



Zimbra Collaboration Administrator Guide

v8.8.15, June 2019

revised 2020-01-24

Table of Contents

License.....	2
Introduction.....	3
Audience.....	3
Third-Party Components	3
Support and Contact Information	3
Product Life Cycle.....	4
Component Deprecation Statements.....	4
Product Overview.....	5
Architectural Overview	5
Core Email, Calendar and Collaboration Functionality	5
Zimbra Components	6
Zimbra Application Packages	7
Mail Flow — Multi-Server Configuration	8
Zimbra System Directory Tree	10
Zimbra Web Clients	11
Web Services and Desktop Clients	11
Offline Mode	12
Security Measures	12
Licensing.....	15
License Types	15
License Requirements.....	15
License Usage by Account Type	16
License Activation	16
Obtain a License.....	17
Managing Licenses	17
Updating Your License	19
Zimbra Mailbox Server	20
Mailbox Server	20
Web Application Server	21
Web Application Server Split	22
Backing Up the Mailbox Server	22
Mailbox Server Logs	23
IMAP	24
Common IMAP Configuration settings	24
Zimbra LDAP Service	26
LDAP Traffic Flow	26
LDAP Directory Hierarchy	26
Zimbra Collaboration LDAP Schema	27

Account Authentication	30
Global Address List	33
Flushing LDAP Cache	34
Zimbra Mail Transfer Agent	37
Incoming Mail Routing Overview	37
Zimbra MTA Deployment	37
SMTP Authentication	38
Anti-Virus and Anti-Spam Protection	39
Receiving and Sending Mail	54
Zimbra Proxy Server	56
Benefits of Using Zimbra Proxy	56
Zimbra Proxy Components	56
Proxy Architecture and Flow	57
Changing the Zimbra Proxy Configuration	57
Zimbra Proxy	58
Configuring Zimbra HTTP Proxy	61
Configuring Zimbra Proxy for Kerberos Authentication	65
Zimbra Administration Console	67
Administrator Accounts	67
Logging into the Administration Console	67
Managing Tasks	69
Navigating the User Interface	70
Message of the Day	90
Functional Reference	91
Zimbra PST Migration Wizard	96
Migration Wizard GUI	96
Migration Wizard CLI	99
Managing Configuration	100
Global Configuration	100
General Information Configuration	101
Attachments Configuration	102
MTA Configuration	104
Working With Domains	107
Managing Server Settings	118
Using DKIM to Authenticate Email Message	123
Anti-spam Settings	126
Anti-virus Settings	131
Zimbra Free/Busy Calendar Scheduling	132
Setting Up S/MIME	134
Storage Management	137
Email Retention Management	139

Customized Admin Extensions	143
Ephemeral Data	145
Configuring a Running Zimbra Collaboration to Use SSDB	145
Migration Procedure	146
Migration Details	146
SSDB Installation and Configuration	149
Installation	149
Overview of Configuration Options	149
Master-Slave Replication	152
Master-Master Replication	158
Multi-Master Scaling / Replication	162
LDAP Attributes	162
Scaling SSDB for Production Load with Zimbra Collaboration	162
Conclusion	163
Class of Service and Accounts	164
Managing Features and Settings with a COS	164
Selecting Features and Preferences	165
Using Server Pools	165
Setting Account Quota	166
Managing Passwords	167
Managing Login Policies	169
Managing Session Timeout Policies	170
Managing Default External COS	171
Customizing Accounts	172
Messaging and Collaboration Applications	172
Address Book Features	178
Calendar Features	178
Zimbra Web Client User Interface Themes	182
Two Factor Authentication	183
Other Configuration Settings for Accounts	185
Hierarchical Address Book (HAB) in Zimbra	188
What is a HAB?	188
Using Hierarchical Address Book	188
Seniority Index	189
Configuring hierarchical address books	189
Manage Organisational Units (OUs)	193
Provisioning User Accounts	195
Creating a Single User Accounts	195
Migrating Accounts and Importing Account Email	195
Auto Provisioning New Accounts from External LDAP	203
Managing Resources	212

Managing User Accounts	215
Status of User Accounts	215
Deleting an Account	215
Viewing an Accounts Mailbox	216
Using an Email Alias	216
Working with Distribution Lists	216
Using Dynamic Distribution Lists	222
Moving a Mailbox	226
Delegated Administration (*)	228
Target Types for Granting Administrative Rights	228
Rights	229
Implementing Delegated Administration	232
Revoking Rights	233
View Rights Granted to Administrators	233
Predefined Delegated Administrator Role	234
Creating Delegated Administrator Roles	234
Monitoring ZCS Servers	239
Zimbra Logger	239
Configuring Disk Space Notifications	241
Monitoring Servers	242
Configuring Denial of Service Filter Parameters	243
Working with Mail Queues	245
Monitoring Mailbox Quotas	247
Viewing MobileSync Statistics	248
Monitoring Authentication Failures	248
Viewing Log Files	248
Reading a Message Header	259
Fixing Corrupted Mailbox Index	260
SNMP Monitoring and Configuration	260
Checking MariaDB	261
Checking for Zimbra Collaboration Software Updates	261
Updating Zimbra Connector for Microsoft Outlook	262
Notifications and Alerts Sent by Zimbra Collaboration	262
Backup and Restore (*)	266
Backing Up the Mailbox Server	266
Backup Methods	266
Directory Structure for Backup Files	268
Backup and Restore Using the Administration Console	269
Backup and Restore Using the Command Line Interface	270
Backing up using the Standard Method	271
Aborting a Full Backup in Progress	276

Backup using the Auto-Grouped Method	276
Backup Options	278
Managing Disk Space for Backups	279
Restoring Data	279
General Steps for Disaster Recovery	286
Using snapshots to Backup and Restore	291
Notes on Ephemeral Data	292
Archiving and Discovery	295
How Archiving Works	295
How Discovery Works	296
Installing the Archiving Package	297
Manage Archiving From the Administration Console	298
Archive Mailboxes	300
Searching Across Mailboxes	301
Legal Requests for Information	303
Legal Intercept Settings	303
Creating Mailbox Snapshots for Legal Discovery	305
Color and Logo Management	306
Changing Theme Color and Logos on the Zimbra Web Client	306
Zimlets	312
Managing Zimlets from the Administration Console	312
Managing Zimlets from the Command Line Interface	314
Using the Voice Service	318
Order of Configuration	318
Voice Service Requirements	319
Using a Third-Party Unified Communications Server	319
Cisco URLs	319
Mitel URLs	320
Creating the Voice/Chat Service	320
Configure Presence (Cisco only)	320
Enabling the Voice/Chat Service	321
Enable Voice/Chat Service on a Domain	321
Enable Voice/Chat Service on a COS	321
Enable Voice/Chat Service on a User Account	321
Enabling the Voice/Chat Zimlets	322
Backup Next Generation NG	323
Real-Time Scan	323
Blobless Backup Mode	324
SmartScan	325
Purge	327
External Backup	328

Restore on New Account	330
Undelete Restore	332
External Restore.....	333
Restore Deleted Account	336
Item Restore	336
Raw Restore.....	339
Disaster Recovery	341
Unrestorable Items	345
doCoherencyCheck	350
Taking Additional and Offsite Backups of Backup NG's Datastore	352
Multistore Information.....	355
Operation Queue and Queue Management.....	357
COS-level Backup Management	359
Incremental Migration with Backup NG	360
Mobile NG.....	367
Enable Mobile NG Synchronization for a COS	367
How to Enable Mobile NG for all Users in a Class Of Service	367
From the Administration Console	367
From the Zimbra CLI.....	367
How to Disable Mobile NG for all Users in a Class Of Service.....	367
From the Administration Console	367
From the Zimbra CLI.....	367
Enable Mobile NG for a Single User	368
The Mobile Password Feature	369
Mobile Device Management a.k.a. Mobile Provisioning	369
SyncStates	371
Advanced Settings	373
Shared Folders	374
EAS Filters	375
Mobile Account Loggers.....	379
HSM NG.....	382
Hierarchical Storage Management	382
Zimbra Stores	382
doMoveBlobs.....	383
Volume Management	385
Centralized Storage	400
Policy Management	401
Volumes on Amazon S3 Compatible Services	403
Item Deduplication	408
Advanced Volume Operations	411
Moving Mailboxes Between Mailstores	416

HSM NG Attachment Indexing	418
ABQ Service	423
Components	423
ABQ Modes	424
ABQ Mode Control	425
Dummy data	425
Notifications	425
ABQ CLI	426
Admin NG	432
Delegated Admin Provisioning	432
Quota Management	435
Domain Limits	436
Zimbra Administration as a Delegated Admin	438
Delegated Admin Log Browsing	439
Reports and Information	440
Configuration Reset	444
NG Modules CLI	446
Network NG Modules CLI	446
<code>zxsuite</code> - Network NG Modules Command-Line Interface	446
Incremental Migration to Zimbra 8.8.0 with Backup NG	455
Description	455
Source Data	456
Pre-migration Checks	456
Setting up the Migration	457
The Situation so Far	460
The Migration	460
Incremental Migration FAQ	461
Zimbra Chat	463
About this document	463
Overview	463
Installation	464
Upgrade	465
Troubleshooting	465
Tools	466
Gathering System Information	466
F.A.Q.	467
Advanced Topics	469
Zimbra Connect	474
What is Zimbra Connect	474
Licensing	475
Zimbra Chat and Zimbra Connect	476

Zimbra Connect Zimlet installation	476
URLs and Ports	477
Zimbra Connect administration	477
Browser compatibility	478
UI	478
Instant Messaging and Corporate Communication	480
File sharing	489
Video Chat	489
Instant Meetings	490
Presence	491
Unread Messages	491
Chat History	492
STUN/TURN Server	492
Zimbra Open Drive	495
About this Document	495
Overview	495
Installation	496
Configuration	498
Upgrade	499
Uninstallation	500
Advanced Topics	501
Manual Upgrade	503
Zimbra Drive	506
Introduction	506
Features	506
Differences between Briefcase and Drive	506
Drive V2 UI	506
Feature Description	507
Technical information	513
Zimbra Drive Backup and HSM	514
Briefcase Migration	515
Zimbra Docs	517
Introduction	517
Components	517
Document Management Flow	518
Networking and ports	519
Installation and Configuration	519
Licensing	520
Removal	520
Commands	520
Troubleshooting	522

Appendix A: Command Line Utilities	524
General Tool Information	524
Zimbra CLI Commands	525
Appendix B: Configuring SPNEGO Single Sign-On	586
Configuration Process	586
Create the Kerberos Keytab File	586
Configure ZCS	589
Configure Your Browser	591
Test your setup	592
Troubleshooting setup	592
Configure Kerberos Auth with SPNEGO Auth	593
Setting Up Single Sign-On Options for ZCO	594
Appendix C: ZCS Crontab Jobs	596
How to read the crontab	596
ZCS Cron Jobs	596
Single Server Crontab -l Example	598
Appendix D: ABQ - SOAP API	602
Introduction	602
ABQ API	603
Glossary	606



If you are upgrading/migrating from a previous version of Zimbra and plan to enable the new mobile sync module for Zimbra, please read "["Things to Know Before Upgrading"](#)" and [the install guide](#) for critical information.

License



Synacor, Inc., 2019

© 2019 by Synacor, Inc. Zimbra Collaboration Administrator Guide

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License unless another license agreement between you and Synacor, Inc. provides otherwise. To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Synacor, Inc., 2016
40 La Riviere Drive, Suite 300
Buffalo, New York 14202

<https://www.synacor.com>

Introduction

Zimbra Collaboration is a full-featured messaging and collaboration solution that includes email, address book, calendaring, tasks, and Web document authoring.

Audience

This guide is for system administrators responsible for installing, maintaining, and supporting the server deployment of Zimbra Collaboration.

Readers of this guide should have the following recommended knowledge and skill sets:

- Familiarity with the associated technologies and standards
- Linux operating system and open source concepts
- Industry practices for mail system management

Third-Party Components

Where possible, Zimbra Collaboration adheres to existing industry standards and open source implementations for backup management, user authentication, operating platform, and database management. However, it only supports the specific implementations described in the Zimbra Collaboration architecture overview in the Product Overview chapter as officially tested and certified. This document might occasionally note when other tools are available in the marketplace, but such mention does not constitute an endorsement or certification.

Support and Contact Information

Visit www.zimbra.com to join the community and to be a part of building the best open source messaging solution. We appreciate your feedback and suggestions.

- Contact sales@zimbra.com to purchase Zimbra Collaboration
- Network Edition customers can contact support at support@zimbra.com
- Explore the [Zimbra Forums](#) for answers to installation or configurations problems
- Join the [Zimbra Forums](#), to participate and learn more about the Zimbra Collaboration

For additional product information, the following resources are available:

- [Zimbra Wiki](#)
- [Security Center](#)

Let us know what you like about the product and what you would like to see in the product. Post your ideas to the Zimbra Forum.

Product Life Cycle

This chapter provides information about the Product Life Cycle stages of Zimbra components.

Component Deprecation Statements

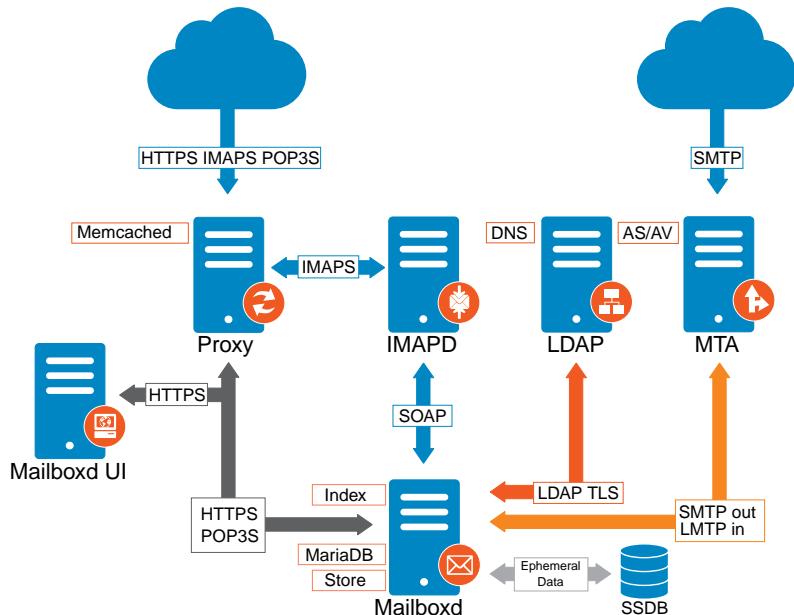
Component	Deprecation Statement
IMAPD	IMAPD was released as Beta with Zimbra 8.8.5, and has not been released as Stable. It has been deprecated.
ZCS Migration Wizard for Exchange	This tool is supported only for PST file import, with End of Technical Guidance set for 31 December 2020. We recommend Audriga's self-service migration solution as a preferred alternative for all account migrations.
ZCS Migration Wizard for Domino	Deprecated
ZCS Account Migration	ZCS Account Migration within the Zimbra Admin UI is no longer supported, with End of Technical Guidance set for 17 December 2019.
Enterprise modules	Zimbra Classic HSM, Classic Backup, and Classic Mobile are deprecated and will be removed in the next release of Zimbra 8.8. Installations that have not yet migrated to new Network Edition NG Modules or ZSP are encouraged to do so.
Zimbra Desktop	This desktop user client is no longer supported, with End of Technical Guidance set for 1 October 2019.
Zimbra Touch Client	Deprecated
Zimbra Mobile Client	Deprecated
HTML Client	No longer supported, with End of Technical Guidance set for 1 July 2022.

Product Overview

This chapter provides a system overview of Zimbra components.

Architectural Overview

The Zimbra Collaboration architecture is built with well-known open source technologies and standards-based protocols. The architecture consists of client interfaces and server components that can run as a single node configuration or be deployed across multiple servers for high availability and increased scalability.



The architecture includes the following core advantages:

Core Advantage	Components/Description
Open source integrations	Linux®, Jetty, Postfix, MariaDB, OpenLDAP®
Industry-standard open protocols	SMTP, LMTP, SOAP, XML, IMAP, POP
Modern technology Design	HTML5, Javascript, XML, and Java
Scalability	Each Zimbra mailbox server includes its own mailbox accounts and associated message store and indexes. The Zimbra platform scales vertically (by adding more system resources) and horizontally (by adding more servers)
Browser-based client interface	
Browser-based Administration Console	Easy, intuitive access to Zimbra Collaboration features, using a standard web platform.

Core Email, Calendar and Collaboration Functionality

Zimbra Collaboration is an innovative messaging and collaboration application that offers the following state-of-the-art solutions that are accessed through the browser based web client.

- Intuitive message management, search, tagging, and sharing.
- Personal, external, and shared calendar.
- Personal and shared Address Books and Distribution Lists.
- Personal and Shared Task lists.

Zimbra Components

Zimbra architecture includes open-source integrations using industry standard protocols. The third-party software listed in [Third-Party Software](#) is bundled with Zimbra software and installed as part of the installation process. These components have been tested and configured to work with the software.

Table 1. Third-Party Software

3rd-Party Component	Description
Jetty	Web application server that runs Zimbra software.
Postfix	Open source mail transfer agent (MTA) that routes mail messages to the appropriate Zimbra server
Open LDAP software	Open source implementation of the Lightweight Directory Access Protocol (LDAP) that stores Zimbra system configuration, the Zimbra Global Address List, and provides user authentication. Zimbra can also work with GAL and authentication services provided by external LDAP directories such as Active Directory
MariaDB	Database software
Lucene	Open source full-featured text and search engine
	Third-party source that converts certain attachment file types to HTML
Anti-virus/anti-spam	Open source components that include: <ul style="list-style-type: none"> • ClamAV, an anti-virus scanner that protects against malicious files • SpamAssassin, a mail filter that attempts to identify spam • Amavisd-new interfaces between the MTA and one or more content checkers
Apache JSieve	Manages filters for email
LibreOffice	High fidelity document preview

Zimbra Application Packages

Zimbra Collaboration provides the application packages listed in [Application Packages](#).

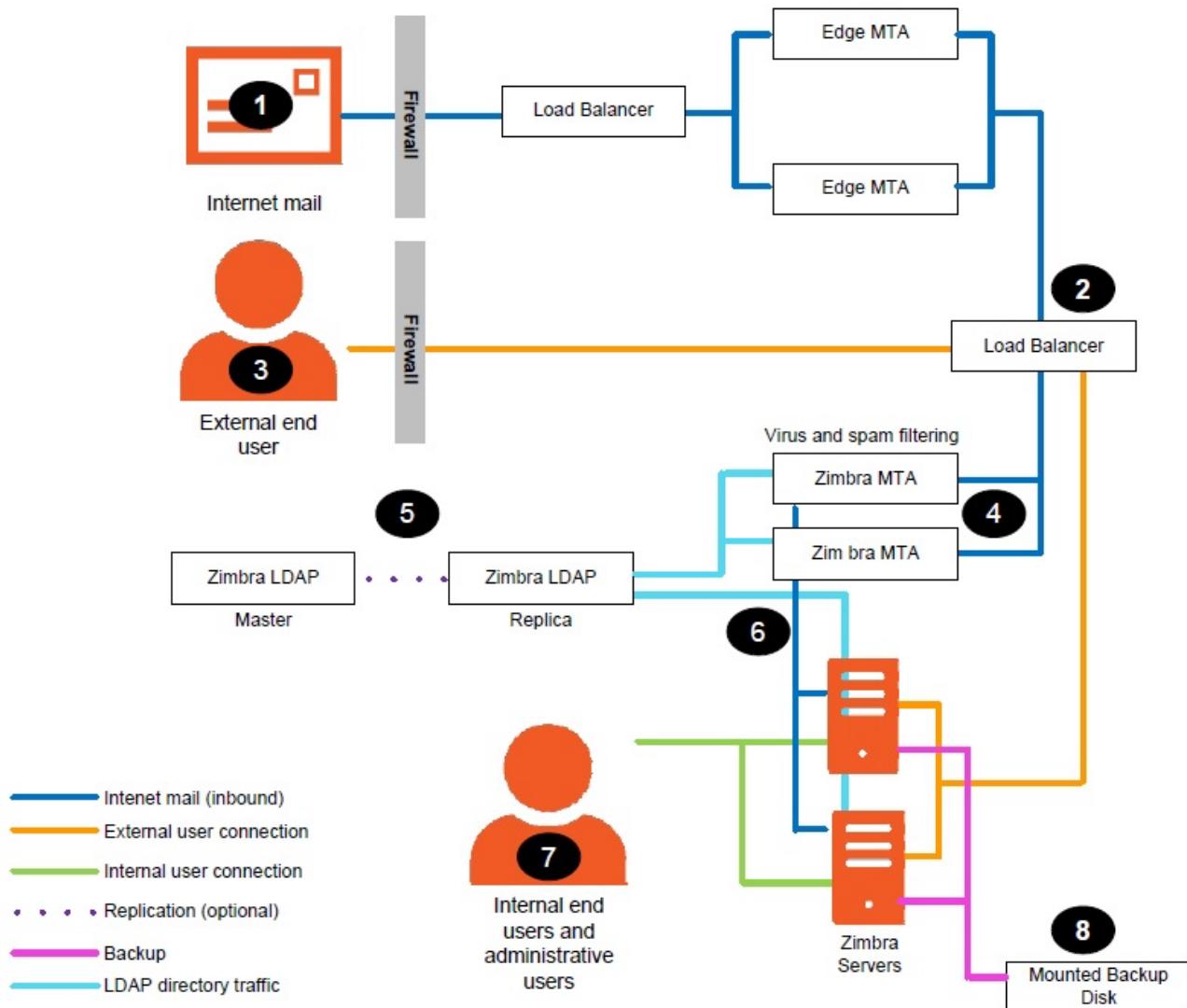
Table 2. Application Packages

Package	Description
Zimbra Core	The libraries, utilities, monitoring tools, and basic configuration files. zmconfigd is contained in the zimbra-core and is automatically enabled to run on all systems.
Zimbra Store	<p>The components for the mailbox server (including Jetty). The Zimbra mailbox server includes the following components:</p> <ul style="list-style-type: none">• Data store—A MariaDB database.• Message store—Location of all email messages and file attachments.• Index store—Index and search technology is provided through Lucene. Index files are maintained for each mailbox.• Web application services—The Jetty web application server runs web applications (webapps) on any store server. It provides one or more web application services.
Zimbra LDAP	Zimbra Collaboration uses the OpenLDAP® software, which is an open source LDAP directory server. User authentication, the Zimbra Global Address List, and configuration attributes are services provided through OpenLDAP. Note that the Zimbra GAL and authentication services can be provided by an external LDAP Directory such as Active Directory.
Zimbra MTA	Postfix is the open source mail transfer agent (MTA) that receives email via SMTP and routes each message to the appropriate Zimbra mailbox server using Local Mail Transfer Protocol (LMTP). The Zimbra MTA also includes the anti-virus and anti-spam components.
Zimbra Proxy	Zimbra Proxy is a high-performance reverse proxy service for passing IMAP[S]/POP[S]/HTTP[S] client requests to other internal ZCS services. This package is normally installed on the MTA server(s) or on its own independent server(s). When the zimbra-proxy package is installed, the proxy feature is enabled by default. Installing the Zimbra Proxy is highly recommended, and required if using a separate web application server.

Package	Description
Zimbra Memcached	Memcached is automatically selected when the zimbra-proxy is installed. At least one server must run zimbra-memcached when the proxy is in use. You can use a single memcached server with one or more Zimbra proxies. zimbra-memcached is required if using a separate web application server.
Zimbra SNMP (Optional)	If you choose to install zimbra-SNMP for monitoring, this package should be installed on every Zimbra server.
Zimbra Logger (Optional)	If used, this is installed on one mailbox server, and must be installed at the same time as the mailbox server. The Zimbra Logger installs tools for syslog aggregation and reporting. If you do not install Logger, the server statistics section of the Administration Console will not display.
Zimbra Spell (Optional)	Aspell is the open source spell checker used on the Zimbra Web Client. When Zimbra-Spell is installed, the Zimbra-Apache package is also installed.
Zimbra Apache	This package is installed automatically when Zimbra Spell or Zimbra Convertd is installed.
Zimbra Convertd	This package is installed on the zimbra-store server. Only one Zimbra-convertd package needs to be present in the Zimbra Collaboration environment. The default is to install one zimbra-convertd on each zimbra-store server. When Zimbra-Convertd is installed, the Zimbra-Apache package is also installed.
Zimbra Archiving (Optional)	Archiving and Discovery offers the ability to store and search all messages delivered to, or sent by the Zimbra Collaboration Server. This package includes the cross mailbox search function which can be used for both live and archive mailbox searches. Note: Using Archiving and Discovery can trigger additional mailbox license usage. To find out more about Zimbra Archiving and Discovery, contact Zimbra sales.

Mail Flow — Multi-Server Configuration

The configuration for each deployment is dependent on numerous variables such as the number of mailboxes, mailbox quotas, performance requirements, existing network infrastructure, IT policies, security methodologies, spam filtering requirements, and more. In general, deployments share common characteristics for incoming traffic and user connectivity, as depicted in the following diagram. Alternate methods for configuring numerous points within the network are also possible.



The numbered sequences are described below:

1. Inbound Internet mail goes through a firewall and load balancing to the edge MTA for spam filtering.
2. The filtered mail then goes through a second load balancer.
3. An external user connecting to the messaging server also goes through a firewall to the second load balancer.
4. The inbound Internet mail goes to any of the Zimbra Collaboration MTA servers and goes through spam and virus filtering.
5. The designated Zimbra Collaboration MTA server looks up the addressee's directory information from the Zimbra Collaboration LDAP replica server.
6. After obtaining the user's information from the Zimbra Collaboration LDPA server, the MTA server sends the mail to the appropriate Zimbra Collaboration server.
7. Internal end-user connections are made directly to any Zimbra Collaboration server that then obtains the user's directory information from Zimbra Collaboration LDAP and redirects the user, as needed.
8. The backups from the Zimbra Collaboration servers can be processed to a mounted disk.

Zimbra System Directory Tree

The following table lists the main directories created by the Zimbra installation packages. The directory organization is identical for any server in the Zimbra Collaboration, when installing under (parent) `/opt/zimbra`.



The directories not listed in the following table are libraries used for building the core Zimbra software or miscellaneous third-party tools.

Table 3. System Directory Tree under `/opt/zimbra`

File	Description
<code>backup/</code>	Backup target contains full and incremental backup data
<code>bin/</code>	Zimbra Collaboration application files, including the utilities described in Command-Line Utilities
<code>cdpolicyd</code>	Policy functions, throttling
<code>clamav/</code>	Clam AV application files for virus and spam controls
<code>conf/</code>	Configuration information
<code>contrib/</code>	Third-party scripts for conveyance
<code>convertd/</code>	Convert service
<code>cyrus-sasl/</code>	SASL AUTH daemon
<code>data/</code>	Includes data directories for LDAP, mailboxd, postfix, amavisd, clamav
<code>db/</code>	Data Store
<code>docs/</code>	SOAP txt files and technical txt files
<code>extensions-extra/</code>	Server extensions for different authentication types
<code>extensions-network-extra/</code>	Server extensions for different network version authentication types
<code>httpd/</code>	Contains the Apache Web server. Used for both aspell and convertd as separate processes
<code>index/</code>	Index store
<code>java/</code>	Contains Java application files
<code>jetty/</code>	mailboxd application server instance. In this directory, the <code>webapps/zimbra/skins</code> folder includes the Zimbra UI theme files
<code>lib/</code>	Libraries
<code>libexec/</code>	Internally used executables
<code>log/</code>	Local logs for Zimbra Collaboration server application
<code>logger/</code>	RRD and SQLite data files for logger services
<code>mariadb/</code>	MariaDB database files
<code>net-snmp/</code>	Used for collecting statistics

File	Description
openldap/	OpenLDAP server installation, pre-configured to work
postfix/	Postfix server installation, pre-configured to work with Zimbra Collaboration
redolog/	Contains current transaction logs for the Zimbra Collaboration server
snmp/	SNMP monitoring files
ssl/	Certificates
store/	Message store
zimbramon/	Contains control scripts and Perl modules
zimlets/	Contains Zimlet zip files that are installed with Zimbra
zimlets-deployed/	Contains Zimlets that are available with the Zimbra Web Client
zimlets-network/	Contains Zimlet zip files for features that are installed with the network edition
zmstat/	mailboxd statistics, saved as .csv files

Zimbra Web Clients

Zimbra offers various web client types that users can log into for use of Zimbra features. The web clients provide mail, calendar, address book, and task functions.

Table 4. Zimbra Web Clients

Client Type	Description
Advanced Web Client	Includes Ajax capability and offers a full set of web collaboration features. This web client works best with newer browsers and fast Internet connections.
Standard Web Client	A good option when Internet connections are slow or users prefer HTML-based messaging for navigating within their mailbox
Mobile HTML Client	Provides mobile access to Zimbra when using the Standard Web Client version.

When users sign in, they view the advanced Zimbra Web Client, unless they use the menu on the login screen to change to the standard version. If ZWC detects the screen resolution to be 800x600, users are automatically redirected to the standard Zimbra Web Client. Users can still choose the advanced ZWC but see a warning message suggesting the use of the standard ZWC for better screen view.

Web Services and Desktop Clients

In addition to using a web browser or mobile device to connect to Zimbra Collaboration, connection is available using a web service, such as Exchange Web Services (EWS), or a desktop client such as

Zimbra Connector to Microsoft Outlook, which uses MAPI. The following are supported:

- **Exchange Web Services (EWS)** provides client access to enable Zimbra Collaboration to communicate with the Exchange Server when using Microsoft Outlook on a Mac device. To enable EWS client access, see the Class of Service section. EWS is a separately licensed add-on feature.
- **Messaging Application Programming Interface (MAPI)** synchronizes to Microsoft Outlook 2016/2013/2010 with full delegate, offline access and support for S/MIME. Use the Zimbra Connector for Outlook to connect to Zimbra Collaboration when using Microsoft Outlook on a Windows device. To enable MAPI (Microsoft Outlook) Connector, see the Class of Service section.
- Support for all POP3, IMAP4, Calendaring Extensions to Web Distributed Authoring and Versioning (CalDAV), and vCard Extensions to Web Distributed Authoring and Versioning (CardDAV) clients.

Offline Mode

Zimbra Offline Mode allows access to data—without network connectivity—when using the Zimbra Web Client (ZWC).

For example, if there is no server connectivity or if server connectivity is lost, ZWC automatically transitions to “offline mode”. When server connectivity is restored, ZWC automatically reverts to “online mode”.

The offline mode uses HTML5, which uses a caching capability that can be considered a super set of the normal browser caching.

Security Measures

The coordinated use of multiple security measures, targeted to increase the security of the whole system, is one of the best approaches to securing your information infrastructure. These measures are implemented in the Zimbra Collaboration platform as a result of defense mechanisms summarized in the following topics:



To view current and detailed security news and alerts, please refer to [Security Center](#) on the [Zimbra Wiki](#).

Identity and Access Management

Key functions built into the system for user identity management are summarized in the following table:

Table 5. Identity and Access Management Functions

Function	Description
Identity Lifecycle Management	The leveraging of LDAP directory for all Create, Read, Update, and Delete (CRUD) functions associated to user administration with Zimbra Collaboration. LDAP usage is optional but all attributes specific to Zimbra Collaboration are stored and managed through the native LDAP directory.
First Factor Authentication	The combined user name and password primarily employed by authorized users when attempting to access the system. These credentials are retained in the user store: the passwords are stored as salted hash that is compared against that of the entered password, for rejection (no match) or acceptance (matched). If external directory (LDAP or Active Directory) is preferred, the appropriate login credentials can be stored in this external LDAP directory. See also Zimbra LDAP Service for more details.
Two Factor Authentication	A second layer of identity security that is configured at the Admin Console to enable or disable passcode generation to mobile devices associated with Zimbra Collaboration. When enabled, user or COS accounts must use the generated passcode to gain access to their client services. See also About 2 Factor Authentication and Two Factor Authentication .
Authorized Access	User accounts are defined by various attributes, permission levels, and policies to allow or disallow what data can be viewed and which functions can be performed. Admin Console administrators can create groups and assign access permissions to support targeted business objectives.

Information Security and Privacy

Functions built into the system to secure data are summarized in the following table:

Table 6. Information Security and Privacy Functions

Key Concept	Description
Management of security, integrity, and privacy	Zimbra Collaboration supports the use of S/MIME certificates (provided by publicly trusted Certification Authority (CA), as well as internal PKI; DomainKeys Identified Mail (DKIM); Domain-based Message Authentication, Reporting and Conformance (DMARC); Amavisd-new, which is housed in the Mail Transfer Agent (MTA) to manage incoming and outgoing DMARC policies.

Encryption methods:

In-transit	Secure connections between endpoints and services use TLS in addition to various other protocols: SMTP, LMTP+STARTTLS, HTTPS, IMAPS/IMAP+STARTTLS, POP3S/POP3+STARTTLS.
At-rest	With S/MIME for end-to-end encryption, data stored in a Zimbra Collaboration message store is encrypted until decryption occurs with the appropriate private key.

Key Concept	Description
Anti-virus and Anti-spam	Both malware and spam are challenged by the Zimbra Collaboration native functionality and third-party plugins: Amavisd-new, ClamAV, and Spam Assassin.

System Logs

The Zimbra Collaboration system logs—generated by SNMP triggers—can be used to record data such as user and administrator activity, login failures, slow queries, mailbox activity, mobile synchronization activity, and data based errors. Events, alerts and traps can be forwarded to log management and event correlation system to create centralized policies and notifications based on your security and compliance requirements.

Table 7. Security Data

Function	Description
Incident response	Administrators can use remote device wiping and/or account lockout in the event of a malicious or accidental activities (such as stolen user account credential, or lost smart phone).
Archiving and discovery	This optional feature allows administrators to select specific user email messages for archival and application of retention policies, which can be used for both archived and live mailboxes.

Licensing

A Zimbra license is required in order to create accounts. When you purchase, renew, or change the Zimbra license, you update the Zimbra server with the new license information.

License Types

Zimbra Collaboration licensing gives administrators better visibility and control into the licensed features they plan to deploy. You can monitor usages and manage the following license types.

License limitations	To set maximum number of...
Accounts limit	Accounts you can create and the number of accounts created are shown.
MAPI accounts limit	Accounts that can use Zimbra Connector for Microsoft Outlook (ZCO).
Exchange web services (EWS) accounts limit	Accounts that can use EWS for connecting to an Exchange server. EWS is a separately licensed add-on.
High-fidelity document preview	Accounts that can use the High-Fidelity document preview. LibreOffice must be installed.
Archiving accounts limit	New archive accounts allowable. The archive feature must be installed.

License Requirements

To try out Zimbra Collaboration, you can obtain trial versions free of charge. Once your system is installed in a production environment, you will need to purchase a subscription or a perpetual license.

License Types	Purpose
Trial	Free of charge: Trial license from the Zimbra website (https://www.zimbra.com). The trial license allows you to create up to 50 users. It expires in 60 days.
Trial extended	Free of charge: Allows you to create up to 50 users and is valid for an extended period of time. Obtainable from Zimbra Sales by contacting sales@zimbra.com or calling 1-972-407-0688.
Subscription	Purchased: Applicable to a specific Zimbra Collaboration system and encrypted with the number of Zimbra accounts (seats) you have purchased, the effective date, and expiration date of the subscription license
Perpetual	Purchased: This license is similar to a subscription license and is valid for a specific Zimbra Collaboration system, is encrypted with the number of Zimbra accounts (seats) you have purchased, the effective date, and an expiration date of 2099-12-31. When you renew your support agreement, no new perpetual license is sent to you, but your Account records in the systems is updated with your new support end date.

License Usage by Account Type

Below is a description of Zimbra Collaboration accounts and if they impact your license limit.

License Account Type	Purpose
System account	System accounts are specific accounts used by Zimbra Collaboration. They include the spam filter accounts for junk mail (spam and ham), virus quarantine account for email messages with viruses, and GALsync account if you configure GAL for your domain. Do not delete these accounts! These accounts do not count against your license
Administrator account	Administrator and delegated administrator accounts count against your license
User account	User accounts count against your license account limit. When you delete an account, the license account limit reflects the change
Alias account	
Distribution list	Not applicable
Resource account	

License Activation

All network edition installations require license activation. New installations have a 10 day grace period from the license issue date before requiring activation. Your license can be activated in the Administration Console.

Admin Console:

Home > Configure > Global Settings > License, from the **Gear** icon select **Activate License**

Upgraded Zimbra Collaboration versions require an immediate activation to maintain network feature functionality.

Automatic License Activation

Licenses are automatically activated if the Zimbra Collaboration server has a connection to the Internet and can communicate with the Zimbra License server. If you are unable to automatically activate your license, see [Manual License Activation](#).

Manual License Activation

For systems that do not have external access to the Zimbra License server, you can use the [Zimbra Support Portal](#) to manually activate your license. Go to the Zimbra website at www.zimbra.com and click **Support** to display the Zimbra Technical Support page. Click the **Zimbra Collaboration Support** link to display the Zimbra Support Portal page. Enter your email and password to log in.

If you have problems accessing the Zimbra Support Portal, contact Zimbra Support at support@zimbra.com.

When Licenses are not Installed or Activated

If you fail to install or activate your Zimbra Collaboration server license, the following scenarios describe how your Zimbra Collaboration server will be impacted.

License Condition	Description/Impact
Not installed	Zimbra Collaboration defaults to single user mode where all features limited by license are limited to one user.
Not valid	Zimbra Collaboration defaults to single user mode.
Not activated	A license activation grace period is 10 days. If for some reason the license is never activated, Zimbra Collaboration defaults to single user mode after 10 days.
For future date	Zimbra Collaboration defaults to single user mode
In grace period	The license ending date has passed and is within the 30 day grace period. All features limited by license are still enabled, but administrators might see license renewal prompts.
Expired	The license ending date has passed and the 30 day grace period has expired. The Zimbra Collaboration server defaults to the feature set of the Open Source Edition.

Obtain a License

On the Zimbra website, go to Downloads to obtain a trial license from the Zimbra Downloads area. Contact Zimbra sales regarding a trial extended license, or to purchase a subscription license or perpetual license, by emailing sales@zimbra.com.

The subscription and perpetual license can only be installed on the Zimbra Collaboration system for which it is purchased. Only one Zimbra license is required for your Zimbra Collaboration environment. This license sets the number of accounts that can be created.

Current license information, including the number of accounts purchased, the number of accounts used, and the expiration date, can be viewed from **Home > Configure > Global Settings > License**.

Managing Licenses

The **Update License** wizard from the Administration Console's **Global Settings** page is used to upload and install a new license. The **Activate License** link on the toolbar activates the license.

Current license information, including the license ID, the issue date, expiration date, number of accounts purchased, and the number of accounts used can be viewed from **Home > Configure > Global Settings > License**.

License Information

You must have a Zimbra Collaboration license to create accounts. When you purchase, renew, or change the Zimbra license, you must update the Zimbra server with the new license information.

The **Update License Wizard** from the Administration Console's Global Settings is used to upload and install a new license. The **Activate License** link on the toolbar activates the license.

Current license information, including the license ID, the issue date, expiration date, number of accounts purchased, and the number of accounts used can be viewed from **Home > Configure > Global Settings > License**.

When the number of accounts created is equal to the number of accounts purchased you will not be able to create new accounts. You can purchase additional accounts or you can delete existing accounts. Contact Zimbra sales to purchase additional accounts.

You must renew your license within 30 days of the expiration date. Starting 30 days before the license expires, when you log on to the Administration Console, a reminder notice is displayed.

License Expiration

When your Zimbra Collaboration Network Edition License expires, a license expiration warning appears in the administrative console and web interface for all users. From the date of the license expiration, there is a 30-day grace period during which the warning message is displayed, but no features are disabled.

Upon expiration of the grace period, the server reverts to the feature set of the Open Source Edition. The following is a list of some of the major functions that are no longer available upon license expiration:

- Backup/Restore
- Exchange Web Services (EWS) — *a separately licensed add-on*
- High-Fidelity Document Preview
- Zimbra Connector for Outlook
- S/MIME

If you maximize your licensed user limit, you are no longer able to create or delete accounts.

If you do not plan to renew your license, you can regain the ability to create or delete accounts by upgrading to Zimbra Collaboration free and open source software (FOSS). You should choose the same version of FOSS that you are currently running on the Zimbra Collaboration Network Edition for this transition, after which you can upgrade to the latest version of Zimbra Collaboration FOSS.

Renewal

When the number of accounts created is equal to the number of accounts purchased you will not be able to create new accounts. You can purchase additional accounts or you can delete existing accounts. Contact Zimbra sales to purchase additional accounts.

You must renew your license within 30 days of the expiration date. Starting 30 days before the license expires, when you log on to the Administration Console, a reminder notice is displayed.

Updating Your License

When you renew or change the Zimbra license, you update Zimbra Collaboration mailbox servers with the new license information. This operation can be performed from either the CLI or the Administration Console.

```
zmlicense
```

Admin Console:

Home > Configure > Global Settings > License

Updating a license:

1. Save the license on the computer you use to access the Administration Console.
2. Log on to the Administration Console, go to **Home > Configure > Global Settings > License**, from the **Gear** icon select **Update License**. The License Installation Wizard opens.
3. Browse to select the license file and click **Next**. The license file is now uploaded.
4. Click **Install** to install the license file.
5. Click **Activate License**. Upgraded Zimbra Collaboration versions require an immediate activation to maintain network feature functionality.

Your license information is updated automatically. The cached account license count is automatically refreshed on each mailbox server.

Zimbra Mailbox Server

The Zimbra mailbox server is a dedicated server that manages all the mailbox content, including messages, contacts, calendar, and attachments.

The Zimbra mailbox server has dedicated volumes for backup and log files. Each Zimbra mailbox server can see only its own storage volumes. Zimbra mailbox servers cannot see, read, or write to another server.

Mailbox Server

Each account is configured on one mailbox server, and this account is associated with a mailbox that contains email messages, attachments, calendar, contacts and collaboration files for that account.

Each mailbox server has its own standalone message store, data store, and index store for the mailboxes on that server. The following is an overview of each store and their directory location.

Message Store

All email messages are stored in MIME format in the Message Store, including the message body and file attachments.

By default, the message store is located on each mailbox server under `/opt/zimbra/store`. Each mailbox has its own directory named after its internal mailbox ID. Mailbox IDs are unique per server, not system-wide.

Messages with multiple recipients are stored as a single -copy on the message store. On UNIX systems, the mailbox directory for each user contains a hard link to the actual file.

When Zimbra Collaboration is installed, one index volume and one message volume are configured on each mailbox server. Each mailbox is assigned to a permanent directory on the current index volume. When a new message is delivered or created, the message is saved in the current message volume.

To manage your email storage resources, you can configure storage volumes for older messages by implementing a Hierarchical Storage Management (HSM) policy. See [Managing Configuration](#).

Data Store

The Data Store is a SQL database where internal mailbox IDs are linked with user accounts. All the message metadata including tags, conversations, and pointers indicate where the messages are stored in the file system. The SQL database files are located in `/opt/zimbra/db`.

Each account (mailbox) resides only on one server. Each server has its own standalone data store containing data for the mailboxes on that server.

- The data store maps the mailbox IDs to the users' LDAP accounts. The primary identifier within the Zimbra Collaboration database is the mailbox ID, rather than a user name or account name.

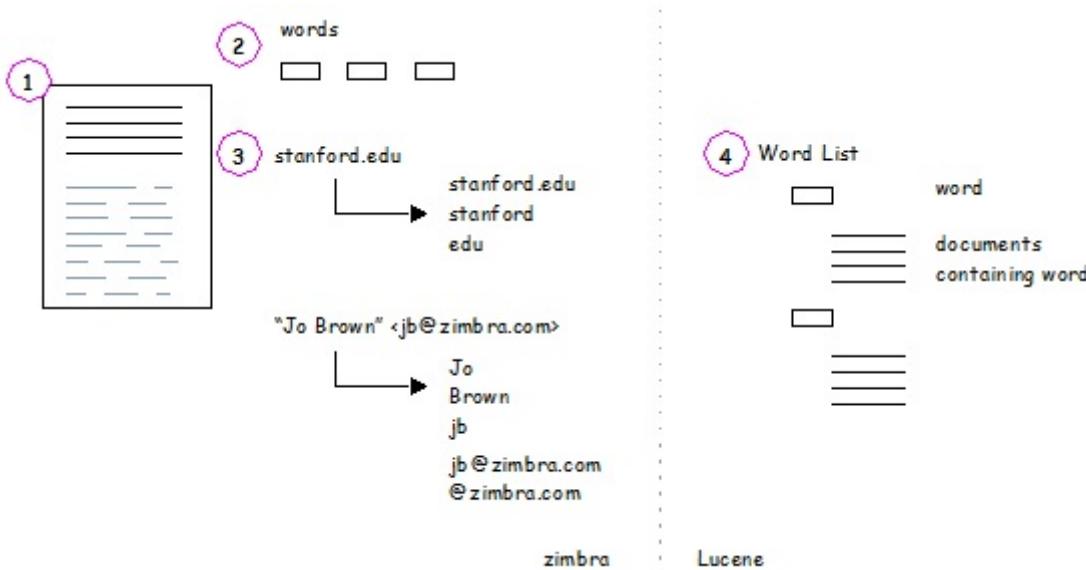
The mailbox ID is only unique within a single mailbox server.

- Metadata including user's set of tag definitions, folders, contacts, calendar appointments, tasks, Briefcase folders, and filter rules are in the data store database.
- Information about each mail message, including whether it is read or unread, and which tags are associated is stored in the data store database.

Index Store

The index and search technology is provided through Apache Lucene. Each email message and attachment is automatically indexed when the message arrives. An index file is associated with each account. Index files are located in `/opt/zimbra/index`.

The tokenizing and indexing process is not configurable by administrators or users.



The process is as follows:

1. The Zimbra MTA routes the incoming email to the mailbox server that contains the account's mailbox.
2. The mailbox server parses the message, including the header, the body, and all readable file attachments such as PDF files or Microsoft Word documents, in order to tokenize the words.
3. The mailbox server passes the tokenized information to Lucene to create the index files.

i Tokenization is the method for indexing by each word. Certain common patterns, such as phone numbers, email addresses, and domain names are tokenized as shown in the Message Tokenization illustration.

Web Application Server

The Jetty web application server runs web applications (webapps) on any store server. It provides one or more web application services.

Mailstore Services

Mailstore services provides the back-end access to mailbox/account data. Webapps for the mailstore include:

- Mailstore (mail server) = `/opt/zimbra/jetty/webapps/service`
- Zimlets = `/opt/zimbra/jetty/webapps/zimlet`

User Interface Services

User Interface services provide front-end user interface access to the mailbox account data and Administration Console, including:

- Zimbra Web Client = `/opt/zimbra/jetty/webapps/zimbra`
- Zimbra administrator console = `/opt/zimbra/jetty/webapps/zimbraAdmin`
- Zimlets = `/opt/zimbra/jetty/webapps/zimlet`

Web Application Server Split

The Web Application Server Split functionality provides an option to separate the mailstore services (mail server) and the user interface services (web client server).

For example, a web client server running 'zimbra,zimbraAdmin' webapps serving the static UI content like html/css pages, and mail server running 'service' webapp serving all the SOAP requests. These servers are running in split mode.

The Web Application Server Split benefits include:

- Splitting the web client server from the mail server makes the customization process more agile, allowing the roll out of new or updated web UI customization without having to restart the mail servers. This means zero down time.
- If you want to customize the Zimbra web client or Zimbra Administration Console, you can take the web client server offline and run customization or maintenance, while not having to take down the mail server.
- The web client server is completely decoupled from mailbox accounts. This means any web client server can service any account request.

Installation and Configuration of the Web Application Server Split

For installation and configuration of the Web Application Server Split, see the Zimbra Collaboration Multi-Server Installation Guide.

Backing Up the Mailbox Server

Zimbra Collaboration includes a configurable backup manager that resides on every Zimbra Collaboration server and performs both backup and restore functions. You do not have to stop the Zimbra Collaboration server in order to run the backup process. The backup manager can be used

to restore a single user, rather than having to restore the entire system in the event that one user's mailbox becomes corrupted. Full and incremental backups are in `/opt/zimbra/backup`. See [Backup and Restore](#).

Each Zimbra mailbox server generates redo logs that contain current and archived transactions processed by the message store server since the last incremental backup. When the server is restored, after the backed up files are fully restored, any redo logs in the archive and the current redo log in use are replayed to bring the system to the point before the failure.

Mailbox Server Logs

A Zimbra Collaboration deployment consists of various third-party components with one or more mailbox servers. Each of the components may generate its own logging output. Local logs are in `/opt/zimbra/log`.

Selected Zimbra Collaboration log messages generate SNMP traps, which you can capture using any SNMP monitoring software. See [Monitoring ZCS Servers](#).



System logs, redo logs, and backup sessions should be on separate disks to minimize the possibility of unrecoverable data loss in the event that one of those disks fails.

IMAP

Zimbra Collaboration has a built-in IMAP server which is installed by default and is part of zimbra-mailboxd process ([Zimbra Mailbox Server](#)).

Common IMAP Configuration settings

The following global and server level configuration attributes are available to control and tune the IMAP service.

- **zimbraImapServerEnabled**. When set to TRUE, in-process IMAP server is enabled. When set to FALSE, in-process IMAP server is disabled. Default value is TRUE.
- **zimbraImapSSLServerEnabled**. When set to TRUE, in-process IMAP SSL server is enabled. When set to FALSE, in-process IMAP SSL server is disabled. Default value is TRUE
- **zimbraImapBindAddress** (can be set only on server level). Specifies interface address on which in-process IMAP server should listen; if empty, binds to all interfaces.
- **zimbraImapBindPort**. Specifies port number on which in-process IMAP server should listen. Default value is 7143.
- **zimbraImapSSLBindAddress** (can be set only on server level). Specifies interface address on which in-process IMAP SSL server should listen; if empty, binds to all interfaces.
- **zimbraImapSSLBindPort**. Specifies port number on which in-process IMAP SSL server should listen on. Default value is 7993.
- **zimbraImapNumThreads**. Specifies number of threads in IMAP handler's thread pool. Zimbra Collaboration uses IMAP NIO by default, which allows each IMAP handler thread to handle multiple connections. The default value of 200 is sufficient to handle up to 10,000 active IMAP clients.
- **zimbraImapCleartextLoginEnabled**. Specifies whether or not to allow cleartext logins over a non SSL/TLS connection. Default value is FALSE.
- **zimbraImapProxyBindPort**. Specifies port number on which IMAP proxy server should listen. Default value is 143. See [Zimbra Proxy Components](#) for more information.
- **zimbraImapSSLProxyBindPort**. Specifies port number on which IMAP SSL proxy server should listen. Default value is 993. See [Zimbra Proxy Components](#) for more information.
- **zimbraImapMaxRequestSize**. Specifies maximum size of IMAP request in bytes excluding literal data. **Note:** this setting does not apply to IMAP LOGIN requests. IMAP LOGIN requests are handled by IMAP Proxy ([Zimbra Proxy Components](#)) and are limited to 256 characters.
- **zimbraImapInactiveSessionCacheMaxDiskSize**. Specifies the maximum disk size of inactive IMAP cache in Bytes before eviction. By default this value is 10GB. This is a rough limit, because due to internals of Ehcache actual size on disk will often exceed this limit by a modest margin.
- **zimbraImapInactiveSessionEhcsize**. Specifies the maximum heap size of the inactive session cache in Bytes before eviction. By default this value is 1 megabyte. This is a rough limit, because due to internals of Ehcache actual size in memory will often exceed this limit by a modest margin.

- **zimbraImapActiveSessionEhcaceMaxDiskSize.** Specifies the maximum amount of disk space the imap active session cache will consume in Bytes before eviction. By default this value is 100 gigabytes. This is a rough limit, because due to internals of ehcache actual size in memory will often exceed this limit by a modest margin.

Zimbra LDAP Service

LDAP directory services provide a centralized repository for information about users and devices that are authorized to use your Zimbra service. The central repository used for Zimbra's LDAP data is the OpenLDAP directory server.



Zimbra Collaboration supports integration with Microsoft's Active Directory Server. Contact support for information on specific directory implementation scenarios.

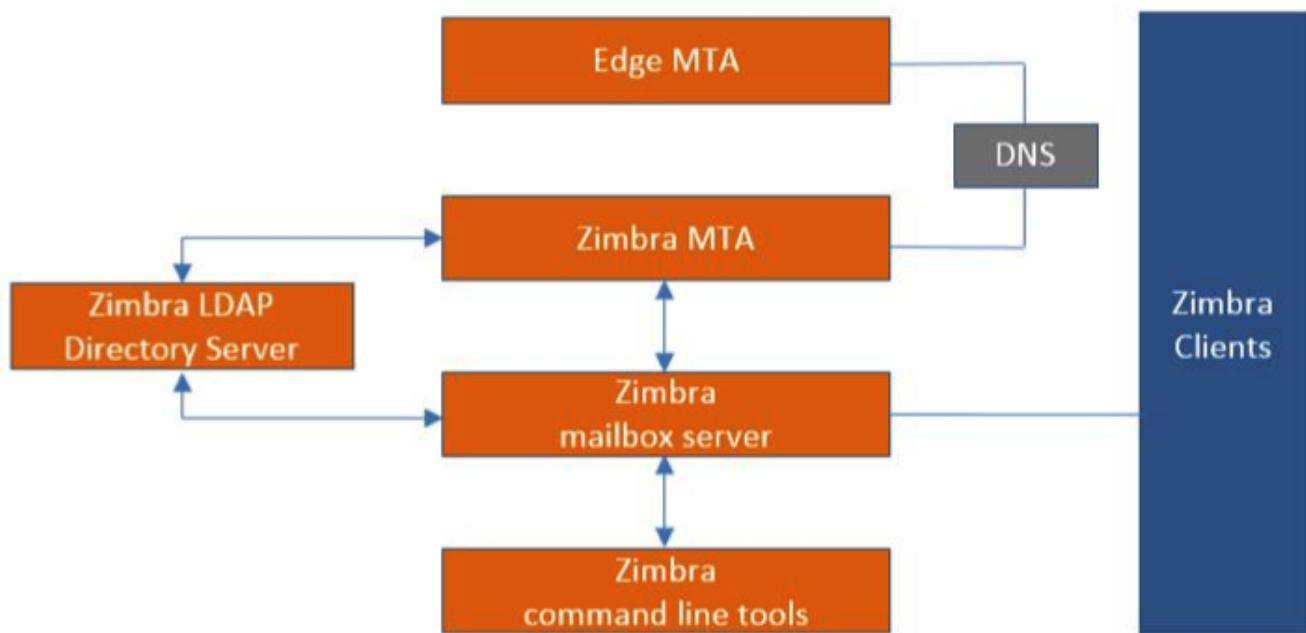
The LDAP server is installed when ZCS is installed. Each server has its own LDAP entry that includes attributes specifying operating parameters. In addition, a global configuration object sets defaults for any server whose entry does not specify every attribute.

A subset of these attributes can be modified through the Zimbra administration console and others through the zmprov commands.

LDAP Traffic Flow

The LDAP Directory Traffic figure shows traffic between the Zimbra-LDAP directory server and the other servers in the Zimbra Collaboration system. The Zimbra MTA and the Zimbra Collaboration mailbox server read from, or write to, the LDAP database on the directory server.

The Zimbra clients connect through the Zimbra server, which connects to LDAP.

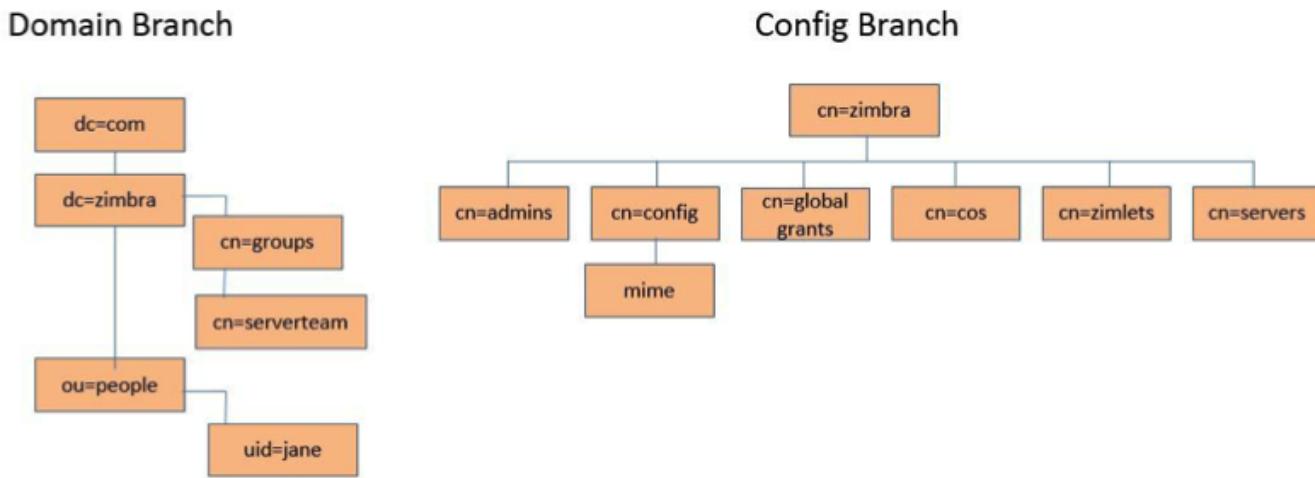


LDAP Directory Hierarchy

LDAP directories are arranged in an hierachal tree-like structure with two types of branches, the mail branches and the config branch. Mail branches are organized by domain. Entries belong to a domain, such as accounts, groups, aliases, are provisioned under the domain DN in the directory.

The config branch contains admin system entries that are not part of a domain. Config branch entries include system admin accounts, global config, global grants, COS, servers, mime types, and Zimlets.

The Zimbra LDAP Hierarchy figure shows the Zimbra LDAP hierarchy. Each type of entry (object) has certain associated object classes.



An LDAP directory entry consists of a collection of attributes and has a globally unique distinguished name ([dn](#)). The attributes allowed for an entry are determined by the *object classes* associated with that entry. The values of the object class attributes determine the schema rules the entry must follow.

An entry's object class that determines what kind of entry it is, is called a structural object class and cannot be changed. Other object classes are called auxiliary and may be added to or deleted from the entry.

Use of auxiliary object classes in LDAP allows for an object class to be combined with an existing object class. For example, an entry with structural object class **inetOrgPerson**, and auxiliary object class **zimbraAccount**, would be an account. An entry with the structural object class **zimbraServer** would be a server in the Zimbra system that has one or more Zimbra packages installed.

Zimbra Collaboration LDAP Schema

At the core of every LDAP implementation is a database organized using a schema.

The Zimbra LDAP schema extends the generic schema included with OpenLDAP software. It is designed to coexist with existing directory installations.

All attributes and object classes specifically created for Zimbra Collaboration are prefaced by "zimbra", such as **zimbraAccount** object class or **zimbraAttachmentsBlocked** attribute.

The following schema files are included in the OpenLDAP implementation:

- core.schema
- cosine.schema
- inetorgperson.schema

- zimbra.schema
- amavisd.schema
- dyngroup.schema
- nis.schema



You cannot modify the Zimbra schema.

Zimbra Collaboration Objects

Object	Description	Object class
Accounts	Represents an account on the Zimbra mailbox server that can be logged into. Account entries are either administrators or user accounts. The object class name is zimbraAccount . This object class extends the zimbraMailRecipient object class. All accounts have the following properties: A name in the format of user@example.domain A unique ID that never changes and is never reused A set of attributes, some of which are user-modifiable (preferences) and others that are only configurable by administrators All user accounts are associated with a domain, so a domain must be created before creating any accounts.	zimbraAccount
Class of Service (COS)	Defines the default attributes an account has and what features are allowed or denied. The COS controls features, default preference settings, mailbox quotas, message lifetime, password restrictions, attachment blocking, and server pools for creation of new accounts.	zimbraCOS
Domains	Represents an email domain such as example.com or example.org . A domain must exist before email addressed to users in that domain can be delivered.	zimbraDomain
Distribution Lists	Also known as mailing lists, are used to send mail to all members of a list by sending a single email to the list address.	zimbraDistributionList

Object	Description	Object class
Dynamic Groups	<p>Are like distribution lists. The difference is members of a dynamic group are dynamically computed by a LDAP search. The LDAP search filter is defined in an attribute on the dynamic group entry.</p> <p> Both distribution lists and dynamic groups can be used as grantee or target in the delegated administrator framework.</p>	zimbraGroup
Servers	Represents a particular server in the Zimbra system that has one or more of the Zimbra software packages installed. Attributes describe server configuration information, such as which services are running on the server.	zimbraServer
Global Configuration	Specifies default values for the following objects: server and domain. If the attributes are not set for other objects, the values are inherited from the global settings. Global configuration values are required and are set during installation as part of the Zimbra core package. These become the default values for the system.	zimbraGlobalConfig
Alias	Represents an alias of an account, distribution list or a dynamic group. The zimbraAliasTarget attribute points to target entry of this alias entry.	zimbraAlias
Zimlet	Defines Zimlets that are installed and configured in Zimbra.	zimbraZimletEntry
Calendar Resource	Defines a calendar resource such as conference rooms or equipment that can be selected for a meeting. A calendar resource is an account with additional attributes on the zimbraCalendarResource object class.	zimbraCalendarResource

Object	Description	Object class
Identity	Represents a persona of a user. A persona contains the user's identity such as display name and a link to the signature entry used for outgoing emails. A user can create multiple personas. Identity entries are created under the user's LDAP entry in the DIT.	zimbraIdentity
Data Source	Represents an external mail source of a user. Two examples of data source are POP3 and IMAP. A data source contains the POP3/IMAP server name, port, and password for the user's external email account. The data source also contains persona information, including the display name and a link to the signature entry for outgoing email messages sent on behalf of the external account. Data Source entries are created under the user's LDAP entry in the DIT.	zimbraDataSource
Signature	Represents a user's signature. A user can create multiple signatures. Signature entries are created under the user's LDAP entry in the DIT.	zimbraSignature

Account Authentication

Supported authentication mechanisms are Internal, External LDAP, and External Active Directory. The authentication method type is set on a per-domain basis. If **zimbraAuthMech** attribute is not set, the default is to use internal authentication.

The internal authentication method uses the Zimbra schema running on the OpenLDAP server.

The **zimbraAuthFallbackToLocal** attribute can be enabled so that the system falls back to the local authentication if external authentication fails. The default is FALSE.

Internal Authentication Mechanism

The internal authentication method uses the Zimbra schema running on the OpenLDAP directory server. For accounts stored in the OpenLDAP server, the **userPassword** attribute stores a salted-SHA512 (SSHA512) digest of the user's password. The user's provided password is computed into the SSHA digest and then compared to the stored value.

External LDAP and External AD Authentication Mechanism

External LDAP and external Active Directory authentication can be used if the email environment uses another LDAP server or Microsoft Active Directory for authentication and Zimbra LDAP for all other Zimbra Collaboration related transactions. This requires that users exist in both OpenLDAP

and in the external LDAP server.

The external authentication methods attempt to bind to the specified LDAP server using the supplied user name and password. If this bind succeeds, the connection is closed and the password is considered valid.

The `zimbraAuthLdapURL` and `zimbraAuthLdapBindDn` attributes are required for external authentication.

- `zimbraAuthLdapURL` attribute `ldap://ldapserver:port/` identifies the IP address or host name of the external directory server, and port is the port number. You can also use the fully qualified host name instead of the port number.

For example:

```
ldap://server1:3268  
ldap://exch1.acme.com
```

If it is an SSL connection, use `ldaps:` instead of `ldap:`. The SSL certificate used by the server must be configured as a trusted certificate.

- `zimbraAuthLdapBindDn` attribute is a format string used to determine which DN to use when binding to the external directory server.

During the authentication process, the user name starts out in the format: `user@example.com`

The user name might need to be transformed into a valid LDAP bind `DN` (distinguished name) in the external directory. In the case of Active Directory, that bind `dn` might be in a different domain.

Custom Authentication

You can implement a custom authentication to integrate external authentication to your proprietary identity database. When an authentication request comes in, Zimbra checks the designated auth mechanism for the domain. If the auth mechanism is set to custom authentication, Zimbra invokes the registered custom auth handler to authenticate the user.

To set up custom authentication, prepare the domain for the custom auth and register the custom authentication handler.

Preparing a domain for custom auth

To enable a domain for custom auth, set the domain attribute, `zimbraAuthMech` to `custom:{registered-custom-auth-handler-name}`.

In the following example, "sample" is the name under which custom authentication is registered.

Example 1. Enable a domain for custom authentication

```
zmprov modifydomain {domain|id} zimbraAuthMech custom:sample
```

Register a custom authentication handler

To register a custom authentication handler, invoke:

```
ZimbraCustomAuth.register( handlerName, handler )
```

in the init method of the extension.

- Class: **com.zimbra.cs.account.ldap.ZimbraCustomAuth**
- Method: **public synchronized static void register (String handlerName, ZimbraCustomAuth handler)**

Definitions:

- **handlerName** is the name under which this custom auth handler is registered to Zimbra's authentication infrastructure. This name is set in the domain's zimbraAuthMech attribute of the domain.
- **handler** is the object on which the authenticate method is invoked for this custom auth handler. The object has to be an instance of **ZimbraCustomAuth** (or subclasses of it).

Example 2. Registering a custom authentication handler

```
public class SampleExtensionCustomAuth implements ZimbraExtension {  
  
    public void init() throws ServiceException {  
        /*  
         * Register to Zimbra's authentication infrastructure  
         * custom:sample should be set for domain attribute zimbraAuthMech  
         */  
        ZimbraCustomAuth.register("sample", new SampleCustomAuth());  
    }  
    ...  
}
```

How Custom Authentication Works

When an authentication request comes in, if the domain is specified to use custom auth, the authenticating framework invokes the authenticate method on the **ZimbraCustomAuth** instance passed as the handler parameter to **ZimbraCustomAuth.register()**.

The account object for the principal to be authenticated and the clear-text password entered by the

user are passed to `ZimbraCustomAuth.authenticate()`.

All attributes of the account can be retrieved from the account object.

Kerberos5 Authentication Mechanism

Kerberos5 Authentication Mechanism authenticates users against an external Kerberos server.

1. Set the domain attribute `zimbraAuthMech` to `kerberos5`.
2. Set the domain attribute `zimbraAuthKerberos5Realm` to the Kerberos5 realm in which users in this domain are created in the Kerberos database. When users log in with an email password and the domain, `zimbraAuthMech` is set to `kerberos5`, the server constructs the Kerberos5 principal by `{localpart-of-the-email}@{value-of-zimbraAuthKerberos5Realm}` and uses that to authenticate to the kerberos5 server.

To specify Kerberos5 for an individual account set the account's `zimbraForeignPrincipal` as `kerberos5:{kerberos5-principal}`. For example: `kerberos5:user1@MYREALM.COM`.

Global Address List

The Global Address List (GAL) is a company directory of users, usually within the organization itself, that is available to all users of the email system. Zimbra Collaboration uses the company directory to look up user addresses from within the company.

For each Zimbra Collaboration domain you can configure GAL to use:

- External LDAP server
- Zimbra Collaboration internal LDAP server
- Both external LDAP server and Zimbra Collaboration LDAP in GAL searches

The Zimbra Collaboration Web Client can search the GAL. When the user searches for a name, that name is turned into an LDAP search filter similar to the following example, where the string `%s` is the name the user is searching for.

Example 3. Searching the GAL

```
(|(cn = %s*)(sn=%s*)(gn=%s*)(mail=%s*)
  (zimbraMailDeliveryAddress = %s*)
  (zimbraMailAlias=%s*)
  (zimbraMailAddress = %s*)
```

GAL Attributes in Zimbra Collaboration

The [Attributes Mapped to Zimbra Collaboration Contact](#) table maps generic GAL search attributes to their Zimbra Collaboration contact fields.

LDAP attributes are mapped to GAL entry fields. For example, the LDAP attribute `displayName` and `cn` can be mapped to GAL entry field `fullName`. The mapping is configured in the `zimbraGalLdapAttrMap` attribute.

Table 8. Attributes Mapped to Zimbra Collaboration Contact

Standard LDAP Attribute	Zimbra Collaboration Contact Field
<code>co</code>	<code>workCountry</code>
<code>company</code>	<code>Company</code>
<code>givenName/gn</code>	<code>firstName</code>
<code>sn</code>	<code>lastName</code>
<code>cn</code>	<code>fullName</code>
<code>initials</code>	<code>initials</code>
<code>l</code>	<code>workCity</code>
<code>street, streetaddress</code>	<code>workStreet</code>
<code>postalCode</code>	<code>workPostalCode</code>
<code>telephoneNumber</code>	<code>workPhone</code>
<code>mobile</code>	<code>mobile</code>
<code>pager</code>	<code>pager</code>
<code>facsimileTelephoneNumber</code>	<code>faxNumber</code>
<code>st</code>	<code>workState</code>
<code>title</code>	<code>jobTitle</code>
<code>mail</code>	<code>email</code>
<code>thumbnailPhoto</code>	<code>thumbnailPhoto</code>
<code>objectClass</code>	Not currently mapped

Zimbra Collaboration GAL Search Parameters

GAL is configured on a per-domain basis. To configure the attributes, you can run the GAL Configuration Wizard from the Administration Console.

Modifying Attributes

Additions, changes and deletions to the GAL attributes are made through the Zimbra Administration Console or from the `zmprov` commands.

Users can modify attributes for their account in the directory when users change their options from the Zimbra Web Client, they also modify the attributes when they change their preferences.

Flushing LDAP Cache

When you modify the following type of entries in the Zimbra LDAP server, you might need to flush

the LDAP cache to make the change available on the server.

- Themes
- Locales
- Account
- Groups
- COS
- Domains
- Global configuration
- Server
- Zimlet configuration

Flush the Cache for Themes and Locales

When you add or change theme (skin) property files and locale resource files for ZCS on a server, you must flush the cache to make the new content available.

To flush skins:

```
zmprov flushCache skin
```

To flush locales

```
zmprov flushCache locale
```

Flush Accounts, Groups, COS, Domains, and Servers

When you modify the account, COS, groups, domain, and server attributes, the change is effective immediately on the server to which the modification is done. On the other servers, the LDAP entries are automatically updated after a period of time if the attributes are cached.

The default ZCS setting to update the server is 15 minutes. The caching period is configured on local config key.

To change the setting:

```
zmlocalconfig ldap_cache_<object>_maxage
```

To enable changes immediately:

```
zmprov flushCache {account|cos|domain|group|server|...} [name|id]...
```

If you do not specify a name or ID along with the type, all entries in cache for that type are flushed and the cache is reloaded.



Some server attributes require a server restart even after the cache is flushed. For example, settings like bind port or number of processing threads.

Flush Global Attributes

When you modify global config attributes, the changes are effective immediately on the server to which the modification is done. On other mailbox servers, you must flush the cache to make the changes available or restart the server. LDAP entries for global config attributes do not expire.

Some global config attributes are computed into internal representations only once per server restart. For efficiency reasons, changes to those attributes are not effective until after a server restart, even after the cache is flushed. Also, some global configuration settings and server settings that are inherited from global config are only read once at server startup, for example port or number of processing threads. Modifying these types of attributes requires a server restart.

To flush the cache for global config changes on all servers:

1. Modify the setting on the local server

```
zmprov mcf zimbraImapClearTextLoginEnabled TRUE
```

The change is performed via the server identified by the localconfig keys `zimbra_zmprov_default_soap_server` and `zimbra_admin_service_port`.

2. To flush the global config cache on all other servers, `zmprov flushCache` must be issued on all servers, one at a time (or use `zmprov flushCache -a`).

For example:

```
zmprov ls server2 flushCache config  
zmprov ls server3 flushCache config
```

3. To determine if the action requires a restart

```
zmprov desc -a <attributename>
```

The `requiresRestart` value is added to the output if a restart is required.

Zimbra Mail Transfer Agent

The Zimbra MTA (Mail Transfer Agent) receives mail via SMTP and routes each message using Local Mail Transfer Protocol (LMTP) to the appropriate Zimbra mailbox server.



You can set MTA parameters with the Admin Console and the CLI. However, it is highly recommended that you use the CLI for MTA configuration to ensure the best results.

The Zimbra MTA server includes the following programs:

MTA Server Programs	Purpose/Description
Postfix MTA	Mail routing, mail relay, and attachment blocking
Clam Anti-Virus	Scanning email messages and attachments in email messages for viruses
Spam Assassin	Identify unsolicited commercial email (spam)
Amavisd-New	Interface between Postfix and ClamAV / SpamAssassin
Zimbra Milter Server	Enforce restrictions on which addresses can send to distribution lists and adds Reply-To and X-Zimbra-DL headers to messages sent from distribution lists
Zimbra policy server	Aid in protecting Alias Domains from Backscatter Spam
Cluebringer	Policy daemon/cbpolicyd used to enforce actions, such as rate limiting. For more information, see https://wiki.zimbra.com/wiki/Postfix_Policyd
Opendkim	Sign outgoing email if it has been configured to do so. For more information, see https://wiki.zimbra.com/wiki/Configuring_for_DKIM_Signing

In the Zimbra Collaboration configuration, mail transfer and delivery are distinct functions: Postfix acts as a MTA, and the Zimbra mail server acts as a Mail Delivery Agent (MDA).

The MTA configuration is stored in LDAP. The **zmconfigd** process polls the LDAP directory every two minutes for modifications and updates the Postfix configuration files with the changes.

Incoming Mail Routing Overview

The Zimbra mailbox server receives the messages from the Zimbra MTA server and passes them through any filters that have been created.

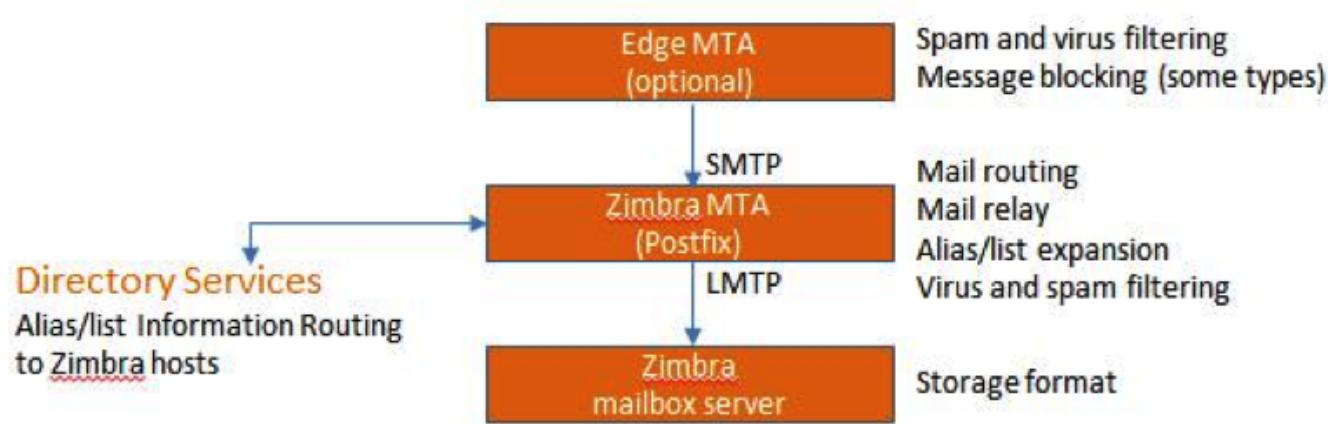
The MTA server receives mail via SMTP and routes each mail message to the appropriate mailbox server using LMTP. As each mail message arrives, its contents are indexed so that all elements can be searched.

Zimbra MTA Deployment

ZCS includes a precompiled version of Postfix to route and relay mail and manage attachments.

Postfix receives inbound messages via SMTP, performs anti-virus and anti-spam filtering and hands off the mail messages to the Zimbra Collaboration server via LMTP.

Postfix also plays a role in transferring outbound messages. Messages composed from the Zimbra Web Client are sent by the Zimbra server through Postfix, including messages sent to other users on the same server.



The Edge MTA can be any edge security solution for mail. You might already deploy such solutions for functions such as filtering. Some filtering might be duplicated between an edge MTA and the Zimbra MTA.

Postfix Configuration Files

Zimbra modified Postfix files—main.cf and master.cf—specifically to work with ZCS:

- **main.cf**—Modified to include the LDAP tables. The `zmconfigd` in the Zimbra MTA pulls data from the Zimbra LDAP and modifies the Postfix configuration files.
- **master.cf**—Modified to use Amavisd-New.



Changes made to postfix configuration files will be overwritten with every upgrade and should be well documented. If possible, try to implement any necessary configuration changes using Zimbra defined parameters.

SMTP Authentication

SMTP authentication allows authorized mail clients from external networks to relay messages through the Zimbra MTA. The user ID and password is sent to the MTA when the SMTP client sends mail so that the MTA can verify if the user is allowed to relay mail.

The user ID and password is sent to the MTA when the SMTP client sends mail. This ensures that the MTA can verify if the user is allowed to relay mail, by checking the associated credentials with the LDAP account.



User authentication is provided through the Zimbra LDAP directory server, or if implemented, through the Microsoft Active Directory Sever.

SMTP Restrictions

You can enable restrictions so that messages are not accepted by Postfix when non-standard or other disapproved behavior is exhibited by an incoming SMTP client. These restrictions provide some protection against spam senders. By default, clients that do not greet with a fully qualified domain name are restricted. DNS based restrictions are also available.



Understand the implications of these restrictions before you implement them. You might have to compromise on these checks to accommodate people outside of your system who have poorly implemented mail systems.

Sending Non Local Mail to a Different Server

You can configure Postfix to send nonlocal mail to a different SMTP server, commonly referred to as a relay or smart host.

A common use case for a relay host is when an ISP requires that all your email be relayed through a designated host, or if you have filtering SMTP proxy servers.

The relay host setting must not be confused with Web mail MTA setting. Relay host is the MTA to which Postfix relays non-local email. Webmail MTA is used by the Zimbra server for composed messages and must be the location of the Postfix server in the Zimbra MTA package.

To use the Administration Console to configure Relay MTA for external delivery:

Admin Console:

Home > Configure > Global Settings > MTA → Network



To prevent mail loops, use caution when setting the relay host.

Zimbra Administration

Configure

Global Settings

General Information

Attachments

MTA

IMAP

POP

AS/AV

FreeBusy Interop

Themes

Advanced

Authentication

Retention Policy

Proxy

Backup/Restore

License

HSM

SMIME

AOL

Recent Objects

inbound at zimbra.com

Home - Configure - Global Settings - MTA

Note: Settings only apply to servers that have the appropriate service(s) installed and enabled. Settings applied to servers, domains and classes of service override global settings.

> Authentication

> Network

Web mail MTA Hostnames: localhost Remove

Web mail MTA Port: 25

Relay MTA for external delivery:

Relay MTA for external delivery (fallback):

If your MX records point to a spam-relay or any other external non-zimbra server, enter the name of that server in "Inbound SMTP host name" field.

Inbound SMTP host name:

MTA Trusted Networks:

Enable DNS lookups
Allow domain administrators to check MX records from Admin Console

Anti-Virus and Anti-Spam Protection

The Amavisd-New utility is the interface between the Zimbra MTA and Clam Anti-Virus (ClamAV)

and SpamAssassin scanners.

Anti-Virus Protection

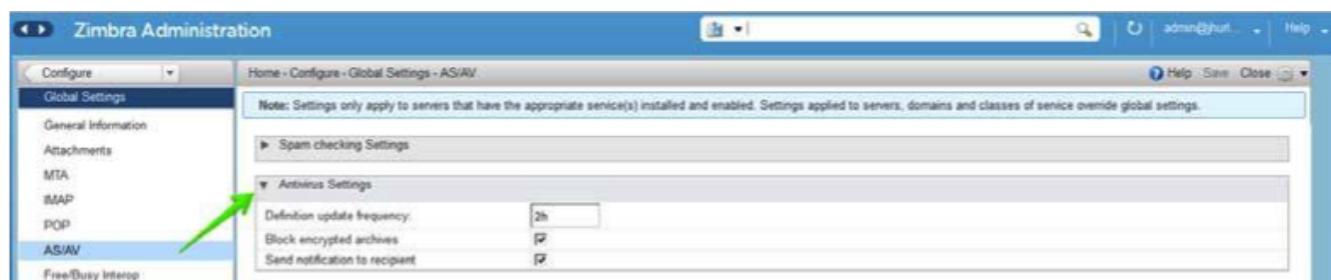
ClamAV software is the virus protection engine enabled for each ZCS server.

The anti-virus software is configured to put messages that have been identified as having a virus to the virus quarantine mailbox. By default, the Zimbra MTA checks every two hours for any new anti-virus updates from ClamAV.

You can change anti-virus settings at the Administration Console.

Admin Console:

Home > Configure > Global Settings > AS/AV → Anti-virus Settings



Updates are obtained via HTTP from the ClamAV website.

Scanning Attachments in Outgoing Mail

You can enable real-time scanning of attachments in outgoing emails sent using the Zimbra Web Client. If enabled, when an attachment is added to an email, it is scanned using ClamAV prior to sending the message. If ClamAV detects a virus, it will block attaching the file to the message. By default, scanning is configured for a single node installation.

To enable scanning, using a single node:

```
zmprov mcf zimbraAttachmentsScanURL clam://localhost:3310/  
zmprov mcf zimbraAttachmentsScanEnabled TRUE
```

To enable scanning in a multi-node environment:

1. Designate the MTA nodes to handle ClamAV scanning.
2. Enable, as follows:

```
zmprov ms <mta_server> zimbraClamAVBindAddress <mta_server>  
zmprov mcf zimbraAttachmentsScanURL clam://<mta_server>:3310/  
zmprov mcf zimbraAttachmentsScanEnabled TRUE
```

Anti-Spam Protection

Zimbra uses SpamAssassin to identify unsolicited commercial email (spam) with learned data stored in either the Berkeley DB database or a MariaDB database. You can also use the Postscreen function to provide additional protection against mail server overload. Both strategies are described in the following topics:

- [Spam Assassin Methods for Avoiding Spam](#)
- [Postscreen Methods for Avoiding Spam](#)

Spam Assassin Methods for Avoiding Spam

Usage guidelines are provided in the following topics:

- [Managing the Spam Assassin Score](#)
- [Training the Spam Filter](#)
- [Configuring Final Destination for Spam](#)
- [Setting Up Trusted Networks](#)
- [Enabling a Milter Server](#)



For information about how to customize SpamAssassin, see https://wiki.zimbra.com/wiki/Anti-spam_strategies.

Managing the Spam Assassin Score: SpamAssassin uses predefined rules as well as a Bayes database to score messages with a numerical range. Zimbra uses a percentage value to determine “spaminess” based on a SpamAssassin score of 20 as 100%. Any message tagged between 33%-75% is considered spam and delivered to the user’s junk folder. Messages tagged above 75% are always considered spam and discarded.

You can change the spam percentage settings, and the subject prefix at the Administration Console.

Admin Console:

Home > Configure > Global Settings > AS/AV → Spam checking Settings

The screenshot shows the Zimbra Administration interface. On the left, there's a sidebar with a 'Configure' dropdown and several menu items: Global Settings, General Information, Attachments, MTA, IMAP, POP, AS/AV (which is highlighted), Free/Busy Interv., Themes, Advanced, and Authentication. The main content area has a title 'Home - Configure - Global Settings - AS/AV'. Below it, a note says: 'Note: Settings only apply to servers that have the appropriate service(s) installed and enabled. Settings applied to servers, domains and classes of service override global settings.' A yellow warning box contains the text: '⚠ Note: Changes to settings require amavisd restart in order to take effect.' Underneath, there are three input fields: 'Kill percent:' with the value '75', 'Tag percent:' with the value '33', and 'Subject prefix:' with an empty input field. At the bottom of the main content area, there's a link 'Antivirus Settings'.

By default, Zimbra uses the Berkeley DB database for spam training. You can also use a MariaDB database.

To use the MariaDB method on the MTA servers:

```
zmlocalconfig -e antispam_mariadb_enabled=TRUE
```

When this is enabled, Berkeley DB database is not enabled.

Training the Spam Filter — The effectiveness of the anti-spam filter is dependent on user input to differentiate spam or ham. The SpamAssassin filter learns from messages that users specifically mark as spam by sending them to their junk folder or not spam by removing them from their junk folder. A copy of these marked messages is sent to the appropriate spam training mailbox.

At installation, a spam/ham cleanup filter is configured on only the first MTA. The ZCS spam training tool, `zmtrainsa`, is configured to automatically retrieve these messages and train the spam filter. The `zmtrainsa` script empties these mailboxes each day.

New installations of ZCS limit spam/ham training to the first MTA installed. If you uninstall or move this MTA, you will need to enable spam/ham training on another MTA, as one host should have this enabled to run `zmtrainsa --cleanup`.



To set this on a new MTA server:

```
zmlocalconfig -e zmtrainsa_cleanup_host=TRUE
```

Initially, you might want to train the spam filter manually to quickly build a database of spam and non-spam tokens, words, or short character sequences that are commonly found in spam or ham. To do this, you can manually forward messages as message/rfc822 attachments to the spam and non-spam mailboxes. When `zmtrainsa` runs, these messages are used to teach the spam filter. Make sure you add a large enough sampling of messages to get accurate scores. To determine whether to mark messages as spam at least 200 known spams and 200 known hams must be identified.

SpamAssassin's `sa-update` tool is included with SpamAssassin. This tool updates SpamAssassin rules from the SA organization. The tool is installed into `/opt/zimbra/common/bin`.

Configuring Final Destination for Spam — You can configure Amavis behavior to handle a spam item's final destination by using the following attribute:

`zimbraAmavisFinalSpamDestiny`

The default is `D_DISCARD` (which will not deliver the email to the addressee).

Setting final spam destiny attributes:

```
zmprov mcf "zimbraAmavisFinalSpamDestiny" D_PASS  
zmprov ms serverhostname.com D_PASS
```

Table 9. Configurable attribute values

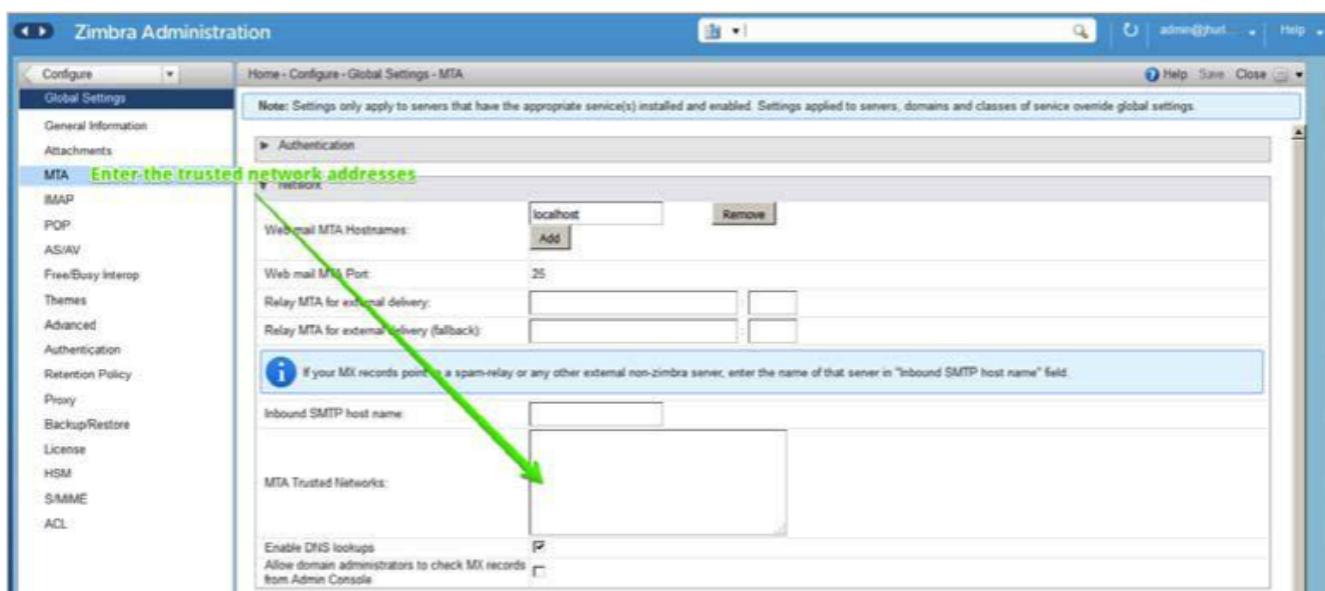
Value	Description
D_PASS	Deliver the email to the recipient. The email is likely to be placed in the recipient's junk folder (although some sites disable junk).
D_BOUNCE	The email is bounced back to the sender. Because this setting can create backscatter—as the "sender" is not the person who actually sent the email—it is not advised.
D_REJECT	Reject the email. This setting reduces the chance of backscatter: <ul style="list-style-type: none"> If the sender is valid, the MTA will notify this person about the rejection. If the sender is not valid, the associated MTA will discard the email (i.e. email that was sent by a spammer spoofing someone else).
D_DISCARD	The email is silently discarded (not delivered).

Setting Up Trusted Networks: The ZCS configuration allows relaying only for the local network, but you can configure trusted networks that are allowed to relay mail. You set the MTA trusted networks as a global setting, but you can configure trusted networks as a server setting. The server setting overrides the global setting.

To use the Administration Console to set up MTA trusted networks as a global setting:

Admin Console:

Home > Configure > Global Settings > MTA → Network



When using the Administration Console to set up MTA trusted networks on a per server basis, first ensure that MTA trusted networks have been set up as global settings.

Admin Console:

Home > Configure > Servers → *server* → MTA → Network

Enter the network addresses separated by *commas* and/or a *space*. Continue long lines by starting the next line with space, similar to the following examples:

127.0.0.0/8, 168.100.189.0/24

127.0.0.0/8 168.100.189.0/24 10.0.0.0/8 [::1]/128 [fe80::%eth0]/64

Enabling a Milter Server: Milter server can be enabled to enforce restrictions on which addresses can send to distribution lists and add **Reply-To** and **X-Zimbra-DL** headers to messages sent from distribution lists. This can be enabled globally or for specific servers from the Administration Console.



Only enable a Milter Server on a server where an MTA is running.

For global configuration, enable the milter server from the Administration Console:

Admin Console:

Home > Configure > Global Settings > MTA → Milter Server

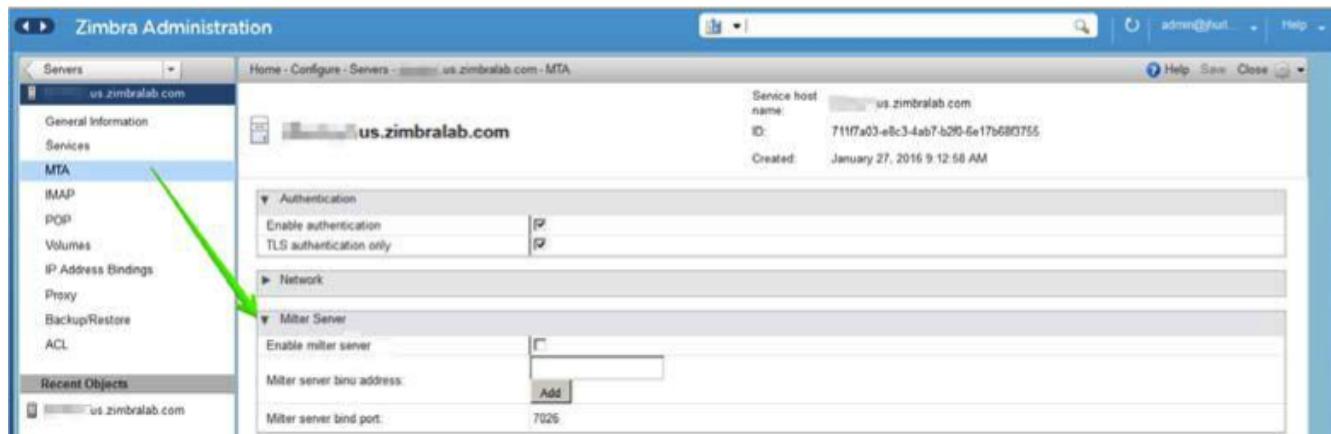
Note: Settings only apply to servers that have the appropriate service(s) installed and enabled. Settings applied to servers, domains and classes of service override global settings.

- ▶ Authentication
- ▶ Network
- ▼ Milter Server
 - Milter server bind port: 7026
 - Enable milter server:
- ▶ Messages
- ▶ Policy Service Checks
- ▶ Protocol checks
- ▶ DNS checks

Use the Administration Console to enable a specific milter server, and to set bind addressing for individual servers.

Admin Console:

Home > Configure > Servers → *server* → MTA → Milter Server



Postscreen Methods for Avoiding Spam

Zimbra Postscreen is the 8.7 enhancement to the Zimbra Collaboration anti-spam strategy, to provide additional protection against mail server overload. By design, Postscreen is not an SMTP proxy. Its purpose is to keep spambots away from Postfix SMTP server processes, while minimizing overhead for legitimate traffic. A single Postscreen process handles multiple inbound SMTP connections and decides which clients may communicate to a Postfix SMTP server process. By keeping spambots away, Postscreen frees up SMTP server processes for legitimate clients, and delays the onset of server overload conditions.

