These release notes describe new features and enhancements that are available in the Zimbra Collaboration (ZCS) 8.6 Open Source 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** on page 2
- **Fixed Issues** on page 3
- **Security Fixes** on page 7
- **Supported Systems** on page 8
- **New Installation** on page 10
- **Upgrade Process** on page 11
- **Upgrade Instructions** on page 15
- **After the Upgrade is Complete** on page 19
- **Status of Your Customization after Upgrade** on page 23
- **Known Issues** on page 24
- **Product Documentation** on page 27
- **Bug Reporting** on page 27
- **Revision History** on page 27
New Features and Enhancements

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

<table>
<thead>
<tr>
<th>Accessibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>32283 - AJAX accessibility - section 508.</td>
</tr>
<tr>
<td>55337 - All items must have accessibility using keyboard.</td>
</tr>
<tr>
<td>96132 - List view header actions should be keyboard accessible.</td>
</tr>
<tr>
<td>96137 - Compose view accessibility.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IMAP/POP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>96492 - Implemented IMAP SPECIAL-USE attributes for LIST command. <strong>Note:</strong> Support for full SPECIAL-USE or CREATE-SPECIAL-USE capabilities is not implemented.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Localization</th>
</tr>
</thead>
<tbody>
<tr>
<td>90038 - [EU] Added Support for Basque (EU) Language.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mail - Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>73789 - LMTP TLS support</td>
</tr>
<tr>
<td>91114 - Add option to make LHLO mandatory in LMTP transactions.</td>
</tr>
<tr>
<td>94176 - Add server attribute to toggle Ctrl-Enter shortcut.</td>
</tr>
<tr>
<td>96077 - Local lmtp client should communicate over ssl.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mail - Web Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>24436 - Shared mailbox - save sent messages to the shared sent folder.</td>
</tr>
<tr>
<td>65605 - Ctrl-Enter send message shortcut need improvement.</td>
</tr>
<tr>
<td>84370 - Identity when sending mail.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Migration</th>
</tr>
</thead>
<tbody>
<tr>
<td>74225 - Schedule migration option shows cryptic message when xml and csv files are not available.</td>
</tr>
<tr>
<td>81529 - Please add a ZimbraCOS command line option.</td>
</tr>
<tr>
<td>90999 - Log version/build number.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other - Web Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>84371 - Better organization of shared folders.</td>
</tr>
<tr>
<td>95328 - Replace file icons with new Zimbra branded icons.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>86759 - Add nginx stub_status module.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Search</th>
</tr>
</thead>
<tbody>
<tr>
<td>91799 - Conversation unread count in SearchResponse.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tech Docs</th>
</tr>
</thead>
<tbody>
<tr>
<td>85295 - Upgrade from Ubuntu 10 to 12 to 14 documented in wiki page.</td>
</tr>
</tbody>
</table>
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.

