These release notes describe new features and enhancements for Zimbra Collaboration 8.5.0 Open Source Edition. Upgrade instructions are included. Review the Known Issues section for outstanding issues in this release.

Sections include:

- **New Features and Enhancements** on page 1
- **Supported Systems** on page 3
- **Fixed Issues** on page 5
- **Security Fixes** on page 6
- **New Installation** on page 7
- **Upgrade Process** on page 7
- **Known Issues** on page 18
- **Product Documentation** on page 20
- **Bug Reporting** on page 20

### New Features and Enhancements

The following are the major new features and enhancements in Zimbra Collaboration 8.5.0.

**MariaDB**

- MariaDB is a drop-in replacement for MySQL
- MariaDB 10.0 is used with XtraDB storage engine
- No data reload required, as uses same database set

**ActiveSync Performance and Scalability**

- Improved ActiveSync performance and scalability
Mapping of Postfix Configuration Keys to LDAP and localconfig by Version

For information about mapping postfix configuration keys to LDAP and localconfig by version, see the Zimbra wiki page https://wiki.zimbra.com/wiki/Postconf_keys.

Enhancement Bugs for 8.5.0

<table>
<thead>
<tr>
<th>Admin</th>
<th>91116: COS and Per user configuration for EWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Briefcase</td>
<td>84042: Access to shared folders for external users no longer restricted to view-only</td>
</tr>
<tr>
<td>Calendar</td>
<td>79345: Freebusy Interop using EWS</td>
</tr>
<tr>
<td>Install &amp; Upgrade</td>
<td>11063: Ability to configure the amavis behavior on the final spam destination via the zimbraAmavisFinalSpamDestiny attribute.</td>
</tr>
<tr>
<td>Mail - MTA/Spam/Virus</td>
<td>11258: Support for smtpd_sender_login_maps for smtp auth</td>
</tr>
<tr>
<td></td>
<td>41872: Disclaimer support from single, global to per-domain</td>
</tr>
<tr>
<td></td>
<td>44061: Option for domain disclaimer for outgoing mails only</td>
</tr>
<tr>
<td></td>
<td>47625: amavisd-release included with amavisd in Zimbra distribution.</td>
</tr>
<tr>
<td></td>
<td>50044: Domain level signatures are supported</td>
</tr>
<tr>
<td>Mail - Server</td>
<td>66027: Font size selection available in web client</td>
</tr>
<tr>
<td></td>
<td>77287: Admins able to replace existing sieve actions</td>
</tr>
<tr>
<td>Mail - Web Client</td>
<td>3904: Ability to forward conversations</td>
</tr>
<tr>
<td></td>
<td>14572: Option to hide trash contents from threaded view</td>
</tr>
<tr>
<td></td>
<td>78163: Utilize contact pictures in conversation view</td>
</tr>
<tr>
<td></td>
<td>82292: Use name from contact, rather than MIME header</td>
</tr>
<tr>
<td></td>
<td>85921: Add &quot;Copy&quot; action to bubble menu for addresses seen when reading mail</td>
</tr>
<tr>
<td></td>
<td>86255: Add filter for messages from Zimbra Community</td>
</tr>
<tr>
<td>Migration</td>
<td>31646: Support migration of Outlook PST to Zimbra Desktop</td>
</tr>
<tr>
<td>Mobile</td>
<td>86626: Outlook 2013 EAS GA</td>
</tr>
</tbody>
</table>
Other

- 2206: Saved searches can be modified from the edit properties dialog
- 47854: Saved searches are not displayed in contexts where they do not apply
- 56372: Missing zmlocalconfig attributes now documented
- 58747: Replaced MySQL with MariaDB
- 79372: System requirements platform support update
- 79402: Find Shares should display all shares available
- 85216: SMIME Zimlet now works in Linux
- 86182: Preferences > General - reorder items into logical groups
- 86548: Increase font sizes and add Small option

Supported Systems

Network Edition and Open Source supported platforms

- Red Hat® 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.