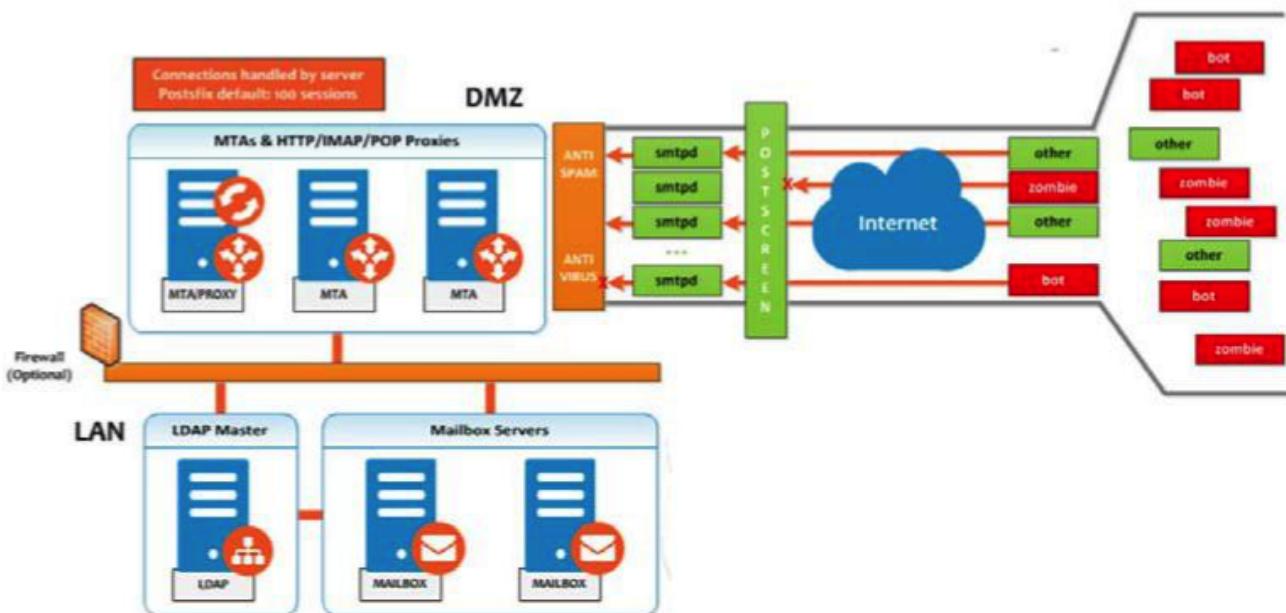
In a typical deployment, Postscreen handles the MX service on TCP port 25, while MUA clients submit mail via the submission service on TCP port 587, which requires client authentication. Alternatively, a site could set up a dedicated, non-Postscreen, “port 25” server that provides submission service and client authentication without MX service.



Postscreen should not be used on SMTP ports that receive mail from end-user clients (MUAs).

Zimbra Collaboration Postscreen maintains a temporary white-list for clients that have passed a number of tests. When an SMTP client IP address is whitelisted, Postscreen immediately passes the connection to a Postfix SMTP server process. This minimizes the overhead for legitimate mail.

In a typical scenario that uses Postscreen service, it is reasonable to expect potentially malicious email entities—such as bots and zombies—to be mixed in with friendly candidates in email loads. This concept is illustrated in the following diagram, in which undesirable entities are depicted in red; good email candidates are green.



Postscreen performs basic checks and denies connection(s) that are clearly from a bot or zombie. If the connection is not in the temporary whitelist, Postscreen passes the email to the local Anti-SPAM and Anti-Virus engines, which can either accept it or deny it. Good connections are accepted via Postscreen security, then allowed to talk directly with the SMTP daemon, which scans the Email (as usual) with the AS/AV. By default, all bots or zombies are rejected.

Use Zimbra CLI attributes to set parameters for Postscreen operations. For any [Postscreen Attributes](#) that provide the ignore, enforce, or drop instruction, use guidelines as follows:

- *ignore* — Ignore this result. Allow other tests to complete. Repeat this test with subsequent client connections. This is the default setting, which is useful for testing and collecting statistics without blocking mail.
- *enforce* — Allow other tests to complete. Reject attempts to deliver mail with a 550 SMTP reply, and log the hello/sender/recipient information. Repeat this test with subsequent client connections.
- *drop* — Drop the connection immediately with a 521 SMTP reply. Repeat this test with subsequent client connections.

Postscreen Attributes:

Go to the `zmprov mcf` prompt (release 8.7+) to use Postscreen commands. You can see example usages of these attributes in [Enabling Postscreen](#).

- `zimbraMtaPostscreenAccessList` — Default = permit_my networks

Postconf `postscreen_access_list` setting, which is the permanent white/ blacklist for remote SMTP client IP addresses. Postscreen(8) searches this list immediately after a remote SMTP client connects. Specify a comma- or whitespace -separated list of commands (in upper or lower case) or lookup tables. The search stops upon the first command that fires for the client IP address.

- `zimbraMtaPostscreenBareNewlineAction` — Default = ignore

The action that postscreen(8) is to take when a remote SMTP client sends a bare newline character, that is, a newline not preceded by carriage return—as either ignore, enforce, or drop.

- **zimbraMtaPostscreenBareNewlineEnable** — Default = no

Enable (yes) or disable (no) “bare newline” SMTP protocol tests in the postscreen(8) server. These tests are expensive: a remote SMTP client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

- **zimbraMtaPostscreenBareNewlineTTL** — Default = 30d

The amount of time allowable for postscreen(8) to use the result of a successful “bare newline” SMTP protocol test. During this time, the client IP address is excluded from this test. The default setting is lengthy because a remote SMTP client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

- **zimbraMtaPostscreenBlacklistAction** — Default = ignore

The action that postscreen(8) is to take when a remote SMTP client is permanently blacklisted with the **postscreen_access_list** parameter, as either ignore, enforce, or drop.

- **zimbraMtaPostscreenCacheCleanupInterval** — Default = 12h

The amount of time allowable between postscreen(8) cache cleanup runs. Cache cleanup increases the load on the cache database and should therefore not be run frequently. This feature requires that the cache database supports the “delete” and “sequence” operators. Specify a zero interval to disable cache cleanup.

After each cache cleanup run, the postscreen(8) daemon logs the number of entries that were retained and dropped. A cleanup run is logged as “partial” when the daemon terminates early after **postfix reload**, **postfix stop**, or no requests for **\$max_idle** seconds.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

- **zimbraMtaPostscreenCacheRetentionTime** — Default = 7d

The amount of time that postscreen(8) is allowed to cache an expired temporary whitelist entry before it is removed. This prevents clients from being logged as “NEW” just because their cache entry expired an hour ago. It also prevents the cache from filling up with clients that passed some deep protocol test once and never came back.

Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

- **zimbraMtaPostscreenCommandCountLimit** — Default = 20

Value to set the limit on the total number of commands per SMTP session for postscreen(8)'s built-in SMTP protocol engine. This SMTP engine defers or rejects all attempts to deliver mail,

therefore there is no need to enforce separate limits on the number of junk commands and error commands.

- **zimbraMtaPostscreenDnsblAction** — Default = ignore

The action that postscreen(8) is to take when a remote SMTP client's combined DNSBL score is equal to or greater than a threshold (as defined with the `postscreen_dnsbl_sites` and `postscreen_dnsbl_threshold` parameters), as either ignore, enforce, or drop.

- **zimbraMtaPostscreenDnsblSites**

Optional list of DNS white/blacklist domains, filters and weight factors. When the list is non-empty, the dnsblog(8) daemon will query these domains with the IP addresses of remote SMTP clients, and postscreen(8) will update an SMTP client's DNSBL score with each non-error reply.



When postscreen rejects mail, it replies with the DNSBL domain name. Use the `postscreen_dnsbl_reply_map` feature to hide “password” information in DNSBL domain names.

When a client's score is equal to or greater than the threshold specified with `postscreen_dnsbl_threshold`, postscreen(8) can drop the connection with the remote SMTP client.

Specify a list of `domain=filter*weight` entries, separated by comma or whitespace.

- When no `=filter` is specified, postscreen(8) will use any non-error DNSBL reply. Otherwise, postscreen(8) uses only DNSBL replies that match the filter. The filter has the form `d.d.d.d`, where each d is a number, or a pattern inside `[]` that contains one or more “;”-separated numbers or number..number ranges.
- When no `*weight` is specified, postscreen(8) increments the remote SMTP client's DNSBL score by 1. Otherwise, the weight must be an integral number, and postscreen(8) adds the specified weight to the remote SMTP client's DNSBL score. Specify a negative number for whitelisting.
- When one `postscreen_dnsbl_sites` entry produces multiple DNSBL responses, postscreen(8) applies the weight at most once.

Examples:

To use example.com as a high-confidence blocklist, and to block mail with example.net and example.org only when both agree:

```
postscreen_dnsbl_threshold = 2
postscreen_dnsbl_sites = example.com*2, example.net, example.org
```

To filter only DNSBL replies containing 127.0.0.4:

```
postscreen_dnsbl_sites = example.com=127.0.0.4
```

- **zimbraMtaPostscreenDnsblThreshold** — Default = 1

Value to define the inclusive lower bound for blocking a remote SMTP client, based on its combined DNSBL score as defined with the `postscreen_dnsbl_sites` parameter.

- **zimbraMtaPostscreenDnsblTTL** — Default = 1h

The amount of time allowable for `postscreen(8)` to use the result from a successful DNS-based reputation test before a client IP address is required to pass that test again.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

- **zimbraMtaPostscreenDnsblWhitelistThreshold** — Default = 0

Allow a remote SMTP client to skip “before” and “after 220 greeting” protocol tests, based on its combined DNSBL score as defined with the `postscreen_dnsbl_sites` parameter.

Specify a negative value to enable this feature. When a client passes the `postscreen_dnsbl_whitelist_threshold` without having failed other tests, all pending or disabled tests are flagged as completed with a time-to-live value equal to `postscreen_dnsbl_ttl`. When a test was already completed, its time-to-live value is updated if it was less than `postscreen_dnsbl_ttl`.

- **zimbraMtaPostscreenGreetAction** — Default = ignore

The action that `postscreen(8)` is to take when a remote SMTP client speaks before its turn within the time specified with the `postscreen_greet_wait` parameter, as either ignore, enforce, or drop.

- **zimbraMtaPostscreenGreetTTL** — Default = 1d

The amount of time allowed for `postscreen(8)` to use the result from a successful PREGREET test. During this time, the client IP address is excluded from this test. The default is relatively short, because a good client can immediately talk to a real Postfix SMTP server.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

- **zimbraMtaPostscreenNonSmtplibCommandAction** — Default = drop

The action that `postscreen(8)` takes when a remote SMTP client sends non-SMTP commands as specified with the `postscreen_forbidden_commands` parameter, as either ignore, enforce, or drop.

- **zimbraMtaPostscreenNonSmtplibCommandEnable** — Default = no

Enable (yes) or disable (no) "non- SMTP command" tests in the `postscreen(8)` server. These tests are expensive: a client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

- **zimbraMtaPostscreenNonSmtplibCommandTTL** — Default = 30d

The amount of time allowable for postscreen(8) to use the result from a successful “non_smtp_command” SMTP protocol test. During this time, the client IP address is excluded from this test. The default is long because a client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

- **zimbraMtaPostscreenPipeliningAction** — Default = enforce

The action that postscreen(8) is to take when a remote SMTP client sends multiple commands instead of sending one command and waiting for the server to respond, as either ignore, enforce, or drop.

- **zimbraMtaPostscreenPipeliningEnable** — Default = no

Enable (yes) or disable (no) “pipelining” SMTP protocol tests in the postscreen(8) server. These tests are expensive: a good client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

- **zimbraMtaPostscreenPipeliningTTL** — Default = 30d

Time allowable for postscreen(8) to use the result from a successful “pipelining” SMTP protocol test. During this time, the client IP address is excluded from this test. The default is lengthy because a good client must disconnect after it passes the test, before it can talk to a real Postfix SMTP server.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

- **zimbraMtaPostscreenWatchdogTimeout** — Default = 10s

Time allowable for a postscreen(8) process to respond to a remote SMTP client command, or to perform a cache operation, before it is terminated by a built-in watchdog timer. This is a safety mechanism that prevents postscreen(8) from becoming non-responsive due to a bug in Postfix itself or in system software. To avoid false alarms and unnecessary cache corruption this limit cannot be set under 10s.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

- **zimbraMtaPostscreenWhitelistInterfaces**

A list of local postscreen(8) server IP addresses where a non-whitelisted remote SMTP client can obtain postscreen(8)'s temporary whitelist status. This status is required before the client can talk to a Postfix SMTP server process. By default, a client can obtain postscreen(8)'s whitelist status on any local postscreen(8) server IP address.

When postscreen(8) listens on both primary and backup MX addresses, the **postscreen_whitelist_interfaces** parameter can be configured to give the temporary whitelist status only when a client connects to a primary MX address. Once a client is whitelisted it can

talk to a Postfix SMTP server on any address. Thus, clients that connect only to backup MX addresses will never become whitelisted, and will never be allowed to talk to a Postfix SMTP server process.

Specify a list of network addresses or network/netmask patterns, separated by commas and/or whitespace. The netmask specifies the number of bits in the network part of a host address. Continue long lines by starting the next line with whitespace.

You can also specify `/file/name` or `type:table` patterns. A `/file/name` pattern is replaced by its contents; a `type:table` lookup table is matched when a table entry matches a lookup string (the lookup result is ignored).

The list is matched left to right, and the search stops on the first match. Specify `!pattern` to exclude an address or network block from the list.



IPv6 address information must be specified inside `[]` in the `postscreen_whitelist_interfaces` value, and in files specified with `/file/name`. IP version 6 addresses contain the ":" character, and would otherwise be confused with a `type:table` pattern.

Example:

```
/etc/postfix/main.cf:  
  
# Don't whitelist connections to the backup IP address.  
postscreen_whitelist_interfaces = !168.100.189.8, static:all
```

- `zimbraMtaPostscreenDnsblMinTTL` — Default = 60s

The minimum amount of time that `postscreen(8)` is allowed—resulting from a successful DNS-based reputation test—before a client IP address is required to pass that test again. If the DNS reply specifies a larger TTL value, that value will be used unless it would be larger than `postscreen_dnsbl_max_ttl`.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

- `zimbraMtaPostscreenDnsblMaxTTL` — Default = `postscreen dnsbl ttl`

The maximum amount of time allowable for `postscreen(8)` to use the result from a successful DNS-based reputation test before a client IP address is required to pass that test again. If the DNS reply specifies a shorter TTL value, that value will be used unless it would be smaller than `postscreen_dnsbl_min_ttl`.

Specify a non-zero time value (an integral value plus an optional one-letter suffix that specifies the time unit). Time units: s (seconds), m (minutes), h (hours), d (days), w (weeks).

Note that the default setting is backwards-compatible with Postscreen versions earlier than 3.1.

Enabling Postscreen:

The example in this section demonstrates settings appropriate for a global configuration with medium-to-high level Postscreen protection.

Example 4. Global Configuration for Postscreen

```
zmprov mcf zimbraMtaPostscreenAccessList permit_mynetworks
zmprov mcf zimbraMtaPostscreenBareNewlineAction ignore
zmprov mcf zimbraMtaPostscreenBareNewlineEnable no
zmprov mcf zimbraMtaPostscreenBareNewlineTTL 30d
zmprov mcf zimbraMtaPostscreenBlacklistAction ignore
zmprov mcf zimbraMtaPostscreenCacheCleanupInterval 12h
zmprov mcf zimbraMtaPostscreenCacheRetentionTime 7d
zmprov mcf zimbraMtaPostscreenCommandCountLimit 20
zmprov mcf zimbraMtaPostscreenDnsblAction enforce
zmprov mcf \
    zimbraMtaPostscreenDnsblSites 'b.barracudacentral.org=127.0.0.2_7' \
    zimbraMtaPostscreenDnsblSites 'dnsbl.inps.de=127.0.0.2*7' \
    zimbraMtaPostscreenDnsblSites 'zen.spamhaus.org=127.0.0.[10;11]*8' \
    zimbraMtaPostscreenDnsblSites 'zen.spamhaus.org=127.0.0.[4..7]*6' \
    zimbraMtaPostscreenDnsblSites 'zen.spamhaus.org=127.0.0.3*4' \
    zimbraMtaPostscreenDnsblSites 'zen.spamhaus.org=127.0.0.2*3' \
    zimbraMtaPostscreenDnsblSites 'list.dnswl.org=127.0.[0..255].0*-2' \
    zimbraMtaPostscreenDnsblSites 'list.dnswl.org=127.0.[0..255].1*-3' \
    zimbraMtaPostscreenDnsblSites 'list.dnswl.org=127.0.[0..255].2*-4' \
    zimbraMtaPostscreenDnsblSites 'list.dnswl.org=127.0.[0..255].3*-5' \
    zimbraMtaPostscreenDnsblSites 'bl.mailspike.net=127.0.0.2*5' \
    zimbraMtaPostscreenDnsblSites 'bl.mailspike.net=127.0.0.[10;11;12]*4' \
    zimbraMtaPostscreenDnsblSites 'wl.mailspike.net=127.0.0.[18;19;20]*-2' \
    zimbraMtaPostscreenDnsblSites 'dnsbl.sorbs.net=127.0.0.10*8' \
    zimbraMtaPostscreenDnsblSites 'dnsbl.sorbs.net=127.0.0.5*6' \
    zimbraMtaPostscreenDnsblSites 'dnsbl.sorbs.net=127.0.0.7*3' \
    zimbraMtaPostscreenDnsblSites 'dnsbl.sorbs.net=127.0.0.8*2' \
    zimbraMtaPostscreenDnsblSites 'dnsbl.sorbs.net=127.0.0.6*2' \
    zimbraMtaPostscreenDnsblSites 'dnsbl.sorbs.net=127.0.0.9*2'
zmprov mcf zimbraMtaPostscreenDnsblTTL 5m
zmprov mcf zimbraMtaPostscreenDnsblThreshold 8
zmprov mcf zimbraMtaPostscreenDnsblTimeout 10s
zmprov mcf zimbraMtaPostscreenDnsblWhitelistThreshold 0
zmprov mcf zimbraMtaPostscreenGreetAction enforce
zmprov mcf zimbraMtaPostscreenGreetTTL 1d
zmprov mcf zimbraMtaPostscreenNonSmtplibCommandAction drop
zmprov mcf zimbraMtaPostscreenNonSmtplibCommandEnable no
zmprov mcf zimbraMtaPostscreenNonSmtplibCommandTTL 30d
zmprov mcf zimbraMtaPostscreenPipeliningAction enforce
zmprov mcf zimbraMtaPostscreenPipeliningEnable no
zmprov mcf zimbraMtaPostscreenPipeliningTTL 30d
zmprov mcf zimbraMtaPostscreenWatchdogTimeout 10s
zmprov mcf zimbraMtaPostscreenWhitelistInterfaces static:all
```

Testing Postscreen:

Testing uses Postscreen to view results without taking any action. In a testing scenario, you instruct

Postscreen to log email connections without taking action on them. Once you are satisfied with the results, you can set Postscreen values to enforce or drop emails, as required.

1. Set up the DNS-based Blackhole List (DNSBL).
2. Set Postscreen to ignore.

The following real-world example demonstrates return of a 550 error from Postscreen during a test session:

```
Mar 1 02:03:26 edge01 postfix/postscreen[23154]: DNSBL rank 28 for [112.90.37.251]:20438
Mar 1 02:03:26 edge01 postfix/postscreen[23154]: CONNECT from [10.210.0.161]:58010 to [10.210.0.174]:25
Mar 1 02:03:26 edge01 postfix/postscreen[23154]: WHITELISTED [10.210.0.161]:58010
Mar 1 02:03:27 edge01 postfix/postscreen[23154]: NOQUEUE: reject: RCPT from [112.90.37.251]:20438: 550 5.7.1 Service unavailable; client [112.90.37.251] blocked using zen.spamhaus.org; from=<hfxgdsgfvfg@gmail.com>, to=<support@zimbra.com>, proto=ESMTP, helo=<gmail.com>
Mar 1 02:03:27 edge01 postfix/postscreen[23154]: DISCONNECT [112.90.37.251]:20438
```

Receiving and Sending Mail

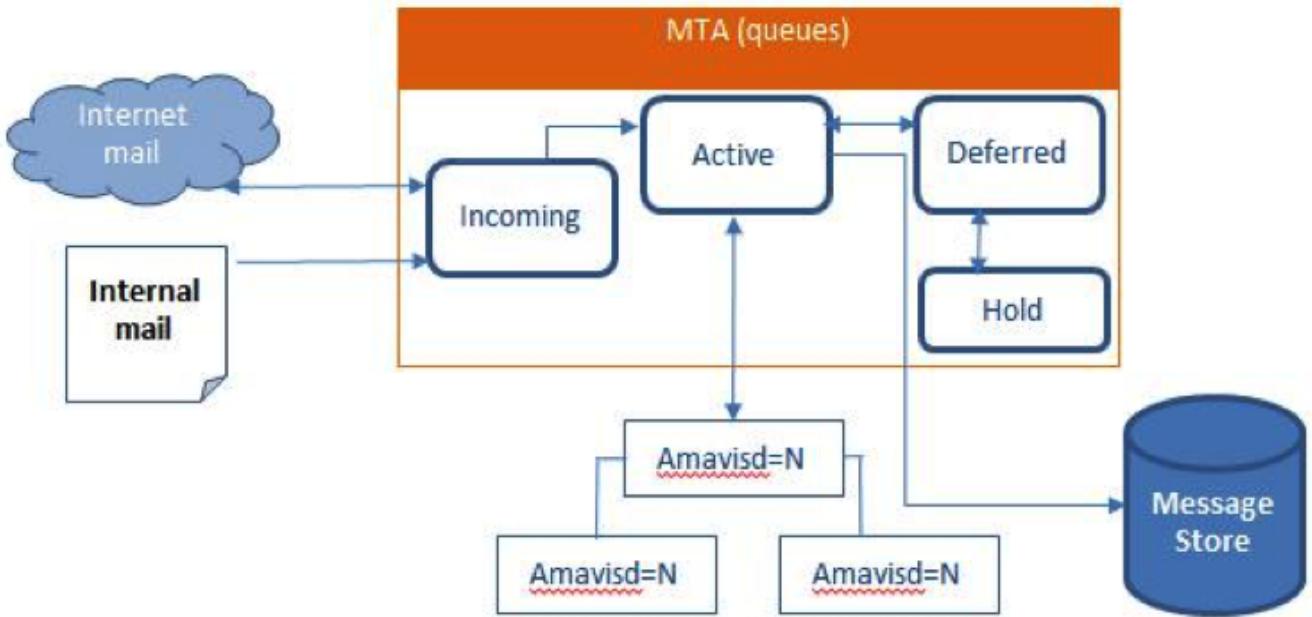
The Zimbra MTA delivers the incoming and the outgoing mail messages. For outgoing mail, the Zimbra MTA determines the destination of the recipient address. If the destination host is local, the message is passed to the Zimbra server for delivery. If the destination host is a remote mail server, the Zimbra MTA must establish a communication method to transfer the message to the remote host. For incoming messages, the MTA must be able to accept connection requests from remote mail servers and receive messages for the local users.

To send and receive email, the MTA must be configured in DNS with both an A record and an MX Record. For sending mail, the MTA uses DNS to resolve hostnames and email-routing information. To receive mail, the MX record must be configured correctly to route messages to the mail server.

You must configure a relay host if you do not enable DNS.

Message Queues

When the Zimbra MTA receives mail, it routes the mail through a series of queues to manage delivery; incoming, active, deferred, hold, and corrupt.



The **incoming** message queue holds the new mail that has been received. Each message is identified with a unique file name. Messages are moved to the active queue when there is room. If there are no problems, message move through this queue very quickly.

The **active** message queue holds messages that are ready to be sent. The MTA sets a limit to the number of messages that can be in the active queue at any one time. From here, messages are moved to and from the anti-virus and anti-spam filters before being delivered to another queue.

Messages that cannot be delivered are placed in the **deferred** queue. The reasons for the delivery failures are documented in a file in the deferred queue. This queue is scanned frequently to resend the message. If the message cannot be sent after the set number of delivery attempts, the message fails and is bounced back to the original sender. You can choose to send a notification to the sender that the message has been deferred.

The **hold** message queue keeps mail that could not be processed. Messages stay in this queue until the administrator moves them. No periodic delivery attempts are made for messages in the hold queue.

The **corrupt** queue stores damaged unreadable messages.

You can monitor the mail queues for delivery problems from the Administration Console. See [Monitoring ZCS Servers](#).

Zimbra Proxy Server

Zimbra Proxy is a high-performance proxy server that can be configured as a POP3/IMAP/HTTP proxy used to reverse proxy IMAP/POP3 and HTTP client requests to a set of backend servers.

The Zimbra Proxy package is installed and configured during the Zimbra Collaboration installation. You can install this package on a mailbox server, MTA server, or on its own independent server. When the Zimbra Proxy package is installed, the proxy feature is enabled. In most cases, no modification is necessary.

Benefits of Using Zimbra Proxy

Benefits for using Zimbra Proxy include:

- Zimbra proxy centralizes access to Mailbox servers
- Load Balancing
- Security
- Authentication
- SSL Termination
- Caching
- Centralized Logging and Auditing
- URL Rewriting
- Strict Server Name Enforcement (optional)

For more information, see the wiki page [Zimbra_Proxy_Guide](#).

Zimbra Proxy Components

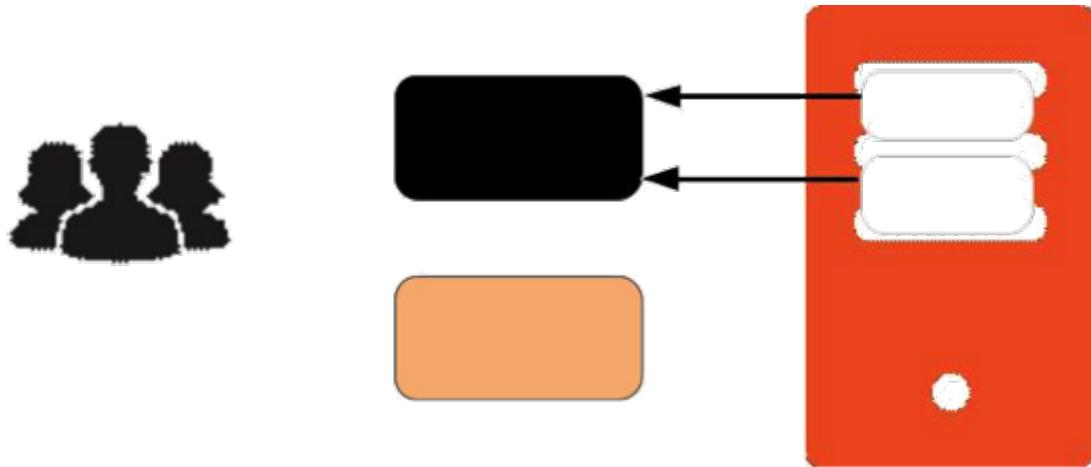
Zimbra Proxy is designed to provide a HTTP/POP/IMAP proxy that is quick, reliable, and scalable. Zimbra Proxy includes the following:

Component	Description
Nginx	High performance HTTP/IMAP/POP3 proxy server that handles all incoming HTTP/POP/IMAP requests.
Memcached	High performance distributed memory object caching system in which routing information is cached to enable increased performance.
Zimbra Proxy Route Lookup Handler	Servelet—located on the ZCS mailbox server—that handles queries for the user account route information. This routing information consists of the server and port number where the user account resides.

Proxy Architecture and Flow

This section describes the architecture and flow sequence of Zimbra proxy.

1. End clients connect to Zimbra Proxy using HTTP/HTTPS/POP/IMAP ports.
2. When Zimbra Collaboration Proxy receives an incoming connection, the Nginx component sends an HTTP request to Zimbra Collaboration Proxy Route Lookup Handler component.



3. Zimbra Collaboration Proxy Route Lookup Handler locates the route information for the account being accessed and returns this to Nginx.
4. The Memcached component stores the route information for the configured period of time (the default is one hour). Nginx uses this route information instead of querying the Zimbra Collaboration Proxy Route Lookup Handler until the default period of time has expired.
5. Nginx uses the route information to connect to Zimbra Collaboration Mailbox.
6. Zimbra Collaboration Proxy connects to Zimbra Collaboration Mailbox and initiates the web/mail proxy session. The end client behaves as if it is connecting directly to Zimbra Collaboration Mailbox.

Changing the Zimbra Proxy Configuration

When Zimbra proxy is configured, the Zimbra proxy config performs keyword substitution as necessary with values from the LDAP configuration and localconfig.

If changes are required after the Zimbra Proxy is set up, modify the Zimbra LDAP attributes or localconfig values and run zmconfigd to generate the updated Zimbra Proxy configuration. The Zimbra proxy configuration file is in </opt/zimbra/conf/nginx.conf>. The nginx.conf includes the main config, memcache config, mail config, and web config files.

Common changes to Zimbra Proxy configuration are IMAP/POP configuration changes from the original default setup

- HTTP reverse proxy configuration changes from the original default setup
- GSSAPI authentication for Kerberos. In this case you manually identify the location of the Kerberos Keytab file, including Zimbra Proxy password

Zimbra Proxy

Zimbra Proxy allows end users to access their Zimbra Collaboration account using clients such as Microsoft Outlook, Mozilla Thunderbird, or other POP/IMAP end-client software. End users can connect using POP3, IMAP, POP3S (Secure POP3), or IMAPS (Secure IMAP).

For example, proxying allows users to enter `imap.example.com` as their IMAP server. The proxy running on `imap.example.com` inspects their IMAP traffic, does a lookup to determine which backend mailbox server a user's mailbox lives on and transparently proxies the connection from user's IMAP client to the correct mailbox server.

Zimbra Proxy Ports

The following ports are used either by Zimbra Proxy or by Zimbra Mailbox (if Proxy is not configured). If you have any other services running on these ports, turn them off.

End clients connect directly to Zimbra Proxy, using the Zimbra Proxy Ports. Zimbra Proxy connects to the Route Lookup Handler or Zimbra Mailbox using the Zimbra Mailbox Ports.

Table 10. Proxy Ports

Zimbra Proxy Ports (External to ZCS)	Port
HTTP	80
HTTPS	443
POP3	110
POP3S (Secure POP3)	995
IMAP	143
IMAPS (Secure IMAP)	993
Zimbra Mailbox Ports (Internal to ZCS)	Port
Route Lookup Handler	7072
HTTP Backend (if Proxy configured)	8080
HTTPS Backend (if Proxy configured)	8443
POP3 Backend (if Proxy configured)	7110
POP3S Backend (if Proxy configured)	7995
IMAP Backend (if Proxy configured)	7143
IMAPS Backend (if Proxy configured)	7993

Strict Server Name Enforcement

Zimbra Proxy has the ability to strictly enforce which values are allowed in the `Host` header passed in by the client.

This is *enabled by default* on **new installations** but left *disabled* for **upgrades** from previous versions unless toggled during the installation.

The functionality may be altered by setting the `zimbraReverseProxyStrictServerNameEnabled` boolean configuration option followed by restarting the proxy server.

- TRUE - strict server name enforcement enabled
- FALSE - strict server name enforcement disabled

```
zmprov mcf zimbraReverseProxyStrictServerNameEnabled TRUE
```

When the strict server name functionality is enabled, additional valid server names may be specified using the `zimbraVirtualHostName` and `zimbraVirtualIPAddress` configuration items at the domain level.

```
zmprov md example.com zimbraVirtualHostName mail.example.com zimbraVirtualIPAddress  
1.2.3.4
```



Only one virtual ip address is needed per domain although more than one is acceptable.

Setting Up IMAP and POP Proxy After HTTP Proxy Installation

IMAP proxy is installed with Zimbra Collaboration and set up during installation from the configuration menus. To set up the HTTP proxy, . proxy must be installed on the identified proxy nodes in order to set up HTTP proxy. No other configuration is usually required.

If you need to set up IMAP/POP proxy after you have already installed . HTTP proxy, and set up the . mailbox server and the proxy node.



You can run the command as `zmproxyconfig -r`, to run against a remote host. This requires the server to be properly configured in the LDAP master.

Set Up IMAP/POP Proxy with Separate Proxy Node

Use steps in this section if your configuration includes a separate proxy server.

1. On each Zimbra mailbox server that you want to proxy with, enable the proxy for IMAP/POP proxy.

```
/opt/zimbra/libexec/zmproxyconfig -e -m -H mailbox.node.service.hostname
```

This configures the following:

Port Attributes	Setting
<code>zimbraImapBindPort</code>	7143
<code>zimbraImapProxyBindPort</code>	143

Port Attributes	Setting
<code>zimbraImapSSLBindPort</code>	7993
<code>zimbraImapSSLProxyBindPort</code>	993
<code>zimbraPop3BindPort</code>	7110
<code>zimbraPop3ProxyBindPort</code>	110
<code>zimbraPop3SSLBindPort</code>	7995
<code>zimbraPop3SSLProxyBindPort</code>	995
<code>zimbraImapCleartextLoginEnabled</code>	TRUE
<code>zimbraReverseProxyLookupTarget</code>	TRUE
<code>zimbraPop3CleartextLoginEnabled</code>	TRUE

2. Restart services on the proxy and mailbox servers.

```
zmcontrol restart
```

Set Up the Proxy Node

On each proxy node that has the proxy service installed, enable the proxy for the web.

```
/opt/zimbra/libexec/zmproxyconfig -e -m -H proxy.node.service.hostname
```

This configures the following:

Port Attribute	Setting
<code>zimbraImapBindPort</code>	7143
<code>zimbraImapProxyBindPort</code>	143
<code>zimbraImapSSLBindPort</code>	7993
<code>zimbraImapSSLProxyBindPort</code>	993
<code>zimbraPop3BindPort</code>	7110
<code>zimbraPop3ProxyBindPort</code>	110
<code>zimbraPop3SSLBindPort</code>	7995
<code>zimbraPop3SSLProxyBindPort</code>	995
<code>zimbraReverseProxyMailEnabled</code>	TRUE

Set Up a Single Node

Use steps in this section if Zimbra proxy is installed with Zimbra Collaboration on the same server.

1. Enable the proxy for the web.

```
/opt/zimbra/libexec/zmproxyconfig -e -m -H mailbox.node.service.hostname
```

This configures the following:

Port Attribute	Setting
<code>zimbraImapBindPort</code>	7143
<code>zimbraImapProxyBindPort</code>	143
<code>zimbraImapSSLBindPort</code>	7993
<code>zimbraImapSSLProxyBindPort</code>	993
<code>zimbraPop3BindPort</code>	7110
<code>zimbraPop3ProxyBindPort</code>	110
<code>zimbraPop3SSLBindPort</code>	7995
<code>zimbraPop3SSLProxyBindPort</code>	995
<code>zimbraImapCleartextLoginEnabled</code>	TRUE
<code>zimbraReverseProxyLookupTarget</code>	TRUE
<code>zimbraPop3CleartextLoginEnabled</code>	TRUE
<code>zimbraReverseProxyMailEnabled</code>	TRUE

2. Restart services on the proxy and mailbox servers.

```
zmcontrol restart
```

Configuring Zimbra HTTP Proxy

Zimbra Proxy can also reverse proxy HTTP requests to the right back-end server.

For example, users can use a web browser to connect to the proxy server at <https://mail.example.com>. The connection from users whose mailboxes live on mbs1.example.com is proxied to mbs1.example.com by the proxy running on the mail.example.com server. REST and CalDAV clients, Zimbra Connector for Outlook, and Zimbra Mobile Sync NG devices are also supported by the proxy.

HTTP reverse proxy routes requests as follows:

- If the requesting URL can be examined to determine the user name, then the request is routed to the backend mailbox server of the user in the URL. REST, CalDAV, and Zimbra Mobile Sync are supported through this mechanism.
- If the request has an auth token cookie (`ZM_AUTH_TOKEN`), the request is routed to the backend mailbox server of the authenticated user.
- If the above methods do not work, the IP hash method is used to load balance the requests

across the backend mailbox servers which are able to handle the request or do any necessary internal proxying.

Setting Up HTTP Proxy

To set up HTTP proxy, Zimbra Proxy must be installed on the identified nodes.



You can run the command as `/opt/zimbra/libexec/zmproxyconfig -r`, to run against a remote host. Note that this requires the server to be properly configured in the LDAP master.

Setting Up HTTP Proxy as a Separate Proxy Node

Use steps in this section if your configuration includes a separate proxy server.

1. On each Zimbra mailbox server that you want to proxy with, enable the proxy for the web.

```
/opt/zimbra/libexec/zmproxyconfig -e -w -H mailbox.node.service.hostname
```

This configures the following:

Attribute	Setting
<code>zimbraMailReferMode</code>	reverse-proxied.
<code>zimbraMailPort</code>	8080 (to avoid port conflicts)
<code>zimbraMailSSLPot</code>	8443 (to avoid port conflicts)
<code>zimbraReverseProxyLookupTarget</code>	TRUE
<code>zimbraMailMode</code>	HTTP

2. Restart services on the proxy and mailbox servers.

```
zmcontrol restart
```

3. Configure each domain with the public service host name to be used for REST URLs, email, and Briefcase folders.

```
zmprov modifyDomain <domain.com> zimbraPublicServiceHostname <hostname.domain.com>
```

Setting Up Proxy Node

On each proxy node that has the proxy service installed, enable the proxy for the web.

```
/opt/zimbra/libexec/zmproxyconfig -e -w -H proxy.node.service.hostname
```

This configures the following:

Attribute	Setting
zimbraMailReferMode	reverse-proxied. To set the proxy server mail mode, add the -x option to the command, with the specific mode as either http, https, both, redirect, or mixed.
zimbraMailProxyPort	80 (to avoid port conflicts).
zimbraMailSSLProxyPort	443 (to avoid port conflicts).
zimbraReverseProxyHttpEnabled	TRUE (to indicate that Web proxy is enabled).
zimbraReverseProxyMailMode	HTTP (default)

To set the proxy server mail mode, add the **-x** option to the command with the specific mode: **http, https, both, redirect, mixed**.

Setting Up a Single Node for HTTP Proxy

Use steps in this section if Zimbra proxy is installed along with ZCS on the same server.

1. On each zimbra mailbox server that you want to proxy with, enable the proxy for the web.

```
/opt/zimbra/libexec/zmproxyconfig -e -w -H mailbox.node.service.hostname
```

This configures the following:

Attribute	Setting
zimbraMailReferMode	reverse-proxied.
zimbraMailPort	8080 (to avoid port conflicts)
zimbraMailSSLPot	8443 (to avoid port conflicts)
zimbraReverseProxyLookupTarget	TRUE
zimbraMailMode	HTTP (the only supported mode)
zimbraMailProxyPort	80 (to avoid port conflicts)
zimbraMailSSLProxyPort	443 (to avoid port conflicts)
zimbraReverseProxyHttpEnabled	TRUE (to indicate that Web proxy is enabled)
zimbraReverseProxyMailMode	HTTP (default)

To set the proxy server mail mode, add the **-x** option to the command with the specific mode: **http, https, both, redirect, mixed**.

2. Restart services on the proxy and mailbox servers.

```
zmcontrol restart
```

Configure each domain with the public service host name to be used for REST URLs, email and Briefcase folders.

```
zmprov modifyDomain <domain.com> zimbraPublicServiceHostname <hostname.domain.com>
```

Set Up Proxy to use Clear Text for Upstream Connections

When setting up the proxy to use clear text for upstream connections, set `zimbraReverseProxySSLToUpstreamEnabled` to FALSE.

This attribute defaults to TRUE. In an "out of the box" proxy set up, the upstream communication defaults to SSL.

REST URL Generation

For REST URL, you set the host name, service protocol, and services port globally or for a specific domain from the following attributes.

- `zimbraPublicServiceHostname`
- `zimbraPublicServiceProtocol`
- `zimbraPublicServicePort`

When generating REST URL's:

- If `domain.zimbraPublicServiceHostname` is set, use `zimbraPublicServiceProtocol + zimbraPublicServiceHostname + zimbraPublicServicePort`
- Otherwise it falls back to the server (account's home server) attributes:
 - protocol is computed from `server.zimbraMailMode`
 - hostname is `server.zimbraServiceHostname`
- port is computed from the protocol.

 About using `zimbraMailReferMode` - In earlier versions, a local config variable — `zimbra_auth_always_send_refer` — determined which action the back-end server took when a user's mailbox did not reside on the server that the user logged in to. The default value of FALSE redirected the user if the user was logging in on the incorrect backend host.

On a multiserver ZCS, if a load balanced name was needed to create a friendly landing page, a user would always have to be redirected. In that case, `zimbra_auth_always_send_refer` was set to TRUE.

Now with a full-fledged reverse proxy, users do not need to be redirected. The localconfig variable `zimbraMailReferMode` is used with nginx reverse proxy.

Setting Proxy Trusted IP Addresses

When a proxy is configured with ZCS, each proxy server's IP address must be configured in LDAP

attribute `zimbraMailTrustedIP` to identify the proxy addresses as trusted when users log in through the proxy. The proxy IP address is added to the `X-Forwarded-For` header information. The `X-Forwarded-For` header is automatically added to the localconfig `zimbra_http_originating_ip` header attribute. When a user logs in, this IP address and the user's address are verified in the Zimbra mailbox log.

Set each proxy IP address in the attribute. For example, if you have two proxy servers:

```
zmprov mcf +zimbraMailTrustedIP {IP of nginx-1} +zimbraMailTrustedIP {IP of nginx-2}
```

To verify that `X-Forwarded-For` was correctly added to the localconfig, type

```
zmlocalconfig | grep -i http
```



You should see

```
zimbra_http_originating_ip_header = X-Forwarded-For
```

Configuring Zimbra Proxy for Kerberos Authentication

Use steps in this section if you use the Kerberos5 authenticating mechanism, and want to configure it for the IMAP and POP proxy.

 Make sure that your Kerberos5 authentication mechanism is correctly configured.

See [Zimbra LDAP Service](#)

1. On each proxy node, set the `zimbraReverseProxyDefaultRealm` server attribute to the realm name corresponding to the proxy server. For example:

```
zmprov ms [DNS name.isp.net] zimbraReverseProxyDefaultRealm [ISP.NET]
```

2. Each proxy IP address where email clients connect must be configured for GSSAPI authentication by the mail server. On each proxy node for each of the proxy IP addresses:

```
zmprov mcf +zimbraReverseProxyAdminIPAddress [IP address]
```

3. On each proxy server:

```
zmprov ms [proxyexample.net] zimbraReverseProxyImapSaslGssapiEnabled TRUE
```

```
zmprov ms proxyl.isp.net zimbraReverseProxyPop3SaslGssapiEnabled TRUE
```

4. Restart the proxy server

```
zmproxyctl restart
```

Zimbra Administration Console

The Zimbra Administration Console is a browser-based user interface that allows you to centrally manage Zimbra servers and user accounts.

Administrator Accounts

When you log in to the Administration Console, the tasks you are authorized to perform display on the Navigation pane. These tasks are based on the rights assigned to the administrator role.

Two types of administrator accounts can be created to manage Zimbra Collaboration:

- **Global Administrators** have full privileges to manage servers, global settings, domains, and accounts as well as create other administrators. One global administrator account is created when the software is installed. Additional global administrator accounts can be created. You can perform administration tasks from the Administration Console or the command line.
- **Delegated Administrators** are granted customized administrator roles by the global administrator to manage different tasks from the Administration Console. See also [Delegated Administration](#) for more details.

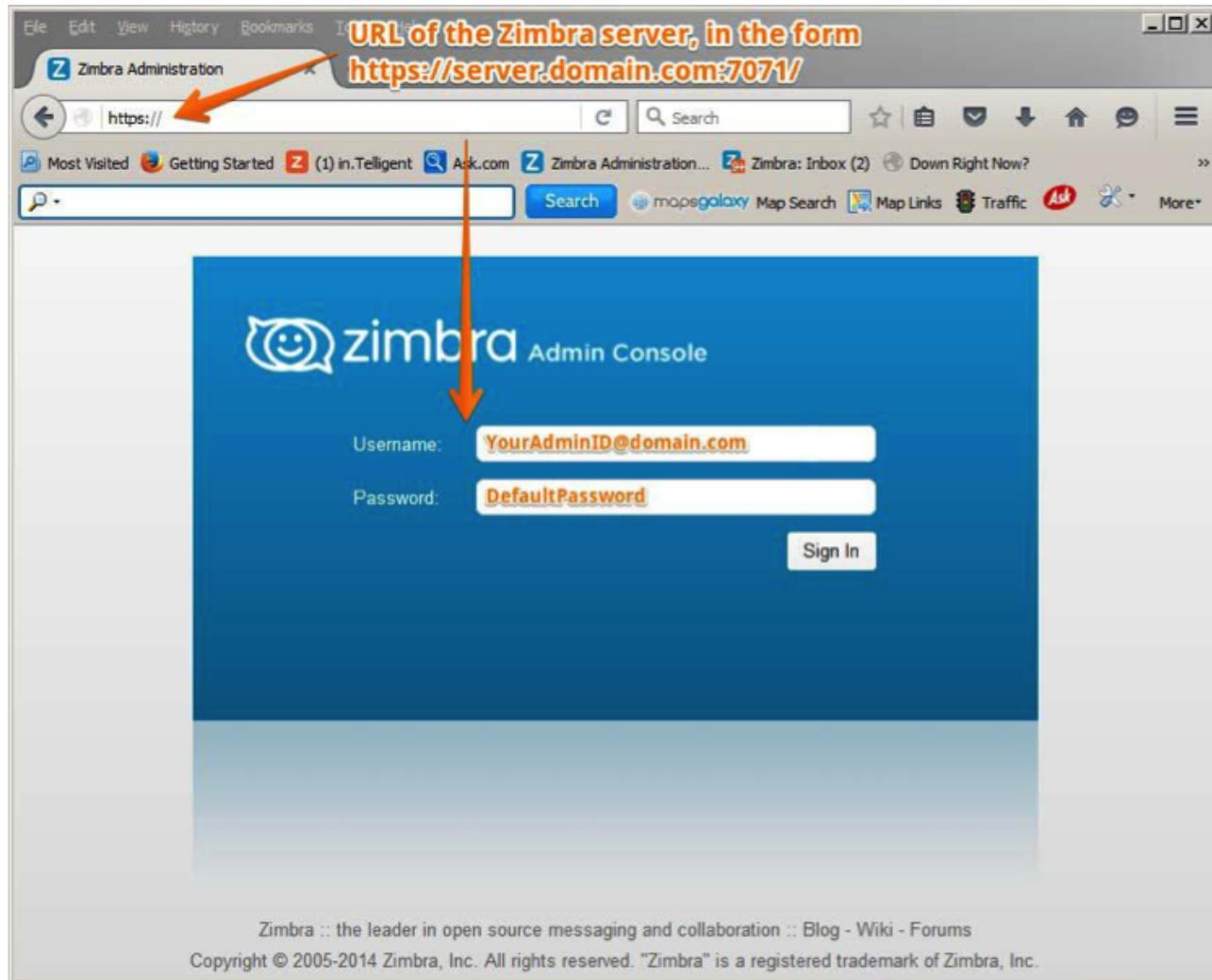
Logging into the Administration Console

1. To launch the Administration Console in a typical installation, use the following URL pattern.

<https://server.domain.com:7071/>

Parameter	Description
server.domain.com	The Zimbra server name or IP address.
7071	The default HTTP listen port.

2. At the login screen, enter the complete administrator address - as **admin@domain.com** - and the password that was configured during server installation of Zimbra Collaboration.



Modifying Administrator Passwords

You can change the password - from either the Administration Console or the CLI - at any time.

From the Administration Console, use the **Change Password** screen to set the new password string, and to define the policy for user password modifications.

Admin Console:

Home > Manage > Accounts

Double click select *user account* or from the **Gear** icon, select **Change Password** from the popup menu.

The dialog box is titled "Change Password (admin@jhurley1.us.zimbralab.com)". It contains two input fields: "Password" and "Confirm password". Below these fields is a checkbox labeled "Must change password". At the bottom of the dialog are three buttons: "Help", "Cancel", and "OK".

```
zmprov sp adminname@domain.com password
```

Customizing the Login and Logout Pages

A different login and logout page can be configured either as a global setting or as a domain setting.

To specify a URL to redirect administrators if their login is not authenticated, or if authentication has expired:

Global:

```
zmprov mcf zimbraAdminConsoleLoginURL <https://example.com>
```

Domain:

```
zmprov md <domain> zimbraAdminConsoleLoginURL <https://example.com>
```

To specify a URL to redirect administrators, for logging out:

Global:

```
zmprov mcf zimbraAdminConsoleLogoutURL <https://example.com>
```

Domain:

```
zmprov md <domain> zimbraAdminConsoleLogoutURL <https://example.com>
```

Managing Tasks

Most ZCS tasks - such as creating accounts and Classes of Service, Server Status Monitoring, Domain management, Backup Scheduling, and Session management - can be managed from the Administration Console.

Other configuration and maintenance tasks cannot be handled from the Administration Console - such as starting and stopping services and managing the local server configuration - and require the use of the Zimbra CLI.

At the Administration Console, if you need to view the attribute associated with a particular function, you can click on the text labels of the configuration page currently in view to view the information in a popup. Guide text is also provided from these popups, as demonstrated in the following illustration.

Viewing Attributes at the Administration Console

Click the field label to view the Attribute popup.

General Information

Most results returned by GAL search:	100
Default domain:	jhurley1.us.zimbraLab.com
Maximum number of simultaneous logins:	zimbraDefaultDomainName
Sleep time before:	More
Maximum size of a file uploaded from the desktop (KB):	10240
Admin help URL:	
Delegated admin help URL:	

With the attribute popup in view, click **More** to view guidetext about the field.

General Information

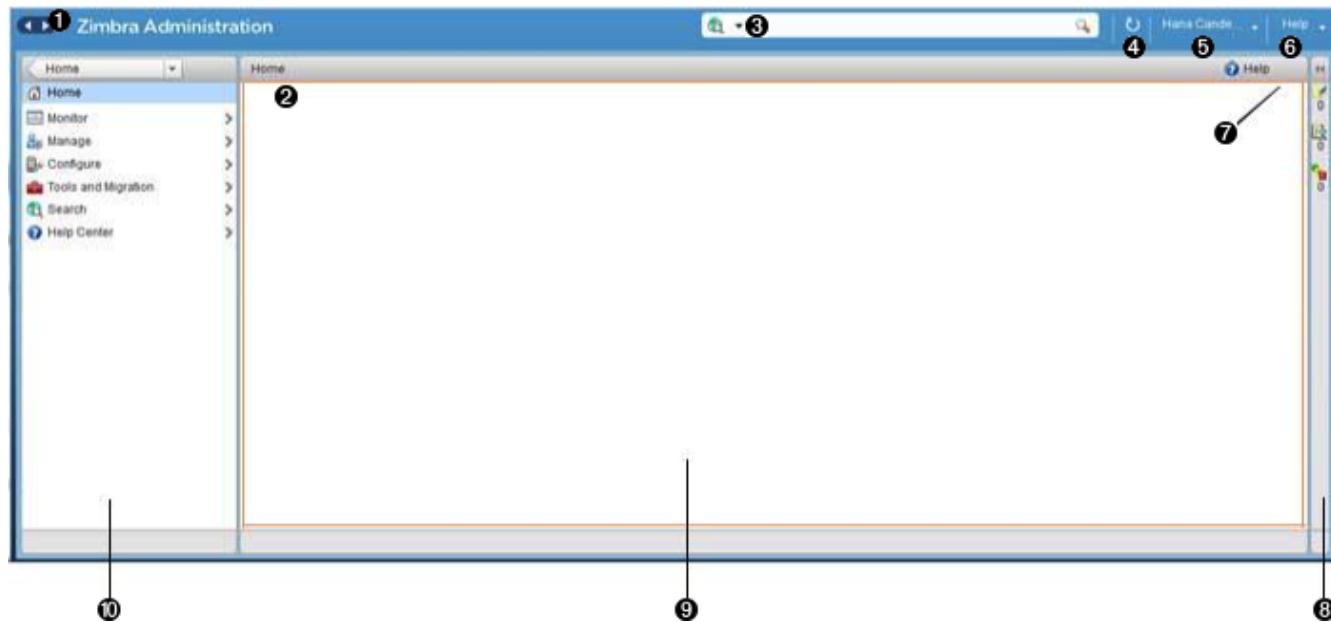
Most results returned by GAL search:	100
Default domain:	jhurley1.us.zimbraLab.com
Maximum number of simultaneous logins:	Attribute Name
Sleep time before:	zimbraDefaultDomainName
Maximum size of a file uploaded from the desktop (KB):	Description name of the default domain for accounts when authenticating without a domain
Admin help URL:	
Delegated admin help URL:	

More **Hide**

Navigating the User Interface

The Zimbra Collaboration Administration Console is organized to provide quick navigation to the configuration and monitoring tools and views associated with your login privileges. It also provides easy access to various types of **Help** and the on-screen guide text.

After logging in to the Administration Console, the **Home** page is displayed to provide status information and options you can select to navigate to the configuration and viewing options described in this user guide.



- <1> Go to Previous or Next page
- <2> Current Location/Path
- <3> Search
- <4> Screen Refresh
- <5> Current User and Logout Option
- <6> Help
- <7> Gear Icon
- <8> Status Pane
- <9> Viewing Pane
- <10> Navigation Pane

The displays and options in the navigation pane and viewing pane change in accordance with your selections. Other portions of the UI—arrow buttons, search field, screen refresh, current location/path, current login, and Help—always remain in view.

The Gear Icon  is displayed with certain screens, to enable quick access to functions associated with the functions provided in the screens. For more information about the Gear icon, see [Using the Gear icon](#)

Home Navigation Pane

The options provided in the **Home** navigation pane are categorically defined under the **Home** directory. Some of the options lead to configuration pages; others lead to pages containing reports, as associated with your selections.

The illustration at right is an expanded view of the options currently supported in the Navigation Pane.

Your current position in the hierarchy is always displayed at the upper bar of the page currently in view, and you can use multiple options for dismissing the current view:

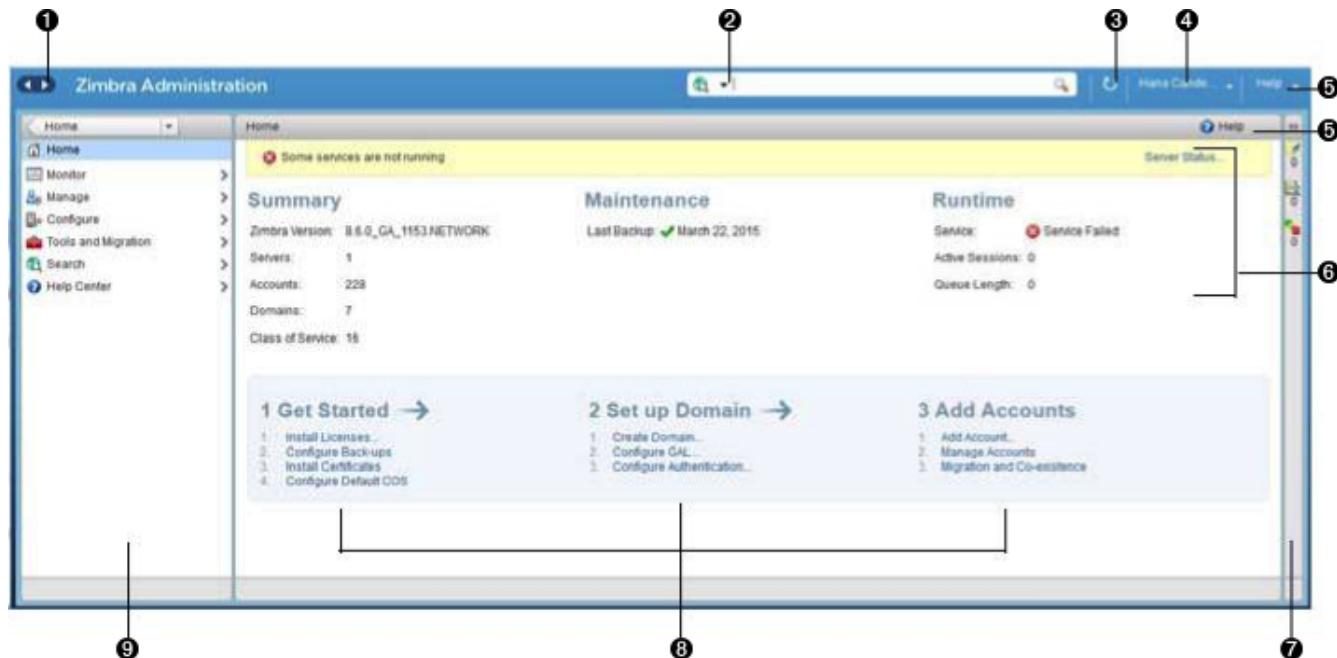
- To return to a previous page or go to a next page, click the left or right arrows.
- To return to a specific portion of the UI, select an option from the Home drop down.
- To go directly to a specific option, click through the hierarchy in the Navigation Pane.

The Navigation pane options are described in the following topics:

- [Home UI](#).
- [Monitor UI](#).
- [Manage UI](#).
- [Configure UI](#).
- [Global Settings UI](#).
- [Tools and Migration UI](#).
- [Search UI](#).

Home UI

The **Home** screen is the default, login view, which provides the **Home** navigation pane and the Home page. This page provides a snapshot view of system status and a series of quick access links for essential tasks.



- <1> Go to Previous or Next page
- <2> Search
- <3> Screen Refresh
- <4> Current User and Logout Option
- <5> Help
- <6> System Status
- <7> Status Pane
- <8> Quick Start
- <9> Navigation Pane

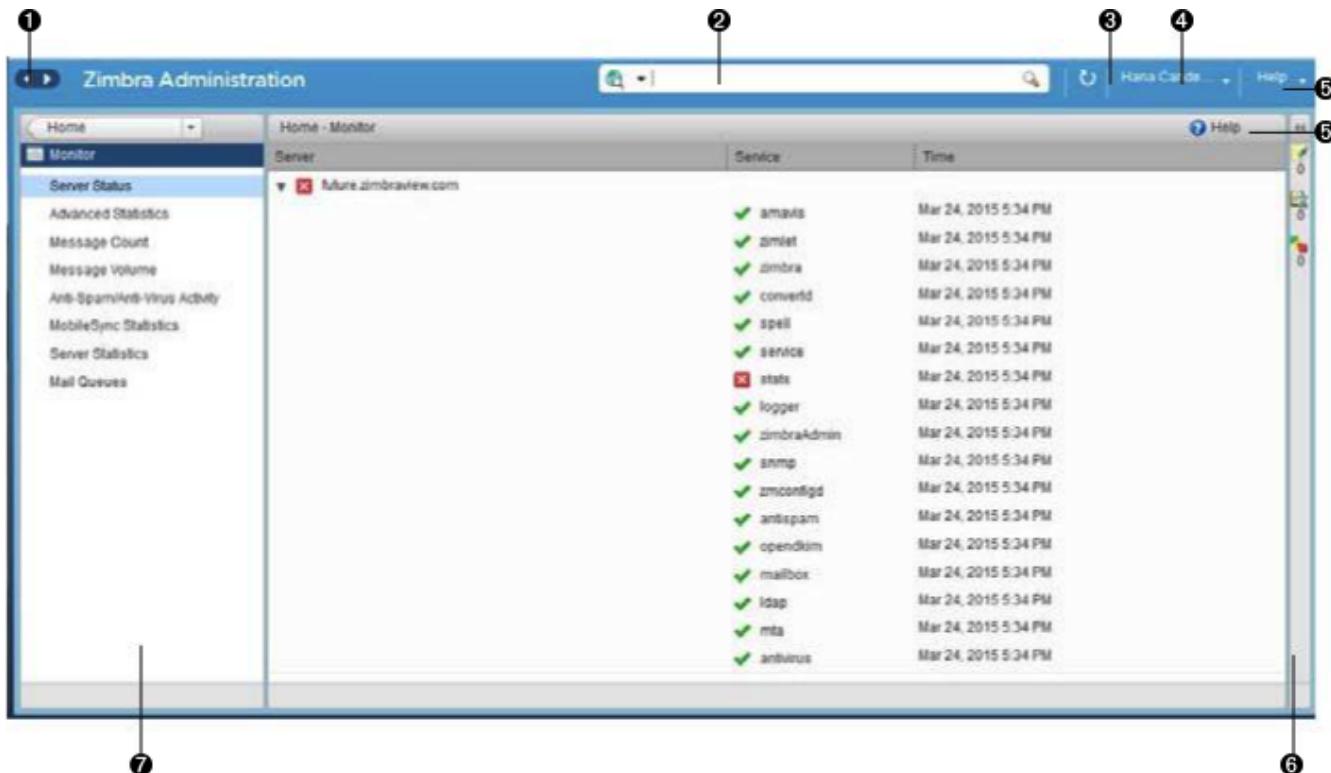
Table 11. Home UI

Topic	Description
Summary	Displays the version of Zimbra Collaboration currently running and in view, and the detected number of servers, account, domains, and classes of service associated with this session.
Maintenance	Displays the most recent software backup performed.
Runtime	Displays the runtime statistics for Service, Active Session, and Queue Length.

Topic	Description
1 Get Started	<p>Displays the steps essential to getting started with your Zimbra Collaboration operations, and provides quick links to the functions in this UI:</p> <ol style="list-style-type: none"> 1. Install Licenses 2. Configure Back-ups 3. Install Certificates 4. Configure Default COS
2 Set up Domain	<p>Displays the steps you use to establish the domain(s) to be managed by the Collaborator. Each step is a link to the function in this UI:</p> <ol style="list-style-type: none"> 1. Create a Domain 2. Configure GAL... 3. Configure Authentication
3 Add Accounts	<p>Displays the steps for adding accounts for management by the Collaborator. Each step is a link to the function in this UI:</p> <ol style="list-style-type: none"> 1. Add Account 2. Manage Accounts 3. Migration and Co-existence

Monitor UI

The **Monitor** screen provides the Monitor navigation pane and the Monitor pages, which display various itemizations about servers monitored by the Collaborator.



- <1> Go to Previous or Next page
- <2> Search
- <3> Screen Refresh
- <4> Current User and Logout Option
- <5> Help
- <6> Status Pane
- <7> Navigation Pane

Monitor Navigation Pane and Pages

The options provided in the **Monitor** pages provide various methods- dynamic charts, or tables-for viewing the individual or system-wide monitored servers and services listed in the following table.

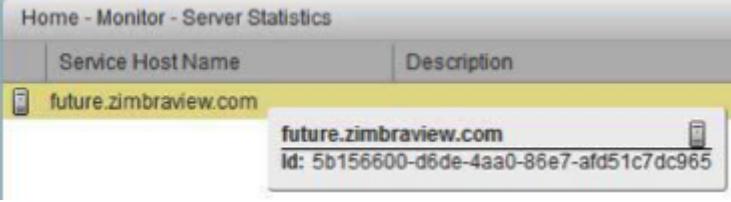


Adobe Flash Player must be activated to enable views of the dynamic charts.

Table 12. Monitor UI

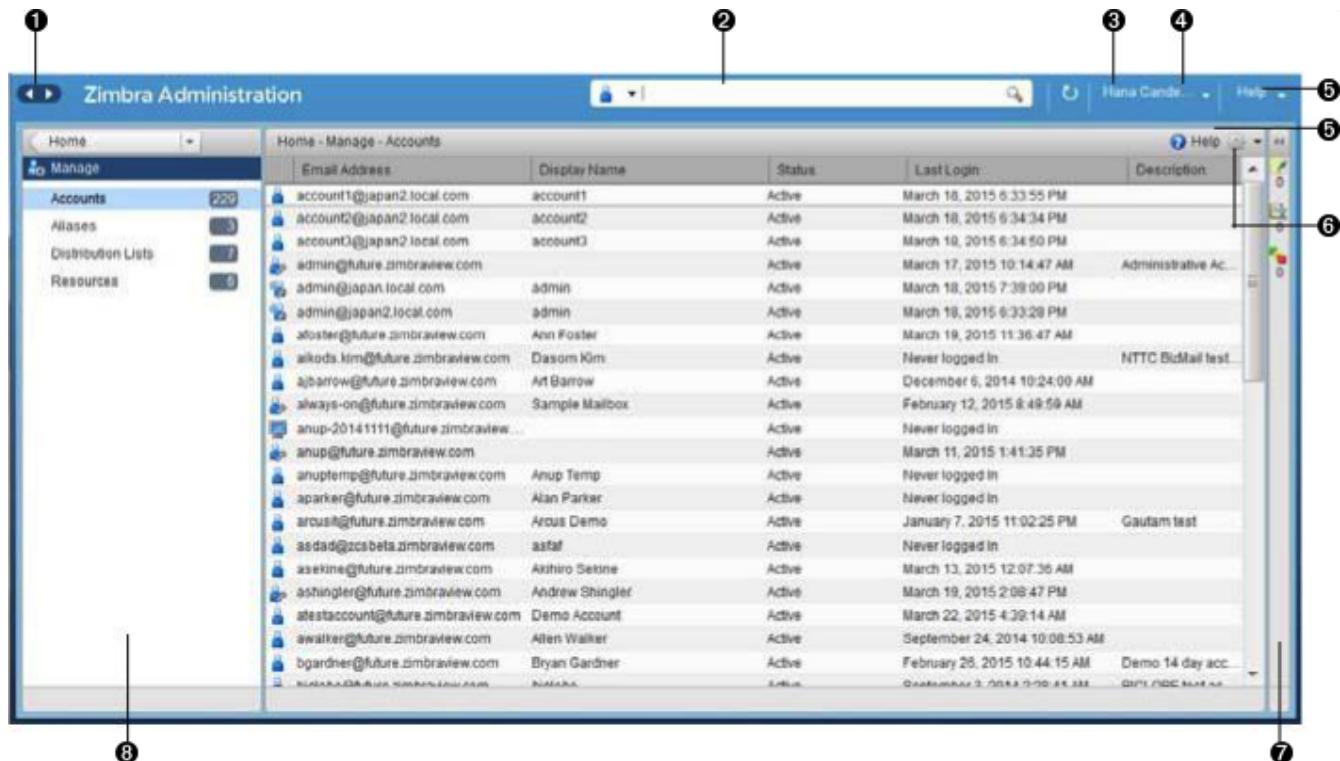
Option	Description
Server Status	Server, Service, and Time details for each server monitored by the Collaborator.

Option	Description
Advanced Statistics	<p>System-wide Information page, for Advanced Statistics, which allows you to set up a new monitoring chart using parameters from the selection fields available from this page: Server, Group, Start, end, and Counters.</p> <p>From this Advanced Statistics page, you can also elect to perform the following operations:</p> <ul style="list-style-type: none"> • Hide Chart Settings • Update Chart • Remove Chart
Message Count	<p>System-wide Information page, for Message Counts, to examine charts depicting counts over the last 48, 30, 60, and 365 days. The information provided is based on the number of recipients of messages using either SMTP or LMTP. The polling intervals for the counts are posted directly beneath each chart.</p>
Message Volume	<p>System-wide Information page, for Message Volume, to view charts depicting the number of recipients of messages-using either SMTP or LMTP-and associated message sizes. These counts are shown in periods over the last 48, 30, 60, and 365 days. The polling intervals for the counts are posted directly beneath each chart.</p>
Anti-Spam/Anti-Virus	<p>System-wide Information page, for Anti-Spam/Anti-Virus</p>
Activity	<p>Activity, depicting the number of unique messages processed by the AS/AC system over the last 48, 30, 60, and 365 days. The polling intervals for the counts are posted directly beneath each chart.</p>

Option	Description
Server Statistics	<p>Access to statistics for a selected Service Host. You can view information for a selected host, as follows:</p> <ul style="list-style-type: none"> Place and hold the cursor on the Service Hostname to view popup license information.  <p>future.zimbraview.com Id: 5b156600-d6de-4aa0-86e7-af51c7dc965</p> <ul style="list-style-type: none"> Right-click on the Service Hostname and select View from the popup to go to the statistics page for it. You can also double-click on the Service Hostname to access the statistics page.  <p>future.zimbraview.com <input checked="" type="checkbox"/> View</p> <p>For the selected Server, the Server Statistics navigation pane provides options to view Disk, Session, Mailbox Quota, Message Count, Message Volume, and Anti-Spam/Anti-Virus Activity.</p>
Mail Queues	Tab pages from which to view counts of Deferred, Incoming, Active, Held, and Corrupt statistics for detected mail queues. Each tab page provides summary filtering information and Message details.

Manage UI

The **Manage** screen provides the **Manage** navigation pane and the **Manage** pages, which display the tables categorically provided as Accounts, Aliases, Distribution Lists, and Resources that are currently managed by Collaborator.



- <1> Go to Previous or Next page
- <2> Search
- <3> Screen Refresh
- <4> Current User and Logout Option
- <5> Help
- <6> Gear Icon
- <7> Status Pane
- <8> Navigation Pane

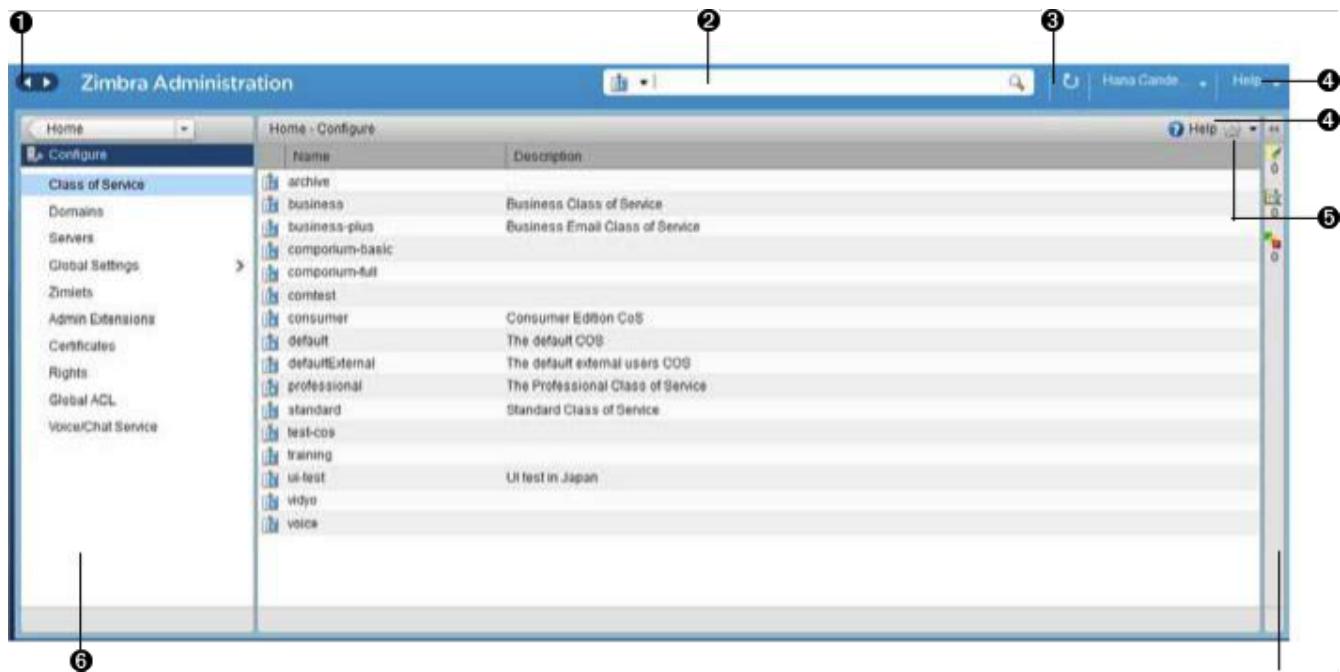
Table 13. Manage UI

Option	Description
Accounts (count)	<p>Table of accounts managed by the Collaborator. Actions you can perform:</p> <ul style="list-style-type: none"> • View ID information from a popup display: Hold the cursor over an Accounts row. • Right-click on a table row, or use the Gear icon to access the following functions: Delete, Edit, Change Password, New Administrator, View Mail, New, Invalidate Session, View Rights, Configure Grants, Move Mailbox, Search Mail.

Option	Description
Aliases (count)	<p>Table of Aliases managed by the Collaborator. Each alias is an email address that forwards all email to a specified account.</p> <p>Actions you can perform:</p> <ul style="list-style-type: none"> • View ID information in a popup display: Hold the cursor over an Alias row. • Right-click on a table row, or use the Gear icon to access the following functions: Delete, Edit, New Administrator, View Mail, Move Alias, New, Invalidate Session, View Rights, Configure Grants, Move Mailbox, Search Mail.
Distribution Lists (count)	<p>Table of Distribution Lists managed by the Collaborator. A Distribution List is a group of mail addresses contained in a list, with a common mail address. When you send to a distribution list, you are sending to everyone whose address is included in the list. The To: address line displays the distribution list address.</p> <p>Actions you can perform:</p> <ul style="list-style-type: none"> • View ID information: Hold the cursor over a Distribution List row. • Right-click on a table row, or use the Gear icon to access the following functions: Delete, Edit, New Administrator, View Mail, New, View Rights, Configure Grants, Search Mail.
Resources (count)	<p>Table of Resources managed by the Collaborator. A Resource is a location or a piece of equipment that can be scheduled for meetings.</p> <p>Actions you can perform:</p> <ul style="list-style-type: none"> • View ID information: Hold the cursor over a Resources row. • Right-click on a table row, or use the Gear icon to access the following functions: Delete, Edit, New Administrator, View Mail, New, View Rights, Configure Grants, Search Mail.

Configure UI

The **Configure** screen provides the **Configure** navigation pane and the **Configure** pages, which enable configurations for individual and/or global components.



- <1> Go to Previous or Next page
- <2> Search
- <3> Screen Refresh
- <4> Help
- <5> Gear Icon
- <6> Status Pane
- <7> Configure Navigation Pane

Table 14. Configure UI

Option	Description
Class of Service	<p>Displays the COSs managed from this AdministrationConsole.</p> <ul style="list-style-type: none"> • Double-click on a table row to access the configuration screens for the selected COS, or • Right-click on a table row, or use the Gear icon to access the following functions: New, Delete, Edit, Duplicate

Option	Description
Domains	<p>Displays the domains managed from this Administration Console.</p> <ul style="list-style-type: none"> • Double-click on a table row to access the configuration screens for the selected domain, or • Right-click on a table row, or use the Gear icon to access the following functions: New, Delete, Edit, Configure GAL, Configure Authentication, View Accounts, Add a Domain Alias, Configure Grants
Servers	<p>Displays the servers managed from this Administration Console.</p> <ul style="list-style-type: none"> • Double-click on a table row to access the configuration screens for the selected server, or • Right-click on a table row, or use the Gear icon to access the following functions: Edit, Flush Cache, Enable Proxy, Disable Proxy
Global Settings	<p>Provides access to tools you use to set various global parameters for your Zimbra Collaboration.</p> <p>Gear Icon: Save, Download, Update License, Activate License, Manually Activate License</p>
Zimlets	<p>Displays the Zimlets managed from this Administration Console.</p> <ul style="list-style-type: none"> • Double-click on a table row to access the configuration screens for the selected Zimlet, or • Right-click on a table row, or use the Gear icon to access the following functions: Deploy, Undeploy, Toggle Status
Admin Extensions	<p>Displays the Admin Extensions managed from this Administration Console.</p> <ul style="list-style-type: none"> • Double-click on a table row to access the configuration screens for the selected Admin Extension, or • Right-click on a table row, or use the Gear icon to access the following functions: Deploy, Undeploy

Option	Description
Certificates	<p>Displays the Certificates managed from this Administration Console.</p> <ul style="list-style-type: none"> • Double-click on a table row to access the General Information screen for the selected certificate, or • Right-click on a table row, or use the Gear icon to access the following functions: Install Certificate, View Certificate
Rights	<p>Displays the various Rights that are managed from this Administration Console.</p> <ul style="list-style-type: none"> • Double-click on a table row to access the General Information screen for the selected Right, or • Right-click on a table row, or use the Gear icon to access the following function: View
Global ACL	<p>Displays the Global Access Control Lists managed from this Administration Console.</p> <ul style="list-style-type: none"> • Double-click on a table row to access the Edit ACE screen for the selected Global ACL, or • Right-click on a table row, or use the Gear icon to access the following functions: Add, Delete, Edit

Global Settings UI

Global Settings define the default global values for servers, accounts, COS, and domains. These default values and parameters apply if the values and parameters have not been explicitly defined in settings configures elsewhere.

The defaults for Global Settings are configured during installation. You can change the settings at any time from Global Settings at the Administration Console.

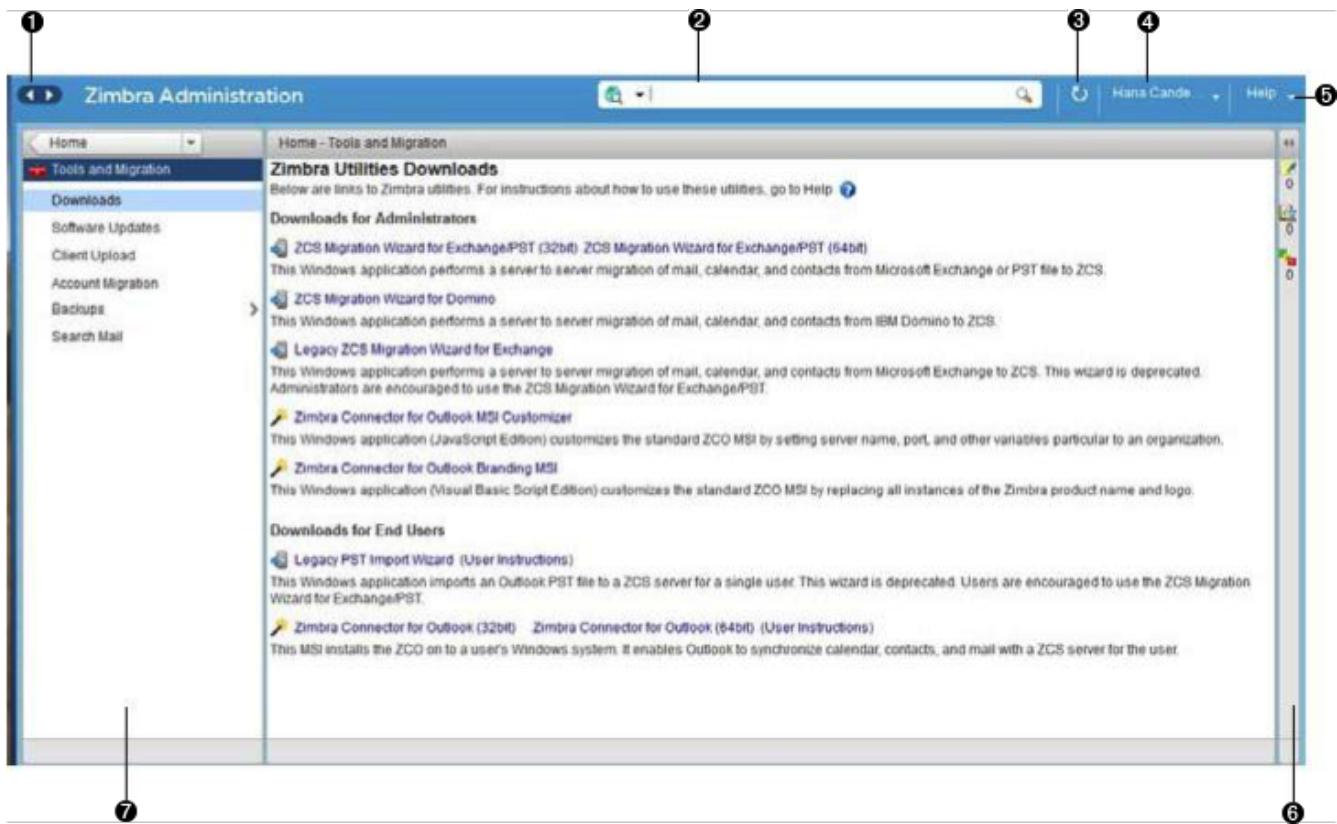
Table 15. Global Settings UI

Option	Description
General Information	<ul style="list-style-type: none"> Set global ceiling for the number of results from a GAL search. Define default domain. Configure the number of threads that can be used to get the content from the remote data sources. <p>For more information, see General Information Configuration</p>
Attachments	<ul style="list-style-type: none"> Enable rules to reject messages that include attachments of a specific extension. Disable attachments from being read. Convert attachments to HTML for viewing. <p>For more information, see Attachments Configuration.</p>
MTA	<ul style="list-style-type: none"> Enable authentication. Set maximum message size. enable or disable protocol and DNS check. Add X-Originating-IP message headers. <p>For more information, see MTA Configuration.</p>
IMAP	Enable IMAP service. Changes to these settings do not take effect until the server is restarted.
POP	Enable POP3 Service. Changes to these settings do not take effect until the server is restarted.
AS/AV	Set anti-spam and anti-virus rules. Changes to the Spam-check settings do not take effect until the server is restarted.
Themes	<ul style="list-style-type: none"> Customize the color scheme of existing themes Add logo to a theme. <p>Change to theme settings require the server theme cache to be flushed, by using the Flush Cache toolbar button at Server settings.</p> <p>For more information, see Color and Logo Management.</p>
Advanced	<ul style="list-style-type: none"> Configure the company name to be displayed in the prompt on the Authentication Required dialog used to log in to Briefcase folders shared with external guests Add regular expression rules for Account Email Validation.

Option	Description
Retention Policy	Set up a retention and deletion time threshold for items in user folders. Retention and deletion policies can be configured as a global setting or you can configure COS-level policies instead of inheriting from the global settings.
Proxy	Set parameters for Web Proxy and Mail Proxy. Tools are also provided for setting Advanced Proxy parameters.
S/MIME	(Secure Multipurpose Internet Mail Extensions): Configure the LDAP settings on the S/MIME tab (if S/MIME feature has been enabled). Users will use LDAP servers to retrieve private keys.
ACL	(Access Control List): Go to ACE (Access Control Entry) configuration for delegated administration rights granted on selected target(s), to add, edit, or delete an ACE.
Backup/Restore	Set parameters for backup-for standard or auto- grouped mode. For more information see Backup and Restore .
HSM	(hierarchical storage management): Configure the aging of messages before they are to be moved to the secondary volume.
License	<ul style="list-style-type: none"> • Update and install your Zimbra license. • View current license information.

Tools and Migration UI

The **Tools and Migration** screen provides the **Tools and Migration** navigation pane, for access to system software management and system backup/restore. Administrators can access and download specific wizards and tools from this page.



- <1> Go to Previous or Next page
- <2> Search
- <3> Screen Refresh
- <4> Current User and Logout Option
- <5> Help
- <6> Status Pane
- <7> _Tools and Migration_ Navigation Pane

Table 16. Tools and Migration

Option	Description
Downloads	Access Zimbra utilities, which provides downloadable zip packages - for general administration use, and to synchronize an individual end user - containing migration wizards for various platforms, and Outlook connectors. Additional information is provided in Downloadable Wizards and Connectors .
Software Updates	Find out if your system needs a Zimbra Server update or not, and use this page to view polling and email contact information pertinent to software updates for your system. See also Checking for Zimbra Collaboration Software Updates .
Account Migration	View tabular details about account migrations, as detected by your system. This page lists total imports and the status of each. This page also provides the name(s) of the owners for each account migration listed. See also Migrating Accounts from a Zimbra Server .

Option	Description
Client Upload	Use this page to browse for the latest version of software to be uploaded to your system. After selecting the image, you can use the Upload button on this page to complete the software upload.
Backups	<p>Access a summary view of current free and total space (MB) based on the most recent system backup. You can also select a specific administrator from this navigation pane to view backup history as associated with the selected administrator. The history lists labels, start and end times, and success or failure for each backup occurrence; each of these is associated with the identical, displayed directory path to the backup target.</p> <p>Additional information is provided in Backup and Restore.</p>

Downloadable Wizards and Connectors

Use the **Tools and Migration** screen **Downloads** option to get the tools described in this section. Check [Zimbra PST Migration](#) to migrate Outlook PSTs to Zimbra Collaboration.

Table 17. Administrator Tools and Migration Options

ZCS Migration Wizard for Exchange/PST (32 bit)	Get zip files to perform a server-to-server migration of mail calendar, and contacts, from Microsoft Exchange or PST file to the Zimbra Collaboration Server.	 This package is supported only for PST file import, with End of Technical Guidance set for 31 December 2020. We recommend Audriga's self-service migration solution as a preferred alternative for all account migrations.
ZCS Migration Wizard for Domino	 This package is deprecated! We recommend Audriga's self-service migration solution as a preferred alternative for all account migrations.	
Legacy ZCS Migration Wizard for Exchange	 This package is deprecated! We recommend Audriga's self-service migration solution as a preferred alternative for all account migrations.	

Zimbra Connector for Outlook MSI Customizer	Present text file containing functions you can use to customize the standard ZCO MSI. Server name, port, and other variables particular to an organization can be customized.
Zimbra Connector for Outlook Branding MSI	Get the Windows Visual Basic Script Edition (VBScript Script File) to customize the standard ZCO MSI. Customization replaces all instances of the Zimbra product name and logo.

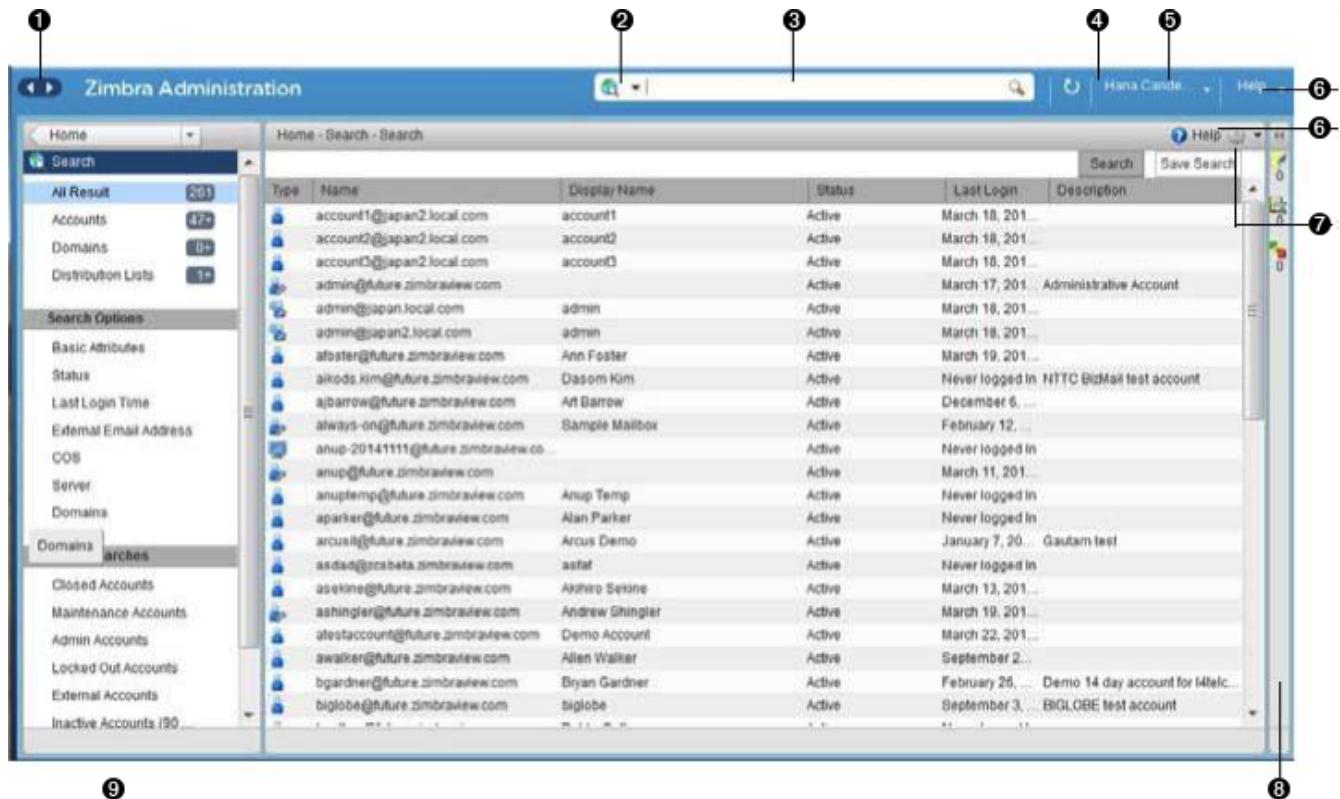
Table 18. End User Desktop Applications and Utilities / Migration and Import Tools

Zimbra Connector for Outlook (32 bits) Zimbra Connector for Outlook (64 bit) (User Instructions)	This application enables the user's Outlook to synchronize calendar, contacts, and mail with the ZCS server. The Zimbra Connector for Microsoft Outlook (ZCO) allows users of Microsoft Outlook to connect to the ZCS server to access ZCS business features. Address books, Contacts, Calendars, Tasks, and mail are synced directly with the ZCS server.
(Legacy) Microsoft Outlook PST Import Tool	 This package is deprecated! Users should use the General Migration Wizard for PST import.
(Legacy) Migration Wizard for Microsoft Exchange	 This package is deprecated! We recommend Audriga's self-service migration solution as a preferred alternative for all account migrations.
General Migration Wizard	This tool imports data within Microsoft Exchange servers and Outlook PST files to the Zimbra Server.  This package is supported only for PST file import. We recommend Audriga's self-service migration solution as a preferred alternative for all account migrations.

Search UI

The **Search** screen displays the **Search** results from queries made in the Search field in the Administration Console header.

- When you open this page without entering a search query, *All Results* is the default search, which displays accounts, domains, and distribution lists in the Content pane.
- The auto-completion function allows you to enter a partial name, then select a searchable name from the displayed list of matched strings.
- You can also use the Zimbra mailbox ID number to search for an account. However, to return a search from a mailbox ID, the complete ID string must be entered in the search.



- <1> Go to Previous or Next page
- <2> Search Options
- <3> Search
- <4> Screen Refresh
- <5> Current User and Logout Option
- <6> Help
- <7> Gear Icon
- <8> Status Pane
- <9> Search Navigation Pane

Table 19. Search UI

Option	Description
All Result	View the count and table of all search results.
Accounts	View the count and table resulting from a query for Accounts.

Option	Description
Domains	View the count and table resulting from a query for Domains.
Distribution Lists	View the count and table resulting from a query for Distribution Lists.
Basic Attributes	Search for a user by first name, last name, display name, or account ID number. You can search for administrators or delegated administrators only.
Status	Search for an account by status: Active, Closed, Locked, Logout, Pending, or Maintenance.
Last Login Time	Search for accounts by the last login time. You can specify a date range to search.
External Email Address	Search for an account with an external email address.
COS	Search for objects by COS or for objects that are not assigned a COS.
Server	Search for accounts on selected servers.
Domains	Search for accounts on selected domains.
Saved Searches	By default, this section includes predefined common search queries. You can also create and save your own queries. After you enter the query syntax, click Save Search and provide a name for the search. The search is then added to this Saved Searches section.

Setting Up a Simple Search

- At the **Search** field, use search options from the drop-down selector to define the type of search, as either *accounts, distribution lists, aliases, resources, domains, class of service, or all objects*.

For accounts, you can search by display name, first/last name, first part of email address, alias, delivery address, or mailbox ID.

- Type the search string into the **Search** field.

Partial entries are allowed as search criteria, but a search based on mailbox ID must include the complete ID string.

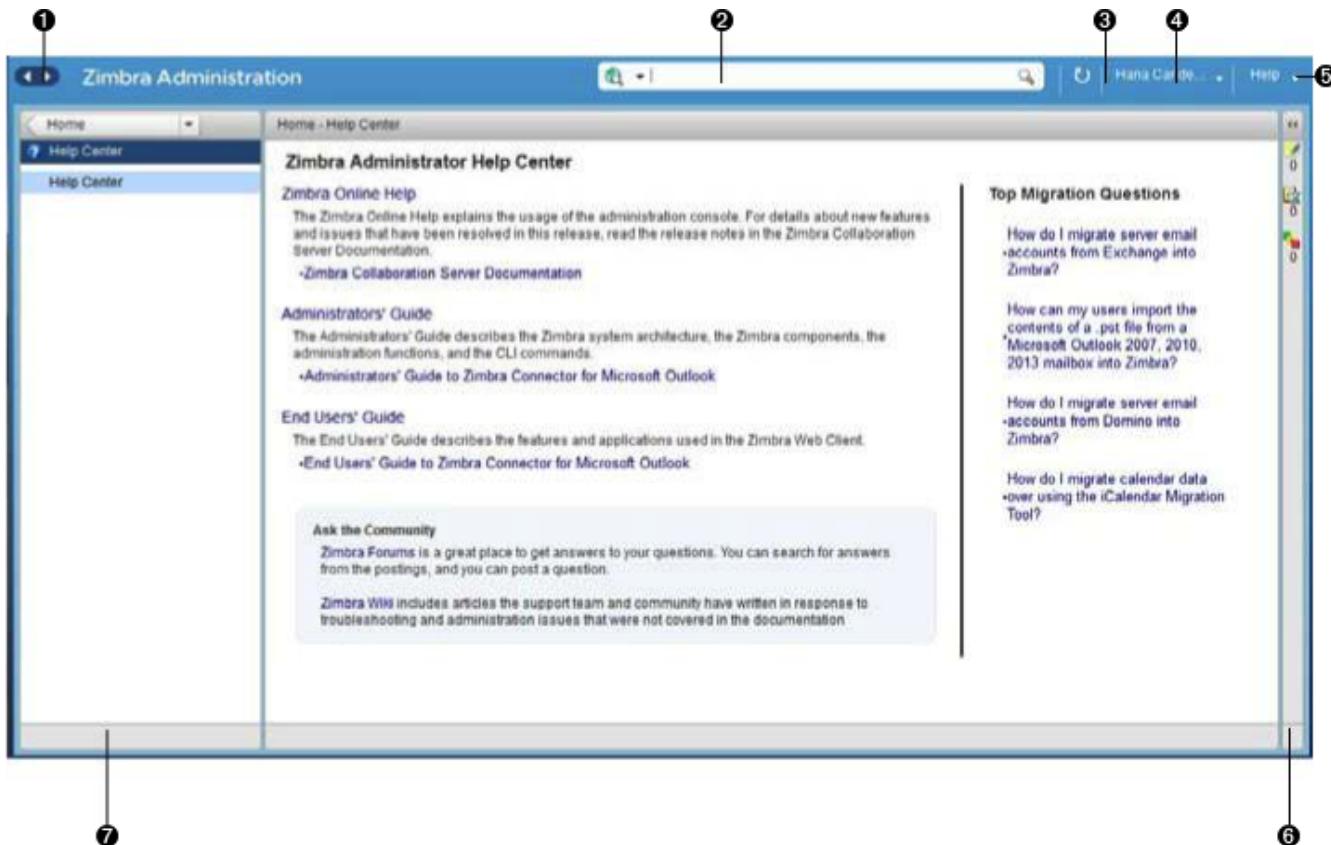
- Click **Search**.

