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

**Important:** If you are running the 8.5.0_GA_3040 build, the 8.5.0 Patch 1 (8.5.0_P1_3043 build) is required. If you are running the 8.5.0_GA_3042 build, you do not need the patch.

Sections include:

- New Features and Enhancements on page 1
- Supported Systems on page 5
- Fixed Issues on page 7
- Security Fixes on page 10
- New Installation on page 10
- Upgrade Process on page 10
- Configuring the Community Tab with Single-Sign On on page 22
- Known Issues on page 24
- Product Documentation on page 29
- Bug Reporting on page 29
- Revision History on page 30

**New Features and Enhancements**

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

**Zimbra Touch Client for Tablet and Phone Devices**

- Provides support for touch-capable mobile devices.
- Features are a subset of the features found in the Zimbra Web Client, including Mail, Contacts, and Calendar.
Zimbra Web Client Offline Mode

- Zimbra Web Client supports offline capability using browser HTML5 API, which allows you to continue using the web client and accessing your data without connectivity to the server.
- When offline, one day to one month cached data is available from the browser.
- Transitioning from online mode (normal mode) to offline mode, and vice versa, is automatic, seamless and CPU conservative.
- A subset of application features are supported and enabled offline.
- Machine registration and other security is supported.
- Supported browsers include Google Chrome and Mozilla Firefox.

High-Fidelity Document Preview

- The document preview feature has been enhanced with a High-Fidelity preview, using LibreOffice.

Exchange Web Services (EWS)

- Native EWS support
- Supports Outlook for Mac and Apple Mail
- No plug-in required
- Free/Busy interoperability with Exchange Server
- Available for an additional charge. Contact Zimbra Sales for more information.

ZCO Improvements

- Log file improvements
- Connection security improvements
- Share message support, with Accept Share and Decline Share options available
- Sync improvements
- Chinese Traditional (zh_TW) added to localization

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 Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>91116: COS and Per user configuration for EWS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Briefcase</th>
</tr>
</thead>
<tbody>
<tr>
<td>84042: Access to shared folders for external users no longer restricted to view-only</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Calendar</th>
</tr>
</thead>
<tbody>
<tr>
<td>79345: Freebusy Interop using EWS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connector for Outlook</th>
</tr>
</thead>
<tbody>
<tr>
<td>44151: Accept Share and Decline Share buttons available in Outlook 2010 main and message windows</td>
</tr>
<tr>
<td>89956: Enable &quot;Secure Connection&quot; per default in ZCO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Installation and Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>11063: Ability to configure the amavis behavior on the final spam destination via the zimbraAmavisFinalSpamDestiny attribute.</td>
</tr>
<tr>
<td>84611: Added RHEL7 64-bit support</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mail - MTA/Spam/Virus</th>
</tr>
</thead>
<tbody>
<tr>
<td>11258: Support for smtpd_sender_login_maps for smtp auth</td>
</tr>
<tr>
<td>41872: Disclaimer support from single, global to per-domain</td>
</tr>
<tr>
<td>44061: Option for domain disclaimer for outgoing mails only</td>
</tr>
<tr>
<td>47625: amavisd-release included with amavisd in Zimbra distribution.</td>
</tr>
<tr>
<td>50044: Domain level signatures are supported</td>
</tr>
<tr>
<td>82888: Migrate MTA related LC keys to LDAP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mail - Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>38631: Exchange Web Services (EWS) support</td>
</tr>
<tr>
<td>66027: Font size selection available in web client</td>
</tr>
<tr>
<td>77287: Admins able to replace existing sieve actions</td>
</tr>
<tr>
<td>82848: EWS Support, Contacts</td>
</tr>
<tr>
<td>82849: EWS Support, Calendar</td>
</tr>
<tr>
<td>82850: EWS Support, Tasks</td>
</tr>
</tbody>
</table>
Mail - Web Client

