when the upgrade includes restoring a configuration that has a large number of accounts.

Example command usage:

```
screen ./install.sh
```

Single Server Upgrade Steps

You do not need to stop the services before upgrading. The upgrade process automatically stops and starts the services as required for the upgrade.

Process

1. Log in as `root` to the Zimbra server and `cd` to the directory where the ZCS Network Edition archive tar file is saved. For example, `cd /var/tmp`. Then type the following commands:

   Unpack the file

   ```
   tar xzvf zcs.tgz
   ```

   Change to the correct directory.

   ```
   cd <expanded-directory>
   ```

   Begin the upgrade installation.

   ```
   ./install.sh
   ```

2. The upgrade script checks if `proxy` and `memcached` are present. If both are found, the upgrade will proceed. If either are missing then the upgrade will abort and alert.

   

   - From 8.7.0 onwards proxy and memcached are required.
   - See Enabling Zimbra Proxy and memcached

3. The Zimbra software agreement is displayed. Read this software license agreement and type `Y`.
4. When `Use Zimbra's packaging server [Y]` is displayed, press `enter` to continue. Your system will be configured to add the Zimbra packaging repository for *'yum'* or *apt-get* so it can install the Zimbra third party packages.
5. When `Do you wish to upgrade? [Y]` is displayed, press `enter` to continue. The upgrade packages are unpacked.
6. The packages are listed. The installer also lists packages that are not installed. If you want to install the packages at this time, type `Y`; otherwise press `enter`. The upgrade checks that there is enough space to perform the upgrade. If there is not enough space, the upgrade stops.
7. When `The system will be modified. Continue? [N]` is displayed, type `Y` and press `enter`. The Zimbra server is stopped, and the older packages are removed. The upgrade process verifies which version of ZCS is being run and proceeds to upgrade the services, restores the existing configuration files, and restarts the server. If you have a configuration with a large number of accounts created, this can take a while.

8. If you have not set the time zone, you will be asked to set it. This sets the time zone in the default COS. The time zone that should be entered is the time zone that the majority of users in the COS will be located in.
9. When Configuration complete, press `enter`.
10. After all *MTA* nodes are upgraded to Zimbra Collaboration 8.8.9, the following commands may be run to fix the default globalconfig values, if necessary.

```
zmprov mcf zimbraMtaCommandDirectory /opt/zimbra/common/sbin
zmprov mcf zimbraMtaDaemonDirectory /opt/zimbra/common/libexec
zmprov mcf zimbraMtaMailqPath /opt/zimbra/common/sbin/mailq
zmprov mcf zimbraMtaManpageDirectory /opt/zimbra/common/share/man
zmprov mcf zimbraMtaNewaliasesPath /opt/zimbra/common/sbin/newaliases
zmprov mcf zimbraMtaSendmailPath /opt/zimbra/common/sbin/sendmail
```

11. DSPAM is not longer shipped starting *Zimbra Collaboration 8.7*. Please enter the following commands to disable it.

```
zmprov ms `zmhostname` zimbraAmavisDSPAMEnabled FALSE
zmlocalconfig -e amavis_dspam_enabled=false
zmamavisdctl restart
```

12. The upgrade is complete. It is recommended that you perform a full backup after performing a major upgrade, due to database schema changes.

Multi-Server Environment Upgrade Steps

Upgrade the servers in the following order. Update each server one at a time, following the instructions under Process below.

1. *LDAP* master server. The *LDAP* master servers must all be upgraded before proceeding, and they must be running as you upgrade the other servers.
2. *LDAP* replicas
3. *MTA* servers - see Using LMDB as the Supported Back-end for On-disk Database Maps.
4. Proxy servers
5. Mailstore servers
6. Optionally install any new IMAPD servers

Process

1. Log in as `root` to the Zimbra server and `cd` to the directory where the ZCS Network Edition archive tar file is saved. For example, `cd /var/tmp`. Then type the following commands:

Unpack the file

```
tar xzvf zcs.tgz
```

Change to the correct directory.

```
cd <expanded-directory>
```

Begin the upgrade installation.

```
./install.sh
```

2. The upgrade script checks if `proxy` and `memcached` are present. If both are found, the upgrade will proceed. If either are missing then the upgrade will abort and alert.