**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.

**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.
<table>
<thead>
<tr>
<th>Issue Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>95000</td>
<td>/opt/zimbra symlink does not break zmstat-fd stat gathering in 8.0.7 and later.</td>
</tr>
<tr>
<td>95420</td>
<td>Certificates validated prior to allowing upgrade to start.</td>
</tr>
<tr>
<td>95461</td>
<td>RHEL rpm packaging sets /opt/zimbra/conf no longer sets files as executable.</td>
</tr>
<tr>
<td>96164</td>
<td>SSL v3.0 is disabled in Java Clients.</td>
</tr>
<tr>
<td>96171</td>
<td>Fixed issue when SSLv3 enabled in zimbra-attrs.xml.</td>
</tr>
<tr>
<td>96602</td>
<td>Upgraded to MariaDB 10.0.15.</td>
</tr>
<tr>
<td><strong>Localization</strong></td>
<td></td>
</tr>
<tr>
<td>95291</td>
<td>Typo fixed in ZsMsg_fr.properties, allowing shares to access URL and embedding in the email.</td>
</tr>
<tr>
<td><strong>Mail MTA/Spam/Virus</strong></td>
<td></td>
</tr>
<tr>
<td>95095</td>
<td>Alias is now supported when enforcing a match between FROM address and sasl username.</td>
</tr>
<tr>
<td>95237</td>
<td>Zimbra Disclaimer/Signature Option per Domain works properly.</td>
</tr>
<tr>
<td>95302</td>
<td>System account for spam/non-spam training disables spam check.</td>
</tr>
<tr>
<td>96408</td>
<td>zmtrainlsa no longer fails to update SA's bayes_* DB; direct sa-learn is OK.</td>
</tr>
<tr>
<td>96513</td>
<td>When enforcing a match to from address and sasl username, zimbraAllowFromAddress values are no longer ignored.</td>
</tr>
<tr>
<td><strong>Mail - Server</strong></td>
<td></td>
</tr>
<tr>
<td>84469</td>
<td>zmmailbox: no longer duplicates mailbox items after incremental import.</td>
</tr>
<tr>
<td>90698</td>
<td>Issue fixed causing garbage characters displayed for Chinese email.</td>
</tr>
<tr>
<td>92561</td>
<td>Fixed the REST API against CSRF attack.</td>
</tr>
<tr>
<td>92783</td>
<td>Fixed issue causing garbage characters to display in Reply To field for Chinese email.</td>
</tr>
<tr>
<td>94771</td>
<td>Fixed issue causing Chinese message body partially missing for messages sent from Share point service with mixed fonts.</td>
</tr>
<tr>
<td>94985</td>
<td>Fixed issue causing mailbox to lock when running multiple EmptyFolder.</td>
</tr>
<tr>
<td>95365</td>
<td>Invalid login filter no longer blocking internal requests.</td>
</tr>
<tr>
<td>95748</td>
<td>zmmboxmove works as expected when copying blobs to the destination server.</td>
</tr>
<tr>
<td>96040</td>
<td>Support enabling/disabling specific SSL/TLS protocol versions allowed for all mailboxd / Jetty services.</td>
</tr>
<tr>
<td>96425</td>
<td>Non-ASCII attachment file name displays page correctly when URL-Link is clicked.</td>
</tr>
<tr>
<td><strong>Mail - Web Client</strong></td>
<td></td>
</tr>
<tr>
<td>85180</td>
<td>Ability to create new calendar on shared mailbox.</td>
</tr>
<tr>
<td>90268</td>
<td>Fixed issued causing conversations to display as flagged when no individual messages are flagged.</td>
</tr>
<tr>
<td>Issue Number</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>94765</td>
<td>In-Reply-to contains the parent message-id, no longer causing broken thread on some mail clients.</td>
</tr>
<tr>
<td>95022</td>
<td>Inline images display during reply/forward compose.</td>
</tr>
<tr>
<td>96356</td>
<td>Compose mail works properly in IE-8 if &quot;Contacts&quot; tab is disabled.</td>
</tr>
<tr>
<td><strong>Migration</strong></td>
<td></td>
</tr>
<tr>
<td>82412</td>
<td>Migration Tool error fixed for &quot;no such folder id: -1&quot;.</td>
</tr>
<tr>
<td>86092</td>
<td>No need to restart each time for multiple run.</td>
</tr>
<tr>
<td>92940</td>
<td>CLI tool no longer puts some mails into the Root folder (id 1).</td>
</tr>
<tr>
<td><strong>Mobile - Mobile HTML Client</strong></td>
<td></td>
</tr>
<tr>
<td>95692</td>
<td>Shared calendar with &quot;view&quot; right is visible in mobile html client.</td>
</tr>
<tr>
<td><strong>Offline - Web Client</strong></td>
<td></td>
</tr>
<tr>
<td>68053</td>
<td>SPNEGO: avoid UNAUTHORIZED for non-internal IP addresses issue fixed.</td>
</tr>
<tr>
<td>91436</td>
<td>User can accept appointment which has an attachment in offline mode.</td>
