Zimbra Collaboration 8.6 Network Edition
Release Notes and Upgrade Instructions

These release notes describe new features and enhancements that are available in the Zimbra Collaboration (ZCS) 8.6 Network Edition, and also include upgrade instructions. Review the Known Issues section for a list of outstanding issues in this release before installing or upgrading.

Sections include:

New Features and Enhancements

This section contains information about new features and enhancements in this release.

Accessibility
Note: Accessibility features for 8.6.0 include the login page and the majority of the Mail application. Full accessibility support will be available in 8.7.0.
32283 - AJAX accessibility - section 508.
55337 - All items must have accessibility using keyboard.
96132 - List view header actions should be keyboard accessible.
96137 - Compose view accessibility.
Connector for Outlook
77637 - Hide the "Force GAL update/reset" buttons on the logging utility. • These buttons no longer appear in the ZCO logging control. Use the Sync Global Address List options on the Zimbra ribbon in Outlook.
91214 - Pick up server-side account changes (Personas) in sync cycle. • Changes made to Persona definitions using the Zimbra Web Client are now synchronized to ZCO at the same time as folders are synchronized. (It is no longer necessary to open and OK the ZCO Personas dialog to pick up changes from the Zimbra server.)
95604 - Improved sync-due-to-local-changes trigger algorithm (Sooner push ~5secs, and guaranteed within 60 secs) • A change made in Outlook will generally be synchronized to the Zimbra server within 7 seconds, although this may be deferred to up to 60 seconds if more changes are made in Outlook in the interim.
IMAP/POP Server
96492 - Implemented IMAP SPECIAL-USE attributes for LIST command. *Note: Support for full SPECIAL-USE or CREATE-SPECIAL-USE capabilities is not implemented.*
Licensing
95460 - Extended zmlicense to send version of package being installed.
Localization
90038 - [EU] Added Support for Basque (EU) Language.
92867 - [JA] - Translations for ZCS 8.6.
Mail - Server
73789 - LMTP TLS support
91114 - Add option to make LHLO mandatory in LMTP transactions.
94176 - Add server attribute to toggle Ctrl-Enter shortcut.
96077 - Local lmtp client should communicate over ssl.
Mail - Web Client
24436 - Shared mailbox - save sent messages to the shared sent folder.
65605 - Ctrl-Enter send message shortcut need improvement.
84370 - Identity when sending mail.

Migration
74225 - Schedule migration option shows cryptic message when xml and csv files are not available.
81529 - Please add a ZimbraCOS command line option.
90999 - Log version/build number.
Mobile - Touch Client
81067 - Allow user to read messages using message view v/s conversation view.
Mobile - Zimbra Mobile Sync
95453 - Support for IOS 8.
Other - Web Client
84371 - Better organization of shared folders.
95328 - Replace file icons with new Zimbra branded icons.
Proxy
86759 - Add nginx stub_status module.
Search
91799 - Conversation unread count in SearchResponse.
Tech Docs
85295 - Upgrade from Ubuntu 10 to 12 to 14 documented in wiki page.
89627 - zmauditswatch feature documented in a wiki page.
WebDav
69984 - Support added for caldav calendar-auto-schedule RFC6638.

Fixed Issues

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

Admin
81325 - root user cannot modify zmlocalconfig using -u or -e
86096 - Ability to Create Dynamic Distribution List.
95265 - Webapp services no longer removed when editing server.
95646 - Fixed issue to initiate Remote Wipe of device through AdminUI.
Backup/Restore
96058 - zmplayredo exits appropriately after removal.
Briefcase
82236 - Fixed issue causing Incorrect share url when selecting files in shared briefcases.
96299 - IE8: Ability to upload files to briefcase.
96395 - Fixed script error issue when using "Send Link(s)" menu from briefcase app file.
Calendar - Server
62674 - Can now run search on description for location or resources.
83679 - CalDAV: Ability to invite attendees or edit event on iOS 6.1.4.