The Search page is now presented, containing results of the search based on your criteria.

- View the total number of results at the Navigation pane, in **Search> All Results**.

Help Center UI

The **Help Center** is a reference of resources available from the online help and documentation, which you can access with the links provided in the **Help Center** screen. Use this page, also, to access community forums and to view expert responses to the top migration questions.



- <1> Go to Previous or Next page
- <2> Search
- <3> Screen Refresh
- <4> Current User and Logout Option
- <5> Help
- <6> Status Pane
- <7> Help Center Navigation Pane

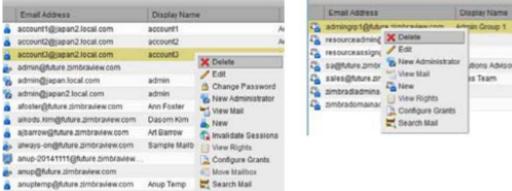
Tools in Collaborator Tables

Selection of a category from the Navigation pane typically results in tabular display of all managed objects for the selected category. All tables display labeled columns in which to view information such as email addresses, display names, status, last logins, and descriptions (if configured).

Each row in a table enables actions you can perform if you require additional information and/or access to the configuration for the selected table entry.

Action at Table Row	Result
Hold cursor	Display ID details for the selection, similar to the example at right (invoked from an Accounts row).

Email Address	Display Name	Status
account1@japan2.local.com	account1	Active
account2@japan2.local.com	account2@japan2.local.com	
account3@japan2.local.com	Mail Server: future.zimbraview.com	
admin@future.zimbraview.com	Id: 22e15bb5-19d7-4600-0da4-14e2d250030f	

Action at Table Row	Result	
Right-click	Access the popup menu for a selected table row. The popup menus from a common table may differ from row to row, as demonstrated in the following examples.	Accounts and Aliases: Dist Lists and Resources: 

Message of the Day

Global administrators can create the message(s) of the day (MOTD) that administrators view when logging into the Administration Console.

The configured message displays at the top left of the Administration Console for each administrative login (similar to the example below).



The message can be closed, replaced, or removed.

Closing a Message of the Day

To remove a message from view, click the **Close** button located alongside the message content.

Creating Message(s) of the Day

Use the `zimbraAdminConsoleLoginMessage` attribute, with guidelines in this section, to create a single message of the day, or to create multiple messages to be displayed.



When creating a message with your command entry, always place double-quote marks at the beginning and end of the message to be displayed.

Creating a global message or domain-specific message.

```
zmprov md <domain> zimbraAdminConsoleLoginMessage "message to display"
```

Creating a multiple-message display:

```
zmprov md <domain> +zimbraAdminConsoleLoginMessage "second message to display"
```

Removing Message(s) of the Day

Use the `zimbraAdminConsoleLoginMessage` attribute, with guidelines in this section, to delete a single message of the day, or to delete multiple messages.



When removing a message with your command entry, use the following guidelines for individual and multiple deletions:

- Place a minus sign (-) before the attribute, and double quote marks at the beginning and end of an individual message to be deleted.
- Use single quote marks with the attribute to remove all messages.

Removing a specific message:

```
zmprov md <domain> -zimbraAdminConsoleLoginMessage "message to display"
```

Removing all messages:

```
zmprov md <domain> zimbraAdminConsoleLoginMessage ''
```

Functional Reference

This section provides birds-eye views of the functions you can use when navigating the Administration Console, in the following topics:

- [GUI Roadmap](#)
- [Popup Menu Options](#)
- [Containers](#)

GUI Roadmap

A high-level view of the Administration Console UI is provided in the following illustration.

High-level View of Administration Console UI

(not applicable)

- o **Accounts:**
New, New Administrator, Edit, Delete, Change Password, Invalidate Sessions, View Mail, Move Mailbox, View Rights, Configure Grants
 - o **Aliases:**
New, New Administrator, Edit, Delete, Move Alias, Invalidate Sessions, View Mail, Move Mailbox, View rights, Configure Grants
 - o **Distribution Lists:**
New, New Administrator, Edit, Delete, View Mail, View Rights, Configure Grants
 - o **Resources:**
New, New Administrator, Edit, Delete, View Mail, View Rights, Configure Grants
 - B o **Class of Service <name>:**
New, Delete, Edit, Duplicate
 - o **Domain:**
New, Delete, Edit, Configure GAL, Configure Authentication, View Accounts, Add a Domain Alias, Configure Grants
 - o **Servers:**
Edit, Flush Cache, Enable Proxy, Disable Proxy
 - o **Global Settings:**
Save, Download, Update License, Activate License, Manually Activate License
 - o **Zimlets:**
Deploy, Undeploy, Toggle Status
 - o **Admin Extensions**
Deploy, Undeploy
 - o **Certificates**
Install Certificate, View Certificate
 - o **Voice/Chat Service:**
New, Delete, Edit, Generate Session ID
 - o **Rights:**
View
 - o **Global ACL:**
Add, Delete, Edit
- d (not applicable)
- All Results:
Delete, Edit, Change Password, View Mail, Move Alias, Invalidate Sessions, Move Mailbox, Download
- All Accounts:
Delete, Edit, Change Password, View Mail, Move Alias, Invalidate Sessions, Move Mailbox, Download
- All Domains:
Delete, Edit, Change Password, View Mail, Move Alias, Invalidate Sessions, Move Mailbox, Download
- All Distribution Lists:
Delete, Edit, Change Password, View Mail, Move Alias, Invalidate Sessions, Move Mailbox, Download

Filter (not applicable)

Popup Menu Options

You can select options to perform on a selected entity from the navigation pane from the Gear icon or a topical popup menu.

Using the Gear icon

The **Gear** icon is always located at the upper right edge of the page view if pertinent to selectable items in the displayed page.

The screenshot shows the Zimbra Administration interface for managing a Class of Service (COS). The left sidebar has a 'General Information' section with various options like Features, Preferences, Themes, Zimlets, Server Pool, Mobile Access, Advanced, Retention Policy, and ACL. Below it is a 'Related' section with a 'Domains' link. The main content area is titled 'defaultExternal' and contains fields for Display name (set to 'defaultExternal'), Description ('The default external users COS'), and Notes. A 'Voice and Chat' section is also present. At the top right of the main window, there are 'Help', 'Save', and 'Close' buttons, with a green arrow pointing to the 'Close' button.

To view the available options, highlight a topic at the navigation pane or in the page view: In the popup, the options that are not applicable to your selection are disabled: other displayed options can be used with your selection. The following example demonstrates Gear options based on selection of a navigation bar topic, versus a table row entry from within the same page view.

This screenshot shows the 'Manage - Accounts' page. The left sidebar has a 'Manage' section with 'Accounts' selected, indicated by a green arrow. The main table lists accounts with columns for Email Address, Display Name, Status, and Last Login. A gear icon in the top right corner of the table header is highlighted with a green arrow and labeled 'Gear options for the selection'.

This screenshot shows the 'Manage - Accounts' page with a single account ('anything@hurley1.us.zimbralab.com') selected, indicated by a green arrow. The gear icon in the top right corner of the table header is highlighted with a green arrow and labeled 'Gear options for the selection'.

The following table provides a high-level view of the operations derived from the Gear icon, which varies for particular functions.

Table 20. Gear Icon Operations

Navigation Pane Topic	Selections	Options  ▾
Home Monitor	Server Statistics	View
	Mail Queues	Flush
Manage	Accounts	New, New Administrator, Edit, Delete, Change Password, Invalidate Sessions, View Mail, Move Mailbox, View Rights, Configure Grants
	Aliases	New, New Administrator, Edit, Delete, Move Alias, Invalidate Sessions, View Mail, Move Mailbox, View Rights, Configure Grants
	Distribution Lists	New, New Administrator, Edit, Delete, View Mail, View Rights, Configure Grants
	Resources	New, New Administrator, Edit, Delete, View Mail, View Rights, Configure Rights
Configure	Class of Service	New, Delete, Edit, Duplicate
	Domains	New, Delete, Edit, Configure GAL, Configure Authentication, View Accounts, Add a Domain Alias, Configure Grants
	Servers	Edit, Flush Cache, Enable Proxy, Disable Proxy
	Global Settings	Save, Download, Update License, Activate License, Manually Activate License
	Zimlets	Deploy, Undeploy, Toggle Status
	Admin Extensions	Deploy, Undeploy
	Certificates	Install Certificate, View Certificate
	Voice/Chat Service	New, Delete, Edit, Generate Session ID
	Rights	View
	Global ACL	Add, Delete, Edit
Tools and Migration	Software Updates	Save, Check Now
	Account Migration	Delete Task, Refresh, Migration Wizard
	Backups	View, Backup, Restore, Configure, Refresh
Search	All Result	Delete, Edit, Change Password, View Mail, Move Alias, Invalidate Sessions, Move Mailbox, Download
	Accounts	
	Domains	
	Distribution Lists	

Using the Topical Popup Menus

You can elect to access options to perform on a selection by using popup menus:



Popup menus are not provided in the Navigation Pane.

The following example demonstrates the popup options provided by a specific selection in the page view.

Example 5. Popup Options

A screenshot of the Zimbra Administration interface. On the left, there's a navigation pane with 'Manage' selected, showing 'Accounts' (2), 'Aliases' (2), 'Distribution Lists' (2), and 'Resources' (0). The main area shows a table of accounts under 'Manage - Accounts'. One account, 'anything@jhurley1.us.zimbralab.com', is selected. A context menu is open over this account, with a green arrow pointing to it from the text 'right-click to reveal the popup menu'. The menu items include: Delete, Edit, Change Password, New Administrator, View Mail, New, Invalidate Sessions, Move Mailbox, View Rights, and Configure Grants. The table has columns for Display Name, Status, Last Login, and Description.

Containers

A wide range of Configuration options are logically grouped into containers in the Administration Console. Applicable configuration options inside these containers are listed in the [High-level View of Administration Console UI](#)

By default, all containers on a page are opened (expanded). You can opt to close (collapse) containers - which can free up additional space in a page view - by clicking on the collapse/ expand button located at the upper left edge of the container.

A screenshot of the Zimbra Administration 'Configure' section. The left sidebar lists various configuration categories: Global Settings, General Information, Attachments, MTA (which is selected and highlighted in blue), IMAP, POP, AS/AV, Free/Busy Interop, Themes, Advanced, Authentication, Retention Policy, Proxy, Backup/Restore, License, and HSM. The main content area is titled 'Home - Configure - Global Settings - MTA'. It contains a note: 'Note: Settings only apply to servers that have the appropriate service(s) installed and enabled'. Below this are several expandable sections: 'Authentication' (closed), 'Network' (closed), 'Milter Server' (closed), 'Messages' (closed), 'Policy Service Checks' (closed), 'Protocol checks' (closed), and 'DNS checks' (closed). The 'Milter Server' section is circled with orange circles around its title and the 'click to toggle between open | close' text. An orange arrow points to the 'Open (expanded) container' link next to the 'Milter Server' section. The 'Milter server bind port' field is set to 7026, and the 'Enable milter server' checkbox is unchecked.

Zimbra PST Migration Wizard

The Zimbra PST Migration Wizard helps migrate Microsoft Outlook personal folders (**PST**) files to Zimbra Collaboration (ZCS).

The tool runs in two modes:

- Migration wizard with a graphical interface
- Migration utility which uses a command line interface

Migration Wizard GUI

Zimbra PST Migration Wizard is an application that helps users migrate their **PST** files to Zimbra Collaboration Server using a very intuitive interface.

The tool has 4 phases:

Source

Locate and select the **PST** file to migrate to Zimbra Collaboration Server.

Destination

Enter login credentials associated with Zimbra Collaboration Server.

Options

Specify folders, items, and other available options for migration.

Results

View migration status, including progress, errors, and warnings.

Source Information

1. Click **Source**.
2. Click  beside **PST File** field to open a file browser window.
3. Navigate to and choose the **PST** file to migrate to Zimbra Collaboration Server.
4. Choose a log detail level. Logs are written to folder **%temp%/ZimbraMigration** and are useful for diagnosing migration issues. Support may request logs when you require assistance. We recommend that you set the log level to **Verbose** while becoming familiar with the tool.

 Logs are automatically deleted after seven days to conserve disk space, so take backup copies if you require assistance after seven days of performing a migration. During migration, you can open a log file by clicking **Open Log File** on the **Results** page.

5. Click **Next**.

Destination Information

An administrator creates the account for you on the Zimbra Collaboration Server and gives you the migration tool application and the following information which you need to migrate your **PST** files.

1. In the **Destination** dialog, box, enter below details.

Hostname

This is the domain name of the Zimbra server.

Port

The port number used by the server is usually **80** for non-secure connections and **443** for secure connections.

Use Secure Connection

Select the option for SSL secure communication with ZCS.

Username

Enter your ZCS account email address as **name@domain.com**.

Password

Enter your ZCS account password.

2. Click **Next**.

Selecting Options to Migrate

1. Under **Item Types**, choose items to import.
2. Choose **Additional Folders** to migrate **Sent**, **Deleted Items** (Trash), and **Junk** (Spam) folders.
3. **Filters:** Choose below filter options to skip unwanted **PST** items during migration.
 - **Migrate On or After:** This option filters out messages from before the provided date. The tool skips the migration of messages before this date.
 - **Maximum message size:** The message size includes the message and attachments. Leave the field blank to use the Zimbra Collaboration server setting for maximum message size.
 - If you set a value here, this value cannot be larger than the global MTA setting for the maximum size of a message. The default maximum message size is 0 (indicating no size limit).



Setting **0** as maximum size does not override the limits specified in the Zimbra Collaboration server.

Skip these folders, and their children (separate with a comma)

Enter names of folders, and all its subfolders, separated by a comma, to skip their migration.

Skip previously migrated items

Select this box to skip migration of Previously migrated items.



You can view and change the Maximum size of a message value from the Administration Console **Configure** → **Global Settings** → **MTA** tab.

4. Click **Save** to save configuration information in a file which can be loaded later using the Load button on the [Source Information](#) page when you next run the migration tool.
5. Click **Back** to go back and change specifics in [Source Information](#) or [Destination Information](#).
6. Click **Migrate** to begin the migration process.

Viewing Migration Results

In the Results dialog, view the migration status of the **PST** file, including progress, errors, and warnings.

To view the results log, double click your account. A new tab opens and displays the account log information.

Account

This shows the migration status. The progress bar shows the state of the migration, accompanied by status messages. **Min/Avg/Max** are the minimum, average and maximum times (in milliseconds) to migrate items in that account. Read/Write indicate proportionally how much time is spent reading data from the source vs. writing data to the Zimbra Collaboration server. These figures are useful for detecting network/server bottlenecks. For example, 90%:10% would indicate the source is the bottleneck.

- Double-click your account name in Accounts, and an individual tab shows folder-by-folder migration status, along with folder-by-folder bottleneck statistics mentioned above. Click X on the appropriate tab to close view.

Open Log File

Opens the log file associated with your **PST** file's migration. The Log files are at **%temp%\ZimbraMigration\Logs*.log**. Each migration generates several log files. ***migrate.log** contains overall migration session data. ***migrate-SUMMARY.log** contains a summary of key events from the migration session. In addition there will be one log for each account migrated—***migrate [src-account-name] to [dest-account-name].log**.

Stop

Click Stop to stop the migration. To restart, go back to the previous view, and click the Migrate button.

Exit

Click Exit to close the migration tool.

Migration Wizard CLI

Zimbra PST Migration Wizard also has a command line interface to help users migrate their **PST** files to Zimbra Collaboration Server using one command with multiple, intuitively named, arguments.

The command requires a configuration file (**XML**) and a **PST** file.

Creating Configurations file

1. Launch Zimbra Collaboration.
2. Specify [Source Information](#).
3. Specify [Destination Information](#).
4. [Select options](#) applicable to current migration.



Options chosen here can be overridden by specifying the arguments available in the command line utility.

5. Once done, click **Save** to save the above configurations as an **XML** file.

Running the Utility

Format

```
ZimbraMigrationConsole ConfigxmlFile=<path to XML file> [arg1] [arg2]
```

Example

```
ZimbraMigrationConsole ConfigxmlFile=../Config.xml Calendar=true Contacts=true
```

Explanation

The tool migrates Calendar and Contacts from the PST mentioned in the **XML** file



The tool accepts multiple other arguments which are precisely like when [selecting options](#) to migrate. Run the utility with **-Help** as a switch to see all supported arguments.



Arguments, when specified in the command line utility, override options selected while creating the configurations file.

Once the command runs successfully, the console displays the status of the migration.

Managing Configuration

The ZCS components are configured during the initial installation of the software. After the installation, you can manage the following components from either the Administration Console or using the CLI utility.

Help is available from the Administration Console about how to perform tasks from the Administration Console. If the task is only available from the CLI, see [Zimbra CLI Commands](#) for a description of how to use the CLI utility.

Global Configuration

Global Settings apply to all accounts in the Zimbra servers. They are initially set during installation. You can modify the settings from the Administration Console.

Configurations set in Global Settings define inherited default values for the following objects: server, account, COS, and domain. If these attributes are set in the server, the server settings override the global settings.

Admin Console:

To configure global settings, navigate to:

Home > Configure > Global Settings

Configured global settings are:

- Default domain
- Maximum number of results returned for GAL searches. Default = 100.
- User views of email attachments and attachment types not permitted.
- Configuration for authentication process, Relay MTA for external delivery, DNS lookup, and protocol checks.
- Spam check controls and anti-virus options to check messages received.
- Free/busy scheduling across a mix of Zimbra Collaboration servers and third party email servers.
- Customization of themes: modify colors and add your logo.
- Configuration of company name display for external guest log on, when viewing a shared Briefcase folder.
- Backup default directory and backup notification information.
- Global HSM schedule that defines when messages should be moved to a secondary storage space.
- View of current Zimbra license information, license updating, and view the number of accounts created.

General Information Configuration

Admin Console:

Home > Configure > Global Settings

Use the **General Information** screen to view and set global parameters for servers that have been installed and enabled.



Settings defined at the server(s) override those configured in the General Information screen.

1. Modify parameters, as appropriate for your requirements.
2. From the **Gear** icon, select **Save** to use your settings.

Table 21. General Information Parameters

Option	Description
Most results returned by GAL search	The maximum number of GAL results returned from a user search. This value can be set by domain: the domain setting overrides the global setting. Default = 100.
Default domain	Domain that users' logins are authenticated against.

Option	Description
Number of scheduled tasks that can run simultaneously	<p>Number of threads used to fetch content from remote data sources. * If set too low, users do not get their mail from external sources pulled down often enough. * If set too high, the server may be consumed with downloading this mail and not servicing "main" user requests.</p> <p>Default = 20</p>
Sleep time between subsequent mailbox purges	<p>The duration of time that the server should "rest" between purging mailboxes. If the message purge schedule is set to 0, messages are not purged, even if the mail, trash and spam message life time is set.</p> <p>Default = message purge is scheduled to run every 1 minute.</p>
Maximum size of an uploaded file for Briefcase files (KB)	<p>The maximum size of a file that can be uploaded into Briefcase.</p> <p> The maximum message size for an email message and attachments that can be sent is configured in the Home > Configure > Global Settings > MTA page, Messages section.</p>
Admin Help URL Delegated Admin Help URL	To use the Zimbra Collaboration Help, you can designate the URL that is linked from the Administration Console Help

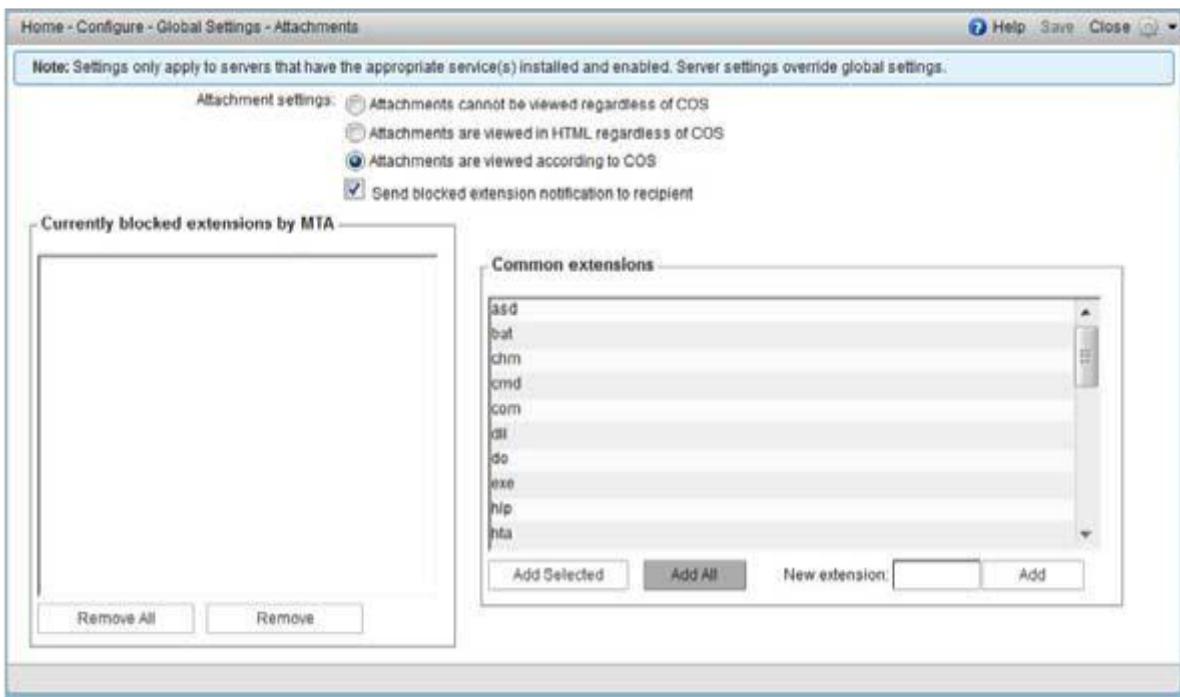
Attachments Configuration

Setting Up Email Attachment Rules

Global email attachment settings allow you to specify global rules for handling attachments to an email message. You can also set rules by COS and for individual accounts. When attachment settings are configured in Global Settings, the global rule takes precedence over COS and Account settings.

Admin Console:

[Home > Configure > Global Settings > Attachments](#)



See [Blocking Email Attachments by File type](#) for information about this section of the screen.

Table 22. Global Settings Advanced

Option	Description
Attachments cannot be viewed regardless of COS	Users cannot view any attachments. This global setting can be set to prevent a virus outbreak from attachments, as no mail attachments can be opened.
Attachments are viewed in HTML regardless of COS	Email attachments can only be viewed in HTML. The COS may have another setting but this global setting overrides the COS setting.
Attachments are viewed according to COS	This global setting states the COS sets the rules for how email attachments are viewed
Send blocked extension notification to recipient	

Blocking Email Attachments by File Type

You can also reject messages with certain types of files attached. You select which file types are unauthorized from the **Common extensions** list. You can also add other extension types to the list. Messages with those type of files attached are rejected. By default the recipient and the sender are notified that the message was blocked.

If you do not want to send a notification to the recipient when messages are blocked, you can disable this option.

Admin Console:

Home > Configure > Global Settings > Attachments

MTA Configuration

Use options from the MTA page to enable or disable authentication and configure a relay hostname, the maximum message size, enable DNS lookup, protocol checks, and DNS checks.

Admin Console:

Home > Configure > Global Settings > MTA

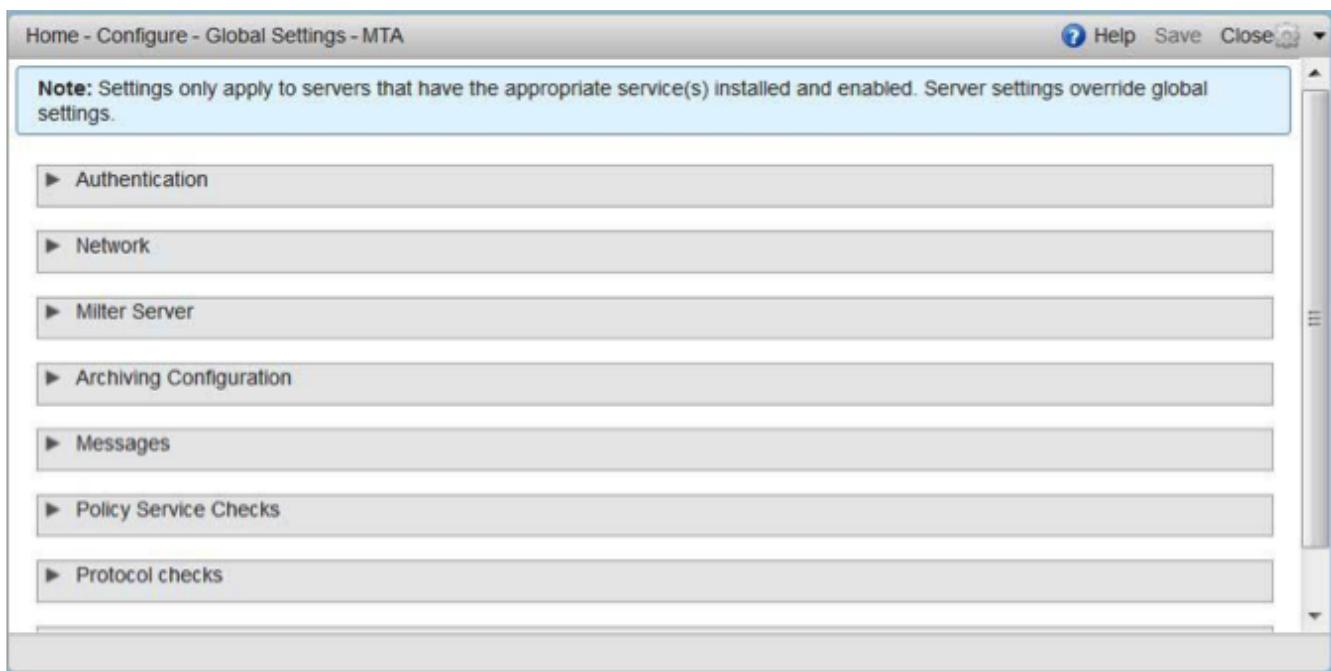


Table 23. MTA Page Options

Option	Description
Authentication	<ul style="list-style-type: none">• Authentication should be enabled, to support mobile SMTP authentication users so that their email client can talk to the Zimbra MTA.• TLS authentication only forces all SMTP auth to use Transaction Level Security to avoid passing passwords in the clear.

Option	Description
Network	<ul style="list-style-type: none"> • Web mail MTA Host name and Web mail MTA Port. The MTA that the web server connects to for sending mail. The default port number is 25. • The Relay MTA for external delivery is the relay host name. This is the Zimbra MTA to which Postfix relays non-local email. • If your MX records point to a spam-relay or any other external non-Zimbra server, enter the name of that server in the Inbound SMTP host name field. This check compares the domain MX setting against the <code>zimbraInboundSmtphostname</code> setting, if set. If this attribute is not set, the domain MX setting is checked against <code>zimbraSmtphostname</code>. • MTA Trusted Networks. Configure trusted networks that are allowed to relay mail. Specify a list of network addresses, separated by commas and/or a space. • If Enable DNS lookups is checked, the Zimbra MTA makes an explicit DNS query for the MX record of the recipient domain. If this option is disabled, set a relay host in the Relay MTA for external delivery. • If Allow domain administrators to check MX records from Administration Console is checked, domain administrators can check the MX records for their domain.
Milter Server	<ul style="list-style-type: none"> • If Enable Milter Server is checked, the milter enforces the rules that are set up for who can send email to a distribution list.
Archiving	<ul style="list-style-type: none"> • If you installed the Archiving feature, you can enable it Configuration here.

Option	Description
Messages	<ul style="list-style-type: none"> Set the Maximum messages size for a message and its attachments that can be sent. <p> To set the maximum size of an uploaded file to Briefcase, go to the General Information page.</p> <ul style="list-style-type: none"> You can enable the X-Originating-IP header to messages checkbox. The X-Originating-IP header information specifies the original sending IP of the email message the server is forwarding.
Policy Service	<ul style="list-style-type: none"> Customize zimbraMtaRestriction (restrictions to reject Checks some suspect SMTP clients).
Protocol checks	<ul style="list-style-type: none"> To reject unsolicited commercial email (UCE), for spam control.
DNS checks	<ul style="list-style-type: none"> To reject mail if the client's IP address is unknown, the hostname in the greeting is unknown, or if the sender's domain is unknown. Add other email recipient restrictions to the List of RBLs field. <p> RBL (Real time black-hole lists) can be turned on or off from the Zimbra CLI.</p>

Global IMAP and POP Configuration

Use the IMAP and POP pages to enable global access.

Admin Console:

[Home > Configure > Global Settings > IMAP](#)

[Home > Configure > Global Settings > POP](#)



When you make changes to the IMAP or POP settings, you must restart Zimbra Collaboration before the changes take effect.

IMAP and POP3 polling intervals can be set from the Administration Console COS Advanced page. Default = No polling interval.



If IMAP/POP proxy is set up, ensure that the port numbers are configured correctly.

With POP3, users can retrieve their mail stored on the Zimbra server and download new mail to their computer. The user's POP configuration in their **Preference > Mail** page determines how their messages are downloaded and saved.

Working With Domains

One domain is identified during the installation process. You can add domains after installation. From the Administration Console you can manage the following domain features.

- Global Address List
- Authentication
- Virtual hosts for the domain to establish a default domain for a user login
- Public service host name that is used for REST URLs, commonly used in sharing.
- Maximum number of accounts that can be created on the domain
- Free/Busy Interop settings for use with Microsoft Exchange.
- Domain SSL certificates

A domain can be renamed and all account, distribution list, alias and resource addresses are changed to the new domain name. The CLI utility is used to changing the domain name. See [Renaming a Domain](#).



Domain settings override global settings.

Domain General Information Configuration

Use the **New Domain** Wizard to set options described in this section.

Admin Console:

Home > 2 Set up Domain > 1. Create Domain...

New Domain

General Information

GAL Mode Settings
SSO
Authentication Mode
Virtual Hosts
Advanced Feature
Domain Configuration Complete

General Information

Domain name: *
 Public service host name:
 Public service protocol:
 Public service port:

Info If your MX records point to a spam-relay or any other external non-zimbra server, enter the name of that server in "Inbound SMTP host name" field.

Inbound SMTP host name:
 Description:
 Default Class of Service:
 Status:
 Notes:

Cancel Previous Next Finish Help

Table 24. New Domain—General Information

Option	Description
Domain name *	Enter the host name of the REST URL. This is commonly used for sharing. See Setting up a Public Service Host
Public service host name	Select HTTP or HTTPS from the drop-down field.
Public service protocol	
Inbound SMTP host name	If your MX records point to a spam-relay or any other external non-Zimbra server, enter the name of the server here.
Description	
Default Class of Service	This COS (for the domain) is automatically assigned to accounts created on the domain if another COS is not set.

Option	Description
Status	<p>The domain status is active in the normal state. Users can log in and mail is delivered. Changing the status can affect the status for accounts on the domain also. The domain status is displayed on the Domain > General page. Domain status can be set as follows:</p> <ul style="list-style-type: none"> • Active. Active is the normal status for domains. Accounts can be created and mail can be delivered. <p> If an account has a different status setting than the domain setting, the account status overrides the domain status.</p> <ul style="list-style-type: none"> • Closed. When a domain status is marked as closed, login for accounts on the domain is disabled and messages are bounced. The closed status overrides an individual account's status setting. • Locked. When a domain status is marked as locked, users cannot log in to check their email, but email is still delivered to the accounts. If an account's status setting is marked as maintenance or closed, the account's status overrides the domain status setting. • Maintenance. When the domain status is marked as maintenance, users cannot log in and their email is queued at the MTA. If an account's status setting is marked as closed, the account's status overrides the domain status setting. • Suspended. When the domain status is marked as suspended, users cannot log in, their email is queued at the MTA, and accounts and distribution lists cannot be created, deleted, or modified. If an account's status setting is marked as closed, the account's status overrides the domain status setting.

Setting up a Public Service Host Name

You can configure each domain with the public service host name to be used for REST URLs. This is the URL that is used when sharing email folders and Briefcase folders, as well as sharing task lists, address books, and calendars.

When users share a Zimbra Collaboration folder, the default is to create the URL with the Zimbra server hostname and the Zimbra service host name. This is displayed as <https://server.domain.com/service/home/username/sharedfolder>. The attributes are generated as follows:

- Hostname is server.zimbraServiceHostname
- Protocol is determined from server.zimbraMailMode
- Port is computed from the protocol

When you configure a public service host name, this name is used instead of the server/service name, as <https://publicservicename.domain.com/home/username/sharedfolder>. The attributes to be used are:

- zimbraPublicServiceHostname
- zimbraPublicServiceProtocol
- zimbraPublicServicePort

You can use another FQDN as long as the name has a proper DNS entry to point at 'server' both internally and externally.

Global Address List (GAL) Mode Configuration

The Global Address List (GAL) is your company-wide listing of users that is available to all users of the email system. GAL is a commonly used feature in mail systems that enables users to look up another user's information by first or last name, without having to know the complete email address.

GAL is configured on a per-domain basis. The GAL mode setting for each domain determines where the GAL lookup is performed.

Use the **GAL Mode Settings** tool with your domain configuration to define the Global Address List.

Admin Console:

Home > 2 Set up Domain > 1 Create Domain... → GAL Mode Settings

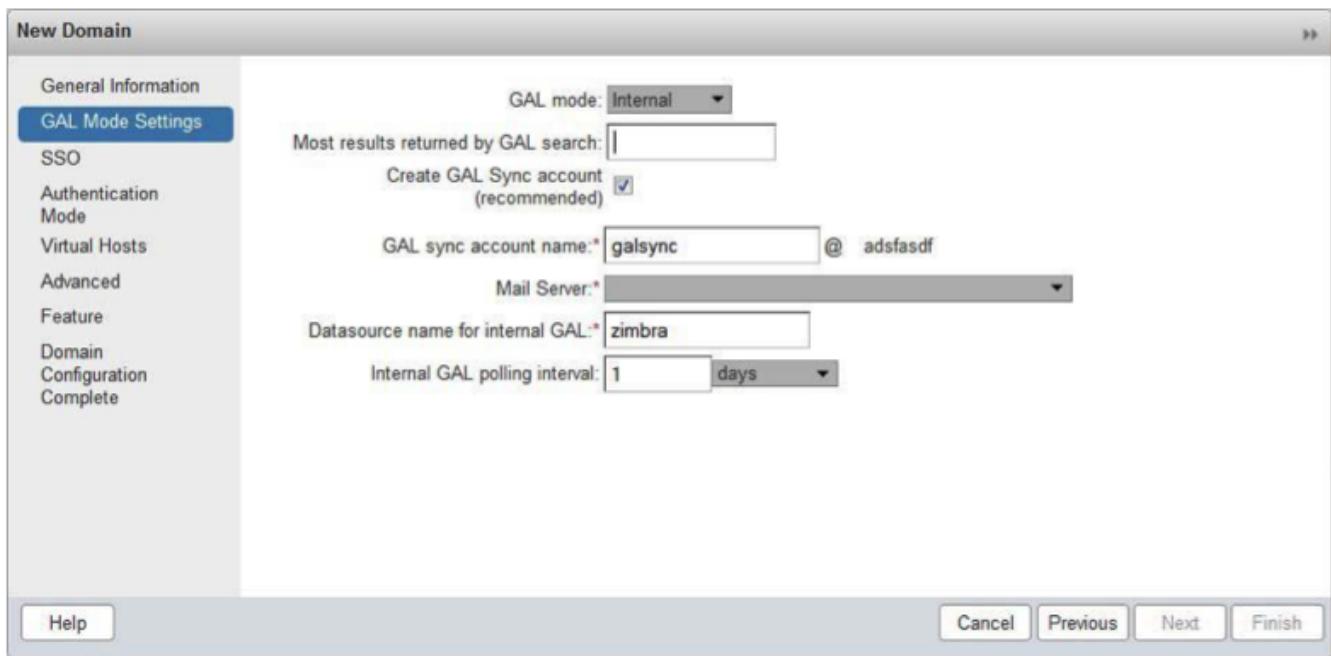


Table 25. New Domain — GAL Mode Settings

Option	Description
GAL Mode	<ul style="list-style-type: none"> Internal. The Zimbra LDAP server is used for directory lookups. External. External directory servers are used for GAL lookups. You can configure multiple external LDAP hosts for GAL. All other directory services use the Zimbra LDAP service (configuration, mail routing, etc.). When you configure an external GAL, you can configure different search settings and sync settings. You might want to configure different search settings if your LDAP environment is set up to optimize LDAP searching by setting up an LDAP cache server, but users also will need to be able to sync to the GAL. Both. Internal and external directory servers are used for GAL lookups.
Most results returned by GAL search	Maximum number of search results that can be returned in one GAL search. If this value is undefined here, the system will use the value defined in Global Settings. Default = 100 results.
GAL sync account name*	Read-only field that displays the galsync name and associated domain.

Option	Description
Datasource name for internal GAL	Read-only field that displays the name of the internal GAL.
Internal GAL polling interval	Define how often—as days, hours, minutes, or seconds—the GAL sync account is to sync with the LDAP server. With the first sync to the LDAP server, all GAL contacts from the LDAP are added to the galsync account's address book. On subsequent syncs, the account is updated with information about new contacts, modified contacts, and deleted contacts.

Using GAL sync accounts for faster access to GAL

A GAL sync account is created for the domain when an internal or external GAL is created, and if you have more than one mailbox server, you can create a GAL sync account for each mailbox server in the domain. Using the GAL sync account gives users faster access to auto complete names from the GAL.

When a GAL sync account is created on a server, GAL requests are directed to the server's GAL sync account instead of the domain's GAL sync account. The GalSyncResponse includes a token which encodes the GAL sync account ID and current change number. The client stores this and then uses it in the next GalSyncRequest. Users perform GAL sync with the GAL sync account they initially sync with. If a GALSsync account is not available for some reason, the traditional LDAP-based search is run.



The GAL sync accounts are system accounts and do not use a Zimbra license.

When you configure the GAL sync account, you define the GAL datasource and the contact data is synced from the datasource to the GAL sync accounts' address books. If the mode **Both** is selected, an address book is created in the account for each LDAP data source.

The GAL polling interval for the GAL sync determines how often the GALSsync account syncs with the LDAP server. The sync intervals can be in x days, hours, minutes, or seconds. The polling interval is set for each data source.

When the GAL sync account syncs to the LDAP directory, all GAL contacts from the LDAP are added to the address book for that GAL. During the sync, the address book is updated with new contact, modified contact and deleted contact information. You should not modify the address book directly. When the LDAP syncs the GAL to the address book, changes you made directly to the address book are deleted.

You create GALSsync accounts from the Administration Console. The CLI associated with this feature is **zmgsautil**.

Creating Additional GALsync Accounts

When ZCS is configured with more than one server, you can add an additional GAL sync account for each server.

Admin Console:

Home > Configure > Domains

1. Select the domain to add another GAL sync account.
2. In the **Gear** icon, select **Configure GAL**.
3. Click **Add a GAL account**.
4. In the GAL sync account name field, enter the name for this account. Do not use the default name.
5. Select the mailbox server that this account will apply to.
6. Enter the **GAL datasource name**, If the GAL mode is BOTH, enter the data source name for both the internal GAL and the external GAL.
7. Set the **GAL polling interval** to how often the GAL sync account should sync with the LDAP server to update.
8. Click **Finish**.

Changing GAL sync account name

The default name for the GAL sync account is **galsync**. When you configure the GAL mode, you can specify another name. After the GAL sync account is created, you cannot rename the account because syncing the data fails.

To change the account name delete the existing GAL sync account and configure a new GAL for the domain.

Admin Console:

Home > Configure > Domains

1. Select the domain where you want to change the GAL sync account name.
2. In the **Gear** icon, select **Configure GAL** to open the configuration wizard and change the GAL mode to internal. Do not configure any other fields. Click **Finish**.
3. In the domain's account Content pane, delete the domain's galsync account.
4. Select the domain again and select Configure GAL to reconfigure the GAL. In the GAL sync account name field, enter the name for the account. Complete the GAL configuration and click **Finish**. The new account is displayed in the Accounts Content pane.

Authentication Modes

Authentication is the process of identifying a user or a server to the directory server and granting access to legitimate users based on user name and password information provided when users log in.

Set the authentication method on a per-domain basis.

Admin Console:

Home > 2 Set up Domain > 1 Create Domain... → Authentication Mode

Table 26. New Domain—Authentication Mode

Option	Description
Authentication mechanism	<ul style="list-style-type: none">Internal. The Internal authentication uses the Zimbra directory server for authentication on the domain. When you select Internal, no other configuration is required.External LDAP. The user name and password is the authentication information supplied in the bind operation to the directory server. You must configure the LDAP URL, LDAP filter, and to use DN password to bind to the external server.External Active Directory. The user name and password is the authentication information supplied to the Active Directory server. You identify the Active Directory domain name and URL.

Virtual Hosts

Virtual hosting allows you to host more than one domain name on a server. The general domain configuration does not change.

When you create a virtual host, this becomes the default domain for a user login. Zimbra Web Client users can log in without having to specify the domain name as part of their user name.

Admin Console:

Home > 2 Set up Domain > 1 Create Domain... → Virtual Hosts

Table 27. New Domain—Virtual Hosts

Option	Description
Add virtual host	Alphanumeric string to identify the virtual host(s) for this domain. The virtual host requires a valid DNS configuration with an A record. To delete a virtual host from the domain, click Remove alongside the host name displayed in this wizard screen.

To open the Zimbra Web Client log in page, users enter the virtual host name as the URL address. For example, <https://mail.company.com>.

When the Zimbra login screen displays, users enter only their user name and password. The authentication request searches for a domain with that virtual host name. When the virtual host is found, the authentication is completed against that domain.

Setting Account Limits

You can limit the number of accounts that can be provisioned on a domain. The maximum number of accounts that can be provisioned for the domain can be set when the domain is created. You can also edit the domain configuration to add or change the number.

In the Administration Console this is set for a domain in the Account Limits page. If this page is not configured, no limits on the domain are set.

Resources, spam, and ham accounts are not counted against this limit.



You cannot exceed the account limit set by the Zimbra Collaboration license.

When multiple Classes of Service (COS) are available, you can select which classes of service can be configured and how many accounts on the domain can be assigned to the COS. This is configured in the domain's Account Limits page. The number of COS account types used is tracked. The limits for all COSS cannot exceed the number set for the maximum accounts for the domain.

The number of COS assigned to accounts is tracked. You can see the number assigned/number remaining from any account's General Information page.

Renaming a Domain

When you rename a domain you are actually creating a new domain, moving all accounts to the new domain and deleting the old domain. All account, alias, distribution list, and resource addresses are changed to the new domain name. The LDAP is updated to reflect the changes.

Before you rename a domain

- Make sure MX records in DNS are created for the new domain name
- Make sure you have a functioning and current full backup of the domain

After the domain has been renamed

- Update external references that you have set up for the old domain name to the new domain name. This may include automatically generated emails that were sent to the administrator's mailbox such as backup session notifications. Immediately run a full backup of the new domain:

```
zmprov -l rd [olddomain.com] [newdomain.com]
```

Domain Rename Process

When you run this `zmprov` command, the domain renaming process goes through the following

steps:

1. The status of the old domain is changed to an internal status of shutdown, and mail status of the domain is changed to suspended. Users cannot login, their email is bounced by the MTA, and accounts, calendar resources and distribution lists cannot be created, deleted or modified.
2. The new domain is created with the status of shutdown and the mail status suspended.
3. Accounts, calendar resources, distribution lists, aliases, and resources are all copied to the new domain.
4. The LDAP is updated to reflect the new domain address.
5. The old domain is deleted.
6. The status for the new domain is changed to active. The new domain can start accepting email messages.

Adding a Domain Alias

A domain alias allows different domain names to direct to a single domain address. For example, your domain is domain.com, but you want users to have an address of example.com, you can create example.com as the alias for the domain.com address. Sending mail to user@example.com is the same as sending mail to user@domain.com.



A domain alias is a domain name just like your primary domain name. You must own the domain name and verify your ownership before you can add it as an alias.

Admin Console:

Home > Configure > Domains, from the Gear icon select, **Add a Domain Alias**.

Enabling Support for Domain Disclaimers

Disclaimers are set per-domain. When upgrading, an existing global disclaimer is converted to domain specific disclaimers on every domain to preserve behavior with previous releases.

Per domain disclaimer support can be enabled using the following steps:

1. Create a new domain (e.g. example.com) and account (e.g. user2@example.com).

```
$ zmprov cd example.com cb9a4846-6df1-4c18-8044-4c1d4c21ccc5  
$ zmprov ca user2@example.com test123 95d4caf4-c474-4397-83da-aa21de792b6a  
$ zmprov -l gaa user1@example.com user2@example.com
```

2. Enable the use of disclaimers

```
$ zmprov mcf zimbraDomainMandatoryMailSignatureEnabled TRUE  
$ zmprov gcf zimbraDomainMandatoryMailSignatureEnabled  
zimbraDomainMandatoryMailSignatureEnabled: TRUE
```

3. Add disclaimers to the new domain

```
$ zmprov md example.com  
zimbraAmavisDomainDisclaimerText "text disclaimer"  
zimbraAmavisDomainDisclaimerHTML "HTML disclaimer"  
  
$ zmprov gd example.com zimbraAmavisDomainDisclaimerText  
zimbraAmavisDomainDisclaimerHTML  
# name example.com  
zimbraAmavisDomainDisclaimerHTML: HTML disclaimer  
zimbraAmavisDomainDisclaimerText: text disclaimer  
  
$ zmprov gd eng.example.com  
# name eng.example.com  
zimbraAmavisDomainDisclaimerText  
zimbraAmavisDomainDisclaimerHTML
```

a. On the first MTA:

```
/opt/zimbra/libexec/zmaltermimeconfig -e example.com  
  
Enabled disclaimers for domain: example.com  
Generating disclaimers for domain example.com.
```

b. On all additional MTAs:

```
/opt/zimbra/libexec/zmaltermimeconfig
```

- To test, send an email from the account (e.g. user2@example.com) in html and plain text format
- To verify, check emails received with correct HTML disclaimer and plain text disclaimer.
- To disable for the domain example.com

1. On the first MTA, as the Zimbra user:

```
/opt/zimbra/libexec/zmaltermimeconfig -d example.com
```

2. On all additional MTAs:

```
/opt/zimbra/libexec/zmaltermimeconfig
```

Disabling Disclaimers for Intra-domain Emails

You can enable the option for emails between individuals in the same domain to not have a disclaimer attached.

Set the attribute `attachedzimbraAmavisOutboundDisclaimersOnly` to `TRUE`.

To preserve backward-compatibility, this attribute defaults to `FALSE`.

Disabling the Disclaimer Feature

It is possible to completely remove support for disclaimers by setting the related attribute to `FALSE`.

```
zmprov mcf zimbraDomainMandatoryMailSignatureEnabled FALSE
```

Zimlets on the Domain

All Zimlets that are deployed are displayed in the domain's **Zimlets** page. If you do not want all the deployed Zimlets made available for users on the domain, select from the list the Zimlets that are available for the domain. This overrides the Zimlet settings in the COS or for an account.

Managing Server Settings

A server is a machine that has one or more of the Zimbra service packages installed. During the installation, the Zimbra server is automatically registered on the LDAP server.

In the Administration Console, you can view the current status of all the servers that are configured with Zimbra software, and you can edit or delete existing server records. You cannot add servers directly to LDAP. The Zimbra Collaboration installation program must be used to add new servers because the installer packages are designed to register the new host at the time of installation.

The server settings that can be viewed from the Administration Console, Configure Servers link for a specific server include:

- General information about the service host name, and LMTP advertised name and bind address, and the number of threads that can simultaneously process data source imports.
- A list of enabled services. You can disable and enable the services.
- Authentication types enabled for the server, setting a Web mail MTA host-name different from global. Setting relay MTA for external delivery, and enabling DNS lookup if required. Enable the Milter Server and set the bind address.
- Enabling POP and IMAP and setting the port numbers for a server. If IMAP/POP proxy is set up, making sure that the port numbers are configured correctly.
- Index and message volumes configuration. Setting HSM policies.
- IP Address Bindings. If the server has multiple IP addresses, IP Address binding allows you to specify which interface to bind to.
- Proxy settings if proxy is configured.

- Backup and Restore configuration for the server. When backup and restore is configured for the server, this overrides the global backup and restore setting.

Servers inherit global settings if those values are not set in the server configuration. Settings that can be inherited from the Global configuration include MTA, SMTP, IMAP, POP, anti-virus, and anti-spam configurations.

General Server Settings

The General Information page includes the following configuration information:

- Server display name and a description field
- Server hostname
- LMTP information including advertised name, bind address, and number of threads that can simultaneously process data source imports.
Default = 20 threads.
- Purge setting. The server manages the message purge schedule. You configure the duration of time that the server should "rest" between purging mailboxes from the Administration Console, Global settings or Server settings, or General Information page.
Default = message purge is scheduled to run each minute.

When installing a reverse proxy the communication between the proxy server and the backend mailbox server must be in plain text. Checking **This server is a reverse proxy lookup target** automatically sets the following parameters:

```
zimbraImapCleartextLoginEnabled TRUE
zimbraReverseProxyLookupTarget TRUE
zimbraPop3CleartextLoginEnabled TRUE
```

The Notes text box can be used to record details you want to save.

Change MTA Server Settings

Admin Console:

Home > Configure > Servers → *server* → MTA

The **MTA** page shows the following settings:

- Authentication enabled.

Enables SMTP client authentication, so users can authenticate. Only authenticated users or users from trusted networks are allowed to relay mail. TLS authentication when enabled, forces all SMTP auth to use Transport Layer Security (successor to SSL) to avoid passing passwords in the clear.

- Network settings, including Web mail MTA hostname, Web mail MTA time-out, the relay MTA for external delivery, MTA trusted networks ID, and the ability to enable DNS lookup for the

server.

- Milter Server.

If **Enable Milter Server** is checked, the milter enforces the rules that are set up for who can send email to a distribution list on the server.

Setting Up IP Address Binding

If the server has multiple IP addresses, you can use IP address binding to specify which specific IP addresses you want a particular server to bind to.

Admin Console:

Home > Configure > Servers → *server* → IP Address Bindings

Table 28. IP Address Bindings

Option	Description
Web Client Server IP Address	Interface address on which the HTTP server listens
Web Client Server SSL IP Address	Interface address on which the HTTPS server listens
Web Client Server SSL Client Cert IP Address	Interface address on which HTTPS server accepting the client certificates listen
Administration Console Server IP Address	Administrator console Interface address on which HTTPS server listens

Managing SSL Certificates for ZCS

A certificate is the digital identity used for secure communication between different hosts or clients and servers. Certificates are used to certify that a site is owned by you.

Two types of certificates can be used - self-signed and commercial certificates.

- A **self-signed certificate** is an identity certificate that is signed by its own creator.

You can use the Certificate Installation Wizard to generate a new self-signed certificate. This is useful when you use a self-signed certificate and want to change the expiration date. Self-signed certificates are normally used for testing.

Default = 1825 days (5 years)

- A **commercial certificate** is issued by a certificate authority (CA) that attests that the public key contained in the certificate belongs to the organization (servers) noted in the certificate.

When Zimbra Collaboration Server is installed, the self-signed certificate is automatically installed and can be used for testing Zimbra Collaboration Server. You should install the commercial certificate when Zimbra Collaboration Server is used in your production environment.



ZCO users in a self-signed environment will encounter warnings about connection security unless the root CA certificate is added to the client's Window Certificate Store. See the [Zimbra Wiki](#) article [ZCO Connection Security](#) for more information.

Installing Certificates

To generate the Certificate Signing Request (CSR) you complete a form with details about the domain, company, and country, and then generate a CSR with the RSA private key. You save this file to your computer and submit it to your commercial certificate authorizer.

To obtain a commercially signed certificate, use the Zimbra Certificates Wizard in the Administration Console to generate the RSA Private Key and CSR.

Admin Console:

Home > 1 Get Started > 2. Install Certificates

Use guidelines from the Install Certificates table to set parameters for your certificates.

Table 29. Install Certificates

Option	Description
Common Name (CN)	Exact domain name that should be used to access your Web site securely. Are you going to use a wildcard common name? If you want to manage multiple sub domains on a single domain on the server with a single certificate, check this box. An asterisk (*) is added to the Common Name field.
Country Name (C)	Country name you want the certificate to display as our company location
State/Province (ST)	State/province you want the certificate to display as your company location.
City (L)	City you want the certificate to display as your company location.
Organization Name (O)	Your company name
Organization Unit (OU)	Unit name (if applicable)
Subject Alternative Name (SAN)	If you are going to use a SAN, the input must be a valid domain name. When SAN is used, the domain name is compared with the common name and then to the SAN to find a match. You can create multiple SANs. When the alternate name is entered here, the client ignores the common name and tries to match the server name to one of the SAN names.

Download the CSR from the Zimbra server and submit it to a Certificate Authority, such as VeriSign

or GoDaddy. They issue a digitally signed certificate.

When you receive the certificate, use the Certificates Wizard a second time to install the certificate on the Zimbra Collaboration. When the certificate is installed, you must restart the server to apply the certificate.

Viewing Installed Certificates

You can view the details of certificates currently deployed. Details include the certificate subject, issuer, validation days and subject alternative name.

Admin Console:

Home > Configure > Certificates → zmhostname

Certificates display for different Zimbra services such as LDAP, mailboxd, MTA and proxy.

Maintaining Valid Certificates

It is important to keep your SSL certificates valid to ensure clients and environments work properly, as the ZCS system can become non-functional if certificates are allowed to expire. You can view deployed SSL certificates from the ZCS administrator console, including their validation days. It is suggested that certificates are checked periodically, so you know when they expire and to maintain their validity.

Install a SSL Certificate for a Domain

You can install an SSL certificate for each domain on a Zimbra Collaboration server. Zimbra Proxy must be installed on Zimbra Collaboration and correctly configured to support multiple domains. For each domain, a virtual host name and Virtual IP address are configured with the virtual domain name and IP address.

Each domain must be issued a signed commercial certificate that attests that the public key contained in the certificate belongs to that domain.

Configure the Zimbra Proxy Virtual Host Name and IP Address.

```
zmprov md <domain> +zimbraVirtualHostName {domain.example.com} +zimbraVirtualIPAddress {1.2.3.4}
```



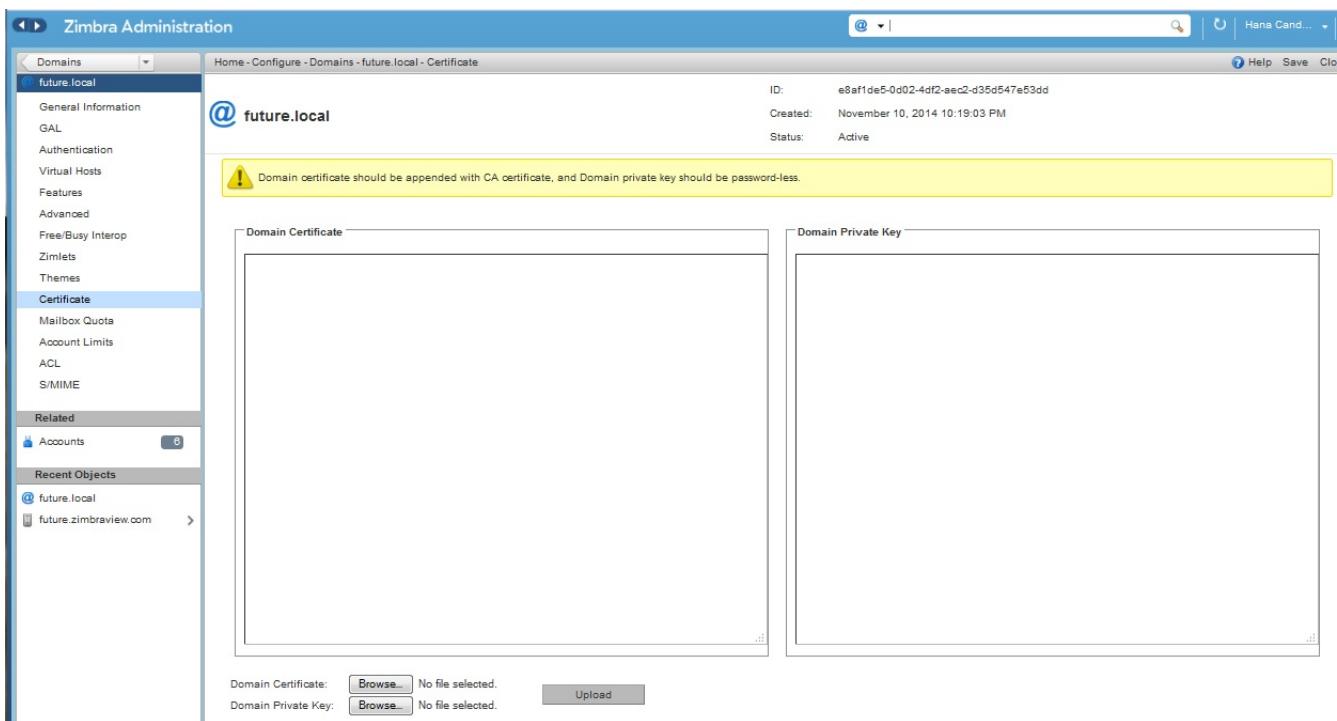
The virtual domain name requires a valid DNS configuration with an A record.

Edit the certificate for the domain:

Admin Console:

Home > 1 Get Started > 2. Install Certificates

Copy the domain's issued signed commercial certificate's and private key files to the **Domain Certificate** section for the selected domain.



1. Copy the root certificate and the intermediate certificates in descending order, starting with your domain certificate. This allows the full certificate chain to be validated.
2. Remove any password (passphrase) from the private key before the certificate is saved.

See your commercial certificate provider for details about how to remove the password.

3. Click **Upload**.

The domain certificate is deployed to `/opt/zimbra/conf/domaincerts`

Using DKIM to Authenticate Email Message

Domain Keys Identified Mail (DKIM) defines a domain-level authentication mechanism that lets your organization take responsibility for transmitting an email message in a way that can be verified by a recipient. Your organization can be the originating sending site or an intermediary. Your organization's reputation is the basis for evaluating whether to trust the message delivery.

You can add a DKIM digital signature to outgoing email messages, associating the message with a domain name of your organization. You can enable DKIM signing for any number of domains that are being hosted by ZCS. It is not required for all domains to have DKIM signing enabled for the feature to work.

DKIM defines an authentication mechanism for email using

- A domain name identifier
- Public-key cryptography
- DNS-based public key publishing service.

The DKIM signature is added to the email message header field. The header information is similar to the following example.

```
DKIM-Signature a=rsa-sha1; q=dns;
d=example.com;
i=user@eng.example.com;
s=jun2005.eng; c=relaxed/simple;
t=1117574938; x=1118006938;
h=from:to:subject:date;
b=dzdVyOfAKCdlXdJ0c9G2q8LoXS1EniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

Receivers who successfully validate a DKIM signature can use information about the signer as part of a program to limit spam, spoofing, phishing, or other undesirable behavior.

Configure Zimbra Collaboration for DKIM Signing

DKIM signing to outgoing mail is done at the domain level.

To set up DKIM you must run the CLI zmdkimkeyutil to generate the DKIM keys and selector. You then update the DNS server with the selector which is the public key.

1. Log in to the ZCS server and as zimbra:

```
/opt/zimbra/libexec/zmdkimkeyutil -a -d <example.com>
```

The public DNS record data that must be added for the domain to your DNS server is displayed. The public key DNS record appears as a DNS TXT-record that must be added for the domain to your DNS server.

Optional. To specify the number of bits for the new key, include **-b <####>**. If you do not add the **-b**, the default setting is 2048 bits.

```
DKIM Data added to LDAP for domain example.com with selector B534F5FC-EAF5-11E1-A25D-54A9B1B23156
```

Public signature to enter into DNS:

```
B534F5FC-EAF5-11E1-A25D-54A9B1B23156._domainkey IN TXT
"v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC+yCHjGL/mJXEVLRZnxZL/VqaN/Jk9VllvIOTkKgwLS
FtVsKC69kVaUDDjb3zkpJ6qpswjOCO+0eGJZFA4aB4BQjFBHb197vgNnpJq1sV3QzRfHrN8X/gdhvfKSIw
SDFFl3DHewKDWNcCzBkNf5wHt5ujeavz2XogL8HfeL0bTwIDAQA B" ; ----- DKIM B534F5FC-EAF5-
11E1-A25D-54A9B1B23156 for example.com
```

The generated DKIM data is stored in the LDAP server as part of the domain LDAP entry.

2. Work with your service provider to update your DNS for the domain with the DKIM DNS text record.
3. Reload the DNS and verify that the DNS server is returning the DNS record.
4. Verify that the public key matches the private key, See the [Identifiers](#) table for **-d**, **-s**, and **-x**

descriptions.

```
/opt/zimbra/common/sbin/opendkim-testkey -d <example.com> -s <0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB> -x /opt/zimbra/conf/opendkim.conf
```

Table 30. Identifiers

Parameter	Description
-d	Domain name
-s	Selector name
-x	Configuration file name.

Update DKIM Data for a Domain

When the DKIM keys are updated, the DNS server must be reloaded with the new TXT record.

Good practice is to leave the previous TXT record in DNS for a period of time so that email messages that were signed with the previous key can still be verified.

Log in to the ZCS server and as zimbra:

```
/opt/zimbra/libexec/zmdkimkeyutil -u -d <example.com>
```

Optional. To specify the number of bits for the new key, include **-b** in the command line, **-b <#####>**. If you do not add the **-b**, the default setting is 2048 bits.

1. Work with your service provider to update your DNS for the domain with the DKIM DNS text record.
2. Reload the DNS and verify that the DNS server is returning the DNS record.
3. Verify that the public key matches the private key: See the Identifiers table for **-d**, **-s**, and **-x** descriptions.

```
/opt/zimbra/common/sbin/opendkim-testkey -d <example.com> -s <0E9F184A-9577-11E1-AD0E-2A2FBBAC6BCB> -x /opt/zimbra/conf/opendkim.conf
```

Remove DKIM Signing from ZCS

Removing DKIM signing deletes the DKIM data from LDAP. New email message no longer are signed for the domain. When you remove DKIM from the domain, good practice is to leave the previous TXT record in DNS for a period of time so that email messages that were signed with the previous key can still be verified.

Use the following command syntax to remove the file:

```
/opt/zimbra/libexec/zmdkimkeyutil -r -d example.com
```

Retrieve DKIM Data for a Domain

Use the following command syntax to view the stored DKIM information for the domain, selector, private key, public signature and identity:

```
/opt/zimbra/libexec/zmdkimkeyutil -q -d example.com
```

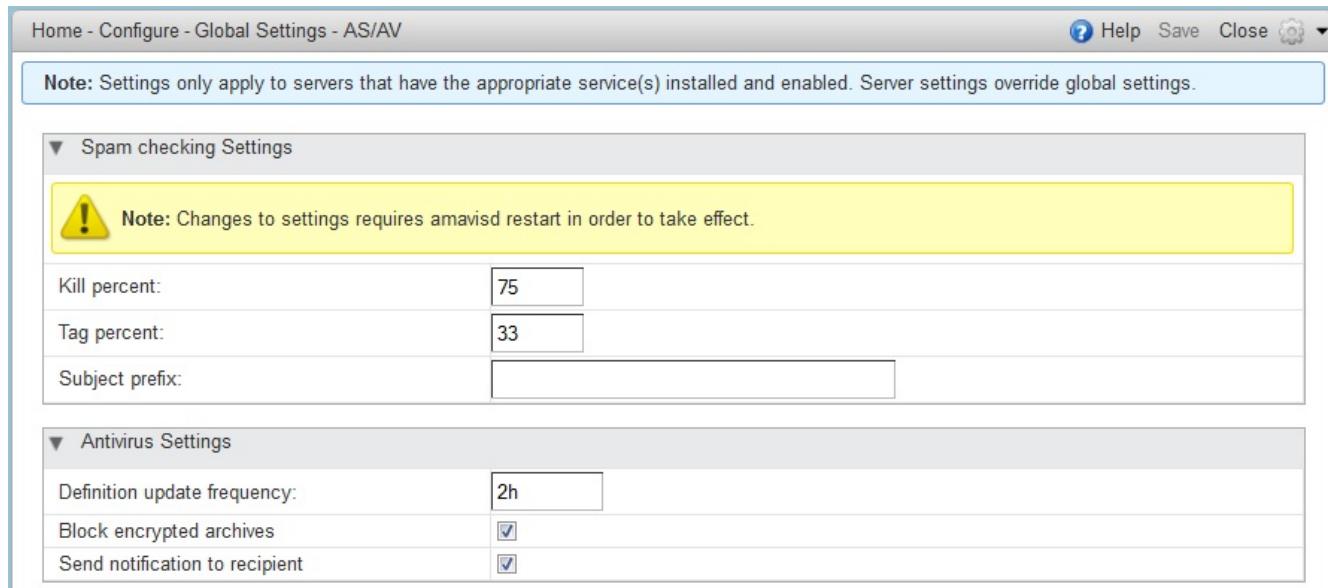
Anti-spam Settings

ZCS uses SpamAssassin to control spam. SpamAssassin uses predefined rules as well as a Bayes database to score messages. Zimbra evaluates spaminess based on percentage. Messages tagged between 33%-75% are considered spam and delivered to the user's junk folder. Messages tagged above 75% are not sent to the user and are discarded.

You can change the anti-spam settings.

Admin Console:

Home > Configure > Global Settings > AS/AV



1. At the Anti-Spam fields, enter parameters, as appropriate for your requirements.
2. From the **Gear** icon, select **Save** to use your settings.

Table 31. Anti-Spam

Option	Description
Kill percent	Percent that scored mail to be considered as spam, and therefore not to be delivered. Default = 75%

Option	Description
Tag percent	Percent that scores mail to be considered as spam, which should be delivered to the Junk folder. Default = 33%
Subject prefix	Text string to be added to the subject line, for messages tagged as spam.

When a message is tagged as spam, the message is delivered to the recipient's junk folder. Users can view the number of unread messages that are in their junk folder and can open the junk folder to review the messages marked as spam. If you have the anti-spam training filters enabled, when users add or remove messages in the junk folder, their action helps train the spam filter.

RBL (Real time black-hole lists) can be turned on or off in SpamAssassin from the Zimbra CLI.

Anti-Spam Training Filters

The automated spam training filter is enabled by default and two feedback system mailboxes are created to receive mail notification.

- **Spam Training User** for mail that was not marked as spam but should be.
- **Non-spam (referred to as ham) training user** for mail that was marked as spam but should not have been.

The mailbox quota and attachment indexing is disabled for these training accounts. Disabling quotas prevents bouncing messages when the mailbox is full.

How well the anti-spam filter works depends on recognizing what is considered spam. The SpamAssassin filter learns from messages that users specifically mark as spam by sending them to their junk folder or not spam by removing them from their junk folder. A copy of these marked messages is sent to the appropriate spam training mailbox.

When ZCS is installed, the spam/ham cleanup filter is configured on only the first MTA. The ZCS spam training tool, **zmtrainsa**, is configured to automatically retrieve these messages and train the spam filter. The **zmtrainsa script** is enabled through a crontab job to feed mail to the SpamAssassin application, allowing SpamAssassin to 'learn' what signs are likely to mean spam or ham. The zmtrainsa script empties these mailboxes each day.

New installs of ZCS limit spam/ham training to the first MTA installed. If you uninstall or move this MTA, you will need to enable spam/ham training on another MTA, as one host should have this enabled to run **zmtrainsa --cleanup**.



To set this on a new MTA server

```
zmlocalconfig -e zmtrainsa_cleanup_host=TRUE
```

Disabling the Spam Training Mailboxes

The ZCS default is that all users can give feedback when they add or remove items from their junk folder.

If you do not want users to train the spam filter you can disable this function.

1. Modify the global configuration attributes, `ZimbraSpamIsSpamAccount` and `ZimbraSpamIsNotSpamAccount`
2. Remove the account addresses from the attributes.

```
zmprov mcf ZimbraSpamIsSpamAccount ''
zmprov mcf ZimbraSpamIsNotSpamAccount ''
```

When these attributes are modified, messages marked as spam or not spam are not copied to the spam training mailboxes.

Manually Training Spam Filters

Initially, you might want to train the spam filter manually to quickly build a database of spam and non-spam tokens, words, or short character sequences that are commonly found in spam or ham. To do this, you can manually forward messages as message/rfc822 attachments to the spam and non-spam mailboxes.

When `zmtrainsa` runs, these messages are used to teach the spam filter. Make sure you add a large enough sampling of messages to get accurate scores. To determine whether to mark messages as spam at least 200 known spams and 200 known hams must be identified.

Protect Alias Domains from Backscatter Spam

To reduce the risk of backscatter spam, you can run a service that runs a Zimbra Access Policy Daemon that validates **RCPT To:** content specifically for alias domains.



For information about creating domain aliases, see the [Zimbra wiki article Managing Domains](#).

1. Set the Postfix LC key.

```
zmlocalconfig -e postfix_enable_smtpd_policyd=yes
```

2. Define the MTA restriction.

```
zmprov mcf +zimbraMtaRestriction "check_policy_service unix:private/policy"
```

The `postfix_policy_time_limit` key is set because by default the Postfix spawn(8) daemon kills its

child process after 1000 seconds. This is too short for a policy daemon that might run as long as an SMTP client is connected to an SMTP process.

Disabling Postfix Policy Daemon

Disable the SMTPD policy.

```
zmlocalconfig -e postfix_enable_smtpd_policyd=no
```

Admin Console:

Home > Configure > Global Settings > MTA

Define the policy restriction. Setting Email Recipient RestrictionsRealtimeBlackhole Lists and Realtime Right-Hand Side Blocking/Black Lists can be turned on or off in the MTA.

For protocol checks, the following three RBLs can be enabled:

- tname
- Client must greet with a fully qualified hostname - `reject_non_fqdn_hostname`
- Sender address must be fully qualified - `reject_non_fqdn_sender`

Hostname in greeting violates RFC - `reject_invalid_host`

```
zmprov mcf -zimbraMtaRestriction "check_policy_service unix:private/policy"
```

The following RBLs can also be set.

- `reject_rbl_client cbl.abuseat.org`
- `reject_rbl_client bl.spamcop.net`
- `reject_rbl_client dnsbl.sorbs.net`
- `reject_rbl_client sbl.spamhaus.org`

As part of recipient restrictions, you can also use the `reject_rbl_client <rbl_hostname>` option.

Admin Console:

Home > Configure > Global Settings > MTA → DNS Checks

Use the DNS tools in MTA configuration to define the restriction lists.

▼ DNS checks	
Client's IP address (reject_unknown_client_hostname)	<input type="checkbox"/>
Hostname in greeting (reject_unknown_reverse_client_hostname)	<input type="checkbox"/>
Sender's domain (reject_unknown_sender_domain)	<input type="checkbox"/>
Client must greet with a resolving hostname (reject_unknown_hello_hostname)	<input type="checkbox"/>
List of Client RBLs:	<input type="text"/>
	Add
List of Client RHSBLs:	<input type="text"/>
	Add
List of Reverse Client RHSBLs:	<input type="text"/>
	Add
List of Sender RHSBLs:	<input type="text"/>
	Add

For a list of current RBL's, see the [Comparison of DNS blacklists](#) article.

Adding RBLs with the CLI

1. View the current RBLs.

```
zmprov gacf zimbraMtaRestriction
```

2. Add new RBLs: list the existing RBLs and the new Add, in the same command entry. For 2-word RBL names, surround the name with quotes in your entry.

```
zmprov mcf zimbraMtaRestriction [RBL type]
```

Example 6. adding all possible restrictions

```
zmprov mcf \
zimbraMtaRestriction reject_invalid_hostname \
zimbraMtaRestriction reject_non-fqdn_hostname \
zimbraMtaRestriction reject_non_fqdn_sender \
zimbraMtaRestriction "reject_rbl_client cbl.abuseat.org" \
zimbraMtaRestriction "reject_rbl_client bl.spamcop.net" \
zimbraMtaRestriction "reject_rbl_client dnsbl.sorbs.net" \
zimbraMtaRestriction "reject_rbl_client sbl.spamhaus.org"
```

Setting Global Rule for Messages Marked as Both Spam and Whitelist

When you use a third-party application to filter messages for spam before messages are received by ZCS, the ZCS global rule is to send all messages that are marked by the third-party as spam to the junk folder. This includes messages that are identified as spam and also identified as whitelisted.

If you do not want messages that are identified as whitelisted to be sent to the junk folder, you can configure `zimbraSpamWhitelistHeader` and `zimbraSpamWhitelistHeaderValue` to pass these messages to the user's mailbox. This global rule is not related to the Zimbra MTA spam filtering rules. Messages are still passed through a user's filter rules.

To search the message for a whitelist header:

```
zmprov mcf zimbraSpamWhitelistHeader <X-Whitelist-Flag>
```

To set the value:

```
zmprov mcf zimbraSpamWhitelistHeaderValue <value_of_third-party_white-lists_messages>
```

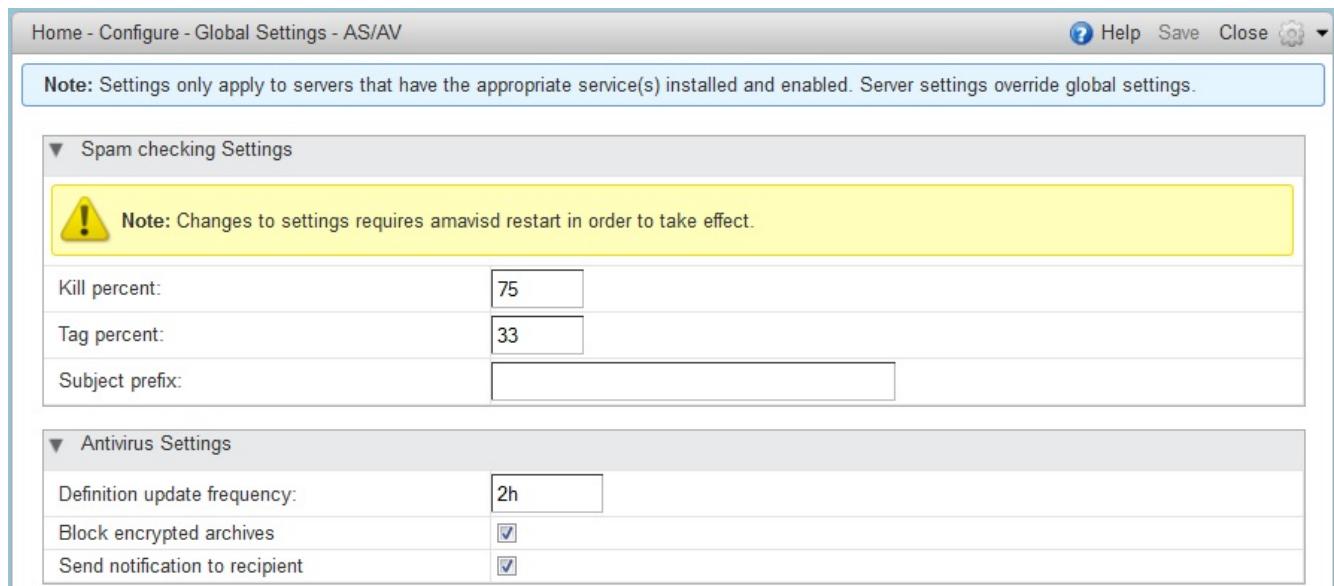
Anti-virus Settings

Anti-virus protection is enabled for each server when the Zimbra software is installed. The anti-virus software is configured to send messages that have been identified as having a virus to the virus quarantine mailbox. An email notification is sent to recipients letting them know that a message has been quarantined. The quarantine mailbox message lifetime is set to 7 days.

From the Admin Console, you can specify how aggressively spam is to be filtered in your Zimbra Collaboration.

Admin Console:

Home > Configure > Global Settings > AS/AV



1. At the Anti-Virus fields, enter parameters, as appropriate for your requirements.
2. From the **Gear** icon, select **Save** to use your settings.

Table 32. Anti Virus

Option	Description
Definition update frequency	By default, the Zimbra MTA checks every two hours for any new anti-virus updates from ClamAV. The frequency can be set between 1 and 24 hours.
Block encrypted archives	Restrict encrypted files, such as password protected zipped files.
Send notification to recipient	To alert that a mail message had a virus and was not delivered.

During Zimbra Collaboration installation, the administrator notification address for anti-virus alerts is configured. The default is to set up the admin account to receive the notification. When a virus has been found, a notification is automatically sent to that address.



Updates are obtained via HTTP from the ClamAV website.

Zimbra Free/Busy Calendar Scheduling

The Free/Busy feature allows users to view each other's calendars for efficiently scheduling meetings. You can set up free/busy scheduling across ZCS and Microsoft Exchange servers.

ZCS can query the free/busy schedules of users on Microsoft Exchange 2003, 2007, or 2010 servers and also can propagate the free/busy schedules of ZCS users to the Exchange servers.

To set free/busy interoperability, the Exchange systems must be set up as described in the Exchange Setup Requirements section, and the Zimbra Collaboration Global Config, Domain, COS and Account settings must be configured. The easiest way to configure Zimbra Collaboration is from the Administration Console.

Exchange 2003/2007/2010 Setup Requirements

The following is required to set up the free/busy feature:

- Either a single Active Directory (AD) must be in the system or the global catalog must be available.
- The Zimbra Collaboration server must be able to access the HTTP(S) port of IIS on at least one of the Exchange servers.
- Web interface to Exchange public folders needs to be available via IIS. (<http://server/public/>)
- Zimbra Collaboration users must be provisioned as a contact on the AD using the same administrative group for each mail domain. This is required only for ZCS to Exchange free/busy replication.
- For Zimbra Collaboration to Exchange free/busy replication, the Exchange user email address must be provisioned in the account attribute **zimbra-ForeignPrincipal** for all Zimbra Collaboration users.

Configuring Free/Busy on Zimbra Collaboration

To set Free/Busy Interoperability up from the Administration Console, the global config, Domain,

COS and Account settings must be configured as described here.

- Configure the Exchange server settings, either globally or per-domain.
 - Microsoft Exchange Server URL. This is the Web interface to the Exchange.
 - Microsoft Exchange Authentication Scheme, either **Basic** or **Form**.
 - Basic is authentication to Exchange via HTTP basic authentication.
 - Form is authentication to Exchange as HTML form based authentication.
 - Microsoft Exchange Server Type, either **WebDav** or **ews**
 - Select WebDAV to support free/busy with Exchange 2003 or Exchange 2007.
 - Select ews (Exchange Web Service) to support free/busy with Exchange 2010, SP1.
- Include the Microsoft Exchange user name and password. This is the name of the account in Active Directory and password that has access to the public folders. These are used to authenticate against the Exchange server on REST and WebDAV interfaces.
- Add the **o** and **ou** values that are configured in the **legacyExchangeDN** attribute for Exchange on the Global Config Free/Busy Interop page, the Domain Free/Busy Interop page or on the Class of Service (COS) Advanced page. Set at the global level this applies to all accounts talking to Exchange.
- In the Account's Free/Busy Interop page, configure the foreign principal email address for the account. This sets up a mapping from the Zimbra Collaboration account to the corresponding object in the AD.



To find these settings on the Exchange server, you can run the Exchange ADSI Edit tool and search the **legacyExchangeDN** attribute for the **o=**, **ou=**, and **cn=** settings.

Zimbra Collaboration to Zimbra Collaboration Free/Busy Interoperability

You can set up free/busy interoperability between ZCS servers. Free/Busy interoperability is configured on each server.



Each server must be running ZCS 8.0.x or later.

1. Enter the server host names and ports.

```
zmprov mcf zimbraFreebusyExternalZimbraURL http[s]://[user:pass@]host:port
```

If the **user:pass** is not included, the server runs an anonymous free/busy lookup.

2. Restart the server.