</tr>
<tr>
<td>95756</td>
<td>Offline client sends message after restart.</td>
</tr>
<tr>
<td>95758</td>
<td>Offline: Moved messages to another folder no longer revert back.</td>
</tr>
<tr>
<td><strong>Online Help</strong></td>
<td></td>
</tr>
<tr>
<td>93050</td>
<td>Product Help no longer shows blank page with Japanese language preference.</td>
</tr>
<tr>
<td><strong>Other - Server</strong></td>
<td></td>
</tr>
<tr>
<td>82192</td>
<td>zimbraPublicSharingEnabled vs zimbraExternalSharingEnabled</td>
</tr>
<tr>
<td>82243</td>
<td>SPNEGO Authentication now working due Zimbra Ews jetty configuration.</td>
</tr>
<tr>
<td>94438</td>
<td>Password change uses the ldapv3 password modify operation.</td>
</tr>
<tr>
<td>94894</td>
<td>Import feature supports *.tar extension.</td>
</tr>
<tr>
<td>95523</td>
<td>Import/export is issue fixed.</td>
</tr>
<tr>
<td>95599</td>
<td>Login page honors zimbraWebClientLogoutURL.</td>
</tr>
<tr>
<td>95630</td>
<td>Context path filter no longer suspend requests when ample threads are available.</td>
</tr>
<tr>
<td>95767</td>
<td>DomainInfoResponse for an unauthenticated session returns multi-valued attributes.</td>
</tr>
<tr>
<td>96041</td>
<td>Deprecated use of SSLv3 in the product as a whole.</td>
</tr>
<tr>
<td>96496</td>
<td>zimbraPasswordMustChange is working in multi-server w/proxy.</td>
</tr>
<tr>
<td>96608</td>
<td>LDAP cache is used for /zimbra and /zimbraAdmin servlet filters.</td>
</tr>
<tr>
<td><strong>Other - Web Client</strong></td>
<td></td>
</tr>
<tr>
<td>88104</td>
<td>Logo dimensions are now correct, and login logos of admin and webclient are the same size.</td>
</tr>
<tr>
<td>95064</td>
<td>Modified Ajax Client to pass CSRF token for REST API.</td>
</tr>
<tr>
<td>95448</td>
<td>Ability to view full window while changing Zoom levels in IE (Webclient).</td>
</tr>
<tr>
<td>95799</td>
<td>Have to log into web client twice issue fixed.</td>
</tr>
<tr>
<td><strong>Proxy</strong></td>
<td></td>
</tr>
<tr>
<td>Bug Number</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>84859</td>
<td>Fixed issue causing Proxy route lookup to fail when a single mailstore is down.</td>
</tr>
<tr>
<td>95195</td>
<td>Proxy routing some EWS requests to wrong host issue fixed.</td>
</tr>
<tr>
<td>95315</td>
<td>zimbraReverseProxySSLToUpstreamEnabled is honored for login &amp; ews urls.</td>
</tr>
<tr>
<td>95319</td>
<td>Domain certificates configuration added to nginx.</td>
</tr>
<tr>
<td>95995</td>
<td>Max wait time increased issue fixed for sites running multiple domains.</td>
</tr>
<tr>
<td>95266</td>
<td>SearchConv no longer fails with offset &gt; 0.</td>
</tr>
<tr>
<td>96616</td>
<td>Calendar search no longer results in JS error.</td>
</tr>
<tr>
<td>84264</td>
<td>Closing an appointment no longer results in error.</td>
</tr>
<tr>
<td>88451</td>
<td>Fixed issue causing NPE client error to occur when clicking date from mini calendar.</td>
</tr>
<tr>
<td>88590</td>
<td>Clicking to Previous page/Next page/Day/Month/List no longer opens new appointment page everytime.</td>
</tr>
<tr>
<td>94570</td>
<td>HTML Client: Fixed issue when contacts added to group from GAL shows account id of those contacts and hence gets garbled.</td>
</tr>
<tr>
<td>95065</td>
<td>Modified Standard Html Client to pass CSRF token for REST API.</td>
</tr>
<tr>
<td>95549</td>
<td>&quot;Must be the appointment organizer&quot; warning issue fixed when grantee tries to send appointment from shared calendar.</td>
</tr>
<tr>
<td>96316</td>
<td>Using Content-Type: text/html when composing message as plain text.</td>
</tr>
<tr>
<td>95025</td>
<td>Intermittently task app broken issue fixed.</td>
</tr>
<tr>
<td>Bug 95657</td>
<td>Updated migration documentation.</td>
</tr>
<tr>
<td>85399</td>
<td>WebEx zimlet does not fail for account.</td>
</tr>
<tr>
<td>87168</td>
<td>Dropbox zimlet console errors fixed.</td>
</tr>
<tr>
<td>95989</td>
<td>LinkedIn Image Zimlet is removed from ZCS during upgrade to 8.6.0. Zimlet has been moved to the Zimbra Gallery.</td>
</tr>
</tbody>
</table>
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
  - 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](https://wiki.zimbra.com/wiki/How_to_disable_SSLv3)