- 3904: Ability to forward conversations
- 12679: Archive button available when Archive Zimlet enabled
- 14572: Option to hide trash contents from threaded view
- 78163: Utilize contact pictures in conversation view
- 82292: Use name from contact, rather than MIME header
- 85921: Add "Copy" action to bubble menu for addresses seen when reading mail
- 86255: Add filter for messages from Zimbra Community

Migration

- 31646: Support migration of Outlook PST to Zimbra Desktop

Mobile

- 60247: Web application available for touch client
- 79365: ActiveSync scalability
- 84581: Touch Client Redesign
- 86626: Outlook 2013 EAS GA

Offline

- 79344: Offline mode web application

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
- 79364: Always On Architecture (Distributed Datastore)
- 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

Server

- 91102: Fixed issues in preview generation for empty csv file
Supported Systems

**Network Edition and Open Source supported platforms**

- Red Hat® Enterprise Linux® 7
- CentOS Linux® 7
- Red Hat Enterprise Linux 6, patch level 4 or later is required
- CentOS Linux 6, patch level 4 or later is required.
- Ubuntu 14.04 LTS
- Ubuntu 12.04.4 LTS Server Edition running the saucy (3.11) or later kernel is required. **Note**: 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](https://wiki.ubuntu.com/Kernel/LTSEnablementStack) for further information.
- SUSE Linux Enterprise Server 11, SP3 or later - Deprecated

**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.

Major Issues Fixed for 8.5.0

Administrator Console

- 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.."
- 95265: Fixed issue causing removal of Webapp services when editing the server.

**Important!** For bug fix 95265, if you are running the 8.5.0 GA build 3040 avoid using the Administrator Console to make any changes to the server config for a store server, as it will lose all of its services the next time it is restarted (no web UI, mailboxes, or admin console). You must install the 8.5.0 Patch 1 (build 8.5.0_P1_3043) for this issue to be resolved. If you are running the 8.5.0 GA build 3042, you do not need the patch.

Admin Utilities

- 70363: Prior to 8.5.0 and at some point after ZCS 3.2, the snmp_trap_host value was incorrectly set to an email address instead of a hostname. However, the snmp_trap_host key was never used by anything in those releases, so this issue was not noticed. Starting with ZCS 8.5.0 and later, snmp_trap_host is correctly used to route SNMP traps. This exposed the issue that the snmp_trap_host value may be set incorrectly. If it is incorrect, the zmswatchctl process will fail to start (see bug 95221). If zmswatchctl refuses to start, it is important to check the value of snmp_trap_host on that server. If it is an email address instead of the server hostname, it will be necessary to modify the value using zmlocalconfig.

Back-up and Restore

- 84548: Restore operation now retrieves all backed up items.

Briefcase

- 80398: Upload file working in User’s Briefcase when authenticated as admin
- 91069: Briefcase sharing with guest access fixed
**Calendar**
- 57930: Appointment summary no longer truncated
- 66603: Fixed split and merge calendar related UI issues in day view
- 68490: Fixed issue causing accepted appointments within shared mailbox adding to random calendars
- 72637: Ability to schedule all day events in Brasilia timezone
- 77517: Fixed issue causing ZCS Calendar Auto-reply message to not send
- 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

**Connector for Outlook**
- 80482: Outlook 2003 has been deprecated and noted in the customer documentation.
- 59788, 83334: If upgrading from a version of ZCO 7.2.5 or 8.0.5 to ZCO 8.5, the alias email address is no longer included in the "To" field when using "reply all" to a mail message. This applies to new mail arriving into the ZDB. If this is desired for existing mail, a new ZDB/profile needs to be created.

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

**Conversion - Server**
- 77446: Preview attached PDF files displays properly

**Installer**
- 94178: The value for snmp_trap_host is now correctly set to an email address instead of a hostname.
- 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
- 89314: Default changed for zimbraMobilePolicyMaxEmailAgeFilter
- 92543: Rolling upgrade: fixed network service error sharing between 8.0.x and 8.5.0
Mail - MTA/Spam/Virus

- 83784: Support added for split domain customizations to be portable
- 95230: Fixed the variable used to enable the policy daemon (smtpd policyd). Changed to the correct attribute of zimbraMtaEnableSmtpdPolicyd.