```
zmcontrol restart
```

3. Repeat these steps at all other servers.

Setting Up S/MIME

S/MIME is a standard to send secure email messages. S/MIME messages use digital signature to authenticate and encrypt messages.

Currently, there are two different methods for providing the S/MIME feature

1. The old client based solution which requires Java 1.6 SE deployed on the client machine
2. The new server based solution which does not require Java on the client machine. The server performs all the cryptographic operations. (Recommended)

Setting up for using the S/MIME feature using the client based solution

Prerequisites

- To use S/MIME, users must have a PKI certificate and a private key. The private key must be installed in the user's local certificate store on Windows and Apple Mac and in the browser certificate store if they use the Firefox browser. See the appropriate computer or browser documentation for how to install certificates.
- Users can use any of the following browsers:
 - Mozilla Firefox 4 or later
 - Internet Explorer 8, 9
 - Chrome 12 or later
- Users computers must have Java 1.6 SE deployed to use S/MIME. If they do not, they see an error asking them to install it.

S/MIME License

You must have a ZCS license that is enabled for S/MIME.

Enable S/MIME Feature

Admin Console:

Home > Configure > Class of Service → *COS* → Features

Home > Manage > Accounts → *account* → Features

The S/MIME feature can be enabled from either the COS or Account FeaturesTab.

1. Select the COS or account to edit.
2. In the Features tab S/MIME features section, check **Enable S/MIME**.
3. Click **Save**.

Importing S/MIME Certificates

Users can send encrypted messages to recipients if they have the recipients' public-key certificate stored in one of the following:

- Recipient's contact page in their Address Book.
- Local OS or browser keystore.
- External LDAP directory.

The certificates should be published into the LDAP directory so that they can be retrieved from the GAL. The format of the S/MIME certificates must be X.509 Base64 encoded DER.

Configure External LDAP Lookup for Certificates

If you use an external LDAP to store certificates, you can configure the Zimbra server to lookup and retrieve certificates from the external LDAP, on behalf of the client.

Admin Console:

Home > Configure > Global Settings > S/MIME
Home > Configure > Domains → *domain* → S/MIME

You can configure the external LDAP server settings from either the **Global Settings > S/MIME** tab or the **Domains > S/MIME** tab.



Global Settings override Domain settings

1. Edit the global settings page or select a domain to edit. Open the **S/MIME** tab.
2. In the **Configuration Name** field, enter a name to identify the external LDAP server. Example, **companyLDAP_1**
3. In the **LDAP URL** field, enter the LDAP server's URL. Example, **ldap://host.domain:3268**
4. To use DN to bind to the external server, in the **S/MIME LDAP Bind DN** field, enter the bind DN. Example, **administrator@domain**

If you want to use anonymous bind, leave the Bind ND and Bind password fields empty.

5. In the **S/MIME Ldap Search Base** field, enter the specific branch of the LDAP server that should be searched to find the certificates.

Example, **ou=Common Users, DC=host, DC=domain**

Or, check **Automatically discover search base** to automatically discover the search base DNs. For this to work, the S/MIME Search Base field must be empty.

6. In the **S/MIME Ldap filter** field, enter the filter template for the search. The filter template can contain the following conversion variables for expansion:
 - %n - search key with @ (or without, if no @ was specified)
 - %u - with @ removed (For example, mail=%n)
7. In the **S/MIME Ldap Attribute** field, enter attributes in the external LDAP server that contain users' S/MIME certificates. Multiple attributes can be separated by a comma (,).

Example, "userSMIMECertificate, UserCertificate"

8. Click **Save**.

To set up another external LDAP server, click **Add Configuration**.

Setting up for using the S/MIME feature using the server based solution

Prerequisites

Same as for the client based S/MIME solution except that Java is not required on the client machine. The private key is also not required to be on the client machine's local/browser certificate store.

S/MIME License

Same as for the client based S/MIME solution

Enable S/MIME Feature

Same as for the client based S/MIME solution

Importing S/MIME Certificates

Same as for the client based S/MIME solution except that the recipients' public-key certificate no longer need to be stored into Local OS or browser keystore. The certificate can be published to all other places mentioned in previous S/MIME version.

List of LDAP attributes introduced to support the server based S/MIME solution

1. zimbraSmimeOCSPEnabled

- Used by server at the time of validating the user as well as public certificates
- If TRUE, the revocation check will be performed during certificate validation
- If FALSE, the revocation check will not be performed during certificate validation

2. zimbraSmimePublicCertificateExtensions

- The supported public certificate file extensions separated by commas
- Contains the list of supported formats for the userCertificate LDAP attribute
- Default values: cer,crt,der,spc,p7b,p7r,sst,st0,pem
- Zimbra web client retrieves the supported file formats/extensions for public certificate upload from the server

3. zimbraSmimeUserCertificateExtensions

- The supported public certificate file extensions separated by commas
- Contains the list of supported formats for the userSmimeCertificate LDAP attribute
- Default values: p12,pfx
- Zimbra web client retrieves the supported file formats/extensions for user certificate upload from the server

Process for Adding the CA certificate to the mailbox truststore for S/MIME

S/MIME uses the mailbox trust store path and its password which are defined in localconfig.xml

The key names are:

- mailboxd_truststore
- mailboxd_truststore_password

If the mailboxd_truststore key is not defined in localconfig.xml, by default the value of mailboxd_truststore is:

- <zimbra_java_home>/jre/lib/security/cacerts

A CA certificate can be imported to the mailbox trust store by executing the following command:

```
keytool -import -alias -keystore <mailboxd_truststore path> -trustcacerts -file  
<CA_Cert>
```

Storage Management

Managing Storage Volumes

In the Volume page you manage storage volumes on the Zimbra Mailbox server. When Zimbra Collaboration is installed, one index volume and one message volume are configured on each mailbox server. You can add new volumes, set the volume type, and set the compression threshold.



If Compress Blobs is enabled (YES), the disk space used is decreased, but memory requirements for the server increases.

Index Volumes

Each Zimbra mailbox server is configured with one current index volume. Each mailbox is assigned to a permanent directory on the current index volume. You cannot change which volume the account is assigned.

As volumes become full, you can create a new current index volume for new accounts. You can add new volumes, set the volume type, and set the compression threshold.

Index volumes not marked current are still actively in use for the accounts assigned to them. Any index volume that is referenced by a mailbox as its index volume cannot be deleted.

Message Volumes

When a new message is delivered or created, the message is saved in the current message volume. Message volumes can be created, but only one is configured as the current volume where new messages are stored. When the volume is full, you can configure a new current message volume. The current message volume receives all new messages. New messages are never stored in the

previous volume.

A current volume cannot be deleted, and message volumes that have messages referencing the volume cannot be deleted.

Implementing Hierarchical Storage Management (*)



*Starting with Zimbra 8.8, there are two versions of this feature. Zimbra 8.8 provides Standard and New Generation (NG) versions. Zimbra 8.7 and earlier include the Standard version, which is explained below. To use and enable the NG version of this feature with Zimbra 8.8, refer to the specific NG chapter later in this Guide.

Hierarchical Storage Management (HSM) allows you to configure storage volumes for older messages. HSM is a process of moving older data from the primary volume to the current secondary volume based on the age of the data.

To manage your disk utilization, implement a global HSM policy or a HSM policy for each mailbox server. The policy configured on individual servers overrides the policy configured as the global policy.

Email messages and the other items in the account are moved from the primary volume to the current secondary volume based on the HSM policy. Users are not aware of any change and do not see any noticeable differences when opening older items that have been moved.

The default global HSM policy moves messages and document files more than 30 days old to the secondary volume. You can also select to move tasks, appointments, and contacts. The schedule for moving can be set for items older than a specified number of days, months, weeks, hours, minutes.

In addition to selecting different items to move, you can use the search query language to set up other HSM policies.

For example: to include all messages marked as spam in messages moved to the current secondary volume, you would add the following to the policy: **message:in:junk before:-[x] days**.



The search string can be added to the default policy or you can write a new policy.

Scheduling HSM Sessions

Sessions to move messages to the secondary volume are scheduled in your cron table. From the Administration Console, when you select a server, you can manually start a HSM session, monitor HSM sessions, and abort HSM sessions that are in progress from the Volumes page.

You can manually start an HSM session from the server's **Gear** icon.

When you abort a session and then restart the process, the HSM session looks for entries in the primary store that meet the HSM age criteria. Any entries that were moved in the previous run would be excluded, as they would no longer exist in the primary store.

HSM jobs can be configured to be a specific batch size. The **zimbraHsmBatchSize** attribute can be

configured either as a global setting or per server to specify the maximum number of items to move during a single HSM operation. The default value is 10000. If the limit is exceeded the HSM operation is repeated until all qualifying items are moved.

Global batch size modification:

```
zmprov mcf zimbraHsmBatchSize <num>
```

Modifying batch size on a server:

```
zmprov ms `zmhostname` zimbraHsmBatchSize <num>
```

Email Retention Management

You can configure retention policies for user account's email, trash, and junk folders. The basic email retention policy is to set the email, trash and spam message lifetime in the COS or for individual accounts.

You can set up specific retention policies that users can enable for the Inbox and other email folders in their account. Users can also create their own retention policies.

You can enable the dumpster feature to save messages that are deleted from Trash. When an message lifetime has been reached based on email lifetime rules or deletion policies, the message is moved to the dumpster if it is enabled. Users can recover deleted items from the dumpster until the threshold set in the **Visibility lifetime in dumpster for end user** setting.

If dumpster is not enabled, messages are purged from the server when the email retention lifetime is reached.

You can also set up a legal hold on an account to prevent message from being deleted.

Configuring Email Lifetime Rules

You can configure when email messages should be deleted from an accounts folders, and the trash and junk folders by COS or for individual accounts.

Table 33. Email Lifetime Options

Email Lifetime Option	Description
Email message lifetime	Number of days a message can remain in a folder before it is purged. This includes data in RSS folders. Default = 0 Minimum = 30 days
Trashed message lifetime	Number of days a message remains in the Trash folder before it is purged. Default = 30 days.

Email Lifetime Option	Description
Spam message lifetime	Number of days a message can remain in the Junk folder before it is purged. Default = 30 days.

Purging Email Messages

By default, the server purges email messages that have exceeded their lifetime every minute. You can change the duration of time that the server should "rest" between purging mailboxes.

Use the global Sleep Time setting to define duration, in minutes, between mailbox purges.

Admin Console:

Home > Configure > Global Settings > General Information

The screenshot shows the 'General Information' section of the Zimbra Admin Console. It includes fields for:

- Most results returned by GAL search: 100
- Default domain: future.zimbraview.com
- Maximum number of scheduled tasks that can run simultaneously: 20
- Sleep time between subsequent mailbox purges: 1 minutes
- Maximum size of a file uploaded from the desktop (KB): 2504800
- Admin help URL: (empty)
- Delegated admin help URL: (empty)

For example, the purge interval is set to 1 minute, after mailbox1 is purged of messages that meet the message lifetime setting, the server waits 1 minute before beginning to purge mailbox2.

If the message purge schedule is set to 0, messages are not purged even if the mail, trash and spam message lifetime is set.



Because users cannot view message lifetime settings, you will need to apprise them of your purge policies.

Configuring Message Retention and Deletion Policies

Retention and deletion policies can be configured as a global setting or as a COS setting. Users can select these policies to apply to their message folders in their account. They can also set up their own retention and deletion policies. Users enable a policy you set up or create their own policies from their folders' Edit Properties dialog box.

Global Retention Policy

System wide retention and deletion policies can be managed from the Administration Console.

Use the global Retention Policy page to set global retention or deletion policies.

Admin Console:

Home > Configure > Global Settings > Retention Policy

The screenshot shows the 'Global Settings - Retention Policy' page. At the top, there's a note: 'Note: Settings only apply to servers that have the appropriate service(s) installed and enabled. Server settings override global settings.' Below this is a section titled 'Retention Policies' with a table header 'Policy Name' and 'Retention Range'. At the bottom of this section are buttons for 'Delete', 'Edit', and 'Add'. Below this section is another titled 'Disposal Policies'.

COS Retention Policy

Use the COS Retention Policy page to set retention or deletion for the selected COS.

Admin Console:

Home > Configure > Class of Service → **COS** → Retention Policy

The screenshot shows the 'Class of Service - standard - Retention Policy' page. It displays a policy named 'standard' with ID 'df02cdbc-4b43-4cccd-a238-0c70e64e85c6' and created on 'August 28, 2014 11:44:23 AM'. There is a checkbox 'Enable COS-level policies instead of inheriting from the policy defined in Global Settings.' which is unchecked. Below this is a 'Retention Policies' section with a table header 'Policy Name' and 'Retention Range', and buttons for 'Delete', 'Edit', and 'Add'. Below this section is another titled 'Disposal Policies'.

Ensure that the **Enable COS-level policies instead of inheriting from the policy defined in Global Settings** is enabled.

The retention policy is not automatically enforced on a folder. If users option an item in a folder that has not met the threshold of the retention policy, the following message is displayed, **You are deleting a message that is within its folder's retention period. Do you wish to delete the message?**

When the threshold for the deletion policy is reached, items are deleted from the account. They are not sent to the Trash folder. If the dumpster feature is enabled, they are sent to the dumpster, if it is not enabled, they are purged from the server.

How Lifetime and Retention/Deletion Policies Work Together

If the Email Message Lifetime is set to a value other than zero (0), this setting applies in addition to the disposal or retention policy values applied to a folder. For example:

Email Message Lifetime is set to 120 days

- Folder A has a policy with a disposal threshold of 360 days. Messages in Folder A are disposed of in 120 days.
- Folder B has a policy with disposal threshold of 90 days. Messages in Folder B are disposed of in 90 days.
- Folder C has a policy with retention range of 150 days. Messages in Folder C are disposed of in 120 days.

Managing the Dumpster

When a message, trash or spam lifetime has been reached, the message is moved to the dumpster if the feature is enabled. When users right-click on Trash, they can click **Recover deleted items** to retrieve items from their trash that has been deleted in the last x days. This threshold is based on the **Visibility lifetime in dumpster for end user** setting.

The **Retention lifetime in dumpster before purging setting** sets retention lifetime for items in dumpster. Items in dumpster older than the threshold are purged and cannot be retrieved.

Administrators can access the individual dumpster's content, including spam, and they can delete data at any time before the message lifetime is reached.

Searching for an item in the dumpster folder

```
zmailbox -z -m <user@example.com> search --dumpster -l <#> --types  
<message,contact,document> <search-field>
```

The search field can be a date range: 'before:mm/dd/yyyy and after:mm/dd/yyyy' or emails from or to a particular person: 'from:Joe', etc.

Deleting items in the dumpster folder

Items in the dumpster folder can be deleted with the CLI or from the Administration Console:

```
zmmailbox -z -m <user@example.com> -A dumpsterDeleteItem <item-ids>
```

Admin Console:

Home > Configure > Class of Service → COS → Features → General Features

1. Enable (check) the **Dumpster folder** checkbox.
2. To set **Visibility lifetime in dumpster for end user**, go to the COS's, **Advanced** page, **Timeout Policy** section.
3. To set **Retention lifetime in dumpster before purging**, go to the COS's **Advanced** page, **Email Retention Policy** section.

Configure Legal Hold on an Account

If the dumpster folder feature is enabled, you can set up a legal hold to preserve all items in user accounts.

When dumpster is enabled, **Can purge dumpster folder** is also enabled. Disabling this feature turns off purging of items in the user's dumpster. This can be set on a COS or for individual accounts. When **Can purge dumpster folder** is enabled, any deletion policies set up on the accounts' folders are ignored.

Configure legal hold:

Admin Console:

Home > Configure > Class of Service → COS → Features

Home > Manage > Accounts → account → Features

Deselect **Can purge dumpster folder** on the **Features** page.

Customized Admin Extensions

Developers can create and add custom modules to the Zimbra Administration Console user interface, to provide new views, manage new data objects, extend existing objects with new properties, and customize existing views.

For the most up-to-date and comprehensive information about how to create an extended Administration Console UI module, go to the Zimbra wiki Extending Admin UI article located at [Extending_Admin_UI](#).

All Zimbra extensions currently incorporated at the Administration Console UI are listed in the content pane as view only.

Only those created by you can be removed (see also Removing Admin Extension Modules).

Deploying New Administration Console UI Modules

Admin Console:

Home > Configure > Admin Extensions

Save the module **zip** file to the computer you use to access the Administration Console.

1. From the **Gear** icon, select **Deploy** to present the **Deploying a Zimlet or an extension** dialog.
2. Browse to the custom module **zip** file you need to upload.
3. Click **Deploy**.

The file is uploaded and the extension is immediately deployed on the server.

Removing An Admin Extension Module

Deleting an Admin Extension results in removal of the selected extension and all associated files. This action does not delete the originating **zip** file.

Admin Console:

Home > Configure > Admin Extensions

Use steps in this section to remove custom Admin Extensions.

1. Select the module to remove, and select **Undeploy** from the **Gear** icon. A confirmation query is presented.
2. At the confirmation query, click **Yes** to proceed.

Ephemeral Data

There are 3 main types of ephemeral data stored in LDAP during normal operation of Zimbra Collaboration.

- Last Logon Time Stamps (`zimbraLastLogonTimestamp`)
- Auth Tokens (`zimbraAuthTokens`)
- CSRF Tokens (`zimbraCsrfTokenData`)

On small systems, storage of these types of ephemeral data may be done in the LDAP Server. However, mail systems with large numbers of active users have been found to overload LDAP for short-lived data storage. Therefore, the preferred option is to store this ephemeral data using an external server.



This document does not cover how to install and maintain the ephemeral storage server.

Configuring the storage location of ephemeral data is done through the following LDAP attribute:

Attribute	Format	Description
<code>zimbraEphemeralBackendURL</code>	[backend name]:[params]	Ephemeral Backend URL Configuration

The two currently supported Ephemeral Data backends are:

Backend	Format	Description
LDAP	ldap://default	Default configuration
SSDB	ssdb:127.0.0.1:8888	SSDB server and port

Frequent authentication requests place a high load on Ephemeral Data storage backend. See the following Zimbra wiki pages for results of authentication-based load tests:

- [LDAP Authentication load tests](#)
- [SSDB Authentication load tests](#)

Configuring a Running Zimbra Collaboration to Use SSDB

Configuring an already running Zimbra Collaboration installation to utilize `SSDB` instead of `LDAP` for short-lived data storage is done through the following process:

1. Install `SSDB` and note the IP address and port configured since you will need this data for the next steps. Refer to [Overview of Configuration Options](#) for more information.
2. Migrate any existing short-lived data to `SSDB` using the `/opt/zimbra/bin/zmmigrateattrs` command.

3. Configure Zimbra Collaboration to utilize **SSDB**.

Migration Procedure

1. Access the command prompt on one of the machines in the installation.
2. Migrate existing ephemeral data to the **SSDB** backend using the **zmmigrateattrs** utility

```
sudo su - zimbra  
/opt/zimbra/bin/zmmigrateattrs ssdb:<ip address|hostname>:port # substituting your  
server values
```

You may use either an IP address or a hostname for the host portion of the destination URL. Either way, you will need to ensure it resolves to the proper IP address on all machines in the cluster. If the provided SSDB address does not resolve to a functioning backend, the migration process will terminate.

3. Configure Zimbra Collaboration to use **SSDB**:

```
sudo su - zimbra  
zmprov mcf zimbraEphemeralBackendURL ssdb:<ip address|hostname>:port # substituting  
your server values
```

As with migration, the host and port must resolve to a functioning SSDB backend. Otherwise, the value of **zimbraEphemeralBackendURL** will not be changed.

Migration Details

Migration Info

Information about the latest migration process can be viewed by running the command **zmmigrateattrs --status**. If the migration is currently in progress, this command may have to be run from a new terminal window. This command will output three pieces of information:

1. The status of the migration: one of IN_PROGRESS, COMPLETED or FAILED
2. The URL of the SSDB backend acting as the destination
3. A timestamp of when the migration process was initiated

The migration info can be reset with the command **zmmigrateattrs --clear**. This should only be done if the status does not reflect the true state of the system.

Changing the Ephemeral Backend URL

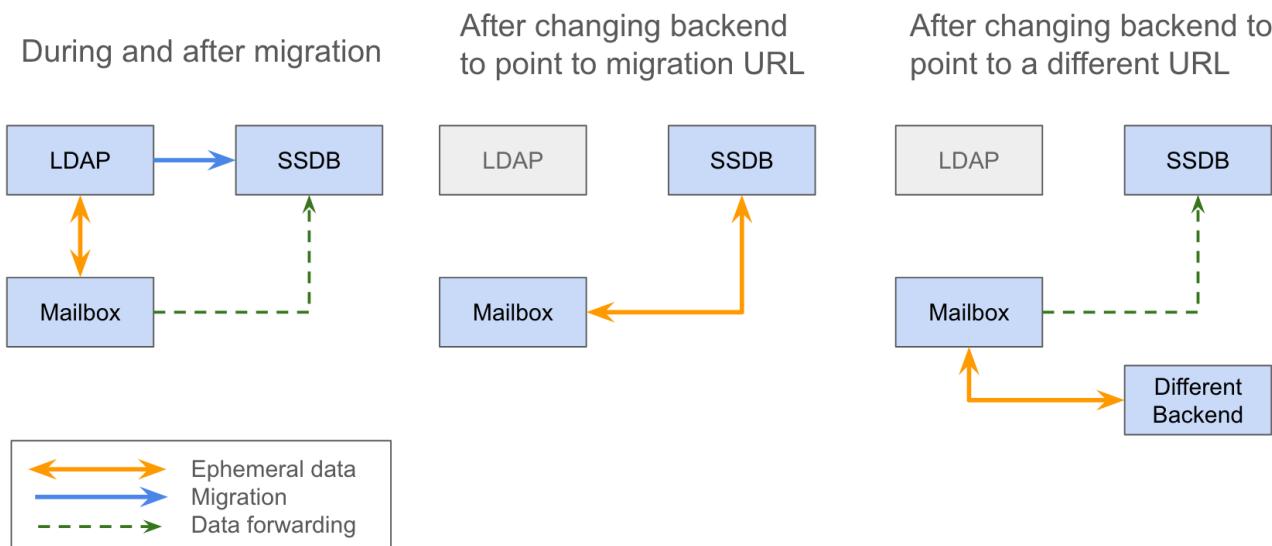
When the value of **zimbraEphemeralBackendURL** is modified, Zimbra Collaboration checks the status of the last known migration. This can result in one of several scenarios:

1. If the migration is completed and the URL of this migration matches the newly provided value, `zimbraEphemeralBackendURL` is changed to the new value and the migration info is reset. This is the expected use case.
2. If a migration is currently in progress, `zimbraEphemeralBackendURL` will not be changed.
3. If no migration info is available, the migration has failed, or the new URL does not match the migration URL, `zimbraEphemeralBackendURL` will be changed; however, a warning will be logged stating that data is not guaranteed to have been migrated.

Forwarding Ephemeral Data

During the migration process, and until the backend URL is changed, Zimbra Collaboration will store new ephemeral data both in LDAP and `SSDB`; this keeps the two backends from getting out of sync. If the new value of `zimbraEphemeralBackendURL` is changed to match the migration URL, migration info is reset and the forwarding mechanism is turned off. If the values do not match, migration info is not reset, and forwarding remains in place. Note that this means that migration only needs to be run once, even if there is a gap between the initial migration and URL change. As long as the target backend is never taken offline, it will stay up-to-date. However, if `SSDB` is taken offline between the end of the migration and the backend URL change, migration will need to be re-run.

These scenarios are demonstrated below:



Advanced Migration Options

The `zmigrateattrs` tool provides several migration options, to be used with careful consideration:

- The `-r` or `--dry-run` option outputs the changes to be made for each account to the console, without actually performing the migration.
- The `-n` or `--num-threads` option specifies how many threads will be used for migration. Omitting this will result in migration happening synchronously.
- The `-a` or `--account` option allows for migration of a comma-separated list of specific accounts. This should be used only for testing or debugging.

- The `-d` or `--debug` option enables debug logging.

If no attribute names are explicitly passed in as arguments, migration will occur for all known ephemeral attributes, as in the example above.

Migration Limitations

Ephemeral data migration is a one-way process. The `zmmigrateattrs` script does not support migrating data from `SSDB` back into LDAP, nor does it support migrating data between different instances of `SSDB`. This means that if the value of `zimbraEphemeralBackendURL` is reverted back to LDAP after migration, prior authentication data will become inaccessible, and all user sessions will be invalidated. If migration to a new `SSDB` backend becomes necessary, the data should be replicated to the new location prior to changing the value of `zimbraEphemeralBackendURL`.

There is one exception to this is: the backend can be safely reverted back to LDAP immediately after the switch to `SSDB` with minimal loss of data. This is because the original values are retained in LDAP during migration; switching the backend to `SSDB` leaves a "snapshot" of ephemeral data in LDAP at the time of the switch. The migration utility does not currently provide a way to delete this data to free up space; however, it allows for the backend to be reverted. The more time passes between the initial change and the reversion, the less the LDAP snapshot will reflect the true state of ephemeral data.

Changes to zmprov

Due to changes in the way multi-valued ephemeral data is stored, the attributes `zimbraAuthTokens` and `zimbraCsrfTokenData` are no longer returned as part of the `zmprov ga <account>` response. The value of `zimbraLastLogonTimestamp` is returned as before, although only if the `-l` flag is not used, as adding the `-l` flag will restrict the server to accessing attributes in LDAP only. It is still possible to modify these attributes using the `zmprov ma <account>` command, regardless of the ephemeral backend. In order to do this, the provided attribute value must match its LDAP format: `tokenId|expiration|serverVersion` for auth tokens; `data:crumb:expiration` for CSRF tokens.

Migration CSV Output

Each run of `zmmigrateattrs` generates a CSV file in the `/opt/zimbra/data/tmp/` folder. The file contains migration info for every migrated account, such as the number of attributes migrated. Note that it is possible for this to be zero, which can happen if all ephemeral data for an account is already present in the destination store.

If any migrations fail, a cutdown CSV file report detailing only the errors is also created in the same directory. The name(s) of the file(s) are logged at the end of the run.

Account Deletion Behavior

Ephemeral data deletion behavior differs slightly between SSDB and LDAP backends. With SSDB as the backend, account deletion results in the `zimbraLastLogonTimestamp` attribute being explicitly deleted from SSDB. `zimbraAuthTokens` and `zimbraCsrfTokenData`, however, are left to be expired by SSDB when the token lifetimes are reached (default of 2 days). Conversely, ephemeral data in LDAP is wiped immediately as part of the account deletion process.

SSDB Installation and Configuration

Installation

Zimbra Collaboration packages do not include SSDB server and Zimbra Collaboration installation and configuration utilities do not alter SSDB configuration. To install the latest version of SSDB, follow instructions provided by SSDB developer community in [SSDB Installation Documentation](#). Please note, that Zimbra Collaboration has been tested with SSDB version 1.9.5. In order to install SSDB 1.9.5, download [stable-1.9.5.zip](#) instead of [master.zip](#) when following [SSDB installation instructions](#).

Overview of Configuration Options

The purpose of this guide is to discuss some of the options available with [SSDB](#), specifically with regards to:

- High-availability via master-slave replication
- High-availability via master-master replication
- Horizontal scaling, with high-availability, via multi-master configuration.

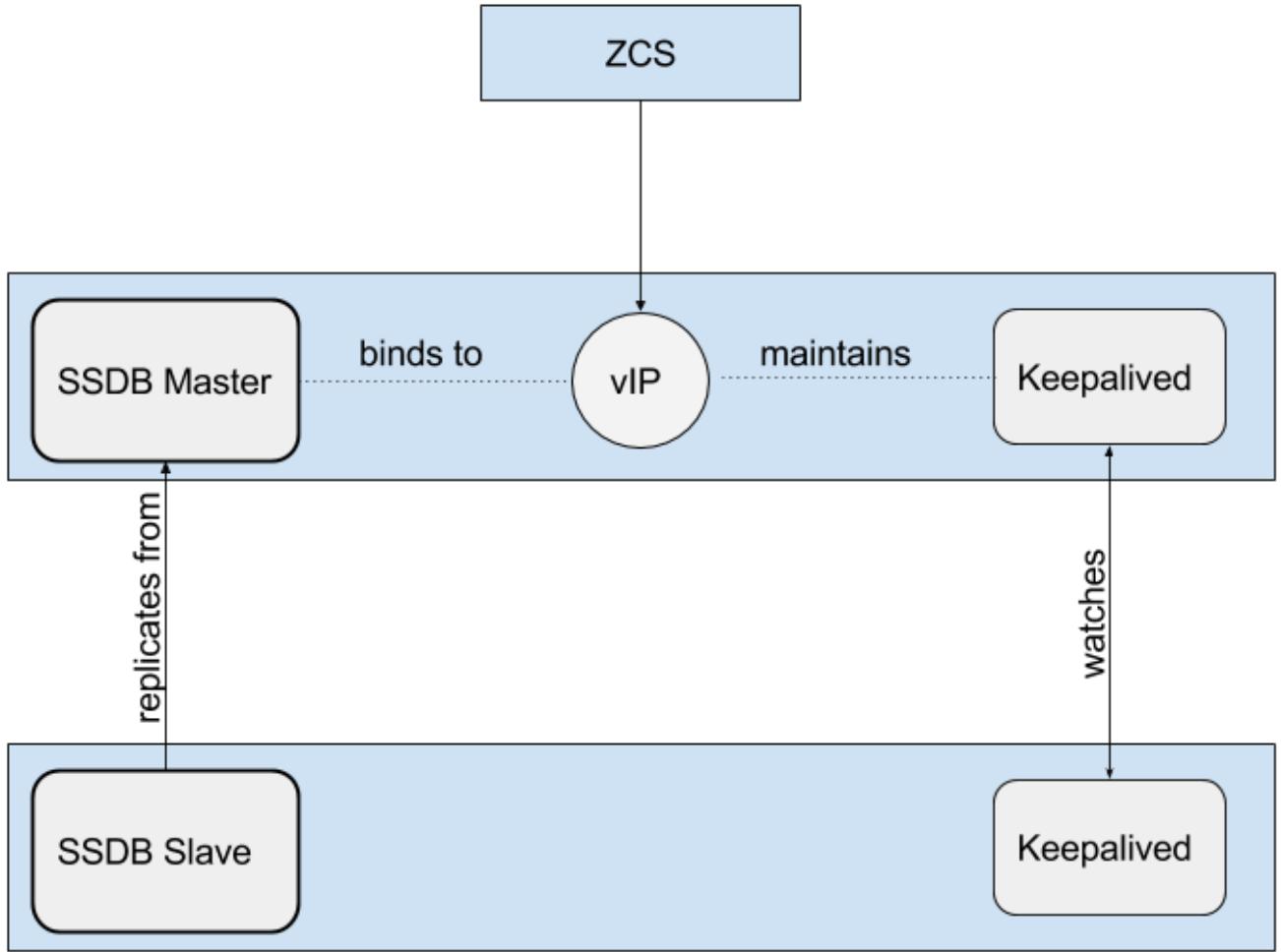
This guide is not meant to be an exhaustive treatment of the subject. Also, as of the time of this writing, [SSDB](#) and any related packages must be installed and configured by the system administrator prior to updating [zimbraEphemeralBackendURL](#) and migrating attributes.

[SSDB](#) is compatible with [Redis](#) clients and Zimbra Collaboration currently uses a [Redis](#)-compatible client for communication with [SSDB](#), so many of the concepts described herein are applicable with a [Redis](#) backend.

High-availability with Master-Slave replication

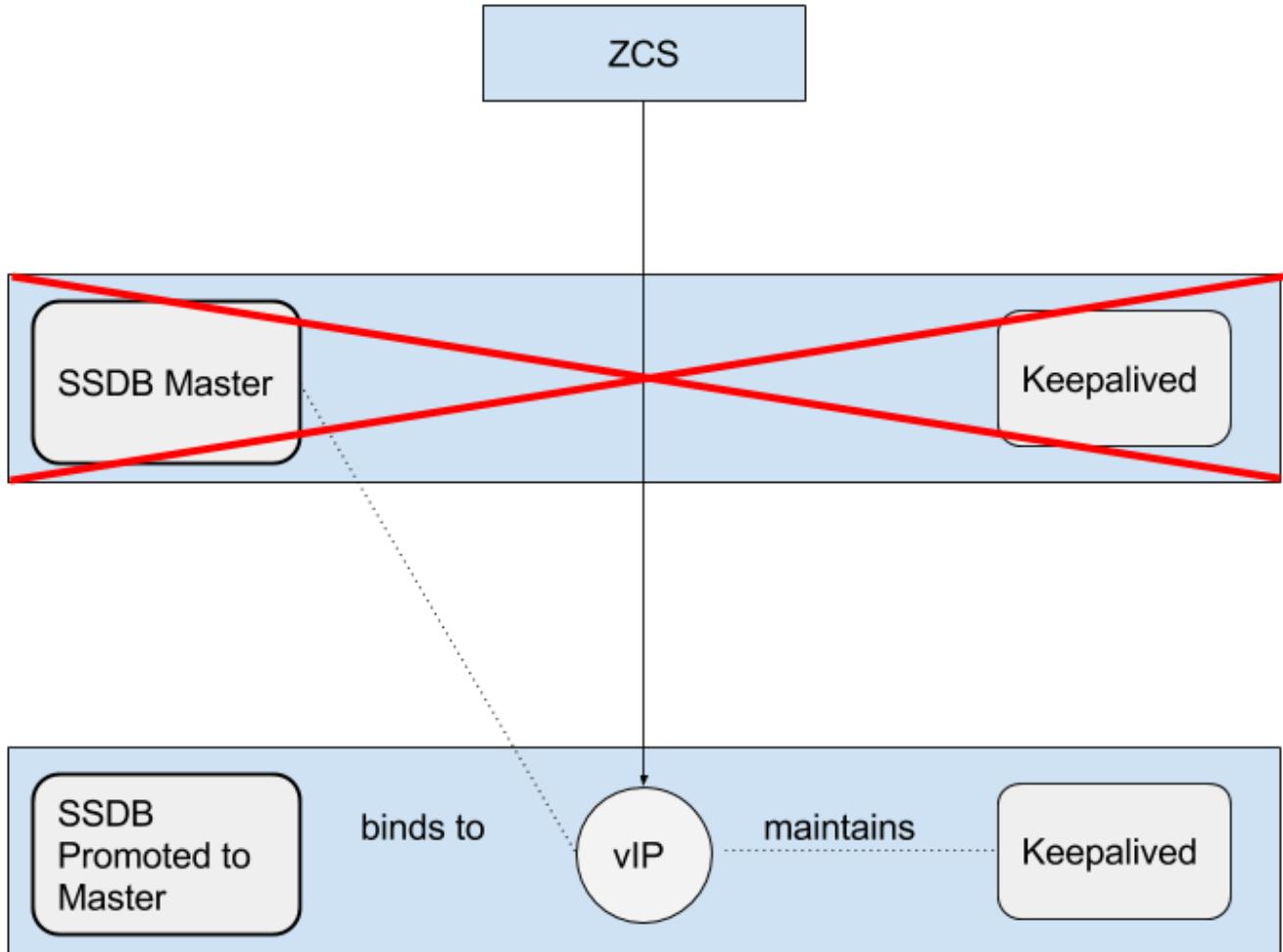
Normal Operation

The method described in this document to implement master-slave replication makes use of [Keepalived](#) to maintain a configured virtual IP address that is bound to the master [SSDB](#) instance under normal conditions.



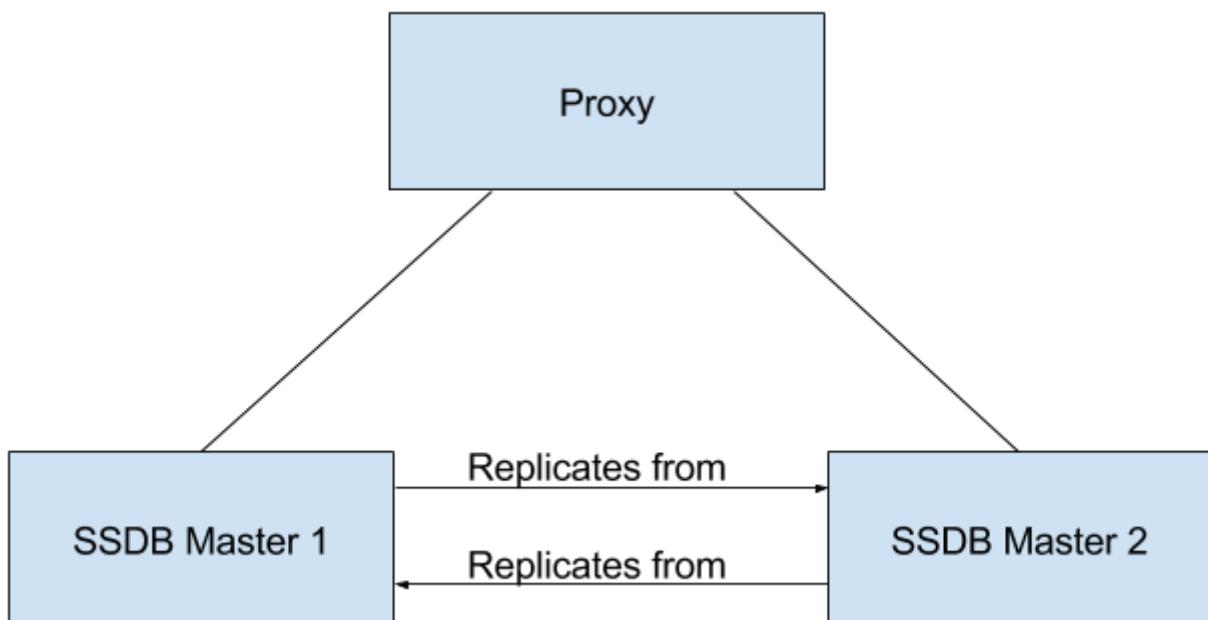
Fail-over

If **Keepalived** detects a failure of the master instance, then the backup instance is promoted to master by re-binding the virtual IP address to the backup.



High-availability with Master-Master replication

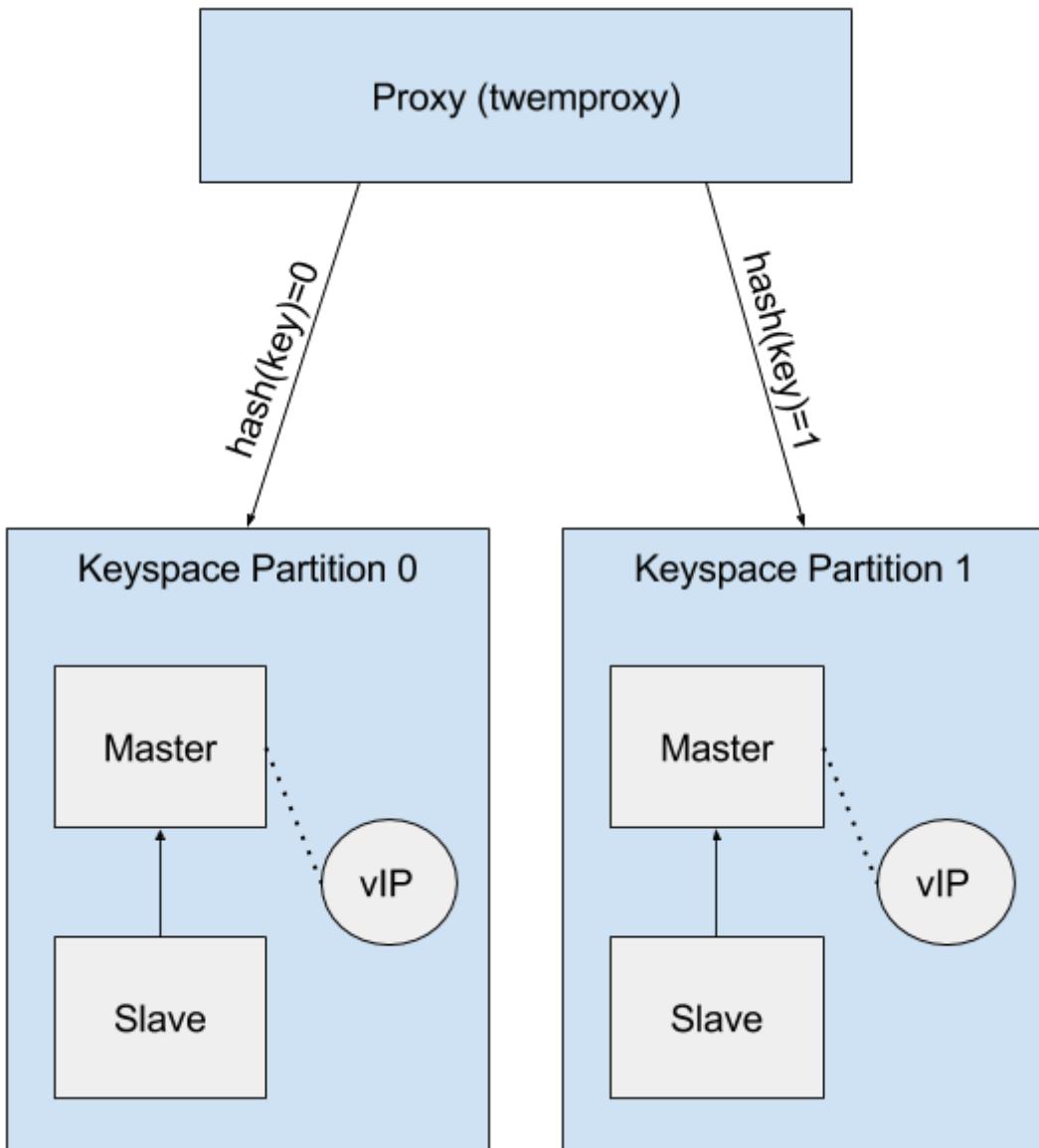
This differs from master-slave replication in that both **SSDB** instances are online and accessible. Each replicates changes from the other. In the example set-up described later, we use [HAProxy](#) as a front-end. Keep in mind that, for production, you must use a proxy service that is, itself, highly-available.



Horizontal Scaling via Multi-Master Configuration

Normally, both **SSDB** and **Redis** contain the entire key-space in a single instance. It is possible to front-end multiple instances using a service such as **twemproxy**. It supports various hashing modes such that the data associated with a particular key is always stored on the same server. This allows for horizontal scaling with very large installations.

By configuring each **SSDB** instance in master-slave configuration, you get both horizontal scaling and high-availability.



Master-Slave Replication

One way to ensure that **SSDB** remains highly-available is to set-up master-slave replication and configure a system that will allow the backup **SSDB** instance to automatically take-over in the event that the primary instance goes down. This document will describe one technique for accomplishing that goal.

Overview

SSDB will be installed on two servers. It will be configured such that one server is the designated master and the other server is the designated slave, or backup, that will constantly replicate changes from the master server.

Keepalived will also be installed on these two servers. Each **Keepalived** instance will monitor the other. In the event that the master server goes down, **Keepalived** will detect that failure and promote the slave, or backup, server to master. **Keepalived** will maintain a **Virtual IP address** bound to whichever server is the current master.

Zimbra Collaboration will be configured such that the **zimbraEphemeralBackendURL** will bind to the **Virtual IP address** that is being maintained by **Keepalived**.

Once the installation and configuration of *both* the **SSDB** master-slave setup and Zimbra Collaboration have been completed, follow the instructions in **Ephemeral Data** to update the **zimbraEphemeralBackendURL** accordingly.

The example documented here was done on servers running [Ubuntu 16.04](#).

Required Packages

- [SSDB](#)
- [Keepalived](#)

Prerequisites

Install **SSDB** and **Keepalived** on two servers in accordance with the procedure that is applicable to the Linux distribution that you are using.

Configuration

The following configuration steps assume that you have installed **SSDB** to `/var/lib/ssdb` and that all **SSDB** configuration files are located in that same directory. It further assumes that the internal host addresses are on the **192.168.56/24** network.

- **192.168.56.111** - This is IP address of the initial master **SSDB** server
- **192.168.56.112** - This is the IP address of the initial slave **SSDB** server
- **192.168.56.120** - This is the virtual IP address that will be maintained by **Keepalived**.

SSDB Configuration, Designated (Initial) Master

The IP address of this machine is **192.168.56.111**.

`/var/lib/ssdb/ssdb_master.conf`

The key configuration items in the following block are:

- **server/ip** - Binding to all available IP addresses

- `server/port` - Binding to standard **SSDB** port
- `server/deny, server/allow` - Restrict **SSDB** access to `localhost` and the internal (host) addresses.

Only the configuration items related to master-slave replication are shown here.

```
# ssdb-server config
# MUST indent by TAB!

# relative to path of this file, directory must exists
work_dir = ./var
pidfile = ./var/ssdb.pid

server:
    ip: 0.0.0.0
    port: 8888
    deny: all
    allow: 127.0.0.1
    allow: 192.168.56

replication:
    binlog: yes
    # Limit sync speed to *MB/s, -1: no limit
    sync_speed: -1
    slaveof:
        # sync|mirror, default is sync
        #type: sync
```

`/var/lib/ssdb/ssdb_slave.conf`

The key configuration items in the following block are:

- `server/ip` - Binding to `localhost`
- `server/port` - Binding to standard **SSDB** port
- `slaveof/type` - `sync`
- `slaveof/host` - `192.168.56.112` is the other **SSDB** server
- `slaveof/port` - `8888` - The standard **SSDB** port

Again, only the configuration items related to master-slave replication are show.

```

# ssdb-server config

# relative to path of this file, must exist
work_dir = ./var_slave
pidfile = ./var_slave/ssdb.pid

server:
    ip: 127.0.0.1
    port: 8888

replication:
    binlog: yes
    # Limit sync speed to *MB/s, -1: no limit
    sync_speed: -1
    slaveof:
        # sync|mirror, default is sync
        type: sync
        # Can use host: <hostname> with SSDB 1.9.2 or newer
        ip: 192.168.56.112
        port: 8888

```

SSDB Configuration, Designated (Initial) Slave

The IP address of this machine is **192.168.56.112**.

The **ssdb_master.conf** file is identical to that of the designated master server.

The **ssdb_slave.conf** file is almost identical to that of the designated master server. Only the following items differ;

- **slaveof/ip (or host)** - 192.168.56.111 is the other SSDB server

Keepalived configuration, Designated (Initial) Master

/etc/keepalived/keepalived.conf

The key configuration items to note are:

- **state** - State is set to **BACKUP** for *both* the designated (initial) master and backup servers. In this scenario, the **priority** is used to negotiate which server will assume **MASTER** status initially.
- **nopreempt** - In the event that the master server fails and the backup server is promoted to master, this configuration directive will keep the original master from reclaiming that role should it come back online automatically. This is required because it will likely be stale. In this case, when it comes back up, it will remain in backup mode and will begin replicating information from the new master. *Note:* Human intervention may be required to bring a failed master back into service.
- **interface** - In this example, **enp0s8** is the interface identifier for which the **virtual_ipaddress** will be defined. You will choose a value that is appropriate to your installation.

- **priority** - The designated initial master must have a higher priority than the designated initial backup.
- **advert_int** - For the purposes of this documentation, the default value of 1 second was used. If you install **Keepalived 1.2.21** or newer, you can specify a floating-point value here; e.g., **0.1** (seconds). This will allow **Keepalived** to detect a master failure more rapidly.
- **notify** - This is the path to a script that will be called for state transitions. The full contents of the script is shown below
- **virtual_ipaddress** - This is the virtual IP address that is maintained by **Keepalived**.

```
vrrp_instance VRRP1 {
    state BACKUP
    nopreempt
    interface enp0s8
    virtual_router_id 41
    priority 200
    advert_int 1
    notify /var/lib/ssdb/notify.sh

    authentication {
        auth_type PASS
        auth_pass 1234
    }
    virtual_ipaddress {
        192.168.56.120 dev enp0s8 label enp0s8:vip
    }
}
```

/var/lib/ssdb/notify.sh

This is the script that is called by **Keepalived** during state transitions. Note that the value assigned to **USER** should be the username that owns the **SSDB** process.

```
#!/bin/bash
# This must be run as root.

ENDSTATE=$3
NAME=$2
TYPE=$1

LOG=/var/log/keepalived-state-transition.log
LOG_ERROR=0
LOG_WARNING=1
LOG_INFO=2
LOG_DEBUG=3
LOG_LEVEL=$LOG_INFO

KPCFG=/etc/keepalived/keepalived.conf
USER=<SSDB-user-name>
```

```

PREFIX=/var/lib/ssdb

function log {
    lvl=$1
    msg="$2"
    if [ $lvl -le $LOG_LEVEL ]
    then
        now=$(date)
        echo "$now [$lvl] $msg" >> $LOG
    fi
}

function log_error {
    log $LOG_ERROR "$1"
}
function log_warning {
    log $LOG_WARNING "$1"
}
function log_info {
    log $LOG_INFO "$1"
}
function log_debug {
    log $LOG_DEBUG "$1"
}

function backup {
    log_info "Transitioning to BACKUP state"
    runuser -l $USER -c "${PREFIX}/ssdb-server ${PREFIX}/ssdb.conf -s stop"
    runuser -l $USER -c "cp ${PREFIX}/ssdb_slave.conf ${PREFIX}/ssdb.conf"
    runuser -l $USER -c "${PREFIX}/ssdb-server -d ${PREFIX}/ssdb.conf"
}

function fault {
    log_error "keepalived is in FAULT state"
}

function master {
    log_info "Transitioning to MASTER state"
    runuser -l $USER -c "${PREFIX}/ssdb-server ${PREFIX}/ssdb.conf -s stop"
    runuser -l $USER -c "cp ${PREFIX}/ssdb_master.conf ${PREFIX}/ssdb.conf"
    runuser -l $USER -c "${PREFIX}/ssdb-server -d ${PREFIX}/ssdb.conf"
}

case $ENDSTATE in
"BACKUP") # Perform action for transition to BACKUP state
    backup
    exit 0
;;

```

```

"FAULT") # Perform action for transition to FAULT state
    fault
    exit 0
    ;;
"MASTER") # Perform action for transition to MASTER state
    master
    exit 0
    ;;
*)    echo "Unknown state ${ENDSTATE} for VRRP ${TYPE} ${NAME}"
    exit 1
    ;;
esac

```

Keepalived configuration, Designated (Initial) Backup

[/etc/keepalived/keepalived.conf](#)

This file is almost identical to the same file on the master node. Exceptions:

- **priority** - It is given a lower initial priority.
- It does not contain the **nopreempt** option. Once the backup server has become master due to a failure of the original master, the system should allow for some human intervention before restoring the original server to master status.

```

vrrp_instance VRRP1 {
    state BACKUP
    interface enp0s8
    virtual_router_id 41
    priority 100
    advert_int 1
    notify /var/lib/ssdb/notify.sh

    authentication {
        auth_type PASS
        auth_pass 1234
    }
    virtual_ipaddress {
        192.168.56.120 dev enp0s8 label enp0s8:vip
    }
}

```

The [/var/lib/ssdb/notify.sh](#) for the backup server is identical to the master.

Master-Master Replication

Overview

Another way to ensure that **SSDB** remains highly-available is to set-up master-master replication and

configure a proxy that understands [Redis](#) protocol in front of the two [SSDB](#) servers. The proxy is responsible for monitoring the health of the two servers and removing a failed server from the pool.

The following simplified example uses a single [HAProxy](#) instance in front of two [SSDB](#) servers.

Required Packages

- [SSDB](#). In the examples shown below it is assumed that version [1.9.2](#) or newer is installed.
- [HAProxy](#)

Prerequisites

Install [SSDB](#) on two servers in accordance with the procedure that is applicable to the Linux distribution that you are using. Install [HAProxy](#) on an additional server. Note that [Keepalived](#) can be used to configure a highly-available pool of [HAProxy](#) servers.

Configuration

SSDB Configuration, First Master

Notes:

- Only the configuration related to master-master replication is shown.

```

# ssdb-server config
## ssdb-server config MUST indent by TAB!

# relative to path of this file, directory must exists
work_dir = ./var
pidfile = ./var/ssdb.pid

server:
    ip: 0.0.0.0
    port: 8888
    deny: all
    allow: 127.0.0.1
    # e.g., 192.168.56
    allow: <ip-address-prefix>

replication:
    binlog: yes
    # Limit sync speed to *MB/s, -1: no limit
    sync_speed: -1
    slaveof:
        id: svc_2
        type: mirror
        host: <hostname-of-other-master>
        port: 8888

```

SSDB Configuration, Second Master

Notes:

- Only the configuration related to master-master replication is shown.

```

# ssdb-server config
# MUST indent by TAB!

# relative to path of this file, directory must exists
work_dir = ./var
pidfile = ./var/ssdb.pid

server:
    ip: 0.0.0.0
    port: 8888
    deny: all
    allow: 127.0.0.1
    # e.g., 192.168.56
    allow: <ip-address-prefix>

replication:
    binlog: yes
    # Limit sync speed to *MB/s, -1: no limit
    sync_speed: -1
    slaveof:
        id: svc_1
        type: mirror
        host: <hostname-of-other-master>
        port: 8888

```

HAProxy Configuration

Notes:

- Only the configuration related to **SSDB** is shown.
- **SSDB** supports **Redis** network protocol. You can use **Redis** clients to connect to an **SSDB** server and operate on it. This is what Zimbra Collaboration does.

```

defaults REDIS
    mode tcp
    timeout connect 4s
    timeout server 30s
    timeout client 30s

frontend ft_redis
    bind <published-ip-address>:8888 name redis
    default_backend bk_redis

backend bk_redis
    option tcp-check
    server R1 <first-master-ip-address>:8888 check inter 1s
    server R2 <second-master-ip-address>:8888 check inter 1s

```

Multi-Master Scaling / Replication

Overview

The details of multi-master configuration will not be covered in this document. In essence, you will install and configure multiple independent **SSDB** master-slave pairs using the instructions included above. Each pair will be responsible for storing a subset of the total key-space.

As in the master-master configuration, all of the pairs in the pool of **SSDB** servers will be front-ended by a proxy service that understands **Redis** protocol. It must also be capable of consistently hashing the data keys that are presented such that all requests relating to a particular key always get routed to the same master-slave pair.

One such product is [twemproxy](#) from [Twitter](#).

LDAP Attributes

The the SSDB backend makes use of a resource pool to manage access to the **SSDB** server; threads attempting ephemeral data operations must first acquire a resource from this pool. To that end, two LDAP attributes have been introduced to control the pool configuration.

zimbraSSDBResourcePoolSize controls the size of the pool. This determines how many client threads can simultaneously perform ephemeral API operations. By default this is set to 0, which results an unlimited pool size.

zimbraSSDBResourcePoolTimeout controls the amount of time a thread will wait for a resource before throwing an exception. The default is 0, which results in no timeout. This attribute has no effect when the pool size is 0, as threads will never have to wait for resources to be freed in order to perform ephemeral data operations.

A non-zero timeout value is recommended when the pool size is finite. Otherwise, a lost **SSDB** connection may cause mailboxd threads to remain blocked indefinitely, even after the connection is re-established. In general, the resource pool should be sized such that the mailbox server is not starved for resources.

Scaling SSDB for Production Load with Zimbra Collaboration

The main characteristics of Zimbra Collaboration production load that affects load on SSDB server are the frequency of authentication requests and frequency of SOAP requests sent by Zimbra Collaboration Web Client and 3rd party SOAP clients. Each authentication request results in a 2 or 3 write operations for SSDB. The write operations update `zimbraLastLogonTimestamp`, `zimbraAuthTokens` and `zimbraCsrfTokenData` values. Note, that `zimbraCsrfTokenData` is updated only when using a CSRF-enabled SOAP client such as Zimbra Collaboration Web Client. Each authenticated SOAP request results in 2 read operations for SSDB.

Minimum Recommended SSDB Configuration

We recommend that your SSDB server has at least 2GB RAM and 1 CPU. If you plan on running additional tools, such as monitoring and configuration management on your SSDB server, consider increasing memory and adding one more CPU core to accommodate additional software. Check out [Zimbra and SSDB Authentication Load Tests](#) for more information.

Conclusion

For installations whose ephemeral data storage requirements will fit in a single instance, simple master-slave replication is the easiest to implement and requires the fewest resources. Master-master replication does allow requests to be load-balanced across both masters; however, each master is also constantly replicating from the other, so **SSDB** must do additional work to maintain consistency.

Class of Service and Accounts

The Class of Service (COS) assigned to an account determines the default attributes for user accounts, and the features to be enabled or denied. Each account is assigned a COS. The COS controls mailbox quotas, message lifetime, password restrictions, attachment blocking, and server pool usage.

A COS is a global object and is not restricted to a particular domain or set of domains.

You can create and edit the classes of services from the Administration Console:

Admin Console:

Home > Configure > Class of Service → *COS*

Managing Features and Settings with a COS

A default COS is created when Zimbra Collaboration is installed. You can modify the default COS and create new ones.

From a COS, you can manage the following functions:

- Features and preferences that users can access.
- Themes and Zimlets that users can access.
- Advanced settings including attachment settings, quotas, and password login policies.
- Web Client Versions (Advanced and Standard).
- Web Services and Desktop Clients (EWS, MAPI and more).
- Offline Mode.
- Retention policies.

As an example, you could create an Executive COS that is configured to enable all features, provide unlimited mailbox quotas, and never purges messages. Another General-Employee COS may also be created, which enables only the mail feature, sets the mailbox quota, and purges messages every 60 days. Grouping accounts to a specific COS allows you update or change account features in bulk. As such, when the COS is changed, all accounts assigned to the COS are changed.

If a COS is not explicitly set for a new account, or if the COS assigned to a user no longer exists, the **default** COS is automatically assigned.

You can create a COS and assign that as a default COS for all accounts that are created on that domain. You can create different COSs and specify which ones are available for the domain. If a domain does not have a COS defined, and you do not specify a COS, the original default COS is automatically assigned when an account is created.

Some COS settings can be overridden either by global settings or by user settings. For example:

- Whether outgoing messages are saved to **Sent** can be changed from the Zimbra Web Client in the user's preferences.

- Attachment blocking set as a global setting can override the COS setting.



Some COS settings assigned to an account are not enforced for IMAP clients.

Selecting Features and Preferences

All the features available for a COS are displayed in its **Features** page. From there, you can select or deselect the features you do not want included in the COS.



Changes made at the account level override the rules in the COS assigned to the account.

You can define the initial preferences for saving and viewing messages, in the **Preferences** page. You can also select a specific locale for the ZWC view. If a locale is not specified, the browser locale is the default.

For a description of the features and preferences, see [Customizing Accounts](#).

Disabling Preferences

By default, Preferences are enabled, and your users can modify the default preferences that are configured for their accounts.

As the Administrator, you can disable Preferences. As a result, the Preferences page will not display in users mailboxes: they therefore cannot modify the default configuration for features that are set up for their accounts.

Setting Default Time Zone

The default time zone setting displayed in an account's Preferences folder is used to localize the time for received messages and calendar activities in the Standard web client.

When the Standard web client is used, the time zone on the computer is not used to set the time a message is received or for calendar activities. Rather, the time zone setting in the **Preferences > Calendar Options** is used.

When using the Advanced web client, the time zone setting on the computer is used as the time stamp for received messages and for calendar activities, not the time zone setting on the **General Information** page.

Because the advanced web client and the Standard web client do not use the same time zone source to render messages, you might notice that a message displayed on multiple clients will be stamped with different times. You can avoid this by setting the computer time zone and the web client time zone set to the same time.

Using Server Pools

In an environment with multiple mailbox servers, the COS is used to assign a new account to a

mailbox server. When you configure the COS, you select which servers to add to the server pool. Within each pool of servers, a random algorithm assigns new mailboxes to any available server.

You can assign an account to a particular mailbox server when you create an account in the New Account Wizard, Server field. Uncheck **auto** and enter the mailbox server in the Server field.

Setting Account Quota

An account quota is the storage limit allowed for an account. Email messages, address books, calendars, tasks, and Briefcase files contribute to the volume of the quota. Account quotas can be set for a COS or for individual accounts from the Administration Console.

If you set the quota to 0, accounts do not have a quota.

Viewing Account Quotas

To view account quotas for all accounts on a domain:

Admin Console:

Home > Configure > Domains → *domain* → Mailbox Quota

Notifying Users When Maximum Quota is Near

Users can be notified that their mailboxes are nearing their quota. The quota percentage can be set and the warning message text can be modified: Go to the **Quotas** container for a specified Class of Service:

Admin Console:

Home > Configure > Class of Service → *COS* → Advanced → Quotas

When the displayed/configured threshold is reached, a quota warning message is sent to the user.

Setting Quotas in Domains

You can set a maximum mailbox quota for a domain. The default for the domain mailbox quota is unlimited. The domain quota is the maximum amount of storage that can be used by all mailboxes within the domain.

You can set an aggregate quota as well. The sum of the quotas for all accounts in the domain can exceed the size of the aggregate.

An aggregate quota policy for how to handle messages that are sent or received once the aggregate quota has been reached can be set up. The policy options include:

- Continue to allow messages to be sent and received as usual.
- Do not allow messages to be sent.
- Do not allow messages to be sent or received.

Notifications can be automatically sent when the quota is within a configured percentage of the

aggregate quota. A cron tab job runs daily to check the aggregate quota percentage and if the percentage has been reached, the quota warning email is sent.



When a domain quota is set, the effective quota for an account is the minimum quota setting of either the domain or account.

To configure domain quotas, go to the **Domain Quota Setting** container for a specified domain:

Admin Console:

Home > Configure > Domains → *domain* → Advanced → Domain Quota Setting

Managing Excess Quota

You can set how message delivery is handled when a user's mailbox exceeds the configured quota. The default behavior is for the MTA to temporarily send the message to the deferred queue. When the mailbox has sufficient space, the message is delivered. You can change this behavior to either have messages bounce back to the sender instead of being sent to the deferred queue first or you can configure to send the message to the mailbox even if the quota has been exceeded.

To bounce messages instead of sending them to the deferred queue:

```
zmprov mcf zimbraLmtpPermanentFailureWhenOverQuota TRUE
```

To send the message to the mailbox even if the quota has been exceeded:

```
zmprov mc {cos-name} zimbraMailAllowReceiveButNotSendWhenOverQuota TRUE
```

When this attribute is set to TRUE, a mailbox that exceeds its quota is still allowed to receive new mail and calendar invites. This quota bypass is only implemented for messages. All other mail items are still affected by the quota.

Managing Passwords

If you use internal authentication, you can quickly change an account's password from the Account's toolbar. The user must be told the new password to log on.



If Microsoft Active Directory (AD) is used for user authentication, you must disable the Change Password feature in the COS. The AD password policy is not managed by Zimbra.

If you want to make sure users change a password that you create, you can enable **Must Change Password** for the account. The user must change the password the next time he logs on.

Password restrictions can be set either at the COS level or at the account level. You can configure settings to require users to create strong passwords and change their passwords regularly, and you can set the parameters to lock out accounts when incorrect passwords are entered.

Directing Users to Your Change Password Page

If your ZWC authentication is configured as external auth, you can configure Zimbra Collaboration to direct users to **your password change page** when users change their passwords. You can either set this URL as a global setting or a per domain setting.

Set the `zimbraChangePasswordURL` attribute to the URL of your password change page.

In ZWC, **Change Password** in **Preferences > General** links to this URL, and when passwords expire, users are sent to this page.

Modifying the password for the domain:

```
zmprov md example.com zimbraChangePasswordURL https://auth.example.com
```

Configuring a Password Policy

If internal authentication is configured for the domain, you can require users to create strong passwords to guard against simple password harvest attacks. Users can be locked out of their accounts if they fail to sign in after the maximum number of attempts configured.

To set password policy, use the **Password** container for a specified Class of Service:

Admin Console:

Home > Configure > Class of Service → COS → Advanced → Password

The password settings that can be configured are listed below.

Table 34. Password Options

Password Options	Description
Minimum/Maximum password length	Specifies the required length of a password. The default minimum and maximum are 6 and 64 characters, respectively.
Minimum/Maximum password age	Configures the password expiration date. Users can change their passwords at any time between the minimum and maximum. They must change it when the maximum password age is reached.

The following settings require users to add complexity to their passwords.

Minimum upper case characters	Uppercase A - Z
Minimum lower case characters	Lowercase a - z
Minimum punctuation symbols	Non-alphanumeric, for example !, \$, #, &, %
Minimum numeric characters	Base 10 digits 0 - 9
Minimum numeric characters or punctuation	Combined Non-alphanumeric and digits

Password Options	Description
Minimum number of unique passwords history	Number of unique new passwords that a user must create before an old password can be reused.
Minimum password age (Days)	Minimum days between password changes
Maximum password age (Days)	Maximum days between password changes
Password locked	Users cannot change their passwords. This should be set if authentication is external.
Must change password	User is required to change password at first sign in.
Change password	When enabled, users can change their password at any time within the password age settings from their account Preferences tab.

Managing Login Policies

You can set the maximum number of failed login attempts before the account is locked out for the specified lockout time. This type of policy is used to prevent password attacks.

To set user login policy, use the **Failed Login Policy** container for a specified Class of Service:

Admin Console:

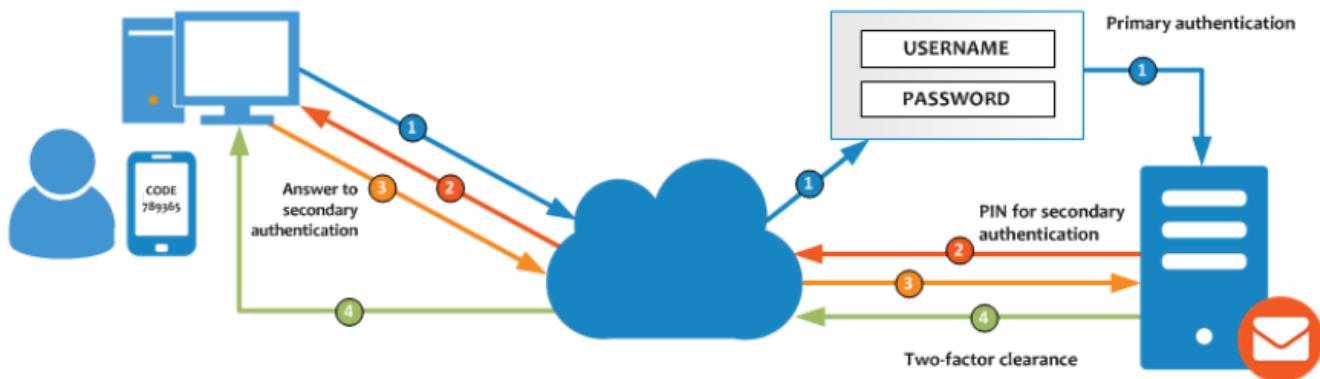
Home > Configure > Class of Service → COS → Advanced → Failed Login Policy

Table 35. Login Policy Options

Login Policy Options	Description
Enable failed login lockout	This enables "failed login lockout" feature. You can configure the following settings.
Number of consecutive failed logins allowed	Number of failed login attempts before the account is locked out. The default is 10. If set to 0, the account is never locked out.
Time to lockout the account	Amount of time the account is locked out. If this is set to 0, the account is locked out until the correct password is entered, or the administrator manually changes the account status and creates a new password. The default is 1 hour.
Time window in which the failed logins must occur to lock the account	Duration of time after which the number of consecutive failed login attempts is cleared from the log. If this is set to 0, the user can continue attempts to authenticate, no matter how many consecutive failed login attempts have occurred. The default is 1 hour.

About 2 Factor Authentication

With the 2 Factor Authentication (FA) feature—introduced in Release 8.7—you can apply additional security policies to COS and/or user accounts to provide another layer of authentication during attempts to access the system. This feature must be enabled or disabled in the Admin Console, to manage 2FA functions applicable to user mailboxes.



For more information, see [2 Factor Authentication](#).

Managing Session Timeout Policies

You can set the period of time to allot for user sessions, as based on various conditions.

To set session timeout policy, use the **Timeout Policy** container for a specified Class of Service:

Admin Console:

Home > Configure > Class of Service → COS → Advanced → Timeout Policy

Table 36. Session Timeout Policy Options

Session Timeout Policy Options	Description
Admin console auth token lifetime	Sets a browser cookie that contains the admin auth token. Administrators can open the Administration Console without having to log on again until the auth token expires. The default is 12 hours.
Auth token lifetime	Sets a browser cookie that contains the ZWC auth token. User can open ZWC without having to log on again until the auth token expires. The default is 2 days. When it expires, the login page is displayed and the user must log on to continue.
Session idle lifetime	How long a user session remains active, if no activity occurs. Activity includes any clickable mouse action, such as viewing folder contents or clicking a button. The default is unlimited.

You can manually expire a user's web client session from the Administration Console **Expire Sessions** link. This forces the current session of the account to expire immediately.

Managing Default External COS

The defaultExternal COS is assigned to external virtual accounts that are created when external users accept a ZCS provisioned users' invitation to share their calendar or briefcase items.

This account is not provisioned on the server, but the external user can sign in to ZWC, create a display name and set a password to view the shared items. The only folders available are for the content they have access to.

The defaultExternal COS is configured with the following general features: Change password, Change UI themes, HTML compose, Export and Search. None of the major features are configured.

Customizing Accounts

This chapter describes the features and user preferences that can be configured for an account, either from the assigned COS or in an individual account.



Mailbox features are enabled for Zimbra Web Client users. When IMAP or POP clients are used, users might not have these features available.

Messaging and Collaboration Applications

Your COS configuration and assignment of a COS to accounts determines the default settings for account features and the restrictions to be applied to groups of accounts. Individual accounts can be configured differently, and any changes you make override the COS setting. When you update the COS, the changes are not reflected in accounts that have COS overrides.

Email Messaging Features

You configure which email messaging features are enabled. Users can then manage many of the enabled features as preferences.

By default, users manage their own preferences, but you can administratively elect not to allow user modifications to their account preferences. Currently supported ZWC Email Messaging Features are listed and described in [Email Features](#).

Table 37. Email Features

Email Messaging Feature	Description
Mail	Enables the email application. Enabled by default. See COS > Features → Major Features container in the Admin Console.
Conversations	Messages can be grouped into conversations by a common thread. The default is to thread messages in a conversation by the References header. If there is no References header, the Subject is used to determine the conversation thread. To change the default, update attribute <code>zimbraMailThreadingAlgorithm</code> from the COS or for individual accounts. See changing conversations thread default . If this feature is enabled, conversation view is the default. You can change the default on the COS Preferences page. Users can also change the default. See COS > Features → Mail Features container in the Admin Console.

Email Messaging Feature	Description
HTML compose	<p>Users can compose email messages with an HTML editor. They can specify default font settings as a preference.</p> <p>See COS > Preferences → Composing Mail container in the Admin Console.</p>
Draft auto save interval	<p>Frequency of saving draft messages. The default is every 30 seconds. Users cannot change the frequency, but they can turn off the save draft feature.</p> <p>See COS > Preferences → Composing Mail container in the Admin Console.</p>
Mail send later	<p>When enabled, users can choose Send Later to send a message at a later time. The user configures the date and time for sending. Messages are saved in the Draft folder.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>
Message priority	<p>When enabled, users can set the priority of the message. The recipient viewing from ZWC sees the priority flag if it is high or low.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>
Enable Attachment indexing	<p>Attachments are indexed. Indexed attachments can be searched.</p> <p>See COS > Advanced → Attachment Settings container in the Admin Console.</p>
Allow the user to specify a forwarding address	<p>You can specify a default forwarding address that the user can use. Users can change the forwarding address from their account Preferences tab.</p> <p>You can also specify forwarding addresses that are hidden from the user. A copy of a message sent to the account is immediately forwarded to the designated forwarding address.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>
Out of office reply	<p>Users can create an email message that automatically replies to incoming messages. By default a message is sent to each recipient only once every seven days, regardless of how many messages that person sends to the address. This setting can be changed in the COS Preferences page, Out of office cache lifetime field.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>

Email Messaging Feature	Description
New mail notification	<p>Allows users the option to specify an address to be notified of new mail. They can turn this feature on or off and designate an address from their account Preferences tab.</p> <p> See Customize the notification email, for an example of changing the email template.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>
Persona	<p>When enabled, users can create additional account names to manage different roles. Account aliases can be selected for the From name of messages sent from that persona account and a specific signature can be set for the persona account. The number of personas that can be created is configurable depending on your requirements. The minimum is 0, and the default is 20 (zimbraIdentityMaxNumEntries).</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>
Maximum length of mail signature	<p>The maximum number of characters that can be in a signature. The default is 1024 characters.</p> <p>The number of signatures users can create is configured in zimbraSignatureMaxNumEntries.</p> <p>See COS > Preferences → Composing Mail container in the Admin Console.</p>
Advanced search	<p>Allows users to build a complex search by date, domain, status, tags, size, attachment, Zimlets, and folders.</p> <p>See COS > Features → Search Features container in the Admin Console.</p>
Saved searches	<p>Users can save a search that they have previously executed or built.</p> <p>See COS > Features → Search Features container in the Admin Console.</p>
Initial search preference	<p>When enabled, the default search mailbox can be changed.</p> <p>See COS > Features → General Options container in the Admin Console.</p>
External POP access	<p>When enabled, users can retrieve their POP accounts' email messages directly from their ZWC account. They add the external account address to their account settings.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>

Email Messaging Feature	Description
External IMAP Access	<p>When enabled, users can retrieve their IMAP accounts' email messages directly from their ZWC account. They can add the external account address to their account settings.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>
Aliases for this account	You can create an aliases for the account. Users cannot change this.
Mail filters	<p>Users can define a set of rules and corresponding actions to apply to incoming and outgoing mail and calendar appointments. When an incoming email message matches the conditions of a filter rule, the corresponding actions associated with that rule are applied.</p> <p> Spam check on a received message is completed before users' mail filters are run. Message identified as spam are moved to the junk folder. To avoid having mail incorrectly marked as spam, users can create a spam whitelist from the Preferences Mail folder to identify email addresses that should not be marked as spam.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>
Flagging	<p>Users can create flags and assign them to messages, contacts, and files in Briefcase folders.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>
Enable keyboard shortcuts	<p>Users can use keyboard shortcuts within their mailbox. The shortcut list can be printed from the Preferences Shortcuts folder.</p> <p>See COS > Preferences → General Options container in the Admin Console.</p>
Global Address List (GAL) access	<p>Users can access the company directory to find names for their email messages.</p> <p>See COS > Features → General Features container in the Admin Console.</p>
Autocomplete from GAL	<p>When enabled, users enter a few letters in their compose header and names listed in the GAL are displayed ranked by usage. See also Autocomplete Ranks Names.</p> <p>See COS > Features → General Features container in the Admin Console.</p>

Email Messaging Feature	Description
Offline support for Advanced (Ajax) client	<p>When enabled, users can use the offline mode to access their data without network connectivity when using the Zimbra Web Client. See also Offline Mode.</p> <p>See COS > Features → General Features container in the Admin Console.</p>
IMAP access	<p>Users can use third party mail applications to access their mailbox using the IMAP protocol.</p> <p>You can set the polling interval from the COS or Account Advanced page, Data Source > IMAP polling interval section. The polling interval is not set by default.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>
POP3 access	<p>Users can use third party mail applications to access their mailbox using the POP protocol. When they retrieve their POP email messages, the messages and attachments are saved on the Zimbra server.</p> <p>Users can configure from their Preferences > Mail page</p> <ul style="list-style-type: none"> • How messages are downloaded. • Whether to include their junk messages. Junk messages are downloaded to their Inbox. • How to delete messages from their POP account. <p>You can set the polling interval from the COS or Account Advanced page, Data Source > POP3 polling interval section. The polling interval is not set by default.</p> <p>See COS > Features → Mail Features container in the Admin Console.</p>

Autocomplete Ranks Names

The autocomplete feature displays names ranked with the most frequently recalled contact listed at the top. If the contact name that appears first should not be listed at the top, the user can click **Forget** and the contact names are re-ranked.

Email Preferences that Users Manage

The default behavior for many of the preferences listed in this section can be set from either the COS or the Accounts Preferences page. Users can modify the following mail preferences from their account Preferences Mail page.

- How often, in minutes, that the Web Client checks for new messages, **Check for new mail**

every...

- Set or change email message alerts. Alerts can be set up to play a sound, highlight the Mail tab when a message arrives, and flash the browser.
- Set the display language for ZWC. If more than one language locale is installed on Zimbra Collaboration, users can select the locale that is different from the browser language settings.
- Whether to save copies of outbound messages to the Sent folder.
- Whether to save a local copy of a message that is forwarded or to have it deleted from their mailbox.
- Whether to compose messages in a separate window.
- Whether to view mail as HTML for messages that include HTML or to view messages as plain text.
- Whether to send a read receipt when it is requested.
- Adjust the default font size for printed messages. The default is 12 points.
- Users can set up their own Spam mail options of whitelist and blacklist email addresses that is used to filter incoming message from their Preferences Mail folder. The default maximum number of whitelist and blacklist addresses is 100 on each list. This value can be changed using CLI `zmprov` for accounts and COS. The attributes are `zimbraMailWhitelistMaxNumEntries` and `zimbraMailBlacklistMaxNumEntries`.
- Users can modify the following mail preferences from their **Preferences Signatures** page.
 - Whether to automatically append a signature to outgoing messages.
 - Preferences for how messages that are replied to or forwarded are composed.

Using Import and Export to Save User's Data

The **Preferences Import/Export** page lets users export all of their account data, including mail, contacts, calendar, and tasks. They can export specific items in their account and save the data to their computer or other location.

The account data is saved as a tar-gzipped (tgz) archive file so that it can be imported to restore their account. Individual contacts are saved as .csv files, and individual calendar files are saved as .ics files. The data are copied, not removed from the user's account.

The exported account data file can be viewed with an archive program such as WinRAR archiver. Any of these files can be imported into their account from the same page.

You can turn the Import/Export feature off from the **COS** or **Account Features** page, **General Features** section.

Setting Up RSS Polling Intervals

Users can subscribe to Websites that provide RSS and podcast feeds and receive updated information directly to their mailboxes. The maximum number of feeds that can be returned is 50. RSS feeds count against users' account quota.

The default is to update the RSS data every 12 hours. Users can right-click on an RSS feed folder to

manually load new feed.

You can change the polling interval from the Administration Console the COS or Account **Advanced** page, **Data Source > RSS polling interval** section.

Address Book Features

The Zimbra Address Book allows users to create multiple contact lists and add contact names automatically when mail is received or sent. Users can import contacts into their Address Book.

To allow users to share their mail folders, address books, and calendars, enable Sharing on the **General Features** container:

Home > Configure > Class of Service → COS → Features → General Features

Table 38. Address Book Features

Feature	Description	COS/Account Tabs
Address Book	Users can create personal contacts lists. By default, a Contacts list and Emailed Contacts list are created.	Features
Address book size limit	Maximum number of contacts a user can have in all address books. 0 means unlimited.	Advanced

Users can modify the following Address Book preferences from their account **Preferences Address Book** page.

To set default behavior:

Admin Console:

Home > Configure > Class of Service → COS → Preferences

Home > Manage > Accounts → account → Preferences

- Enable auto adding of contacts to automatically add contacts to their Emailed Contact list when they send an email to a new address.
- Enable the ability to use the Global Access List when using the contact picker to look up names.
- Enable the options to include the GAL addresses and names in shared address books when using autocomplete to address a message.

Calendar Features

Zimbra Calendar lets users schedule appointments and meetings, establish recurring activities, create multiple calendars, share calendars with others, and delegate manager access to their calendars. They can subscribe to external calendars and view their calendar information from Zimbra Web Client. They can also use search for appointments in their calendars.



To allow users to share their calendars, address books, and Briefcase files, enable Sharing in the **General Features** container.

Admin Console:

Home > Configure > Class of Service → **COS** → **Features** → **General Features**

Table 39. Calendar Features

Calendar Feature	Description	COS/Account Tabs
Calendar	Lets users maintain their calendar, schedule meetings, delegate access to their calendar, create multiple personal calendars, and more.	Features
Group Calendar	When Group Calendar is not checked, users can create personal appointments and accept invitations to meetings only. The Find Attendees, Schedule and Find Resources tabs are not displayed.	Features
Nested Calendars	Calendars can be nested within Zimbra Collaboration folders like Mail, Contact, and Calendar folders. The administrator creates a nested list of calendars using CLI. A nested calendar grouping can be imported through migration as well. See example below.	
Time zone	Sets the time zone to use for Calendar scheduling. Domain admins set this in the Accounts, General Information page.	Preferences
Forward calendar invitation to specific addresses	You can specify email addresses to forward a user's calendar invitations. Users can also specify forwarding address from the Preferences Calendar folder. The account the invitation is forwarded to must have admin privileges on the shared calendar to reply to the invitation.	Accounts Forwarding

Create a calendar nested under the "Calendar Name" folder:

```
zmmailbox -z -m user1 cf -V appointment "/Calendar Name/Sub Calendar"
```

Troubleshooting Calendar Appointment Problems

Use the `zmcalchk` command to check for discrepancy between different users' calendars for the same meeting, and send an email notification regarding the discrepancies.

You can also use this command to notify the organizer and/or all attendees when an appointment is out of sync.

Changing Remote Calendar Update Interval

Remote calendars are updated every 12 hours, by default. The frequency can be modified at the Admin Console.

To modify the frequency of calendar updates in the Admin Console go to the desired COS or Account **Advanced** page, **Data Source > Calendar polling interval** field.

Disabling Attendee Edits to Appointments

Attendees can edit appointments in their calendars, but their changes do not affect anyone else. If the appointment organizer makes changes, these changes overwrite the attendees edits. You can modify the COS attribute `zimbraPrefCalendarApptAllowAtendeeEdit` to prevent attendees from editing appointments in their calendar.

```
zmprov mc <cosname> zimbraPrefCalendarApptAllowAtendeeEdit FALSE
```

Setting Other User Calendar Preferences

Users can modify the Calendar preferences listed in the Calendar Preference table. You can set the default behavior in the COS or Accounts Preferences page.

Calendar Preference	Description
Time zone	Time zone displayed in the user's Preferences. See Setting Default Time Zone . If the time zone is configured in the COS, the time zone configured in the domain is ignored.
Number of minutes before an appointment to show reminder	Sets the minutes before the meeting to send a reminder notice.
Initial calendar view	Sets the default view. Options are Day, Work Week, 7-Day Week, Month, List, or Schedule.
First day of the week	Sets the default first day of a user's work week.

Calendar Preference	Description
Default appointment visibility	<p>Options are Public or Private. Sets the default visibility options on the new appointment page.</p> <p>The default is Public, appointments details can be viewed by others.</p> <p>When the default is Private, all incoming calendar invites are marked as private on the user's calendar and details are hidden.</p>
Use iCal delegation model for shared calendars for CalDAV	<p>Apple iCal can be configured to access users' calendars using the CalDAV protocol. When enabled, shared calendars are displayed in users' iCal account's Delegation tab and they can delegate access to their calendars.</p> <p>For automatic polling, the polling interval can be set up in the COS or Account Advanced page, Data Source > CalDAV polling interval field.</p>
Enable past due reminders	<p>Users log into the ZWC, the reminder notifications for the last two weeks pop up for meeting reminders that were not dismissed. When this is disabled, Zimbra Collaboration silently dismisses the old reminders.</p>
Enable toaster notification for new calendar events	<p>A popup displays in ZWC when new calendar events are received.</p>
Allow sending cancellation email to organizer	<p>When users receive an invitation they cannot attend at the scheduled time, they have the option to click Propose New Time and select another time. The meeting organizer receives an email with the proposed time.</p>
Automatically add invites with PUBLISH method	<p>A calendar invitation email should have method=REQUEST in the calendar object but some third-party email clients incorrectly set method=PUBLISH. These emails are not processed as invitations by default. You can relax the rules by enabling this option.</p>
Automatically add forwarded invites to calendar	<p>Invites that have been forward to users are automatically added to the forwarded recipient's calendar.</p>
Flash browser title on appointment reminder	<p>When appointment reminders pop up, the browser flashes until the user closes the pop-up.</p>
Enable audible appointment notification	<p>When an appointment reminder pops up, users can be notified by a beep on their computer. Users must have either QuickTime or Windows Media installed.</p>

Calendar Preference	Description
Auto-decline invites from users who are denied from inviting this user	Users can configure who can send them calendar invites. When enabled, an auto-reply message is sent to those users to let them know they do not have permission to invite the user.
Automatically add appointments when invited	When enabled, appointments are automatically added to user's default calendar and declined appointments display on the ZWC calendar in a faded view.
	 When viewing appointments from mobile devices users do not see the deleted invite information in a faded view and they might not know that the invite was deleted.
Notify of changes made via delegated access	Users that delegated their calendar are notified of changes made to an appointment by a delegated access grantee.
Always show the mini-calendar	The mini-calendar automatically displays in the Calendar view.
Use the QuickAdd dialog when creating new appointments	When is enabled, the QuickAdd dialog displays when users double-click or drag on the calendar.
Show time zone list in appointment view	When enabled, a time zones list displays in their appointment dialog, giving them the opportunity to change time zones while making appointments.

Setting Up Zimbra Tasks

Zimbra Tasks lets users create to-do lists and manage tasks through to completion.



To allow users to share their Task lists, enable Sharing in the Features page. Task lists can be shared with individuals, groups, and the public.

To enable or disable the Tasks feature:

Admin Console:

Home > Configure > Class of Service → COS → Features

Home > Manage > Accounts → account → Features

Zimbra Web Client User Interface Themes

The appearance of the Zimbra Web Client user interface can be changed. A number of Zimbra themes are included with ZCS, and you can create others. You can select a theme to be the default and the themes that users can select to customize their user experience. To develop themes, see [Color and Logo Management](#).

The following theme usage options can be configured either from COS or by individual accounts.

- **Limit users to one theme**

On the Features page, remove the check mark from **Change UI Themes**. The ZWC theme is the theme listed in Current UI theme field on the Themes page.

- **Let users access any of the installed Zimbra themes**

If the **Change UI Themes** is checked, users can access any of the themes that are listed in the Available UI themes list.

Two Factor Authentication

The Two Factor Authentication (2FA) function allows you to configure a secondary set of security requirements that may be applicable to any or all critical mailboxes or users in the environment. You can set 2FA for user accounts and/or class of service.

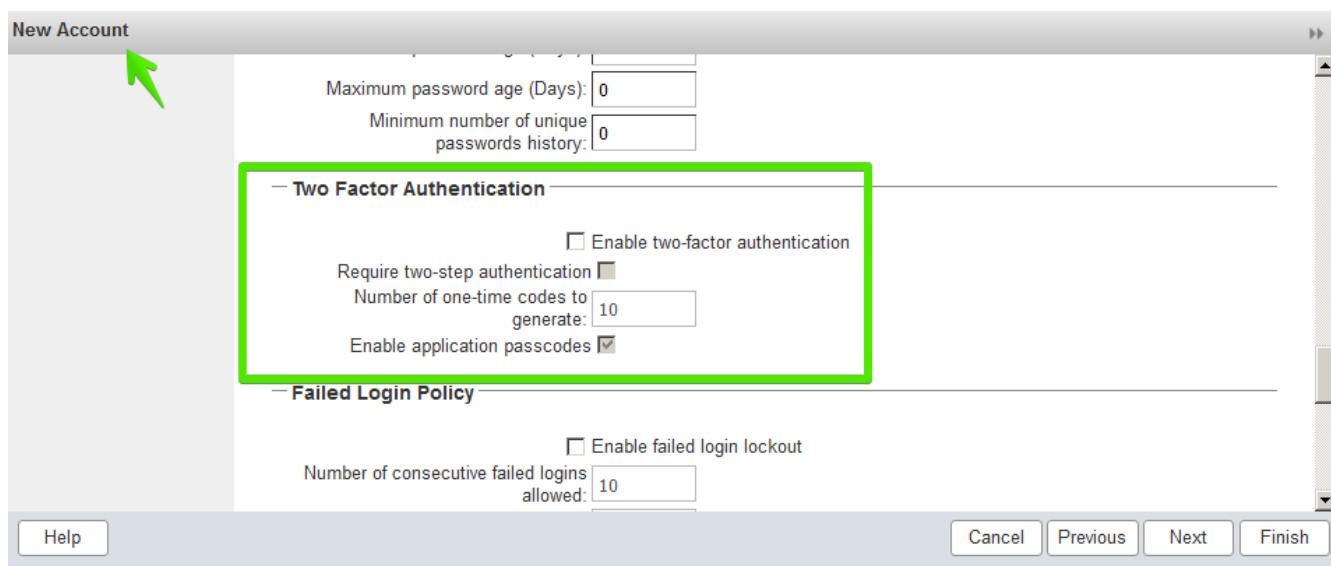
2FA for New User Account

In the Wizard setup for a new user account, you will find settings for 2FA with other **Advanced** options.

Admin Console:

Home → **3 Add Accounts** → **1. Add Account**

—Next until **Advanced**, scroll down to **Two Factor Authentication**



See [Two Factor Authentication Parameters](#) for parameter descriptions.

2FA for Existing User Account

For an existing user account, you can apply 2FA settings from the **Advanced** options.

Admin Console:

Home > Manage > Accounts

Locate the **Two Factor Authentication** container within the editable configurations for an account:

1. Select an *account* from the list of accounts.
2. Select **Edit** from the **Gear** icon.
 - The **General Information** for the *account* is now displayed.
3. Select **Advanced** from the left panel.
4. Scroll down to the **Two Factor Authentication** container in the main panel.

The screenshot shows the Zimbra Administration interface. On the left, there's a sidebar with various account management options like General Information, Contact Information, Member Of, Features, Preferences, Aliases, Forwarding, Free/Busy Interop, Themes, Zimlets, Mobile Access, and Advanced. A green arrow points to the 'Advanced' option, which is currently selected. In the main pane, it shows a user profile for 'd d. sss' with details like Email: anything@jhurley1.us.zimbralab.com, Quota: 0 MB of unlimited, and various status metrics. Below this, there are several expandable sections: Attachment Settings, Quotas, Data Source, Proxy Allowed Domains, Password, and Two Factor Authentication. The 'Two Factor Authentication' section is highlighted with a green border. It contains the following parameters:

Enable two-factor authentication	<input type="checkbox"/>
Active	<input checked="" type="checkbox"/>
Require two-step authentication	<input checked="" type="checkbox"/>
Number of one-time codes to generate:	10
Enable application passcodes	<input checked="" type="checkbox"/>

See [Two Factor Authentication Parameters](#) for parameter descriptions.

2FA for Class of Service

Parameters you can use to set up 2FA for a Class of Service are included with other Advanced features.

To apply 2FA to a class of service, use the **Two Factor Authentication** container to set parameters.

Admin Console:

Home > Configure > Class of Service → **COS** → Advanced → **Two Factor Authentication**

The screenshot shows the Zimbra Administration interface. On the left, there's a sidebar with various tabs: General Information, Features, Preferences, Themes, Zimlets, Server Pool, Mobile Access, Advanced (which is highlighted with a blue background), Retention Policy, and ACL. Below these are Related and Accounts tabs. The main content area has a title 'Home - Configure - Class of Service - default - Advanced'. It contains several input fields for password complexity (symbols, minimum/maximum age, history) and a 'Two Factor Authentication' section. This 'Two Factor Authentication' section is highlighted with a green border and contains four items: 'Enable two-factor authentication' (checked), 'Require two-step authentication' (unchecked), 'Number of one-time codes to generate:' (set to 10), and 'Enable application passcodes' (checked). A green arrow points from the top right towards the 'Two Factor Authentication' section.

See [Two Factor Authentication Parameters](#) for parameter descriptions.

Table 40. Two Factor Authentication Parameters

Parameters	Description
Enable two factor authentication	Enable (check) or disable (un-check) this function for the selected COS account.
Require two-step authentication	Enable (check) or disable (un-check) mandatory use of this function for the selected COS account.
Number of one-time codes to generate	<p>Value to assign maximum number of 6-digit passcodes that may be viewed/used by the account when attempting to access the system. The passcode is presented to the account once the initial login credentials are accepted.</p> <p>Each passcode has a 15-second life cycle.</p>
Enable application passcodes	For legacy application that do not support two-factor authentication, you can generate exceptions codes for them.

Other Configuration Settings for Accounts

Enable Sharing

When the Sharing feature is enabled, users can share any of their folders, including their mail folders, calendars, address books, task lists, and Briefcase folders.

A user specifies the type of access permissions to give the grantee. A user can share with internal users who can be given complete manager access, external guests who must use a password to view the folder content, as well as public access so that anyone who has the URL can view the folder's content.

When internal users share a mail folder, a copy of the shared folder is put in the grantee's folder list on the Overview pane. Users can manage their shared folders from their ZWC Preferences Sharing page.

Configure SMS Notification

The ZWC **Preferences > Notification** page lets users configure an email address or SMS alert to their mobile device to receive a reminder message for a task or a meeting on their calendar. Notification by SMS is disabled by default.

SMS notification can be configured by domain, COS or for individual accounts. SMS notification set in a COS overrides SMS notifications set on a domain. In the Administration Console, this is set on the domain, COS or account's Feature page.

Users select a region and a carrier when setting up their SMS alert. The list of SMS/email gateways is in **ZmSMS.properties**. You can customize this list to add SMS/email gateways that are not listed.

Configure Attachment Viewing

You can set attachment viewing rules as a global setting, by COS, or for a specific account. The global setting takes precedence over COS and account Settings. You can select from four options.

Table 41. Attachment Viewing Features

Feature Name	Description	COS/Account Tabs
Disable attachment viewing from web mail UI	Attachments cannot be viewed. This can also be set as a global setting.	Advanced
Attachments can be viewed in HTML only	Attachments received in another format are opened in HTML view.	Advanced
Attachments can be viewed in their original format only	 Users might not be able to open attachments that require a specific application that is not on their computer.	Advanced
Attachments can be viewed in HTML and their original format	Users can select to open either in the original format or as HTML.	Advanced

Display a Warning When Users Try to Navigate Away

Users can click the Back and Forward arrows in the browser, or close their browser without logging out of their account.

- If this preference is checked, users are asked to confirm that they want to navigate away from their account.
- If this preference is not checked, the question is not asked.

Enabling the Check Box for the Web Client

If **Show selection checkbox for selecting email, contact, voicemail items in a list view for batch operations** is enabled, when users view email messages, contacts, and tasks lists in the Content pane, a check box displays for each item. Users can select items and then perform an action such as mark as read/unread, move to a specific folder, drag and drop to a folder, delete, and tag for all those selected items.

Preferences Import/Export

The Preferences Import/Export page lets users export all of their account data, including mail, contacts, calendar, tasks, and Briefcase folders. They can export specific items in their account and save the data to their computer or other location. The account data is saved as a tar-gzipped (tgz) archive file so that it can be easily imported to restore their account. Individual contacts are saved as **.csv** files, and individual calendar files are saved as **.ics** files. The data are not removed from their accounts. The exported account data file can be viewed with an archive program such as WinRAR archiver. Any of these files can be imported into their account from the same page.

If you do not want users to the Import/Export capability, you can disable the feature from the COS or Admin Features page.

Adding Words to Spell Dictionary

If ZWC users frequently use words, abbreviations or acronyms that are marked as spelling errors during a ZWC spell check, you can update the COS or domain attribute **zimbraPrefSpellIgnoreWord** with the words that should be ignored when spell check is run.

To configure words to ignore for a domain:

```
zmprov md example.com +zimbraPrefSpellIgnoreWord <word> +zimbraPrefSpellIgnoreWord  
<word2>
```

Hierarchical Address Book (HAB) in Zimbra

What is a HAB?

The hierarchical address book (HAB) allows users to look for recipients in their address book using organizational hierarchy. Typically, users only see the default global address list (GAL) whose structure doesn't help understand who reports to whom or to identify one John Doe from another. Being able to customize a HAB, which maps to your organization's unique business structure, provides your users with an efficient method for locating internal recipients.

Using Hierarchical Address Book

In a Hierarchical Address Book (HAB), your root organization (e.g., Zimbra) is the top-level tier. Under this top-level tier, you can add several child tiers to create a customized HAB that is segmented by division, department, or any other organizational level you want to specify. The following figure illustrates a HAB for Zimbra with the following structure:

- The top-level tier represents the root organization — Zimbra.
- The second-level child tiers represent the business divisions within Zimbra — Corporate Office, Engineering, Product Support, and Sales & Marketing.
- The third-level child tiers represent departments within the Corporate Office division — Human Resources, Accounts, and Administration.

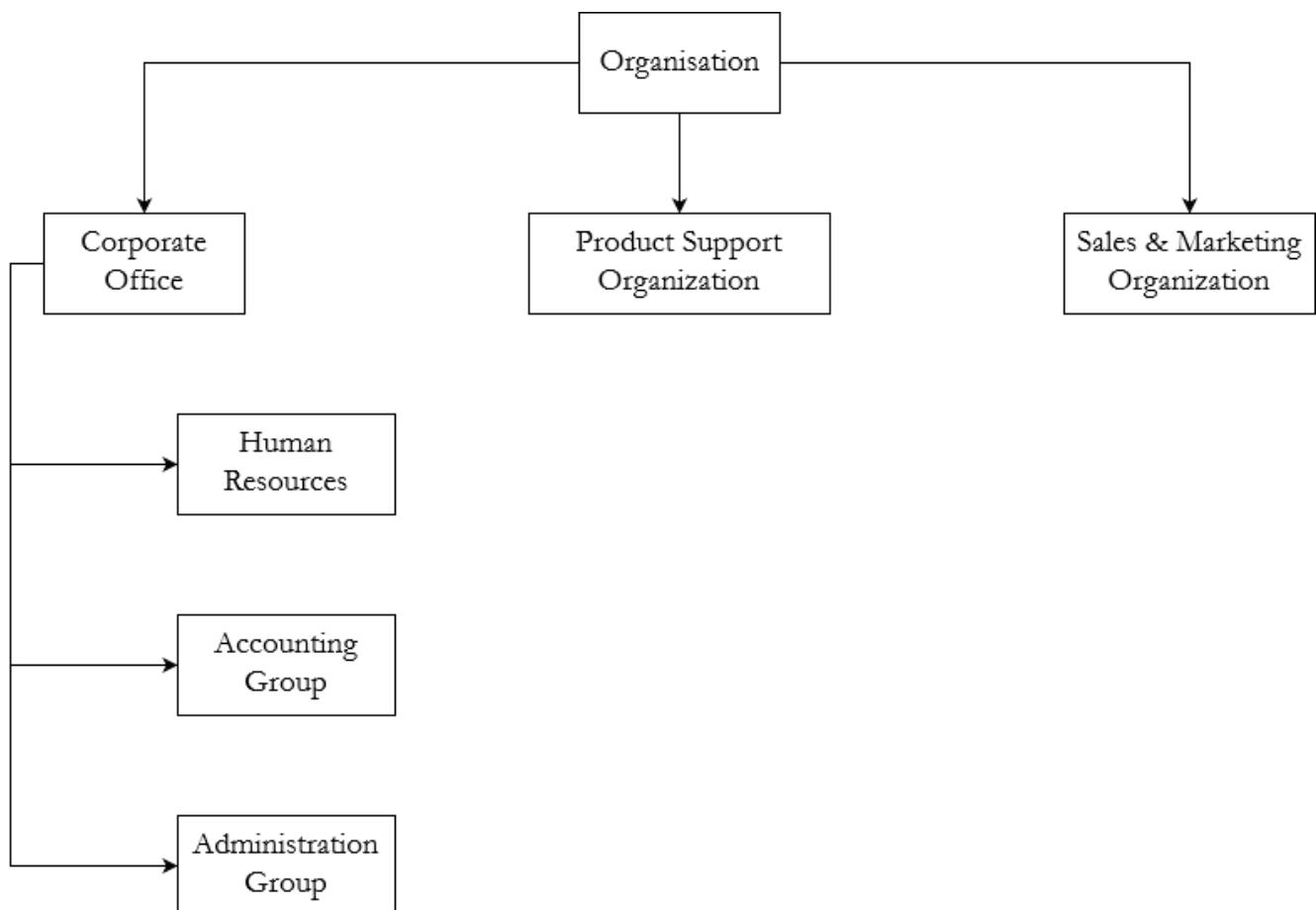


Figure 1. Example Hierarchy

Seniority Index

Seniority Index provides an additional level in the hierarchy. When creating a HAB, use this parameter to rank individuals or organizational groups by seniority within these organizational tiers. This ranking specifies the order in which HAB displays recipients or groups. A higher seniority index ensures that a user or group appears above another with a lower seniority index.

- **100** for Vice President
- **50** for Administration Operations Manager
- **25** for Business Administrator



If the **Seniority Index** parameter isn't set or is equal for two or more users, the HAB sorting order lists the users and groups in ascending alphabetical order.

Configuring hierarchical address books

Create an organizational unit (OU)

Format

```
zmprov createHABOrgUnit <domain name of OU> <OU Name>
```

Example

```
zmprov createHABOrgUnit example.com ZimbraOU
```

Explanation

ZimbraOU as an organizational unit created.

Create groups within this OU

You have to create a group and assign an email address for each department.

Format

```
zmprov createHABGroup <name of the group> <name of OU> <group email address>
```

Example

In this series of commands, we create **8** HAB groups — as per the [Example Hierarchy](#).

```
zmprov createHABGroup Zimbra ZimbraOU zimbra@example.com
```

```
zmprov createHABGroup CorporateOffice ZimbraOU CorpOffice@example.com
```

```
zmprov createHABGroup Engineering ZimbraOU eng@example.com
```

```
zmprov createHABGroup ProdSupport ZimbraOU prodsupport@example.com
```

```
zmprov createHABGroup SalesAndMarketing ZimbraOU sales-mark@example.com
```

```
zmprov createHABGroup HumanResources ZimbraOU hr@example.com
```

```
zmprov createHABGroup Accounts ZimbraOU accounts@example.com
```

```
zmprov createHABGroup Administration ZimbraOU administration@example.com
```

Create Hierarchy

Each of these groups (except Zimbra) needs to be assigned a parent group to create a hierarchy.

Format

```
zmprov addHABGroupMember ParentGroupEmailAddress ChildGroupEmailAddress
```

In this series of commands, we designate 7 HAB groups — except Zimbra because it is root — as per the hierarchy in the figure [Example Hierarchy](#).

For this, we add **Human Resources**, **Accounts**, and **Administration** to **Corporate Office**; and add **Corporate Office**, **Engineering**, **Product Support**, and **Sales & Marketing** to **Zimbra**.

```
zmprov addHABGroupMember CorpOffice@example.com hr@example.com
```

```
zmprov addHABGroupMember CorpOffice@example.com accounts@example.com
```

```
zmprov addHABGroupMember CorpOffice@example.com administration@example.com
```

```
zmprov addHABGroupMember zimbra@example.com CorpOffice@example.com
```

```
zmprov addHABGroupMember zimbra@example.com eng@example.com
```

```
zmprov addHABGroupMember zimbra@example.com prodsupport@example.com
```

```
zmprov addHABGroupMember zimbra@example.com sales-mark@example.com
```

Get Zimbra ID

zimbraId is a unique identifier associated with an email address. It is used to [assign users to groups](#) and to [specify a group as root](#).



For this example, and everywhere else we have used a placeholder (xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx) for **zimbraId**.

Format

```
zmprov gdl <group email address> zimbraId
```

Example

```
zmprov gdl zimbra@example.com zimbraId
```

Example Output

```
# distributionList zimbra@example.com memberCount=4
zimbraId: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Explanation

zimbra@example.com is the email address of the group which is to become root.

Add users to Groups

This example adds the users *Jane Doe* and *John Smith* to the group named *CorporateOffice* without affecting other existing members.

Format

```
zmprov addHABGroupMember <group email address> <user's email address>
```

Example

```
zmprov addHABGroupMember hr@example.com jane.doe@example.com
```

```
zmprov addHABGroupMember accounts@example.com john.smith@example.com
```

Set Sort Order

Configure the sort order for groups in the HAB. Groups with higher seniority index appear above groups with lower seniority index.

Format

```
zmprov modifyHABGroupSeniority <zimbra ID> <seniority index>
```

Example

To have *Engineering* appear above *CorporateOffice*—irrespective of their names and alphabetical order, get [Zimbra ID](#), decide on a number in place of [SeniorityIndexNumber](#), and run the below command.

Assign *CorporateOffice* a seniority index of 90

```
zmprov modifyHABGroupSeniority xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx 90
```

Assign *Engineering* a seniority index of 100

```
zmprov modifyHABGroupSeniority xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx 100
```



Commands used to set seniority index for groups also set [Seniority Index](#) for users.

Specify the root organization for the HAB

A group needs to be specified as root so that other groups can be added as child groups to comply with the organizational hierarchy. Run below command to make *zimbra@example.com* as root.