94725 - Updated Zimbra to be aware of the latest timezone information, in particular reflecting changes Russia has made to its existing time zones from October 26, 2014.

95440 - iCal/CalDAV synchronization problem fixed. Yosemite treats ActiveSync originated timezone appropriately.

Calendar - Web Client

87613 - Drag and drop of recurring all day event functions correctly.

94818 - Editor displays all attendees present in an invite.

95789 - Chrome: Client no longer hangs if you scroll-up the vertical scrollbar from reminder dialog.

Connector for Outlook

94727 - "Local Rules Warning" dialog for Clear Categories rule not very helpful. The Cancel button on the "Local Rules Warning" dialog has been removed and the dialog is now only shown if the "Clear Categories on Mail" local rule is active.

95112 - Signature image not embedding correctly in e-mail, instead references local path. No change made in ZCO. To address this used the "Send Pictures With Document" registry setting as per http://www.msoutlook.info/question/730.

96160 - ZCO should warn when too large an attachment is added.

A standard Outlook (2010 and 2013) error is now displayed when adding an attachment which causes a message to exceed the configured Zimbra size limit (zimbraMtaMaxMessageSize). Note that since attachments are typically larger once converted to MIME for the server, some messages will avoid the Outlook error but still trigger a Zimbra error when synchronized to the server.

Contacts - Server

91944 - First and Last name is set correctly when adding an emailed contact in Japanese.

Conversion - Server

86304 - Attachments processed correctly by conversion when previewed.

Exchange Web Services - Server

89548 - Read/unread properties retained correctly in native Mail app.

94560 - Opening folders shared by calendar resource works correctly.

94779 - Zimbra EWS no longer causes Mail issues when on OS X Yosemite.

94929 - No issues when using Mail on Mac Account going Offline.

94947 - EWS Sharing - Shared Subcalendar (different mailstore) syncs after MacOutlook restart.

94968 - EWS Sharing: Sharing by Admin MacOutlook user sends share notification to has correct owner.

Install & Upgrade

84399 - Installer checks license before upgrading system.

89303 - Installer reports when localconfig.xml is owned by root and exit.

94070 - ssl_allow_untrusted_certs state sets properly on upgrades.

95000 - /opt/zimbra symlink does not break zmstat-fd stat gathering in 8.0.7 and later.

95420 - Certificates validated prior to allowing upgrade to start.

95461 - RHEL rpm packaging sets /opt/zimbra/conf no longer sets files as executable.
96008 - Security fix. See Security Fixes on page 8.
96164 - SSL v3.0 is disabled in Java Clients.
96171 - Fixed issue when SSLv3 enabled in zimbra-attrs.xml.
96602 - Upgraded to MariaDB 10.0.15.
Localization
95291 - Typo fixed in ZsMsg_fr.properties, allowing shares to access URL and embedding in the email.
Mail MTA/Spam/Virus
95095 - Alias is now supported when enforcing a match between FROM address and sasl username.
95237 - Zimbra Disclaimer/Signature Option per Domain works properly.
95302 - System account for spam/non-spam training disables spam check.
96408 - zmtrainsa no longer fails to update SA's bayes_* DB; direct sa-learn is OK.
96513 - When enforcing a match to from address and sasl username, zimbraAllowFromAddress values are no longer ignored.
Mail - Server
84469 - zmmailbox: no longer duplicates mailbox items after incremental import.
90698 - Issue fixed causing garbage characters displayed for Chinese email.
92561 - Fixed the REST API against CSRF attack.
92783 - Fixed issue causing garbage characters to display in Reply To field for Chinese email.
94771 - Fixed issue causing Chinese message body partially missing for messages sent from Share point service with mixed fonts.
94985 - Fixed issue causing mailbox to lock when running multiple EmptyFolder .
95365 - Invalid login filter no longer blocking internal requests.
95748 - zmmboxmove works as expected when copying blobs to the destination server.
96040 - Support enabling/disabling specific SSL/TLS protocol versions allowed for all mailboxd / Jetty services.
96105 - Security fix. See Security Fixes on page 8.
96425 - Non-ASCII attachment file name displays page correctly when URL-Link is clicked.
Mail - Web Client
85180 - Ability to create new calendar on shared mailbox.
90268 - Fixed issued causing conversations to display as flagged when no individual messages are flagged.
94765 - In-Reply-to contains the parent message-id, no longer causing broken thread on some mail clients.
95022 - Inline images display during reply/forward compose.
96356 - Compose mail works properly in IE-8 if "Contacts" tab is disabled.