**Important!** For bug fix 95230, if you are running the 8.5.0_GA_3040 build, the 8.5.0 Patch 1 (8.5.0_P1_3043 build) is required for this bug fix. If you are running the 8.5.0_GA_3042 build, you do not need the patch.

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 l18n 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
- 81834: Fixed issue causing DL not showing expand option
- 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

Migration

- 89594: All categories are now migrated using PST/Exchange migration tools

Mobile

- 61123: Ability for iPad to scroll body when forwarding large message
- 87170: Fixed issued causing calendar data to not display correctly.

Other

- 68198: Ability to drag and drop from new search window
- 82561: Ability to configure GetGrantsRequest
- 84489: OpenOfficeExtension default in ZCS.Next
- 84675: WaitSetRequest is no longer fails for block=1
- 86954: Script error fixed when using Delete appointment/Popup dialog button actions
- 89623: Fixed Jetty ThreadMonitor related thread leak

Search

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

Standard HTML Client

- 59966: Ability to edit appointments within a shared calendar
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 10
- **Preparing Your OS** on page 11
- **Verify Certificates Expiration Date** on page 11
- **License Activation** on page 12
- **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 12
- **Update Default Proxy SSL Ciphers Attribute** on page 13
- **Customizing ZCO Installations** on page 13

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`.

---

### Third Party Software

- 50272: Fixed issue causing errors reported by zmdbintegrityreport

### Zimlets

- 90182: S/MIME requirements build process revised.
- 84061: Fixed issue causing S/MIME Zimlet to bypass Foxyproxy to get Firefox's browser proxy.
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 12.04.4 LTS Server Edition running the saucy (3.11) or later kernel is required. **Note:** 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 OS/CentOS Linux

- 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

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

License Activation

All network edition installations require license activation. New installs will have a 10 day grace period from the license issue date before requiring activation. For upgrade installations, 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 ZCS installation guides 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 `MAPICConnectorAccountsLimit` set to 0 or `ArchivingAccountsLimit` missing in the license. Contact 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.

**Important:** Note that an upgrade installation will not proceed without automatic activation or a manually activated license file. Also, 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.

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.
   
   ./install.sh -s

2. On each replica or additional master LDAP server in MMR mode, as zimbra user:
   a. Stop the server:
      
      ldap stop or 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:
   
   ldap start or 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 on page 16.

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)

Customizing ZCO Installations

Administrators who want to customize the ZCO installation MSI should use the unsigned version of the MSI (ZimbraConnectorOLK_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.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

- To upgrade from 7.0.x - 8.0.7 to 8.5.0, go to www.zimbra.com Network 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:**
- 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.

**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 Network 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 and then checks for the Zimbra license. If the license is found, the number of current users and the number of user licenses is listed.

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. The installer checks for a recent backup. If one is not found, Do you wish to continue without a backup? is displayed. The default is N. If you select N, you exit the upgrade. Run a backup and then restart the upgrade.

4. 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.

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 return to exit** displays, press **Enter**.
The upgrade is complete.

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

**Important:** Restoring a full backup to a newer release can fail due to schema differences. It is highly recommended to perform a full backup after every major upgrade to ensure that you have a restore point on the upgraded version.