Format

```
zmprov md <domain name> zimbraHierarchicalAddressBookRoot <ZimbraID of the group to be made root>
```

Example

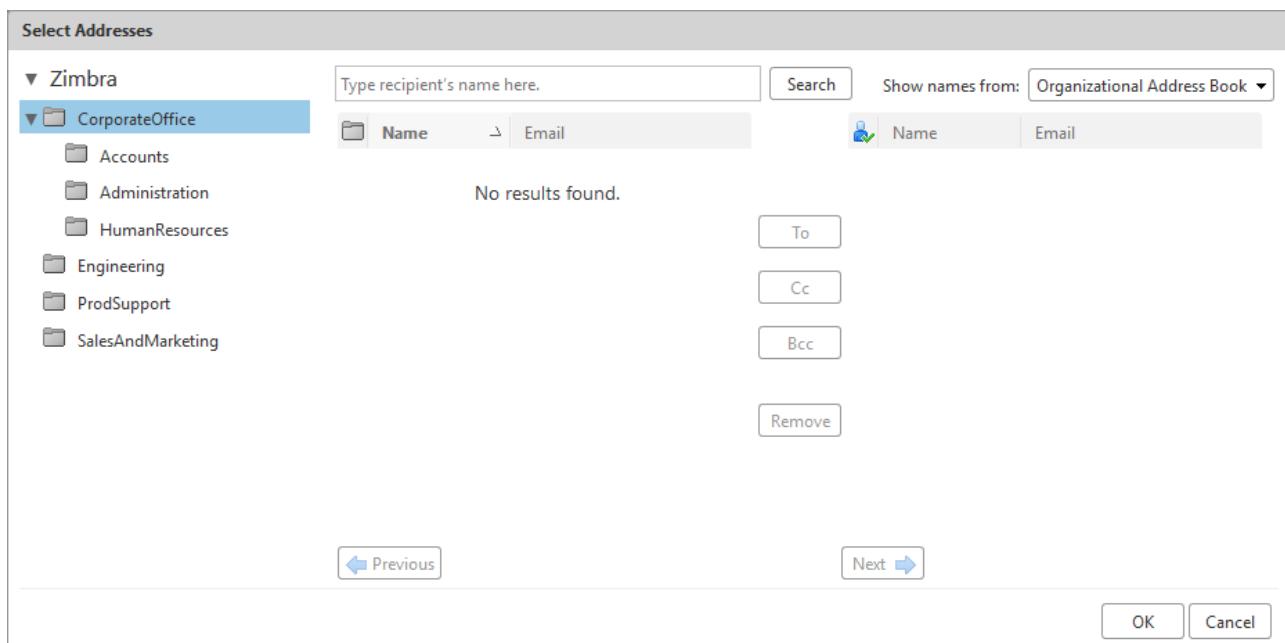
```
zmprov md 'example.com' zimbraHierarchicalAddressBookRoot xxxxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxx
```

Example Output

```
# distributionList zimbra@example.com memberCount=4  
zimbraId: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

Did it work?

1. Log in to Zimbra client.
2. Click **New Message**.
3. In the **Compose** window, click the **To** field.
4. On **Select Addresses** window, locate the **Show Names from:** drop-down on the top right corner.
5. Choose **Organizational Address Book**.
6. The address book in a hierarchical format appears in the left pane.



7. Click any group to view and select users of that group.

Manage Organisational Units (OUs)

List Organisational Units (OUs)

There can be multiple organizational units in a domain. This command lists all the OUs in a specified domain.

Format

```
zmprov listHABOrgUnit <domain name of OU>
```

Example

```
zmprov listHABOrgUnit example.com ZimbraOU
```

Explanation

All OUs in *example.com* listed.

Rename Organisational Units (OUs)

This command renames the specified OU in a domain.

Format

```
zmprov renameHABOrgUnit <domain name of OU> <OU Name> <New name for OU>
```

Example

```
zmprov renameHABOrgUnit example.com ZimbraOU ZMXOU
```

Explanation

ZimbraOU renamed to *ZMXOU*.

Rename Organisational Units (OUs)

This command deletes the specified OU in a domain.

Format

```
zmprov renameHABOrgUnit <domain name of OU> <OU Name>
```

Example

```
zmprov renameHABOrgUnit example.com ZimbraOU
```

Explanation

ZimbraOU deleted.

Provisioning User Accounts

When an account is provisioned, you create the mailbox, assign the primary account email address, and assign a class of service (COS) to enable Zimbra Collaboration applications and features.

You can configure one account at a time or migrate multiple existing accounts from a server.

Creating a Single User Accounts

Before adding a user account, determine which features and access privileges should be assigned. You can either assign a class of service (COS) with the features enabled when you create the account or you can configure the features for the individual accounts. For a description of the features, see [Class of Service and Accounts](#).

If the COS you assign has the correct functionality for the account, you do not need to perform any additional configuration.

Creating an account sets up the appropriate entries on the Zimbra LDAP directory server. When the user logs in for the first time or when an email is delivered to the user's account, the mailbox is created on the mailbox server.

Basic user account setup:

Admin Console:

Home → 3 Add Accounts → 1. Add Account

1. In the **Account Name** section, enter the account name and the last name as a minimum to configure the account.

The default COS is assigned to the account.

2. Click **Finish** to create the account.

You can continue to configure features and functionality for the individual account. Changes you make to the account override the COS that is assigned to the account.

Migrating Accounts and Importing Account Email



ZCS Account Migration within the Zimbra Admin UI is no longer supported, with End of Technical Guidance set for 17 December 2019. We recommend [Audriga's self-service migration solution](#) as a preferred alternative for all account migrations.

You can provision multiple accounts at one time using the Account Migration Wizard from the Administration Console. You can import accounts from either a generic IMAP server or from another ZCS server.



Only accounts on ZCS 7.2 or later can be migrated to ZCS 8.

You can also import account names to provision from an XML file that you create.

You can run the migration wizard one time to provision accounts and import data or you can run the migration wizard the first time to provision the accounts and then run the wizard again to import the provisioned accounts' data.

Whether you get the account records from an LDAP directory or use an XML file, you need to set the password requirements for the newly provisioned accounts. The options are to have ZCS randomly create passwords for each account or to set the same password on each account. You have the option to force users to change the password when they sign in the first time.

When the provisioning is complete, the wizard generates a **.csv** file with a list of new accounts. This includes the passwords that are generated. You should download this file for future reference. Choose a secure location to store the file as it can contain password information for the user accounts you provisioned.

If you're running a split-domain configuration, you can set the SMTP host and port in the wizard. For more information about split domains, see the wiki article about split domains at https://wiki.zimbra.com/wiki/Split_Domain.

Migrating Accounts from a Zimbra Server

To migrate accounts from a server running ZCS 7.2 or later to ZCS 8.

Admin Console:

Home → 3 Add Accounts → 3. Migration and Co-existence

1. In the **Type of mail server** field, select **Zimbra Collaboration**.
2. If you are provisioning accounts, select **Yes** to import the account's records. If you are not going to import the data at this time, in the **Would you like to import mail**, select **No**.
3. Click **Next**.
4. On the **Overview** dialog, Import from another Zimbra LDAP directory is selected. Click **Next**.
5. On the **Bulk provisioning options** page, select whether to generate random passwords or to assign the same password for each account.

Table 42. Bulk Provisioning Features

Bulk Provisioning Feature	Description
Generate random password	If you select Generate a random password for each account, set the length for the password. The password can be from 6 to 64 characters. Default = 8 characters If you select to generate a random password, you must download the .csv file that is created so that you can give the password information to each user.

Bulk Provisioning Feature	Description
Use same password	If you select Use same password for all new accounts, enter the password to use.
Require users to change password after first login	It is recommended that this is checked to force users to change their passwords when they log on the first time.
SMTP Host / SMTP Port	For split domain configurations, set the SMTP Host name and port.

6. Click **Next**.
7. On the **Directory connection** dialog enter the information to connect to the server.

Table 43. Directory Connection Options

Directory Connection Options	Description
Automatically create missing domains	<p>Enable this option to create a domain when an account is imported and the domain they were on is not created.</p> <p>If you do not enable this, accounts from domains that do not exist on the server are not created. Disabling this option makes it easy to import accounts from specific domains that have been pre-created.</p>
Maximum records to fetch	Enter the maximum number of accounts to import at one time. The default is 0, which means that no limits are set.
Server name, LDAP URL, Port, and Use of SSL	<ul style="list-style-type: none"> • The LDAP URL is entered as <code>ldap://<ldapdirectory.example.com></code> • The default port is 389, but you can change this. • Check SSL if this is used.
Bind DN	The Zimbra setting is in the field by default as <code>uid=zimbra,cn=admins,cn=zimbra</code>
Bind password	Enter the password for the server.
LDAP filter	In this field enter the LDAP search filter to run. Here you can define search criteria to collect the type of account information you want to import. The default filter in the field is <code>(objectclass=zimbraAccount)</code> . This filter includes the email address, the account ID, and attributes for the account.
LDAP search base	Configure the subsections of the LDAP forest to search.

8. Click **Next**.

The **Account Migration Wizard** connects to the directory server and generates a report showing the number of domains found; number of accounts found on the server and how many of those accounts are already created on ZCS. This dialog also shows the password options you configured.

9. Review the report generated and then click **Next**. The accounts are provisioned on the Zimbra Collaboration server.
10. Download the **.csv** file that lists the provisioned accounts and their passwords. The **.csv** file is deleted when you close the wizard. If you do not download the file, you cannot access the report later.

Migrating Accounts from Generic IMAP Servers

Use steps in this section to provision accounts on the Zimbra server.

Admin Console:

Home → **3 Add Accounts** → **3. Migration and Co-existence**

1. In the **Type of mail server** field, select **Generic IMAP Server**.
2. If you are provisioning accounts, select **Yes** to import the account's records. If you are not going to import the data at this time, in the Would you like to import mail, select **No**.
3. Click **Next**.
4. On the **Overview** dialog, Import from another LDAP directory is selected. Click **Next**.
5. On the **Bulk provisioning options** page, select whether to generate random passwords or to assign the same password for each account.

Table 44. Bulk Provisioning Features

Bulk Provisioning Feature	Description
Generate random password	If you select Generate a random password for each account, set the length for the password. The password can be from 6 to 64 characters. Default = 8 characters If you select to generate a random password, you must download the .csv file that is created so that you can give the password information to each user.
Use same password	If you select Use same password for all new accounts, enter the password to use.
Require users to change password after first login	It is recommended that this is checked to force users to change their passwords when they log on the first time.
SMTP Host / SMTP Port	For split domain configurations, set the SMTPHost name and port.

6. Click **Next**.

7. On the **Directory connection** dialog enter the information to connect to the server.

Table 45. Directory Connection Options

Directory Connection Options	Description
Automatically create missing domains	<p>Enable this option to create a domain when an account is imported and the domain they were on is not created.</p> <p>If you do not enable this, accounts from domains that do not exist on the server are not created. Disabling this option makes it easy to import accounts from specific domains that have been pre-created.</p>
Maximum records to fetch	Enter the maximum number of accounts to import at one time. The default is 0, which means that no limits are set.
Server name, LDAP URL, Port, and Use of SSL	<ul style="list-style-type: none"> The LDAP URL is entered as: <code>ldap://<ldapdirectory.example.com></code> The default port is 389, but you can change this. Check SSL if this is used.
Bind DN	The Zimbra setting is in the field by default as <code>uid=zimbra,cn=admins,cn=zimbra</code>
Bind password	Enter the password for the server.
LDAP filter	In this field enter the LDAP search filter to run. Here you can define search criteria to collect the type of account information you want to import. The default filter in the field is (<code>objectclass=zimbraAccount</code>). This filter includes the email address, the account ID, and attributes for the account.
LDAP search base	Configure the subsections of the LDAP forest to search.

8. Click **Next**.

The Migration Wizard connects to the directory server and generates a report showing the number of domains found; number of accounts found on the server and how many of those accounts are already created on ZCS. This dialog also shows the password options you configured.

9. Review the report generated and then click **Next**. The accounts are provisioned on the Zimbra Collaboration server.
10. Download the `.csv` file that lists the provisioned accounts and their passwords. The `.csv` file is deleted when you close the wizard. If you do not download the file, you cannot access the report later.

Migrating Accounts using an XML File

Use steps in this section to create an XML file with the account information and save it to a computer you can access.

Admin Console:

Home → 3 Add Accounts → 3. Migration and Co-existence

1. In the **Type of mail server** field, select the type of server your are migrating from.
2. If you are provisioning accounts, select **Yes** to import the account's records. If you are not going to import the data at this time, in the **Would you like to import mail**, select **No**.
3. Click **Next**.
4. On the **Overview** dialog, select **Import from an XML file**.
5. Click **Next**.
6. The **Review** options dialog displays the number of domains; number of accounts and the password options configured in the XML file.
7. If this information is correct, click **Next**. If this information is not correct, fix your XML file before proceeding.

If you clicked **Next**, the accounts are provisioned on the Zimbra Collaboration server.

8. Download the **.csv** file that lists the provisioned accounts and their passwords. The **.csv** file is deleted when you close the wizard. If you do not download the file, you cannot access the report later.

Importing Email for Selected Accounts

Use steps in this section to specify the list of accounts whose mail you want to import by either selecting the accounts to import data or by using an XML file to select the accounts.



Ensure that accounts are provisioned on the ZCS server before attempting this procedure.

Admin Console:

Home → 3 Add Accounts → 3. Migration and Co-existence

1. In the **Type of mail server** field, select the type of server your are importing the data from.
2. In the **Would you like to import account records** menu, select **No**.
3. In the **Would you like to import mail menu**, select **Yes**.
4. Click **Next**.
5. On the **Import options** dialog box, select which way you are going to specify the accounts whose mail is being imported.
6. Click **Next**.

If you are selecting accounts, go to step 7. If you are using an XML file go to step 9.

7. If you are selecting the accounts to import, on the Selected Accounts dialog box, search for the accounts to add. You can search by domain or user name. If you click Search without entering text, all accounts are returned.

Add the accounts to the **Accounts for data import** column.

8. Click **Next**.
9. If you are using an XML file with the accounts listed, browse to the XML file to use.
10. Click **Next**.
11. In the IMAP Connection details dialog box, enter the information necessary to connect to the exporting server's IMAP, this includes the IMAP host name, port and administrator login information.
12. Click **Next**.
13. Review the data import options. If the information is correct, click **Next**.

XML File Examples

This section contains three examples of the XML file structure to provision accounts and import data.

Example 7. Using an XML file to provision accounts

The following example shows an XML file that is used to provision multiple email accounts without importing mail:

```
<?xml version="1.0" encoding="UTF-8"?>
<ZCSImport>
<ImportUsers>
<User>
<sn>Sample</sn>
<givenName>Sam</givenName>
<displayName>Sam Sample</displayName>
<RemoteEmailAddress>ssample@example.com</RemoteEmailAddress>
<password>test123</password>
<zimbraPasswordMustChange>TRUE</zimbraPasswordMustChange>
</User>
<User>
<sn>Zackry</sn>
<givenName>Zak</givenName>
<displayName>Zak Zackry</displayName>
<RemoteEmailAddress>zzackry@example.com</RemoteEmailAddress>
<password>test123</password>
<zimbraPasswordMustChange>TRUE</zimbraPasswordMustChange>
</User>
</ImportUsers>
</ZCSImport>
```

Example 8. Using an XML file to provision accounts from externally hosted domains

The following example shows an XML file that is used to provision multiple email accounts for externally hosted domain without importing mail.

In this example, the `zimbraMailTransport` attribute of newly provisioned accounts will be set to point to external SMTP server instead of the ZCS server.

```
<?xml version="1.0" encoding="UTF-8"?>
<ZCSImport>
<SMTPHost>smtp.example.com</SMTPHost>
<SMTPPort>25</SMTPPort>
<ImportUsers>
<User>
<sn>Sample</sn>
<givenName>Sam</givenName>
<displayName>Sam Sample</displayName>
<RemoteEmailAddress>sam@example.com</RemoteEmailAddress>
</User>
<User>
<sn>Zackry</sn>
<givenName>Zak</givenName>
<displayName>Zak Zackry</displayName>
<RemoteEmailAddress>zzackry@example.com</RemoteEmailAddress>
</User>
</ImportUsers>
</ZCSImport>
```

Example 9. Using an XML file to import email

The following example shows an XML file that is used to import email for one account via IMAP from a gmail account without provisioning the email account in ZCS. The account must be provisioned on ZCS before running this type of XML file.

```
<?xml version="1.0" encoding="UTF-8"?>
<ZCSImport>
<IMAPHost>imap.gmail.com</IMAPHost>
<IMAPPort>993</IMAPPort>
<ConnectionType>ssl</ConnectionType>
<UseAdminLogin>0</UseAdminLogin>
<ImportUsers>
<User>
<sn>Sample</sn>
<givenName>Sam</givenName>
<display_name>Sam Sample</display_name>
<RemoteEmailAddress>sam@example.com</RemoteEmailAddress>
<RemoteIMAPLogin>sam@example.com</RemoteIMAPLogin>
<remoteIMAPPASSWORD>test123</remoteIMAPPASSWORD>
</User>
</ImportUsers>
</ZCSImport>
```

Auto Provisioning New Accounts from External LDAP

Auto provisioning of new accounts from external LDAP is supported via the CLI. This section describes the supported CLI attributes and auto provisioning methods.

Overview

When an external LDAP authentication mechanism - such as external LDAP authentication, preauth, or SPNEGO - is configured for a ZCS domain, you can set up ZCS to automatically create user accounts on ZCS. Primary email address and account attributes are mapped from an external directory. You can configure how and when new accounts should be created from the external directory data.

Three modes are supported for auto-provisioning configuration.

Mode	Description
Eager	ZCS polls the external directory for accounts to auto provision. For this mode, you configure how often the external directory is polled for new users, the maximum number of users to process at each interval, and which domains are scheduled for account auto provision on specified servers. Guidelines are provided in Eager Mode Configuration .

Mode	Description
Lazy	If a user logs into ZWC the first time through one of the authentication mechanisms supported for auto provisioning, and if the user does not exist in the ZCS directory, a new account is automatically created in ZCS for this user. Guidelines are provided in Lazy Mode Configuration .
Manual	Auto provisioning does not occur: instead, the administrator manually searches from the configured external auto-provisioning LDAP source and selects an entry from the search result to create the corresponding Zimbra account for the external entry. Guidelines are provided in Manual Mode Configuration .

When an account is created, the account name (consisting of the characters alongside the @ symbol) is mapped from a user attribute on the external directory that you define in `zimbraAutoProvAccountNameMap`. Other account information, such as first and last name, phone numbers, and address, is populated from the attributes mapped from the external directory based on `zimbraAutoProvAttrMap`. You can review the external directory's attributes to determine those that should be mapped to a Zimbra attribute.

The COS assignment for auto-provisioned accounts is identical to the way that COS is determined for manually provisioned accounts:

- If a COS is defined for the domain, this COS is assigned to the accounts that are created.
- If a domain COS is not defined, the ZCS default COS is assigned.

You can configure a **Welcome** email message to be sent to newly created accounts. The subject and body of this email can be configured with `AutoProvNotification` attributes on the domain.

Auto-Provisioning Attributes

The attributes listed in this section can be used with the `zmprov` command to configure auto provisioning of new accounts with an external LDAP directory.

`zimbraAutoProvMode`

Set auto provision mode as either EAGER, LAZY, and/or MANUAL. Multiple auto-provisioning modes can be enabled on a domain.

`zimbraAutoProvAuthMech`

Set type of authentication mechanism - as either LDAP, PREAUTH, KRB5, or SPNEGO - to enable for LAZY mode. Once a user authenticates via the specified authentication mechanism, and if the user account does not yet exist in the Zimbra directory, an account will be automatically created in the Zimbra directory.

`zimbraAutoProvLdapURL`

Set the LDAP URL of the external LDAP source for auto provisioning

zimbraAutoProvLdapStartTlsEnabled

Enable (TRUE) or disable (FALSE) the StartTLS protocol when accessing the external LDAP server for auto provisioning.

Default = FALSE.

zimbraAutoProvLdapAdminBindDn

Defines the LDAP search bind DN for auto provisioning.

zimbraAutoProvLdapAdminBindPassword

Set the LDAP search admin bind password for auto provisioning.

zimbraAutoProvLdapSearchBase

Set the LDAP search base for auto provisioning, used in conjunction with zimbra [zimbraAutoProvLdapSearchFilter](#).

If not set, LDAP root DSE will be used.

zimbraAutoProvLdapSearchFilter

Defines the LDAP search filter template for account auto provisioning. For LAZY mode, either [zimbraAutoProvLdapSearchFilter](#) or [zimbraAutoProvLdapBindDn](#) must be set.

If both are set, [zimbraAutoProvLdapSearchFilter](#) will take precedence. See [Placeholders](#) for supported placeholders.

zimbraAutoProvLdapBindDn

Defines the LDAP external DN template for account auto provisioning. For LAZY mode, either [zimbraAutoProvLdapSearchFilter](#) or [zimbraAutoProvLdapBindDn](#) must be set.

If both are set, [zimbraAutoProvLdapSearchFilter](#) will take precedence. See [Placeholders](#) for supported placeholders.

zimbraAutoProvAccountNameMap

Defines the attribute name in the external directory that contains local part of the account name. This is the name used to create the Zimbra account. If this is not specified, the local part of the account name is the principal user used to authenticated to Zimbra.

zimbraAutoProvAttrMap

Defines the attribute map for mapping attribute values from the external entry to Zimbra account attributes. Values are in the format of `{external attribute}={zimbra attribute}`. If this is not set, no attributes from the external directory are populated in Zimbra account.

Invalid mapping configuration will cause the account creation to fail. Bad mapping may be due to conditions such as:



- Invalid external attribute name.
- Invalid Zimbra attribute name.
- External attribute contains multiple values; the Zimbra attribute contains only a single value.
- Syntax violation (such as external attribute=string, but Zimbra attribute=integer).

zimbraAutoProvNotificationFromAddress

Defines the email address to put in the **From** header for the Welcome email sent to the newly created account. If not set, no notification email is sent to the newly created account.

zimbraAutoProvNotificationSubject

Template used to construct the subject of the notification message sent to the user when the user's account is auto provisioned.

Supported variables: \${ACCOUNT_ADDRESS}, \${ACCOUNT_DISPLAY_NAME}

zimbraAutoProvNotificationBody

Template used to construct the body of the notification message sent to the user when the user's account is auto provisioned.

Supported variables: \${ACCOUNT_ADDRESS}, \${ACCOUNT_DISPLAY_NAME}

zimbraAutoProvListenerClass

Domain setting to define the class name of auto provision listener. The class must implement the `com.zimbra.cs.account.Account.AutoProvisionListener` interface. The singleton listener instance is invoked after each account is auto created in Zimbra. Listener can be plugged in as a server extension to handle tasks like updating the account auto provision status in the external LDAP directory.

At each eager provision interval, ZCS does an LDAP search based on the value configured in `zimbraAutoProvLdapSearchFilter`. Returned entries from this search are candidates to be auto provisioned in this batch. The `zimbraAutoProvLdapSearchFilter` should include an assertion that will only hit entries in the external directory that have not yet been provisioned in ZCS, otherwise it's likely the same entries will be repeatedly pulled in to ZCS. After an account is auto provisioned in ZCS, `com.zimbra.cs.account.Account.AutoProvisionListener.postCreate (Domain domain, Account acct, String external DN)` will be called by the auto provisioning framework. Customer can implement the AutoProvisionListener interface in a ZCS server extension and get their `AutoProvisionListener.postCreate()` get called. The implementation of customer's post Create method can be, for example, setting an attribute in the external directory on the account just provisioned in ZCS. The attribute can be included as a condition in the `zimbraAutoProvLdapSearchFilter`, so the entry won't be returned again by the LDAP search in the next interval.

zimbraAutoProvBatchSize

Domain | Global setting to define the maximum number of accounts to process in each interval for EAGER auto provision.

zimbraAutoProvScheduledDomains

Server attribute that lists the domains scheduled for EAGER auto provision on this server. Scheduled domains must have EAGER mode enabled in [zimbraAutoProvMode](#). Multiple domains can be scheduled on a server for EAGER auto provision. Also, a domain can be scheduled on multiple servers for EAGER auto provision.

zimbraAutoProvPollingInterval

Domain | Global setting to define the interval between successive polling and provisioning accounts in EAGER mode. The actual interval might take longer since it can be affected by two other factors: [zimbraAutoProvBatchSize](#) and number of domains configured in [zimbraAutoProvScheduledDomains](#).

At each interval, the auto provision thread iterates through all domains in [zimbraAutoProvScheduledDomains](#) and auto creates accounts up to [domain.zimbraAutoProvBatchSize](#). If that process takes longer than [zimbraAutoProvPollingInterval](#) than the next iteration starts immediately instead of waiting for [zimbraAutoProvPollingInterval](#) amount of time.

- If set to 0 when server starts up, the auto provision thread will not start.
- If changed from a non-0 value to 0 while server is running, the auto provision thread will be shutdown.
- If changed from 0 to a non-0 value while server is running, the auto provision thread will be started.

Placeholders

Table 46. Placeholders for use with auto provisioning attributes

Tag	Description	Result
%/n	User name and the @ symbol	This returns <i>user1@example.com</i>
%u	User name without the @ symbol	This returns <i>user1</i> .
%d	Domain	This returns <i>example.com</i>
%D	Domain as dc	This returns <i>example,dc=com</i>

Eager Mode Configuration

With Eager mode, ZCS polls the external directory for accounts to auto provision. You configure how often the external directory is polled for new users, the maximum number of users to process at each interval, and the domains to be scheduled for account auto-provisioning on specified servers.

1. Log in to the ZCS server as zimbra and type [zmprov](#) at the command prompt.

```
zmprov
```

2. Enable EAGER mode on the domain.

```
md <example.com> zimbraAutoProvMode EAGER
```

3. Set the maximum number of accounts to process in each interval

```
md <example.com> zimbraAutoProvBatchSize <#>
```

4. Configure the interval (in minutes) between polling and provisioning of accounts. This must be set to a non-0 value for the auto provisioning thread to start. Default = 15 minutes.

```
ms <server.com> zimbraAutoProvPollingInterval <x minutes>
```

5. Select the domains to be scheduled for auto provisioning. Multiple domains can be scheduled on the server.

A domain can be scheduled on multiple servers.

```
ms <server.com> +zimbraAutoProvScheduledDomains <domain1.com> \
+zimbraAutoProvScheduledDomains <domain2.com>
```

6. Configure the external LDAP settings:

- a. LDAP URL

```
md <example.com> zimbraAutoProvLdapURL "ldap://xxx.xxx.xxx.xxx:<port>"
```

The LDAP port is typically 389.

- b. (Optional) Enable StartTls.

```
md <example.com> zimbraAutoProvLdapStartTlsEnabled TRUE
```

- c. LDAP admin bind DN for auto provision:

```
md <example.com> zimbraAutoProvLdapAdminBindDn "cn=admin, dc=autoprov, dc=company, dc=com"
```

- d. Administrator's LDAP search bind password for auto provision.

```
md <example.com> zimbraAutoProvLdapAdminBindPassword <password>
```

- e. Search template to use when searching for users to auto provision.

Example using the LDAP search filter:

```
md <example.com> zimbraAutoProvLdapSearchFilter "(uid=<%placeholder>)"
```

Refer to [Placeholders](#) for supported placeholders.

- f. LDAP search base for auto provisioning

This is the location in the directory from which the LDAP search begins. This is used with [zimbraAutoProvLdapSearchFilter](#). If this is not set, the LDAP directory root, [rootDSE](#), is the starting point.

```
md <example.com> zimbraAutoProvLdapSearchBase "dc=autoprov,dc=company,dc=com"  
md <example.com> zimbraAutoProvLdapBindDn <"placeholder1">
```

Refer to [Placeholders](#) for supported placeholders.

7. (Optional) Define the attribute name that is mapped to the local part of the account name on the external directory. This is used to define the account name on ZCS. If this is not specified, the local part of the account name is the principal user name used to authenticate to ZCS.

```
md <example.com> zimbraAutoProvAccountNameMap <value>
```

8. (Optional) Map the attribute values from the external entry to the ZCS account attributes. If this is not set up, no attributes from the external directory are populated in the ZCS directory. The value is mapped in the form of [{external attribute}={zimbra attribute}](#).



Invalid mapping configuration will cause the account creating to fail.

To map the "sn" value on the external entry to "displayName" on the Zimbra account and map description value on the external entry to description on the ZCS account, type

```
md <example.com> +zimbraAutoProvAttrMap sn.displayName +zimbraAutoProvAttrMap  
description.description
```

9. (Optional) If you want to send a Welcome email to new accounts, enter the *from* address of the originator.

```
md <example.com> zimbraAutoProvNotificationFromAddress <name@example.com>
```

10. To exit zmprov, type

```
exit
```

Lazy Mode Configuration

Lazy mode auto provisioning automatically creates a new account after a user authenticates from an external authentication mechanisms (LDAP, preauth, Kerberos 5, and/or Spnego).

1. Log in to the ZCS server as zimbra and type `zmprov` at the command prompt.
2. Enable LAZY mode,

```
md <example.com> zimbraAutoProvMode LAZY
```

3. Select the external authentication mechanism for the LAZY mode: LDAP, PREAUTH, KRB5, SPNEGO. You can specify multiple authentication mechanisms.

```
md <example.com> zimbraAutoProvAuthMech <type> +zimbraAutoProvAuthMech <type2>
```

4. Configure the external LDAP settings

- a. LDAP URL:

```
md <example.com> zimbraAutoProvLdapURL "ldap://xxx.xxx.xxx.xxx:<port>"
```

The LDAP port is usually 389.

- b. (Optional) Enable StartTls

```
md <example.com> zimbraAutoProvLdapStartTlsEnabled TRUE
```

- c. LDAP Admin bind DN for auto provision in the format `cn=<LDAPadmin_name>, dc=autoprov, dc=<company_name>, dc=<com>`

```
md <example.com> zimbraAutoProvLdapAdminBindDn <"bindDN">
```

For example, "`cn=admin, dc=autoprov, dc=company, dc=com`"

- d. Administrator's LDAP search bind password for auto provision.

```
md <example.com> zimbraAutoProvLdapAdminBindPassword <password>
```

- e. (Optional) Search template to use when searching for users to auto provision.

Example: using LDAP search filter:

```
md <example.com> zimbraAutoProvLdapSearchFilter "<placeholder>"
```

Refer to [Placeholders](#) for supported placeholders.



zimbraAutoProvLdapSearchFilter or zimbraAutoProvLdapBindDn MUST be configured for LAZY mode.

- f. LDAP search base for auto provision. This is the location in the directory from which the LDAP search begins. This is used with [zimbraAutoProvLdapSearchFilter](#). If this is not set, the LDAP directory root, [rootDSE](#), is the starting point.

```
md <example.com> zimbraAutoProvLdapSearchBase "<location>"
```

For example, "[dc=autoprov,dc=company,dc=com](#)"

- g. (Optional) Define the LDAP external DN template for account provisioning.

```
md <example.com> zimbraAutoProvLdapBindDn "uid=%<placeholder1>, %<placeholder2>"
```

Refer to [Placeholders](#) for supported placeholders.

5. (Optional) Identify the attribute name on the external entry that contains the local part of the account name to be provisioned in ZCS. If this is not specified, the local part of the account name is the principal user used to authenticate to ZCS.

```
md <example.com> zimbraAutoProvAccountNameMap <value>
```

6. (Optional) Map the attribute values from the external entry to the ZCS account attributes. If this is not set up, no attributes from the external directory are populated in the ZCS directory. Value is in the form of [{external attribute}={zimbra attribute}](#).

To map the **sn** value on the external entry to **displayName** on the Zimbra account and map description value on the external entry to description on the ZCS account, type as

```
md <example.com> +zimbraAutoProvAttrMap sn=displayName +zimbraAutoProvAttrMap  
description=description
```

7. (Optional) If you want to send a **Welcome** email to new accounts, enter the *from* address of the originator.

```
md <example.com> zimbraAutoProvNotificationFromAddress <name@example.com>
```

8. Exit zmprov, type **exit**.

Manual Mode Configuration

Use the Manual Mode setting to disable auto provisioning with an external LDAP server.

1. Log in to the ZCS server as zimbra and type **zmprov** at the command prompt.
2. Enable MANUAL mode:

```
md <example.com> zimbraAutoProvMode MANUAL
```

Managing Resources

A resource is a location or equipment that can be scheduled for a meeting. Each meeting room location and other non-location specific resources such as AV equipment is set up as a resource account. The **Manage > Resources** section in the Administration Console shows all resources that are configured for Zimbra Collaboration.

User accounts with the Calendar feature can select these resources for their meetings. The resource accounts automatically accept or reject invitations based on availability.

Administrators do not need to monitor these mailboxes on a regular basis. The contents of the resource mailboxes are purged according to the mail purge policies.

A Resource Wizard guides you through the resource configuration. You can configure the account with the following details about the resource:

- Type of resource, either location or equipment
- Scheduling policy
- Forwarding address to receive a copy of the invite
- Description of the resource
- Contact information, which can be a person to contact if there are issues
- Location information, including room name, specific building location including building and address, and room capacity
- Customize auto response message and signatures to be used in the reply email messages

When you create a resource account, a directory account is created in the LDAP server.

To schedule a resource, users invite the equipment resource and/or location to a meeting. When they select the resource, they can view the description of the resource, contact information and free/busy status for the resource, if these are set up.

When the meeting invite is sent, an email is sent to the resource account, and, based on the scheduling policy, if the resource is free the meeting is automatically entered in the resource's calendar and the resource is shown as Busy.

Set Up the Scheduling Policy

The scheduling policy establishes how the resource's calendar is maintained. The following resource scheduling values can be set up:

- **Auto decline all recurring appointments**—This value is enabled when the resource can be scheduled for only one meeting at a time. No recurring appointments can be scheduled for this resource.
- **Auto accept if available, auto-decline on conflict**—When this option is selected, the resource account automatically accepts appointments unless the resource is already scheduled. The free/busy times can be viewed. You can modify the auto-decline rule to accept some meetings that conflict.
- **Manual accept, auto decline on conflict**—When this option is selected, the resource account automatically declines all appointments that conflict. Appointment requests that do not conflict are marked as tentative in the resource calendar and must be manually accepted. If you set this up, configure the forwarding address so a copy of the invite is sent to the account that can manually accept the invitation. You can modify the auto-decline rule to accept some meetings that conflict.
- **Auto accept always**—The resource account automatically accepts all appointments that are scheduled. In this case, free/busy information is not maintained, thus more than one meeting could schedule the resource at the same time. Because the resource always accepts the invitation, the suggested use for this policy would be for a frequently used location off premises that you want the location address to be included in the invite to attendees.
- **No auto accept or decline**—The resource account is manually managed. A delegated user must log into the resource account and accept or decline all requests.

Conflict Rules—For accounts that include the auto decline on conflict value, you can set up a threshold, either as a number of conflicts or as a percentage of all the recurring appointments to partially accept recurring appointments.

Maximum allowed number of conflicts and/or **Maximum allowed percent of conflicts** are configured to allow a recurring resource to be scheduled even if it is not available for all the requested recurring appointment dates.

The resource accepts appointments even if there are conflicts until either the number of conflicts reaches the maximum allowed or the maximum percentage of conflicts allowed. In order for partial acceptance of a series to work, both fields must be set to nonzero values.

Manage Resource Accounts

You can log on to the resource account and set preferences for the resource. The **Resource Accounts Preference > Calendar** can be configured to let users manage the Resource's Calendar. You can configure the following options to manage the resource.

- An address to forward invites. If the forwarding address was set up when the account was provisioned, you can change the address
- Who can use this resource. In the Permissions section, Invites, select **Allow only the following internal users to invite me to meetings** and add the appropriate users' email addresses to the list.

You can share the resource calendar with a user and give the user Manager rights. Users delegated as Manager have full administrative rights for that calendar. They can view, edit, add, remove, accept or decline the invites.

Managing User Accounts

Status of User Accounts

Admin Console:

Home > Manage > Accounts

The status of an account determines whether a user can log in and receive mail. The account status is displayed on the **Accounts** pane of the Administration Console.

Table 47. Status - User Accounts

Status	Description
Active	The normal state for a mailbox account. Mail is delivered and users can log in to the client interface.
Maintenance	Logging is disabled and any mail addressed to this account is queued at the MTA. Note that this state is automatically set for the account during a backup or when importing/exporting/ restoring the account.
Pending	Assignment for an account when it is created but not yet ready to become active. While pending, the login is disabled and messages are bounced.
Locked	The user cannot log in but mail continues to be delivered to the account. The locked state can be set if you suspect that a mail account has been compromised (used in an unauthorized manner).
Closed	Login is disabled and messages are bounced. This status is used to soft-delete the account before deleting it from the server. A closed account does not change the account license.
LockOut	The automatic state that occurs if the user attempts to log in with an incorrect password. A LockOut cannot be administratively assigned but will occur after the number of user attempts exceeds the configured number of attempts allowed. The duration of the lockout is also configurable. The administrator can remove the locked out status at any time.

Deleting an Account

Admin Console:

Home > Manage > Accounts

You can delete accounts from the Administration Console. This removes the account from the server, deletes the messages in the message store, and changes the number of accounts used against your license.



Before you delete an account, run a full backup of that account to save the account information. See also [Backup and Restore](#).

Viewing an Accounts Mailbox

You can view a selected account's mailbox content, including all folders, calendar entries, and tags from the Administration Console.

Admin Console:

Home > Manage > Accounts → *account*

Select an *account*, from the **Gear** icon select **View Mail**. The user's ZWC account opens in a new browser window.

This feature can be used to assist users who are having trouble with their mail account as you and the account user can be logged on to the account at the same time.

Any View Mail action to access an account is logged to the **audit.log** file.

Using an Email Alias

An email alias is an email address that redirects all mail to a specified mail account. An alias is not an email account. Each account can have unlimited numbers of aliases.

When you select Aliases from the Manage Aliases navigation pane, all aliases that are configured are displayed in the content pane. You can create an alias, view the account information for a specific alias, move the alias from one account to another, and delete the alias.

Working with Distribution Lists

A distribution list is a group of email addresses contained in a list with a common email address. When users send to a distribution list, they are sending the message to everyone whose address is included in the list. The address line displays the distribution list address; the individual recipient addresses cannot be viewed.

You can create distribution lists that require an administrator to manage the member list and you can create dynamic distribution lists that automatically manages adding and deleting members in the list. For more information about dynamic distribution lists, see [Using Dynamic Distribution Lists](#).

You can see which distribution lists a user is a member of from the user's account "Member of" page. When a Zimbra user's email address is added to a distribution list, the user's account Member Of page is updated with the distribution list name. When a distribution list is deleted, the distribution list name is automatically removed from the account's Member Of page.

Setting Subscription Policies for Distribution Lists

Subscription policies can be set up to manage a distribution list's membership. Owners of the list

manage the subscription policy from the Properties page of a distribution list.

Distribution Option	Description
New Subscription Requests	<ul style="list-style-type: none">• Automatically accept—Membership is open to anyone who subscribes.• Require list owner approval— To subscribe, users send an email to the owner of the distribution list and the owner replies to this email request.• Automatically reject— No one can be added to this distribution list.
Unsubscription Requests	<ul style="list-style-type: none">• Automatically accept— Anyone can remove their name from the list.• Require list owner approval— To be removed from the distribution list, users send an email to the owner. The owner must accept the email request to remove the name.• Automatically reject— Users cannot remove themselves from the list.

Management Options for Owners of Distribution Lists

You can add owners to distribution lists and they manage the list from their ZWC account's Address Book, Distribution List folder. Owners of a list can right-click a distribution list and click the **Edit Group** link to edit a list.

Besides adding and deleting members, distribution list properties that owners can configure include:

- Marking the list as private so it is hidden in the Global Address List
- Managing who can send messages to the list
- Setting a member subscription policy
- Adding additional owners

Creating a Distribution List

Use steps in this section to create a distribution list:

Admin Console:

Home > Manage > Distribution Lists

1. From the **Gear** icon, click **New**.
2. On the **Members** page, add the distribution list name. Do not use spaces. The other fields are optional.
3. Find members to add to the distribution list in the right column. Select the members to add and click **Add Selected**. If you want to add all addresses on the page, click **Add This Page**. If

you want to add members that are not in the company list, in the **Or enter addresses below** section, type a complete mail address.

4. Click **Next** to configure the **Properties** page.

Table 48. Distribution Properties Options

Distribution Properties Options	Description
Can receive mail	Enabled by default. If this distribution list should not receive mail select this box.
Hide in GAL	Enable to create distribution lists that do not display in the Global Address List (GAL). You can use this feature to limit the exposure of the distribution list to only those that know the address.
Mail Server	This is set to auto by default. To select a specific mail server, uncheck auto and select a specific server from the list.
Dynamic Group	If you check this box, the Member URL field displays and you create a dynamic distribution list. See Create Dynamic Distribution Lists .
New Subscription Requests	Select from: <ul style="list-style-type: none">• Automatically accept• Require list owner approval• Automatically reject
Unsubscription Requests	Select from: <ul style="list-style-type: none">• Automatically accept• Require list owner approval• Automatically reject

5. In the **Members Of** page, select distribution lists that should be direct or indirect members of the list.
6. If the distribution list should have an alias, create it.
7. If this distribution list can be managed by other users, enter these email addresses in the **Owners** page.
8. Set how messages received to the distribution list should be replied to.
9. Click **Finish**. The distribution list is enabled and the URL is created.

Managing Access to Distribution Lists

After a distribution list is created, you can manage who can view members of a distribution list and who can send messages to a distribution list. The default is all users have access to all distribution lists. This section describes how to use the CLI to manage access.

To limit who can access distribution lists, grant rights to individual users on a domain or if you want only members of a domain to access distribution lists, you can grant rights on the domain. When you grant the right on the domain, all distribution lists on the domain inherit the grant.

You can grant the right on individual distribution lists and configure specific users that are allowed to access the distribution list.

You can restrict access to a distribution list from the CLI `zmprov grantRight (grr)` command.



For more information about how granting rights works, see [Delegated Administration](#).

Who Can View Members of a Distribution List

The default is that all users can view members addresses in a distribution list. A distribution list address displays a + in the address bubble. Users can click on this to expand the distribution list. A list of the addresses in the distribution list is displayed. Users can select individual addresses from the expanded list.

Restricting who can view addresses in a distribution list to individuals or to a domain:

- For individual users:

```
zmprov grr domain <domain_name> usr <user1@example.com> viewDistList
```

- For all users in a domain:

```
zmprov grr domain <domain_name> dom <example.com> viewDistList
```

- To grant rights on a distribution list and let specific users view the list:

```
zmprov grr dl <dl_name@example.com> usr <user1@example.com>
```

Who Can Send to a Distribution List

The default is that all users can send messages to all distribution lists. You can grant rights to a distribution list or to a domain that defines who can send messages to a distribution list. When users attempt to send to a distribution list that they are not authorized to use, a message is sent stating that they are not authorized to send messages to the recipient distribution list.



The **Milter Server** must be enabled from **Home > Configure > Global Settings > MTA**.

Restricting who can send messages to a distribution list to individuals or to a domain:

- Granting rights to an individual user in a domain to send messages to all distribution lists.

```
zmprov grr domain <domain_name> usr <user1@example.com> sendToDistList
```

- Granting rights to all users in a domain to send messages to all distribution lists.

```
zmprov grr domain <domain_name> dom <example.com> sendToDistList
```

Restricting access and to remove the restriction to individual distribution lists for different user types.

- Access to specific internal users:

```
zmprov grr dl <dlname@example.com> usr <username@example.com> sendToDistList
```

Revoke access

```
zmprov rvr dl <dlname@example.com> usr <username@example.com> sendToDistList
```

- Access only to members of the distribution list:

```
zmprov grr dl <dlname@example.com> grp <dlname2@example.com> sendToDistList
```

Revoke access

```
zmprov rvr dl <dlname@example.com> grp <dlname2@example.com> sendToDistList
```

- Access only to all users in a domain:

```
zmprov grr dl <dlname@example.com> dom <example.com> sendToDistList
```

Revoke access

```
zmprov rvr dl <dlname@example.com> dom <example.com> sendToDistList
```

- Access only to all users in an external domain:

```
zmprov grr dl <dlname@example.com> edom <example.com> sendToDistList
```

Revoke access

```
zmprov rvr dl <dlname@example.com> edom <example.com> sendToDistList
```

- Access only to internal users:

```
zmprov grr dl <dlname@example.com> all sendToDistList
```

Revoke access

```
zmprov rvr dl <dlname@example.com> all sendToDistList
```

- Access only to all public email addresses:

```
zmprov grr dl <dlname@example.com> pub sendToDistList
```

Revoke access

```
zmprov rvr dl <dlname@example.com> pub sendToDistList
```

- Access only to specific external email address:

```
zmprov grr dl <dlname@example.com> gst <someone@foo.com> "" sendToDistList
```

Revoke access

```
zmprov rvr dl <dlname@example.com> gst <someone@foo.com> "" sendToDistList
```

Enabling View of Distribution List Members for AD Accounts

To view Active Directory distribution list members in messages or in the address book, the GAL group handler for Active Directory must be configured in the ZCS GALsync account for each Active Directory.

Use steps in this section to update the GALsync account for each Active Directory. This configuration requires that you know the GALsync account name and all data sources on that GALsync account.

1. Display the Zimbra ID of the GAL sync account:

```
zmprov gd {domain} zimbraGalAccountId
```

To find the name:

```
zmprov ga {zimbraId-of-the-GAL-sync-account} name
```

2. Display data sources for the GALsync account:

```
zmprov gds {gal-sync-account-name-for-the-domain}
```

3. Enable the group handler for the Active Directory:

```
zmprov mds {gal-sync-account-name-for-the-domain} {AD-data-source-name} \
zimbraGalLdapGroupHandlerClass com.zimbra.cs.gal.ADGalGroupHandler
```

Using Dynamic Distribution Lists

Dynamic distribution lists automatically manage their membership. Users are added and removed from the distribution list automatically. When you create a dynamic distribution list, a member URL is specified. This member URL is used to identify who should be members of the list. You can view this URL from the Administration Console distribution list's Properties page.

You can create dynamic distribution lists from the Administration Console or from the CLI. In the URL, you specify specific object classes that identify the type of users to be added to the dynamic distribution list. For example, you can configure a dynamic distribution list with the object class=zimbraAccount. In this case, when accounts are provisioned or accounts are deleted, the dynamic distribution list is updated.

You can create dynamic distribution lists for all mobile users or POP/IMAP users.

You can modify a distribution list to change the filter rules. When you modify a distribution list, the members in the list are changed to reflect the new rule.

Create Dynamic Distribution Lists

You can create a dynamic distribution list with the admin console or with the CLI, as described in this section.

Admin Console:

[Home > Manage > Distribution Lists.](#)

1. From the **Gear** icon, click **New**.
2. On the **Members** page, add the dynamic distribution list name. Do not use spaces. Do not add members to the list.

3. Click **Next** to configure the **Properties** page.

Table 49. Dynamic Distribution Lists Options

Option	Description
Can receive mail	Enabled by default. If this distribution list should not receive mail select this box.
Hide in GAL	Enable to create distribution lists that do not display in the Global Address List (GAL). You can use this feature to limit the exposure of the distribution list to only those that know the address.
Mail Server	This is set to auto by default. To select a specific mail server, uncheck auto and select a specific server from the list.
Dynamic Group	Check this box.
Can be used in right management	Uncheck this box.

Option	Description
Member URL	<p>The Member URL is an LDAP-type URL defining a filter that determines which users are added to and removed from the list.</p> <p>Type the URL for this list. In the command, <code>ldap:///?sub?</code> is the URL. You can add any combination of filters to this to create different types of dynamic distribution lists.</p>
	<p><i>Example 10. All users, GAL account names, and spam/ham account list</i></p>
	<pre data-bbox="536 541 1133 579">ldap:///?sub?(objectClass=zimbraAccount)</pre>
	<p><i>Example 11. Delegated administrators list</i></p>
	<pre data-bbox="536 788 1389 855">ldap:///?sub?(&(objectClass=zimbraAccount)(zimbraIsDelegatedAdminAccount=TRUE))</pre>
	<p><i>Example 12. All active accounts</i></p>
	<pre data-bbox="536 1073 1389 1140">ldap:///?sub?(&(objectClass=zimbraAccount)(ZimbraAccountStatus=active))</pre>
	<p><i>Example 13. All users with the title manager</i></p> <p>The title is taken from the account's Contact Information Job Title field. In this example, this field would be set to "Manager".</p>
	<pre data-bbox="536 1468 1389 1536">ldap:///?sub?(&(objectClass=zimbraAccount)(title=Manager))</pre>
New Subscription Requests	Select Automatically reject .
Unsubscription Requests	Select Automatically reject .

4. If the dynamic distribution list should have an alias, create it.
5. If this dynamic distribution list can be managed by other users, enter these email addresses in the **Owners** page.

6. If you want to set up a reply to address, enter it here. Any replies to this distribution list are sent to this address.
7. Click **Finish**. The dynamic distribution list is created.

Users are added automatically to the list based on the filter you specified. If you add or delete users, the list is updated.



If you use the CLI to modify a dynamic distribution list originally created on the Administration Console, you must set `zimbraIsACLGroup` **FALSE** for that dynamic distribution list.

Use the CLI `zmprov` command to manage dynamic distribution lists. In the command, `ldap:///?sub?` is the URL. You can add any combination of filters to this to create different types of dynamic distribution lists.

1. Creating a dynamic distribution list of all new and existing accounts

All users, GAL account names, and spam/ham account names are included. When user accounts are deleted, they are removed from the list.

```
zmprov cddl <all@domain.com> zimbraIsACLGroup FALSE \
memberURL 'ldap:///?sub?(objectClass=zimbraAccount)'
```

2. Creating a COS and Assign Users

If you create COSs and assign users to the COS based on specific criteria, such as all managers, you can quickly modify a dynamic distribution list to be used for a specific COS.

Example 14. A dynamic distribution list that includes all users that have active accounts in a specific COS

```
zmprov cddl <allusers@domain.com> zimbraIsACLGroup FALSE \
memberURL 'ldap:///?sub?(&(objectClass=zimbraAccount) (zimbraCOSId=513e02e-9abc-4acf-863a-6dccb38252e3) (zimbraAccountStatus=active))'
```

Example 15. A dynamic distribution list that includes all users based on job titles

To use this, the account's Contact Information **Job Title** field must include the title. In this example it would be set to "Manager".

```
zmprov cddl <allmanagers@domain.com> zimbraIsACLGroup FALSE' \
memberURL ldap:///?sub?(&(objectClass=zimbraAccount) (zimbraCOSId=513e02e-9abc-4acf-863a-6dccb38252e3) (title=Manager))'
```

Example 16. A dynamic distribution list for all delegated administrators

```
zmprov cddl <alldelegatedadmins@domain.com> zimbraIsACLGroup FALSE \
    memberURL 'ldap:///??sub?(&(objectClass=zimbraAccount) (zimbraCOSId=513e02e-
    9abc-4acf-863a-6dccf38252e3) (zimbraIsDelegatedADminAccount=TRUE))'
```

Moving a Mailbox

Mailboxes can be moved between Zimbra servers that share the same LDAP server.

You can move a mailbox from either the Administration Console or use the CLI command **zmmboxmove** to reposition a mailbox from one server to another, without taking down the servers.

The destination server manages the mailbox move process. The move runs in the background and the account remains in active mode until most of the data has been moved. The account is locked briefly to move the last data and then returned to active mode.

The mailbox move process goes through the following steps:

- Mailbox blobs are moved to the new server
- When most of the content has been moved, the account is put into maintenance mode
- Database tables, index directories, and any changed blobs are moved
- The account is put back into active mode

After the mailbox is moved to a new server, a copy still remains on the older server, but the status of the old mailbox is closed. Users cannot log on and mail is not delivered. Check to see that all the mailbox content was moved successfully before purging the old mailbox.

- Moving a mailbox to a new server

```
zmmboxmove -a <email@address> --from <servername> --to <servername>
```

- Purging the mailbox from the old server

```
zmpurgeoldbox -a <email@address> -s <servername>
```

Global Configuration Options for Moving Mailboxes

Global configuration options for moving a mailbox can be set to exclude search indexes, blobs, and HSM blobs when mailboxes are moved. The following configuration options can be set on either the exporting server or the destination server:

- **zimbraMailboxMoveSkipSearchIndex**—If you do not include the search index data, the mailbox

will have to be reindexed after the move.

- **`zimbraMailboxMoveSkipBlobs`** — Blobs associated with the mailbox, including primary and secondary volumes (HSM) are excluded.
- **`zimbraMailboxMoveSkipHsmBlobs`** — This is useful when HSM blobs already exist for the mailbox being moved. Set this if `zimbraMailboxMoveSkipBlobs` is not configured, but you want to skip blobs on HSM volumes.

Delegated Administration (*)

 *Starting with Zimbra 8.8, there are two versions of this feature. Zimbra 8.8 provides Standard and New Generation (NG) versions. Zimbra 8.7 and earlier include the Standard version, which is explained below. To use and enable the NG version of this feature with Zimbra 8.8, refer to the specific NG chapter later in this Guide.

The global administrator can create different delegated administrator roles.

Delegated administrator roles can be as simple as having the rights to manage one or more distribution lists or reset forgotten passwords for one or more users, to having domain administration rights on one or more domains.

Two frequently used delegated administrator roles, domain administrator and distribution list administrator, are already defined. You can add administrators to these predefined roles with no other configuration necessary.

Target Types for Granting Administrative Rights

Delegated administration provides a way to define access control limits on targets and grant rights to administrators to perform tasks on the target.

A target is a Zimbra Collaboration object on which rights can be granted. Each target is associated with a target type that identifies the type of access control entries you can grant on the target.

When selecting a target type for a target consider the following:

- Target. Which specific target are you granting rights? For example, if the target type you select is "domain", which domain do you mean? You specify a specific domain's name (Target Name = example.com). Access Control Entries (ACE) are granted on that target. An ACE is stored in an LDAP attribute on the target entry.
- Is the right you want to grant applicable to the selected target type? A right can only be applied on the relevant target type. For example, creating an account can only apply to a domain target type, and the setting passwords can only apply to accounts and calendar resources target types. If a right is granted on a target that is not applicable to the target, the grant is ignored.
- When defining rights, you need to consider the scope of targets in which granted rights are effective. For example, the right to set the password is applicable only to accounts and calendar resources, but if this right is included in the domain targets list of rights, it is effective for all accounts or calendar resource in the domain.

Table 50. Targets for rights

Target Type	Description of Target Scope
Account	An account entry (a specific user)
Calendar Resource	A calendar resource entry

Target Type	Description of Target Scope
COS	COS entry
Distribution List	<p>Includes the distribution list and all distribution lists under this distribution list.</p> <p>If the right is applicable to accounts and calendar resources, all accounts and calendar resources that are direct or indirect members of this distribution list.</p>
Domain	<p>Applicable to a specific domain, not to any sub-domains.</p> <p>Sub-domains must be explicitly marked as targets.</p> <p>When domain is the target, the rights are granted for all accounts, calendar resources and distribution lists in the domain.</p>
Config	Grants specific to global config
Global ACL	<p>Administrator rights for all entries in a target type. For example, you could add an ACE to the Global Access Control List (ACL) that grants the right to create accounts on domains.</p> <p>Delegated administrator accounts that are granted this right can create accounts in all domains in the system.</p>
Server	Server entry
Zimlet	Zimlet entry

Rights

Rights are the functions that a delegated administrator can or cannot perform on a named target. A right is either system-defined or granted at the attribute level.

System-defined rights

Types of system defined rights include:

- Preset rights (**preset**). For example, `createAccount` creates an account; `renameDomain`, renames the domain.

Preset rights are associated with a fixed target type. For example, `createAccount` is a right only on a domain; `renameAccount` is a right on an account; `getServer` is a right on a server

No other rights are required to administer that action on the target.

Preset rights could involve accessing multiple targets. The grantee needs to have adequate rights on all pertinent targets. For example, to create an alias for an account, the grantee must have rights to add an alias to an account and to create an alias on a domain.

Attribute Right

Granting rights at the attribute level allow a delegated administrator/ administrator group to modify or view (or not modify or view) a specific attribute on a target.

Types of attributes rights include:

- Attribute (`setAttrs`) rights allow the domain administrator to modify and view an attribute value. For example, the `modifyAccount` right allows the domain administrator to modify all attributes of the account.
- Get attribute rights (`getAttrs`) let the domain administrator view an attribute value. For example, the `getAccount` right shows all the attributes for a user's account.

The specific attribute being granted is configured on the target and the type of permission, read (get) or write (set), is specified.

Attribute rights can be granted in any combination of attributes to grant positive or negative rights. This lets you negate some attributes from a grant.

Combo Rights

Combo rights can be assigned to any target type and can include preset rights and attribute rights. You can use combo right to grant multiple attribute rights quickly on targets.

Negative Rights

Rights can be either positive or negative. Negative rights are rights specifically denied to a grantee.

- When a negative right is granted to an admin group, all administrators in the group are denied that right for the target and sub-targets on which the right is granted.
- When a negative right is granted to an administrator who may or may not be in an admin group, the specific administrator is denied that right for the target and sub-targets on which the right is granted.

An admin group is granted domain administrator rights, including the right to create accounts on Domain1. AdminA is in this admin group, but you want AdminA to have all domain administrator rights, except the right to create accounts. You would grant a negative `createAccount` right to AdminA on the target Domain1.

For grants on the same level, negative rights always take precedence. For example, AdminGroup1 is granted a positive right to view accounts in a domain; AdminGroup2 is granted a negative right to view accounts in the same domain. AdminA is a member in both admin groups. AdminA cannot view any account in this domain because the negative right takes precedence.

For grants on different levels, the most specific grant takes precedence. For example, AdminA is granted the negative right to view accounts in GroupDistributionList1, which User1 is a member. AdminA is also granted the positive right to view account directly on User1's account. In this case, AdminA can view User1's account as the grant on the account target is more specific than the grant on the distribution list.

Using the Rights List

System rights are listed and described in the Rights folder in the Administration Console Overview pane. You can use the Rights folder to help you define which system-defined rights to grant to delegated administrators. This folder displays the name of the right, the target types associated with that right, the right type and a brief description.

When you select a right on the page and click on it, another page displays more information:

- For combo rights, a list of the rights associated with the combo right are listed.
- For the other system rights, a list of attributes associated with the right are listed

You can use `zmprov` commands to view combo rights.

- Direct sub-rights of a combo right

```
zmprov gr adminConsoleDLRights
```

- Second level sub-rights of the combo

```
zmprov gr adminConsoleDLRights -e
```

Viewing System Defined Rights Lists

You can use `zmprov` commands to view system defined rights for a specific topic:

Table 51. Viewing Combo Rights with zmprov

To View This	Use This <code>zmprov</code> Command
Account	<code>zmprov gar -t account</code>
Calendar Resources	<code>zmprov gar -t calresource</code>
COS	<code>zmprov gar -t cos</code>
Distribution List ^[4]	<code>zmprov gar -t dl</code>
Domain	<code>zmprov gar -t domain</code>

To View This	Use This <code>zmprov</code> Command
Global Config ^[5]	<code>zmprov gar -t config</code>
Global Grant ^[6]	<code>zmprov gar -t global</code>
Server	<code>zmprov gar -t server</code>
Zimlets	<code>zmprov gar -t zimlet</code>

Implementing Delegated Administration

Before you create delegated administrators and grant rights, define the role and which rights to assign to the targets the administrator will manage.

For more efficient management of delegated administrators, create administrator groups and add individual administrator accounts to the group. An administrator group allows you to create role-based access control. Administrators with the same or almost the same responsibilities can be grouped into an admin group.

Delegated administration rights can be set up in one of the following methods:

- Create an administrator or an administrator group and grant rights to the account using the Administrator Wizard.
- Configure grants on existing administrator accounts. Add new rights or modify rights to an existing delegated administrator or administrator group account.
- Add, modify and delete rights directly in a target's Access Control List page.

Administrator Groups and Administrators

Administrator and group administrator accounts are created in the Administration Console.

Use the administration wizard to

1. Create the create either an Admin Group or an Admin Account.
 - a. **Admin Groups** are distribution lists (DL) that have Admin Group enabled, which flags it as a delegated administrator DL. After the admin group administrator is created and configured with rights and admin views, you add administrator user accounts to the admin group.
 - b. **Admin Account** is a user account that has Administrator enabled on the account.
2. Configure the admin views for the account. You select the views from the Directly Assigned Admin views list. An admin view represent the items the delegated administrator sees when

logged on to the Administration Console.

A directly assigned admin view is the view set on the admin account. An inherited admin view is the view set on the admin group the account belongs to.

3. **Configure the Grants.** The Grants dialog displays a list the grants required to display the items you selected in the Directly Assigned Views column. You can accept these rights and add additional rights, skip this page to not configure these rights, or click **Finish** to accept these rights and quit the wizard.

Configure Grants on Administrator Accounts or Admin Groups

You can manage the rights granted to an administrator or an administrator group through the Configure Grants link on the accounts toolbar. When you click **Configure Grant** on the Manage Accounts Addresses toolbar, the Content pane shows a list of direct and inherited grants. You can grant rights, modify rights or delete rights on existing administrator accounts.

Grant ACLs to a Target

When you want to add a specific grantee or specific rights on a target you can edit the target directly. Each target has an ACL page which lists the granted ACLs. You can add, edit or delete the target's grants. The administration account (grantee) is updated to reflect the change.

Revoking Rights

Global administrators can revoke any rights granted to an administrator.

Admin Console:

[Home > Manage > Accounts](#)

Open the desired administrator account and click **Configure Grants**.

1. Select the *right* to revoke and click **Delete**.
2. When the dialog asks if are sure, click **Yes**.

Delegated administrators can revoke rights if the right was created with the **Can Grant the right to other admins** enabled.

Temporarily Revoke Delegated Admin Rights

To temporarily revoke rights to a delegated administrator account, you can edit the administrator account and remove the check next to the Administrator field. The ACLs are not removed from the account.

View Rights Granted to Administrators

The View Rights link from an admin account or admin group account toolbar displays the granted rights, readable attributes and modifiable attributes associated with a specific target. Click on the

tabs to view rights for different targets.

Predefined Delegated Administrator Role

The following preconfigured administrator groups are created automatically. You can assign administrator accounts to these groups.

Domain Administration Group

The `zimbraDomainAdmins` delegated admin group grants all the rights necessary to support Zimbra Collaboration domain administration for accounts, aliases, distribution lists and resources.

Administrators who are part of the `zimbraDomainAdmins` group can create and manage accounts including setting the account quota, aliases, distribution lists, and resources accounts in their domain.

When domain administrators log onto the Administration Console, only the functions they are authorized to manage are displayed on the console's Navigation pane.

Create Link from Zimbra Web Client Account to Admin Console

For domain administrators, all tasks are performed from the Administration Console. To facilitate easy log in, when a delegated administrator account is created, their ZWC account can have a link to the Administration Console.

The link is created from the `zmprov` CLI

```
zmprov md {server.example.com} zimbraWebClientAdminReference  
{https://server.example.com:7071/}
```

Distribution List Administration Group

The `zimbraDlAdmin` delegated admin group grants all the rights necessary to log on to the Administration Console and manage distribution lists.

Administrators who are part of this group can

- View the account list
- Create new distribution lists and delete distribution lists
- Add, edit and remove members in a distribution list

Creating Delegated Administrator Roles

Manage multiple domains

To have one domain administrator manage more than one domain, you assign the rights to manage individual domains to the administrator account or administrator group.

For example, to set up `domanadministrator1@example.com` to manage `domainexample1.com` and `domainexample2.com`. Create a new administrator account on one of the domains to be managed.

1. Create the administrator account on one of the domains to be managed (`domainexample1.com`)
2. Select the views that domain administrators need to manage a domain. When the views are selected, the rights associated with these views automatically display on the Configure the Grants dialog.
3. Configure the grants for this domain if they are different from the grants associated with the views you select.
4. To add another domain to be managed (`domainexample2.com`).
 - On the Configure Grants page, click **Add**
 - Select the target type as **domain**
 - Enter the target's domain name (`domainexample2.com`)
 - For Right Type, select System Defined Right
 - For Right Name type, `adminConsoleAccountRights`. **Is Positive Right** should be selected.
 - Click **Add and More**
 - The **Add ACE** page displays again and the Right Name field is empty. Type, `adminConsoleDLRights` and click **Add and More**.
 - Continue to add the following right names:
 - `adminConsoleAliasRights`
 - `adminConsoleResourceRights`
 - `adminConsoleSavedSearchRights`
 - `adminConsoleDomainRights`
 - After the last right, click **Add and Finish**. The Configure the Grants dialog displays these rights associated with the target domain. If you are adding another domain to manage, click **Add and More**. Repeat Step 4. If not, click **Finish**.

Manage Distribution Lists

To assign a user to manage a distribution list, you create a distribution list and enable Admin Group, select the view, grant the distribution list rights, add the user to the list and make that user an administrator.

1. Create a new distribution list:
 - Check **Admin Group**
 - Add the user who will be the administrator as a member of the DL.
 - Go to the **Admin Views** page and check **Distribution List View** so the admin can view the distribution list.
 - Click **Save**.
2. In the **Configure Grants** page, add the following rights.

Table 52. Rights

Right Name	Target Type	Target	Right Type
The following right let the administrator manage distribution lists.			
listDistributionList	dl	DL email address	SD Right
addDistributionListAlias	dl	DL email address	SD Right
addDistributionListMember	dl	DL email address	SD Right
modifyDistributionList	dl	DL email address	SD Right
getDistributionListMembership	dl	DL email address	SD Right
removeDistributionListMember	dl	DL email address	SD Right
This domain right displays user account list that the administrator can select from to add to a distribution list.			
listAccount	domain	DL email address	SD Right

Change Passwords

To create delegated administrators who only change passwords, you create the admin or admin group, select the views and grant the set Account Password combo right.

1. Select the following views
 - **Account List** view to be able to select accounts to change passwords
 - **Alias List** view to be able to find users who use an alias instead of account name.
2. The Configure the Grants page displays recommended grants for the views you have chosen. For Change Password rights, do not configure these grants. Select **Skip**. Click **Add** to add the following right:

Right Name	Target Type	Target	Right Type
setAccountPassword	domain	domain name	SD Right

View Mail Access Right

View Mail access right can be granted on accounts, domains, and distribution lists.

Right Name	Target Type	Target	Right Type
adminLoginAs	account, domain, dl	account, domain, or distribution list address	SD Right ^[8]

To prevent administrators from viewing an account with a domain or distribution list, assign the **Is Negative Right** to the account.

Manage Class of Service Assigned to Users

You can expand the domain administrator role to be able to view and change the class of service (COS) assigned to a user. To add the rights to manage the COS for a domain, add the following rights to the domain administrator account or domain administrator admin group.

Add the System Defined Rights to each COS in the domain.

Table 53. System Defined Rights for COS

Right Name	Target Type	Target	Right Type
listCos	cos	COS name	SD Right
getCos	cos	COS name	SD Right
assignCos	cos	COS name	SD Right
This domain right displays the COS information in the user account's General Information page.			
zimbraCOSId	domain	domain name	Attribute Right Verb: Write AR Target: account

Manage Cross Mailbox Search

This role creates a delegated administrator role that can run the Search Mail tool to search mail archives or live mail for accounts. This also allows the administrator to create, abort, delete, purge or get status of a cross mailbox search request.



The Archiving and Discovery feature must be installed for this feature to work.

Right Name	Target Type	Target	Right Type
adminConsoleCrossMailboxSearchRights	(combo)	server name where cross mailbox searches can be run	SD Right

For full functionality, this role includes the ability to create new accounts so that the admin can create the target mailbox to receive the search results. If you do not want this role to have the ability to create accounts, grant the following negative right as well.

Right Name	Target Type	Target	Right Type
CreateAccount	domain	domain name	SD Right ^[10]

If you want this admin to also view the target mailbox with the results of the cross mailbox search, grant the right to view that mailbox only.

Right Name	Target Type	Target	Right Type
adminLoginAs	account	cross mailbox search target account name	SD Right ^[12]

Manage Zimlets

This role creates a delegated administrator role that can create, deploy and view Zimlets.

Right Name	Target Type	Target	Right Type
adminConsoleZimletRights	server, domain	server name or domain name	SD Right
adminConsoleAccountsZimletsTabRights	server, domain	server name or domain name	SD Right

Manage Resources

This role creates a delegated administrator that can create and manage resources.

Right Name	Target Type	Target	Right Type
adminConsoleResourceRights	combo	server name or domain name	SD Right

Access to the Saved Searches

This role creates a delegated administrator that can access all the searches saved in the Administration Console Navigation pane, Search section.

Right Name	Target Type	Target	Right Type
adminConsoleSavedSearchRights	combo	server name or domain name	SD Right

Access to the Server Status Pages

This role creates a delegated administrator that can access the Server Status page. In addition to granting this right, you must also select the Admin View, **Global Server Status View**.

Right Name	Target Type	Target	Right Type
adminConsoleServerStatusRights	global		SD Right



Accounts that are configured as global administrator accounts cannot be granted ACLs. Global administrator accounts automatically have full rights on Zimbra Collaboration. If an ACL is added to a global administrator account, it is ignored. If a delegated administrator account is changed to a global administrator account, any ACLs associated with the account are ignored.

Monitoring ZCS Servers

The Zimbra Collaboration (ZCS) includes the following to help you monitor the Zimbra servers, usage, and mail flow:

- Zimbra Logger package to capture and display server statistics and server status, and to create nightly reports
- Mailbox quota monitoring
- MTA mail queue monitoring
- Log files

Also, selected error messages generate SNMP traps, which can be monitored using an SNMP tool.



Checking the overall health of the system as a whole is beyond the scope of this document.

Zimbra Logger

The Logger includes tools for syslog aggregation and reporting. Installing the Logger is optional, but if you do not install it, server statistics and server status information are not captured.

In environments with more than one Zimbra Collaboration server, Logger is enabled on one mailbox server only. This server is designated as the monitor host. The Zimbra Collaboration monitor host is responsible for checking the status of all the other Zimbra Collaboration servers and presenting this information on the Zimbra administration console. Real-time service status, MTA, spam, virus traffic and performance statistics can be displayed. The Logger creates a daily report about mail activity, such as the number of messages, average delivery delay, and errors generated.



In a multi-server installation, you must set up the syslog configuration files on each server to enable Logger to display the server statistics on the Administration Console, and you must enable the Logger host. If you did not configure this when you installed Zimbra Collaboration, do so now.

Enabling Server Statistics

Enable server statistics to show both system-wide and server specific data about the inbound message volume, inbound message count, anti-spam/anti-virus activity and disk usage for messages processed in the last 48 hours, 30 days, 60 days, and the last year.

1. On each server, as root, type `/opt/zimbra/libexec/zmsyslogsetup`. This updates the syslog configuration to enable gathering server statistics.
2. On the logger monitor host, you must configure **syslog** to accept syslog messages from remote machines. See <https://wiki.zimbra.com/wiki/Configuring-Logger-Host> for details.



These steps are not necessary for a single-node installation.

Reviewing Server Status

Admin Console:

Home > Monitor

The **Server Status** page lists all servers and services, their status, and when the server status was last checked. The servers include the MTA, LDAP, and mailbox server. The services include MTA, LDAP, Mailbox, SNMP, Anti-Spam, Anti-Virus, Spell checker, and Logger.

To start a server if it is not running, use the `zmcontrol` CLI command. You can stop and start services from the Administration Console.

Enabling or Disabling Server Services

Admin Console:

Home > Configure > Servers → *server*

Server services are enabled or disabled from the **Servers → *server*** page. Select **Services** in the Navigation pane and select to enable or disable services.

Viewing Server Performance Statistics

If the Logger package is installed on a Zimbra mailbox server, Server Statistics shows bar graphs of the message count, message volume, anti-spam, and anti-virus activity. The information is displayed for the last 48 hours, and 30 days, 60 days, and 365 days.

When Server Statistics is selected in the Navigation pane, consolidated statistics for all mailbox servers is displayed. Selecting a specific server in the expanded view shows statistics for that server only. Server specific information also includes disk usage, session information, and mailbox quota details.

The following display system-wide information:

- **Message Count**—counts message transactions. A transaction is defined as either the SMTP receipt of a message per person (by Postfix) or a LMTP delivery of it (by mailboxd) per person. For example, if a message is sent to three people, six transactions are displayed. Three for SMTP to Postfix and three for LMTP to mailboxd. The message count is increased by six.
- **Message Volume**—displays the aggregate size in bytes of transactions sent and received per hour and per day. Graphs show the total inbound data by volume in bytes.
- **Anti-Spam/Anti-Virus Activity**—displays the number of messages that were checked for spam or viruses and the number of messages that were tagged as spam or deemed to contain a virus. The AS/AV count is increased by one per message scanned. One message sent to three people counts as only one message processed by AS/AV.

The Message Count and the Anti-spam/Anti-virus Activity graphs display a different message count because:

- Outbound messages may not go through the Amavisd filter, as the system architecture might not require outbound messages to be checked.
- Messages are received and checked by Amavisd for spam and viruses before being delivered to all recipients in the message. The message count shows the number of recipients who received messages.

Server-specific statistics also include the following details:

- **Disk**—for a selected server displays the disk used and the disk space available. The information is displayed for the last hour, day, month, and year.
- **Session**—displays information about the active Web client, administrator and IMAP sessions. You can see how many active sessions are opened, who is logged on, when the session was created and the last time the session was accessed.
- **Mailbox Quota**—displays information about each account sorted by mailbox size in descending order. See [Monitoring Mailbox Quotas](#).

Configuring Logger Mail Reports

The Logger generates a report about mail activity daily at 11:30 p.m. and sends it to the administrator's email address.

You can configure the number of accounts to include in the report. The default is 25 sender and 25 recipient accounts.

- Changing the number of recipients to add to the report:

```
zmlocalconfig -e zimbra_mtareport_max_recipients=<number>
```

- Changing the number of senders to add to the report:

```
zmlocalconfig -e zimbra_mtareport_max_senders=<number>
```

Configuring Disk Space Notifications

You should regularly review your disk capacity and when disks are getting full, take preventative measures to maintain service. A warning alert email notification is sent to the administrator account when disk space is low. The default is to send a warning alert when the threshold reaches 85% and a critical alert when the threshold reaches 95%.

You can change these values. Use `zmlocalconfig` to configure the disk warning thresholds.

- Warning alerts

```
zmdisklog_warn_threshold
```

- Critical alert:

```
zmdisklog_critical_threshold
```

When starting services with `zmcontrol`, if the threshold is exceeded a warning is displayed before the services are started. You should clean up your disk to free up space.

Monitoring Servers

The Zimbra Collaboration server collects many performance related statistics that can help you diagnose problems and load issues.

Admin Console:

[Home > Monitor > Advanced Statistics](#)

The **Advanced Statistics** page includes advanced graphing options that lets you generate various charts based on statistical information for the CPU, IO, mailboxd, MTA queue, MariaDB and other components.

To chart the graphics in Advanced Statistics, select one of these groups and then select from the list of specific counters for the type of information to display.

The information covers a wide array of data:

- **cpu.csv**— CPU utilization. This group contains counters to keep track ofCPU usage (iowait, idle, system, user, time etc.). CPU information can be tracked both at the server level and the process level.
- **df.csv**— Captures disk usage. Disk utilization is tracked for each diskpartition.
- **fd.csv**—file descriptor count. Keeps track of system file descriptor usageover time. This is primarily used to track down "out-of-file descriptor" errors.
- **mailboxd.csv**— Zimbra Collaboration server and JVM statistics. Mailboxdstores almost all of its statistics here. Interesting numbers to keep track of are heap_used, heap_free, imap_conn, soap_sessions, pop_conn, db_conn_count.
- **mtaqueue.csv**— Postfix queue. This measures the mail queue size innumber of messages and the size in bytes.
- **proc.csv**— Process statistics for Zimbra processes. For example mailboxd/java, MariaDB, OpenLDAP, etc.)
- **soap.csv**— SOAP request processing time.
- **threads.csv**— JVM thread counts. Counts the number of threads with acommon name prefix.
- **vm.csv**— Linux VM statistics (from the vmstat command).
- **io-x.csv** and **io.csv**— store data from the `iostat(1)` command (`io-x.csv` with `iostat -x`).

Configuring Denial of Service Filter Parameters

The denial-of-service filter (DoSFilter) limits exposure to requests flooding over HTTP/HTTPS. The DoSFilter throttles clients sending a large number of requests over a short period of time.

DosFilter is only applied to HTTP and HTTPS requests, in other words, it does not affect requests for any other protocols like POP3, IMAP or SMTP. You can modify the configuration to accommodate your specific environmental needs. DoSFilter is enabled by default on ZCS. Disabling the DoSFilter is not recommended. For information on preventing multiple failed login attempts see [Password Policy](#)

Identifying False Positives

Sometimes Zimbra Connector for Outlook (ZCO), mobile ActiveSync clients, or running some `zmprov` commands trigger the DoSFilter. When this happens, the Zimbra mailbox service is unavailable. You can review the following logs to see if the DoSFilter was applied.

- `/opt/zimbra/log/sync.log`.

Example 17. `sync.log` entry showing the DoSFilter

```
2013-01-15 15:52:20,426 WARN [qtp1635701107-91:https://x.x.x.x/
Microsoft-Server-
ActiveSync?User=zsupport2&DeviceId=App15dddd3NR&DeviceType=iPhone&Cmd=FolderSync]
[name=zsupport2@domain.com;mid=64;ip=10.1.2.3;Cmd=FolderSync;DeviceID=App15K0113UN
3NR;Version=12.1;] sync - Service exception
com.zimbra.common.service.ServiceException: error while proxying request to target
server: HTTP/1.1 503 Service Unavailable
ExceptionId:qtp1635701107-91:https://10.10.0.54:443/Microsoft-Server-
ActiveSync?User=zsupport2&DeviceId=App15K0113UN3NR&DeviceType=iPhone&Cmd=FolderSyn
c:1358286740426:c5ca7f36bb0a038f Code:service.PROXY_ERROR Arg:(url,
STR,"http://mail.domain.com:80/service/soap/SyncRequest")
```

- `/opt/zimbra/log/zmmailboxd.out`

Example 18. `zmmailboxd.out` entry showing the DoSFilter

```
2013-01-15 15:57:32.537:WARN:oejs.DoSFilter:DOS
ALERT:ip=127.0.1.1,session=null,user=null
```

Customizing DoSFilter Configuration

The following attributes are used with `zmprov` to configure the DoSFilter. These attributes can be configured as global settings and as server settings. If these attributes are set in the server, the server settings override the global settings.

You can modify these settings, but the default configuration is recommended.

Attribute	Description
DoSFilter Delay <code>zimbraHttpDosFilterDelay-Millis</code>	The delay given to all requests over the rate limit before they are considered. The default is -1. <ul style="list-style-type: none">• -1 = Reject request• 0 = No delay• Any other value = Delay is in ms <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><code>zmprov mcf zimbraHttpDosFilterDelayMillis {x}</code></div>
DoSFilter Maximum Requests Per Second <code>zimbraHttpDosFilterMaxRequestsPerSec</code>	The maximum number of requests from a connection per second. Requests in excess of this are throttled. The default is 30 and the minimum is 1. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><code>zmprov mcf zimbraHttpDosFilterMaxRequestsPerSec {x}</code></div>
DoSFilter IP Addresses Whitelist <code>zmprov mcf zimbraHttpThrottleSafeIPs {x.x.x.x,192.168.x.x}</code>	IP addresses to ignore when applying the DosFilter. This attribute does not have a default value, however the following loopback IPs are whitelisted by default. <ul style="list-style-type: none">• 127.0.0.1• ::1 <p>The IP addresses should be comma separated.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"><code>zmprov mcf zimbraHttpThrottleSafeIPs {addresses}</code></div>

A mailbox server restart is required after modifying these attributes. Type:

`zmmailboxdctl restart`

Tuning Considerations for ZCS 8.0.3 and later

- **ZCS Member Servers**—ZCS servers under the control of a single masterLDAP server are automatically whitelisted by IP address. These hosts are discovered using a **GetAllServersRequest**. Type as `zmprov gas`.
- **External Provisioning Hosts/SOAP API**—External provisioning hosts can be added to the IP whitelist to ensure that the DoSFilter does not block some requests. For example, a mailbox

reindex might make several calls per second that can trigger the DoSFilter.

Working with Mail Queues

When the Zimbra MTA receives mail, it routes the mail through a series of queues to manage delivery; incoming, active, deferred, held, and corrupt.

The **incoming** message queue holds the new mail that has been received. Each message is identified with a unique file name. Messages are moved to the active queue when there is room. If there are no problems, message move through this queue very quickly.

The **active** message queue holds messages that are ready to be sent. The MTA sets a limit to the number of messages that can be in the active queue at any one time. From here, messages are moved to and from the anti-virus and anti-spam filters before being delivered to another queue.

Messages that cannot be delivered are placed in the **deferred** queue. The reasons for the delivery failures are documented in a file in the deferred queue. This queue is scanned frequently to resend the message. If the message cannot be sent after the set number of delivery attempts, the message fails. The message is bounced back to the original sender. The default for the bounce queue lifetime is five days.

The **held** message queue keeps mail that could not be processed. Messages stay in this queue until the administrator moves them. No periodic delivery attempts are made for messages in the held queue.

The **corrupt** queue stores damaged unreadable messages.

Change the Bounce Queue Lifetime

- The MTA server's bounce queue lifetime is set for five days. To change the default queue lifetime setting

```
zmlocalconfig -e bounce_queue_lifetime={#}
```

- To permanently have messages bounced back to the sender, instead of being sent to the deferred queue first

```
zmlocalconfig -e zimbraLmtpPermanentFailureWhenOverQuota=TRUE
```

Notifying Senders of Bounced Messages

Before the bounce queue lifetime sends the message back to the sender, senders can be notified that the message they sent is in the deferred queue and has not been delivered.

Configure the following attributes to send a warning message to the sender.

- Configure the time after which the sender receives the message headers of email that is still

queued.

```
zmlocalconfig -c postfix_delay_warning_time=0h
```

- Configure the recipient of postmaster notifications with the message headers of mail that the MTA did not deliver.

```
zmlocalconfig -c postfix_bounce_notice_recipient=postmaster
```

- Configure the list of error classes that are reported to the postmaster.

```
zmlocalconfig -c postfix_notify_classes=resource,software
```



See Postfix documentation for details on the impact of changes to these Postfix attributes.

You can monitor the mail queues for delivery problems from the Administration Console.

Viewing Mail Queues

Admin Console:

[Home > Monitor > Mail Queues](#)

If you are having problems with mail delivery, you can view the mail queues from the **Mail Queues** page in the Administration Console to see if you can fix the mail delivery problem. When you open mail queues, the content of the deferred, incoming, active, hold, and corrupt queues at that point in time can be viewed. You can view the number of messages and where they are coming from and going to.

For each queue, the Summary pane shows a summary of messages by receiver domain, origin IP, sender domain, receiver address, sender address, and for the deferred queue, by error type. You can select any of the summaries to see detailed envelope information by message in the Messages pane.

The Messages pane displays individual message envelope information for search filters selected from the Summary pane.

The following mailbox queue functions can be performed for all the messages in a queue:

- Hold** to select a set of messages that you want to hold. Incoming, active, deferred, and corrupt messages can be moved to the Held queue. Messages stay in this queue until the administrator moves them.
- Release** to remove all message from the Held queue. Messages are moved to the Deferred queue.
- Requeue** all messages in the queue being viewed. Requeuing messages can be used to send

messages that were deferred because of a configuration problem that has been fixed. Messages are re-evaluated and earlier penalties are forgotten.

- **Delete** all messages in the queue being viewed.

The Zimbra MTA, Postfix queue file IDs are reused. If you requeue or delete a message, note the message envelope information, not the queue ID. It is possible that when you refresh the mail queues, the queue ID could be used on a different message.

Flushing Message Queues

You can flush the server of all messages. When you click **Flush** on the Mail Queue toolbar, delivery is immediately attempted for all messages in the Deferred, Incoming and Active queues.

Monitoring Mailbox Quotas

Mailbox quotas apply to email messages, attachments, calendar appointments, and tasks in a user's account. When an account quota is reached, all mail messages are rejected. Users must delete mail from their account to get below their quota limit - this includes emptying their Trash, or you can increase their quota.

Viewing Quota

You can check mailbox quotas for individual accounts from **Server Statistics** on the Administration Console. Mailbox Quota gives you an instant view of the Mailbox Size and Quota Used information for each account.

Admin Console:

Home > Monitor > Server Statistics

1. Select the **server** for which you want to view statistics.
2. In the Navigation pane, select **Mailbox Quota**. The Mailbox Quota page displays with the following information:
 - Quota column shows the mailbox quota allocated to the account. Quotas are configured either in the COS or by account.
 - Mailbox Size column shows the disk space used.
 - Quota Used column shows what percentage of quota is used.

Increase or Decrease Quota

From a COS or Account, you can configure a quota threshold that, when reached, sends a message alerting users that they are about to reach their mailbox quota.

Admin Console:

Home > Configure > Class of Service → COS → Advanced

Home > Manage > Accounts → account → Advanced

1. Scroll down to the Quota section.

2. Modify the quota settings.
3. Click **Save**.

Viewing MobileSync Statistics

The **MobileSync Statistics** page in the Monitor section in the admin console displays the number of currently connected ActiveSync devices that are on the Zimbra Collaboration system.

Monitoring Authentication Failures

To protect against dictionary-based and distributed attacks, you can configure the `zmauditwatch`. The script attempts to detect more advanced attacks by looking at where the authentication failures are coming from and how frequently they are happening for all accounts on a Zimbra mailbox server and sends an email alert to the administrator's mailbox.

The types of authentication failures checked include:

- **IP/Account hash check**—The default is to send an email alert if 10 authenticating failures from an IP/account combination occur within a 60 second window.
- **Account check**—The default is to send an email alert if 15 authentication failures from any IP address occur within a 60 second window. This check attempts to detect a distributed hijack based attack on a single account.
- **IP check**—The default is to send an email alert if 20 authentication failures to any account occur within a 60 second window. This check attempts to detect a single host based attack across multiple accounts.
- **Total authentication failure check**—The default is to send an email alert if 1000 auth failures from any IP address to any account occurs within 60 seconds. The default should be modified to be 1% of the active accounts on the mailbox server.

The default values that trigger an email alert are changed in the following `zmlocalconfig` parameters:

- IP/Account value, change `zimbra_swatch_ipacct_threshold`
- Account check, change `zimbra_swatch_acct_threshold`
- IP check, change `zimbra_swatch_ip_threshold`
- Total authentication failure check, change `zimbra_swatch_total_threshold`

Configure `zimbra_swatch_notice_user` with the email address that should receive the alerts.

Viewing Log Files

Zimbra Collaboration logs its activities and errors to a combination of system logs through the syslog daemon as well as Zimbra specific logs on the local file system. The logs described below are the primary logs that are used for analysis and troubleshooting.

Local logs containing Zimbra Collaboration activity are in the `/opt/zimbra/log` directory.

- **audit.log**— This log contains authentication activity of users and administrators and login failures. In addition, it logs admin activity to be able to track configuration changes.
- **clamd.log**— This log contains activity from the anti-virus application clamd.
- **freshclam.log**— This log contains log information related to the updating of the clamd virus definitions.
- **mailbox.log**— This log is a mailboxd log4j server log containing the logs from the mailbox server. This includes the mailbox store, LMTP server, IMAP and POP servers, and Index server.
- **myslow.log**— This slow query log consists of all SQL statements from the mailbox server that took more than `long_query_time` seconds to execute.



`long_query_time` is defined in `/opt/zimbra/conf/my.cnf`.

- **spamtrain.log**— This log contains output from `zmtrainsa` during regularly scheduled executions from the cron.
- **sync.log**— This log contains information about Zimbra Collaboration mobilesync operations.

Other logs include:

- **/opt/zimbra/jetty/logs/**— This is where Jetty-specific activity is logged.
- **/opt/zimbra/db/data/<hostname>.err**— This is the message store database error log.
- **/opt/zimbra/logger/db/data/<hostname>.err**— This is the Logger database error log.

Zimbra Collaboration activity logged to System syslog

- **/var/log/zimbra.log**— The Zimbra syslog details the activities of the ZimbraMTA (Postfix, amavisd, anti-spam, anti-virus), Logger, Authentication (cyrus-sasl), and Directory (OpenLDAP). By default LDAP activity is logged to `zimbra.log`.

Syslog

Zimbra Collaboration modifies the systems syslog daemon to capture data from the mail and local syslog facility to `/var/log/zimbra.log`. This allows syslogd to capture data from several Zimbra Collaboration components including Postfix, Amavis, ClamAV, mailboxd, zmconfigd, and logger. The SNMP module uses the data from the log file to generate traps for critical errors. The zmlogger daemon also collects a subset of the data in this file to provide statistics on the utilization of Zimbra Collaboration via the Administration Console.

By default, mailboxd is configured to log its output to `/opt/zimbra/log/mailbox.log`. You can enable mailboxd to take advantage of a centralized syslogd infrastructure by enabling the following either globally or by server:

```
zmprov mcf zimbraLogToSysLog TRUE
```

Using log4j to Configure Logging

The Zimbra Collaboration server uses `log4j`, a Java logging package as the log manager. By default, the Zimbra Collaboration server has `log4j` configured to log to the local file system. You can configure `log4j` to direct output to another location. Go to the [Log4j website](#) for information about using `log4j`.

ZCS does not check the `log4j` changes. To remove all account loggers and reloads in `/opt/zimbra/conf/log4j.properties`, use the `zmprov resetAllLoggers` command.

Logging Levels

The default logging level is set to include logs that are generated for INFO, WARNING, ERROR and FATAL. When problems start to occur, you can turn on the DEBUG or TRACE log levels.

To change the logging levels, edit the `log4j` properties, `log4j.properties`, `log4j.logger.zimbra`.

When enabling DEBUG, you can specify a specific category to debug. For example, to see debug details for POP activity, you would type `logger.zimbra.pop=DEBUG`.

The following categories are predefined in `log4j`:

<code>zimbra.account</code>	Account operations
<code>zimbra.acl</code>	ACL operations
<code>zimbra.backup</code>	Backup and restore
<code>zimbra.cache</code>	Inmemory cache operations
<code>zimbra.calendar</code>	Calendar operations
<code>zimbra.dav</code>	DAV operations
<code>zimbra.dbconn</code>	Database connection tracing
<code>zimbra.extensions</code>	Server extension loading
<code>zimbra.filter</code>	Mail filtering
<code>zimbra.gal</code>	GAL operations
<code>zimbra imap</code>	IMAP protocol operations
<code>zimbra.index</code>	Index operations
<code>zimbra.io</code>	Filesystem operations
<code>zimbra.ldap</code>	LDAP operations
<code>zimbra.lmtp</code>	LMTP operations (incoming mail)
<code>zimbra.mailbox</code>	General mailbox operations
<code>zimbra.misc</code>	Miscellaneous
<code>zimbra.op</code>	Changes to mailbox state
<code>zimbra.pop</code>	POP protocol operations

<code>zimbra.redolog</code>	Redo log operations
<code>zimbra.security</code>	Security events
<code>zimbra.session</code>	User session tracking
<code>zimbra.smtp</code>	SMTP operations (outgoing mail)
<code>zimbra.soap</code>	SOAP protocol
<code>zimbra.sqltrace</code>	SQL tracing
<code>zimbra.store</code>	Mail store disk operations
<code>zimbra.sync</code>	Sync client operations
<code>zimbra.system</code>	Startup/shutdown and other system messages
<code>zimbra.wiki</code>	Wiki operations
<code>zimbra.zimlet</code>	Zimlet operations



Changes to the log level take affect immediately.

Table 54. Logging Events

Level	Local?	Syslog	SNMP Trap	When Used
FATAL	Y	Y	Y	Designates very severe error events that the application to abort or impact a large number of users. For example, being unable to contact the MariaDB database.
ERROR	Y	Y	N	Designates error events that might still allow the application to continue running or impact a single user. For example, a single mailbox having a corrupt index or being unable to delete a message from a mailbox.
WARN	Y	N	N	Designates potentially harmful situations but are usually recoverable or can be ignored. For example, user log in failed.
INFO	Y	N	N	Designates information messages that highlight the progress of the application, basic transaction-level logging. For example, server start-ups, mailbox creation/deletion, account creation.
DEBUG	Y	N	N	Events that would generally be useful to help a customer debug problems.

(*) A few non-critical messages such, as service startup messages, will generate traps.

Protocol Trace

Protocol trace is available in the following logging categories:

```
zimbra.smtp  
zimbra.lmtp  
zimbra.soap  
zimbra imap  
zimbra imap-client  
zimbra.pop  
zimbra.pop-client
```

Reviewing mailbox.log Records

The `mailbox.log` file contains every action taken on the mailbox server, including authentication sessions, LMTP, POP3, and IMAP servers, and Index server. Review the `mailbox.log` to find information about the health of your server and to help identify problems.

`mailbox.log` records valid and invalid login attempts, account activity such as opening email, deleting items, creating items, indexing of new mail, server activities including start and stop. The progress of an activity on the mail server is logged as INFO. If the expected results of the activity fails and errors occurs, an exception is written to the log.

You can set up logging options for a single account in order to trace account activity for one user without filling up `mailbox.log` with log messages for unrelated accounts. See [Command-Line Utilities](#), the `zmprov` miscellaneous section.

Log pattern

by default log entries in `mailbox.log` have the following Log4j pattern:

```
%d %-5p [%t] [%z] %c{1} - %m%n
```

This pattern consists of 6 blocks of data:

- Date and time (e.g.: `2018-01-22 19:23:07,100`)
- Log level (e.g. `INFO`)
- Thread name (e.g. `[qtp1043351526-547:https://localhost:7071/service/admin/soap/DeleteAccountRequest], [Index-9]`, etc.)
- Zimbra Collaboration context
- Component name (e.g. `soap`, `mailbox`, `mbxmgr`, etc.)
- Log message. **Note:** the log message section may span multiple lines. When a log message contains an exception, the stack trace will always start on a new line below the error message.

You can read more about Log4j patterns in [Log4j PatternLayout documentation](#).

Thread name in mailbox.log

Thread names in `mailbox.log` are prefixed to identify internal components. Most threads have one of the following naming convention: "`{thread prefix}-{thread number}`" or "`{thread prefix}-`

{thread number}:{url}".

The following {thread prefix} values are currently used for thread names in Zimbra Collaboration: `btpool`, `pool`, `LmtpServer`, `ImapServer`, `ImapSSLServer`, `Pop3Server`, `Pop3SSLServer`, `ScheduledTask`, `Timer`, `AnonymousIoService`, `CloudRoutingReaderThread`, `GC`, `SocketAcceptor`, `Thread`, `qtp`.

Threads with prefix `qtp` are created by Jetty `QueuedThreadPool` and have the following naming convention: "`qtp{hash code}-{thread number}:{url}`" where `{hash code}` is the hash code value of the instance of `QueuedThreadPool` that owns the thread (see `Object::hashCode` in Java platform documentation).

`{thread number}` in thread names is an integer that monotonically increases within each thread factory. Thread numbers are reset when `mailboxd` process is stopped or restarted.

Log records reported by threads that serve SOAP requests will usually contain URL of the request being served in `{url}` part of thread name, as in the following example:

Log messages reported by threads serving HTTP/S requests also contain request URL



```
2017-10-25 00:00:04,365 INFO [qtp649734728-21794;http://server1.mydomain.com/service/soap/SearchRequest] [name=user1@mydomain.com;mid=443;oip=129.113.231.190;port=56632;ua=ZimbraWebClient - FF56 (Win)/8.8.3_GA_1872;] soap - SearchRequest elapsed=2
```

Due to a known bug in Zimbra Collaboration `{url}` part of the thread name may contain duplicate protocol identifier, as in the following example:

```
[qtp1043351526-547:https:https://localhost:7071/service/admin/soap/DeleteAccountRequest]
```

Zimbra Collaboration Context in mailbox.log

`[%z]` section in the log pattern describes Zimbra Collaboration context and consists of key-value pairs in the format `key=value`, separated by semi-colons (;). In cases where a value contains a semi-colon, the semi-colon is replaced with a double semi-colon (;;). E.g., browser UserAgent strings often include semi-colons, such as this one "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36". In `mailbox.log`, this UserAgent string will appear as following:

```
2017-10-25 00:20:52,608 INFO [qtp649734728-22666:http://[REDACTED]/service/upload?fmt=extended,raw] [name=[REDACTED];mid=2404;oip=[REDACTED];port=33690;ua=Mozilla/5.0 (Windows NT 10.0;; Win64;; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36;] FileUploadServlet - Received plain: Upload: { accountId=[REDACTED], size=[REDACTED], time=[REDACTED], uploadId=[REDACTED], name=Oct-2017.zip, path=/opt/zimbra/data/tmp/upload/upload_[REDACTED].8000_00002167.tmp }
```

double ";" inside "ua" value

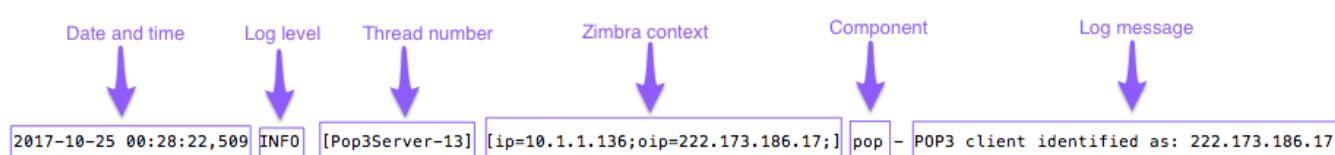
19734728-22666: http://[REDACTED]service/upload?
;mid=2404;oip=[REDACTED];port=33690
/in64;; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/6
LoadServlet - Received plain: Upload: { accountId=[REDACTED]
1 Oct 25 00:20:52 PDT 2017, size=4269535, uploadId=[REDACTED]
[REDACTED], name=Oct-2017.zip, path=/opt/
[REDACTED]_8000_00002167.tmp }

inside "ua" value

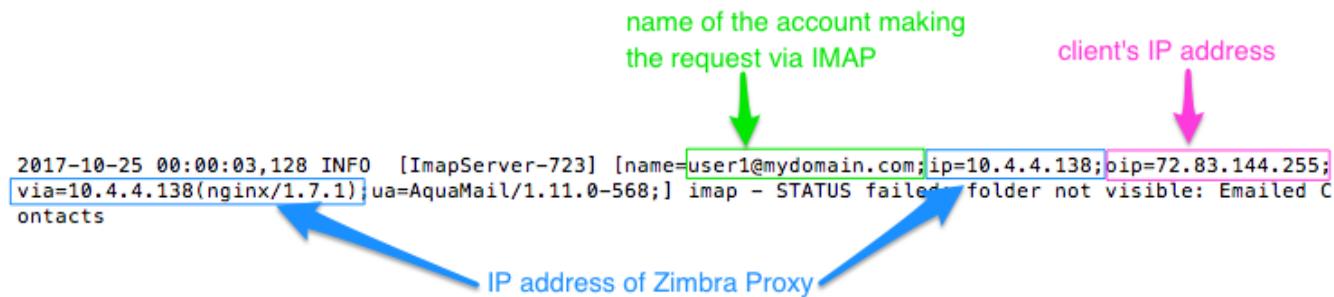
The following key value pairs are currently supported and may be recorded in log entries in any order and any combination:

- **ip** — IP of the TCP/IP client making a request
- **oip** — originating IP address. When a request is made through NGINX proxy, this value will contain the IP address of the client application, while **ip** value will contain the IP address of the proxy server
- **cid** — connection id of a server that is monotonically increasing - useful for tracking individual connections
- **id** — ID of the target account
- **name** — name of the target account (email address)
- **aid** — ID of the authenticated account. Only present if target account is different than authenticated account
- **aname** — name of the authenticated account. Only present if target account is different than authenticated account
- **mid** — ID of requested mailbox. Only present if request is dealing with a mailbox
- **ua** — name of the client application (i.e. User Agent)
- **via** — list of IP addresses and user-agents of the request's proxy chain
- **soapId** — ID assigned to a SOAP request to track proxied hops for a particular request
- **msgid** — value of Message-ID header of the message being operated on
- **ds** — name of the Data Source being operated on
- **port** — server port to which the client connected
- **oport** — originating port number of request
- **oproto** — originating protocol of request. This can be passed by internal components that make SOAP requests on behalf of a user (e.g. MTA)

The example below is a record showing that on October 25, 2017, 28 minutes after midnight, a POP3 client with IP address **222.173.186.17** has contacted the Zimbra Collaboration server and that the request was proxied through a local proxy server with IP **10.1.1.136**.



The following example shows a record of a failed **IMAP STATUS** request sent by `user1@mydomain.com` using AquaMail mobile app. The user's device has IP address `72.83.144.255` (as reported in `oip` field). The request came to IMAP server via Zimbra Collaboration nginx proxy, which has IP address `10.4.4.138` (as reported in `ip` and `via` fields).



The following example shows a record of LMTP server delivering a message. The IP address in this log message most likely belongs to Zimbra Collaboration MTA running on local network.