Operating Systems and Browsers supported with the Administration Console

- Window 7 and Windows XP
  - Internet Explorer 9
  - Firefox 12
  - Safari 5.1.4
  - Chrome 19.0.1084.56 m
- Mac "Leopard", "Snow Leopard"
  - Firefox 12
  - Safari 5.1.4
  - Chrome 19.0.1084.52
- RHEL, Ubuntu, SUSE
  - Firefox - 3.6.17.
  - Chrome - 19.0.1084.52
Zimbra Web Client (Advanced)

- Window XP SP3, Vista and Windows 7
  - IE 8.0 and higher (IE 8 for XP, 9+ for Vista/Win7)
  - Firefox (latest stable version)
  - Safari (latest stable version)
  - Chrome (latest stable version)
- Mac OS X 10.5 "Leopard", 10.6 "Snow Leopard", 10.7 "Lion"
  - Firefox (latest stable version)
  - Safari (latest stable version)
  - Chrome (latest stable version)
- Linux (RHAT, Ubuntu, Fedora, SUSE)
  - Firefox (latest stable version)
  - Chrome (latest stable version)

Zimbra Web Client (Standard)

- Window XP SP3, Vista and Windows 7
  - IE 7.0 and higher (IE 7,8 for XP, 9+ for Vista/Win7)
  - Firefox (latest stable version)
  - Safari (latest stable version)
  - Chrome (latest stable version)
- Mac OS X 10.5 "Leopard", 10.6 "Snow Leopard", 10.7 "Lion"
  - Firefox (latest stable version)
  - Safari (latest stable version)
  - Chrome (latest stable version)
- Linux (RHAT, Ubuntu, Fedora, SUSE)
  - Firefox (latest stable version)
  - Chrome (latest stable version)
Fixed Issues

This section contains information about major fixed issues in this release.

To see a list of all the changes for this release, see the Zimbra Product Portal, (http://pm.zimbra.com/pm_release.php?rel=8.5&prod=zcs)

Major Issues Fixed for 8.5.0

Admin
- 70363: snmpargs uses variable snmp_trap_host
- 76232: Logo image on login screen now renders the same as client login
- 77813: Fixed missing permission issue when trying to edit resource as a delegated admin
- 77832: Fixed issue causing Active Sessions to hang on "Loading.."

Briefcase
- 80398: Upload file now working in User's Briefcase when authenticated as admin
- 91069: Briefcase sharing with guest access fixed

Calendar
- 57930: Appointment summary no longer truncated
- 72637: Ability to schedule all day events in Brasilia timezone
- 81647: Grantee can accept/decline/propose new time appointment for manager rights shared calendar
- 86864: Forward Calendar invites no longer showing as ics attachments when zimbraPrefCalendarAutoAddInvites is set to false
- 87511: Ability to view shared calendar appointments in any Calendar view
- 88287: 'Suggested times' and 'Suggested location' panel moved to bottom pane displays properly
- 89418: "msg: invalid request: no longer missing required attribute

Contacts
- 77796: Name of a new contact shown in auto complete field now considers the value of FileAs

Install
- 94542: Upgrade to OpenSSL 1.0.1i

Mail - Server
- 82279: TagActionRequest and ItemActionRequest for delete operation work properly
- 82703: Draft folder reporting correct counts of mail
- 82739: MTA runs appropriately during SOAP automation run
## Mail - Web Client

- 4098: Saved searches available under "Folders"
- 76253: Forwarding a mail with attached email does not lose attachments when using default options in preferences
- 76776: Fixed issue causing forwarded messages to cache attachments
- 77884: Fixed issues concerning quick reply
- 79590: Alt-a no longer selects whole text instead of inserting i18n character
- 80224: Fixed issue causing message replies to send saved draft copies as part of conversation
- 81794: ZWC now displays new messages as they arrive
- 84713: Fixed issue causing unwanted prompt in IE8/9 when changing font color
- 84984: Fixed issue causing JS error during move operation
- 85084: Ability to move items from shared Sent folder to another shared folder