Migration
82412 - Migration Tool error fixed for "no such folder id: -1".
86092 - No need to restart each time for multiple run.
92940 - CLI tool no longer puts some mails into the Root folder (id 1).
Mobile - Mobile HTML Client
95692 - Shared calendar with "view" right is visible in mobile html client.
Mobile - Touch Client
81069 - External images display appropriately after sending mail or saving as draft or view mail.
90770 - Touch client allows you to go back after couple of folder create/move navigation.
94933 - Field prompt takes user to compose body.
94998 - Long time to log in issue fixed.
95040 - rfc822 attachment sent if draft message is sent from touch client.
95062 - Touch client loads if Calendar or Contacts feature is disabled in the COS or account.
95181 - Swipe-deleting last item in folder no longer results in JS error.
95550 - Ability to attach files in compose message.
95654 - Japanese translation issue fixed for date representation in the day view calendar.
95924 - Ability to view subfolders of shared folders.
Mobile - Zimbra Mobile Sync
94534 - Sync client no longer fails to sync all emails.
84553 - MobileSync syncs Calendar Event Alert which is set as "At time of event" on iOS.
84705 - iOS7: Reminder of tasks without start or and end date are synced to device..
94939 - User with Calendar feature disabled in COS can no longer sync/create calendar through Activesync.
94984 - Sync client no longer loses track of messages moved via ZWC.
85080 - If subject contains 0x00, the message can be synced.
95356 - Device syncs post upgrade to 8.5.
95649 - Mobile Sync returns error for SendMail request with NO recipient.
95770 - Http/1.1 503 Server Unavailable error issue fiexed for FolderSync request after folder is permanently deleted from server.
95845 - Items created by device are no longer lost in case syncstate migration fails and device re-sync happens, items created after re-sync complete syncs fine.
Offline - Web Client
68053 - SPNEGO: avoid UNAUTHORIZED for non-internal IP addresses issue fixed.
91436 - User can accept appointment which has an attachment in offline mode.
95756 - Offline client sends message after restart .

95758 - Offline: Moved messages to another folder no longer revert back.
Online Help
93050 - Product Help no longer shows blank page with Japanese language preference.
Other - Server
82192 - zimbraPublicSharingEnabled vs zimbraExternalSharingEnabled
82243 - SPNEGO Authentication now working due Zimbra Ews jetty configuration.
94438 - Password change uses the ldapv3 password modify operation.
94894 - Import feature supports *.tar extension.
95523 - Import/export is issue fixed.
95599 - Login page honors zimbraWebClientLogoutURL.
95630 - Context path filter no longer suspend requests when ample threads are available.
95767 - DomainInfoResponse for an unauthenticated session returns multi-valued attributes.
95976 - Security fix. See Security Fixes on page 8.
96041 - Deprecated use of SSLv3 in the product as a whole.
96496 - zimbraPasswordMustChange is working in multi-server w/proxy.
96608 - LDAP cache is used for /zimbra and /zimbraAdmin servlet filters.
Other - Web Client
88104 - Logo dimensions are now correct, and login logos of admin and webclient are the same size.
95064 - Modified Ajax Client to pass CSRF token for REST API.
95448 - Ability to view full window while changing Zoom levels in IE (Webclient).
95799 - Have to log into web client twice issue fixed.
Proxy
84859 - Fixed issue causing Proxy route lookup to fail when a single mailstore is down.
95195 - Proxy routing some EWS requests to wrong host issue fixed.
95315 - zimbraReverseProxySSLToUpstreamEnabled is honored for login & ews urls.
95319 - Domain certificates configuration added to nginx.
95995 - Max wait time increased issue fixed for sites running multiple domains.
Search - Server
95266 - SearchConv no longer fails with offset > 0.
Search - Web Client
96616 - Calendar search no longer results in JS error.
Standard HTML Client
84264 - Closing an appointment no longer results in error.
88451 - Fixed issue causing NPE client error to occur when clicking date from mini calendar.