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

```
sudo /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.

Mailstore server - The installer checks for a recent backup. If one is not found, **Do you wish to continue without a backup?** is displayed. The default is **N**. If you select N, you exit the upgrade. Run a backup and then restart the upgrade.

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.

**Note:** When upgrading the zimbra mail store, the upgrade checks for the Zimbra license. If the license is found it lists the number of current users and the number of user licenses. If it is not found, press **Enter to continue**. You can add the license later from the administrator's console.

8. When **Configuration complete – press return to exit** displays, press **Enter**. The upgrade is complete. Continue to upgrade the remaining servers.

9. It is recommended that you perform a full backup after performing a major upgrade, due to database schema changes.
**Important:** Restoring a full backup to a newer release can fail due to schema differences. It is highly recommended to perform a full backup after every major upgrade to ensure that you have a restore point on the upgraded version.

**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 8.5. Check if your customizations are correctly carried forward when upgrading. (Bug 77586)

**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 11.

- If using zmlogger prior to ZCS 8.0.7, see Cleanup Procedure for Logger Host on page 20.

- 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`
  - `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`
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 == ${nhostid}" | egrep "^[0-9]+$" | 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
rm /opt/zimbra/logger/db/data/logger.sqlitedb.backup
```

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 zmdbintegrityreport are going to flag warnings in your MariaDB table. Customers can avoid these errors in the zmdbintegrityreport 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>`
   
   `<param-name>allowInFrame</param-name>`
   
   `<param-value>true</param-value>`

   `/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 Network Edition as a new installation, when you run the Zimbra Collaboration Network Edition 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. 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 8.5.0, 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)

### Configuring the Community Tab with Single-Sign On

1. Deploy a Zimbra Community Server with "zimbracollaboration" integration
   For more information about deploying the Zimbra Community Server, contact your Zimbra sales or support representative.

2. In Zimbra Community configure an OAuth client for Zimbra Collaboration. This will produce two settings: Client ID and Client Secret.

3. Create users user1 and user2 in Zimbra Community.

5. Create domain example.com in Zimbra Collaboration Server.

6. Use zmprov to configure the following attributes of domain example.com in Zimbra Collaboration:
   • zimbraCommunityAPIClientID - set to Client ID that you created on step 2
   • zimbraCommunityAPIClientSecret - set to Client Secret that you created on step 2
   • zimbraCommunityBaseURL - set to the root URL of your Zimbra Community deployment
   • zimbraCommunityHomeURL - set to "/integration/zimbracollaboration"
   • zimbraCommunityUsernameMapping - set to "uid"

7. Use zmprov to configure the following attribute of default COS (or the COS that users who have Community tab will be assigned to):
   zimbraFeatureSocialExternalEnabled = TRUE

8. Create users - user1@example.com and user2@example.com in Zimbra Collaboration with default COS

9. Log in to Zimbra Web Mail UI as user1@example.com and verify that Community Tab is visible and that it loads user1’s content from Zimbra Community

10. Log in to Zimbra Web Mail UI as user2@example.com and verify that Community Tab is visible and that it loads user2’s content from Zimbra Community

Community Tab Attribute Descriptions

- **zimbraCommunityUsernameMapping** - specifies the name of Zimbra Account LDAP attribute that maps to Zimbra Community user names. Normally, this should be "uid", however, it is possible to configure both products in the way that user1@example.com maps to "someotherusername" in Zimbra Community or that Zimbra Community uses full email addresses for login instead of the uid.

- **zimbraCommunityHomeURL** - this is the URL that loads in Community Tab. It can be configured differently on global >domain >cos >account level so that different accounts load different pages in Community Tab. Currently, only /integration/zimbracollaboration is suitable for being loaded in the tab.

- **zimbraCommunityBaseURL** - points to Zimbra Community installation. It is possible to configure different domains, COSes or even accounts to point to different Zimbra Community servers.

**Note:** zimbraCommunityAPIClientID and zimbraCommunityAPIClientSecret have to be provisioned on Zimbra Community server that matches zimbraCommunityBaseURL
- **zimbraFeatureSocialExternalEnabled** - turns Community tab in Zimbra Mail UI on/off on COS/account level
- **zimbraCommunityID** - can be used when user IDs in Community do not correspond to any attribute of users in Collaboration. In this case, the admin must set zimbraCommunityID of each user to their Community ID and set zimbraCommunityUsernameMapping to "zimbraCommunityID". Normally, both Community and Collaboration should be using the same Directory.