**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 11
- **Preparing Your OS** on page 11
- **Verify Certificates Expiration Date** 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 and later** on page 13
- **Disable SSLv3 Support** on page 14
- **Update Default Proxy SSL Ciphers Attribute** on page 14

Zimbra Database Integrity Check

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

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

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

Preparing Your OS

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

- Ubuntu 14.04 LTS Server Edition (64-bit)
- Ubuntu 12.04.4 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:

```bash
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`
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 16.
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 7.

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.
Upgrade Instructions

Download the Software

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

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

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

*Example command usage:* `screen ./install.sh`

**Note:** You cannot revert to a previous Zimbra Collaboration release after you upgrade.

Single-Server Upgrade Steps

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

**Process**

1. Log in as *root* to the Zimbra server and *cd* to the directory where the ZCS Open Source Edition archive tar file is saved (cd /var/tmp). Type the following commands:
   
   `tar xzvf zcs.tgz`, to unpack the file
   
   `cd [zcsversionfullname]`, to change to the correct directory
   
   `./install.sh`, to begin the upgrade installation

   The upgrade script begins by checking for an existing installation.

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

3. The installer checks for prerequisites. If any are missing, the upgrade stops. Next, *Do you want to verify message store database integrity (Y)* is displayed. The default is Yes. This step runs zmdbintegrityreport to verify that the MariaDB database is not corrupt before upgrading to the latest ZCS.
The zmdbintegrityreport can take minutes to an hour to run, depending on your system size and disk bandwidth. It is preferable that you run zmdbintegrityreport at the time of the ZCS upgrade. If you choose to skip this now, the zmdbintegrityreport will run during a regular scheduled interval after the upgrade is finished.

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

5. The packages are listed. The installer also lists packages that are not installed. If you want to install the packages at this time, type **Y**; otherwise press **Enter**. The upgrade checks that there is enough space to perform the upgrade. If there is not enough space, the upgrade stops.

6. When **The system will be modified. Continue? [N]** is displayed, type **Y** and press **Enter**. The Zimbra server is stopped, and the older packages are removed. The upgrade process verifies which version of ZCS is being run and proceeds to upgrade the services, restores the existing configuration files, and restarts the server. If you have a configuration with a large number of accounts created, this can take a while.

7. If you have not set the time zone, you will be asked to set it. This sets the time zone in the default COS. The time zone that should be entered is the time zone that the majority of users in the COS will be located in.

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

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.

**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.

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

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

   When the MariaDB software versions are changed during upgrades, the underlying database tables need to be upgraded. The zmdbintegrityreport does this automatically during it's first run and will report the changes. These are normal and should not cause alarm when upgrading.

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

   The upgrade packages are unpacked.

6. The packages you want to install on the server should be marked **Y**. All other packages should be marked **N**.

   The upgrade checks that there is enough space to perform the upgrade. If there is not enough space, the upgrade stops.