## Other

- 68198: Ability to drag and drop from new search window
- 82561: Ability to configure GetGrantsRequest
- 84675: WaitSetRequest is no longer fails for block=1
- 86954: Script error fixed when using Delete appointment/Popup dialog button actions

## Search

- 79131: Fixed issue causing Include Shared Items to remain unchecked after changing to Calendar

## Standard

- 59966: Ability to edit appointments within a shared calendar

## Third Party Software

- 50272: Fixed issue causing errors reported by zmdbintegrityreport

## Security Fixes

Zimbra Collaboration 8.5.0 includes other security fixes for previous releases.
New Installation

If you do not want to upgrade as described in the following sections, but prefer to install Zimbra Collaboration as a new installation, when you run the install script, enter N (no) 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 Zimbra Collaboration installation guides for complete installation instructions.

Upgrade Process

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 on page 10.

- Zimbra Database Integrity Check on page 7
- Preparing Your OS on page 7
- Verify Certificates Expiration Date on page 9
- Upgrading LDAP Replica Servers or Multi-Master Server from ZCS 8.0.0, 8.0.1, 8.0.2 to ZCS 8.0.4 through 8.5.0 on page 9
- Update Default Proxy SSL Ciphers Attribute on page 10

Zimbra Database Integrity Check

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`.

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

Note: The 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 your normal maintenance windows and prior to running any ZCS upgrades.

Preparing Your OS

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 14.04 LTS Server Edition (64-bit)
- Ubuntu 12.04 LTS Server Edition (64-bit), patch level 4 or later. The saucy or later kernel is also required.

**Note:** If the original install was done with Ubuntu 12.04.2 or earlier, manual intervention is required to switch to the saucy or later kernel series. See [https://wiki.ubuntu.com/Kernel/LTSEnablementStack](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 OS/CentOS Linux

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

SLES 11 OS only

- SUSE Linux Enterprise Server (SLES) 11, SP3 (64-bit) is required. This is the last supported release of SLES 11.
Verify Certificates Expiration Date

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 Collaboration install have a default expiration.

If you have an 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 zmcertmgr createca -new`
- `sudo zmcertmgr deployca`
- `sudo zmcertmgr deploycrt self -new`

Upgrading LDAP Replica Servers or Multi-Master Server from ZCS 8.0.0, 8.0.1, 8.0.2 to ZCS 8.0.4 through 8.5.0

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. (Bug 81048)

1. On the master LDAP server, perform a software installation only of ZCS 8.0.4 and later.
   
   ```bash
   ./install.sh -s
   ```

2. On each replica or additional master LDAP server in MMR mode, as zimbra user:
   a. Stop the server:
      
      ```bash
      ldap stop or zmcontrol stop
      ```
   b. Move the zimbra schema out of the way
      
      ```bash
      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.
      
      ```bash
      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:
      
      ```bash
      dn: cn=zimbra,cn=schema,cn=config ------->     dn: cn={4}zimbra
      cn: zimbra ------->     cn: {4}zimbra
      ```
   e. Start the server:
      
      ```bash
      ldap start or zmcontrol start
      ```
3. On the master LDAP server run:
   ```bash
   /opt/zimbra/libexec/zmsetup.pl
   ```

4. On each replica server run:
   ```bash
   ./install.sh
   ```

To continue the upgrade, see Multi-Server Environment Upgrade Steps on page 12.

Update Default Proxy SSL Ciphers Attribute

Insecure SSL ciphers have been removed from the default proxy configuration. Existing sites are recommended to review their enabled ciphers and set `zimbraReverseProxySSLCiphers` to `RC4:HIGH:!aNULL:!MD5:!kEDH:!AD:!SSLv2` for maximum security.

**Note:** Some clients might need to be reconfigured if they were previously using a cipher which is now disabled. (Bug 80133)

---

Upgrade Instructions

Download the Software

- To upgrade from 7.0.x - 8.0.7 to 8.5.0, go to www.zimbra.com Open Source Edition Download page to access the software.
- If upgrading 8.0.8, the recommended path is to upgrade to the upcoming 8.6.0 release.