### 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, and known issues for the Exchange Web Services and Web Application Server Split.

<table>
<thead>
<tr>
<th>Issue #</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.5.0</td>
<td></td>
</tr>
</tbody>
</table>

#### Administrator Console

- 83352: Wizard disappears when user tries to move it and leaves the screen locked.
- 84432: Active sessions of the domain are not getting displayed at monitor > sever statistics.
- 92303: Add community tab related settings in admin console at domain/cos/account level.
- 93180: Delegated admin cannot create new delegated admin.
- 93756: Admin group members do not become delegated admins.
- 93620: Cannot add voice/chat service.
- 94158: Session information not displayed in admin console.
- 94306: Clicking on backup in admin console shows no data.
- 94096: EWS and touch client license count missing in "Current License Information".

#### Briefcase

- 89056: In IE 10, the delete confirmation dialog is hidden behind briefcase (PDF) document preview.

#### Calendar

- 94924: Cannot unselect tags in calendar.
- 87613: Drag and drop of recurring all day event changes from 1 day to 2 days.
- 83558: Appointment becomes read-only if saved with from address as persona (delegated access).

#### Connector for Outlook

- 92875: MoveZDB functionality broken for OL 2013.
## Conversion Server

## Exchange Web Services - Calendar
- 94923: SOBO meeting: Attendee participation status is not updated in sharee's MacOutlook.
- 94925: SOBO meeting: Meeting created in sharee's primary calendar.

## Exchange Web Services - Misc
- 89548: Read/unread properties not retained in native Mail app.
- 89550: Native mail app keeps on downloading messages.
- 90254: Wrong recurrence pattern for yearly recurring type task created in MacOutlook.
- 91089: Forwarding a mail to attendee from web client does not add attendee in EWS.
- 91512: Attendee freebusy status is always tentative in meeting synced to MacOutlook.
- 92108: Draft updated in MacOutlook becomes non-editable.
- 92130: Clear message category from MacOutlook - doesn't remove category in ZWC.
- 92138: Draft created in Mail, MacOutlook if updated from ZWC - creates duplicate draft.
- 92648: No OOO reply to external user in case of modified OOO preference.
- 94146: Renaming server rule in MacOutlook does not work.
- 94410: Line breaks replaced by "D;" in out of office message in Outlook.
- 94562: ResolveNames sometimes does not return Name thus showing blank user name of sharee.
- 94757: Updating contact in MacOutlook adds field "postaladdressIndex" in ZWC/ZCO contact.
- 94779: Zimbra EWS crashes Mail on OS X Yosemite.
- 95049: Deleting message from trash in ZWC does not delete in Native Mac Mail.

## Exchange Web Services - Rules
- 90997: ZWC rule with size (specified range) condition is not synced correctly in MacOutlook.
- 94420: "Sent to" exception in MacOutlook rule is not mapped correctly.
Exchange Web Services - Sharing

- 91434: Update Item failures observed for items in "folder with Reviewer rights" mounted in MacOutlook.
- 91448: MacOutlook allows to update items in folder shared with Viewer rights.
- 91456: From address is of sharee for replied email in shared folder.
- 91458: Move message to subfolder in shared folder generates synchronization.
- 91462: Message delete action in shared folder with Manager rights is not synced to the owner.
- 91466: Sharing already shared folder in MacOutlook by non-admin user sends share created notification.
- 91506: Category applied to shared item is not syncing to/from MacOutlook.
- 91524: Updating calendar item fails in MacOutlook for sharee having "Manager" rights on share.
- 93134: Private appointment cannot be opened in MacOutlook.
- 94693: Shared Contacts folder not syncing if sharer is on different mailstore.
- 94755: Shared contact created in MacOutlook is duplicated in MacOutlook.
- 94960: "On behalf of" meeting response is not sent if sharer and sharee are on different mailstores.
- 94968: Sharing by Admin MacOutlook user sends share notification for local folder.
- 94970: Update/Delete Calendar items not synced for MacOutlook user.
- 95004: Update/Cancellation notification by sharee does not have Sent by info.