- From 8.7.0 onwards proxy and memcached are required.
- See Enabling Zimbra Proxy and memcached

3. The Zimbra software agreement is displayed. Read this software license agreement and type `Y`.
4. When `Use Zimbra's packaging server [Y]` is displayed, press `enter` to continue. Your system will be configured to add the Zimbra packaging repository for *'yum'* or *apt-get* so it can install the Zimbra third party packages.
5. When `Do you wish to upgrade? [Y]` is displayed, press `enter` to continue. The upgrade packages are unpacked.
6. The packages are listed. The installer also lists packages that are not installed. If you want to install the packages at this time, type `Y`; otherwise press `enter`. The upgrade checks that there is enough space to perform the upgrade. If there is not enough space, the upgrade stops.
7. When `The system will be modified. Continue? [N]` is displayed, type `Y` and press `enter`. The Zimbra server is stopped, and the older packages are removed. The upgrade process verifies which version of ZCS is being run and proceeds to upgrade the services, restores the existing configuration files, and restarts the server. If you have a configuration with a large number of accounts created, this can take a while.
8. If you have not set the time zone, you will be asked to set it. This sets the time zone in the default COS. The time zone that should be entered is the time zone that the majority of users in the COS will be located in.
9. When Configuration complete, press `enter`.
10. After all *MTA* nodes are upgraded to Zimbra Collaboration 8.8.9, the following commands may be run to fix the default globalconfig values, if necessary.

```
zmprov mcf zimbraMtaCommandDirectory /opt/zimbra/common/sbin
zmprov mcf zimbraMtaDaemonDirectory /opt/zimbra/common/libexec
zmprov mcf zimbraMtaMailqPath /opt/zimbra/common/sbin/mailq
zmprov mcf zimbraMtaManpageDirectory /opt/zimbra/common/share/man
zmprov mcf zimbraMtaNewaliasesPath /opt/zimbra/common/sbin/newaliases
zmprov mcf zimbraMtaSendmailPath /opt/zimbra/common/sbin/sendmail
```

11. DSPAM is not longer shipped starting *Zimbra Collaboration 8.7*. Please enter the following commands to disable it.

```
zmprov ms `zmhostname` zimbraAmavisDSPAMEnabled FALSE
zmlocalconfig -e amavis_dspam_enabled=false
zmamavisdctl restart
```

12. The upgrade is complete. It is recommended that you perform a full backup after performing a major upgrade, due to database schema changes.

Using LMDB as the Supported Back-end for On-disk Database Maps

Starting with ZCS 8.5 and later, *Postfix* is linked to *LMDB*, the same back-end ZCS uses with *OpenLDAP*. Prior to ZCS 8.0, *Postfix* was linked to *Berkeley DB*.

ZCS has not officially supported using any *Postfix* on-disk database maps prior to ZCS 8.5. However, these have been used through custom non-preserved modifications to the `postconf` configuration. These modifications will be lost on upgrade.

To restore the modifications post-upgrade, the following steps need to be performed:

1. Run postmap against the database input file to generate an LMDB database.
2. It will be necessary to iterate through the postconf keys that have `hash:/path/to/db` values and update them in LDAP to use `lmdb:/path/to/db` values instead.

Many previously unsupported features that could be used with on-disk database maps are now fully supported by ZCS. Check if your customizations are correctly carried forward when upgrading. See Bug 77586.

After the Upgrade is Complete

After you completed the upgrade, the following might need to be addressed.

- Review How to disable SSLv3.
- Review Cipher suites.

- During the upgrade process, Zimbra might make a binary backup of existing databases when there are major structural changes occurring to the database format for ease of downgrading. Administrators will want to clean these up once they have confirmed a successful upgrade. For *LDAP* servers, these backups are in `/opt/zimbra/data/ldap`, and in the form of `<dbname>.prev.$$` where `$$` is the process ID of the upgrade script. See Bug 81167.
- You should run `zmldapupgrade -b 66387` after upgrading. The `zimbraAllowFromAddress` attribute cannot be set for internal accounts or distribution lists. Running this script will change `zimbraAllowFromAddress` values to grants.