**Important:** Even though the upgrade process does not delete accounts on the mailbox server, you should back up the mailbox server before you begin the upgrade. After you upgrade, you should back up your server again.

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.

**Important:** 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`

**Note:** You cannot revert to a previous Zimbra Collaboration release after you upgrade.
Single-Server Upgrade Steps

Read the release notes before you begin.

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 Open Source Edition archive tar file is saved (cd /var/tmp). Type the following commands:
   
   `tar xzvf zcs.tgz`, to unpack the file
   `cd [zcsversionfullname]`, to change to the correct directory
   `.install.sh`, to begin the upgrade installation
   
   The upgrade script begins by checking for an existing installation.

2. The Zimbra software agreement is displayed. Read this software license agreement and type Y.

3. The installer checks for prerequisites. If any are missing, the upgrade stops. Next, Do you want to verify message store database integrity (Y) is displayed. The default is Yes. This step runs zmdbintegrityreport to verify that the MariaDB database is not corrupt before upgrading to the latest ZCS.

   The zmdbintegrityreport can take minutes to an hour to run, depending on your system size and disk bandwidth. It is preferable that you run zmdbintegrityreport at the time of the ZCS upgrade. If you choose to skip this now, the zmdbintegrityreport will run during a regular scheduled interval after the upgrade is finished.

4. When Do you wish to upgrade? [Y] is displayed, press Enter to continue. The upgrade packages are unpacked.

5. 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.

6. 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.

7. 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.
8. When Configuration complete – press return to exit displays, press Enter. The upgrade is complete.

Multi-Server Environment Upgrade Steps

Upgrade the servers in the following order. Update each server one at a time.

- LDAP master server. The LDAP master servers must all be upgraded before proceeding, and they must be running as you upgrade the other servers.
- LDAP replicas
- MTA servers
- Proxy servers
- Mailstore servers

IMPORTANT: Certificates. If self-signed certificates are used, after the LDAP master is upgraded, the self-signed certificates must be redeployed on all remaining nodes BEFORE they are upgraded. If you do not do this, the upgrade will fail. Use CLI zmcertmgr to add the certificates. As root, type

/opt/zimbra/bin/zmcertmgr deploycrt self

Process

1. Log in as root to the Zimbra server and cd to the directory where the ZCS upgrade archive tar file is saved (cd /var/tmp). Type the following commands:

   tar xzvf zcs.tgz, to unpack the file
   cd [zcsversionfullname], to change to the correct directory
   ./install.sh, to begin the upgrade installation

   The upgrade script begins by checking for an existing installation.

2. Three software license agreements are displayed. Read these license agreements and enter Y for each.

3. The installer checks for prerequisites. If any are missing, the upgrade stops.

4. When you upgrade the mailstore server, the installer displays Do you want to verify message store database integrity (Y) is displayed. The default is Yes. This step runs zmdbintegrityreport to verify that the MariaDB database is not corrupt before upgrading to the latest ZCS.

   Running zmdbintegrityreport can take minutes to an hour to run, depending on your system size and disk bandwidth. It is preferable that you run zmdbintegrityreport at the time of the ZCS upgrade. If you choose to skip this now, the zmdbintegrityreport will run during a regular scheduled interval after the upgrade is finished.
When the MariaDB software versions are changed during upgrades, the underlying database tables need to be upgraded. The zmdbintegrityreport does this automatically during it's first run and will report the changes. These are normal and should not cause alarm when upgrading.

5. When **Do you wish to upgrade? [Y]** is displayed, press **Enter** to continue.
   The upgrade packages are unpacked.

6. The packages you want to install on the server should be marked **Y**. All other packages should be marked **N**.
   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?** is displayed, type **Y** and press **Enter**. The 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 system. If you have a configuration with a large number of accounts created, this can take a while.

8. When **Configuration complete – press return to exit** displays, press **Enter**.
   The upgrade is complete. Continue to upgrade each server.
After the Upgrade is Complete

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

- 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. (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 `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. (Bug 66387)

- If your self-signed SSL certificates have expired, update them. See Verify Certificates Expiration Date on page 9.