```
2017-10-25 00:00:03,646 INFO [LmtpServer-726] [ip=10.0.1.17;] lmtp - Delivering message: size=4096 bytes, nrcpts=1, sender=us er4@mydomain.com, msgid=<421926844.25781.2504914800041.JavaMail.zimbra@mydomain.com>
```

The next example shows a record of **MailboxPurge** thread purging message with ID 462 from the mailbox of `test@mydomain.net`. This log message does not have `ip`, `oip`, `port` or `via` fields, because it originates from an internal process rather than from an external request.

```
2017-10-25 00:00:05,234 INFO [MailboxPurge] [name=test@mydomain.net;mid=462;] purge - Purging messages.
```

Handler Exceptions and Stack Traces

If an error occurs during the progress of an activity, a handler exception is added to the end of the log record to notify you that an event occurred during the execution of the process that disrupted the normal flow. This signals that some type of error was detected.

Example 19. Handler Exception

```
007-06-25 00:00:10,379 INFO [btpool0-1064]
[name=nriess@example.com;mid=228;ip=10.2.3.4;ua=zimbra Desktop/0.38;] SoapEngine -
handler exception
```

Sometimes a stack trace is displayed after the exceptions notification. A stack trace reports the threads and monitors in Zimbra's **mailboxd** service. This information aids in debugging, because the trace shows where the error occurred. The last few entries in the stack often indicate the origin of the problem. When the **caused by** descriptor is included in the log line, this is the root of the error. In the example below, the error was caused by 501, bad address syntax.

Example 20. Stack Trace

```
com.example.cs.mailbox.MailServiceException: Invalid address: Jon R
at com.example.cs.mailbox.MailServiceException.internal_SEND_FAILURE
(MailServiceException.java:412)
at com.example.cs.mailbox.MailServiceException.SEND_ABORTED_ADDRESS_FAILURE
MailServiceException.java:416)
...
at org.mortbay.thread.BoundedThreadPool$PoolThread.run(BoundedThreadPool.java:442)

Caused by: com.example.cs.mailbox.MailSender$SafeSendFailedException: 501 Bad
address syntax; chained exception is:
com.sun.mail.smtp.SMTPAddressFailedException: 501 Bad address syntax
at com.sun.mail.smtp.SMTPTransport.rcptTo(SMTPTransport.java:1196)
at com.sun.mail.smtp.SMTPTransport.sendMessage(SMTPTransport.java:584)
at javax.mail.Transport.send0(Transport.java:169)
at javax.mail.Transport.send(Transport.java:98)
at com.example.cs.mailbox.MailSender.sendMessage(MailSender.java:409)
at com.example.cs.mailbox.MailSender.sendMimeMessage(MailSender.java:262)
... 30 more
```

Mailbox log files

The `mailbox.log` files rotate daily. The mailbox log files are saved in `/opt/zimbra/log`. Previous `mailbox.log` file names include the date the file was made. The log without a date is the current log file. You can back up and remove these files.

Troubleshooting Mail Problems

To review the `mailbox.log` for errors, search for the email address or the service that is experiencing the problem. Also, search for WARN or ERROR log levels, read the text of the message. When you find the error, review the records, tracing the events that happened before the problem was recorded.

System Crashing

When your system crashes, locate the startup message and then look for errors before the startup message date. This example shows an out-of-memory error on June 17, 2007.

Example 21. Startup message

```
2007-06-25 01:56:18,725 INFO [main] [] soap - Servlet SoapServlet starting up
```

Look for errors before the startup message.

Example 22. Error message

```
2007-06-17 20:11:34,194 FATAL [btpool0-3335]
[name=samd@example.com;aname=abcadmin@example.com;mid=142;ip=10.3.4.5;ua=zimbraCon
nectorForBES/5.0.207;] system - handler exception java.lang.OutOfMemoryError:
PermGen space
```

Mail Delivery Problem

Locate the "LmtpServer" service. This example includes a stack trace report with a **caused by** explanation that the recipient address was rejected as the address must be a fully-qualified address.

Example 23. Mail delivery problem

```
2007-06-25 10:47:43,008 INFO [LmtpServer-250]
[name=bigen@example.com;mid=30;msgid=<1291804360.35481182793659172.JavaMail.root@example.com>;] lmtp - rejecting message bigen@example.com: exception occurred
com.zimbra.cs.mailbox.MailServiceException: redirect to too failed
at com.zimbra.cs.mailbox.MailServiceException.internal_SEND_FAILURE
(MailServiceException.java:412)
at
com.zimbra.cs.mailbox.MailServiceException.SEND_FAILURE(MailServiceException.java:424)
at
com.zimbra.cs.filter.zimbraMailAdapter.executeActions(zimbraMailAdapter.java:286)
at org.apache.jsieve.SieveFactory.evaluate(SieveFactory.java:151)
at com.zimbra.cs.filter.RuleManager.applyRules(RuleManager.java:177)
at
com.zimbra.cs.lmtpserver.zimbraLmtpBackend.deliverMessageToLocalMailboxes(zimbraLmtpBackend.java:325)
at com.zimbra.cs.lmtpserver.zimbraLmtpBackend.deliver(zimbraLmtpBackend.java:140)
at com.zimbra.cs.lmtpserver.LmtpHandler.doDATA(LmtpHandler.java:441)
at com.zimbra.cs.lmtpserver.LmtpHandler.processCommand(LmtpHandler.java:205)
at
com.zimbra.cs.tcpserver.ProtocolHandler.processConnection(ProtocolHandler.java:231
)
at com.zimbra.cs.tcpserver.ProtocolHandler.run(ProtocolHandler.java:198)
at EDU.oswego.cs.dl.util.concurrent.PooledExecutor$Worker.run(Unknown Source)
at java.lang.Thread.run(Thread.java:619)
```

Caused by:

```
com.zimbra.cs.mailbox.MailSender$SafeSendFailedException: 504 <too>: Recipient
address rejected: need fully-qualified address ;
chained exception is: com.sun.mail.smtp.SMTPAddressFailedException: 504 <too>:
Recipient address rejected: need fully-qualified address
at com.sun.mail.smtp.SMTPTransport.rcptTo(SMTPTransport.java:1196)
at com.sun.mail.smtp.SMTPTransport.sendMessage(SMTPTransport.java:584)
at javax.mail.Transport.send0(Transport.java:169)
at javax.mail.Transport.send(Transport.java:120)
at
com.zimbra.cs.filter.zimbraMailAdapter.executeActions(zimbraMailAdapter.java:281)
... 10 more
```

Account Error - Login error

mailbox.log logs any successful or unsuccessful login attempts from IMAP, POP3 or ZWC. When you are looking for a login error, start by looking for "Auth." This example shows that someone from IP address 10.4.5.6 was trying to log in as admin on the Zimbra Web Client, using Firefox in a Windows OS. Permission was denied because it was not an admin account.

Example 24. Account Error - Login error

```
2007-06-25 09:16:11,483 INFO [btpool0-251] [ip=10.4.5.6;ua=zimbraWebClient - FFX.X  
(Win);] SoapEngine - handler exception  
com.zimbra.common.service.ServiceException: permission denied: not an admin  
account  
at  
com.zimbra.common.service.ServiceException.PERM_DENIED(ServiceException.java:205)  
at com.zimbra.cs.service.admin.Auth.handle(Auth.java:103)
```

Account Errors - IMAP or POP related

When you are looking for a log because of an IMAP or POP issue, look for "ImapServer/Pop3Server." This example shows a fatal IMAP server error occurred while trying to connect sires@example.com.

Example 25. Account Error - IMAP error

```
mailbox.log.2007-06-19:2007-06-19 15:33:56,832 FATAL [ImapServer-2444]  
[name=sires@example.com;ip=127.0.0.1;] system - Fatal error occurred while  
handling connection
```

Reading a Message Header

Each email message includes a header that shows the path of an email from its origin to destination. This information is used to trace a message's route when there is a problem with the message. The Zimbra email message header can be viewed from the Zimbra Web Client Message view. Right-click on a message and select **Show Original**.

The following lines are in the message header:

- **Date** — The date and time the message was sent. When you specify time, you can specify range by adding start and stop time to search for messages.
- **From** — The name of the sender and the email address
- **To** — The name of the recipient and the email address. Indicates primary recipients.
- **Message-ID** — Unique number used for tracing mail routing
- **In-Reply-To** — Message ID of the message that is a reply to. Used to link related messages together.
- **Received: from** — The name and IP address the message was sent from. The header displays Received: from information from the MTA to the LMTP and from the local host.

Fixing Corrupted Mailbox Index

Mail messages and attachments are automatically indexed before messages are deposited in a mailbox. Each mailbox has an index file associated with it. This index file is required to retrieve search results from the mailbox.

If a mailbox's index file becomes corrupt or is accidentally deleted, you can re-index the messages in the mailbox from the Administration Console.

Text searches on an account might or might not fail with errors when the index is corrupt. You cannot count on a user reporting a failed text search to identify that the index is corrupt. You must monitor the index log for messages about corrupt indexes. If the server detects a corrupt index, a message is logged to the Zimbra mailbox.log at the WARN logging level. The message starts with **Possibly corrupt index**. When this message is displayed, the administrator must correct the problem. In many cases correcting the problem might mean reindexing the mailbox.

Reindexing a mailbox's content can take some time, depending on the number of messages in the mailbox. Users can still access their mailbox while reindexing is running, but because searches cannot return results for messages that are not indexed, searches may not find all results.

Checking for Index Corruption

Run a sanity check on a specific mailbox index using the `zmprov verifyIndex` command.

```
zmprov verifyIndex <user@example.com>
```

If problems are detected, a failure status is returned and a repair can be performed on the index.

Repairing and Reindexing a Corrupt Index

Use the `reIndexMailbox` command to repair and reindex a corrupt index.

```
zmprov reIndexMailbox <user@example.com> start
```

This returns a status of *started*.

SNMP Monitoring and Configuration

SNMP Monitoring Tools

You will probably want to implement server monitoring software in order to monitor system logs, CPU and disk usage, and other runtime information.

Zimbra Collaboration uses swatch to watch the syslog output to generate SNMP traps.

SNMP Configuration

Zimbra Collaboration includes an installer package with SNMP monitoring. This package should be run on every server (Zimbra Collaboration, OpenLDAP, and Postfix) that is part of the Zimbra Collaboration configuration.

The only SNMP configuration is the destination host to which traps should be sent.

Errors Generating SNMP Traps

The Zimbra Collaboration error message generates SNMP traps when a service is stopped or is started. You can capture these messages using third-party SNMP monitoring software and direct selected messages to a pager or other alert system.

Checking MariaDB

The MariaDB database is automatically checked weekly to verify the health of the database. This check takes about an hour. If any errors are found, a report is sent to the administrator's account. The report name that runs the MariaDB check is **zmbintegrityreport**, and the crontab is automatically configured to run this report once a week.



When the MariaDB database is checked, running this report can consume a significant amount of I/O. This should not present a problem, but if you find that running this report does affect your operation, you can change the frequency with which `zmbintegrityreport` is run. See [ZCS Crontab Jobs](#).

Checking for Zimbra Collaboration Software Updates

When Zimbra Collaboration is installed, the Zimbra Collaboration software update utility is automatically configured to check for the latest Zimbra Collaboration version once a day and if there is an update, to send notification to the address that is configured in the Administration Console's **Server Updates**.

The dates and times Zimbra Collaboration checked for updates is saved to the **Updates** tab and an email notification is sent out until you update the ZCS version. If you do not want to receive an email notification of updates, disable **Send notification email when updates are available**.

You can configure the following:

- **Server that checks for updates**—Available servers are listed and only one server is configured. The selected server checks for updates and the result of the update response from www.zimbra.com is stored in LDAP.
- **Check for updates every x**—The default is to check once a day. You can change the frequency interval to check every x hours, minutes, or seconds. A cron job is configured to check for new updates. If the frequency interval is less than 2 hours, the crontab file must be modified.
- **Updates URL**—This address is the URL that the server connects to when checking for updates. When a Zimbra Collaboration server checks for updates, it transmits its version, platform, and

build number to Zimbra. Normally, this URL is not changed.

- To be notified of updates, check the **Send notification email when updates are available** and enter the send to and send from addresses. The default address is the administrator's address.
- A generic email is created. The subject and content of the email can be changed.
- When a server polls the URL specified, the response is displayed.

Updating Zimbra Connector for Microsoft Outlook

The Zimbra Connector for Microsoft Outlook (ZCO) msi file is available from the Zimbra Utilities Downloads page on the Administration Console. When a newer version of ZCO is released before a new version of ZCS, you can upload the newer ZCO msi file to the ZCS server from the Administration Console. The file is uploaded to the `/opt/zimbra/jetty/webapps/zimbra/downloads` folder.

Admin Console:

Home > Tools and Migration > Client Upload

1. Download the new ZCO file to a computer that you can access from **Client Upload** in the Administration Console
2. Click **Browse** to locate the ZCO file to upload.
3. Restart ZCS:

```
zmcontrol restart
```

or run

```
/opt/zimbra/libexec/zmupdatedownload
```

The `downloads/index.html` file is updated with the latest ZCO client version. This new file can be downloaded from the ZCO link on the Administration Console **Home > Tools and Migration > Download** page.



If you do not restart the server, the ZCO download link on the Zimbra Utilities Download page does not select the newer version to download.

Notifications and Alerts Sent by Zimbra Collaboration

Service status change notification

This notification is sent when service are stopped or restarted.

Server Start Notification Message

Subject: Service <service_name> started on <zimbra_host>

Service status change: <zimbra_host> <service> changed from stopped to running

Server Stop Notification Message

Subject: Service <service_name> stopped on <zimbra_host>

Service status change: <zimbra_host> <service> changed from running to stopped

Disk usage notification

A warning alert email notification is sent to the admin account when disk space is low. The default is to send a warning alert when the threshold reaches 85% and a critical alert when the threshold reaches 95%

Subject: Disk <volume> at ##% on <zimbra_host>

Disk warning: <zimbra_host> <volume> on device <device_name> at ##%

Duplicate mysqld processes running notification

A script is executed to see if mysqld process is running to detect cases where corruption is likely to be caused. An email is generated if it finds more than 1 mysqld process running.

Subject: ZCS: Duplicate mysqld processes detected!

PID:\$pid PPID:\$ppid PGRP:\$pgrp

CMD: \$cmdline

More than \$maxcnt mysqld processes are running Parent processes include: \$procs This should be investigated immediately as it may lead to database corruption

SSL certificates expiration notification

A report runs on the first of each month and warns of certificates expiring with the next 30 days.

Subject: ZCS: SSL Certificates approaching expiration!

The Administration Console and CLI Certificate Tools guide provides instructions on how to replace you self-signed or commercial certificate.

https://wiki.zimbra.com/index.php?title=Administration_Console_and_CLI_Certificate_Tools SSL Certificate expiration checked with \$0 on <zimbra_host>.

Daily report notification

When the logger package is installed, a daily mail report is automatically scheduled in the crontab. The report is sent daily to the administrator's mailbox.

Subject: Daily mail report for <day>

<daily report data>

Database integrity check notification

The MariaDB database can be checked by running the zmdbintegrityreport automatically scheduled in the crontab to run on a weekly basis. A report is sent to the administrator's mailbox.

Subject: Database Integrity check report for <zimbra_host>

Generating report can't run \$cmd: \$!

Database errors found.

\$cmd --password=XXXXXXXX

<cmd output>

No errors found

command failed \$!

Backup completion notification

When configuring the type of backups that should be run, you can set up to receive notification about the results of a backup session.

Subject: ZCS BackupReport:SUCCESS

Server: <server>

Type: incremental

Status: completed

Started: Fri, 2012/07/13 01:00:05.488 PDT

Ended: Fri, 2012/07/13 01:10:09.842 PDT

Redo log sequence range: 2 .. 2

Number of accounts: 500

Backup and Restore (*)

 Starting with Zimbra 8.8, there are two versions of this feature. Zimbra 8.8 provides Standard and New Generation (NG) versions. Zimbra 8.7 and earlier include the Standard version, which is explained below. To use and enable the NG version of this feature with Zimbra 8.8, refer to the specific NG chapter later in this Guide.

 Standard Backup (aka Classic Backup) is deprecated and will be removed in the next release following Zimbra 8.8.12. Installations that have not yet migrated to new Network Edition NG Modules or ZSP are encouraged to do so.

Zimbra Collaboration includes a configurable backup manager that resides on every Zimbra Collaboration server and performs both backup and restore functions. You do not have to stop the Zimbra Collaboration server in order to run the backup process.

This chapter describes how data is backed up and restored and how to use the CLI tools to backup or restore your Zimbra Collaboration mailbox server. In addition, this chapter also provides information and general guidelines for disaster recovery.

Backing Up the Mailbox Server

Zimbra Collaboration includes a configurable backup manager that resides on every Zimbra Collaboration server and performs both backup and restore functions. You do not have to stop the Zimbra Collaboration server in order to run the backup process. The backup manager can be used to restore a single user, rather than having to restore the entire system in the event that one user's mailbox becomes corrupted. Full and incremental backups are saved in </opt/zimbra/backup>.

Redo Log

Each Zimbra mailbox server generates redo logs that contain current and archived transactions processed by the message store server since the last incremental backup.

When the server is restored, after the backed up files are fully restored, any redo logs in the archive and the current redo log in use are replayed to bring the system to the point before the failure.

When the current redo log file size reaches 100MB, the current redo log rolls over to an archive directory. At that point, the server starts a new redo log. All uncommitted transactions from the previous redo log are preserved. In the case of a crash, when the server restarts, the current redo logs are read to re-apply any uncommitted transactions.

When an incremental backup is run, the redo logs are moved from the archive to the backup directory.

Backup Methods

Two backup methods are available:

- The **standard backup method** is appropriate for enterprise deployments where full backups are run during non-working days.
- The **auto-grouped backup method** is recommended for large Zimbra Collaboration environments where running a full backup of all accounts at one time would take too long.

Standard Backup

The standard backup method runs a weekly full backup and daily incremental backups. A full backup process backs up all the information needed to restore mailboxes, including the LDAP directory server, database, index directory, and message directory for each mailbox.

When backing up shared messages, if a file representing a message already exists in the backup, it flags this object as such and does not copy its content again.

An incremental backup process backs up the LDAP data and gathers all the redo logs written since the last incremental backup. If the incremental backup process finds no previous full backup for a mailbox, a full backup is performed on that mailbox.

Incremental backups move the redo logs to the backup directory. The redo logs are a journal of every activity that has taken place. They contain a full copy of all messages delivered, as well as metadata such as tags, contacts, and conversations.

These backup files can be used to restore the complete mailbox server or individual mailboxes so that account and message data is completely restored.

The LDAP directory is backed up as part of either the full or incremental backup process. All accounts, domains, servers, COS, and other data are backed up.

Each mailbox server generates redo logs that contain every transaction processed by that server. If an unexpected shutdown occurs to the server, the redo logs are used for the following:

- To ensure that no uncommitted transactions remain, the server reads the current redo log upon startup and re-executes and completes any uncommitted transactions.
- To recover data written since the last full backup in the event of a server failure.

When the server is restored, after the backed up files are fully restored, any redo logs in the archive and the current redo log in use are replayed to bring the system to the point before the failure.

The Zimbra MTA is not backed up, as the data is only on the server for a very short time.

Custom configurations—such as `mailboxd's 'jetty/etc/*.xml'`—are not backed up.

Backup Notification

A backup report is sent to the admin mailbox when full and incremental backups are performed. This report shows the success or failure of the backup and includes information about when the backup started and ended, the number of accounts backed up and redo log sequence range.

If the backup failed, additional error information is included.

Auto-Grouped Backup Method

The auto-grouped backup method runs a full backup for a different group of mailboxes at each scheduled backup. The auto-grouped backup method is designed for very large Zimbra Collaboration environments where backing up all accounts can take a long time. Because auto-grouped backups combine full and incremental backup functions, there is no need for incremental backups. Each auto-grouped session runs a full backup of the targeted group of mailboxes. It is not recommended to run auto-grouped backups manually since they are scheduled from the CLI and run automatically at the scheduled times.

Directory Structure for Backup Files

The backup destination is known as a backup target. To the backup system, it is a path in the file system of the mail server. The Zimbra default backup directory is `/opt/zimbra/backup`.

The backup directory structure created by the standard backup process is shown in [Standard Backup directory structure](#). You can run regularly scheduled backups to the same target area without overwriting previous backup sessions.

The **accounts.xml** file lists all accounts that are in all the backups combined. For each account, this file shows the account ID, the email address, and the label of the latest full backup for that account. If you save your backup sessions to another location, you must also save the latest accounts.xml file to that location. The accounts.xml file is used to look up the latest full Backup for an account during restore. If the accounts.xml file is missing you must specify the backup label to restore from.

The redo log directory is located at `/opt/zimbra/redolog/redo.log`. When the current redo log file size reaches 100MB, the current redo log rolls over to an archive directory, `/opt/zimbra/redolog/archive`. At this point the server starts a new redo log. All uncommitted transactions from the previous redo log are preserved. In the case of a crash, when the server restarts, the current redo logs are read to re-apply any uncommitted transactions.

Redo operations are time critical, therefore a directory move is performed instead of a copy-then-delete function. This directory move can only be performed if the source and destination paths are on the same file system volume. In other words, the **redo** log and **redo-archive** log must be on the same file system volume because the archive files are a subdirectory of the redo log file system.

All incremental and auto-grouped backup sessions must be saved to the same directory as all the redo logs must be found in the same backup target. Standard full backup sessions can use a different target directory.

Table 55. Standard Backup directory structure

<code>/opt/zimbra/backup</code>	Default root of backups
<code>accounts.xml/</code>	List of all accounts, each with email file address, Zimbra ID, and latest full backup label. The accounts.xml maintains the mapping of email addresses to their current zimbraIds and also the most recent full backup for each account.
<code>sessions/</code>	Root of backup sessions.

<code>full-<timestamp>/</code>	A full backup directory. The timestamp for a session is the backup start time in GMT, including milliseconds. GMT is used rather than local time to preserve visual ordering across daylight savings transitions.
<code>session.xml</code>	Metadata about this backup label for a full or incremental session, such as start and stop times.
<code>shared_blobs/</code>	Contains message files that are shared among accounts in this backup.
<code>sys/</code>	Global database tables and <code>localconfig</code> .
<code>db_schema.xml</code>	Database schema information for global tables. Each table dump file has a <code>.csv</code> format.
<code>localconfig.xml</code>	Copy of <code>/opt/zimbra/conf/localconfig.xml</code> at the time of the backup.
<code><table name>.dat</code>	Database table data dump.
<code>LDAP/ldap.bak</code>	LDAP dumps.
<code>accounts/</code>	Each account's data is saved in a subdirectory of this.
<code><@/zimbraId>/</code>	Root for each account.
<code>meta.xml</code>	Metadata about this account's backup.
<code>ldap.xml</code>	Account's LDAP information, including aliases, identities, data sources, distribution lists, etc.
<code>ldap_latest.xml</code>	If this is present, this file links to <code>ldap.xml</code> of the most recent incremental backup.
<code>db/</code>	Account-specific database table dumps.
<code>db_schema.xml</code>	Database schema information for this account's tables.
<code><table name>.dat</code>	Database table data dump.
<code>blobs/</code>	Contains blob files.
<code>index/</code>	Contains Lucene index files.
<code>incr-<timestamp></code>	An incremental backup directory. This directory is similar to the full backup directory schema and includes these metafiles.
<code>session.xml</code>	
<code>sys/db_schema.xml</code>	
<code>accounts/@<zimbraId>/ldap.xml</code>	<code>incr-<timestamp></code> does not include <code>accounts/@<zimbraId>/db/db_schema.xml</code> because incremental backup does not dump account tables.



For auto-grouped backups, the directory structure saves the redo log files to the full backup session. There are no incremental backup sessions.

Backup and Restore Using the Administration Console

Many of the backup and restore procedures can be run directly from the Administration Console. In the Navigation pane, **Monitoring>Backup** lists each of the servers.

Configure Backup from the Admin Console

Backups can be configured from the Administration Console as a global settings configuration and as a server-specific configuration. Server settings override global settings.

In the global settings, you can configure the email addresses to receive notification about the results of the backup. The default is to send the notification to the admin account.

For Auto-grouped, you configure the number of groups to divide the backups into.

The standard backup is the default and is automatically scheduled. You do not need to make any additional changes. But when running the auto-grouped backup you must manually configure the backup schedule. To do so, access the CLI and follow the steps under [Schedule Auto-Group Backups](#) to run `zmschedulebackup -D` to set the default schedule for auto-grouped backups.

Throttling option with auto-grouped backup. The auto-grouped backup method automatically backs up mailboxes that have never been backed up when the next backup is scheduled. This might not be the best option every time a full backup is required on all mailboxes, such as immediately after massive mailbox migrations or after a major upgrade. Enabling **Throttle automatic backups** limits the mailbox count in a daily backup to T/N. This breaks the constraint of backing up all mailboxes in N days, but it helps backup to finish during off hours.

When all mailboxes are backed up at least once, disable throttling:

```
zmprov mcf zimbraBackupAutoGroupedThrottled TRUE
```

Backup and Restore Using the Command Line Interface

The Zimbra backup and restore procedures can be run as CLI commands.

The following utilities are provided to create backup schedules, perform full and incremental backups, restore the mail server, or restore the LDAP server.

- **`zmschedulebackup`** — This command is used to schedule full backups, incremental backups, and deletion of old backups.
- **`zmbackup`** — This command executes full or incremental backup of the Zimbra Collaboration mailbox server. This is run on a live server, while the `mailboxd` process and the mailbox server are running. This command also has an option to manually delete old backups when they are no longer needed.
- **`zmbackupabort`** — This command stops a full backup that is in process.
- **`zmbackupabort -r`** — This command stops an ongoing restore.
- **`zmbackupquery`** — This command lists the information about ongoing and completed backups, including labels and dates.
- **`zmrestore`** — This command restores a backup to a running Zimbra Collaboration mailbox server.

- **zmrestoreoffline**—This command restores the Zimbra Collaboration mail server when the **mailboxd** process is stopped.
- **zmrestoreldap**—This command restores the complete LDAP directory server, including accounts, domains, servers, COS and other data.

Refer to [Appendix A: Command Line Utilities](#) for usage and definitions for each of these commands.

Backing up using the Standard Method

When you initiate a backup, you can issue the command from the same server being backed up, run the command remotely and specify the target server on the command line, or use the Administration Console to start a backup session.

Scheduling a Standard Backup

When Zimbra Collaboration was installed, the backup schedule for the standard method of full and incremental backups was added to the crontab. Under the default schedule, the full backup is scheduled for 1:00 a.m., every Saturday. The incremental backups are scheduled for 1:00 a.m., Sunday through Friday.

By default, backups older than a month are deleted every night at 12 a.m.

You can change the backup schedule using the **zmschedulebackup** command.

Specify the fields as follows, separate each field with a blank space:

- minute—0 through 59
- hour—0 through 23
- day of the month—1 through 31
- month—1 through 12
- day of the week—0 through 7 (0 or 7 is Sunday, or use names)

Type an asterisk (*) in the fields you are not using.

Example 26. `zmschedulebackup` options

- Replace the existing full backup, incremental backup and delete backup schedule. When you use `-R`, the complete backup schedule is replaced. If you use this command, remember to set the deletion schedule, if you want backup sessions to be scheduled for automatic deletion. This example replaces the existing schedule to have full backups run on Sunday at 1 a.m., incremental backups to run Monday through Saturday at 1 a.m., and old backups deleted at 12:00 a.m. every day.

```
zmschedulebackup -R f "0 1 * * 7" i "0 1 * * 1-6" d 1m "0 0 * * *"
```

- Add an additional full backup time to your current schedule. This example adds a full backup on Thursday at 1 a.m.

```
zmschedulebackup -A f "0 1 * * 4"
```

- Review your backup schedule. The schedule is displayed.

```
zmschedulebackup -q
```

- Save the schedule command to a text file. This would allow you to easily recreate the same schedule after a reinstall or upgrade

```
zmschedulebackup -s
```



To return backups to the default schedule use the command `zmschedulebackup -D`.

Default Standard Backup Schedule

The default backup schedule is displayed similarly to the following example:

Example 27. Default Backup Schedule

```
0 1 * * 6 /opt/zimbra/bin/zmbbackup -f - all
0 1* * 0-5 /opt/zimbra/bin/zmbbackup -i
0 0 * * * /opt/zimbra/bin/zmbbackup -del 1m
```

Read as follows:

The full backup runs on 1 a.m. on Saturdays

```
0 1 * * * 6 /opt/zimbra/bin/zmbackup -f - all
```

An incremental backup runs at 1 a.m. from Sunday through Friday

```
0 1* * 0-5 /opt/zimbra/bin/zmbackup -i
```

Backup sessions are deleted at midnight 1 month after they were created.

```
0 0 * * * /opt/zimbra/bin/zmbackup -del 1m
```

How to read the crontable

Each crontab entry contains six fields that appear in this order:

Field					
1	2	3	4	5	6
0	1	*	*	6	/opt/zimbra/bin/zmbackup -f - all

1. minute (0-59 allowed)
2. hour (0-23)
3. day of the month (1-31)
4. month (1-12 or names)
5. day of the week (0-7 or names allowed, with both 0 and 7 representing Sunday)
6. string to be executed



The asterisk character works as a wild card, representing every occurrence of the field's value.

Admin Console:

[Home > Configure > Global Settings > Backup/Restore](#)

You can add additional recipient addresses or change the notification email address in the Administration Console.

Full Backup Process

The full backup process goes through the following steps to back up the mailbox, the database, the indexes, and the LDAP directory:

1. Backs up the global system data including system tables and [localconfig.xml](#).
2. Iterates through each account to be backed up and backs up the LDAP entries for those

- accounts.
3. Places the account's mailbox in maintenance mode to temporarily block mail delivery and user access to that mailbox.
 4. Backs up the mailbox.
 - a. Creates MariaDB dump for all data related to that mailbox.
 - b. Backs up the message directory for that mailbox.
 - c. Creates a backup of the index directory for that mailbox.
 5. Returns that account's mailbox to active mode and moves on to the next one.
 6. Backs up the LDAP directory.

A full backup is usually run asynchronously. When you begin the full backup, the label of the ongoing backup process is immediately displayed. The backup continues in the background. You can use the `zmbackupquery` command to check the status of the running backup at any time.

Backup files are saved as `zip` files without compression. To change the default `zip` option, see [Appendix A: Command Line Utilities](#), `zmbackup` section.

Incremental Backup Process

Incremental backups are run using the CLI command, `zmbackup`. The process for incremental backup is as follows:

1. Backs up the global system data including system tables and `localconfig.xml`.
2. Iterates through each account to be backed up and backs up the LDAP entries for those accounts.
3. Moves the archive redo logs, created since the last backup, to the `<backup_target>/redologs` folder.

Archived logs that are less than an hour old at the time of incremental backup are copied to the backup and are not deleted. These redologs are deleted one hour after the backup. The interval is set by the `localconfig` key `backup_archived_redolog_keep_time`. The default is 3600 seconds.

If no full backup for this account is found, the backup process performs a full backup on this account, even if only an incremental backup was specified.

4. Backs up the LDAP directory.

Performing Manual Backups

Use the `zmbackup` command to perform the following backup operations:

- Perform a manual backup of all mailboxes on server<1>:

```
zmbackup -f -s server1.domain.com -a all
```

- Perform a manual, incremental backup of all mailboxes on **server1** since last full backup

```
zmbackup -i -s server1.domain.com -a all
```

- Perform a manual, full backup of only **user1**'s mailbox on **server1**

```
zmbackup -f -s server1.domain.com -a user1@domain.com
```

Deleting Backup Sessions

You can delete backup sessions either by label or by date.

- Deleting by label deletes that session and all backup sessions before that session.
- Deleting by date deletes all backup session prior to the specified date.

For example, `zmbackup -del 7d` deletes backups older than 7 days from now. You can specify day (**d**), month (**m**), or year (**y**).

Finding a Specific Backups

Each full or incremental backup is a backup session.

Each backup session is labeled with date and time. For example, the label `full-20070712.155951.123` says this is a backup from July 12, 2007 at 3:59:51.123.



The times set in the session label are GMT, not the local time. GMT is used rather than local time to preserve visual ordering across daylight savings transitions.

Use the `zmbackupquery` command to find full backup sessions.

- To find a specific full backup session:

```
zmbackupquery -lb full-20070712.155951.123
```

- To find a full backup sessions since a specific date:

```
zmbackupquery --type full --from "2007/01/01 12:45:45"
```

- To find all full backup sessions in the backup directory:

```
zmbackupquery --type full
```

- To find the best point in time to restore for an account specify a time window

```
zmbackupquery -a user1@example.com --type full --from "2007/07/05 12:01:15" --to "2007/07/12 17:01:45"
```



If a backup session is interrupted because the server crashes during backup (not aborted), the interrupted backup session is saved as a temporary session. The temporary backup session is put in <backup_target>/sessions_tmp folder. You can use the `rm` command to delete the directory.

Aborting a Full Backup in Progress

1. Before you can abort a backup, you must know the backup session label. This label is displayed when `zmbackup` first starts. If you do not know the full backup label, use `zmbackupquery` to find the label.
2. Use the `zmbackupabort` command to stop a backup that is in progress. The backup is immediately stopped and becomes a partially successful backup.
 - Stop the backup, if you know the label name

```
zmbackupabort -lb full-20070712.155951.123 -s server1
```

- Stop the backup, if you do not know the label

```
zmbackupquery  
zmbackupabort -s server1 -lb full-20070712.155951.123
```

Backup using the Auto-Grouped Method

The auto-grouped backup method is configured either from the Administration Console or from the CLI.

Admin Console:

Home > Configure > Global Settings > Backup/Restore or
Home > Configure > Servers → *server* → Backup/Restore

Configuring Auto-Grouped Backup from the CLI

Set the backup method in the global configuration, and you can override the configuration on a per server basis if you do not want a particular server to use the auto-grouped backup method.

To set up auto-grouped backup, you modify LDAP attributes with the `zmprov` command:

```
zmprov mcf <ldap_attribute> <arg>
```

You can also set the attributes at the server level using `zmprov ms`.

The following LDAP attributes are modified:

- `zimbraBackupMode` — Set it to be **Auto-Grouped**. The default is Standard.
- `zimbraBackupAutoGroupedInterval` — Set this to the interval in either days or weeks that backup sessions should run for a group. The default is `1d`. Backup intervals can be 1 or more days, entered as `xd` (e.g. `1d`); or 1 or more weeks, entered as `xw` (e.g. `1w`).
- `zimbraBackupAutoGroupedNumGroups` — This is the number of groups to spread mailboxes over. The default is 7 groups.

Schedule Auto-Group Backups

You must configure the auto-group backup schedule.

Run `zmschedulebackup -D` to set the default schedule for auto-grouped backups based on your `zimbraBackupAutoGroupedInterval` setting.

One group is backed up each interval. The auto-grouped backup automatically adjusts for changes in the number of mailboxes on the server. Each backup session backs up the following:

- All mailboxes that have never been backed up before. These are newly provisioned mailboxes.
- All mailboxes that have not been backed up within the number of scheduled backup days. For example, if backups are scheduled to run over six days, mailboxes that have not been backed up in the past 5 days are backed up.
- More mailboxes, the oldest backup first. This is done so that the daily auto-grouped backup load is balanced.

For example, if you configured the auto-grouped backup interval to be daily (`1d`) and the number of groups to be 7, the first time auto-grouped backup runs, all accounts are backed up. After the initial backup, auto-grouped backup runs again the next day. This time accounts that have been newly provisioned and a percentage of accounts close to one-seventh of the total are backed up again. Accounts with the oldest backup date are backed up first. The backup continues with newly provisioned accounts and approximately one-seventh of accounts being backed up daily over seven days.

When backing up shared messages, if a file representing a message already exists in the backup, it flags this object as such and does not copy its content again.

Backup files are saved as `zip` files without compression. To change the default `zip` option, see [Appendix A: Command Line Utilities](#), `zmbbackup` section.

These backup files can be used to restore the complete Zimbra Collaboration system or individual mailboxes so that account and message data is completely restored. Archived redo logs are moved to the backup session as part of the full backup. When the server is restored from an auto-grouped backup, redo logs are replayed to bring the system to the point before the failure.

Backup Options

The backup process can be configured to selectively backup content and to back up the MariaDB database.

Backup Up content Options

You can configure these backup options so that search indexes, blobs, and HSM blobs are not backed up during a full backup session.

- `zimbraBackupSkipSearchIndex` — Default is **FALSE**. If set to **TRUE**, the search index is not backed up. The mailbox will have to be reindexed after restoring from a backup without the search index.
- `zimbraBackupSkipBlobs` — Default is **FALSE**. If this is set to **TRUE**, blobs are not backed up. This might be useful for getting a quicker backup of just database data when the blobs reside on fault-tolerant storage. This configuration applies to all blobs, those on the primary volumes as well as secondary (HSM) volumes.
- `zimbraBackupSkipHsmBlobs` — Default is **FALSE**. If this is set to **TRUE**, blobs on HSM volumes are not backed up. Set this if `zimbraBackupSkipBlobs` is **FALSE** but you want to skip blobs on HSM volumes.

Backup the MariaDB Database

You can configure Zimbra Collaboration backups to run `mysqldump` to back up your MariaDB database during backup sessions. When this is enabled, a `mysqldump` backup runs with each full, incremental, and auto-grouped backup.

The `mysqldump` is a backup of your MariaDB database at a specific time. Data changes that occur later than the dump file are written to the binary log. To recover to a specific point in time, binary logging must be enabled. See the Zimbra wiki article, MariaDB Backup and Restore at https://wiki.zimbra.com/wiki/MySQL_Backup_and_Restore.

The MariaDB dump files are gzipped and placed in the backup target directory, or to `/opt/zimbra/backup`, if no directory is specified.

These files can be quite large. Make sure that the free disk space is at least three times greater than the actual MariaDB database file for each MariaDB database backup file that is saved.

- Enable `mysqldump` to run automatically with your backups, type

```
zmlocalconfig edit mysql_backup_retention=<N>
```

N is the number of copies of the MariaDB database backups that are retained.



To restore a MariaDB database, contact Zimbra support for assistance.

Managing Disk Space for Backups

Backup sessions fail if the target disk does not have enough space. All data backed up in the backup session is discarded and deleted.

You can choose to receive notification when your disk might not have enough space to complete the backup

Configuring the `zimbraBackupMinFreeSpace` attribute helps you manage running backup session by notifying you.

Set the value for attribute `zimbraBackupMinFreeSpace` to the amount of free space required on the backup target disk before a backup session is run. If the disk has less space than the value set in the attribute, the back up session will not run and an email notification is sent to the administrator.



If you are also backing up the MariaDB database, make sure you set the value large enough to include the `mysqldump` file size.

The value for this attribute can be specified as a percentage of the total disk space, for example `25%`, or as a number of bytes, for example `300MB`, `50GB`, etc. The default value is `0`, meaning the check is disabled and backup is always allowed to start.

The attribute can be set globally or by server.

- As global:

```
zmprov mcf zimbraBackupMinFreeSpace <value>
```

- By server:

```
zmprov ms <zimbrahostname> zimbraBackupMinFreeSpace <value>
```

Backup sessions run if the free disk space is at least the value you set. If your backup file is larger than the value, the backup session fails. You should monitor the size of the backup files and adjust the attribute value if the backup requires more space than the configured value.

Restoring Data

Three types of restore procedures can be run:

- The `zmrestore` command is used to restore the mailboxes while the Zimbra Collaboration mailbox server is running.
- The `zmrestoreoffline` command is used to restore the mailbox server when just the `mailboxd` process it is stopped. This command is run for disaster recovery.
- The `zmrestoreldap` command is used to restore the content of the LDAP directory server.

The restore process allows all accounts or individual accounts to be specified.

Restore Process

The **zmrestore** process goes through the following steps to restore the mailbox, the database, the indexes, and the LDAP directory.

1. Retrieves specified accounts to be restored, or specify **all** for all accounts that have been backed up.
2. Iterates through each mailbox:
 - a. Deletes the mailbox on the server to clear any existing data
 - b. Restores the last full backup of the MariaDB data, the index directory, and the message directory for that mailbox
 - c. Replays redo logs in all incremental backups since last full backup
 - d. Replays all archived redo logs for that mailbox, from the redo log archive area on the mailbox server
 - e. Replays the current redo log



Accounts are restored, even if the account exceeds its quota. The next time the user performs an action that affects quota, they receive a warning that they have exceeded their quota.



Users using the Zimbra Connector for Microsoft Outlook must perform an initial sync on the Outlook client when they log on after the Zimbra server is restored.

Examples

Example 28. Perform a full restore of all accounts on server1

Including last full backup and any incremental backups since last full backup

```
zmrestore -a all
```

Example 29. Perform a single account restore on server1

```
zmrestore -a account@company.com
```

Example 30. Restore to a specific point in time (PIT)

The following restore options affect redo log replay. If you do not specify one of these options, all redo logs since the full backup you're restoring from are replayed



After you perform any of the following point-in-time restores, you should immediately run a complete backup for those accounts to avoid future restore problems with those accounts.

A restore that is run using any of the following options is a point-in-time restore:

- **-restoreToTime <arg>** - Replay the redo logs until the time specified.
- **-restoreToIncrLabel <arg>** - Replay redo logs up to and including this incremental backup.
- **-restoreToredoSeq <arg>** - Replay up to and including this redo log sequence.
- **-br** - Replays the redo logs in backup only, therefore excluding archived and current redo logs of the system.
- **-rf** - Restores to the full backup only. This does not include any incremental backups at all.

Example 31. Specify an exact time, the incremental backup label, or the redo log sequence to restore to.

Restore stops at the earliest possible point in time if more than one point in time restore options are specified.

```
zmrestore -a account@company.com-restoreToTime <arg>
```

Two common ways to write the <timearg> are

- "YYYY/MM/DD hh:mm:ss"
- YYYYMMDD.hhmmss

Example 32. Perform an incremental restore only to last full backup, excluding incremental backups since then, for all accounts

```
zmrestore -rf --a all
```

Example 33. Restore mailbox and LDAP data for an account

```
zmrestore -ra -a account@company.com
```

Example 34. Restore to a new target account

A prefix is prepended to the original account names

```
zmrestore -ca -a account@company.com -pre restore
```

The result from the above example would be an account called [restoreaccount@company.com](#).

Example 35. Restore system tables in the database (db) and localconfig.xml

```
zmrestore -sys
```

Example 36. Include --continueOnError (-c) to the command so that the restore process continues if an error is encountered.

```
zmrestore -a all -c
```

When **-c** is designated, accounts that could not be restored are displayed when the restore process is complete.

Example 37. Restore a specific account

Can also be used to restore deleted accounts

```
zmrestore -a account@company.com
```

Example 38. Avoid restoring accounts that were deleted

```
zmrestore -a account@company.com -skipDeletedAccounts
```

Example 39. Restore a mailbox, but exclude all the delete operations that were in the redolog replay

When the mailbox is restored it will contain messages that were deleted. This is useful if users use POP and remove messages from the server

```
zmrestore -a account@company.com --skipDeletes
```



When the latest point in time is requested, do not add a backup label (**-lb**). Without specifying the label, the most recent full backup before the requested point is automatically used as the starting point.

Stop a Restore Process

The **zmbackupabort -r** command interrupts a restore that is in process. The restore process stops after the current account finishes being restored. The command displays a message showing which accounts were not restored.

To stop the restore type:

```
zmbackupabort -r
```

Restore Mailboxes When Mail Server Is Down

The offline restore process can only be run when the `mailboxd` server is not running. In general, offline restore is run under the following circumstances:

- Certain components of the Zimbra server are corrupted, and the server cannot be started. For example, the data in LDAP or the database are corrupted.
- A disaster requires the Zimbra software to be reinstalled on the server.

The offline restore must be run before the Zimbra Collaboration mailbox store server is started to keep the redo logs in sequence.

In a disaster recovery when the Zimbra software is reinstalled, if **mailboxd** is started before the backup files are restored, the mail server would begin to accept email messages and perform other activities, producing redo logs in the process. Since the pre-disaster data have not been restored to the server, the redo logs would be out of sequence. Once **mailboxd** is running, it would be too late to restore the pre-disaster data.

The offline restore process goes through the following steps.

1. Specified accounts to be restored are retrieved. If the command-line does not specify any mailbox address, the list of all mailboxes on the specified mail host is retrieved from Zimbra LDAP directory server.
2. Iterates through each mailbox:

- a. Deletes the mailbox on the server to clear any existing data
- b. Restores the last full backup of the MariaDB data, the index directory, and the message directory for that mailbox
- c. Replays redo logs in all incremental backups since last full backup
- d. Replays all archived redo logs for that mailbox, from the redo log archive area on the mailbox server
- e. Replays the current redo log

Restore All Accounts

1. Restore all accounts on server1 when **mailboxd** is stopped

```
zmrestoreoffline -a all
```

2. Start **mailboxd** after the offline restore is complete

```
zmcontrol startup
```

Restore Individual Accounts on a Live System

Use the **zmrestore** command to restore one or more selected accounts. In the event that a user's mailbox has become corrupted, you might want to restore that user from the last full and incremental backup sets.

1. For each account to be restored, put the account into maintenance mode

```
zmprov ma <account> zimbraAccountStatus maintenance
```

Maintenance mode prevents the delivery of new emails during the restore. Otherwise, the emails would be overwritten during the restore process.

2. Run the **zmrestore** command to restore the accounts

```
zmrestore -a account@abc.com
```

3. For each account that was restored, put the account back into active mode

```
zmprov ma <account> zimbraAccountStatus active
```



If a user account is restored and the COS that the account was assigned no longer exists, the default COS is assigned to the account.

Exclude Items from a Restore

When you restore from a full backup, you can exclude the search index and blobs.

- **Search index**—If you do not restore the search index data, the mailbox will have to be reindexed after the restore.

```
zmrestore -a <all|account> --exclude-search-index
```

- **Blobs**—This is a useful option when all blobs for the mailbox being restored already exist.

```
zmrestore <all or account>|--exclude-blobs
```

- **HSM-blobs**—This is useful when all HSM blobs for the mailbox being restored already exist.

```
zmrestore <all or account> --exclude-hsm-blobs
```

Restore the LDAP Server

In a disaster recovery where you need to restore the entire system, restore the LDAP directory server first.

The `zmrestoreldap` command restores the global LDAP data including COS, distribution lists, etc. You can restore the complete LDAP server, which recreates the entire schema or you can restore specific accounts. You specify the session to restore. The restore command has to be run on the LDAP server being restored.

Examples

Example 40. Find the LDAP session labels

```
zmrestoreldap -lbs
```

Example 41. Restore the complete LDAP directory server

```
zmrestoreldap -lb full20061130135236
```

Example 42. Restore LDAP data for specific accounts

```
zmrestoreldap -lb full20061130135236 -a tac@abc.com jane@abc.com
```

General Steps for Disaster Recovery

Use the following steps to restore a mailbox store server in a general disaster scenario involving multiple machines.

Preparation

1. Restore the LDAP directory server to a known good state before doing anything with the mailbox store server.
2. Put all mailboxes into maintenance mode to prevent mail delivery and user login while restoring the mailboxes.
3. Stop the mailbox store server if it is running.

Recovery

1. Reinstall the Zimbra Collaboration software on the mailbox server, if necessary.
2. Restore mailboxes.
3. Start the Zimbra Collaboration server.
4. Put all Zimbra Collaboration mailboxes back in active mode.
5. Run a full backup of the server.

Crash Recovery Server Startup

When your system unexpectedly stops and then restarts on startup, the server searches the redo log for uncommitted transactions and replays any that it finds. Replaying the redo logs brings the system to a consistent state.

Restore the Zimbra Collaboration Server

If a complete machine failure occurs, use the following steps to restore to a new server.



The Zimbra Collaboration version you install on the new server **must be the same version** as installed on the old server. The server can have a different operating system.

The new server hardware must meet the requirements described in the Installation Prerequisites section of the Zimbra Collaboration Single Server Installation guide. Install the new operating system, making any necessary OS configuration modifications as described in the installation guide.

You do the following to restore to a new server:

1. Prepare the new server.
2. Block client access to the old server's IP address with firewall rules.
3. Mount any volumes that were in use on the older server.
4. Delete the MariaDB data that is set up in the initial installation of Zimbra Collaboration.

5. Copy the backup files to the new server.
6. Run `zmrestoredap` to restore the global LDAP data.
7. Run `zmrestoreoffline` to restore account data from the backup sessions.
8. Prepare and run a new backup.

Old Server Status

Two scenarios for disaster recovery are the server has died and the Zimbra Collaboration files cannot be accessed, or Zimbra Collaboration is still running, but the server hardware needs to be replaced.

If the server is not running:

1. Block client access to the server IP address with firewall rules.
2. Find the latest full Zimbra Collaboration backup session to use.

If the server is still running, to prepare the move to the new server:

1. Block client access to the server's IP address with firewall rules.
2. Run a full backup of the old service, or if the backup is recent, run an incremental backup to get the most current incremental backup session.
3. Run `zmcontrol stop`, to stop Zimbra Collaboration. In order to restore to the most current state, no new mail should be received after the last incremental backup has run.
4. Change the hostname and IP address on the old server to something else. Do not turn off the server.

Install ZCS on a New Server

Before you begin, make sure that the new server is correctly configured with the IP address and hostname and that Zimbra Collaboration is installed and configured with the same domain, hostname, passwords, etc. as the previous server. See the Zimbra Collaboration installation guide for more information about preparing the server. Before you begin to install Zimbra Collaboration, note the information you need from the old server including admin account name and password, LDAP, Amavis, and Postfix passwords, spam training, and non-spam training user account names, exact domain name, and the global document account name.



Make sure the computer time is set to the same time as the old server. Verify that the old hostname and MX DNS records resolve to the new server.

1. Copy the Zimbra Collaboration License.xml file to a directory on the new server. You cannot complete the Zimbra Collaboration installation if the license is not on the new server.
2. Run `./install.sh` and follow the directions in the installation guide to install Zimbra Collaboration. Make sure that you configure the same domain, hostname, passwords as on the old server. During Zimbra Collaboration install, the following settings must be changed to match the original server settings:
 - a. **Zimbra LDAP Server**—For **Domain to create**, identify the same default domain as on the

old server.

b. **Zimbra Mailbox Server**—An administrator’s account is automatically created.

- Make sure that the account name for **Admin user to create** is the same name as on the original server.
- Set the admin password to be the same as on the old server.
- Set the LDAP password to be the same as on the old server.
- Set the Postfix user and Amavis user passwords to be the same as on the old server
- Change the **Spam training user** and the **Non-spam (HAM) training user** account names to be the same as the spam account names on the old server.
- **Global Document Account**—This account name is automatically generated and is usually named wiki. If you changed this, change the Global Document Account name to be the same account name as on the original server.

c. Change any other settings on the new server to match the configuration on the original server.

d. In the main menu, set the default backup schedule and the automatic starting of servers after the configuration is complete to **NO**.

Restoring a Backup to a New Server

1. Stop the new server

```
zmcontrol stop
```

2. If the old server had additional storage volumes configured, mount the additional volumes now.

3. Delete the MariaDB data and reinitialize an empty data directory. If you do not do this, **zmrestoreoffline** will have errors. As **zimbra**, type:

```
rm -rf /opt/zimbra/db/data/* /opt/zimbra/libexec/zmmyinit
```

The MariaDB service is now running.

4. Copy all the files in the **/backup** folder from the old server or from an archive location to **/opt/zimbra/backup**.

5. Restore the LDAP.

```
zmrestoreldap -lb <latest_label>
```

If you are restoring a large number of accounts, you might run a command such as the UNIX command, **nohup**, so that the session does not terminate before the restore is complete.



To find the LDAP session label to restore, type **zmrestoreldap lbs**.

6. Ensure that the following services are running before attempting to execute `zmrestoreoffline`.

- `mysqld` (MariaDB)
- `slapd` (OpenLDAP)

```
zmcontrol start
```

7. Ensure that the following services are stopped before attempting to execute `zmrestoreoffline`.

- `mailboxd`

```
zmmailboxdctl stop
```

Because some Zimbra Collaboration services are running at this point, type `zmconvertctl start`. This is required before running `zmrestoreoffline`.

1. Sync your LDAP password from backup directory to the new production servers LDAP config.

```
zmlocalconfig -f -e zimbra_ldap_password=<password>
```

2. Start the offline restore after stopping `mailboxd`.

```
zmmailboxdctl stop  
zmrestoreoffline -sys -a all -c -br
```

You might run a command such as `nohup` here also. To watch the progress, tail `/opt/zimbra/log/mailbox.log`.



Use `-c` on the command line so that accounts are restored, even if some accounts encounter errors during the offline restore process.

3. Because some Zimbra Collaboration services are running at this point, type `zmcontrol stop` to stop all services.

4. Remove any old backup sessions because these sessions are no longer valid.

```
rm -rf /opt/zimbra/redolog/* /opt/zimbra/backup/*
```

5. Start Zimbra Collaboration.

```
zmcontrol start
```

6. Run a full backup.

```
zmbackup -f -a all
```

7. Remove the firewall rules and allow client access to the new server.

Restoring from Different Failure Scenarios

The restoration steps are similar for most server failures you may encounter. If a failure occurs, review the disaster recovery section to understand the process and then follow the steps below for the specific type of failure.

Restore When LDAP is Corrupted

1. Reinstall the LDAP server. See the Zimbra Collaboration Installation guide.
2. Find the label for the LDAP session to restore. Run the `zmrestoreldap - lb <label>` command, with no arguments to restore all accounts, domains, servers, COS, etc. for the LDAP server.
3. Make sure that all accounts are in active mode. From the command line, type `zmprov ma zimbraAccountStatus active`

Restore After Replacing Corrupted Partitions

1. If a partition becomes corrupted, replace the failed disk.
2. To restore the latest full and incremental backup files, run

```
zmrestore -a all
```

The `zmrestore` process automatically retrieves the list of all mailboxes on the specified mail host from the backup date and iterates through each mailbox to restore the mailboxes to the last known good state.

Restore After Corrupted or Unreadable Redo Log

If the redo log becomes unreadable, the `mailboxd` service stops and cannot restart. If this happens, inspect the hardware and software to find the source of the problem before proceeding.

Without the latest redo log, the Zimbra mailbox server cannot be returned to the most current state. The Zimbra mailbox data can be restored to the latest archived redo log state. A new redo log for current transactions is created after the Zimbra mailbox server is restored.



The `mailboxd` service must not be running, and all accounts must be in maintenance mode before beginning.

1. Put all accounts into maintenance mode.

```
zmprov md <domain> zimbraDomainStatus maintenance
```

- With the `mailboxd` service not running, type

```
zmrestoreoffline
```

The offline restore process begins by retrieving the list of all mailboxes on the specified mail host from the backup.

The offline restore then iterates through each mailbox to:

- Delete the mailboxes on the server
- Restore the last full backup from the backup area
- Restore all incremental backups for that mailbox in order, since the last full backup. This involves replaying the redo logs from the backup target area
- Replay all archived redo logs

Because the redo log for current transactions is not available, the mailbox server is returned to the state of the last archived redo log.

- After the offline restore is complete, start ZCS.

```
zmcontrol startup
```

- When the Zimbra mailbox server is up, run a full backup of the Zimbra server. The full backup must be run immediately to have the latest data backed up because the latest redo log is not available.

Change Local Configuration Files After Restoring Zimbra

The `localconfig.xml` file, located in the `/opt/zimbra/conf` folder, includes the core Zimbra server configuration, such as paths and passwords. This file is backed up in full and incremental backups. When you run an incremental or full restore, the backed-up version of the `localconfig.xml` is renamed `localconfig.xml.restore` and is copied to the `/opt/zimbra/conf` directory.

If you have made changes since the last backup, you might need to replace the `localconfig.xml` file with the restored copy. Compare these files, and if the `.restore` file has the latest local configuration data, delete the `localconfig.xml` file and rename the file with the `.restore` extension to `localconfig.xml`.

Using snapshots to Backup and Restore

You can backup and restore a server using the snapshot feature provided by the storage layer rather than using Zimbra's backup and restore feature. Using snapshots, you can maintain a standby site and reroute users to the standby site to keep operations running if the primary site fails.

Snapshots are taken for all volumes of data and are transferred to the standby site periodically.

Data volumes that are backed up using snapshots include MariaDB, blobs, Lucene index, and **redologs**.

When the primary site is down, the **zplayredo** command is used to bring consistency to the snapshots and to reapply any changes in data to minimize data loss across volumes

There are four volumes of data:

- MariaDB
- Blob
- Lucene index
- Redologs

Sets of snapshots are taken every hour and transferred to the remote standby site. However, all snapshots are not taken at one instant and could be a second to a minute apart from each other. Also, snapshots of redologs may be taken more frequently. The sequence of events could look like:

```
8:00:00 - snapshot mysql
8:00:01 - snapshot blob
8:00:02 - snapshot index
8:00:03 - snapshot redolog
8:05:00 - transfer the snapshot set to remote site completed
...
8:15:00 - snapshot redolog
8:15:05 - transfer of redolog snapshot to remote site completed
...
8:30:00 - snapshot redolog
8:30:05 - transfer of redolog snapshot to remote site completed
...
8:35:00 - primary site fails
```

On the remote site, there are snapshots from the 8:00 set of data as well as subsequent snapshots of the redologs. They all have to be brought together so that the most recent information is available on the standby site once users are rerouted to it.

You can now run the **zplayredo** command to replay changes from 8:00:00.

```
zplayredo --fromTime "2008/10/17 08:00:00:000"
```

All data is brought forward to the current time and the standby site is set up and running. Data from 8:30:00 to 8:35:00 is lost but that is expected when the restore process is being carried out.

Notes on Ephemeral Data

As of ZCS 8.8, ephemeral data is not backed up as part of the backup process. Since auth tokens are ephemeral attributes, the implication is that clients accessing accounts restored after deletion will

need to re-authenticate; auth tokens generated prior to the backup will no longer work.

Ephemeral Storage SSDB Backend

Backing up Ephemeral Data in SSDB

If SSDB is used as the ephemeral backend, a backup will not include any ephemeral attributes.

Note: This section does not detail how to deploy and administer an SSDB server. For that information please see section [SSDB Configuration Options](#).

Backing up the data stored in SSDB (if so configured) is done as follows:

```
ssdb-dump -h localhost -p 8888 -o /tmp/ephemeral-backup-<date>
```

Note: If running in master / slave configuration the `ssdb-dump` should be run on the **master**.

Example backup

```
ssdb-dump - SSDB backup command
Copyright (c) 2012-2015 ssdb.io

recv begin...
received 1 entry(s)
received 10 entry(s)
received 100 entry(s)
received 1000 entry(s)
received 10000 entry(s)
received 100000 entry(s)
received 200000 entry(s)
received 300000 entry(s)
received 400000 entry(s)
received 400021 entry(s)
recv end

total dumped 400021 entry(s)

Compactions
Level  Files Size(MB) Time(sec) Read(MB) Write(MB)
-----
2       1      7          0        0        7

compacting data...
Compactions
Level  Files Size(MB) Time(sec) Read(MB) Write(MB)
-----
2       2     10          0        0       10

backup has been made to folder: /tmp/ephemeral-backup-<date>
```

Restoring Ephemeral Data to SSDB

Restoring ephemeral data to SSDB from a backup can only be done with a backup from an SSDB server.

Restoration can be done in one of two ways:

- import into a running server
- override of existing data

Importing into a running server

Using the `leveldb-import` command provided with the SSDB software a backup created with the `ssdb-dump` command can be imported into a running SSDB server.

```
leveldb-import localhost 8888 /tmp/ephemeral-backup-<date>/data
```

Data override

- Stop the SSDB server.
- Copy the directory created using the `ssdb-dump` command previously to a known location.
- Update `ssdb.conf` configuration file to update the `work_dir` option to the proper path.
- Start the SSDB server back up and verify previously working logins still work.

Backups with LDAP backend

If the ephemeral backend is LDAP, a backup will not include auth tokens or CSRF tokens, but it will include the last login timestamp. Upon account restore, the appropriate "Last Login" value in the admin console will be restored.

Archiving and Discovery

Zimbra Archiving and Discovery is an optional feature that enables archiving of messages that were delivered to or sent by Zimbra Collaboration and to search across mailboxes.

The installation of the archiving feature provides the ZCS discovery tool (also known as cross mailbox search) and sets the attributes that allow archiving to be enabled on the Zimbra MTAs.

Archiving is configured on a per account basis. Each account enabled for archiving requires a Zimbra archive license. When archiving is enabled for an account, a copy of all email from or to that account is forked at the MTA and a copy of the message is delivered to a predefined archive mailbox. The archiving process is transparent to account users.

Discovery allows you to conduct a search for email messages across live and archived mailboxes and copy the results to a specified mailbox.

How Archiving Works

When a message is sent or received by a user, the message is always routed through the Postfix MTA. The Postfix MTA allows integrating software that can perform actions on messages that are in flight. When archiving is enabled for the sender or the recipient of messages, Zimbra Archiving integrates with an MTA hook and the Amavisd-New utility to fork a copy of the message.

The “**does recipient or sender have archiving enabled**” check is performed on the SMTP standard envelope and not on the From or To/Cc headers. Since checks are performed on the envelope, Bcc copies and messages sent to distribution lists are captured.

Example 43. Sending messages with archiving enabled

For example, if User A sends a message to User B, and if User B has archiving enabled, the MTA delivers two messages — one to User B's mailbox and one to User B's archive mailbox. The message received in User B's mailbox looks normal, as shown in the following example:

```
Received: from localhost (localhost.localdomain [127.0.0.1])  
From: userA@example.com  
To:userB@example.com  
Subject: New License Key  
Message-ID: <015f01c717fe$70f042d1$b1d6f61d@thom>  
Date: Mon, 04 Nov 2008 23:48:18 -0000  
  
Hi B,  
  
Can you send me the license key for the software again?  
  
Thanks, A
```

The message received in User B's archive mailbox contains additional **X-Envelope-From** and **X-Envelope-To** headers. These headers show the real email address the message was sent from and each of the email addresses that the message was sent to.

```
Received: from localhost (localhost.localdomain [127.0.0.1])  
From: userA@example.com  
To:userB@example.com  
Subject: New License Key  
Message-ID: <015f01c717fe$70f042d1$b1d6f61d@thom>  
X-Envelope-From: userA@example.com  
X-Envelope-To: userB@example.com  
Date: Mon, 04 Nov 2008 23:48:18 -0000  
  
Hi B,  
  
Can you send me the license key for the software again?  
  
Thanks, A
```

Zimbra archiving can be set up to create archiving accounts that are maintained within Zimbra Collaboration or to work with third-party archiving systems using SMTP forwarding to send messages to a third-party archive server. For third-party archiving, Zimbra Collaboration is configured to act as the forwarding agent.

How Discovery Works

The discovery feature of Archiving and Discovery is used to search across live* and archive

mailboxes for email messages and attachments. The discovery tool can be run from the Administration Console and the results are copied to a target mailbox that you specify.

* A live mailbox is an account on the system other than archive accounts and system accounts.

You can search outgoing and incoming email by date, from, to, cc, subject, keywords, and attachments. You can also create queries to search by name, dates and time ranges, distribution list, aliases.

Search results are placed in a target mailbox. You can organize your search results by creating different target mailboxes or by creating individual folders within a target mailbox for each search you run. **X-zimbra-Source** header information is added to each message header that is copied to the targeted mailbox. This header label includes the account ID, the account name, and the server that the account resides on.

You can see the results of the search by logging on to the target mailbox address.

Installing the Archiving Package

You can install the archiving package on an existing single-server deployment or on a multi-server deployment.

If the mailbox server and the MTA server reside on the same node, you configure and enable archiving as a single process. If your mailbox and MTA servers are on separate nodes, the **zimbra-archive** package is installed first on at least one mailbox server and then the archiving component is enabled on each MTA in the deployment.

Installing **zimbra-archiving** in a Single-Server Environment

The following scenario assumes that the LDAP, MTA, mailstore and archiving servers are on the same node.

1. Refer to the Zimbra Collaboration Single Server Installation Guide to open an SSH connection to the Zimbra Collaboration server. Log on to the server as **root** and run the **./install.sh** command to begin the upgrade process.
2. Accept the license agreement and type **Yes** to run the upgrade.
3. Type **Yes** for **zimbra-archiving** when presented with the packages to be installed.

The upgrade process begins and the archiving package is installed. At this point, the Discovery feature is installed and can be used.

To enable archiving, switch to the **zimbra** user and enable archiving on the MTA server.

```
zmprov ms <zimbrahostname> +zimbraServiceEnabled archiving
```

Restart the server.

```
zmcontrol restart
```

Installing **zimbra-archiving** in a Multi-Server Environment

The following upgrade scenario is adding a new server that is dedicated as an archiving server to your Zimbra Collaboration environment.

Before beginning the install process, record the following information. You need this information when you install the archiving server. Run the `zmlocalconfig -s` command to find the information.

LDAP Admin Password	-----
LDAP Hostname	-----
LDAP Port	-----

Refer to the Multiple-Server Installation chapter in the Zimbra Collaboration Multi-Server Installation guide for detailed steps on installing the packages.

1. Open an SSH connection to the mailbox server that is being configured for archiving. Log on to the server as **root** and unpack the Zimbra software. Run the `./install.sh` command to begin the install process.
2. Type **y** and press **Enter** to install the following packages:
 - **zimbra-store**
 - **zimbra-archiving**

The **zimbra-core** package is installed by default.

3. Type **y** and press **Enter** to modify the system.
4. The Main menu displays the default entries for the Zimbra component you are installing. To expand the menu, type **x** and press **Enter**.
5. Select the **Common Configuration** menu and configure the LDAP Hostname, LDAP password, and LDAP port.
6. Select the **zimbra-store** menu and configure the Admin password and the License file location.

Complete the installation process following the steps in the Multi-server Installation guide, under Installing Zimbra Mailbox Server.

At this point, the Discovery feature is installed and can be used.

Manage Archiving From the Administration Console

After Archiving is installed, you can set up archiving and manage it from the Administration Console.

Enable Archiving

Admin Console:

Home > Configure > Global Settings > MTA, from Archiving Configuration check **Enable archiving**

Restart ZCS from the command line

```
zmcontrol restart
```

Creating a Dedicated Archive COS

You can configure attributes in the COS to set mailbox features, quotas, and passwords, turn off spam and virus checks, and hide the archive accounts from GAL.

Admin Console:

Home > Configure > Class of Service, from the Gear icon select New

1. Change **Features** and **Preferences** as required for an Archiving COS.
2. If you have a dedicated archive server, in the Server Pool page, deselect the archiver server from the list. In a multi-server deployment with a dedicated archive server, the server should be removed from the COS server pool so that the archive server is not randomly assigned to new accounts.



These steps to remove the server from the server pool are not done in a single-server deployment. Creating a dedicated archiving COS is a good idea as this makes it easy to create archive mailboxes that are configured the same.

3. Modify the options on the **Advanced** page if required.
4. In the **Archiving** page, check the **Enable archiving** box to make this COS an archiving cos.
5. If you want to change the format for the naming scheme for archive accounts, modify the two template fields. See the [Setting Up an Archive Account Name](#) section for more information.
6. Click **Finish**.

Setting Up an Archive Account Name

You use attributes to create and manage the naming scheme for archive accounts. You can set up these attributes either by COS or by account. For COS, these attributes can be changed from the Administration Console, COS or individual account's Archiving page.

- **Account date template.** Sets the date format used in the name template. The default is `yyyyMMdd`. Adding the date to the account name makes it easier to roll off older data from the system to backups.
- **Account name template.** Sets up how the archive mailbox name is created. The default value is

`${USER} ${DATE}@${DOMAIN}.archive.`

The archive account address would be similar to the following example:

`user-20070510@example.com.archive`

If you change the default value, you must use syntax that creates a valid email address. We recommend that you add `.archive` to all archive accounts to create archive mailboxes in a non-routable domain to prevent spoofing of the archives.

When the template based on the `zimbraArchiveAccountDateTemplate` attribute is set up, `amavisArchiveQuarantineAccount` is updated to the new template name when `zmconfigarchive` is run.

Administering the archive server

The `amavisd-new` server process controls account archiving as well as antivirus and anti-spam processes. The `zmarchivectl` command can be used to start, stop, restart or obtain the status of the `amavisd-new` server process that controls account archiving. Caution should be taken when starting or stopping the archiving process as it is a shared server process between archiving, antivirus, and anti-spam processes. Performing actions on any of them affect any of the other services that may be enabled in your deployment.

If you want to disable archiving but not antivirus or anti-spam services, disable the respective service either through the CLI or through the Administration Console.

Set Up Archiving for a Users Mailbox

Four attributes are related to the archive feature for accounts. Two that configure a mailbox and two template attributes to construct the archive account names.

To set up archiving for a mailbox two attributes are configured on the primary user's mailbox. One attributed enables archiving and the second shows where messages are being archived.

- **Currently archived to**—The current archive address. Archiving is to a single account. If this is unset, archiving is not enabled.
- **Archived accounts**—Any previous and current archive addresses that this mailbox was archived to. containing all the accounts that have been archived for the given account.

Archive Mailboxes

You can create an archive mailbox with or without an assigned COS. You can also forward archive email to a third-party.

Accounts with archiving enabled are counted against the number of Zimbra licenses purchased for archiving. Archive mailboxes are listed in the Administration Console along with the live accounts. To see current license information, go to the Administration Console:

Home > Configure > Global Settings > License.



Creating an archive mailbox and assigning a COS

Archive accounts are created based on the Zimbra Archive name templates.

- The attribute — `zimbraIsSystemResource` — is added to the archive account and set to TRUE.
- The archive account is displayed in the Administration Console.
- When a message is received in a mailbox with archiving enabled, a copy of the message is sent to the archive mailbox.

Log on as `zimbra`, and use the `zmarchiveconfig` command:

```
zmarchiveconfig enable <account@example.com> archive-cos <archive>
```

Creating an Archive Mailbox with No COS or Password

If the archive account is not assigned a COS, the following settings are set by default.

- Mailbox quota is set to 0, unlimited quota.
- Spam and virus checks are disabled.
- Hide in GAL is enabled, so the archive account does not display in the GAL

Log on as `zimbra`, and use the `zmarchiveconfig` command:

```
zmarchiveconfig enable <user@example.com>
```

Enabling Archive Forwarding to a Third-party Archiving Server

If the archive account is not maintained within Zimbra Collaboration, you do not need to set a password, COS, or other attributes.

Log on as `zimbra`, and use the `zmarchiveconfig` command:

```
zmarchiveconfig enable <account@example.com> \
archive-address account-archive@offsite.com \
archive-create false
```

Searching Across Mailboxes

When the archiving and discovery feature is installed, you can search across mailboxes either from the Administration Console or through the command line interface.



You do not need to have any archive mailboxes configured to search across mailboxes, but the Archive package must be installed.

You can assign a user to run the mailbox searches from the Administration Console by creating a delegated administrator with rights to access the mailbox search tool.

Cross Mailbox Search from the Administration Console

The discovery tool, **Search Mail**, is added to **Tools and Migration** on the Navigation pane when the archiving package is added. To set up a cross-mailbox search you configure the following information.

Admin Console:

Home > Tools and Migration > Search Mail, from the Gear icon select New

- **Server name.** The server name to be searched.
- **Target mailbox and folders.** One target mailbox and folder are created automatically. You can use this mailbox for all your search results and create new folders for each search, or you can create a new target mailbox for each separate search.

A target mailbox is like any other mailbox and can have any features or preferences that are defined by the COS or by account. Target mailboxes are listed in the Administration Console Accounts list. You might want to give the target mailboxes account names that identify them as target mailboxes for cross-mailbox searches and configure a COS specific for target mailboxes to be able to manage access.

- **Limit the number of messages returned by the search.** The default is 500 results.
- You can select to send an email notification when the search is completed. The email notification includes the search task ID and status on the subject line and you can specify the type of information to include in the message, such as the number of messages found, the list of addresses resulting from the search and the search query used.
- Select which mailboxes to search. When you check **Select accounts to search**, you select which account addresses to search.
- **Create the search query.** You can search outgoing and incoming email by date, from, to, cc, subject, keywords, and attachments. Advanced can be used to quickly create a query to search by name, dates and time ranges, distribution list, aliases.

When searching archive messages, you can search by the envelope address using the **envfrom** and **envto** query language extensions.

As the search runs, the Search Mailbox Content pane lists the search and the status. Click **Refresh** to update this page.

Delete the search task when it is completed because it occupies server memory. When the server is restarted, past searches are deleted.

When you use the discovery feature in the Administration Console, the tool makes copies of messages in the target mailbox you create. The messages occupy server space, increasing the size of your server. You might want to delete these messages from the target mailbox when they are no longer needed.

Legal Requests for Information

The Legal Intercept feature makes copies of email messages sent, received, or saved as drafts from targeted accounts and sends these messages to a designated “shadow” email address.

Legal Intercept can be configured to send the complete content of the message or to send only the header information. When a targeted account sends, receives, or saves a draft message, an intercept message is automatically created to forward copies of the messages as attachments to the specified email address.

Legal Intercept Settings

The Legal Intercept feature can be configured either for a Class of Service or an individual account. The feature is configured from the CLI, using `zmprov`.

The only required configuration to set up Legal Intercept is to enable the feature — `zimbraInterceptAddress` — on target accounts or COS.

You can enable the attribute `zimbraInterceptSendHeadersOnly` to send only the header information of the email message instead of sending the complete message.

Setting Up Legal Intercept

Specify the intercept address to receive intercepted messages.

- If enabling intercept by COS:

```
zmprov mc <cosname> zimbraInterceptAddress <account@intercept.example.com>
```

- If enabling Intercept for an account:

```
zmprov ma <accountname@example.com> zimbraInterceptAddress  
<account@intercept.example.com>
```

If you are going to use the default intercept message template and From address (`postmaster@<yourdomain.com>`), a Legal Intercept is set up.

Setting Up Legal Intercept to Forward the Message Header

To forward the header information, instead of the complete message for an account:

```
zmprov ma <accountname@example.com> zimbraInterceptSendHeadersOnly TRUE
```

Modifying the Intercept Cover Email Message

An email message is automatically created to forward copies of the intercepted messages as attachments. The default message includes:

- **From** address is “postmaster@<yourdomain.com>”
- **Subject** line “Intercept message for <account@yourdomain.com> <interceptedmessage subject>”
- **Message** “Intercept message for <account@yourdomain.com>. Operation=<type of message>, folder=<foldername>, folder ID=<#>”.

The cover email message can be modified. Use the following parameters to modify the email message.

ACCOUNT_DOMAIN	Domain of the account being intercepted.
ACCOUNT_ADDRESS	Address being intercepted
MESSAGE SUBJECT	Subject of the message being intercepted.
OPERATION	Operation that the user is performing, “add message”, “send message”, or “save draft”.
FOLDER_NAME	Name of the folder to which the message was saved.
FOLDER_ID	ID of the folder to which the message was saved.
NEWLINE	Used for formatting multi-line message bodies.

Use steps in this section to change the from-name, the subject line, or text in the message body:

- To change the **From** name:

```
zmprov ma <accountname@example.com> zimbraInterceptFrom '<newname@example.com>'
```

- To change the text of the **Subject** line:

```
zmprov ma <accountname@example.com> zimbraInterceptSubject \
'<Intercepted message subject text> parameter <text> parameter'
```

- To change the text in the **message body**:

```
zmprov ma <accountname@example.com> zimbraInterceptBody \
'<Intercepted message text> parameter <text> parameter'
```



To modify by COS, type `zmprov mc {cosname}`.

Creating Mailbox Snapshots for Legal Discovery

You can create a query for the user's mailbox using the REST URL format to search for specific types of email messages and attachments and have these messages zipped and saved to your computer. This **zip** file can be forwarded to a requesting law enforcement agency.

The email message appears as an **.eml** file name after the subject line. The attachments get saved in the format that they were delivered.

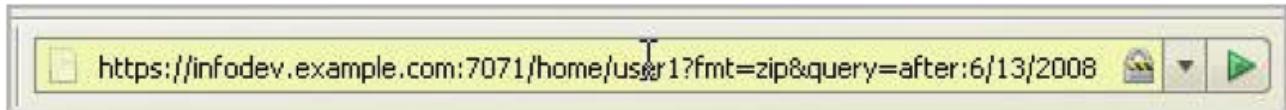
Creating a Mailbox Snapshot **zip** File

You must be logged into the ZCS Administration Console to create the **zip** file. You create a query for one account at a time.

1. In the Administration Console address field of the browser, after the port number **7071/**, type:

```
home/<username>?fmt=zip&query=<searchquerystring>
```

For example:



In the above example, the search query is requesting a **zip** file of all accounts called **user1**.

You can use any search operators supported for searching in ZCS. For example, you can search by folder (**in:folder_name**), by sender's name (**from:<someone>**), and you can use multiple search terms. See the Search Tips wiki page for keyword examples, https://wiki.zimbra.com/wiki/Search_Tips.

2. Press **Enter** or the arrow to create the zip. A **Confirm** box displays, asking if you want to navigate away from this page.
3. Click **OK**.
4. Choose where you want to save the **zip** file. This **zip** file is ready to be delivered.

Color and Logo Management

You can change the logo and base colors of the Zimbra Web Client themes without having to customize individual Zimbra Collaboration themes. This can be done from the administration console or the CLI.

Changing Theme Color and Logos on the Zimbra Web Client

Base colors for themes, and custom logos can be configured as a global setting or as a domain setting.

- When the global settings are changed, the changes apply to themes on all servers.
- When the domain settings are changed, the base color and logos for themes on the domain are changed.

If global settings and domain-level settings for theme base colors or logos are not identical, the domain values are displayed for the domain.



If the logo and base colors are customized in multi-domain Zimbra Collaboration environments, you must set a virtual host as the base color: logo attributes are displayed based on the Host header sent by the browser.



Various Zimbra themes are included with Zimbra Collaboration. Some of these themes - such as lemongrass, Hot Rod, and Waves - have been designed with graphics or color codes that do not change when you modify the base color. You might want to disable those themes from user's Theme preferences selection.

Customizing Base Theme Colors

The following base colors in Zimbra Web Client themes can be changed:

- The primary background color displayed in the client.

This color is the background of the page. Variants of the color are used for buttons, background color of the Content and panes, tabs, and selection highlight. In the following image, the background color displays with the logo, the variant of the background color displays in the login area.

- The secondary color is the color used for the toolbar.
- The selection color is the color displayed for a selected item such as a message or an item in the Overview pane.
- The foreground color is the text color displayed. The default text color is black. The text color usually does not need to be changed.

Replacing the ZWC Logo

You can replace the log with your company's logo globally or per domain.



License Policy for Logo Replacement

The Zimbra Public License does not allow removing the Zimbra logo in the Zimbra Web Client. Only Network Edition customers can replace Zimbra logos that display in the Zimbra Web Client. Therefore, only customers of the Network Edition should use these instructions. Additional information about the license usage can be found at <https://www.zimbra.com/license/>.

Graphics to Replace

The following logo files can be changed. Your logos must be the same size as specified here or the image might not display correctly. These graphic files can be saved on another server or in a directory that is not overwritten when Zimbra Collaboration is upgraded.

- Company logo that displays on the login and splash screens for Zimbra Web Client and the Zimbra Collaboration administration console. The dimension of the graphic must be exactly 300 x 30.
- Small company logo in the upper-left of the Zimbra Web Client application and the administration console. The dimension of the graphic must be exactly 170 x 35.
- Company Web address that links from the company logos.

Graphics not replaced

The icon that displays in the Advanced search toolbar and the favicon.ico that displays in the URL browser address field cannot be changed at this time.

Using the Admin Console to Modify Theme Colors and Logo

On the administration console, the Global Settings and the Domains settings include a Themes page that can be configured to customize the color scheme and to add a company logo and logo URL. You upload your company logo to be used on the Zimbra Web Client and administration console pages.

Changing Base Theme Colors

You can either select colors from popup view of predefined colors, or enter the six-digit hexadecimal color value for an exact color match to set theme colors for the following categories:

- Foreground, which is the text color.
- Background, which is the primary background color displayed in the client.
- Secondary, which is the color used for the toolbar and selection headers in the pane.
- Selection, which is the color displayed for a selected item such as a message, right-click, or drop down menu selection.



Changes to theme settings require the server theme cache to be flushed. To flush a server, go to **Home > Configure > Servers** to get the list of servers. Right-click on a server and select **Flush Cache** from the popup menu.

Use the **Customize the theme colors** container to set colors for your theme categories:

Admin Console:

Home > Configure > Global Settings > Themes or
Home > Configure > Domains → *domain* → Themes

1. Click on the field alongside the theme category to be modified, then use the popup color selector to define the color for your selection.

You can either click directly on a color, or use the entry field to write the hexadecimal value of the color. In either case, your selection will be displayed in the field.

If you opt out of your color selections, click **reset all theme colors** to discard your settings.

2. Navigating away from this page results in query for save of the settings.

Click **Yes** (to save) or **No** (to discard your settings).

Adding Your Logo

You can replace the Zimbra Collaboration logo with your company's logo globally or per domain from the appropriate Themes page. Your logos must be the same size as specified in the **Graphics to Replace** section or the images might not display correctly. The graphic files are saved on another server or in a directory that is not overwritten when Zimbra Collaboration is upgraded.



When you configure the **Customize the logo of the themes** section in the **Global Settings > Theme** page, all fields in this section must be completed to display the graphics correctly.

The Zimlet icon that displays in the Advanced search toolbar and the favicon.ico that displays in the URL browser address field are not changed.

Use the **Customize the logo of the themes** container to a logo to accompany the theme:

Admin Console:

Home > Configure > Global Settings > Themes or
Home > Configure > Domains → *domain* → Themes

Table 56. Logo Settings

Option	Description
Logo URL of the themes	The company web address to be linked from the logo.

Option	Description
Application logo banner URL of the themes	The company logo that displays on the login and splash screens for the Zimbra Web Client and admin console. the dimension of the graphic must be exactly 450x100.
Application logo banner preview (200x35)	The company logo in the upper-left of the Zimbra Web Client application and the administration console. the dimension of the graphics must be exactly 120x35.
Login logo banner URL of the themes	
Login logo banner preview (440x60)	

Using the CLI to Change Theme Colors and Logo

To change the Zimbra Web Client theme base colors and logos, use the zmprov command. The following attributes are configured either as a global config setting or as a domain settings. Color values are entered as a six-digit hexadecimal codes.

Table 57. Color Attributes

Attribute	Description
<code>zimbraSkinBackgroundColor</code>	The hex color value for the primary background color displayed in the client.
<code>zimbraSkinSecondaryColor</code>	The hex color value for the toolbar and selected tabs.
<code>zimbraSkinSelectionColor</code>	The hex color value for the color of the selected item.
<code>zimbraSkinForegroundColor</code>	The hex color value for the text. This usually does not need to be changed as the default is black.

Changing base colors for themes

Before you begin, identify the six-digit hexadecimal base color values for the various elements you are changing. You will be using these in your command entries.

Global Settings

```
zmprov modifyConfig <attribute-name> [#[HEX_6digit_colorcode#]]
```

Domain Settings

```
zmprov modifyDomain <domain> <attribute-name> [#[HEX_6digit_colorcode#]]
```

Modifying a domain

The example in this section demonstrates how to change to the following base colors:

- Background color = Coral, #FF7F50
- Secondary color = turquoise, #ADEAEA
- Selection color = yellow, #FFFF00

1. Specify the skin colors: Log in as the `zimbra` user and use `zmprov` to modify the domain:

```
zmprov modifyDomain example.com \
zimbraSkinBackgroundColor "#FF7F50" \
zimbraSkinSecondaryColor "#ADEAEA" \
zimbraSkinSelectionColor "#FFFF00"
```

The quote marks, "", are required so the use of the # sign does not comment out the text that follows.

2. Use the `zmmailboxdctl` command to apply the changes by restarting the mailbox server process:

```
zmmailboxdctl restart
```

Reload the web client and Zimbra Collaboration themes for that domain should now display these colors.

Adding Your Logos

You add the company logo information and URL by modifying these the following attributes for logos:

Table 58. Logo Settings

Attribute	Description
<code>zimbraSkinLogoURL</code>	The company Web address that you want linked from the logo.
<code>zimbraSkinLogoLoginBanner</code>	The company logo file name that is displayed on the login and splash screens for the ZWC and the Zimbra Collaboration administration console.
<code>zimbraSkinLogoAppBanner</code>	The logo graphic file name for the graphic in the upper-left of the ZWC application and the administration console.

To add logos for a domain

If logo files are saved in the Zimbra Collaboration server, they must be in a subdirectory of `/opt/zimbra/jetty/webapps/zimbra`.

If the logos are hosted on another machine, enter the full URL when identifying the logo.

Use steps in this section to update the logo(s) displayed over a domain:

1. Change the URL link:

```
zmprov modifyDomain zimbraSkinLogoURL https://url.example.com/
```

2. Modify the logo display:

To change the logo displayed in the login and splash screens:

```
zmprov modifyDomain zimbraSkinLogoLoginBanner /zimbra/loginlogo.png
```

To change the logo displayed on the Zimbra Web Client main page:

```
zmprov modifyDomain zimbraSkinLogoAppBanner /zimbra/applogo.png
```

3. Stop/start the server:

```
zmcontrol restart
```



Not currently supported: Logo modification for the Zimbra Web Client.

Zimlets

Zimlets are a mechanism to integrate ZCS with different third-party applications to enhance the user experience from the Zimbra Web Client. With Zimlets, users can look at information and interact with the third-party application from within their email messages. Zimlets can be made available from the Zimbra Web Client Overview Pane to users by modifying the Class of Service (COS).

ZCS includes several predefined Zimlets. You can also create Zimlets or download them from the Zimlet Gallery located on the Zimbra Web site.

Predefined Zimlets when enabled let users preview the following:

- Mouse over a date or time and see what is in calendar.
- Mouse over a name or email address and see details from the address book for this name.
- Right-click on a phone number to make a call with your soft-phone.
- Right-click on a date to schedule a meeting.
- Right-click on a name, address, or phone number to update address book information.

For information about creating Zimlets, see the Zimlet Development section on the Zimbra Wiki.

Managing Zimlets from the Administration Console

The following Zimlet management tasks are available from the Zimbra Administration Console.

- Deploy a Zimlet, which creates the Zimlet entry in the LDAP server, installs the Zimlet files on the server, enables the Zimlet and makes it available to the members of the default COS.
- Make a Zimlet available or not available per COS or account.
- Make a Zimlet mandatory.
- Disable a Zimlet, which leaves it on the server, but the Zimlet is not used.
- Undeploy a Zimlet, which removes it from the COS listings and the Zimlets list but does not uninstall the Zimlet from the server.



You cannot uninstall the Zimlet from the Administration Console.

Deploying Custom Zimlets

You can download and deploy custom Zimlets from the Zimlet Gallery located on the Zimbra Web site. When a Zimlet is deployed, it is available immediately to everyone in the default COS. If a Zimlet is not deployed to another COS directly, the COS displays the Zimlets but they are not enabled.

Admin Console:

Home > Configure > Zimlets, from the **Gear** icon select **Deploy**

1. Browse to the Zimlet you want to deploy, then click **Deploy**.

The Zimlet deploys to the server. A dialog displays indicating the server name where the Zimlet is deployed and the status of the deployment.

2. Click **Finish**.

Verify the Zimlet is enabled by viewing the Zimlets page.

Enable, Disable, or Make Zimlets Mandatory

You can enable, disable, or make Zimlets mandatory. You can also use the toggle feature to choose if an installed Zimlet will be made available for users to choose from.

Admin Console:

Home > Configure > Class of Service → COS → Zimlets

Table 59. Zimlet Operational Status Settings.

Setting	Description
Mandatory	Zimlet will always be enabled in user accounts. Users do not see these Zimlets on their Zimlet page.
Disabled	Zimlet will not be immediately available to users in the associated COS.
Enabled	All deployed Zimlets will be enabled.



Users can enable or disable optional Zimlets from their account's **Preferences > Zimlets** page. If you select a Zimlet as mandatory, it cannot be disabled by the user.

Undeploying a Zimlet

When a Zimlet is undeployed, it is removed from all COSS and then removed from the LDAP.

Admin Console:

Home > Configure > Zimlets

1. Select a *Zimlet* to undeploy.
2. From the **Gear** icon menu select **Undeploy**.
3. Click **Yes** to confirm.

Adding Proxy-Allowed Domains to a Zimlet

Proxy Allowed Domains lets you configure which external domains can be accessed through a Zimlet. For the Zimlets that are included in ZCS, proxy allowed domains are already configured. If you download and deploy other Zimlets, you can add additional proxy domain names.

Admin Console:

Home > Configure > Class of Service

1. Select the *COS* to edit.
2. In the **Advanced** page, scroll down to the **Proxy Allowed Domains** section.
3. Click **Add Domain** to add domains.
4. Click **Save**.

Upgrading a Zimlet

Use the same steps as deploying a new Zimlet to upgrade a customized Zimlet. The new Zimlet **zip** file should have the same name as the existing Zimlet **zip** file.

Admin Console:

Home > Configure > Zimlets, from the **Gear** icon select **Deploy**

1. Check **Flush Zimlet cache**, so that the upgraded zimlet will be used.
2. Browse to the *Zimlet* you want to upgrade, then click **Deploy**.
3. Click **Finish**.

Managing Zimlets from the Command Line Interface

The following Zimlet management tasks are available from the command line interface.

Deploying Zimlets

When a Zimlet is deployed, it is available immediately to everyone in the default COS. If a Zimlet is not deployed to another COS directly, the COS displays the Zimlets but they are not enabled.

Deploy a Zimlet using the CLI, including modifying the COS before deploying.

1. Select a Zimlet and copy the Zimlet **zip** file to **/tmp** folder on your Zimbra server.
2. Login as the **zimbra** user **su - zimbra**
3. Deploy the Zimlet

```
zmzimletctl deploy /tmp/<zimlet>.zip
```

Adding Proxy Allowed Domains to a Zimlet

When deploying a Zimlet, the COS attributes, **zimbraProxyAllowedDomains**, must be set for the domain address that the Zimlet might call to get information.

To set the **zimbraProxyAllowedDomains** attribute, type:

```
zmprov mc <COSname> +zimbraProxyAllowedDomains '*.example.com'
```

The * must be added before the [example.com](#).

This must be applied to all COSs that have your Zimlet enabled.

Deploying a Zimlet and Granting Access to a COS

Use steps in this section to deploy a Zimlet to one or more COSs other than the default:

1. Login as zimbra user: su – zimbra
2. Copy the Zimlet file from Gallery to /tmp folder.
3. Install the Zimlet to the default COS:

```
zmzimletctl deploy /tmp/<zimlet>.zip
```

4. To deploy the zimlet to additional COSs, run:

```
zmzimletctl acl <zimletname> <cosname1> grant
```

This will grant permission to [cosname1](#). You can also grant access to more than one COS on the same command line:

```
zmzimletctl acl <zimletname> <cosname1> grant <cosname2> grant
```

5. To allow this zimlet to use the allowed proxy domains, run the following on each COS and add the allowed domains.