7. When **The system will be modified. Continue?** is displayed, type **Y** and press **Enter**. The server is stopped and the older packages are removed. The upgrade process verifies which version of ZCS is being run and proceeds to upgrade the services, restores the existing configuration files, and restarts the system. If you have a configuration with a large number of accounts created, this can take a while.

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

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 14
- Review Update Default Proxy SSL Ciphers Attribute on page 14
- 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 12.
- 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`
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 Open Source Edition as a new installation, when you run the Zimbra Collaboration install script, enter **N** (no) when asked **Do you wish to upgrade?**

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

Upgrading to the newest release does not delete your accounts or change your configuration.

Configuration settings stored in LDAP and localconfig are preserved during upgrades. Any files installed by Zimbra Collaboration might be deprecated and/or overwritten during upgrades, removing any customizations. This includes customized themes, logo branding changes, and crontab changes.

Only the core Zimlets are enabled after the upgrade. Zimlets that you customized and/or deployed are preserved during the upgrade but will be disabled. As upgrading of customized Zimlets cannot be tested before the release, Zimbra recommends that you verify that your customized Zimlets work correctly before re-enabling them for your end-users after the upgrade.

**Note:** When upgrading to Zimbra Collaboration 8.5.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.

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.

<table>
<thead>
<tr>
<th>Issue #</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.6.0</td>
<td></td>
</tr>
<tr>
<td>95933</td>
<td>Mail Server - item_id_checkpoint does not update, causes account to be unusable.</td>
</tr>
<tr>
<td>96092</td>
<td>Install &amp; Upgrade - About link from ZWC not updated after patch install.</td>
</tr>
<tr>
<td>96147</td>
<td>Calendar Web Client - Remove unnecessary timezones from ZWC.</td>
</tr>
<tr>
<td>96166</td>
<td>Mobile Zimbra Mobile Sync - Imap delete leaves orphan item on device.</td>
</tr>
<tr>
<td>9623</td>
<td>Mobile Zimbra Mobile Sync - Creating and editing an invite results in duplicate corrupt appointment.</td>
</tr>
<tr>
<td>96727</td>
<td>WebDav - Sending invite to external user sends two invitations.</td>
</tr>
<tr>
<td>96728</td>
<td>EWS Server - Responding to exception in Mac Outlook fails.</td>
</tr>
<tr>
<td>96766</td>
<td>Mobile Zimbra Mobile Sync - ActiveSync: Mail not getting marked read at web client when already read from device.</td>
</tr>
<tr>
<td>96815</td>
<td>Mail Web Client - Copy/Paste of Excel/Word data results in image inserted into MIME.</td>
</tr>
<tr>
<td>CalDav</td>
<td></td>
</tr>
<tr>
<td>96641</td>
<td>Delete series does not delete &quot;all day instances&quot; of recurring appointment in caldav</td>
</tr>
<tr>
<td>96644</td>
<td>CalDAV:Stale event never synchronizes - Wrong HTTP Status code 409 Conflict instead of 412 Precondition failed</td>
</tr>
<tr>
<td>96726</td>
<td>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.</td>
</tr>
<tr>
<td>96727</td>
<td>Sending invite to external user sends 2 invitations</td>
</tr>
<tr>
<td>96729</td>
<td>Multiple notifications sent to organizer on responding from Yosemite calendar</td>
</tr>
<tr>
<td>96799</td>
<td>Multiple meeting request are sent when scheduling Full Day meeting through CalDav</td>
</tr>
</tbody>
</table>

8.5.x

Administrator Console

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

Conversion Server

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`).
  ```bash
  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.
    ```bash
    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.

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.

8.0.0

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.

Previous General Known Issues

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

<table>
<thead>
<tr>
<th>Zimbra Collaboration 8.6.0 GA</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Released December, 2014</td>
</tr>
</tbody>
</table>

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
December 2014
Zimbra Collaboration 8.6.0