88590 - Clicking to Previous page/Next page/Day/Month/List no longer opens new appointment page everytime.
89318 - org.apache.jsp.tag.web.imginfo_tag: high CPU in java.util.HashMap.get issue fixed.
94570 - HTML Client: Fixed issue when contacts added to group from GAL shows account id of those contacts and hence gets garbled.
95065 - Modified Standard Html Client to pass CSRF token for REST API.
95549 - "Must be the appointment organizer" warning issue fixed when grantee tries to send appointment from shared calendar.
96316 - Using Content-Type: text/html when composing message as plain text.
Tasks - Web Client
95025 - Intermittently task app broken issue fixed.
Tech Docs
Bug 95657 - Updated migration documentation.
Zimlets
85399 - WebEx zimlet does not fail for account.
87168 - Dropbox zimlet console errors fixed.
89142 - S/MIME: Fixed issue causing Insecure temp dir handling in applet on multi user Linux.
95989 - LinkedIn Image Zimlet is removed from ZCS during upgrade to 8.6.0. Zimlet has been moved to the Zimbra Gallery.

Security Fixes

Zimbra Collaboration security fixes include the following.

Note: *For more information, see the Zimbra Security Response Policy and Zimbra Vulnerability Rating Classification sections below.*

- Bug 96105
  - CVE ID: CVE-2014-8563
  - CVSS base score: 5.8 "Major".
  - Versions affected: 8.0.0-8.0.8, 8.5.0
  - **Important**: This issue is an important vulnerability only to those Zimbra installations that have not deployed the ZCS nginx proxy in front of mailboxd for POP/IMAP. nginx is not vulnerable to this issue - only jetty (mailboxd) received this fix.

- Bug 96008: Upgraded to OpenSSL 1.0.1j
  - SRTP Memory Leak
    - CVE ID: CVE-2014-3513
    - CVSS base score: 5.0
    - Versions affected: 8.0.0-8.0.8, 8.5.0
  - Session Ticket Memory Leak
    - CVE ID: CVE-2014-3567
    - CVSS base score: 4.3
    - Versions affected: All supported versions.
- Bug 95976: Poodle SSLv3 Vulnerability
  - CVE ID: CVE-2014-3566
    - For more information, see https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
  - CVSS base score: 4.3
  - Versions affected: All supported versions prior to 8.6.
    - For more information, see https://wiki.zimbra.com/wiki/How_to_disable_SSLv3

Zimbra Security Response Policy

For more information about the Zimbra Security Response Policy, see https://community.zimbra.com/support/w/security_prgm/41842.zimbra-security-response-policy.

Zimbra Vulnerability Rating Classification

For more information about the Zimbra Vulnerability Rating Classification, see https://community.zimbra.com/support/w/security_prgm/41843.zimbra-vulnerability-rating-classification.

Supported Systems

Platform: 64-bit is supported; 32-bit is EOL

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 for further information.
- SUSE Linux Enterprise Server (SLES) 11, SP3 or later - Deprecated ***Important! Zimbra Collaboration 8.6 is the last supported release of SLES 11.***

Operating Systems and Browsers supported with the Administration Console

The following operating system/browser combinations are supported. Other configurations might work.