```
zmprov mc <COSname1> +zimbraProxyAllowedDomains '*.example.com'  
zmprov mc <COSname2> +zimbraProxyAllowedDomains '*.example.com'
```

Viewing Installed Zimlets

Use the [zmzimletctl](#) command to view currently installed Zimlets:

```
zmzimletctl listZimlets all
```

The output from this command displays the Zimlets installed on the server, installed in LDAP, and those available by COS.

Changing Zimlet Configurations

Some Zimlets may require additional configuration after they are deployed.

The Zimlet configuration template allows you to make changes on the configuration template and then install the new configuration file on the Zimbra server.

Use steps in this section to change a Zimlet configuration:

1. Extract the configuration template:

```
zmzimletctl getConfigTemplate <zimlet.zip>
```

2. Make the required changes in the template, taking care to change only the required areas, then save the file.



If you have more than one custom Zimlet, rename the config template.xml file before updating the configuration in LDAP so that files are not overwritten.

3. Use the `zmzimletctl` command to update the configuration in the LDAP. If you changed the name of the configuration template, replace `config_template.xml` with the new name.

```
zmzimletctl configure config_template.xml
```

Upgrading a Zimlet

Upgrading a customized Zimlet is performed by using the same steps as those used to deploy a new Zimlet.



The new Zimlet `zip` file should be named identically to the existing Zimlet `zip` file.

Use steps in this section upgrade a Zimlet:

1. Copy the Zimlet `zip` file to the `/opt/zimbra/zimlets-extra` folder, replacing the older version.
2. Deploy the Zimlet

```
zmzimletctl deploy <zimlet.zip file name>
```

The Zimlet is copied to the `/opt/zimbra/zimlets-deployed` folder. If your Zimlet includes a `.jsp` file, the `.jsp` file is also copied to the `/opt/zimbra/jetty/webapps/zimlet/<zimletnamefolder>`.

3. To ensure availability of the newer version, flush the cache:

```
zmprov flushCache zimlet
```

Using the Zimbra Gallery

You can download and deploy Zimlets from the Zimlet Gallery located on the Zimbra web site. Go to <https://www.zimbra.org/extend/> and scroll through the Extensions from the Zimbra Gallery section.

Developing Customized Zimlets

To develop your own custom Zimlets, see the Zimlet Developers Guide on the Zimbra Wiki at <https://wiki.zimbra.com>.

Using the Voice Service

Unified Communications (UC) is the integration of multiple modes of communication services, allowing users to receive communication from one service, such as voice mail, and respond using another service, such as Click-to-Call.

Zimbra uses real-time communications services such as voice, telephony and presence to inter-operate with non-real-time services such as email and voice mail. The Zimbra Collaboration Voice Service feature includes Visual Voice Mail, Click-to-Call, and Presence (Cisco only). Zimbra Collaboration uses Cisco or Mitel servers, as a third-party voice server, or UC server, to bridge calls between Zimbra Collaboration and the Zimbra Web Client (ZWC).

Note: UC system administrators are responsible for configuring the UC server based on that UC server's documentation.

You enable the voice service from the administration console. Users use the voice service feature from the Voice tab in the ZWC.

When users sign into the voice service from their ZWC account, they are actually logging into a UC server. After the initial user set-up, the voice service is seamless and requires no additional account configuration.

Voice service features include:

- **Visual Voice Mail:** From the Voice tab, users can easily view and listen to voice mails and view details such as caller name, time details, and length of message. Users can call back the person that left the message, forward or reply to the message by email, save or delete the message, and select how to be notified of a new voice message. Supported audio formats include WAV and MP3.
- **Click-to-Call:** The ability to make a phone call from a ZWC account. Users can highlight and click phone number in their email to dial, or select a contact's phone number from their contact lists. The call is bridged from the registered physical or soft phone the user selects to use to call the recipient. Click-to-Call eliminates the use for a dial pad on a phone.
- **Click-to-Chat:** (Cisco clients only) The ability to chat with a contact using the Cisco Jabber client and ZCS. Users must have the recipient's IM address stored in their contact information. They can then access the recipient's contact card and click the IM link to initiate a chat session.
- **Presence:** (Cisco clients only) The ability to display in real time the availability information about users or contacts. When using Cisco Jabber, users can manually set their presence status or it is automatically set for them. For example, when users are on a phone call their presence status is automatically set to "on a call". Presence status is displayed as available, away, on a call, or do not disturb.

Order of Configuration

To create voice service, follow the order of configuration as follows:

1. Access URLs, as described in Using a Third-Party Unified Communications Server.

2. Create the voice service, as described in Creating the Voice/Chat Service.
3. Enable the voice service and the voice feature, as described in Enabling the Voice/Chat Service. Enabling the voice feature allows the Voice tab to display in the ZWC.
4. Enable the appropriate Zimlets for the vendor server you are using, as described in Enabling the Voice/Chat Zimlets.

Voice Service Requirements

The following are required for ZCS voice service:

- **Voice Service license:** A ZCS license with the voice service feature is required. To obtain this license, see the Zimbra Collaboration Server License section for more information.
- **Unified Communications Server:** Third-Party Unified Communications server requirements for either Cisco or Mitel are listed below. URLs from the UC server are used in the configuration of the ZCS voice service, as described in Using a Third-Party Unified Communications Server.
 - **For Cisco:** **Cisco Unity Connection (UC) 8.5 and above.** Cisco UC generates the Voice URL used in the voice service configuration. **Cisco Unified Communications Manager (CUCM) 7.1(3):** Enable Web Dialer service for Click-to-Call functionality. Cisco CUCM generates the Call URL used in the voice service configuration. **Cisco Unified Presence Server (CUPS) 8.0:** Cisco CUPS requires Presence Web Service to be enabled, and an application user must be created for viewing the presence. This is done in Cisco Communications Manager (CUCM) > User Management. Cisco CUPS generates the Presence URL used in the voice service configuration. **Cisco Jabber client provided to users for UC collaboration.**
 - **For Mitel:** **Mitel Unified Communicator Advanced (Mitel UCA) 5.0.23.0 release and above.** Mitel UCA generates the URLs used in the voice service configuration.
- **ZCS Zimlets:** Voice Preferences Zimlet, Cisco Click2Call Zimlet or Mitel Click2Call Zimlet

Using a Third-Party Unified Communications Server

The ZCS Voice Service uses a third-party Unified Communications (UC) server to bridge calls between ZCS and the UC server. UC server domain information is added to the ZCS administrator console as a Proxy Allowed Domain. This allows Zimlets that are used in the configuration of the voice service to send requests to the UC servers, such as for the Click-To-Call and/or Presence feature. The following URLs from the UC server are used to configure the voice service.

Cisco URLs

- **Voice URL:** The Voice URL is the URL of the Cisco UC server. For example, <https://xx.xx.xxx.xx>. This URL is used by the ZCS server to fetch user's voice mails from the Cisco UC server on behalf of users.
- **Call URL:** The Call URL is the URL of the Cisco CUCM server. For example, <https://xx.xx.xxx.xx/webdialer/services/WebdialerSoapService70>. This URL is used by the ZCS Cisco Click2Call Zimlet to send requests to the Cisco CUCM server to bridge calls.

- **Presence URL:** The Presence URL is the URL of the Cisco CUPS server and used to generate a session ID. For example, <http://xx.xx.xxx.xx:8082/presence-service/users>. This URL is used by the ZCS Email Zimlet to send fetch requests to the contact's presence from the Cisco CUPS server.

Note: Provision an application user name and password using the Cisco Unified Presence Server (CUPS).

Mitel URLs

- **Voice URL:** The Voice URL is the URL of the Mitel server. For example <https://xx.xx.xxx.xx>. This URL is used by the ZCS server to fetch user's voice mails from the Mitel Voice server on behalf of users.
- **Call URL:** The Call URL is the URL of the Mitel server. For example, <https://xx.xx.xxx.xx/webdialer/services/WebdialerSoapService70>. This URL is used by the ZCS Mitel Click2Call Zimlet to send requests to the Mitel server to bridge calls.
- **User URL:** The User URL is the URL of the Mitel server. This URL is used by ZCS for user identification/authentication.

Creating the Voice/Chat Service

When creating the voice/chat service in ZCS, you are enabling the bridge between ZCS and a third-party UC server. You create a service for a domain, Class of Service (COS), or user.

1. In the ZCS administrator console, go to the **Home>Configure>Voice/Chat Service** page.
2. From the gear icon menu, select **New**.
3. On the Choose Voice/Chat Vendor, select your vendor from the drop-down menu.
4. Click **OK**.
5. Add a **Display name** for the domain, COS, or user you are creating.
6. Add the URLs for the voice services you want to enable.
7. Click **OK**.

Configure Presence (Cisco only)

If configuring Presence, you must generate a Presence Session ID.

1. Go to **Configure>Voice/Chat Service** page.
2. Select the voice service for which you want to generate a Presence Session ID.
3. Click the gear icon drop down menu and select **Generate Session ID** from the menu.
4. Enter the **Presence User Name** and **Presence Password**, which are the credentials for the presence server to authenticate the voice connection between ZCS and the UC server. This allows ZCS to retrieve presence information for users.
5. Click **OK**. A presence session ID is generated and displays as the **Presence Session ID**.

Enabling the Voice/Chat Service

After you create the voice/chat service for a domain, COS, or user, you must enable the voice/chat service. For COS and User accounts, you also enable the voice feature which displays the Voice tab in the ZWC.

Enable Voice/Chat Service on a Domain

For Voice/Chat service on a domain, enable the service on the Domains>General Information page.

1. Go to the **Configure>Domains** page.
2. Select the domain for which you want to enable voice service.
3. Click the gear icon menu and select **Edit**.
4. Scroll down to Voice and Chat section and from the **Voice/Chat Service** drop-down menu select the voice service to enable.
5. Click **Save**.

Enable Voice/Chat Service on a COS

For Voice/Chat service on a COS, you must first enable the voice/chat service and then enable the voice feature.

1. Go to the **Configure>Class of Service** page.
2. Select the COS for which you want to enable the voice service.
3. Click the gear icon drop and select **Edit**.
4. On the General Information page, scroll down to **Voice and Chat** section and from the **Voice/Chat Service** drop-down menu select the voice service to enable.
5. In the Navigation pane, click **Features**.
6. On the Features page, scroll down to **Voice and Chat Features** section and click **Enable Voice Feature**. This displays the Voice tab in the ZWC.
7. Click **Save**.

Enable Voice/Chat Service on a User Account

For Voice/Chat service on a User Account, you must first enable the voice/chat service and then enable the voice feature.

1. Go to the **Home>Manage>Accounts** page.
2. Select the account for which you want to enable voice service.
3. Click the gear icon drop and select **Edit**.
4. On the General Information page, scroll down to **Voice and Chat** section.
5. From the **Voice/Chat Service** menu select the voice service to enable.

6. Enter a **Chat/Voice Username** for the user. This is the user account name in the third-party UC server. If you do not provide a name, the default name is used. For example for email account “user1@domain.com”, the default voice username is “user1”.
7. From the **Voice/Chat Service** menu select the voice service to enable.
8. In the Navigation pane, click **Features**.
9. On the Features page, scroll down to **Voice and Chat Features** section and click **Enable Voice Feature**. This displays the Voice tab in the ZWC.
10. Click **Save**.

Enabling the Voice/Chat Zimlets

Zimlets are used in the configuration of the voice service to enable the service and send requests to the UC servers. The Voice Preferences Zimlet adds a voice page to the user interface, and the vendor specific Click2Call Zimlets provide the click to call capability.

1. Go to the **Home>Configure>Zimlets** page.
2. Enable the Voice Preferences Zimlet.
 - Select the **Voice Preferences** Zimlet in the Content pane.
 - Go to the gear icon menu and select **Deploy**.
3. Enable the vendor Zimlet for Click2Call.
 - Select the Zimlet appropriate to the vendor server you are using:
4. If you are using Cisco, select the **Cisco Click2Call** Zimlet.
5. If you are using Mitel, select the **Mitel Click2Call** Zimlet.
 - Go to the gear icon menu and select **Deploy**.

If you want to undeploy a Zimlet, select the Zimlet and go to the gear icon drop down menu and select **Undeploy**, or you can toggle the Zimlet.

Backup Next Generation NG

Real-Time Scan

What is the Real-Time Scanner?

The Real-Time Scanner is the most significant innovation in Backup NG. Each event on the system is recorded live to Zimbra's RedoLog and saved by Backup NG, which means that it is always possible to rollback an account to a previous state. Thanks to the Real-Time Scanner, all the restore modes work with split-second precision.

How Does it Work?

The Real-Time Scanner reads all the events of the mail server almost real-time by following the flow of information provided by the RedoLog. Then it 'replicates' the same operations on its data structure, creating items or updating their metadata. No information in the backup gets overwritten, so every item has its complete history.

Managing the Real-Time Scanner

Enabling the Real-Time Scanner

Via the Administration Zimlet

- Select the Backup NG Tab.
- Under Real-Time Scanner, press the **Enable** button.

 When the Real-Time Scanner is enabled for the first time or re-enabled after a stop, a SmartScan is required. A warning gets displayed after enabling the Real-Time Scanner, prompting you to start the SmartScan either via the CLI or the Admin Console.

Via the CLI

The `ZxBackup_RealTimeScanner` property of the Backup NG module must be set to `true` to enable the Real-Time Scanner via the CLI:

```
zxsuite backupsetProperty ZxBackup_RealTimeScanner TRUE
```

Disabling the Real-Time Scanner

Via the Administration Zimlet

- Select the Backup NG Tab.
- Under Real-Time Scanner, press the **Disable** button.

Via the CLI

The `ZxBackup_RealTimeScanner` property of the Backup NG module must be set to `false` to disable the Real-Time Scanner via the CLI:

```
zxsuite backupsetProperty ZxBackup_RealTimeScanner FALSE
```

Why Should I Disable the Real-Time Scanner?

The only time you should disable the Real-Time Scanner is while performing an External Restore of multiple domains, as a safety measure to avoid high load on your server. After the import, re-enable the Real-Time Scanner and perform a SmartScan when prompted.

Limitations and Safety Scan

The main limitation when restoring data acquired via the Real-Time Scanner is:

- **Emptied Folder** - when a user uses the `Empty Folder` button in the right-click context menu

In this case, and any time Backup NG cannot determine the status of an item by reading the metadata saved by the Real-Time Scan, an Account Scan on the given account is triggered BEFORE the restore.

Doing so fixes any misaligned data and sanitizes the backed up metadata for the mailbox.

Blobless Backup Mode

Blobless Backup Mode is a new feature that avoids backing up item blobs while still safeguarding all other item-related information.

This mode takes advantage of advanced storage capabilities of the storage solution, such as built-in backup or data replication, optimizing both the backup module's disk space usage and restore speed.

Blobless Backup Requirements

These are the requirements to enable Blobless Backup Mode:

- The server is running Zimbra 8.8.15 or higher.
- No "independent" third-party volumes must exist: Blobless Backup Mode is only compatible with local volumes and centralized third-party volumes.

Blobless Backup Mode is storage-agnostic and can be enabled on any server or infrastructure that meets the requirements above regardless of the specific storage vendor.

How Blobless Backup Mode works

Blobless Backup Mode works exactly as its default counterpart: the RealTime Scanner takes care of backing up item changes while the SmartScan manages domain/cos/account consistency. The only

difference between the two is that in Blobless Backup Mode, the backup contains no items of kind **blob** while still saving all metadata and transaction history.

It's essential to consider that once enabled, Blobless Backup Mode affects the entire server, and no blobs get backed up regardless of the target volume and HSM policies.

Restoring Data from a Blobless Backup dataset

To date, Blobless Backup Mode is only compatible with the "Raw Restore" operation. In the future, additional restore operations will become compatible with blobless datasets.

Enabling Blobless Backup Mode

Blobless Backup Mode can be enabled or disabled through the **backupBloblessMode** NG attribute at global and server level:

```
zxsuite config global set attribute backupBloblessMode value true  
zxsuite config server set mail.example.com attribute backupBloblessMode value true
```

SmartScan

What is the SmartScan?

The SmartScan is the primary coherency check for the health of your backup system. It's **Smart** because it operates only on accounts modified since the last SmartScan, hence improving system performance and decreasing scan time exponentially.

The default SmartScan schedule executes each night (if **Scan Operation Scheduling** is enabled in the Backup NG section of the Administration Zimlet). Once a week, on a day set by the user, a Purge executes together with the SmartScan to clear Backup NG's datastore from any deleted item that exceeded the retention period.

How Does it Work?

The Backup NG engine scans all the items on the Zimbra Datastore, looking for items modified after the last SmartScan. It updates any outdated entry and creates any item not yet present in the backup while flagging as deleted any item found in the backup and not in the Zimbra datastore.

Finally, it updates all configuration metadata in the backup to store domains, accounts, COSSs, and server configurations along with a dump of all LDAP data and config.

When is a SmartScan Executed?

- When the Backup NG module starts.
- Daily, if the Scan Operation Scheduling is enabled in the Administration Zimlet.
- When re-enabling the Real-Time Scanner via the Administration Zimlet after being previously disabled.

Running a SmartScan

Starting the Scan via the Administration Zimlet

To start a SmartScan via the Administration Zimlet,

- Open the Administration Zimlet.
- Click the Backup NG tab (be sure to have a valid license).
- Click [Run Smartscan](#).

Starting the Scan via the CLI

To start a FullScan via the CLI, use the [doSmartScan](#) command:

Syntax:

```
zxsuite backup doSmartScan [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE
notifications(0)	Email Address[...]

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup dosmartscan notifications user1@example.com,user2@example.com
Performs a smart scan and sends notifications to user1@example.com and
user2@example.com
```

Checking the Status of a Running Scan

To check the status of a running scan via the CLI, use the [monitor](#) command:

Syntax:

```
zxsuite backup monitor {operation_uuid} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE
operation_uuid(M)	Uiid
operation_host(0)	String

(M) == mandatory parameter, (0) == optional parameter

Purge

What is the Backup Purge?

The Backup Purge is a cleanup operation that removes from the Backup Path any deleted item that exceeded the retention time defined by the [Data Retention Policy](#).

How Does it Work?

The Purge engine scans the metadata of all deleted items, and it removes any item whose last update (deletion) timestamp is higher than the retention time.

Any item BLOB still referenced by one or more valid metadata files is not deleted, thanks to Backup NG's built-in deduplication.

SPostfix customizations backed up by Backup NG also follow the backup path's purge policies. Change policies in the [Backup NG](#) section of the Administration Zimlet by unchecking the [Purge old customizations](#) checkbox.

When is a Backup Purge Executed?

- Weekly, if the Scan Operation Scheduling is enabled in the Administration Zimlet.
- When manually started either via the Administration Console or the CLI.

Infinite Retention

When the [Data Retention Policy](#) is set to `0`, meaning infinite retention, the Backup Purge immediately exits since no deleted item can exceed an infinite retention time.

Running a Backup Purge

Starting the Backup Purge via the Administration Zimlet

To start a BackupPurge via the Administration Zimlet:

- Click the Backup NG tab (be sure to have a valid license).
- Click the [Run Purge](#) button in the top-right part of the UI.

Starting the Backup Purge via the CLI

To start a BackupPurge via the CLI, use the `doPurge` command:

Syntax:

```
zxsuite backup doPurge [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE
purgeDays(0)	String
backup_path(0)	Path

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup dopurge purgeDays 30 backup_path /opt/zimbra/backup/backup_name
```

Checking the Status of a Running Backup Purge

To check the status of a running Purge via the CLI, use the `monitor` command:

Syntax:

```
zxsuite backup monitor {operation_uuid} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE
operation_uuid(M)	Uiid
operation_host(0)	String

(M) == mandatory parameter, (0) == optional parameter

External Backup

What is the External Backup?

The External Backup is one of the Backup Methods of Backup NG. It creates a snapshot of the mail system, which is ready for migration or Disaster Recovery. Exported data is deduplicated and compressed to optimize disk utilization, transfer times, and I/O rates.

How Does it Work?

The Backup NG engine scans all the data in the Zimbra datastore, saving all the items (deduplicated and compressed) into a folder of your choice.

Folder Permissions

The destination folder must be readable and writable by the **zimbra** user.

To create a valid export directory, run the following commands:

```
mkdir /opt/zimbra/backup/yourdestfolder  
chown -R zimbra:zimbra /opt/zimbra/backup/yourdestfolder
```

Preparing the Migration

To minimize the risk of errors, please perform the following maintenance procedures before migrating:

- Double check Zimbra permissions with the following command (must run as root):
`/opt/zimbra/libexec/zmfixperms --verbose --extended`
- Reindex all mailboxes.
- Check the BLOB consistency with the `zxsuite hsm doCheckBlobs` utility.

Running an External Backup

Via the Administration Zimlet

To start an External Backup via the Administration Zimlet:

- Click the Backup NG tab.
- Click the **Export Backup** button under **Import/Export** to open the Export Backup wizard.
- Enter the Destination Path in the textbox, and press Next. The software checks if the destination folder is empty and whether the 'zimbra' user has R/W permissions.
- Select the domains you want to export, and press Next.
- Verify all your choices in the Operation Summary window. You can also add additional email addresses for notification when the restore operation finishes. Please note that the system sends notifications by default to the Admin account and the user who started the restore procedure.

Via the CLI

To start an External Backup via the CLI, use `doExport` command:

Syntax:

```
zxsuite backup doExport {destination_path} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	DEFAULT
destination_path(M)	Path	
domains(0)	Domain Name[,...]	all
notifications(0)	Email Address[,...]	

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup doexport /opt/zimbra/backup/ domains example.com notifications
john@example.com
Exports a backup of example.com to /opt/zimbra/backup/ and notifies john@example.com
```

Scheduling Script

You can use the NG CLI to schedule External Backup operations. Scheduling is handy; for example, when you need to keep a daily/weekly/monthly backup for corporate or legal reasons.

Restore on New Account

What is the Restore on New Account?

The Restore on New Account procedure allows you to restore the contents and preferences of a mailbox as it was in a moment in time, into a completely new account. The source account is unchanged in any way, so it is possible to recover one or more deleted items in a user's account without actually rolling back the whole mailbox. When you run this kind of restore, you can choose to hide the newly created account from the GAL as a security measure.

How Does it Work?

When a Restore on New Account starts, a new account gets created (the Destination Account), with all the items existing in the source account at the moment selected, including the folder structure and all the user's data. All restored items are created in the current primary store unless you check the **Obey HSM Policy** box.



When restoring data on a new account, shared items consistency is lost, as the original share rules refer to the source account's ID, not to the new (restored) account.

Running a Restore on New Account via the Administration Zimlet

A Restore on New Account can run in two ways.

From the Account List

Running Restore from the **Accounts** tab in the Zimbra Administration Console allows you to operate on users currently existing on the server.

If you need to restore a deleted user, please proceed to Restore via the Administration Zimlet.

- Select **Accounts** in the left pane of the Administration Console to show the Accounts List.
- Browse the list and click the account to restore (Source).
- On the top bar, press the wheel and then the `Restore` button.
- Select **Restore on New Account** as the Restore Mode and enter the name of the new account (Destination) into the text box. You can then choose whether to Hide in GAL the new account or not, then press **Next**.
- Choose the restore date. Day/Month/Year can be selected via a minical, the hour via a drop-down menu and minute and second via two text boxes. Click **Next**.
- Verify all your choice in the Operation Summary window. You can also add additional email addresses for notification when the restore operation finishes. Please note that the system sends notifications by default to the Admin account and the user who started the restore procedure.

Click **Finish** to start the restore.

Running a Restore on New Account via the CLI

To start a Restore on New Account via the CLI, use the `doRestoreOnNewAccount` command:

Syntax:

```
zxsuite backup doRestoreOnNewAccount {source_account} {destination_account}  
{"dd/MM/yyyy HH:mm:ss"}[last] [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
source_account(M)	Account Name	
destination_account(M)	Account Name/ID	
date(M)	Date	'dd/MM/yyyy HH:mm:ss' last
restore_chat_buddies(0)	Boolean	true false
notifications(0)	Email Address[...]	

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup dorestoreonnewaccount John NewJohn '28/09/2012 10:15:10'  
Restores John's account in a new account named NewJohn
```

Undelete Restore

What is Undelete Restore?

Undelete Restore is one of the Restore Modes available in Backup NG. It allows an administrator to restore all items deleted from a mailbox during a given period and put them into a dedicated Zimbra folder inside the mailbox itself.

How Does it Work?

During an Undelete Restore, the Backup NG engine searches the backup datastore for items flagged as **DELETED** and restores them in a dedicated folder in the selected mailbox.



The IMAP **deleted** flag is stripped from restored items so that they are visible for the user in the Zimbra Web Client.

Running an Undelete Restore

Via the Administration Console

- Select **Accounts** in the left pane of the Administration Console to show the Accounts List.
- Browse the list and click the account to restore (Source).
- On the top bar, press the wheel and then the `Restore` button".
- Select **Undelete** as the Restore Mode and press **Next**.
- Choose the restore date-time slot. Day/Month/Year can be selected via a minical, the hour via a drop-down menu and the minute and second via two text boxes. Click **Next**.
- Verify your choices in the Operation Summary window. You can also add additional email addresses for notification when the restore operation finishes. Please note that the system sends notifications by default to the Admin account and the user who started the restore procedure.
- Click **Finish** to start the Restore.

Via the CLI

To start an Undelete Restore operation, use the **doUndelete** command:

Syntax:

```
zxsuite backup doUndelete {account} {"dd/MM/yyyy HH:mm:ss"}|first} {"dd/MM/yyyy  
HH:mm:ss"}|last} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
account(M)	Account Name	
start_date(M)	Date	'dd/MM/yyyy HH:mm:ss' first
end_date(M)	Date	'dd/MM/yyyy HH:mm:ss' last
notifications(0)	Email Address[...]	

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup doun-delete John '08/10/2012 10:15:00' last  
Performs an undelete on John's account of all items created between 08/10/2012  
10:15:00 and the latest data available
```

External Restore

What is the External Restore?

The External Restore is one of the Restore Modes of Backup NG.

How Does it Work?

The External Restore adds to the current Zimbra server all the data, metadata, and configuration data stored on an external backup.

The workflow of the import procedure is as follows:

PHASE1

- "*Operation Started*" notification
- Read Server Backup Data
- Create empty Domains
- Create needed COS (only those effectively used by the imported accounts)
- Create empty DLs
- Create empty Accounts
- Restore all Accounts' attributes
- Restore all Domains' attributes
- Restore all DLs' attributes and share information

- "PHASE1 Feedback" Notification

PHASE2

- Restore all Items

PHASE3

- Restore all Mountpoints and Datasources
- "*Operation Ended*" notification with complete feedback

Before You Start

If Backup NG previously initialized on the destination server, disable the RealTime Scanner to improve both memory usage and I/O performance.

To reduce the I/O overhead and the amount of disk space used for the migration, advanced users may tweak or disable Zimbra's RedoLog for the duration of the import.

To further reduce the amount of disk space used, it's possible to enable compression on your current primary volume before starting the import. If you do not wish to use a compressed primary volume after migration, it's possible to create a new and uncompressed primary volume. Set the new volume to **Current** and the old one to **Secondary**. All of this is supported using the HSM NG module.

Running an External Restore

Via the Administration Zimlet

- Click the Backup NG tab.
- Click the **Import Backup** button under **Import/Export** to open the Import Backup wizard.
- Enter the Destination Path into the text box and press Forward. The software checks if the destination folder contains a valid backup and whether the 'zimbra' user has Read permissions.
- Select the domains you want to import and press Forward.
- Select the accounts you want to import and press Forward.
- Verify all your choices in the Operation Summary window. You can also add additional email addresses for notification when the restore operation finishes. Please note that the system sends notifications by default to the Admin account and the user who started the restore procedure.

Via the CLI

To start an External Restore operation, use the **doExternalRestore** command:

Syntax:

```
zxsuite backup doExternalRestore {source_path} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
source_path(M)	Path		
accounts(0)	Account Name[...]		all
domains(0)	Domain Name[...]		all
filter_deleted(0)	Boolean	true false	true
skip_system_accounts(0)	Boolean	true false	true
skip_aliases(0)	Boolean	true false	false
skip_distribution_lists(0)	Boolean	true false	false
provisioning_only(0)	Boolean	true false	false
skip_coses(0)	Boolean	true false	false
notifications(0)	Email Address		

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup doexternalrestore /opt/zimbra/backup/restorePath/ accounts  
john@example.com,jack@example.com domains example.com filter_deleted false  
skip_system_accounts false
```

Restores the example.com domain, including all system accounts, and the john@example.com and jack@example.com accounts from a backup located in /opt/zimbra/backup/restorePath/

Speeding up the Restore through Multithreading

The **concurrent_accounts** parameter allows you to restore multiple accounts at the same time, thus greatly speeding up the restore process. **This feature is not available via the Administration Console.**



Although resource consumption does not grow linearly with the number of accounts restored at once, it can easily become taxing. Start from a low number of concurrent accounts and raise it according to your server's performance.

Usage example:

```
zxsuite backup doExternalRestore /tmp/external1 domains example0.com,example1.com  
concurrent_accounts 5
```

Restores the example0.com and example1.com domain, excluding system accounts, restoring 5 accounts at the same time from a backup located in /tmp/external1

After the Restore: Message Deduplication

We strongly recommend running volume-wide deduplication with the HSM NG module after an External Restore. The native deduplication system can be ineffective when sequentially importing accounts.

Restore Deleted Account

What is the Restore Deleted Account?

The Restore Deleted Account procedure allows you to restore the contents and preferences of a mailbox into a completely new account, as it was when deleting the said mailbox.

How Does it Work?

When a Restore Deleted Account starts, a new account gets created (the Destination Account), with all the items existing in the source account at the moment of the deletion, including the folder structure and all the user's data. All restored items are created in the current primary store unless you've checked the **Obey HSM Policy** box.



When restoring data on a new account, shared items consistency is lost, as the original share rules refer to the source account's ID, not to the new (restored) account.

From the Backup NG tab

- Select **Backup NG** in the left pane of the Administration Console to show the Backup NG tab.
- On the top bar, push the **Restore Deleted Account** button.
- Choose the restore date. Day/Month/Year can be selected via a minical, the hour via a drop-down menu and the minute and second via two text boxes. Click **Next**.
- Browse the list and click the account to restore (Source).
- Enter the name of the new account (Destination) in the text box. You can then choose whether to Hide in GAL the new account or not then press **Next**.
- Verify all your choices in the Operation Summary window. You can also add additional email addresses for notification when the restore operation finishes. Please note that the system sends notifications by default to the Admin account and the user who started the restore procedure.
- Click **Finish** to start the Restore.

Item Restore

What is the Item Restore?

The Item Restore is one of the Restore Modes of Backup NG.

How Does it Work?

A single item restores from the backup to the owner's account. You may restore any type of item this way.

Running an Item Restore

Via the Administration Zimlet

Item Restore is only available through the CLI.

Via the CLI

To start an Item Restore operation, use the `doItemRestore` command:

Syntax:

```
zxsuite backup doItemRestore {account_name} {item_id} [attr1 value1 [attr2  
value2...]
```

PARAMETER LIST

NAME	TYPE
account_name(M)	Account Name
item_id(M)	Integer
restore_folder(0)	String

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup doitemrestore john@example.com 4784  
Restores item 4784 in the 'john@example.com' mailbox
```

How to Obtain the itemID

The `itemID` is part of the `metadata` of an item, consisting of a unique code that identifies an item in a mailbox.

It resides along with all other metadata in a file inside the `items` directory of the proper account in
`[backup path]/accounts/[accountID]/items/[last 2 digits of itemID]/[itemID]`

e.g.:

Item 2057 of account 4a217bb3-6861-4c9f-80f8-f345ae2897b5, default backup path
`/opt/zimbra/backup/ng/accounts/4a217bb3-6861-4c9f-80f8-f345ae2897b5/items/57/2057`

Metadata storage uses a plain text file, so tools like `grep` and `find` are effective for searching contents. To see the metadata contained in a file in a more readable format, you can use the `zxsuite backup getItem` command:

Syntax:

```
zxsuite backup getItem {account} {item} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
account(M)	Account Name/ID		
item(M)	Integer		
backup_path(0)	Path		/opt/zimbra/backup/ng/
dump_blob(0)	Boolean	true false	false
date(0)	Date	dd/mm/yyyy hh:mm:ss all	last

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup getItem a7300a00-56ec-46c3-9773-c6ef7c4f3636 1
```

Shows item with id = 1 belonging to account a7300a00-56ec-46c3-9773-c6ef7c4f3636

```
zimbra@simone:~$ zxsuite backup getItem
```

command getItem requires more parameters

Syntax:

```
zxsuite backup getItem {account} {item} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
account(M)	Account Name/ID		
item(M)	Integer		
backup_path(0)	Path		/opt/zimbra/backup/ng/
dump_blob(0)	Boolean	true false	false
date(0)	Date	dd/mm/yyyy hh:mm:ss all	last

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup getItem a7300a00-56ec-46c3-9773-c6ef7c4f3636 1
```

Shows item with id = 1 belonging to account a7300a00-56ec-46c3-9773-c6ef7c4f3636

"Real Life" Example

Let's say a user moves one item to the trash:

```
2013-07-18 15:22:01,495 INFO [btppool0-
4361://localhost/service/soap/MsgActionRequest [name=user@domain.com;mid=2538;oip=258.236.789.6
47;ua=zclient/7.2.4_GA_2900;] mailop - moving Message (id=339) to Folder Trash (id=3)
```

and then empties the trash.

```
2013-07-18 15:25:08,962 INFO [btppool0-  
4364://localhost/service/soap/FolderActionRequest] [name=user@domain.com;mid=2538;oip=258.236.7  
89.647;ua=zclient/7.2.4_GA_2900;] mailbox -  
Emptying 9 items from /Trash, removeSubfolders=true.
```

She then calls the Administrator to restore the deleted item. Knowing the itemID and the email address, the Administrator runs the following as the **zimbra** user to restore the missing item:

```
zxsuite backup doItemRestore user@domain.com 339
```

Raw Restore

The "Raw Restore" operation is a DR-type restore operation compatible with both standard and blobless backup. In contrast to similar restore modes such as the External Restore, Raw Restore operates at a lower level to restore all item metadata, thus maintaining the original IDs for all objects restored.

The Raw Restore restores the source server's Centralized Storage configuration. This step ensures that any data stored inside of a Centralized Storage is immediately available. If you are using local or independent third-party volumes, it is easy to move the item BLOBS from the primary storage or to restore those from a backup using the Blob Restore operation.

Differences between External Restore and Raw Restore

External Restore	Raw Restore
Useable on any Zimbra version regardless of the source	Must match the very same Zimbra version and patch level as those on the source server
Does not restore any setting	Restores Centralized Storage settings
Does not support blobless Backup Paths	Is designed for blobless Backup Paths and compatible with standard Backup Paths
Does restore item BLOBS	Does not restore item BLOBS
Restored objects get created anew	Restored objects maintain their original ID

What will be restored

- Centralized Storage configuration and settings
- Domains
- Classes of Service
- Distribution lists
- Mailboxes
- Mailbox preferences
- Item metadata

What will not be restored

- Item Blobs

Running a Raw Restore

The Raw Restore is only available through the **zxsuite** CLI tool:

```
[zimbra@mail ~]$ zxsuite backup doRawRestore
Perform a disaster recovery

Syntax:
  zxsuite backup doRawRestore {source_path} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
source_path(M)	String		
notifications(0)	Email Address[,...]		
skipProvisioning(0)	Boolean	true false	false
deleteWhenConflict(0)	Boolean	true false	false

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup doRawRestore /my/backup/path notifications
user1@example.com,user2@example.com skipProvisioning false deleteWhenConflict false
Performs a Raw Restore without restoring provisioning or deleting a mailbox when ids
are conflicting, and sends notifications to user1@example.com and user2@example.com
The disaster recovery operation does not perform blob restore, use doRestoreBlobs when
needed.
```

Usage scenarios

Restore of a single-server infrastructure

1. Set up a new server (install Zimbra, configure Global and Server settings).
2. Manually create any local or independent 3rd-party volume as it was on the original server.
3. Start a Raw Restore using to restore domains, CoS mailboxes, and item metadata (mailboxes won't be accessible until this step completes).
4. If the source backup was not running in Blobless Mode, run `zxsuite backup doRestoreBlobs` for all volumes to restore item BLOBS.

Loss of a single mailbox node in a multiserver infrastructure

1. Add a new mailbox node to the infrastructure.

2. Manually create any local or independent 3rd-party volume as it was on the original server.
3. Start a Raw Restore using the `skipProvisioning true` parameter to restore item metadata (mailboxes won't be accessible until this step completes).
4. If the source backup was not running in Blobless Mode, run `zxsuite backup doRestoreBlobs` for all volumes to restore item BLOBS.

Loss of multiple mailbox servers in an infrastructure

1. Setup a new empty infrastructure (all servers and roles, setting up Global and Server configuration).
2. Delete default `admin`, `gal`, `ham`, and `spam` accounts.
3. On all mailbox servers, manually create any local or independent 3rd-party volume as it was on the original server.
4. On the first mailbox server, start a Raw Restore using to restore domains, CoS mailboxes, and item metadata (mailboxes won't be accessible until this step completes).
5. On all other mailbox servers, start a Raw Restore using the `skipProvisioning true` parameter to restore item metadata.
6. Once steps 3 and 4 complete, If the source backup was not running in Blobless Mode, run `zxsuite backup doRestoreBlobs` for all volumes on all mailbox servers to restore item BLOBS.

Disaster Recovery

The Disaster

What Can go Wrong

Any of these occurrences serve to classify a problem as a *Disaster*:

- Hardware failure of one or more vital filesystems (such as / or /opt/zimbra/)
- Contents of a vital filesystem made unusable by internal or external factors (like a careless `rm *` or an external intrusion)
- Hardware failure of the physical machine hosting the Zimbra service or of the related virtualization infrastructure
- A critical failure on a software or OS update/upgrade

Minimizing the Chances

Some suggestions to minimize the chances of a disaster:

- Always keep vital filesystems on different drives (namely /, /opt/zimbra/ and your Backup NG path)
- Use a monitoring/alerting tool for your server to become aware of problems as soon as they appear
- Carefully plan your updates and migrations

The Recovery

How to Recover Your System

Consider the recovery of a system divided into 2 steps:

- Base system recovery (OS installation and configuration, Zimbra installation and base configuration)
- Data recovery (reimporting the last available data to the Zimbra server, including domain and user configurations, COS data and mailbox contents)

How can Backup NG Help with Recovery?

The **Import Backup** feature of Backup NG provides an easy and safe way to perform step 2 of recovery.

Using the old server's backup path as the import path allows you to restore a basic installation of Zimbra to the last valid moment of your old server.

Here we've seen just one possible Disaster Recovery scenario: more advanced scenarios and techniques appear in the Zimbra Wiki.

The Recovery Process

- Install Zimbra on a new server and configure the Server and Global settings.
- Install Network NG modules on the new server.
- Mount the backup folder of the old server onto the new one. If this is not available, use the last external backup available or the latest copy of either.
- Begin an External Restore on the new server using the following CLI command:

```
zxsuite backup doExternalRestore /path/to/the/old/store
```

- The External Restore operation creates the domains, accounts and distribution lists, so as soon as the first part of the Restore completes (check your Network NG Modules Notifications), the system is ready for your users. Emails and other mailbox items restore afterward.

Settings and Configs

Server and Global settings are backed up but not restored automatically. Backup NG's high-level integration with Zimbra allows you to restore your data to a server with a different OS/Zimbra Release/Networking/Storage setup without any constraints other than the minimum Zimbra version required to run Network NG Modules.

Whether you wish to create a perfect copy of the old server or just take a cue from the old server's settings to adapt those to a new environment, Backup NG comes with a very handy CLI command: **getServerConfig**.

```
zimbra@test:~$ zxsuite backup getServerConfig  
command getServerConfig requires more parameters
```

Syntax:

```
zxsuite backup getServerConfig {standard|customizations} [attr1 value1 [attr2  
value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
type(M)	Multiple choice	standard customizations	
date(0)	String	'dd/MM/yyyy HH:mm:ss' "last" "all"	
backup_path(0)	Path		
/opt/zimbra/backup/ng/			
file(0)	String	Path to backup file	
query(0)	String	section/id/key	
verbose(0)	String		false
colors(0)	String		false

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup getserverconfig standard date last
```

Display the latest backup data for Server and Global configuration.

```
zxsuite backup getserverconfig standard file /path/to/backup/file
```

Display the contents of a backup file instead of the current server backup.

```
zxsuite backup getserverconfig standard date last query zimlets/com_zimbra_ymemoticons
```

colors true verbose true

```
Displays all settings for the com_zimbra_ymemoticons zimlet, using colored output and  
high verbosity.
```

Specifically, this will display the latest backed up configurations:

```
zxsuite backup getServerConfig standard backup_path /your/backup/path/ date last query  
/ | less
```

You can change the **query** argument to display specific settings, e.g.

```
zimbra@test:~$ zxsuite backup getServerConfig standard date last backup_path  
/opt/zimbra/backup/ng/ query serverConfig/zimbraMailMode/test.domain.com
```

```
config  
date-----  
----- 28/02/2014 04:01:14 CET  
test.domain.com-----  
----- both
```

The {zimbrahome}/conf/ and {zimbrahome}/postfix/conf/ directories are backed up as well:

```
zimbra@test:~$ zxsuite backup getServerConfig customizations date last verbose true  
ATTENTION: These files contain the directories {zimbraHome}/conf/ and  
{zimbraHome}/postfix/conf/ compressed into a single archive.  
Restore can only be performed manually. Do it only if you know what you're  
doing.
```

archives

```
filename  
customizations_28_02_14#04_01_14.tar.gz  
path  
/opt/zimbra/backup/ng/server/  
modify date  
04:01:14 CET 28/02/2014
```

VMs and Snapshots

Thanks to the advent of highly evolved virtualization solutions in the past years, virtual machines are now the most common way to deploy server solutions such as Zimbra Collaboration Suite.

Most hypervisors feature customizable snapshot capabilities and snapshot-based VM backup systems. In case of a disaster, it's always possible to roll back to the latest snapshot and import the missing data using the [External Restore](#) feature of Backup NG - using the server's backup path as the import path.

Disaster Recovery from a Previous VM State

Snapshot-based backup systems allow you to keep a [frozen](#) copy of a VM in a valid state and rollback to it at will. To 100% ensure data consistency, it's better to take snapshot copies of switched off VMs, but this is not mandatory.

When using these kinds of systems, it's vital to make sure that the Backup Path isn't either

part of the snapshot (e.g., by setting the vdisk to `Independent Persistent in VMWare ESX/i) or altered in any way when rolling back, so the missing data is available for import.

To perform a disaster recovery from a previous machine state with Backup NG, you need to:

- Restore the last valid backup into a separate (clone) VM in an isolated network, making sure that users can't access it and that both incoming and outgoing emails are not delivered.
- Switch on the clone and wait for Zimbra to start.
- Disable Backup NG's RealTime Scanner.
- Connect the Virtual Disk containing the untampered Backup Path to the clone and mount it (on a different path).
- Start an External Restore using the Backup Path as the Import Path.

Doing so parses all items in the Backup Path, and import the missing ones, speeding up the disaster recovery. These steps can be repeated as many times as needed as long as you suppress user access and mail traffic.

After the restore completes, make sure that everything is functional and restore user access and mail traffic.

The Aftermath

What Now?

Should you need to restore any content from before the disaster, just initialize a new Backup Path and store the old one.

Unrestorable Items

How can I check if all of my items have been restored?

It's very easy. Check the appropriate **Operation Completed** notification you received as soon as the restore operation finished. The notification is shown in the **Notifications** section of the Administration Zimlet and emailed to the **Notification E-Mail recipient address** you specified in the **Core** section of the Administration Zimlet.

The **skipped items** section contains a per-account list of unrestored items:

```
[...]
- stats -
Restored Items: 15233
Skipped Items: 125
Unrestored Items: 10

- unrestored items -
account: account1@domain.com
unrestored items: 1255,1369

account: account2@domain.com
unrestored items: 49965

account: account14@domain.com
unrestored items: 856,13339,45200, 45655
[...]
```

Skipped Items vs. Unrestored Items

- **Skipped** item: An item previously restored, either during the current restore or in a previous one.
- **Unrestored** item: An item not restored due to an issue in the restore process.

Why have some of my items not been restored?

There are different possible causes, the most common of which are:

- **Read Error:** Either the raw item or the metadata file is not readable due to an I/O exception or a permission issue.
- **Broken item:** Both the raw item and the metadata file are readable by Backup NG, but their content is broken/corrupted.
- **Invalid item:** Both the raw item and the metadata file are readable, and the content is correct, but Zimbra refuses to inject the item.

How Can I Identify Unrestored Items?

There are two ways to do so: via the CLI to search for the item within the backup/import path or via the Zimbra Web Client to view the items in the source server.

Identifying Unrestorable Items through the CLI

The `getItem` CLI command can display an item and the related metadata, extracting all information from a backup path/external backup.

The syntax of the command is:

```
zxsuite backup getItem {account} {item} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
account(M)	Account Name/ID		
item(M)	Integer		
backup_path(0)	Path		/opt/zimbra/backup/ng/
dump_blob(0)	Boolean	true false	false
date(0)	Date	dd/mm/yyyy hh:mm:ss all	last

(M) == mandatory parameter, (0) == optional parameter

To extract the raw data and metadata information of the item whose itemID is 49965 belonging to *account2@domain.com*, also including the full dump of the item's BLOB, the command would be:

```
zxsuite backup getItem account2@domain.com 49965 dump_blob true
```

Identifying Unrestorable Items through the Zimbra WebClient

The comma-separated list of unrestored items displayed in the **Operation Complete** notification can serve as a search argument in the Zimbra Web Client to perform an item search.

To do so:

- Log into the Zimbra Administration Console in the source server.
- Use the **View Mail** feature to access the account containing the unrestored items.
- In the search box, enter **item:** followed by the comma-separated list of itemIDs.

e.g.

item: 856,13339,45200,45655



Remember that any search executes only within its tab, so if you are running the search from the **Email** tab and get no results try to run the same search in the **Address Book**, **Calendar**, **Tasks** and **Briefcase** tabs.

How Can I Restore Unrestored Items?

An item not being restored is a clear sign of an issue, either with the item itself or with your current Zimbra setup. In some cases, there are good chances of being able to restore an item through subsequent attempts.

The following paragraphs contain a collection of tips and tricks that can be helpful when dealing with different kinds of unrestorable items.

Items Not Restored because of a Read Error

Carefully distinguish the read errors that can cause items not to restore:

- **hard** errors: Hardware failures and all other **destructive** errors that cause an unrecoverable data loss.
- **soft** errors: **non-destructive** errors such as wrong permissions, filesystem errors, RAID issues (e.g., broken RAID1 mirroring).

While there is nothing much to do about hard errors, you can prevent or mitigate soft errors by following these guidelines:

- Run a filesystem check.
- If using a RAID disk setup, check the array for possible issues (depending on RAID level).
- Make sure that the 'zimbra' user has r/w access to the backup/import path, all its subfolders, and all thereby contained files.
- Carefully check the link quality of network-shared filesystems. If link quality is poor, consider transferring the data with rsync.
- If using SSHfs to remotely mount the backup/import path, make sure to run the mount command as root using the **-o allow_other** option.

Items Not Restored because Identified as Broken Items

Unfortunately, this is the worst category of unrestored items in terms of **salvageability**.

Based on the degree of corruption of the item, it might be possible to recover either a previous state or the raw object (this is only valid for emails). To identify the degree of corruption, use the **getItem** CLI command:

```
zxsuite backup getItem {account} {item} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
account(M)	Account Name/ID		
item(M)	Integer		
backup_path(0)	Path		/opt/zimbra/backup/ng/
dump_blob(0)	Boolean	true false	false
date(0)	Date	dd/mm/yyyy hh:mm:ss all	last

(M) == mandatory parameter, (0) == optional parameter

Searching for the broken item, setting the **backup_path** parameter to the import path, and the **date** parameter to **all**, displays all valid states for the item.

```

zimbra@test:~$ zxsuite backup getItem admin@example.com 24700 backup_path /mnt/import/
date all
    itemStates
        start_date          12/07/2013
16:35:44
        type                message
        deleted              true
        blob path /mnt/import/items/c0/c0,gUlvzQfE21z6YRXJnNkKL85PrRHw0KMQUqo,p
MmQ=
        start_date          12/07/2013
17:04:33
        type                message
        deleted              true
        blob path /mnt/import/items/c0/c0,gUlvzQfE21z6YRXJnNkKL85PrRHw0KMQUqo,p
MmQ=
        start_date          15/07/2013
10:03:26
        type                message
        deleted              true
        blob path /mnt/import/items/c0/c0,gUlvzQfE21z6YRXJnNkKL85PrRHw0KMQUqo,p
MmQ=

```

If the item is an email, you are able to recover a standard **.eml** file through the following steps:

- Identify the latest valid state

```

/mnt/import/items/c0/c0,gUlvzQfE21z6YRXJnNkKL85PrRHw0KMQUqo,pMmQ=
    start_date          15/07/2013
10:03:26
    type                message
    deleted              true
    blob path /mnt/import/items/c0/c0,gUlvzQfE21z6YRXJnNkKL85PrRHw0KMQUqo,pM
mQ=

```

- Identify the **blob path**

blob path /mnt/import/items/c0/c0,gUlvzQfE21z6YRXJnNkKL85PrRHw0KMQUqo,pMmQ=

- Use gzip to uncompress the BLOB file into an **.eml** file

```

zimbra@test:~$ gunzip -
c /mnt/import/items/c0/c0,gUlvezQfE21z6YRXJnNkKL85PrRHw0KMQUqo,pMmQ= > /tmp/restored.eml

zimbra@test:~$ cat /tmp/restored.eml

Return-Path: zimbra@test.example.com

Received: from test.example.com (LHLO test.example.com) (192.168.1.123)
by test.example.com with LMTP; Fri, 12 Jul 2013 16:35:43 +0200 (CEST)

Received: by test.example.com (Postfix, from userid 1001) id 4F34A120CC4;
Fri, 12 Jul 2013 16:35:43 +0200 (CEST)
To: admin@example.com
From: admin@example.com
Subject: Service mailboxd started on test.example.com
Message-Id: <20130712143543.4F34A120CC4@test.example.com>
Date: Fri, 12 Jul 2013 16:35:43 +0200 (CEST)

Jul 12 16:35:42 test zmconfigd[14198]: Service status change: test.example.com mailboxd changed from stopped to running

```

- Done! You can now import the `.eml` file into the appropriate mailbox using your favorite client.

Items Not Restored because Identified as Invalid Items

An item is identified as **Invalid** when, albeit being formally correct, it is discarded by Zimbra's LMTP Validator upon injection. This behavior is common when importing items created on an older version of Zimbra to a newer one; Validation rules update very often, so some messages considered valid by a certain Zimbra version may not be considered valid by a newer version.

If you experience a lot of unrestored items during an import, momentarily disable the LMTP validator and repeat the import:

- To disable Zimbra's LMTP Validator, run the following command as the Zimbra user:

```
zmlocalconfig -e zimbra_lmtp_validate_messages=false
```

- Once the import completes, you can enable the LMTP validator running

```
zmlocalconfig -e zimbra_lmtp_validate_messages=true
```



This is a **dirty** workaround, as items deemed invalid by the LMTP validator might cause display or mobile synchronization errors. Use it at your own risk.

doCoherencyCheck

What is the Coherency Check?

The [Coherency Check](#) performs a deeper check of a Backup Path than the one done by the SmartScan.

While the SmartScan works [incrementally](#) by only checking items that changed since the last SmartScan, the Coherency Check performs a thorough check of all metadata and BLOBs in the backup path.

The objective is to detect corrupted metadata and BLOBs.

How Does it Work?

The Coherency Check verifies the integrity of all metadata in the backup path and the related BLOBs. Should any errors be found, try running the check with the [fixBackup](#) option to move any orphaned or corrupted metadata/BLOB to a dedicated directory within the backup path.

When Should a Coherency Check be Executed?

- At interval periods to make sure that everything is ok (e.g. every 3 or 6 months).
- After a system crash.
- After the filesystem or storage device containing the backup path experiences any issue.

Should the SmartScan detect a possible item corruption, a Coherency Check starts automatically.



The Coherency Check is highly I/O consuming, so make sure to run it only during off-peak periods

Running a Coherency Check

Starting the Check via the Administration Zimlet

The Coherency Check is not available via the Administration Zimlet.

Starting the Check via the CLI

To start a Coherency Check via the CLI, use the [doCoherencyCheck](#) command:

Syntax:

```
zxsuite backup doCoherencyCheck {backup_path} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
backup_path(M)	Path		
accounts(0)	Account Name/ID[,...]		all
checkZimbra(0)	Boolean	true false	false
fixBackup(0)	Boolean	true false	false
notifications(0)	Email Address[,...]		

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup docoherencycheck /opt/zimbra/backup/ng/ accounts
```

```
jack@exmaple.com,john@exmaple.com
```

Performs a coherency check on /opt/zimbra/backup/ng/ for Jack's and John's accounts

```
zxsuite backup docoherencycheck /opt/zimbra/backup/ng/ fixBackup true
```

Performs a coherency check on /opt/zimbra/backup/ng/ and moves corrupted backup files and blob files not referenced by any metadata out of backup

Checking the Status of a Running Check

To check the status of a running scan via the CLI, use the **monitor** command:

Syntax:

```
zxsuite backup monitor {operation_uuid} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE
operation_uuid(M)	Uiid
operation_host(0)	String

(M) == mandatory parameter, (0) == optional parameter

Taking Additional and Offsite Backups of Backup NG's Datastore

Who Watches the Watchmen?

Having backup systems is a great safety measure against data loss. Still, each backup system must be part of a broader **backup strategy** to ensure the highest possible level of reliability. The lack of a

proper backup strategy gives a false sense of security while turning even the best backup systems in the world into yet another breaking point.

Devising a backup strategy is no easy matter, and at some point, you will most likely face the following question: ***What if I lose the data I backed up?***. The chances of this happening ultimately only depend on how you make and manage your backups. You are more likely lose all of your backed up data if you store both your data and your backups in a single SATAII disk than if you store your backed up data on a dedicated SAN using a RAID 1+0 setup.

Here are some suggestions and best practices to improve your backup strategy by making a backup of the Backup NG's datastore and storing it offsite.

Making an Additional Backup of Backup NG's Datastore

- **Atomicity:** Any transaction is committed and written to the disk only when completed.
- **Consistency:** Any committed transaction is valid, and no invalid transaction is committed and written to the disk.
- **Isolation:** All transactions execute sequentially so that no more than 1 transaction can affect the same item at once.
- **Durability:** A committed transaction remains so even in case of a crash (e.g., power loss or hardware failure).

Due to this, it's very easy to make a backup. The best (and easiest) way to do so is by using `rsync`. Specific options and parameters depend on many factors, such as the amount of data to sync and the storage in use, while connecting to an rsync daemon instead of using a remote shell as a mode of transport is usually much faster in transferring the data.

You can leave both Zimbra and the Real-Time Scanner running, yet make an additional backup of Backup NG's datastore using rsync, and you are always able to stop the sync at any time and reprise it afterward if needed.

Storing Your Backup NG's Datastore Backup Offsite

As seen in the previous section, making a backup of Backup NG's Datastore is very easy, and the use of rsync makes it just as easy to store your backup in a remote location.

We recommend the following best practices to optimize your backup strategy when dealing with this kind of setup:

- If you schedule your rsync backups, make sure that you leave enough time between an rsync instance and the next one for the transfer to complete.
- Use the `--delete` options, so that deleted files in the source server are deleted in the destination server to avoid inconsistencies.
 - If you notice that using the `--delete` option takes too much time, schedule two different rsync instances: one with `--delete` to run after the weekly purge and one without this option.
- Make sure you transfer the whole folder tree recursively starting from Backup NG's Backup

Path, and include server config backups and mapfiles.

- Make sure the destination filesystem is case sensitive (just as Backup NG's Backup Path must be).
- If you plan to restore directly from the remote location, make sure that the *zimbra* user on your server has read and write permissions on the transferred data.
- Expect to experience slowness if your transfer speed is much higher than your storage throughput (or vice versa).

Additional/Offsite Backup F.A.Q.

Q: Why shouldn't I use the [Export Backup](#) feature of Backup NG instead of [rsync](#)?

For many reasons:

- The [Export Backup](#) feature is designed to perform migrations. It exports a [snapshot](#) that is an end in itself with no capacity for incremental management. Each Export Backup run time remains more-or-less constant while using rsync is much more time-efficient.
- Being a Backup NG operation, any other operation started while the Export Backup is running is queued until the Export Backup completes.
- An [Export Backup](#) operation has a higher impact on system resources than an rsync.
- Should you need to stop an Export Backup operation, you won't be able to reprise it, and you'll need to start from scratch.

Q: Can I use this for Disaster Recovery?

Yes. If your Backup Path is still available, it's better to use that, as it restores all items and settings to the last valid state. However, should your Backup Path be lost, you'll be able to use your additional/offsite backup.

Q: Can I use this to restore data back to the server that produced the backup copy?

Yes, but not through the [External Restore](#) operation, since item and folder IDs are the same.

The most appropriate steps to restore data from a copy of the backup path to the very same server are as follows:

- Stop the RealTime Scanner.
- Change the Backup Path to the copy you wish to restore your data from.
- Run either [Restore on New Account](#) or a [Restore Deleted Account](#).
- Once the restore is over, change the backup path to the original one.
- Start the RealTime Scanner. A SmartScan triggers to update the backup data.

Q: Can I use this to create an Active/Standby infrastructure?

No, because the [External Restore](#) operation does not perform any deletions. By running several External Restores, you'll end up filling up your mailboxes with unwanted content, since items

deleted from the original mailbox persist on the **standby** server.

The **External Restore** operation's design ensures that accounts are available for use as soon as the operation starts, so your users are able to send and receive emails even if the restore is running.

Q: Are there any other ways to do an Additional/Offsite backup of my system?

There are for sure, and some of them might even be better than the one described here. These are just guidelines that apply to the majority of cases.

Multistore Information

Backup NG in a Multistore Environment

Command Execution in a Multistore Environment

The new Network Administration Zimlet makes the management of multiple servers very easy. You can select a server from the Backup NG tab and perform all backup operations on that server, even when logged into the Zimbra Administration Console of another server.

Specific differences between SingleStore and MultiStore environments are:

- In a Multistore environment, **Restore on New Account** operations ALWAYS create the new account in the Source account's mailbox server.
- All operations are logged on the target server, not in the server that launched the operation.
- If a target server for an operation is inappropriate, Zimbra automatically proxies the operation request to the correct server.

Backup and Restore

Backup and Restore in a Multistore environment works exactly like in a SingleStore environment.

The different servers are configured and managed separately via the Administration Zimlet, but certain operations like Live Full Scan and Stop All Operations can be 'broadcast' to all the mailstores via the **zxsuite_ CLI** using the **--hostname all_servers** option. Backup NG settings support this, too. (See the CLI wiki page for more details.)

Backup and Restore operations behave as follows:

- Smartscans can be executed on single servers via the Administration Zimlet or on multiple servers via the CLI.
- Restores can start from the **Accounts** tab in the Zimbra Admin Console, from each server tab in the Backup NG menu of the Administration Zimlet and via the CLI. The differences between these methods are:

Operation started from:	Options
Accounts tab	The selected account's restore is automatically started in the proper server.

Operation started from:	Options
Server tab	Any accounts eligible for a restore on the selected server can serve as the restore 'source'.
CLI	Any account on any server can be restored, but there is no automatic server selection.

Export and Import

Export and Import functions are those that differ the most when performed on a Multistore environment.

Here are the basic scenarios.

Export from a Singlestore and Import to a Multistore

Importing multiple accounts of a single domain to a different store breaks the consistency of ALL items shared from/to a mailbox on a different server.

A command in the CLI is available to fix the shares for accounts imported on different servers.

Export from a Multistore and Import to a Single or Multistore

Two different scenarios apply here:

- **Mirror** import: Same number of source and destination mailstores. Each source mailstore import occurs on a different server. This import breaks the consistency of ALL items shared from/to a mailbox on a different server. The `doCheckShares` and `doFixShares` CLI commands are available to check and fix share consistency (see below).
- **Composite** import: Same or different number of source and destination servers. Domains or accounts get manually imported into different servers. This import breaks the consistency of ALL items shared from/to a mailbox on a different server. The `doCheckShares` and `doFixShares` CLI commands are available to check and fix share consistency (see below)

The `doCheckShares` and `doFixShares` Commands

The `doCheckShares` command parses all share information in local accounts and report any error:

```
zimbra@test:~$ zxsuite help backup doCheckShares
```

Syntax:

```
zxsuite backup doCheckShares
```

Usage example:

```
zxsuite backup doCheckShares
Check all shares on local accounts
```

The **doFixShares** fixes all share inconsistencies using a migration.

```
zimbra@test:~$ zxsuite help backup doFixShares
```

Syntax:

```
zxsuite backup doFixShares {import_idmap_file}
```

PARAMETER LIST

NAME	TYPE
import_idmap_file(M)	String

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup doFixShares idmap_file
```

Fixes the shares' consistency after an import according to the mapping contained in the /opt/zimbra/backup/ng/idmap_file

Operation Queue and Queue Management

Backup NG's Operation Queue

Every time a Backup NG operation starts, either manually or through scheduling, it queues in a dedicated, unprioritized FIFO queue. Each operation executes as soon as any preceding operation is dequeued (either because it completes or terminates).

The queue system affects the following operations:

- External backup
- All restore operations
- Smartscan

Changes to Backup NG's configuration are not enqueued and are applied immediately.

Operation Queue Management

Through the Administration Console

Viewing the Queue

To view the operation queue, access the **Notifications** tab in the Administration Zimlet and click the **Operation Queue** button.



The Administration Zimlet displays operations queued both by Backup NG and HSM NG in a single view. No dependency should be inferred by that view, as the two queues are completely separate, in that one Backup NG operation and one HSM NG operation can run at the same time.

Emptying the Queue

To stop the current operation and empty Backup NG's operation queue, enter the [Backup NG](#) tab in the Administration Zimlet and click the [Stop all Operations](#) button.

Through the CLI

Viewing the Queue

To view Backup NG's operation queue, use the [getAllOperations](#) command:

```
zimbra@server:~$ zxsuite help backup getAllOperations
```

Syntax:

```
zxsuite backup getAllOperations [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
verbose(0)	Boolean	true false	false

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup getAllOperations  
Shows all running and queued operations
```

Emptying the Queue

To stop the current operation and empty Backup NG's operation queue, use the [doStopAllOperations](#) command:

```
zimbra@mail:~$ zxsuite help backup doStopAllOperations
```

Syntax:

```
zxsuite backup doStopAllOperations
```

Usage example:

```
zxsuite backup doStopAllOperations
```

Stops all running operations

Removing a Single Operation from the Queue

To stop the current operation or to remove a specific operation from the queue, use the **doStopOperation** command:

```
zimbra@mail:~$ zxsuite help backup doStopOperation
```

Syntax:

```
zxsuite backup doStopOperation {operation_uuid}
```

PARAMETER LIST

NAME	TYPE
operation_uuid(M)	Uiid

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite backup doStopOperation 30ed9eb9-eb28-4ca6-b65e-9940654b8601
```

Stops operation with id = 30ed9eb9-eb28-4ca6-b65e-9940654b8601

COS-level Backup Management

What is COS-level Backup Management?

COS-level Backup Management allows the administrator to disable ALL Backup NG functions for a whole Class of Service to lower storage usage.

How Does COS-level Backup Management Work?

What happens if I disable the Backup NG Module for a Class of Service?

- The Real-Time Scanner ignores all accounts in the COS.
- The Export Backup function DOES NOT EXPORT accounts in the COS.

- The backup system treats accounts in the COS as **Deleted**. After the data retention period expires, all data for such accounts gets purged from the backup store. Re-enabling the backup for a Class of Service resets this.

How is the **backup enabled/backup disabled** information saved?

Disabling the backup for a Class of Service adds the following marker to the Class of Service's **Notes** field: **\${ZxBackup_Disabled}**

While the Notes field remains fully editable and usable, changing or deleting this marker re-enables the backup for the COS.

Incremental Migration with Backup NG

Description

- This guide describes how to perform an Incremental Migration using Backup NG.
- Incremental Migration is specifically designed for the migration of a production environment, minimizing the downtime and aiming to be transparent for the users.
- If correctly planned and executed, your mail system won't suffer any downtime, and the impact on the users is close to zero.



All the CLI commands in this guide must be executed as the **zimbra** user unless otherwise specified.

What Gets Migrated?

- Emails and email folders
- Contacts and address books
- Appointments and calendars
- Tasks and task lists
- Files and briefcases
- Share information
- User preferences
- User settings
- Class of Service settings
- Domain settings

What Will NOT be Migrated?

- Server settings (migrated for reference but not restored)
- Global settings (migrated for reference but not restored)
- Customizations (e.g., Postfix, Jetty.)

- Items moved or deleted during the process are not moved or deleted on the destination server.
- Preferences (e.g., passwords) changed during the process are reset upon each import



Avoid using incremental migration to set up a server-to-server mirroring. Using multiple imports to create a mirrored copy of the source server won't create a **mirrored** copy at all, since the import process performs no deletions.

Pre-Migration Checks

Servers

- Source Server: Any Zimbra server can be the source of your migration, provided that it's running Backup NG or Zimbra Suite Plus.
- Destination Server: Any Zimbra server can be the destination of your migration, provided that it's running Backup NG.

Storage

- On the Source server: Before enabling Backup NG on the source server, make sure you have an amount of free disk space *comparable* to the size of the `/opt/zimbra/store/` folder. Compressing the exported data using the gzip algorithm and deduplicating all Zimbra items typically reduces the exported size to 70% of the original size.
- On the Destination server: Make sure you free space greater than the size of the `/opt/zimbra/store/` and of the `export` folders on the source server combined.

Data Transfer

While you can choose to transfer the data in any other way, rsync is our method of choice because it's a good compromise between speed and convenience.

The main data transfer executes, while the source server is still active and functional. Since the transfer is via the network, carefully plan your transfer so that you'll transfer **all of your data** before migrating.

Alternative Ways to Transfer Your Data

Anything from a remote mount to a physical drive move is ok as long as it suits your needs.

Never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway.

— Andrew S. Tanenbaum(1996), Computer Networks. New Jersey: Prentice-Hall. p. 83. ISBN 0-13-349945-6

DNS

Set the TTL value of your MX record to **300** on your *real* DNS to allow a fast switch between source and destination servers.

The Setup

Step 1: Coherency Checks

To avoid any possible data-related issues, run the following checks on the source server:

- `zxsuite hsm doCheckBlobs` checks the consistency between Zimbra's metadata and BLOBS.
- `zmdbintegrityreport` checks the integrity of the Zimbra database.

Repair any error found.

Running a reindex of all mailboxes is also suggested.

Step 2: Network NG Modules Setup

Disable the Real-Time Scanner on both servers:

```
zxsuite backup setProperty ZxBackup_RealTimeScanner false
```



We strongly recommend a dedicated device for data export for the best performance and least impact on the running system.

Mount any such device on the `/opt/zimbra/backup/` path, and ensure the `zimbra` user has r/w permissions for it.

Step 3: Data Export (SmartScan)

Run a SmartScan on the source server:

```
zxsuite backup doSmartScan
```

All your data is exported to the default backup path (`/opt/zimbra/backup/ng/`).

Pro-Tip: Single Domains Export

You can also choose to only migrate one or more domains instead of all of them. To do so, run the following command **instead** of the SmartScan:

```
zxsuite backup doExport /path/to/export/folder/ domains  
yourdomain.com,yourdomain2.com[...]
```

Mind that if you start with the `SmartScan` method, you'll have to carry on the migration with this method. If you start with the `Single Domains` method, you'll have to carry on the migration with this method. Do not mix the two methods.

Data Export (SmartScan) via the Administration Zimlet

You can also choose to export your data using the Administration Zimlet.

Step 4: Data Synchronization



If Backup NG is used or planned for use on the destination server, ensure the destination folder is not in Backup NG's backup path there, to avoid unnecessary backup activity.

(You can skip this step if you choose to transfer your data by other means than rsync.)

Using `rsync`, copy the data contained in the `/opt/zimbra/backup/ng/` onto a directory in the destination server (make sure the Zimbra user has r/w permissions on the folder). Use a terminal multiplexer like `screen` or `tmux`. This process might need **considerable time** depending on network speed and amount of data involved.

[run this command as Root]

```
rsync -avH /opt/zimbra/backup/ng/ root@desinationserver:/path/for/the/data/
```

Alternate Synchronization Method

While the suggested method is great for high-bandwidth situations, the first synchronization can involve large amounts of data. If the `rsync` method is too slow, you might consider a physical move of the device (or the proper disk file if running on a virtual environment).

After moving the disk, you can remotely mount it back to the source server (e.g., via SSHFS), as the additional synchronizations needed for the migration involves substantially less data. In this case, be sure to remount the device on the source server as `/opt/zimbra/backup/ng/` with all due permissions.

Step 5: First Import

Import all previously exported data to the destination server.

```
zxsuite backup doExternalRestore /path/for/the/data/
```

Network NG imports your data onto the destination server.



Do not edit or delete the backup path after this step.

First Import via the Administration Zimlet

You can also choose to import your data using the Administration Zimlet. While importing via the Administration Zimlet, be sure to remove all system accounts (like GalSync, Ham, Spam, and Quarantine.) from the imported account list.

Step 5 (alternate): First Import for Large Migrations [ADVANCED Users Only]

If you are planning to migrate a very large infrastructure where an export/import lasts for hours or even days, there is an alternative way to handle the migration from this point forward.

Instead of importing all of your data to the destination server, you can run a **Provisioning Only** import that only creates Domains, classes of service, and accounts on the destination server, skipping all mailbox contents.

```
zxsuite backup doExternalRestore /path/for/the/data/ provisioning_only TRUE
```

After doing this, switch the mail flow to the new server. When the switch completes, start the **real** import.

```
zxsuite backup doExternalRestore /path/for/the/data/
```

Your users may now connect to the new server where new emails are delivered while restoring old emails.

This approach has pros and cons.

Pros

- Since items are only imported once and never modified or deleted afterward, using this method results in fewer discrepancies than the **standard** incremental migration.
- This is the option that has less impact on the source server (e.g. good if you are in a hurry to decommission it).

Cons

- Items are restored to users' mailboxes while they work on it. Depending on the scheduling of the operation, this method has a higher impact on your users.
- Since the import uses compute resources on a running system, you might notice some slowdowns.

The Situation so Far

Now the vast majority of the data has already been imported to the destination server. The source server is still active and functional, and you are ready to perform the actual migration.

The Migration

Step 6: Pre-Migration Checks

Before switching the mail flow, **ALWAYS** make sure that the new server is ready to become active (check things like your firewall, your DNS settings, and your security systems.)

Step 7: The Switch

At the end of this step, the destination server is active and functional.

- Repeat step 3, step 4, and step 5 (only new data is exported and synchronized).
- Switch the mail flow to the new server.
- Once NO MORE EMAILS arrive at the source server, repeat step 3, step 4 and step 5.

The Destination server is now active and functional.

Step 8: Post-Migration Checks

Run the following command to check for inconsistencies with shares:

```
zxsuite backup doCheckShares
```

Should this command report any inconsistency, this command parses the import mapfile used as the first argument and fix any broken share:

```
zxsuite backup doFixShares
```

Mapfiles reside in the Backup Path of the destination server as `map_[source_serverID]`.

Step 9: Galsync

Delete any imported GalSync accounts from the Zimbra Administration Console. Then, if needed, create new GalSync accounts on all the imported domains and resync all the GalSync accounts with the following command:

```
zmgsutil forceSync -a galsync.randomstring@domain.com -n [resourcename]
```

Step 10: Message Deduplication

Running a Volume Deduplication using the HSM NG module is highly suggested after a migration.

What Now?

- Initialize Backup NG on the new server to make sure all of your data is safe.

Incremental Migration FAQ

Q: Do I need a valid license to perform an incremental migration?

Yes. It can be either a trial license or a purchased one.

Q: What gets migrated?

Everything except the server configuration is migrated, including:

- User data
- User preferences
- Classes of Service configurations
- Domain configurations

Q: Will I lose my shares? Will I need to re-configure all my shares?

Not at all!

Q: How should I transfer the exported data between my servers?

Again, anything that suits your needs is ok. You just need to be very sure about what your **needs** are.

Do you need to move the data very fast? Physically moving a USB disk between your servers might not be a good idea.

Do you need to move the data in a very reliable way? Mounting the export folder via SSHFS to the destination server might not be a good idea if your internet connection is sloppy.

Mobile NG

Enable Mobile NG Synchronization for a COS

By enabling Mobile NG for all users in a Class of Service, you authorize all users in that COS to use all the mobile functions of Mobile NG.

How to Enable Mobile NG for all Users in a Class Of Service

From the Administration Console

To enable Mobile NG for all users in a COS from the Administration Console:

- Open the Zimbra Administration Console.
- Double-click the Class Of Service you want to edit (on the left, under Configuration → Class of Service).
- Click the Mobile tab.
- Check the `Enable mobile synchronization` button.

From the Zimbra CLI

To enable Mobile NG for all users in a COS from the CLI:

- As the 'zimbra' user run: `zmprov mc COSName zimbraFeatureMobileSyncEnabled TRUE`

How to Disable Mobile NG for all Users in a Class Of Service

From the Administration Console

To disable Mobile NG for all users in a COS from the Administration Console:

- Open the Zimbra Administration Console.
- Double-click the Class Of Service you want to edit (on the left, under Configuration → Class of Service).
- Click the Mobile tab and uncheck the `Enable mobile synchronization` button.

From the Zimbra CLI

To disable Mobile NG for all users in a COS from the CLI:

- As the 'zimbra' user run: `zmprov mc COSName zimbraFeatureMobileSyncEnabled FALSE`

Note about Settings Hierarchy

COS-level settings are overridden by user-level settings.

Enable Mobile NG for a Single User

By enabling the Mobile NG Module for a single user you authorize a single user to use all the mobile functions of the Mobile NG Module.

How to Enable Mobile NG for a Single User

From the Zimbra Administration Console

To enable Mobile NG for a single user from the Administration Console:

- Open the Zimbra Administration Console.
- Double-click the user you want to edit (on the left, under Manage → Accounts).
- Click the Mobile tab.
- Check `Enable mobile synchronization`.

From the Zimbra CLI

To enable Mobile NG for a single user from the CLI:

- As the 'zimbra' user run: `zmprov ma user@domain.tld zimbraFeatureMobileSyncEnabled TRUE`

How to Disable Mobile NG for a Single User

From the Zimbra Administration Console

To disable Mobile NG for a single user from the CLI:

- Open the Zimbra Administration Console.
- Double-click the user you want to edit (on the left, under Manage → Accounts).
- Click the Mobile NG tab and uncheck `Enable mobile synchronization`.

From the Zimbra CLI

To disable Mobile NG for a single user from the CLI:

- As the 'zimbra' user run: `zmprov ma user@domain.tld zimbraFeatureMobileSyncEnabled FALSE`

Note about Settings Hierarchy

User-level settings override COS-level settings.

The Mobile Password Feature

Mobile Passwords and You

The **Mobile Password** feature allows Global and Delegated Admins to set an additional password for an account to be used for Exchange ActiveSync authentications only.

The main benefits of using this feature are:

- Enforce **set-and-forget** safe passwords, regardless of any other password policy, so that you won't need to change the password saved on all mobile devices synchronized with an account should this account's Zimbra password change.
- Avoid the **real** password to be disclosed in case of unauthorized access to the device/client.

A **Mobile Password** will not be valid for Webmail/POP3/IMAP/SMTP logins, and the account password will not be valid for mobile logins.

How to Set a Mobile Password for a Mailbox

Setting a mobile password is easy:

- Open the Zimbra Administration Console.
- Right-click the user for which you want to set a Mobile Password and select **Edit**.
- In the **Mobile** tab within the user's settings, check the **Enable mobile password** checkbox.
- Enter the desired password in the **Mobile password** field and enter it again in the 'Confirm mobile password' field. You can also choose to generate a random mobile password by clicking the 'Generate random password' button.
- Save.

Mobile Device Management a.k.a. Mobile Provisioning

What is Mobile Device Management?

Mobile Device Management (MDM - also known as provisioning) allows an administrator to define a set of rules and security settings that are applied Over The Air to one or more mobile devices, ranging from PIN policies to Allowed/Blocked app lists and including **one time** commands, such as the remote wipe of the entire device.

MDM effectively allows administrators to limit and restrict the use of corporate mobile devices to avoid risky or improper behaviors.

MDM is also a priceless aid for **Bring Your Own Device** corporate policies, allowing users to connect their personal mobile devices to the corporate servers, while reducing the risk of security breaches to a minimum.

Provisioning Features Available on Your Client

Not all provisioning features are available on all clients.

Network NG and MDM

Network NG features advanced MDM features through the Exchange ActiveSync protocol version 14+.

Mobile policies can be enabled at COS and mailbox levels, allowing both a quick **one for many** setup and user-based customized management. In both cases, Mobile Management Options are available in the **Mobile** tab.

Provisioning Options

The following provisioning options are available:

- Enable Mobile Device Management: Enable or disable the use of mobile policies for the current user/COS.
- Allow non-provisionable devices: Allow the user to synchronize any device that does not support provisioning.
- Allow partial policy enforcement on device: Allow the user to synchronize any device that does not support one or more applicable policies.



By default, MDM is disabled in NG MobileSync. To enable navigate to Network Modules NG → Mobile → Advanced Settings and check the “Enable Mobile Device Management” option

Enforceable Policies

Enforceable Policies are available right below the **Mobile Devices** list, grouped in the following categories:

- Sync Settings: Set synchronization spans and limits.
- Device Settings: Enable or disable device features such as camera, WiFi, removable storage or Bluetooth.
- Device Security Settings: Force an unlock code and define the minimum requirements for the code itself.
- Device Applications: Enable or disable **standard** device applications such as the Browser and POP/IMAP client or unsigned apps.

Two lists are also available for application whitelist/blacklist management:

- Approved Applications: A customizable list of approved applications.
- Blocked Applications: A customizable list of blocked applications that won't be usable on the device.

Mobile Password

While conceptually similar, the mobile password feature is not part of Mobile Device Management and can be used with any version of the EAS protocol.

SyncStates

Mobile NG and the SyncState

The SyncState (short for Synchronization Status) is a set of information kept on the server about the synchronization with a mobile device. Each time a device establishes a connection with Mobile NG, the following steps take place:

- 1. The device requests a folderSync operation to synchronize the local Folders with the ones on the server.

One SyncKey per local folder is sent (or a single SyncKey set to '0' if this is the first connection between the device and the server)

- 2. The server replies with a list of available folders.

One SyncKey per folder is sent by the server.

- 3. Then, the device requests an itemSync operation to synchronize all due items.

The server stores the items synchronized in the SyncState.

- 4. After completing the itemSync operation, the device sends a 'ping' command to keep the connection alive.

Step 4 is repeated as long as no changes happen to the synchronized account.

Every time a new item is stored on the mailbox or an old item is modified, the server notifies the availability to the device, which closes the active connection (the one kept alive by the ping command) and repeats steps 3 and 4.

The SyncState is the combination of the SyncKeys saved on step 2 and the itemIds saved on step 3. It's saved by the server per the userId/deviceId unique pair.

Sync Request

The Sync Request is the actual synchronization process, started by either Mobile NG or by the client. During a sync request, any change in the mailbox that happened since the last request is synchronized to the device and vice versa.

A sync request is issued when:

- The SyncState changes.
- A sync is forced client-side.
- The current *ping* expires and a new one is sent by the device (the keepalive duration is defined by the client).

Managing the SyncStates

Via the Administration Zimlet

Mobile NG provides two options in the Administration Zimlet to manage the SyncStates of synchronized mobile devices:

- Reset Device: Resets the device's SyncState for a single account, forcing a full re-synchronization the next time the device connects to the server.
- Wipe Device: Removes all the device's SyncState and history from the server. Useful when a mobile device is not used anymore or is assigned to a different employee in the same company.

Via the CLI

To manage the SyncStates of synchronized mobile devices via the CLI, use one of the following commands:

The doRemoveDevice command

Syntax:

```
zxsuite mobile doRemoveDevice {account} {device_id}
```

PARAMETER LIST

NAME	TYPE
account(M)	Account Name
device_id(M)	String

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite mobile doRemoveDevice john@example.com Appl79032X2WA4S
Removes John's Appl79032X2WA4S device SyncState
```

The doResetAccount command

Syntax:

```
zxsuite mobile doResetAccount {account}
```

PARAMETER LIST

NAME	TYPE
account(M)	Account Name

(M) == mandatory parameter, (O) == optional parameter

Usage example:

```
zxsuite mobile doResetAccount john@example.com
```

Resets all the device states for John's account

The doResetDevice command**Syntax:**

```
zxsuite mobile doResetDevice {account} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	DEFAULT
account(M)	Account Name	
device_id(O)	String	all

(M) == mandatory parameter, (O) == optional parameter

Usage example:

```
zxsuite mobile doResetDevice john@example.com Appl79032X2WA4S
```

Resets John's Appl79032X2WA4S device SyncState

Advanced Settings

Mobile NG Performance Tuning

Mobile NG provides three useful options to fine-tune Mobile NG according to system performance.

Performance Tuning Settings

Available Settings

- Notifications Latency (ZxMobile_NotificationsLatency): The seconds of delay between an event on the server and its notification to the mobile device.
- Use Instant Notifications (ZxMobile_UseInstantNotifications): Enable/Disable instant notifications. Overrides Notifications Latency if true.

- Max Ping Heartbeat (ZxMobile_MaxPingHeartbeat): Maximum interval between 'ping' commands.

All settings can be edited in the Administration Zimlet or via CLI using the `setProperty` command.

When to Edit the Performance Tuning Settings

Default settings should be optimal for most situations. If you experience one or more of the problems below, please apply the proper solution.

Problem	Solution
High system load	Disable instant notifications
High system load after disabling instant notifications	Raise notification latency
Mobile users experience high network usage	Disable instant notifications and tweak notifications latency
Devices can connect but sessions are interrupted frequently	Adjust Max Ping Heartbeat according to your network configuration
Items are synchronized from server-to-device with an excessive delay	Lower notification latency or enable instant notifications

Shared Folders

Shared Folders and You (and Your Mobile)

With Network NG, it's possible to synchronize folders that are not owned by the user itself to mobile devices. This applies to all item types available through the Exchange ActiveSync protocol, so you'll be able to sync any shared email folder, address book, calendar or task list to mobile devices.

Specific features available on mobile devices might differ, based on the client in use.



Not all clients support the synchronization of multiple address books, calendars or task lists via Exchange ActiveSync.

How to Sync a Shared Folder to Your Mobile Devices

To allow a higher level of control over synchronization, users are allowed to choose which shared folders are to be synchronized with their mobile devices.

Enable Mobile Synchronization for a Folder

To enable mobile synchronization for a shared folder:

- Log in to the Zimbra Web Client.
- Right-click the shared folder you want to sync.

- Select **Folder Sync Settings** in the drop-down menu.
- Check the **Enable synchronization for this folder** checkbox.
- Press OK.

The new folder will be synchronized to any mobile device connected to the account.

Restrictions

The following restrictions apply to shared folder synchronization:

- It's not possible to sync a mountpoint referring to a full account share.
- It's not possible to sync a subfolder of a shared folder, as doing so would return an incomplete folder tree.
- It's not possible to sync a read-only share, as the Exchange ActiveSync protocol does not envision the concept of a **read-only** resource. Synchronizing a read-only folder will cause severe inconsistencies between the client and the server, along with many errors.

EAS Filters

In the EAS protocol, the protocol version used for the synchronization is defined during the initial handshake and never changed. The server presents a list of all available protocol versions and the client chooses one among that list.

EAS filters are a way to limit the EAS version available to a subset of users or clients to ensure that the proper version is used.

Multiple EAS filters can be set up and will be evaluated in sequential order (see the `getAllEASFilters` and `doMoveEASFilter` commands below).

Anatomy of an EAS Filter

An EAS filter is composed of 5 parts:

- **Type**: Defines the type of filter rule.
- **Parameter**: The filtering identifier (e.g. device brand or email address).
- **Mode**: Defines whether the software will limit the available versions or provide a fixed list.
- **easversions** field: Contains the protocol versions enforced by the filter.
- **Blocking** boolean value: Defines whether other filters are executed once the current one is successfully matched.

Managing EAS Filters

EAS filters are managed through the CLI using the following four dedicated commands.

zxsuite mobile getAllEASFilters

This command lists all existing filters.

Sample Output:

```
filters

    ID          0
    mode        fixed
    rule        [type =
or; rules = [[type = contains; rule = outlook/] OR [type = contains; rule =
microsoft.outlook]]
    easversions 14.0
    blocking    true

    ID          1
    mode        limit
    rule        [type =
contains; rule = samsung]
    easversions 2.5
    blocking    false

    ID          2
    mode        limit
    rule        [type =
always]
    easversions 14.1
    blocking    false
```

zxsuite mobile doAddEASFilter

This command adds a new EAS filter.

```
zxsuite mobile doAddEASFilter
```

Syntax:

```
zxsuite mobile doAddEASFilter {and|or|regex|contains|account}  
{text|people@example.com|account=example@ff.com,contains=android}  
{add|subtract|fixed|limit} {easversions} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
type(M)	Multiple choice	and or regex contains account
parameter(M)	String	text people@example.com account=example@ff.com,contains=android
mode(M)	Multiple choice	add subtract fixed limit
easversions(M)	String[...]	
blocking(0)	Boolean	true false

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite mobile doAddEASFilter contains android fixed 2.5,12.0,14.1  
Adds a protocol filter that will restrict the pool of available EAS versions to 2.5,  
12.0 and 14.1 if the user agent name  
contains the string 'android'.
```

```
zxsuite mobile doAddEASFilter and account=user@example.com,contains=android fixed 14.1  
blocking true  
Adds a protocol filter that will restrict the pool of available EAS versions to 14.1  
if the user agent name  
contains the string 'android' only for user@example.com. No more EAS filters will be  
evaluated after this one due to the 'blocking' directive.
```

zxsuite mobile doDeleteEASFilter

This command deletes an existing EAS Filter.