- If using zmlogger prior to ZCS 8.0.7, see Cleanup Procedure for Logger Host on page 15.

- 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`

  and are replaced by the following keys:

  - `httpclient_internal_client_connection_timeout`
  - `httpclient_internal_connmgr_connection_timeout`
  - `httpclient_internal_connmgr_idle_reaper_connection_timeout`
Cleanup Procedure for Logger Host

When 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 contains 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. (Bug 85222)

Cleanup Script

```
sudo su - zimbra
zmloggerctl stop
cd logger/db/data
mkdir -p wrong_rrds
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 == ${nhostid}" | grep "^[0-9]+$" | cut -d'|' -f1 | sort -n | uniq); do mv rdds/${nhostid}-${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
```
Updating Your MariaDB Table

If you upgrading from 6.X to ZCS 8.5.0, MariaDB table upgrade is required after upgrading. If you do not upgrade MariaDB, regular reports from zmdbintegritreport are going to flag warnings in your MariaDB table. Customers can avoid these errors in the zmdbintegritreport output by executing /opt/zimbra/libexec/scripts/migrate20100913-Mysql51.pl.

MariaDB upgrades are not automatically run during the upgrade to 8.5.0, because of the time that it takes this process to run. There is no known performance impact when running in production without doing this MariaDB table upgrade.

Applying the Mysql51.pl script requires all Zimbra services except mysql.server to be stopped.

This script should be executed on all the mailstore servers where the mailboxd process is running. For a 4000 mailbox, 250 MB mailbox size, the script could take about 70 minutes to run. Customers should schedule their maintenance window accordingly. To run the script:

1. Switch to zimbra user.
   su - zimbra
2. Stop mailboxd services to avoid email communications that might cause an interruption.
   zmmailboxdctl stop
3. Execute the perl script to upgrade the database tables.
   /opt/zimbra/libexec/scripts/migrate20100913-Mysql51.pl
4. Start the mailboxd service.
   zmmailboxdctl start

Setting iframes

Zimbra Web Client no longer works in an iframe. If you want to continue to use iframe, modify zimbra.web.xml.in. The parameter must be set to TRUE.

1. As zimbra user, change directories. Type
   cd /opt/zimbra/jetty/etc
2. Edit the file zimbra.web.xml.in
3. To use iframes, in the <filter-name>Set Header Filter</filter-name> <filter-class>com.zimbra.webClient.filters.SetHeaderFilter</filter-class> section, add the following
   <init-param>
4. Restart ZCS.
  zmcontrol restart

Remove Current Version and Perform Clean Install of ZCS

If you do not want to upgrade, but prefer to install Zimbra Collaboration Open Source Edition as a new installation, when you run the Zimbra Collaboration install script, enter N (no) 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.

Note: When upgrading to Zimbra Collaboration 8.5.0 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. (Bug 77836)

All entries between the designated comments in the Zimbra crontab file are overwritten with new defaults upon upgrade.
Changes to Customized Themes

In Zimbra Collaboration 8.5.0, a new design for default skins was implemented. Custom skins created for Zimbra 7.x might not work as intended with Zimbra Collaboration 8.5.0. 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 8.5.0 skin, duplicate it, and update the skin to meet the same needs as the old skin. (Bug 62523)

Known Issues

Zimbra engineering has identified a number of issues with the software, and we are actively working to resolve them. The following are issues that are most likely to occur. All known bugs are listed in Zimbra’s Bugzilla database, available on the Zimbra web site, at www.zimbra.com.

Known Issues for 8.5.0

The following are known issues in Zimbra Collaboration 8.5.0. This section includes miscellaneous known issues, EWS and Mailstore Split Server known issues.