  - This step was not included into the installer-driven upgrade due to potentially long delay for sites that set `zimbraAllowFromAddress` on many accounts.
  - The migration command reports how many accounts had the `zimbraAllowFromAddress` attribute set and how many of them needed migration. One way to verify all accounts got migrated is to run the command again. The total won't change, and the number migrated should be 0. See Bug 66387 for more information.

- If your self-signed SSL certificates have expired, update them.

To check for expired certificates, run the following command as the `zimbra` user:

```
/opt/zimbra/libexec/zmcheckexpiredcerts -days 1 -verbose
```

Zimbra Collaboration requires a valid self-signed or commercial SSL certificate for communication between some components. The self-signed certificates that are automatically created by the Zimbra install have a default expiration.

If you have a Zimbra Collaboration installation that is over one year old and are using self-signed certificates, your certificates will need to be updated either prior to the upgrade or immediately following the upgrade.

After you upgrade, the following commands run as the zimbra user will regenerate the self-signed SSL certificates:

```
sudo /opt/zimbra/bin/zmcertmgr createca -new
sudo /opt/zimbra/bin/zmcertmgr deployca
sudo /opt/zimbra/bin/zmcertmgr deploycrt self -new
```

- If you were using `zmlogger` prior to ZCS 8.0.7, it is possible that numerous `rdd` files could be generated causing large amounts of disk space to be used. ZCS 8.0.7 and later contain a patch that prevents future additional growth of `rdd` files on the logger server. To clean up existing `rdd` files, use the following script to remove `rdd` files from your server. See Bug 85222.

```
sudo su - zimbra
zmloggerctl stop
cd /opt/zimbra/logger/db/data

for nhostid in $(sqlite3 /opt/zimbra/logger/db/data/logger.sqlitedb 'select
id from hosts'); do for ID in $(sqlite3 logger.sqlitedb "select rrd_file,
col_name_19 from rrds Where csv_file == 'imap.csv' and host_id == ${nhostid}" |
egrep "__[0-9]+$" | cut -d'|' -f1 | sort -n | uniq); do mv rrds/${nhostid}-$ID.rrd
/opt/zimbra/logger/db/data/wrong_rrds/; done ; done

for mon in {1..12}; do MON=$(LANG=en_US; date +%b -d 2013-${mon}-01); sqlite3
logger.sqlitedb "DELETE FROM rrds WHERE col_name_19 LIKE '${MON}_%'"; done

sqlite3 logger.sqlitedb "VACUUM;"

zmloggerctl start
rm -R /opt/zimbra/logger/db/data/wrong_rrds
rm /opt/zimbra/logger/db/data/logger.sqlitedb.backup
```

- If you have configured the following keys, you will need to replace them as described here.

The following keys are deprecated:

```
httpclient_client_connection_timeout
httpclient_connmgr_connection_timeout
httpclient_connmgr_idle_reaper_connection_timeout
httpclient_connmgr_idle_reaper_sleep_interval
httpclient_connmgr_keepalive_connections
httpclient_connmgr_max_host_connections
httpclient_connmgr_max_total_connections
httpclient_connmgr_so_timeout
httpclient_connmgr_tcp_nodelay
```

They are replaced by the following keys:

```
httpclient_internal_client_connection_timeout
httpclient_internal_connmgr_connection_timeout
httpclient_internal_connmgr_idle_reaper_connection_timeout
httpclient_internal_connmgr_idle_reaper_sleep_interval
httpclient_internal_connmgr_keepalive_connections
httpclient_internal_connmgr_max_host_connections
httpclient_internal_connmgr_max_total_connections
httpclient_internal_connmgr_so_timeout
httpclient_internal_connmgr_tcp_nodelay
httpclient_external_client_connection_timeout
httpclient_external_connmgr_connection_timeout
httpclient_external_connmgr_idle_reaper_connection_timeout
httpclient_external_connmgr_idle_reaper_sleep_interval
httpclient_external_connmgr_keepalive_connections
httpclient_external_connmgr_max_host_connections
httpclient_external_connmgr_max_total_connections
httpclient_external_connmgr_so_timeout
httpclient_external_connmgr_tcp_nodelay
```

Ephemeral Data Migration

Versions of Zimbra prior to 8.8.9 stored *ephemeral data* in *LDAP*. Examples of *ephemeral data* include:

- `zimbraAuthTokens`
- `zimbraCsrfTokenData`
- `zimbraLastLogonTimestamp`

Zimbra Collaboration version 8.8.9 introduced the ability to store *ephemeral data* in an external service such as SSDB. This is an optional feature; however, it can improve *LDAP* performance and stability.