Exchange Web Services - Server

- 95072: Native Mac Mail trash folder display issue
- 95074: Delete folder action sometimes fails in Native Mac Mail

Exchange Web Services - Syncing

- 90152: Issues with task syncing on native Mac Reminders client.
- 91342: Error while syncing exceptions from web client to EWS.
- 94721: Meeting content synced from ZWC to MacOutlook has additional info.
- 94819: Few items are not immediately synced to MacOutlook using GetEvents.

Exchange Web Services - Tasks

- 88864: "Not Started" task status is synced as "In Progress" in MacOutlook.
- 88924: Issues with update/delete task reminder from MacOutlook.
- 89099: Wrong recurrence pattern for task created in ZCO.
- 90236: Recurrence task without start date created in MacOutlook is synced as regular task in ZCO.
- 90250: Incorrect recurrence pattern for task created with week day option in ZCO.
- 91946: Editing recurrence pattern of task in MacOutlook results creation of duplicate task.
- 94400: "Mark as Complete" task in MacOutlook does not remove reminder.

Installer

- 91322: Installer does not preserve split mode of zimbra-store module between upgrades.

Localization:

- 90842: [pt-PT] TM and UI strings in pt-BR.
### Mail - Server
- 93545: Subjects which contains some unicode characters are garbled.
- 90268: Conversations are shown as flagged when no individual messages are flagged.
- 92561: Fix the REST API against CSRF attack.

### Mail - Web Client
- 86326: New Message Button Fails.
- 92100: Intermittently message content shows partially blank for long message.
- 93210: Updating Contacts from TO, CC and BCC lines.
- 90010: Adding signature while composing a reply in text mode results in a warning message.

### Migration
- 91007: ZMT: A certain mail crashes the migration tool.
- 92940: ZMT: CLI tool puts some mails into the Root folder (id 1).
- 90018: Sent message after editing a reply draft becomes a separate conversation.

### Standard HTML Client
- 84264: Workflows in the standard HTML client are broken.
- 88451: NPE(A client error occurred) on clicking to date from mini calendar.
- 94570: Contacts added to group from GAL shows account id of those contacts and gets garbled.
- 88590: Clicking to Previous page/Next page/Day/Month/List opens new appointment page every time.
- 95065: Modify Standard HTML Client to pass CSRF token for REST API.

### Tasks
- 85396: Notification/Reminder.
- 95025: Intermittently task app broken.

### Third Party
- 92379: Outlook forcing database rebuild.
### Web Application Server Split

- Proxy and Memcached are mandatory for a mailstore to operate in Web Application Server split mode.
- Localconfig attribute `zimbra_zmprov_default_soap_server` should be set on the UI server to one of the mailstore servers (running the `service webapp`).
  ```sh
  zimbra@zqa-067:~$ zmlocalconfig -e zimbra_zmprov_default_soap_server=zqa-063.eng.example.com
  ```
- The UI server needs to know where the memcached is running. This is done by setting `zimbraMemcachedClientServerList` to the server where the memcached is running.
  ```sh
  zimbra@zqa-067:~$ zmprov gcf zimbraMemcachedClientServerList
  zimbraMemcachedClientServerList: zqa-063.eng.example.com:11211
  ```
- Need to have at least one mailstore server and one UI server for the proxy to be up and running and split setup to work. `zmproxyctl restart` is required after adding the new UI/mailstore servers to regenerate the correct proxy configurations.
- Administrator console is working, but only through the proxy using port 9071 (default value for zimbraAdminProxyPort) instead of 7071 (default value for zimbraAdminPort) after setting `zimbraReverseProxyAdminEnabled` to TRUE.
- For service (SOAP/REST) to User Interface (JS/css/html) requests from mailstore server in split mode. Set `zimbraWebClientURL` on mailstore server to point to the Proxy. For example `zmprov mcf zimbraWebClientURL https://zqa-063.eng.example.com`
- 92634: MariaDB is running on webapps only nodes.
- 92694: "View mail" not working in the admin console in split server mode.
- 92702 and 92732: In order for features such as change password link, calendar launch in separate window, etc., to work in split server 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
  ```
- 92799: NPE when user tries to access external share invitation link in split server mode.

### Zimlets

- 93587: Rebuild "Undo Send" zimlet.
- 94853: SMIME Attachment gets removed from compose window while selecting 'Don't sign' option and tried to attach any file.

### 8.0.5

83727 Contacts sub-folders and Global Address List do not sync when using an Outlook 2013 Exchange ActiveSync profile.

83801 Numerous known issues when using Outlook 2013 Exchange ActiveSync.

### 8.0.4

80268 Applying a custom theme (skin) to the administration console is not supported.

### 8.0.0

75553 Rolling Upgrade. While in rolling upgrade mode, cross mailbox search will not work for 7.2 or 8.0 versions from the admin console.

Workaround: While in rolling upgrade mode, use the command line search across accounts.