<table>
<thead>
<tr>
<th>Issue #</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>84264</td>
<td>Workflows in the standard HTML client are broken.</td>
</tr>
<tr>
<td>88451</td>
<td>Error received when clicking to date from mini-calendar.</td>
</tr>
<tr>
<td>91102</td>
<td>Problems in preview generation for empty csv file.</td>
</tr>
<tr>
<td>92347</td>
<td>FlushCache for skin does not work in split server environment.</td>
</tr>
<tr>
<td>92403</td>
<td>GetAvailableLocalesRequest returns only English locales in split server environment.</td>
</tr>
<tr>
<td>92405</td>
<td>Skins not available in split server environment. GetAvailableSkinsRequest returns empty list.</td>
</tr>
</tbody>
</table>
Mailstore Split Server Known Issues:

- Proxy+Memcached is mandatory for a mailstore to operate in split mode.
- Need to have at least one web-only node and one service-only node for the proxy to work. Without this, the proxy will not run and will cause an error.
- Localconfig attribute `zimbra_zmprov_default_soap_server` should be set to one of the servers running SOAP (for example, one of the mailstores running 'service' webapp).
  
  ```
  zimbra@zqa-067:~$ zmlocalconfig -e zimbra_zmprov_default_soap_server=zqa-063.eng.example.com
  ```
- The web-only node needs to know where the memcached is running. This is done by setting `zimbraMemcachedClientServerList` to the server where the memcached is running.
  
  ```
  zimbra@zqa-067:~$ zmprov gcf zimbraMemcachedClientServerList
  zimbraMemcachedClientServerList: zqa-063.eng.example.com:11211
  ```
- `zmproxyconfgen` needs to be run after both the web-only and service nodes are installed to regenerate the correct nginx confs. `zmproxyctl restart` is required after this.
- Administrator console is working, but only through the proxy using `zimbraAdminProxyPort(9071)` after setting `zimbraReverseProxyAdminEnabled` to TRUE.
- For service (SOAP/REST) to User Interface (JS/css/html) reqs from mailclient server in splitmode. Set `zimbraWebClientURL` on mailclient server to point to Nginx. For example
  
  ```
  zmprov mcf zimbraWebClientURL https://zqa-063.eng.example.com
  ```
- Skins not available in split server environment.
- GetAvailableLocalesRequest returns only English locales in split server environment. See bug 92403
- FlushCache for skin does not work in split server environment. See bug 92347
- Skims are not fully functional. See bug 92068
- MariaDB running on webapps only nodes. See bug 92634
- GetAvailableLocalesRequest returns only English locales in split server environment. See bug 92403
- FlushCache for skin does not work in split server environment. See bug 92347
- Skims not available in split server environment.
- GetAvailableLocalesRequest returns empty list. See bug 92405
- In order for some things like change password link, calendar launch in separate window etc to work in split-mode & use proxy instead of jetty the following attributes have to be set:
  
  ```
  zimbraPublicServiceHostname - proxy hostname
  zimbraPublicServiceProtocol - proxy protocol (http or https)
  zimbraPublicServicePort - proxy port
  ```
  See the following bugs 92702 and 92732
- Mailstore split: "View mail" not working in admin console - not found error. See bug 92694
- Split server: NPE when user tries to access external share invitation link. See bug 92799
Product Documentation

Online help and ZCS documents are available on the administration console. Documentation can also be found on the Zimbra web site, and the Zimbra wiki has articles that the support team and the community have written in response to troubleshooting and administration issues.

Bug Reporting

If you encounter problems with this software, go to http://bugzilla.zimbra.com to submit a bug report. Make sure to provide enough detail so that the bug can be easily duplicated. Also, to discuss issues and this software in general, please visit our community forums at http://www.zimbra.com/forums.

Legal Notices

Copyright © 2005-2014 Zimbra, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. "Zimbra" is a registered trademark of Zimbra, Inc. in the United States and other jurisdictions. You may not alter or remove any trademark, copyright, or other notice from copies of the content. All other marks and names mentioned herein may be trademarks of their respective companies.

Zimbra, Inc.
3000 Internet Blvd., Suite 200
Frisco, Texas 75034
www.zimbra.com
August 2014