- Windows XP with required updates, Vista, Windows 7, or Windows 8 with one of the following:
  - Internet Explorer 8.0 and higher
    - IE8.x for XP
    - IE9.x and higher for Vista/Windows 7
    - IE10 and higher for Windows 8
  - The latest stable release of:
    - Firefox
    - Safari
    - Google Chrome
- Mac OS X 10.5, 10.6, 10.7, or 10.8 with one of the following:
  - The latest stable release of:
    - Firefox
    - Safari
    - Google Chrome

- Linux (Red Hat, Ubuntu, Fedora, or SUSE) with one of the following:
  - The latest stable release of:
    - Firefox
    - Google Chrome

Zimbra Web Client (Advanced)

The following operating system/browser combinations for the advanced Zimbra Web Client are supported. Other configurations might work.

- Windows XP with required updates, Vista, Windows 7, or Windows 8 with one of the following:
  - Internet Explorer 8.0 and higher
    - IE8.x for XP
    - IE9.x and higher for Vista/Windows 7
    - IE10 and higher for Windows 8
  - The latest stable release of:
    - Firefox
    - Safari
    - Google Chrome
- Mac OS X 10.5, 10.6, 10.7, or 10.8 with one of the following:
  - The latest stable release of:
    - Firefox
    - Safari
    - Google Chrome
- Linux (Red Hat, Ubuntu, Fedora, or SUSE) with one of the following:
  - The latest stable release of:
    - Firefox
    - Google Chrome

Zimbra Web Client (Standard)

The following operating system/browser combinations for the standard Zimbra Web Client are supported. Other configurations might work.

- Windows XP with required updates, Vista, Windows 7, or Windows 8 with one of the following:
  - Internet Explorer 8.0 and higher
    - IE8.x for XP
    - IE9.x and higher for Vista/Windows 7

    - IE10 and higher for Windows 8
  - The latest stable release of:
    - Firefox
    - Safari
    - Google Chrome
- Mac OS X 10.5, 10.6, 10.7, or 10.8 with one of the following:
  - The latest stable release of:
    - Firefox
    - Safari
    - Google Chrome
- Linux (Red Hat, Ubuntu, Fedora, or SUSE) with one of the following browsers:
  - The latest stable release of:
    - Firefox
    - Google Chrome

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. Be sure to read the release note information before upgrading.

- Zimbra Database Integrity Check on page 13
- Preparing Your OS on page 13
- Verify Certificates Expiration Date on page 14
- License Activation on page 14
- Upgrading LDAP Replica Servers or Multi-Master Server from ZCS 8.0.0, 8.0.1, 8.0.2 to ZCS 8.0.4 and later on page 15

- Disable SSLv3 Support on page 16
- Update Default Proxy SSL Ciphers Attribute on page 16
- Customizing ZCO Installations on page 17

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 the 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
```

Note: *See the Zimbra Wiki for more information about support for upgrading Ubuntu.*

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. ***Important! Zimbra Collaboration 8.6 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

> ***Important:*** *For upgrade installations:*
>
> - 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 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 **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 from 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. (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 19.

Disable SSLv3 Support

If upgrading to ZSC 8.6.0, you need to completely disable SSLv3 support after the upgrade. Disabling SSLv3 is recommended as a result of the SSLv3 vulnerability described in Security Fixes on page 8.

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 8.6.0 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 https://wiki.zimbra.com/wiki/How_to_disable_SSLv3 to disable SSLv3 after upgrading to ZCS 8.6.0.

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>**).

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.

zimbraReverseProxySSLCiphers

zimbraReverseProxySSLProtocols

zimbraSSLExcludeCipherSuites

zimbraMailboxdSSLProtocols

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.

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

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] i**s 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 each server.

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. 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.

- Review Disable SSLv3 Support on page 16
- Review Update Default Proxy SSL Ciphers Attribute on page 16
- 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 14.
- If using zmlogger prior to ZCS 8.0.7, see Cleanup Procedure for Logger Host on page 23.
- 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
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
```

Updating Your MariaDB Table

If you upgrading from 6.X to ZCS 8.5.x and later, 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, 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.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. (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. (Bug 62523)

Known Issues

Zimbra engineering has identified known issues, and 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 https://bugzilla.zimbra.com.