```
/opt/zimbra/bin/zmmboxsearch -m "*" -q "test"
```
### Previous General Known Issues

<table>
<thead>
<tr>
<th>Issue ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>50238</td>
<td>Third-party issue. Windows Mobile 6 removes all occurrences of a recurring meeting when the first instance is deleted.</td>
</tr>
<tr>
<td>50239</td>
<td>Third-party issue. Android SDK 2.2 cannot display inline image content.</td>
</tr>
<tr>
<td>54278</td>
<td>Family Mailbox was not supported in ZCS 7.X.</td>
</tr>
<tr>
<td>47823</td>
<td>A forwarded recurring appointment instance will not update the organizer’s attendee list. Therefore, if the organizer modifies the appointment, the user with the forwarded appointment will not get updated.</td>
</tr>
<tr>
<td>51641</td>
<td>Third-party issue. iPhone calendar might not sync correctly when declining or accepting an appointment in ZWC after the appointment has already been accepted/declined from iPhone.</td>
</tr>
</tbody>
</table>

### 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](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](http://www.zimbra.com/forums).
Revision History

Zimbra Collaboration 8.5.0, GA
• Released August, 2014

Zimbra Collaboration 8.5.0, Revision 1
• Release notes updated September 2014
• Added section Using LMDB as the Supported Back-end for On-disk Database Maps on page 18.
• Added bugs to Enhancement Bugs for 8.5.0, Major Issues Fixed for 8.5.0, and Known Issues for 8.5.0.
• Fixed issues 95230 and 95265 in 8.5.0 GA build 3042. See Major Issues Fixed for 8.5.0. If you are running the 8.5.0_GA_3040 build, the 8.5.0 Patch 1 (8.5.0_P1_3043 build) is required. If you are running the 8.5.0_GA_3042 build, you do not need the patch.

Zimbra Collaboration 8.5.0, Revision 2
• Release notes updated September 2014
• Added bug information for 59788, 83334: If upgrading from a version of ZCO 7.2.5 or 8.0.5 to ZCO 8.5. alias is not included in "To" field now, when "reply all" to a mail.
• Added to Exchange Web Services (EWS) information: Available for an additional charge. Contact Zimbra Sales for more information.

Zimbra Collaboration 8.5.0, Revision 3
• Release notes updated November 2014
• Updated Network Edition and Open Source supported platforms on page 5.
• In the single server, and multi-server upgrade steps, added the last step:
  • It is recommended that you perform a full backup after performing a major upgrade, due to database schema changes.
  • Important: Restoring a full backup to a newer release can fail due to schema differences. It is highly recommended to perform a full backup after every major upgrade to ensure that you have a restore point on the upgraded version.

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
September 2014
Zimbra Collaboration 8.5.0, Revision 3