Please refer to the *Zimbra Collaboration Administration Guide* for more information. Migration of *ephemeral data* out of *LDAP* and into *SSDB* must be performed after an install or upgrade has been completed.

IMAPD Service

Version 8.8.9 of Zimbra Collaboration introduced a new `zimbra-imapd` service that allows you to run the IMAP[S] endpoints outside of the `mailboxd` process. This new service may be deployed on your mailbox servers or on stand-alone machines and it gives you the ability to scale IMAP separately from the mailboxes. This will also reduce the load on your mailbox servers.

Although installation of the new `zimbra-imapd` is intended for larger multi-server installations, it is also fine to use with a single-server installation.

Using `zimbra-imapd` on a single server means that 2 different JVMs will be used to service IMAP[S] requests instead of one, which means that each of them will use less memory which may improve garbage collection performance in each JVM. The separation will improve the robustness of the system. However, this needs to be balanced against the additional overhead of communication between the JVMs.

If the `zimbra-imapd` package is selected for installation during an upgrade, it will be installed, but not configured to start. To enable it to start, you much update the following global configuration options:

- `zimbraRemoteImapServerEnabled`
- `zimbraRemoteImapSSLServerEnabled`

```
zmprov mcf zimbraRemoteImapServerEnabled TRUE
zmprov mcf zimbraRemoteImapSSLServerEnabled TRUE
zmimapdctl start
```

Please refer to the *Zimbra Collaboration Administration Guide* for help with configuration.

Remove Current Version and Perform Clean Install of ZCS

If you do not want to upgrade, but prefer to install Zimbra Collaboration Network Edition as a new installation, when you run the Zimbra Collaboration Network Edition install script, enter `N` when asked `Do you wish to upgrade?`

A warning displays asking if you want to delete all existing users and mail. If you enter `Yes`, all users, mail, and previous files are removed before proceeding with the new installation. Refer to the installation guides for installation instructions.

Status of Your Customization after Upgrade

Upgrading to the newest release does not delete your accounts or change your configuration. Configuration settings stored in *LDAP* and *localconfig* are preserved during upgrades. Any files installed by Zimbra Collaboration might be deprecated and/or overwritten during upgrades, removing any customizations. This includes customized themes, logo branding changes, and crontab changes. Only the core Zimlets are enabled after the upgrade. Zimlets that you customized and/or deployed are preserved during the upgrade but will be disabled. As upgrading of customized Zimlets cannot be tested before the release, Zimbra recommends that you verify that your customized Zimlets work correctly before re-enabling them for your end-users after the upgrade.

When upgrading to Zimbra Collaboration 8.5.x and later from a previous major ZCS version, the upgrade step disables Zimlets that are not the core Zimlets for ZCS in all COSs. If you have enabled other Zimlets at the account level, you might need to manually disable these Zimlets. See Bug 77836.

All entries between the designated comments in the Zimbra crontab file are overwritten with new defaults upon upgrade. Customized backup schedules stored in the Zimbra crontab and customizations to the crontab entry outside the designated comments are preserved.

Changes to Customized Themes

In Zimbra Collaboration 8.5.x and later, a new design for default skins was implemented. Custom skins created for Zimbra 7.x might not work as intended with Zimbra Collaboration 8.5.x and later. Depending on what is in the skin, the issues might range from simple things such as colors being used in the wrong places to larger issues like functional components being hidden or placed in inaccessible areas of the screen. The proper fix for this is to take an existing 8.5.x or later skin, duplicate it, and update the skin to meet the same needs as the old skin. See Bug 62523.