Issue #	Summary
8.6.0	• 95933: Mail Server - item_id_checkpoint does not update, causes account to be unusable. • 96092: Install & Upgrade - About link from ZWC not updated after patch install. • 96147: Calendar Web Client - Remove unnecessary timezones from ZWC. • 96166: Mobile Zimbra Mobile Sync - Imap delete leaves orphan item on device. • 96723: Mobile Zimbra Mobile Sync - Creating and editing an invite results in duplicate corrupt appointment. • 96727: WebDav - Sending invite to external user sends two invitations. • 96728: EWS Server - Responding to exception in Mac Outlook fails. • 96766: Mobile Zimbra Mobile Sync - ActiveSync: Mail not getting marked read at web client when already read from device. • 96815: Mail Web Client - Copy/Paste of Excel/Word data results in image inserted into MIME.
CalDav	• 96641 - Delete series does not delete "all day instances" of recurring appointment in caldav • 96644 - CalDAV:Stale event never synchronizes - Wrong HTTP Status code 409 Conflict instead of 412 Precondition failed • 96726 - Delete event in recurring appointment from android SolCalendar app does not send notification to organizer. Replies are not sent from SolCalendar to the ORGANIZER when instances of a series are deleted by an ATTENDEE. • 96727 - Sending invite to external user sends 2 invitations • 96729 - Multiple notifications sent to organizer on responding from Yosemite calendar • 96799 - Multiple meeting request are sent when scheduling Full Day meeting through CalDav
8.5.x **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.
- 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

- 91102: Problems in preview generation for empty csv file.

Exchange Web Services - Calendar

- 94923: SOBO meeting: Attendee participation status is not updated in sharee's MacOutlook.

EWS - Misc

- 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

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.

Exchange Web Services - Server

- 95072: Native Mac Mail trash folder display issue

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.

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.

Mail - Web Client

- 86326: New Message Button Fails.
- 92100: Intermittently message content shows partially blank for long message.
- 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.
- 90018: Sent message after editing a reply draft becomes a separate conversation.

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**).

  ```
  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.

  ```
  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.

Zimlets

- 94853: S/MIME 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"`
75523	Rolling Upgrade: Address Book. While in rolling upgrade mode, contact Group members are not displayed when users on a 7.2 mailbox server share their address book with users on an 8.0.x mailbox server.

76665	Large attachments (greater than 1MB) might result in errors due to Java memory limitations when using S/MIME signed or encrypted messages.
77417	ZCO: When sharing folders with an external account, the email that is sent shows the user name and password but does not give the URL on how to access the share.
78566	When folders are assigned in ZCO, when viewing the folder from the ZWC, the folder is not displayed in that color.
Previous General Known Issues	
50238	Third-party issue. Windows Mobile 6 removes all occurrences of a recurring meeting when the first instance is deleted.
50239	Third-party issue. Android SDK 2.2 cannot display inline image content.
54278	Family Mailbox was not supported in ZCS 7.X.
47823	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.
51641	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.

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. See http://www.zimbra.com/support and https://wiki.zimbra.com/wiki.

Bug Reporting

If you encounter problems with this software, go to https://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 https://community.zimbra.com/collaboration.

Revision History

Zimbra Collaboration 8.6.0 GA

- Released December, 2014

Zimbra, Inc.
3000 Internet Blvd., Suite 200
Frisco, Texas 75034

www.zimbra.com

December 2014

Zimbra Collaboration 8.6.0