```
zxsuite mobile doDeleteEASFilter  
command doDeleteEASFilter requires more parameters
```

Syntax:

```
zxsuite mobile doDeleteEASFilter {id}
```

PARAMETER LIST

NAME	TYPE
id(M)	Integer

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite mobile doDeleteEASFilter 2  
Removes the filter with id = 2.  
To show a list of the filters, use the  
    zxsuite mobile getAllEASFilters  
command.
```

zxsuite mobile doMoveEASFilter

This command is used to move EAS filters to a different position in the filter queue.

```
zxsuite mobile doMoveEASFilter  
command doMoveEASFilter requires more parameters
```

Syntax:

```
zxsuite mobile doMoveEASFilter {from} {to}
```

PARAMETER LIST

NAME	TYPE
from(M)	Integer
to(M)	Integer

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite mobile doMoveEASFilter 0 5  
Moves the filter with id = 0 to the position 5.  
To show a list of the filters, use the  
    zxsuite mobile getAllEASFilters  
command.
```

Mobile Account Loggers

Mobile account loggers are dedicated loggers that can output the entirety of a user's EAS logs into a dedicated logfile, with a different verbosity than the one of the `sync.log`. This allows for quicker troubleshooting.

When creating an account logger, the following parameters must be specified:

- The target `account`.
- The `log_level` (verbosity) of the log.
- The dedicated `log_file`.
- The `window_size` to enforce on all devices synchronizing with the account while the logger is running.



Account loggers are removed automatically when the mailboxd is stopped or restarted and do not usually survive a mailboxd crash. Log files won't be affected.

Account Logger Management

Account loggers can only be managed via the CLI through the following commands:

`zxsuite mobile doAddAccountLogger`

```
zxsuite mobile doAddAccountLogger  
command doAddAccountLogger requires more parameters
```

Syntax:

```
zxsuite mobile doAddAccountLogger {account} {debug|info|warn|err|crit} {log_file}  
[attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
account(M)	Account Name	
log_level(M)	Multiple choice	debug info warn err crit
log_file(M)	Path	
window_size(0)	Integer	a value > 0

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite mobile doaddaccountlogger john@example.com info /tmp/john_logger  
Creates an info account logger for john's account to file /tmp/john_logger
```

```
zxsuite mobile doaddaccountlogger john@example.com info /tmp/john_logger window_size 1  
Creates an info account logger for john's account to file /tmp/john_logger with window  
size set to 1.
```

zxsuite mobile doRemoveLogger

```
zxsuite mobile doRemoveLogger  
command doRemoveLogger requires more parameters
```

Syntax:

```
zxsuite mobile doRemoveLogger {logger_id|"all_loggers"}
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
logger_id(M)	Multiple choice	logger_id "all_loggers"

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite mobile doremovelogger 5  
Removes the account logger with ID = 5
```

zxsuite mobile getAccountLoggers

Sample output:

```
zxsuite mobile getAccountLoggers

loggers

    id          7
    level       DEBUG
    name

AccountLogger
    description      Logging
account user@domain.com using level debug, log file /tmp/user.log
    remove command   zxsuite
mobile doRemoveLogger 7
```

HSM NG

Hierarchical Storage Management

The Hierarchical Storage Management Technique

HSM is a data storage technique that moves data between different stores according to a defined policy.

The most common use of the HSM technique is the move of *older* data from a faster-but-expensive storage device to a slower-but-cheaper one based on the following premises:

- Fast storage costs more.
- Slow storage costs less.
- *Old* data will be accessed much less frequently than *new* data.

The advantages of the HSM technique are clear: Lowering the overall storage cost since only a small part of your data needs to be on costly storage, and improving the overall user experience.

Stores, Volumes and Policies

Using HSM requires a clear understanding of some related terms:

- Primary Store: The *fast-but-expensive* store where all your data is initially placed.
- Secondary Store: The *slow-but-cheap* store where *older* data will be moved to.

Zimbra Stores

The Basics: Types of Stores and Their Uses

Zimbra allows for **two** different types of stores:

- **Index Store:** A store that contains information about your data that is used by Apache Lucene to provide indexing and search functions.
- **Data Store:** A store that contains all your Zimbra data organized in a MySql database.

You can have multiple stores of each type, but only one Index Store, one Primary Data Store and one Secondary Data Store can be set as *Current* (meaning that is currently used by Zimbra).

Primary and Secondary Data Stores

A data store in Zimbra can be either a Primary Data Store or a Secondary Data Store.

Data is moved between the *current* Primary Data Store and the *current* Secondary Data Store according to a defined policy.

HSM NG: Moving Items between Stores

The main feature of the HSM NG module is the ability to apply defined HSM policies.

The move can be triggered in three ways:

- Click the *Apply Policy* button in the Administration Zimlet.
- Start the `doMoveBlobs` operation through the CLI.
- Enable Policy Application Scheduling in the Administration Zimlet and wait for it to start automatically.

Once the move is started, the following operations are performed:

- HSM NG scans through the Primary Store to see which items comply with the defined policy.
- All the Blobs of the items found in the first step are copied to the Secondary Store.
- The database entries related to the copied items are updated to reflect the move.
- If the second and the third steps are completed successfully (and only in this case), the old Blobs are deleted from the Primary Store.

The Move operation is *stateful* - each step is executed only if the previous step has been completed successfully - so the risk of data loss during a Move operation is nonexistent.

doMoveBlobs

The doMoveBlobs Operation of HSM NG

The `doMoveBlobs` is the heart of HSM NG.

It moves items between the Current Primary Store and the Current Secondary Store according to the proper HSM policy.

The move is performed by a transactional algorithm. Should an error occur during one of the steps of the operation, a rollback takes place and no change will be made to the data.

Once HSM NG identifies the items to be moved, the following steps are performed:

- A copy of the Blob to the Current Secondary Store is created.
- The Zimbra Database is updated to notify Zimbra of the item's new position.
- The original Blob is deleted from the Current Primary Store.

What is Moved?

Every item that complies with the specified HSM policy is moved.

Example:

The following policy

```
message,document:before:-20day  
message:before:-10day has:attachment
```

will move all emails and documents older than 20 days along with all emails older than 10 days that contain an attachment.

Policy Order

All conditions for a policy are executed in the exact order they are specified. HSM NG will loop on all items in the Current Primary Store and apply each separate condition before starting the next one.

This means that the following policies

```
message,document:before:-20day  
message:before:-10day has:attachment
```

```
message:before:-10day has:attachment  
message,document:before:-20day
```

applied daily on a sample server that sends/receives a total of 1000 emails per day, 100 of which contain one or more attachments, will have the same final result. However, the execution time of the second policy will probably be slightly higher (or much higher, depending on the number and size of the emails on the server).

This is because in the first policy, the first condition (message,document:before:-20day) will loop on all items and move many of them to the Current Secondary Store, leaving fewer items for the second condition to loop on.

Likewise, having the `message:before:-10day has:attachment` as the first condition will leave more items for the second condition to loop on.

This is just an example and does not apply to all cases, but gives an idea of the need to carefully plan your HSM policy.

Executing the `doMoveBlobs` Operation (a.k.a. Applying the HSM Policy)

Applying a policy means running the `doMoveBlobs` operation in order to move items between the Primary and Secondary store according to the defined policy.

HSM NG gives you three different options:

- Via the Administration Zimlet
- Via the CLI
- Through Scheduling

Apply the HSM Policy via the Administration Zimlet

To apply the HSM Policy via the Administration Zimlet:

- Log into the Zimbra Administration Console.
- Click the *HSM NG* entry in the Administration Zimlet.
- Click the *Apply Policy* button.

Apply the HSM Policy via the CLI

To apply the HSM Policy via the CLI, run the following command as the *zimbra* user:

```
` zxsuite hsm doMoveBlobs`
```

Apply the HSM Policy through Scheduling

To schedule a daily execution of the *doMoveBlobs* operation:

- Log into the Zimbra Administration Console.
- Click the *HSM NG* entry in the Administration Zimlet.
- Enable scheduling by selecting the *Enable HSM Session scheduling:* button.
- Select the hour to run the operation under *HSM Session scheduled for:*.

doMoveBlobs Stats and Info

Information about disk space savings, operation performances and more are available by clicking the *Stats* button under the *Secondary Volumes* list in the HSM NG tab of the Administration Zimlet.

Volume Management

Both primary and secondary volumes can be created on either local storage or on supported third-party storage solutions.

Zimbra Volumes

A volume is a distinct entity (path) on a filesystem with all the associated properties that contain Zimbra Blobs.

Volume Properties

All Zimbra volumes are defined by the following properties:

- Name: A unique identifier for the volume.
- Path: The path where the data is going to be saved.



The *zimbra* user must have r/w permissions on this path.

- Compression: Enable or Disable the file compression for the volume.

- Compression Threshold: The minimum file size that will trigger the compression. 'Files under this size will never be compressed even if the compression is enabled.'
- Current: A *Current* volume is a volume where data will be written upon arrival (Primary Current) or HSM policy application (Secondary Current).

Volume Management with HSM NG - Administration Zimlet

Creating a New Volume with the Administration Zimlet

To create a new volume from the HSM NG tab of the Administration Zimlet:

- Click the appropriate *Add* option in the *Volumes Management* section according to the type of volume you want to create.
- Select the store type, choosing between local mount point or S3 Bucket.
- Enter the new volume's name.
- Enter a path for the new volume.
- Check the *Enable Compression* button if you wish to activate data compression on the new volume.
- Select the Compression Threshold.
- If you are using an S3 Bucket, it's possible to store information for multiple buckets.
- Press *OK* to create the new volume. Should the operation fail, a notification containing any related errors will be generated.

Editing a Volume with the Administration Zimlet

To edit a volume from the Administration Zimlet, simply select an existing volume and press the appropriate *Edit* button.

Deleting a Volume with the Administration Zimlet

To delete a volume from the Administration Zimlet, select an existing volume and press the appropriate *Delete* button. Remember that only **empty** volumes can be deleted.

Volume Management with HSM NG - From the CLI



Beginning with release 8.8.9, all volume creation and update commands have been updated, as the `storeType` argument is now required.

The `storeType` argument is **mandatory**, it is always the on the first position and accepts any one value corresponding to the [S3-Compatible Services](#) listed previously. The arguments that follow in the command now depend on the selected `storeType`.

FileBlob (Local)

Updated `zxsuite` syntax to create new FileBlob zimbra volume:

```

# Add volume, run as zimbra user
zxsuite hsm doCreateVolume FileBlob name secondary /path/to/store
# Delete volume
zxsuite hsm doDeleteVolume name
# set current
zxsuite hsm doUpdateVolume FileBlob name current_volume true

```

`zxsuite hsm doCreateVolume FileBlob`

Syntax:

```

zxsuite hsm doCreateVolume FileBlob {volume_name} {primary|secondary|index}
{volume_path} [attr1 value1 [attr2 value2...]]

```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
DEFAULT		
volume_name(M)	String	
volume_type(M)	Multiple choice	primary secondary index
volume_path(M)	Path	
volume_compressed(0)	Boolean	true false
compression_threshold_bytes(0)	Long	false 4096

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```

zxsuite hsm doCreateVolume FileBlob volumeName secondary /path/to/store
volume_compressed true compression_threshold_bytes 4096

```

`zxsuite hsm doUpdateVolume FileBlob`

Syntax:

```
zxsuite hsm doUpdateVolume FileBlob {current_volume_name} [attr1 value1 [attr2  
value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
DEFAULT		
current_volume_name(M)	String	
volume_type(0)	String	primary secondary index
volume_name(0)	String	
volume_path(0)	Path	
current_volume(0)	Boolean	true false
volume_compressed(0)	String	
compression_threshold(0)	String	

(M) == mandatory parameter, (0) == optional parameter

S3 (Amazon and any S3-compatible solution not explicitly supported)

```
# Add volume, run as zimbra user
zxsuite hsm doCreateVolume S3 name secondary bucket_name bucket access_key accessKey
secret secretString region EU_WEST_1
# Delete volume
zxsuite hsm doDeleteVolume name
# set current
zxsuite hsm doUpdateVolume S3 name current_volume true
```

zxsuite hsm doCreateVolume S3

Syntax:

```
zxsuite hsm doCreateVolume S3 {Name of the zimbra store} {primary|secondary}  
[attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
volume_name(M)	String	Name of the zimbra store
volume_type(M)	Multiple choice	primary secondary
bucket_name(0)	String	Amazon AWS bucket
access_key(0)	String	Service username
secret(0)	String	Service password
server_prefix(0) all objects keys	String	Prefix to the server id used in
bucket_configuration_id(0) service credentials	String	UUID for already existing S3 (zxsuite config global get)
attribute s3BucketConfigurations)		
region(0)	String	Amazon AWS Region
url(0) s3api.service.com)	String	S3 API compatible service url (ex:
prefix(0)	String	Prefix added to blobs keys
use_infrequent_access(0)	Boolean	true false
infrequent_access_threshold(0)	String	

(M) == mandatory parameter, (0) == optional parameter

Usage example:

S3 AWS Bucket:

```
zxsuite hsm doCreateVolume S3 volumeName primary bucket_name bucket access_key  
accessKey secret secretKey prefix objectKeysPrefix region EU_WEST_1  
user_infrequent_access TRUE infrequent_access_threshold 4096
```

S3 compatible object storage:

```
zxsuite hsm doCreateVolume S3 volumeName primary bucket_name bucket access_key  
accessKey secret secretKey url http://host/service
```

Using existing bucket configuration:

```
zxsuite hsm doCreateVolume S3 volumeName primary bucket_configuration_id 316813fb-  
d3ef-4775-b5c8-f7d236fc629c
```

zxsuite hsm doUpdateVolume S3

Syntax:

```
zxsuite hsm doUpdateVolume S3 {current_volume_name} [attr1 value1 [attr2  
value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
current_volume_name(M)	String	
volume_name(0)	String	
volume_type(0)	String	primary secondary
server_prefix(0)	String	Prefix to the server id used in all objects keys
bucket_configuration_id(0)	String	UUID for already existing service credentials
attribute s3BucketConfigurations)		(zxsuite config global get
use_infrequent_access(0)	Boolean	true false
infrequent_access_threshold(0)	String	
current_volume(0)	Boolean	true false

(M) == mandatory parameter, (0) == optional parameter

Scality (S3 compatible object storage)

```
# Add volume, run as zimbra user
zxsuite hsm doCreateVolume ScalityS3 name secondary bucket_name mybucket access_key
accessKey1 secret verySecretKey1 url http://{IP_ADDRESS}:{PORT}
# Delete volume
zxsuite hsm doDeleteVolume name
# set current
zxsuite hsm doUpdateVolume ScalityS3 name current_volume true
```

zxsuite hsm doCreateVolume ScalityS3

Syntax:

```
zxsuite hsm doCreateVolume ScalityS3 {volume_name} {primary|secondary} [attr1  
value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
volume_name(M)	String	
volume_type(M)	Multiple choice	primary secondary
bucket_name(0)	String	Bucket name
url(0)	String	S3 API compatible service url (ex: s3api.service.com)
access_key(0)	String	Service username
secret(0)	String	Service password
server_prefix(0) all objects keys	String	Prefix to the server id used in
bucket_configuration_id(0) credentials	String	UUID for already existing service (zxsuite config global get attribute s3BucketConfigurations)
prefix(0)	String	Prefix added to blobs keys

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite hsm doCreateVolume ScalityS3 volumeName primary bucket_name bucket url  
http://host/service access_key accessKey secret secretKey  
zxsuite hsm doCreateVolume ScalityS3 volumeName primary bucket_configuration_id uuid
```

zxsuite hsm doUpdateVolume ScalityS3

Syntax:

```
zxsuite hsm doUpdateVolume ScalityS3 {current_volume_name} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
current_volume_name(M)	String	
volume_name(0)	String	
volume_type(0)	String	primary secondary
server_prefix(0)	String	Prefix to the server id used in all objects keys
bucket_configuration_id(0)	String	UUID for already existing S3 service credentials
attribute s3BucketConfigurations		(zxsuite config global get
current_volume(0)	Boolean	true false
		false

(M) == mandatory parameter, (0) == optional parameter

EMC (S3 compatible object storage)

```
# Add volume, run as zimbra user
zxsuite hsm doCreateVolume EMC name secondary bucket_name bucket access_key ACCESSKEY
secret SECRET url https://url.of.storage
# Delete volume
zxsuite hsm doDeleteVolume name
# set current
zxsuite hsm doUpdateVolume EMC name current_volume true
```

zxsuite hsm doCreateVolume EMC

Syntax:

```
zxsuite hsm doCreateVolume EMC {volume_name} {primary|secondary} [attr1 value1  
[attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
volume_name(M)	String	
volume_type(M)	Multiple choice	primary secondary
bucket_name(0)	String	Bucket name
url(0)	String	S3 API compatible service url (ex: s3api.service.com)
access_key(0)	String	Service username
secret(0)	String	Service password
server_prefix(0) all objects keys	String	Prefix to the server id used in
bucket_configuration_id(0) credentials	String	UUID for already existing service (zxsuite config global get attribute s3BucketConfigurations)
prefix(0)	String	Prefix added to blobs keys

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite hsm doCreateVolume EMC volumeName primary bucket_name bucket url  
http://host/service access_key accessKey secret secretKey  
zxsuite hsm doCreateVolume EMC volumeName primary bucket_configuration_id uuid
```

zxsuite hsm doUpdateVolume EMC

Syntax:

```
zxsuite hsm doUpdateVolume EMC {current_volume_name} [attr1 value1 [attr2  
value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
current_volume_name(M)	String	
volume_name(0)	String	
volume_type(0)	String	primary secondary
server_prefix(0)	String	Prefix to the server id used in all objects keys
bucket_configuration_id(0)	String	UUID for already existing service credentials
attribute s3BucketConfigurations)		(zxsuite config global get
current_volume(0)	Boolean	true false
		false

(M) == mandatory parameter, (0) == optional parameter

OpenIO

```
# add volume, run as zimbra user  
zxsuite hsm doCreateVolume OpenIO name secondary http://{IP_ADDRESS} ZeXtras OPENIO  
# Delete volume  
zxsuite hsm doDeleteVolume name  
# set current  
zxsuite hsm doUpdateVolume OpenIO name current_volume true
```

zxsuite hsm doCreateVolume OpenIO

Syntax:

```
zxsuite hsm doCreateVolume OpenIO {volume_name} {primary|secondary} {url}  
{account} {namespace} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
volume_name(M)	String	
volume_type(M)	Multiple choice	primary secondary
url(M)	String	
account(M)	String	
namespace(M)	String	
proxy_port(0)	Integer	
account_port(0)	Integer	

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite hsm doCreateVolume OpenIO volumeName primary http://host/service
```

accountName namespaceString proxy_port 6006 account_port 6009

Syntax:

```
zxsuite hsm doUpdateVolume OpenIO {current_volume_name} [attr1 value1  
[attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
DEFAULT		
current_volume_name(M)	String	
volume_name(0)	String	
volume_type(0)	String	primary secondary
url(0)	String	
account(0)	String	
namespace(0)	String	
proxy_port(0)	Integer	
account_port(0)	Integer	
current_volume(0)	Boolean	true false
		false

(M) == mandatory parameter, (0) == optional parameter

Swift

```

# add volume, run as zimbra user
zxsuite hsm doCreateVolume Swift name secondary http://{IP_ADDRESS}:8080/auth/v1.0/
user:username password maxDeleteObjectsCount 100
# Delete volume
zxsuite hsm doDeleteVolume name
# set current
zxsuite hsm doUpdateVolume Swift name current_volume true

```

zxsuite hsm doCreateVolume Swift

Syntax:

```

zxsuite hsm doCreateVolume Swift {volume_name} {primary|secondary} {url}
{username} {password} [attr1 value1 [attr2 value2...]]

```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
volume_name(0)	String		
volume_type(0)	String	primary secondary	
url(0)	String		
username(0)	String		
password(0)	String		
maxDeleteObjectsCount(0)	Integer	Number of object in a single bulk delete request	500

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```

zxsuite hsm doCreateVolume Swift volumeName primary http://host/service accountName
password max_delete_objects_count 100

```

zxsuite hsm doUpdateVolume Swift

Syntax:

```
zxsuite hsm doUpdateVolume Swift {current_volume_name} [attr1 value1 [attr2  
value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
current_volume_name(M)	String		
volume_name(0)	String		
volume_type(0)	String	primary secondary	
url(0)	String		
username(0)	String		
password(0)	String		
maxDeleteObjectsCount(0)	Integer	Number of object in a single bulk delete request	
			500
current_volume(0)	Boolean	true false	false

(M) == mandatory parameter, (0) == optional parameter

Cloudian (S3 compatible object storage)

```
# add volume, run as zimbra user
zxsuite hsm doCreateVolume Cloudian name secondary bucket_name bucket access_key
ACCESSKEY secret SECRET url https://url.of.storage
# Delete volume
zxsuite hsm doDeleteVolume name
# set current
zxsuite hsm doUpdateVolume Cloudian name current_volume true
```

zxsuite hsm doCreateVolume Cloudian

Syntax:

```
zxsuite hsm doCreateVolume Cloudian {volume_name} {primary|secondary} [attr1  
value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
volume_name(M)	String	
volume_type(M)	Multiple choice	primary secondary
bucket_name(0)	String	Bucket name
url(0)	String	S3 API compatible service url (ex: s3api.service.com)
access_key(0)	String	Service username
secret(0)	String	Service password
server_prefix(0) all objects keys	String	Prefix to the server id used in
bucket_configuration_id(0) credentials	String	UUID for already existing service (zxsuite config global get attribute s3BucketConfigurations)
prefix(0)	String	Prefix added to blobs keys

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite hsm doCreateVolume Cloudian volumeName primary bucket_name bucket url  
http://host/service access_key accessKey secret secretKet  
zxsuite hsm doCreateVolume Cloudian volumeName primary bucket_configuration_id uuid
```

zxsuite hsm doUpdateVolume Cloudian

Syntax:

```
zxsuite hsm doUpdateVolume Cloudian {current_volume_name} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
DEFAULT		
current_volume_name(M)	String	
volume_name(0)	String	
volume_type(0)	String	primary secondary
server_prefix(0) all objects keys	String	Prefix to the server id used in
bucket_configuration_id(0) credentials	String	UUID for already existing service (zxsuite config global get)
attribute s3BucketConfigurations		
current_volume(0)	Boolean	true false
		false

(M) == mandatory parameter, (0) == optional parameter

Volume Deletion

`zxsuite hsm doDeleteVolume`

Syntax:

```
zxsuite hsm doDeleteVolume {volume_name}
```

PARAMETER LIST

NAME	TYPE
volume_name(M)	String

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite hsm dodeletevolume hsm
Deletes volume with name hsm
```

Move all data from a volume to another

Syntax:

```
zxsuite hsm doVolumeToVolumeMove {source_volume_name} {destination_volume_name}
```

PARAMETER LIST

NAME	TYPE
source_volume_name(M)	String
destination_volume_name(M)	String

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite hsm doVolumeToVolumeMove sourceVolume destVolume  
Moves the whole contents of sourceVolume to destVolume
```

Centralized Storage

The Centralized Storage feature allows to use an S3 bucket to host data coming from multiple servers at the same time sharing the same directory structure, as opposed to "independent" volumes which are self-contained and whose directory structure is strictly related to the server and volume itself.

This allows for better data management in large multistore environments and greatly improves mailbox move speed.

Enabling Centralized Storage

1. Create the centralized volume on any one of your servers using the `zxsuite hsm doCreateVolume` command.
 1. All volume types except for FileBlob are compatible;
 2. Make sure to add the centralized TRUE flag to set the volume as a Centralized Storage;
 3. The full syntax for the command depends on the storage type;
2. Once the Centralized Volume has been created, use the `zxsuite doCreateVolume Centralized` command on all other mailbox servers to copy the Centralized Volume's configuration from the first server and add it to the volume list.
 1. The full syntax for the command is `zxsuite hsm doCreateVolume Centralized {server_name} {volume_name}`

Centralized Storage Structure

Storage Structure Data is stored in a Centralized Volume plainly, as the main directory of the volume contains a single empty directory for each server connected to the volume and a directory for each mailbox stored in it at the very same level.

In the following example, servers 3aa2d376-1c59-4b5a-94f6-101602fa69c6 and 595a4409-6aa1-413f-

9f45-3ef0f1e560f5 are both connected to the same Centralized volume, where 3 mailboxes are stored. As you can see, the effective server where the mailboxes are hosted is irrelevant to the storage.

```
- 3aa2d376-1c59-4b5a-94f6-101602fa69c6/
|- 595a4409-6aa1-413f-9f45-3ef0f1e560f5/
|- ff46e039-28e3-4343-9d66-92adc60e60c9/
\-
|-- 357-104.msg
|-- 368-115.msg
|-- 369-116.msg
|-- 373-120.msg
|-- 374-121.msg
|-- 375-122.msg
|-- 376-123.msg
|-- 383-130.msg
|- 4c022592-f67d-439c-9ff9-e3d48a8c801b/
\-
|-- 315-63.msg
|-- 339-87.msg
|-- 857-607.msg
|-- 858-608.msg
|-- 859-609.msg
|-- 861-611.msg
|-- 862-612.msg
|-- 863-613.msg
|-- 864-614.msg
|-- 865-615.msg
|-- 866-616.msg
|-- 867-617.msg
|-- 868-618.msg
|- dafdf5569-4114-4268-9201-14f4a895a3d5/
\-
|-- 357-104.msg
|-- 368-115.msg
|-- 369-116.msg
|-- 373-120.msg
|-- 374-121.msg
|-- 375-122.msg
|-- 376-123.msg
|-- 383-130.msg
|-- 384-131.msg
```

Policy Management

What is a Policy?

An HSM policy is a set of rules that define what items will be moved from the Primary Store to the Secondary Store when the `doMoveBlobs` operation of HSM NG is triggered, either manually or by scheduling.

A policy can consist of a single rule that is valid for all item types (*Simple* policy) or multiple rules valid for one or more item types (*Composite* policy). Also, an additional *sub-rule* can be defined using Zimbra's [search syntax](#).

Policy Examples

Here are some policy examples. To see how to create the policies in the HSM NG module, see below.

- *Move all items older than 30 days*
- *Move emails older than 15 days and items of all other kinds older than 30 days*
- *Move calendar items older than 15 days, briefcase items older than 20 days and all emails in the "Archive" folder*

Defining a Policy

Policies can be defined both from the HSM NG tab of the Administration Zimlet and from the CLI. You can specify a Zimbra Search in both cases.

From the Administration Zimlet

To define a policy from the Administration Zimlet:

- Log into the Zimbra Administration Console.
- Click *HSM NG* on the Administration Zimlet.
- Click the *Add* button in the Storage Management Policy section.
- Select the Item Types from the `Items to Move:` list.
- Enter the Item Age from the `Move Items older than:` box.
- **OPTIONAL:** Add a Zimbra Search in the *Additional Options* box.
- You can add multiple *lines* to narrow down your policy. Every *line* will be evaluated and executed after the line before has been applied.

From the CLI

Two policy management commands are available in the CLI:

- `setHsmPolicy`
- `+setHsmPolicy`

```
zxsuite hsm setHsmPolicy {policy}
```

This command resets the current policy and creates a new one as specified by the *policy* parameter.

The *policy* parameter must be specified in the following syntax

```
itemType1[, itemType2, itemtype3, etc]:query
```

```
zxsuite hsm +setHsmPolicy {policy}
```

This command adds the query specified by the *policy* parameter to the current HSM Policy.

The *policy* parameter must be specified in the following syntax

```
itemType1[, itemType2, itemtype3, etc]:query
```

Volumes on Amazon S3 Compatible Services

HSM NG and S3 buckets

Primary and Secondary volumes created with HSM NG can be hosted on S3 buckets, effectively moving the largest part of your data to secure and durable cloud storage.

S3-compatible Services

While any storage service compatible with the Amazon S3 API should work out of the box with HSM NG, listed here are the only officially supported platforms:

- FileBlob (standard local volume)
- Amazon S3
- EMC
- OpenIO
- Swift
- Scality S3
- Cloudian
- Custom S3 (any unsupported S3-compliant solution)

Primary Volumes and the "Incoming" directory

In order to create a remote *Primary Store* on a mailbox server a local "Incoming" directory must exist on that server. The default directory is `/opt/zimbra/incoming`, but you can check or modify the current value using these commands:

```
zxsuite config server get $(zmhostname) attribute incomingPath  
zxsuite config server set $(zmhostname) attribute incomingPath value /path/to/dir
```

Local Cache

Storing a volume on third-party remote storage solutions requires a local directory to be used for item caching, which must be readable and writable by the *zimbra* user.

The local directory must be created manually and its path must be entered in the *HSM NG* section of the Administration Zimlet in the Zimbra Administration Console.

If the Local Cache directory is not set, you won't be able to create any secondary volume on an S3-compatible device or service.



Failing to correctly configure the cache directory will cause items to be unretrievable, meaning that users will get a **No such BLOB** error when trying to access any item stored on an S3 volume.

Local Volumes

Local Volumes (i.e. FileBlob type) can be hosted on any mountpoint on the system regardless of the mountpoint's destination and are defined by the following properties:

- **Name:** A unique identifier for the volume.
- **Path:** The path where the data is going to be saved. The *zimbra* user must have r/w permissions on this path.
- **Compression:** Enable or Disable file compression for the volume.
- **Compression Threshold:** the minimum file size that will trigger the compression.



Files under this size will never be compressed even if compression is enabled.

Current Volumes

A *Current Volume* is a volume where data will be written upon arrival (Primary Current) or HSM Policy Application (Secondary Current). Volumes not set as Current won't be written upon except by specific manual operations such as the Volume-to-Volume move.

Bucket Setup

HSM NG doesn't need any dedicated setting or configuration on the S3 side, so setting up a bucket for your volumes is easy. Although creating a dedicated user bucket and access policy are not required, they are strongly suggested because they make it much easier to manage.

All you need to start storing your secondary volumes on S3 is:

- An S3 bucket. You need to know the bucket's name and region in order to use it.
- A user's Access Key and Secret.
- A policy that grants the user full rights on your bucket.

Bucket Management

A centralized Bucket Management UI is available in the Zimbra Administration Console. This facilitates saving bucket information to be reused when creating a new volume on an S3-compatible storage instead of entering the information each time.

To access the Bucket Management UI:

- Access the Zimbra Administration Console
- Select the "Configure" entry on the left menu
- Select the "Global Settings" entry
- Select the S3 Buckets entry

Any bucket added to the system will be available when creating a new volume of the following type: Amazon S3, Cloudian, EMC, Scality S3, Custom S3.

Bucket paths and naming

Files are stored in a bucket according to a well-defined path, which can be customized at will in order to make your bucket's contents easier to understand even on multi-server environments with multiple secondary volumes:

`/Bucket Name/Destination Path/[Volume Prefix-]serverID/`

- The **Bucket Name** and **Destination Path** are not tied to the volume itself, and there can be as many volumes under the same destination path as you wish.
- The **Volume Prefix**, on the other hand, is specific to each volume and it's a quick way to differentiate and recognize different volumes within the bucket.

Creating Volumes with HSM NG

To create a new volume with HSM NG from the Zimbra Administration Console:

- Enter the HSM Section of the NG Administration Zimlet in the Zimbra Administration Console
- Click on *Add* under either the *Primary Volumes* or *Secondary Volumes* list
- Select the Volume Type among the available storage choices
- Enter the required volume information



Each volume type will require different information to be set up, please refer to your storage provider's online resources to obtain those details.

Editing Volumes with HSM NG

To edit a volume with HSM NG from the Zimbra Administration Console:

- Enter the HSM Section of the NG Administration Zimlet in the Zimbra Administration Console
- Select a volume
- Click on *Edit*
- When done, click *Save*

Deleting Volumes with HSM NG

To delete a volume with HSM NG from the Zimbra Administration Console:

- Enter the HSM Section of the NG Administration Zimlet in the Zimbra Administration Console
- Select a volume
- Click on *Delete*



Only empty volumes can be deleted.

Amazon S3 Tips

Bucket

Storing your secondary Zimbra volumes on Amazon S3 doesn't have any specific bucket requirements, but we suggest that you create a dedicated bucket and disable Static Website Hosting for easier management.

User

To obtain an Access Key and the related Secret, a [Programmatic Access](#) user is needed. We suggest that you create a dedicated user in Amazon's IAM Service for easier management.

Rights Management

In Amazon's IAM, you can set access policies for your users. It's mandatory that the user of your Access Key and Secret has a set of appropriate rights both on the bucket itself and on its contents. For easier management, we recommend granting full rights as shown in the following example:

```
{  
  'Version': '[LATEST API VERSION]',  
  'Statement': [  
    {  
      'Sid': '[AUTOMATICALLY GENERATED]',  
      'Effect': 'Allow',  
      'Action': [  
        's3:*'  
      ],  
      'Resource': [  
        '[BUCKET ARN]/*',  
        '[BUCKET ARN]'  
      ]  
    }  
  ]  
}
```



This is not a valid configuration policy. Don't copy and paste it into your user's settings as it won't be validated.

If you only wish to grant minimal permissions, change the **Action** section to:

```
"Action": [  
    's3:PutObject',  
    's3:GetObject',  
    's3:DeleteObject',  
    's3:AbortMultipartUpload'  
,
```

The bucket's ARN is expressed according to Amazon's standard naming format: **arn:partition:service:region:account-id:resource**. For more information about this topic, please see Amazon's documentation.

Bucket Paths and Naming

Files are stored in a bucket according to a well-defined path, which can be customized at will to make your bucket's contents easier to understand (even on multi-server environments with multiple secondary volumes):

/Bucket Name/Destination Path/serverID/

The **Bucket Name** and **Destination Path** are not tied to the volume itself, and there can be as many volumes under the same destination path as you wish.

The **Volume Prefix**, on the other hand, is specific to each volume and it's a quick way to differentiate and recognize different volumes within the bucket.

Infrequent Access Storage Class

HSM NG is compatible with the [Amazon S3 Standard - Infrequent access](#) storage class and will set any file larger than the **Infrequent Access Threshold** value to this storage class as long as the option has been enabled on the volume.

For more information about Infrequent Access, please refer to the [official Amazon S3 Documentation](#).

Intelligent Tiering Storage Class

HSM NG is compatible with the [Amazon S3 - Intelligent Tiering](#) storage class and will set the appropriate Intelligent Tiering flag on all files, as long as the option has been enabled on the volume.

For more information about Intelligent Tiering, please refer to the [official Amazon S3 Documentation](#).

Item Deduplication

What is Item Deduplication

Item deduplication is a technique that allows you to save disk space by storing a single copy of an item and referencing it multiple times instead of storing multiple copies of the same item and referencing each copy only once.

This might seem like a minor improvement. However, in practical use, it makes a significant difference.

Item Deduplication in Zimbra

Item deduplication is performed by Zimbra at the moment of storing a new item in the Current Primary Volume.

When a new item is being created, its **message ID** is compared to a list of cached items. If there is a match, a hard link to the cached message's BLOB is created instead of a whole new BLOB for the message.

The dedupe cache is managed in Zimbra through the following config attributes:

zimbraPrefDedupeMessagesSentToSelf

Used to set the deduplication behavior for sent-to-self messages.

```
<attr id="144" name="zimbraPrefDedupeMessagesSentToSelf" type="enum" value="dedupeNone,secondCopyIfOnToOrCC,dedupeAll" cardinality="single" optionalIn="account,cos" flags="accountInherited, domainAdminModifiable">
  <defaultCOSValue>dedupeNone</defaultCOSValue>
  <desc>dedupeNone|secondCopyIfOnToOrCC|moveSentMessageToInbox|dedupeAll</desc>
</attr>
```

zimbraMessageIdDedupeCacheSize

Number of cached Message IDs.

```
<attr id="334" name="zimbraMessageIdDedupeCacheSize" type="integer" cardinality="single" optionalIn="globalConfig" min="0">
  <globalConfigValue>3000</globalConfigValue>
  <desc>
    Number of Message-Id header values to keep in the LMTP dedupe cache.
    Subsequent attempts to deliver a message with a matching Message-Id to the same mailbox will be ignored. A value of 0 disables deduping.
  </desc>
</attr>
```

zimbraPrefMessageIdDedupingEnabled

Manage deduplication at account or COS-level.

```
<attr id="1198" name="zimbraPrefMessageIdDedupingEnabled" type="boolean"
cardinality="single" optionalIn="account,cos" flags="accountInherited"
since="8.0.0">
  <defaultCOSValue>TRUE</defaultCOSValue>
  <desc>
    Account-level switch that enables message deduping. See
zimbraMessageIdDedupeCacheSize for more details.
  </desc>
</attr>
```

zimbraMessageIdDedupeCacheTimeout

Timeout for each entry in the dedupe cache.

```
<attr id="1340" name="zimbraMessageIdDedupeCacheTimeout" type="duration"
cardinality="single" optionalIn="globalConfig" since="7.1.4">
  <globalConfigValue>0</globalConfigValue>
  <desc>
    Timeout for a Message-Id entry in the LMTP dedupe cache. A value of 0 indicates no
timeout.
    zimbraMessageIdDedupeCacheSize limit is ignored when this is set to a non-zero
value.
  </desc>
</attr>
```

(older Zimbra versions might use different attributes or lack some of them)

Item Deduplication and HSM NG

The HSM NG features a **doDeduplicate** operation that parses a target volume to find and deduplicate any duplicated item.

Doing so you will save even more disk space, as while Zimbra's automatic deduplication is bound to a limited cache, HSM NG's deduplication will also find and take care of multiple copies of the same email regardless of any cache or timing.

Running the **doDeduplicate** operation is also highly suggested after a migration or a large data import in order to optimize your storage usage.

Running a Volume Deduplication

Via the Administration Zimlet

To run a volume deduplication via the Administration Zimlet, simply click on the *HSM NG* tab, select the volume you wish to deduplicate and press the *Deduplicate* button.

Via the CLI

To run a volume deduplication through the CLI, use the `doDeduplicate` command:

```
zimbra@mailserver:~$ zxsuite hsm doDeduplicate
```

```
command doDeduplicate requires more parameters
```

Syntax:

```
zxsuite hsm doDeduplicate {volume_name} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
volume_name(M)	String[...]		
dry_run(O)	Boolean	true false	false

(M) == mandatory parameter, (O) == optional parameter

Usage example:

```
zxsuite hsm dodeduplicate secondvolume  
Starts a deduplication on volume secondvolume
```

To list all available volumes, you can use the `zxsuite hsm getAllVolumes` command.

doDeduplicate Stats

The `doDeduplicate` operation is a valid target for the `monitor` command, meaning that you can watch the command's statistics while it's running through the `zxsuite hsm monitor [operationID]` command.

Sample Output

```
Current Pass (Digest Prefix): 63/64  
Checked Mailboxes: 148/148  
Deduplicated/duplicated Blobs: 64868/137089  
Already Deduplicated Blobs: 71178  
Skipped Blobs: 0  
Invalid Digests: 0  
Total Space Saved: 21.88 GB
```

- *Current Pass (Digest Prefix)*: The `doDeduplicate` command will analyze the BLOBS in groups based on the first character of their digest (name).
- *Checked Mailboxes*: The number of mailboxes analyzed for the current pass.
- *Deduplicated/duplicated Blobs*: Number of BLOBS deduplicated by the current operation / Number of total duplicated items on the volume.

- *Already Deduplicated Blobs*: Number of deduplicated blobs on the volume (duplicated blobs that have been deduplicated by a previous run).
- *Skipped Blobs*: BLOBs that have not been analyzed, usually because of a read error or missing file.
- *Invalid Digests*: BLOBs with a bad digest (name different from the actual digest of the file).
- *Total Space Saved*: Amount of disk space freed by the doDeduplicate operation.

Looking at the sample output above we can see that:

- The operation is running the second to last pass on the last mailbox.
- 137089 duplicated BLOBs have been found, 71178 of which have already been deduplicated previously.
- The current operation deduplicated 64868 BLOBs, for a total disk space saving of 21.88GB.

Advanced Volume Operations

HSM NG: More than Meets the Eye

At first sight, HSM NG seems to be strictly dedicated to HSM. However, it also features some highly useful volume-related tools that are not directly related to HSM.

Due to the implicit risks in volume management, these tools are only available through the CLI.

Volume Operations at a Glance

The following volume operations are available:

doCheckBlobs: Perform BLOB coherency checks on one or more volumes.

doDeduplicate: Start Item Deduplication on a volume.

doVolumeToVolumeMove: Move all items from one volume to another.

getVolumeStats: Display information about a volume's size and number of thereby contained items/blobs.

Volume Operation Analysis

doCheckBlobs

Usage

```
zimbra@mail:~$ zxsuite hsm doCheckBlobs
```

command doCheckBlobs requires more parameters

Syntax:

```
zxsuite hsm doCheckBlobs {start} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
action(M)	String	start	
volume_ids(0)	Integer[,...]	1,3	
mailbox_ids(0)	Integer[,...]	2,9,27	
missing_blobs_crosscheck(0)	Boolean	true false	true
traced(0)	Boolean	true false	false

(M) == mandatory parameter, (0) == optional parameter

Usage example:

Usage examples:

`zxsuite hsm doCheckBlobs start`: Perform a BLOB coherency check on all message volumes.

`zxsuite hsm doCheckBlobs start volume_ids 1,3`: Perform a BLOB coherency check on volumes 1 and 3.

`zxsuite hsm doCheckBlobs start mailbox_ids 2,9,27`: Perform a BLOB coherency check on mailboxes 2,9 and 27.

`zxsuite hsm doCheckBlobs start missing_blobs_crosscheck false`: Perform a BLOB coherency check without checking on other volumes.

`zxsuite hsm doCheckBlobs start traced true`: Perform a BLOB coherency check, logging even the correct checked items.

Description and Tips

The doCheckBlobs operation can be used to run BLOB coherency checks on volumes and mailboxes. This can be useful when experiencing issues related to broken or unviewable items, which are often caused because either Zimbra cannot find or access the BLOB file related to an item or there is an issue with the BLOB content itself.

Specifically, the following checks are made:

- DB-to-BLOB coherency: For every Item entry in Zimbra's DB, check whether the appropriate BLOB file exists.
- BLOB-to-DB coherency: For every BLOB file in a volume/mailbox, check whether the appropriate DB data exists.
- Filename coherency: Checks the coherency of each BLOB's filename with its content (as BLOBS

are named after their file's SHA hash).

- Size coherency: For every BLOB file in a volume/mailbox, checks whether the BLOB file's size is coherent with the expected size (stored in the DB).



The old `zmblobchk` command is deprecated and replaced by `zxsuite hsm doCheckBlobs` on all infrastructures using HSM NG module.

doDeduplicate

Usage

```
zimbra@mail:~$ zxsuite hsm doDeduplicate
command doDeduplicate requires more parameters
```

Syntax:

```
zxsuite hsm doDeduplicate {volume_name} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
volume_name(M)	String[...]		
dry_run(O)	Boolean	true false	false

(M) == mandatory parameter, (O) == optional parameter

Usage example:

```
zxsuite hsm dodeduplicate secondvolume
Starts a deduplication on volume secondvolume
```

doVolumeToVolumeMove

Usage

```
zimbra@mail:~$ zxsuite hsm doVolumeToVolumeMove  
command doVolumeToVolumeMove requires more parameters
```

Syntax:

```
zxsuite hsm doVolumeToVolumeMove {source_volume_name} {destination_volume_name}
```

PARAMETER LIST

NAME	TYPE
source_volume_name(M)	String
destination_volume_name(M)	String

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite hsm doVolumeToVolumeMove sourceVolume destVolume  
Moves the whole sourceVolume to destVolume
```

Description and Tips

This command can prove highly useful in all situations where you need to stop using a volume, such as:

- Decommissioning old hardware: If you want to get rid of an old disk in a physical server, create new volumes on other/newer disks and move your data there.
- Fixing *little mistakes*: If you accidentally create a new volume in the wrong place, move the data to another volume.
- Centralize volumes: Centralize and move volumes as you please, for example, if you redesigned your storage infrastructure or you are tidying up your Zimbra volumes.

getVolumeStats

Usage

```
zimbra@mail:~$ zxsuite hsm getVolumeStats
```

command getVolumeStats requires more parameters

Syntax:

```
zxsuite hsm getVolumeStats {volume_id} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
volume_id(M)	Integer		
show_volume_size(0)	Boolean	true false	false
show_blob_num(0)	Boolean	true false	false

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
**BE CAREFUL** show_volume_size and show_blob_num options are IO intensive and thus disabled by default
```

```
zxsuite hsm getVolumeStats 2  
Shows stats for the volume with ID equal to 2
```

Description and Tips

This command provides the following information about a volume:

name	description
id	The ID of the volume
name	The Name of the volume
path	The Path of the volume
compressed	Compression enabled/disabled
threshold	Compression threshold (in bytes)
lastMoveOutcome	Exit status of the latest doMoveBlobs operation
lastMoveTimestamp	End timestamp of the latest doMoveBlobs operation
lastMoveDuration	Duration of the last doMoveBlobs operation
lastItemMovedCount	Number of items moved to the current secondary volume during the latest doMoveBlobs operation
bytesSaved	Total amount of disk space freed up thanks to deduplication and compression

name	description
bytesSavedLast	Amount of disk space freed up thanks to deduplication and compression during the latest doMoveBlobs operation

The `show_volume_size` and `show_blob_num` options will add the following data to the output:

option	name	description
show_volume_size	totSize	Total disk space used up by the volume
show_blob_num	blobNumber	Number of BLOB files in the volume

Moving Mailboxes Between Mailstores

The `doMailboxMove` command allows you to move a single mailbox or all accounts from a given domain, from one mailbox server to another within the same Zimbra infrastructure.



If the HSM NG module is installed and enabled, this command replaces the old `zmmboxmove` and `zmmailboxmove` commands. Using any of the legacy commands will return an error and won't move any data.

Syntax

Syntax:

```
zxsuite hsm doMailboxMove {an account name: john@example.com or a domain name:  
example.com} {destinationHost} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
destinationHost(M)	String	
accounts(0)	String[,...]	john@example.com,smith@example.com[,...]
domains(0)	String[,...]	example.com,test.com[,...]
input_file(0)	String	
stages(0)	String[,...]	blobs backup data account
data=blobs+backup[,...]	blobs,backup,account	
compress(0)	Boolean	true false
true		
checkDigest(0)	Boolean	if false skip digest calculation and check
true		
overwrite(0)	Boolean	true false
false		
threads(0)	Integer	
1		
hsm(0)	Boolean	true false
true		
notifications(0)	Email Address	
ignore_partial(0)	Boolean	true false
false		
drop_network_backup(0)	Boolean	true false
false		
read_error_threshold(0)	Integer	

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite HSM NG domailboxmove john@example.com mail2.example.com  
Move mailbox for account john@example.com to mail2.example.com host
```

doMailboxMove Details

- When moving a domain, each account from the current server is enumerated and moved sequentially.
- The mailbox is set to maintenance mode only during the 'account' stage.
- The move will be stopped if 5% or more write errors are encountered on items being moved.
 - When multiple mailboxes are moved within the same operation, the error count is global and not per-mailbox.
- Moves will not start if the destination server does not have enough space available to host the mailbox.

- When a single operation is used to move multiple mailboxes, the space check will be performed before moving each mailbox.
- All data is moved at a low-level and will not be changed except for the mailbox id.
- The operation is made up of 3 stages: blobs | backup | account. For each mailbox:
 - blobs: All blobs are copied from the source server to the destination server.
 - backup: All backup entries are copied from the source server to the destination server.
 - account: All database entries are moved as-is and LDAP entries are updated, effectively moving the mailbox.
- All of the stages are executed sequentially.
- On the reindex stage's completion, a new HSM operation is submitted to the destination server, if not specified otherwise.
- All volumes' compression options are taken.
- The MailboxMove operation can be executed if and only if no others operations are running on the source server.
- A move will not start if the destination server does not have enough space available or the user just belongs to the destination host.
- By default, items are placed in the Current Primary volume of the destination server.
 - The `hsm true` option can be used to apply the HSM policies of the destination server after a mailbox is successfully moved.
- If, for any reason, the move stops before it is completed the original account will still be active and the appropriate notification will be issued.
- Should the mailboxd crash during move, the "Operation Interrupted" notification is issued as for all operations, warning the users about the interrupted operation.
- Index information are moved during the 'account' stage, so no manual reindexing is needed nor one will be triggered automatically.

HSM NG Attachment Indexing

How Indexing Works

A new indexing engine has been added to HSM NG to index attachment contents.

The indexing engine works together with Zimbra's default engine. The main Zimbra indexing process analyzes the contents of an item, splitting it into several parts based on the MIME parts of the object. Next, Zimbra handles the indexing of *known* contents - plaintext - and passes the datastream on to the HSM NG handlers for all other content.

The indexing engine includes an indexing cache that speeds up the indexing process of any content that has already been analyzed. Datastreams over 10Kb are cached by default, and the cache holds 10000 entries, while smaller datastreams are not cached as the cache benefits only apply to large datastreams.

Indexed Formats

Web

Extension	Parser	Content-type
asp	HtmlParser	application/x-asp
htm	HtmlParser	application/xhtml+xml
html	HtmlParser	application/xhtml+xml, text/html
shtml	HtmlParser	application/xhtml+xml
xhtml	HtmlParser	application/xhtml+xml

Documents

Extension	Parser	Content-type
rtf	RTFParser	application/rtf
pdf	PDFParser	application/pdf
pub	OfficeParser	application/x-mspublisher
xls	OfficeParser	application/vnd.ms-excel
xlt	OfficeParser	application/vnd.ms-excel
xlw	OfficeParser	application/vnd.ms-excel
ppt	OfficeParser	application/vnd.ms-powerpoint
pps	OfficeParser	application/vnd.ms-powerpoint
mpp	OfficeParser	application/vnd.ms-project
doc	OfficeParser	application/msword
dot	OfficeParser	application/msword
msg	OfficeParser	application/vnd.ms-outlook
vsd	OfficeParser	application/vnd.visio
vst	OfficeParser	application/vnd.visio
vss	OfficeParser	application/vnd.visio
vsw	OfficeParser	application/vnd.visio
xlsm	OOXMLParser	application/vnd.ms-excel.sheet.macroenabled.12
pptm	OOXMLParser	application/vnd.ms-powerpoint.presentation.macro.enabled.12

Extension	Parser	Content-type
xltx	OOXMLParser	application/vnd.openxmlformats-officedocument.spreadsheetml.template
docx	OOXMLParser	application/vnd.openxmlformats-officedocument.wordprocessingml.document
potx	OOXMLParser	application/vnd.openxmlformats-officedocument.presentationml.template
xlsx	OOXMLParser	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
pptx	OOXMLParser	application/vnd.openxmlformats-officedocument.presentationml.presentation
xlam	OOXMLParser	application/vnd.ms-excel.addin.macroenabled.12
docm	OOXMLParser	application/vnd.ms-word.document.macroenabled.12
xltm	OOXMLParser	application/vnd.ms-excel.template.macroenabled.12
dotx	OOXMLParser	application/vnd.openxmlformats-officedocument.wordprocessingml.template
ppsm	OOXMLParser	application/vnd.ms-powerpoint.slideshow.macroenabled.12
ppam	OOXMLParser	application/vnd.ms-powerpoint.addin.macroenabled.12
dotm	OOXMLParser	application/vnd.ms-word.template.macroenabled.12

Extension	Parser	Content-type
ppsx	OoxMLParser	application/vnd.openxmlformats-officedocument.presentationml.slideshow
odt	OpenDocumentParser	application/vnd.oasis.opendocument.text
ods	OpenDocumentParser	application/vnd.oasis.opendocument.spreadsheet
odp	OpenDocumentParser	application/vnd.oasis.opendocument.presentation
odg	OpenDocumentParser	application/vnd.oasis.opendocument.graphics
odc	OpenDocumentParser	application/vnd.oasis.opendocument.chart
odf	OpenDocumentParser	application/vnd.oasis.opendocument.formula
odi	OpenDocumentParser	application/vnd.oasis.opendocument.image
odm	OpenDocumentParser	application/vnd.oasis.opendocument.text-master
ott	OpenDocumentParser	application/vnd.oasis.opendocument.text-template
ots	OpenDocumentParser	application/vnd.oasis.opendocument.spreadsheet-template
otp	OpenDocumentParser	application/vnd.oasis.opendocument.presentation-template
otg	OpenDocumentParser	application/vnd.oasis.opendocument.graphics-template
otc	OpenDocumentParser	application/vnd.oasis.opendocument.chart-template
otf	OpenDocumentParser	application/vnd.oasis.opendocument.formula-template
oti	OpenDocumentParser	application/vnd.oasis.opendocument.image-template
oth	OpenDocumentParser	application/vnd.oasis.opendocument.text-web
sxw	OpenDocumentParser	application/vnd.sun.xml.writer

Packages and Archives

Extension	Parser	Content-Type
z	CompressorParser	application/x-compress
bz	CompressorParser	application/x-bzip
boz	CompressorParser	application/x-bzip2
bz2	CompressorParser	application/x-bzip2
gz	CompressorParser	application/gzip
gz	CompressorParser	application/x-gzip
gzip	CompressorParser	application/x-gzip
xz	CompressorParser	application/x-xz
tar	PackageParser	application/x-tar
jar	PackageParser	application/java-archive
7z	PackageParser	application/x-7z-compressed
cpio	PackageParser	application/x-cpio
zip	PackageParser	application/zip
rar	RarParser	application/x-rar-compressed
txt	TXTParser	text/plain

Parser Controls

Parsers can be turned on or off by changing the related value to `true` or `false` via the `zxsuite config` CLI command.

Attribute	Parsers
pdfParsingEnabled	PDFParser
odfParsingEnabled	OpenDocumentParser
archivesParsingEnabled	CompressorParser, PackageParser, RarParser
microsoftParsingEnabled	OfficeParser, OOXMLParser, OldExcelParser
rtfParsingEnabled	RTFParser

e.g. to disable PDF parsing run:

```
zxsuite config server set server.domain.com attribute pdfParsingEnabled value false
```

By default, all parsers are active.

ABQ Service

The "Allow/Block/Quarantine" feature allows for granular access control of mobile devices connecting to the server. It's a "pre-emptive" type of security feature, meaning that it acts upon the first connection to the server and it's made to ensure that only authorized devices can finalize synchronization with server. This allows a full administrator to keep track of all mobile device used in their network. Presently only CLI tools are provided; a web GUI will be released in the future.

Components

The ABQ feature is composed of three main logical components:

- a Device Control List
- an Authorization Engine
- a set of CLI tools

Device Control List

The Device Control List, also known as the "ABQ List", holds the information about allowed devices within the NG config engine. Devices can be added to the Device Control List via CLI based on their "Device ID" which can be obtained via CLI.

It is also possible to further limit access by limiting the accounts that can synchronise with the server on a specific device.



On module startup, if the Device Control List is empty all mobile devices previously recognized by the Zimbra server will be imported as **Allowed**.

Authorization Engine

The Authorization Engine takes care of checking devices against the Device Control List and setting their ABQ status to the appropriate value.

Each rule is applied to all accounts connecting using a device it is a device id. It applies to a specific account connecting using that device if it has the format device_id/account_id or device_id/accountName

CLI Toolset.

The CLI Toolset allows administrators to interact with the device control list and with the synchronization status of a device, specifically to:

- Display the Device Control List
- Display all Quarantined and Blocked Devices
- Add one or more devices to the Device Control List
- Move a device from "Quarantine" to "Allowed" or "Blocked"

- Change the synchronization status of a device

Every time the administrator changes a device's status in an ABQ-enabled environment, depending on the issued state the device will be forced to re-sync folders with the server resulting in an immediate re-route to either a *dummy virtual mailbox* that will explain to the user what's happened, or to the real mailbox to perform the re-sync.

ABQ Modes

The ABQ feature is triggered for every mobile device that tries to synchronize with server, and can be set to one of four possible modes: "Permissive", "Interactive", "Strict" and "Disabled". This attribute is Global for all the cluster.

"Permissive" mode:

The Authorization Engine is not active, so after authenticating the user and checking their account status for safety reasons, the synchronization will continue. It is still possible to block specific devices but non-blocked devices will always be allowed to sync.

"Interactive" mode:

After authenticating the user and checking their account status for safety reasons, the Device Control system will check the "Device ID" sent by the device against the list of allowed devices:

- if the device/user couple is in the "allowed" list the synchronization will continue.
- if the device/user couple is not in the device list but device is in the "allowed" list the synchronization will continue.
- if the device is not in the "allowed" list the synchronization will be paused, a dummy email notifying the user of its "Quarantine" status will be sent and the connection will be set to "Quarantine" status.

Administrators can be notified at regular intervals, and every notification email will only include new Quarantined devices. They will then be able to allow or deny the synchronization for each device using the appropriate CLI tools.

"Strict" mode:

After authenticating the user and checking their account status for safety reasons, the Device Control system will check the "Device ID" sent by the device against the list of allowed devices:

- if the device/user couple or the device by itself is in the "allowed" list the synchronization will continue.
- if the device is not in the "allowed" list the synchronization will be put in "Blocked" state, no data will be synchronized and a dummy email notifying the user of the device's "Blocked" status will be sent.

"Disabled" mode:

ABQ is disabled, no checks are triggered and no policies are enforced.

ABQ Mode Control

The current mode can be checked by running the following command:

```
zxsuite config global get attribute abqMode
```

The ABQ mode can be changed running the following command:

```
zxsuite config global set attribute abqMode value  
[Permissive|Interactive|Strict|Disabled]
```

Dummy data

The feature makes use of “Dummy emails” and a “Dummy mailbox” to put devices on hold while waiting for authorization (Interactive Mode) or to notify their “Blocked” status (Permissive Mode, Interactive Mode and Strict Mode).

The Dummy Mailbox is a virtual mailbox consisting of only an “Inbox” folder that will be synchronized to the device while this is in either Quarantine or Block status. Dummy Emails are predefined email messages that are synchronized to a device in Quarantine or Block status to alert the user. For now these messages aren’t customizable, and will be localized in the future. Whenever the ABQ status of a device is changed, the device’s sync state will be reset.

This was designed to make sure the user knows what’s happening, the alternative being forcing the synchronization to fail with no descriptive response for the user itself – which would likely cause a significant overhead on support calls.

Notifications

Administrators can be notified via email of quarantined devices at a specific interval defined by the **abqNotificationsInterval** NG configuration attribute, expressed in milliseconds:

The interval can be checked by running the following command:

```
zxsuite config global get attribute abqNotificationsInterval
```

The interval can be changed running the following command:

```
zxsuite config global set attribute abqNotificationsInterval value [delay in  
milliseconds]
```

By default, the `abqNotificationsInterval` is set to 0 - meaning that no notifications will be delivered.

ABQ Service Status

The ABQ service status can be checked running the following command:

```
zxsuite mobile getServices
```

The service can be stopped or started using the default service control of the Mobile NG module:

```
zxsuite mobile doStartService abq  
zxsuite mobile doStopService abq
```

When mode is Disabled ABQ service won't automatically start and devices are always allowed to sync.

ABQ CLI

A list of all ABQ CLI commands can be displayed running:

```
$ zxsuite mobile abq
```

Allow/Block/Quarantine mobile devices management

```
list          - List devices.  
              zxsuite mobile ABQ list [attr1 value1 [attr2 value2...]]  
]  
  
add          - add/import devices  
              zxsuite mobile ABQ add [attr1 value1 [attr2 value2...]]  
  
allow        - Allow synchronization for a quarantined device  
              zxsuite mobile ABQ allow {device_id}  
  
block        - Deny synchronization for a quarantined device  
              zxsuite mobile ABQ block {device_id}  
  
set          - Set synchronization status for a device  
              zxsuite mobile ABQ set {device_id}  
{Allowed|Blocked|Quarantined}  
  
delete       - Delete device from ABQ  
              zxsuite mobile ABQ delete {device_id}  
  
setNotificationInterval - Set the notification interval for new quarantined  
devices  
              zxsuite mobile ABQ setNotificationInterval {45m|6h|1d|0}
```

ABQ "list" Command

List all devices ABQ status. The "status" argument will filter the list in order to only show devices in that specific status.

```
$ zxsuite mobile abq list
```

List devices.

Syntax:

```
zxsuite mobile ABQ list [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
status(0)	String	Allowed Blocked Quarantined

(M) == mandatory parameter, (0) == optional parameter

Example:

```
[zimbra@mail ~]$ zxsuite mobile abq list
```

devices

device_id	androidc133785981
status	Quarantined
device_id	androidc1024711770
status	Blocked
device_id	SAMSUNG1239862958
status	Allowed

ABQ "import" Command

This command imports a list of device ids from a file, and always requires two parameters: an Input File with a list of Device IDs separated by a newline and the "status" the imported device(s) will be set to.

```
[zimbra@mail ~]$ zxsuite mobile abq import  
command import requires more parameters
```

Syntax:

```
zxsuite mobile ABQ import {Path to file} {Allowed|Blocked|Quarantined}
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
input_file(M)	String	Path to file
status(M)	String	Allowed Blocked Quarantined

(M) == mandatory parameter, (O) == optional parameter

Usage example:

```
zxsuite mobile ABQ import /path/to/file Allowed
```

Example:

```
[zimbra@mail ~]$ zxsuite mobile abq import /tmp/list Allowed  
3 devices added
```

```
[zimbra@mail ~]$ cat /tmp/list  
androidc133785981  
androidc1024711770  
SAMSUNG1239862958/user@domain.com
```

In the example above, devices `androidc133785981` and `androidc1024711770` are allowed to sync entirely regardless of the account, while device `SAMSUNG1239862958` can only synchronise the `user@domain.com` account

ABQ "allow" Command

This is a specific command for quarantined device, and sets device status to **Allowed**.

```
$ zxsuite mobile abq allow  
Allow synchronization for a quarantined device
```

Syntax:

```
zxsuite mobile ABQ allow {device_id} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
device_id(M)	String	
account(0)	String	27ee8dd9-d813-4ca7-a988-580df0027a58 user1@example.com

(M) == mandatory parameter, (0) == optional parameter

ABQ "block" Command

This is a specific command for quarantined device, and sets device status to **Blocked**.

```
$ zxsuite mobile abq block  
Deny synchronization for a quarantined device
```

Syntax:

```
zxsuite mobile ABQ block {device_id} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
device_id(M)	String	
account(0)	String	27ee8dd9-d813-4ca7-a988-580df0027a58 user1@example.com

(M) == mandatory parameter, (0) == optional parameter

ABQ "set" Command

Set any status for any single device (either known or unknown).

```
$ zxsuite mobile abq set  
Set synchronization status for a device
```

Syntax:

```
zxsuite mobile ABQ set {device_id} {Allowed|Blocked|Quarantined} [attr1 value1  
[attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
device_id(M)	String	
status(M)	String	Allowed Blocked Quarantined
account(0)	String	27ee8dd9-d813-4ca7-a988-580df0027a58 user1@example.com

(M) == mandatory parameter, (0) == optional parameter

ABQ "delete" Command

Delete a device from all lists.

```
$ zxsuite help mobile abq delete  
Delete device from ABQ
```

Syntax:

```
zxsuite mobile ABQ delete {device_id} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
device_id(M)	String	
account(0)	String	27ee8dd9-d813-4ca7-a988-580df0027a58 user1@example.com

(M) == mandatory parameter, (0) == optional parameter

ABQ "setNotificationInterval" Command

Set notification interval for new quarantined devices.

```
$ zxsuite mobile abq setNotificationInterval  
command setNotificationInterval requires more parameters
```

Syntax:

```
zxsuite mobile ABQ setNotificationInterval {45m|6h|1d}
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
interval(M)	String	45m 6h 1d

(M) == mandatory parameter, (0) == optional parameter

Usage example:

Set notification of new quarantined devices every 45 minutes
zxsuite mobile abq setNotificationInterval 45m

Set notification of new quarantined devices every 6 hours
zxsuite mobile abq setNotificationInterval 6h

Set notification of new quarantined devices once every day
zxsuite mobile abq setNotificationInterval 1d

Disable notifications of new quarantined devices
zxsuite mobile abq setNotificationInterval 0

Admin NG

Delegated Admin Provisioning

What is Delegated Admin Provisioning?

Delegated Admin Provisioning is the set of operations that allow you to grant, edit and revoke Domain Admin rights to a user.

All Delegated Admin Provisioning operations can be performed:

- From the Admin NG tab of the Administration Zimlet
- From the CLI, running the appropriate `zxsuite` command as the `zimbra` user

Granting Delegated Admin Rights to a User

From the Administration Zimlet

In the **Delegated Admins** section of the Admin NG tab in the Administration Zimlet, click the **Add** button.

You will be prompted for the following information:

- Account: The email address to which you want to grant Delegated Admin rights.
- Domain: The domain on which the Delegated Admin will have control.
- Delegated Auth: Check this box to allow the Delegated Admin to use the **View Mail** features on any mailbox in the selected domain.
- Grant Limit: The maximum mailbox quota this Delegated Admin can assign to a user.
- Edit Features: Defines whether the Delegated Admin is able to edit the contents of the **Features** tab for its assigned users.



If the **Domain Quota** is lower than the **Grant Limit**, the **Grant Limit** value will be ignored.

Disk space and Quota limits can be entered in Gigabytes (gb), Megabytes (mb) or Kilobytes (kb).

From the CLI

To grant Delegated Admin rights to a user, use the `doAddDelegationSettings` command:

Syntax:

```
zxsuite admin doAddDelegationSettings {account} {domain} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
account(M)	String		
domain(M)	String		
viewMail(0)	Boolean	true false	false
editFeatures(0)	Boolean	true false	false
adminQuota(0)	String		-1

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite admin doAddDelegationSettings john@example.com example.com viewMail true  
adminQuota -1
```

Adds John as delegated administrator of domain example.com, with the right to view user mail on such domain and no right to grant quotas to users.

```
zxsuite admin doAddDelegationSettings john@example.com example.com adminQuota 0  
Adds John as delegated administrator of domain example.com, with the right to assign unlimited quotas to users.
```

```
zxsuite admin doAddDelegationSettings john@example.com example.com adminQuota 10gb  
Adds John as delegated administrator of domain example.com, with the right to assign quotas up to 10gb to each user.
```

Editing the Rights of an Existing Delegated Admin

From the Administration Zimlet

In the **Delegated Admins** section of the Admin NG tab in the Administration Zimlet, select an entry in the list and click the **Edit** button.

You can also double click an entry on the list to edit it.

From the CLI

To edit the rights of an existing Delegated Admin, use the **doEditDelegationSettings** command:

Syntax:

```
zxsuite admin doEditDelegationSettings {account} {domain} [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
account(M)	String	
domain(M)	String	
viewMail(0)	Boolean	true false
editFeatures(0)	Boolean	true false
adminQuota(0)	String	

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite admin doEditDelegationSettings john@example.com example.com viewMail true  
adminQuota -1
```

Edits John's delegation rights for domain example.com, with the right to view user mail on such domain and no right to grant quotas to users.

```
zxsuite admin doEditDelegationSettings john@example.com example.com adminQuota 0  
Edits John's delegation rights for domain example.com, with the right to assign unlimited quotas to users.
```

```
zxsuite admin doEditDelegationSettings john@example.com example.com adminQuota 10gb  
Edits John's delegation rights for domain example.com, with the right to assign quotas up to 10gb to each user.
```

Revoke Delegated Admin Rights from a User

From the Administration Zimlet

In the **Delegated Admins** section of the Admin NG Tab in the Administration Zimlet, select an entry in the list and click the **Delete** button.

From the CLI

To revoke Delegated Admin rights from a user, use the **doRemoveDelegationSettings** command:

```
zxsuite admin doRemoveDelegationSettings {account} {domain}
```

PARAMETER LIST

NAME	TYPE
account(M)	String
domain(M)	String

(M) == mandatory parameter, (O) == optional parameter

Usage example:

```
zxsuite admin doRemoveDelegationSettings john@example.com example.com
John no longer administers domain example.com
```

Quota Management

What is Quota Management?

Admin NG allows the Global Administrator to set two different types of quota limits: the **Grant Limit** and the **Domain Quota**.

Neither the **Domain Quota** nor the **Grant Limit** are mandatory, meaning that a Delegated Admin can be allowed to grant any quota to a user and that a domain can lack a maximum quota limit.

The Grant Limit

The **Grant Limit** is one of the properties of a Delegated Admin.

It specifies the maximum mailbox quota that the Delegated Admin can grant to a mailbox and can be set and changed in the Delegated Admin's settings.

Three options are available:

- None: The Delegated Admin cannot edit the Quota attribute of a mailbox.
- Custom: The Delegated Admin can grant up to the specified value. This overrides any domain/COS quota setting.
- Unlimited: The Delegated Admin can grant any quota to the mailbox. This overrides any domain/COS quota setting.

The Domain Quota

The **Domain Quota** is a property that specifies the maximum mailbox quota that **any Administrator** can grant to a mailbox in the domain.



Assigning an unlimited quota to a mailbox will override the Domain Quota setting.

Grant Limit vs Domain Quota

The **Grant Limit** and **Domain Quota** properties are mutually exclusive on a restrictive basis.

This means that the following scenarios may occur:

- A Global Admin grants a user a higher quota than the allowed Domain Quota
- A Delegated Admin grants a user a higher quota than the allowed Domain Quota
- A Delegated Admin's Grant Limit is lower than the Domain Quota

Let's examine these scenario one by one.

A Global Admin grants a user a higher quota than the allowed Domain Quota

Since the Domain Quota applies to a given domain, not to a given Admin, the effective quota for the user will be the maximum quota allowed by the **Domain Quota** setting.

A Delegated Admin grants a user a higher quota than the allowed Domain Quota

In this case, the effective quota for the user will be the maximum quota allowed by the **Domain Quota** setting, even if the Delegated Admin's Grant Limit is higher than the Domain Quota.

A Delegated Admin's Grant Limit is lower than the Domain Quota

In this case, the maximum quota that the Delegated Admin can grant to a user will be the one defined by the Grant Limit, even if the Domain Quota is higher. A Global Admin, which is not bound to any Grant Limit restriction, will be allowed to assign any mailbox quota to the user up to the limit allowed by the Domain Quota.

Domain Limits

What is Domain Limit Management (a.k.a. **Domain Settings**)?

Domain Limit Management is a feature of the Admin NG module. It allows a Global Administrator to set domain level limits that cannot be exceeded by any Administrator.

The only way to exceed a Domain Limit is to change the Domain Limit itself.

Domain Limits

- Global Account Limit: The maximum number of accounts that can be created on this domain.
- Domain Quota: The maximum mailbox quota that any Administrator can grant to a mailbox in the domain.
- COS Limits: Define which Classes of Service can be used for users in the domain and the maximum number of users per Class of Service.

Edit the Limits of a Domain

From the Administration Zimlet

All the domains in the Zimbra infrastructure are listed in the [Domain Settings](#) list in the Admin NG tab of the Administration Zimlet.

To edit the limits of a domain, select the domain from the [Domain Settings](#) list and press the [Edit](#) button.

From the CLI

To edit the limits of a domain through the CLI, use the [setDomainSettings](#) command:

Syntax:

```
zxsuite admin setDomainSettings {domain} [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
domain(M)	String		
account_limit(0)	Integer		don't change
setting			
domain_account_quota(0)	String		don't change
setting			
cos_limits(0)	String	cosname1:limit1,cosname2:limit2	don't change
setting			

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite admin setDomainSettings example.com account_limit 100 domain_account_quota  
100mb cos_limits cos1:30,cos2:80
```

Sets a global account limit on the domain example.com of 100 accounts, with a domain account quota of 100 megabytes and with cos account limits of 30 for cos1 and 80 for cos2.

Note: A cos limit of -1 removes the limit for the cos.

Reset the Limits of a Domain

From the Administration Zimlet

All the domains in the Zimbra infrastructure are listed in the [Domain Settings](#) list in the Admin NG tab of the Administration Zimlet.

To reset the limits of a domain, select the domain from the [Domain Settings](#) list and press the [Reset](#)

button, then click **Ok** in the confirmation pop-up.

From the CLI

To reset the limits of a Domain through the CLI, use the `resetDomainSettings` command:

Syntax:

```
zxsuite admin resetDomainSettings {domain}
```

PARAMETER LIST

NAME TYPE

domain(M) String

(M) == mandatory parameter, (O) == optional parameter

Zimbra Administration as a Delegated Admin

Accessing the Zimbra Administration Console as a Delegated Admin

To access the Zimbra Administration Console, connect to port 7071 of your mailserver with a web browser and login with your Zimbra credentials.

E.g: <https://mail.domain.com:7071>

Delegated Admin CAN and CAN'T Table

Here is a quick reference of what a Delegated Admin CAN and CAN'T do through the Admin NG module.

CAN	CAN'T
View the account list of any domain for which they are granted Delegate Admin rights	View the account list belonging to any other domain
Edit any user account in any domain for which they are granted Delegate Admin rights	Edit any user account belonging to any other domain
Edit any alias, distribution list or resource in any domain for which they are granted Delegate Admin rights	Edit any alias, distribution list or resource belonging to any other domain
	Edit any Global Admin account
	Grant Global Admin or Delegated Admin rights to any user
Create an account on a domain for which they are granted Delegated Admin rights	Create an account on any other domain

CAN	CAN'T
Select the Class Of Service of an account between those available for that account's domain	Arbitrarily set the Class of Service of an account between those available on the server
	Edit COS settings
	Edit Domain Settings that may interfere with the proper functioning of the server
	See or edit any server setting
	See or edit any global setting

Overview of the Zimbra Administration Console for Delegated Admins

- **Manage:**
 - **Accounts:** Manage the Accounts belonging to any domain for which delegated admin rights have been granted.
 - **Aliases:** Manage Aliases of accounts belonging to any domain for which delegated admin rights have been granted.
 - **Distribution Lists:** Manage the Distribution Lists belonging to any domain for which delegated admin rights have been granted.
 - **Resources:** Manage the Resources belonging to any domain for which delegated admin rights have been granted.
- **Configure:** View the configuration of any domain for which delegated admin rights have been granted.
- **Search:** Perform advanced Searches.
- **Network NG**
 - **Mobile NG:** Manage the synchronization of mobile devices and clients belonging to any domain for which delegated admin rights have been granted.
 - "Admin NG: View the list of Delegated Admins belonging to any domain for which delegated admin rights have been granted as well as quota usage informations.
- **Search Bar:** Perform quick searches.
- **[username]:** Log Out from the Zimbra Administration Console.

Delegated Admin Log Browsing

What is Delegated Admin Log Browsing?

The Admin NG allows a Global Admin to easily keep track of all Admins' activity through a search-based graphical log browser.

The Admin NG Log Browser

The Admin NG Log Browser can be accessed by clicking [Browse Logs](#) in the Admin NG tab of the Administration Zimlet. The [Filter Log](#) pop-up dialog will open, allowing you to apply some filters to the logs you want to browse.

The available filters are:

- [Basic](#) filters
 - [Admin](#): Filter the logs to only view operations performed by a single Domain Admin.
 - [Action](#): Filter the logs to only view one particular action. See below for the available actions.
- [Advanced](#) filters
 - [Client IP](#): Filters the logs to only show operations performed from a determined IP address.
 - [Show Logins](#): Select this checkbox to also show when the Domain Admins log into the Zimbra Web Client.
 - [Outcome](#): Filters the logs to either show all operations, successful operations or failed operations.
 - [Start](#) and [End](#): Limits the logs shown to a specific timespan (default: the current day).

Clicking the [Details](#) button will apply the selected filters and show the log browser.

The [Action](#) filter

Any operation an Administrator can perform is available in the drop-down menu of the [Action](#) filter.

All of these operations are important to keep track of your admin's actions and to troubleshoot issues.

- [Auth](#): All ZWC authentications.
- [DelegateAuth](#): All Delegated Authentications, either through the [View Mail](#) button or through the [-z](#) option of the `zmmailbox` command.
- [CreateAccount](#): All account creations.
- [DeleteAccount](#): All account deletions.
- [Set Password](#): All mailbox password changes.
- [RemoveAccountAlias](#): All alias deletions.
- [DeleteDistributionList](#): All distribution lists deletions.

Reports and Information

Admin NG Monthly Reports

The Admin NG module includes a very useful [Monthly Reports](#) feature that allows Global Administrators to keep track of both Delegated Admin operations and domain status for a given

month.

How does the Monthly Report system work?

On the first day of each month, the Admin NG module automatically creates a report based on the data gathered in the Admin NG Log.

This monthly report includes:

GLOBAL REPORT	
First logged action	Timestamp of the first action performed by an Admin this month
Last logged action	Timestamp of the last action performed by an Admin this month
Last admin login by	Latest administrative login timestamp
Most active admin	Name of the Admin with the highest number of actions logged
Most used address	Most common IP Address for admin logins
Total accounts	Total number of mailboxes
Total created accounts	Number of mailboxes created during the month
Total deleted accounts	Number of mailboxes deleted during the month
Total created domains	Number of domains created during the month
Total created distribution lists	Number of distribution lists created during the month
Total deleted distribution lists	Number of distribution lists deleted during the month
DOMAIN REPORT	
Domain	The name of the domain this data refers to
Last admin login	Latest administrative login timestamp
Account/max accounts	Current and maximum number of accounts
Current Domain Size	Sum of the quotas used by all mailboxes in the domain
Maximum Domain Size	Sum of the maximum quota of all mailboxes (excluding Unlimited mailboxes)
Accounts with no quota limit	Number of mailboxes that don't have a quota limit
Total size of accounts with no quota limit	Sum of the quotas used by all mailboxes with no quota limit
System Resources in the domain	Number of system resource accounts in the domain

DOMAIN REPORT	
Calendar Resources in the domain	Number of calendar resource accounts in the domain
Successful domain actions	Number of successful actions done by admins on this domain
Unsuccessful domain actions	Number of unsuccessful actions done by admins on this domain
ADMIN REPORT	
Admin	The name of the admin this data refers to
Successful logins	Number of successful logins into the Admin Console
Unsuccessful logins	Number of unsuccessful logins into the Admin Console
View mails	Number of times this admin used the View Mail feature during the month
Last login	Timestamp of the last login of this admin into the Administration Console
Most used address	The email address most used by this admin to login
Total actions	The number of actions performed by this admin during the month
Accounts created	Number of accounts created by this admin during the month
Accounts deleted	Number of accounts deleted by this admin during the month

How to Access the Monthly Reports

From the Administration Zimlet

To access the [Monthly Reports](#):

- Log into the Zimbra Administration Console as a Global Admin.
- On the Admin NG tab of the Administration Zimlet, click the [Monthly Reports](#) button on the top-right of the page.
- Select the month you wish to view and click [Show Report](#).

From the CLI

To view the Monthly Reports from the CLI, use the `getMonthlyReport` command:

```
zxsuite admin getMonthlyReport [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
month(0)	String	mm/yyyy	12/2012
local(0)	Boolean	true false	false

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite admin getMonthlyReport
```

Shows the monthly report for the previous month

```
zxsuite admin getMonthlyReport month 11/2012
```

Shows the monthly report for the month '11/2012'

Partial Reports

To create a partial report for the current month, use the **doMonthlyReport** command:

```
zxsuite admin doMonthlyReport [attr1 value1 [attr2 value2...]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES	DEFAULT
month(0)	String	mm/yyyy	12/2012
force(0)	Boolean	true false	false

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite admin doMonthlyReport
```

Generates the monthly report for the previous month and saves it in the current Admin NG log path

```
zxsuite admin doMonthlyReport month 01/2013
```

Generates a PARTIAL monthly report for the current month, without saving it to disk

**** NOTE****

This command is automatically executed once a month to generate a file containing the report for the previous month. To overwrite an existing report file, set the 'force' parameter to true.

The Admin NG Log Path

The Admin NG Module stores all monthly reports, together with the logs used to generate the Monthly reports and to provide information via the [Admin Log Browser](#) feature, in a path inside the `/opt/zimbra/conf/` folder (default `/opt/zimbra/conf/zextras/zxadmin/`). This particular default path has been chosen because it is the only directory that CANNOT be deleted during a Zimbra update.

The Admin NG Log Path Structure and Contents

The Admin NG log path is a flat directory containing the following files:

- One or more `YYYY_MM` files containing the logs for the file's namesake month.
- Zero or more `YYYY_MM.report` files containing the monthly report for the file's namesake month.
- Zero or more `YYYY_MM.X` files containing partial logs for the file's namesake month. These files are created when changing the Admin NG Log Path.

Changing the Admin NG Log Path



Carefully read this paragraph before changing the Admin NG Log Path. Any error on the procedure will cause a potential log loss that will render the [Monthly Report](#) and [Show Admin Logs](#) features highly unreliable.

To safely change the Admin NG Log Path, follow these steps:

- Create the folder that will contain the logs:
 - The folder's ownership must be `zimbra:zimbra`.
 - The 'zimbra' user must have read and write permissions to the folder.
 - The folder must be empty.
- Log into the Zimbra Administration Console as a Global Admin.
- Open the Admin NG tab in the Administration Zimlet.
- In the [Basic Module Configuration](#) section, click the [Change](#) button near the Admin Log Path line.
- Enter the new path and click [Change Path](#).
- If no errors are shown, move all the contents of the old log path.
 - It's perfectly normal to only see `.report` and `.X` files in the old log path, as the current log file will be given the `.1` extension to mark it as a partial. Any previous `.X` files will have their extension number increased by 1.

Configuration Reset

What is the Admin NG Configuration Reset?

The Admin NG Configuration Reset is a free feature of the Admin NG module that allows a Global Administrator to completely wipe all delegation rights from the server.

This is not a **rollback** feature that cleans the Admin NG module's configuration. Resetting the Admin Configuration will affect both Admin NG and Zimbra delegation rights.



Using the Admin Configuration Reset feature will completely wipe all delegation configuration from the server, bringing it back to the state of a fresh installation. Only Admin Delegation settings will be wiped, no other kind of data will be affected.

What does the Admin Configuration Reset clear?

The Admin Configuration Reset clears the following configurations:

- The **isDelegatedAdmin** account property for all accounts on the server
- All Access Control Entries and all Access Control Lists for
 - Users
 - Domains
 - Classes of service
 - Local configuration
 - Server configuration
 - Zimlets

When should I use the Admin Config Reset?

The Admin Config Reset should only be used in the following cases:

- To completely reset a compromised situation
 - If one or more wrong ACL or ACE settings cause your Zimbra Administration Console to be unstable or not to properly show (e.g. displaying a blank page or missing one or more UI elements), use the Admin Configuration Reset as a final resolution.
- If you plan to stop using the Admin NG module
 - The reset option is available even if no valid Network NG license is active. Remember that this will also wipe any manually set Delegation settings.

How do I use the Admin Configuration Reset?

If you **really** want to reset the Admin Delegation configuration, simply run this CLI command:

```
zxsuite core doDeleteAllDelegatedRights
```

You will be asked to enter a confirmation string to avoid any accidental use of the command.

NG Modules CLI

Network NG Modules CLI

zxsuite - Network NG Modules Command-Line Interface

Basic Usage

Every module of Network NG, including the core, has its own set of `zxsuite` commands. All `zxsuite` commands are invoked with the following syntax:

```
:: zxsuite [--host | --offline] [--json] [--progress] [--sync] {module} {action} [options]
```

Available switches:

- `--host` [hostname|ip] - Specify a target host for the command. Leave blank for localhost. Use `all_servers` to broadcast the command to all servers.
- `--offline` - Use if Zimbra is not started. Some commands will not work
- `--json` - The output of the command will be presented in JSON format. Good for scripting.
- `--progress` - Prints the operation's feedback directly to STDOUT. Press Ctrl+C to interrupt the output. The operation itself won't be interrupted.
- `--sync` - Runs the command in synchronous mode, waiting for the operation's execution to end and returning an exit code relevant with the operation's result among the following:
 - 0 - Successful
 - 1 - Failed
 - 2 - Stopped
 - 3 - Removed
 - 4 - Interrupted

Online Help: An Online Help for every command is available through `zxsuite help {module} [command]`. Omitting the command will display the full list of available commands.

Core CLI

Basic Usage:

```
zxsuite core {action} [options]
```

Core Commands

```
:: getVersion - Display Network NG Modules version
```

```
zxsuite core getVersion
```

:: **getProperty** - Get configuration properties
zxsuite core getProperty [attr1 value1 [attr2 value2]]

:: **setProperty** - Set configuration property
zxsuite core setProperty {property_name} {property_value}

:: **getLicenseInfo** - Display Network NG Modules license informations
zxsuite core getLicenseInfo core getLicenseInfo

:: **doUploadLicense** - Upload a Network NG license
zxsuite core doUploadLicense {license_path}

:: **doLicenseChecks** - Force Network NG license checks
zxsuite core doLicenseChecks

:: **getAccountStats** - Show statistic informations about provided account name or ID
zxsuite core getAccountStats {account}

:: **getNotification** - Shows Network NG notifications
zxsuite core getNotification [attr1 value1 [attr2 value2]]

:: **doDeleteAllDelegatedRights** - This command deletes both Admin NG and Zimbra's own Admin Delegation settings
zxsuite core doDeleteAllDelegatedRights {confirmation string}

Update CLI

Basic Usage:

```
zxsuite update {action} [options]
```

Update Commands

:: **doCheckUpdate** - Fetch update information

```
zxsuite update doCheckUpdate
```

:: **doStartService** - start a given service

```
zxsuite update doStartService {service_name}
```

:: **doStopService** - stop a given service

```
zxsuite update doStopService {service_name}
```

:: **download** - [BETA] Update Network NG with the latest update available, the version will be loaded on the next mailboxd restart

```
zxsuite update download  
:: enable - [BETA] Enable Network NG automatic update capabilities  
zxsuite update enable  
:: getServices - show current status of all services for this module  
zxsuite update getServices  
:: info - Info on Network NG updates  
zxsuite update info  
:: start - [BETA] Load a new Network NG version  
zxsuite update start [attr1 value1 [attr2 value2]]
```

Backup NG CLI

Basic Usage:

```
zxsuite backup {action} [options]
```

Backup NG Commands

```
:: getProperty - Get configuration properties  
zxsuite backup getProperty [attr1 value1 [attr2 value2]]  
:: setProperty - Set configuration property  
zxsuite backup setProperty {property_name} {property_value}  
:: doSmartScan - Perform a Smart Scan  
zxsuite backup doSmartScan [attr1 value1 [attr2 value2]]  
:: doAccountScan - Perform a Full Scan on a single account  
zxsuite backup doAccountScan {account} [attr1 value1 [attr2 value2]]  
:: doExport - Perform an Export limited by domains  
zxsuite backup doExport {destination_path} [attr1 value1 [attr2 value2]]  
:: doRestoreOnNewAccount - Perform a Restore on New Account  
zxsuite backup doRestoreOnNewAccount {source_account} {destination_account} {dd/MM/yyyy  
HH:mm:ss|last} [attr1 value1 [attr2 value2]]  
:: doEnableDisableCOS - Enable or disable the backup for a specific COS  
zxsuite backup doEnableDisableCOS {cos_name} {enable|disable}  
:: doUndelete - Perform an Undelete Restore
```

```
zxsuite backup doUndelete {account} dd/MM/yyyy HH:mm:ss|first} dd/MM/yyyy  
HH:mm:ss|last} [attr1 value1 [attr2 value2]]
```

:: **doItemSearch** - Search for an item

```
zxsuite backup doItemSearch {account} [attr1 value1 [attr2 value2]]
```

:: **doItemRestore** - Restores a single item

```
zxsuite backup doItemRestore {account_name} {item_id}
```

:: **doExternalRestore** - Perform an External Restore

```
zxsuite backup doExternalRestore {source_path} [attr1 value1 [attr2 value2]]
```

:: **doStopOperation** - Stop a single running operation

```
zxsuite backup doStopOperation {operation_uuid}
```

:: **doStopAllOperations** - Stops all running operations and empties the operations queue

```
zxsuite backup doStopAllOperations
```

:: **doCheckShares** - Check all shares on local accounts

```
zxsuite backup doCheckShares
```

:: **doFixShares** - Try to fix all shares on local accounts

```
zxsuite backup doFixShares {import_idmap_file}
```

:: **doFixOrphans** - Delete orphan digest files

```
zxsuite backup doFixOrphans [attr1 value1 [attr2 value2]]
```

:: **doCoherencyCheck** - Check backup coherency

```
zxsuite backup doCoherencyCheck {backup_path} [attr1 value1 [attr2 value2]]
```

:: **getAccountInfo** - Shows an account's information

```
zxsuite backup getAccountInfo {account} [attr1 value1 [attr2 value2]]
```

:: **getBackupInfo** - Displays informations about the backup system

```
zxsuite backup getBackupInfo [attr1 value1 [attr2 value2]]
```

:: **getMap** - Show binary Map object as human readable table

```
zxsuite backup getMap {file_path}
```

:: **getItem** - Display an item in a human-readable format.

```
zxsuite backup getItem {account} {item} [attr1 value1 [attr2 value2]]
```

:: **getAvailableAccounts** - Displays all accounts available for restore

```
zxsuite backup getAvailableAccounts [attr1 value1 [attr2 value2]]
```

:: getAvailableDomains - Displays all domains available for restore

```
zxsuite backup getAvailableDomains {dd/MM/yyyy HH:mm:ss|last} {backup_path}
```

:: getServerConfig - Provides a list of stored server configs

```
zxsuite backup getServerConfig dd/MM/yyyy  
HH:mm:ss|last|all} {standard|customizations} [attr1 value1 [attr2 value2]]
```

:: getCOSBackupStatus - Displays the backup status of all COS

```
zxsuite backup getCOSBackupStatus [attr1 value1 [attr2 value2]]
```

:: getAllOperations - Displays all running and queued operations

```
zxsuite backup getAllOperations
```

:: monitor - Monitor a running operation

```
zxsuite backup monitor {operation_uuid} [attr1 value1 [attr2 value2]]
```

:: getServices - Show the current status of all the module's services

```
zxsuite backup getServices
```

:: doBackupLDAP - Backup LDAP

```
zxsuite backup doBackupLDAP
```

:: doRestartService - Restart one given service

```
zxsuite backup doRestartService {service_name}
```

:: doRestoreBlobs - Start a "restore blobs" operation which tries to restore broken zimbra blobs.

```
zxsuite backup doRestoreBlobs {volume_id} [attr1 value1 [attr2 value2]]
```

Mobile NG CLI

Basic Usage:

```
zxsuite mobile {action} [options]
```

Mobile NG Commands

:: getProperty - Get configuration properties

```
zxsuite mobile getProperty [attr1 value1 [attr2 value2]]
```

:: setProperty - Set configuration property

```
zxsuite mobile setProperty {property_name} {property_value}
```

:: getDeviceList - Display all devices for the provided account

```
zxsuite mobile getDeviceList {account}
```

:: getDeviceInfo - Display information about the provided device

```
zxsuite mobile getDeviceInfo {account} {device_id}
```

:: doResetAccount - Reset ALL device states for the provided account

```
zxsuite mobile doResetAccount {account}
```

:: doResetDevice - Resets the device's SyncState for a single account

```
zxsuite mobile doResetDevice {account} [attr1 value1 [attr2 value2]]
```

:: getAllSessions - Returns informations about all stored mobile sessions

```
zxsuite mobile getAllSessions
```

:: getActiveSessions - Returns all active mobile sessions

```
zxsuite mobile getActiveSessions
```

:: doRemoveDevice - Removes all the device's SyncState and history from the server

```
zxsuite mobile doRemoveDevice {account} {device_id}
```

:: getAccountLoggers - Returns informations about all account loggers

```
zxsuite mobile getAccountLoggers
```

:: doRemoveLogger - Removes an account logger

```
zxsuite mobile doRemoveLogger {logger_id|all_loggers}
```

:: doAddAccountLogger - Add an account logger

```
zxsuite mobile doAddAccountLogger {account} {debug|info|warn|err|crit} {log_file}
```

HSM NG CLI

Basic Usage:

```
zxsuite powerstore {action} [options]
```

HSM NG Commands

:: +setHsmPolicy - Add an additional policy to HSM.

```
zxsuite powerstore +setHsmPolicy {hsm_policy}
```

:: addS3Store - Add an S3 compatible store

```
zxsuite powerstore addS3Store {Name of the zimbra store} [attr1 value1 [attr2 value2]]
```

:: doCheckBlobs - Start the doCheckBlobs operation.

```
zxsuite powerstore doCheckBlobs {start} [attr1 value1 [attr2 value2]]
```

:: doCreateVolume - Create a volume on the server

```
zxsuite powerstore doCreateVolume {primary|secondary|index} {volume_name} {volume_path} {true|f
alse} {compression_threshold_bytes}

:: doDeduplicate - Start a deduplication operation.

zxsuite powerstore doDeduplicate {volume_name} [attr1 value1 [attr2 value2]]

:: doDeleteVolume - Delete a specific volume on the server

zxsuite powerstore doDeleteVolume {volume_id}

:: doMoveBlobs - Start the doMoveBlob operation.

zxsuite powerstore doMoveBlobs [attr1 value1 [attr2 value2]]

:: doRemoveHsmPolicy - Remove a policy from HSM.

zxsuite powerstore doRemoveHsmPolicy {hsm_policy}

:: doRestartService - restart a given service

zxsuite powerstore doRestartService {service_name}

:: doStartService - start a given service

zxsuite powerstore doStartService {service_name}

:: doStopAllOperations - Stops all running operations and empties the operations queue

zxsuite powerstore doStopAllOperations

:: doStopOperation - Stop a single running operation

zxsuite powerstore doStopOperation {operation_uuid}

:: doStopService - stop a given service

zxsuite powerstore doStopService {service_name}

:: doUpdateVolume - Update a specific volume on the server

zxsuite powerstore doUpdateVolume {volume_id} [attr1 value1 [attr2 value2]]

:: doVolumeToVolumeMove - Start the doMoveVolumeBlobs operation.

zxsuite powerstore doVolumeToVolumeMove {source_volume_name} {destination_volume_name}

:: getAllOperations - Displays all running and queued operations

zxsuite powerstore getAllOperations [attr1 value1 [attr2 value2]]

:: getAllVolumes - Prints all the volumes present in the server

zxsuite powerstore getAllVolumes

:: getHsmPolicy - Prints all the policies

zxsuite powerstore getHsmPolicy
```

:: getProperty - Get configuration properties

```
zxsuite powerstore getProperty [attr1 value1 [attr2 value2]]
```

:: getServices - show current status of all services for this module

```
zxsuite powerstore getServices
```

:: getVolumeStats - Show space occupation, number of items and blobs contained in a volume

```
zxsuite powerstore getVolumeStats {volume_id} [attr1 value1 [attr2 value2]]
```

:: monitor - Monitor a running operation

```
zxsuite powerstore monitor {operation_uuid} [attr1 value1 [attr2 value2]]
```

:: setHSMPolicy - Set the default HSM policy

```
zxsuite powerstore setHSMPolicy {hsm_policy}
```

:: setProperty - Set configuration property

```
zxsuite powerstoresetProperty {property_name} {property_value}
```

:: testS3Connection - Test the connection to an S3 bucket.

```
zxsuite powerstore testS3Connection {s3BucketConfigurationUuid}
```

Admin NG CLI

Basic Usage:

```
zxsuite admin {action} [options]
```

Admin NG Commands

:: getDelegationSettings - Shows delegated admins with their domains of competency, the viewMail attribute and the admin-assignable quota

```
zxsuite admin getDelegationSettings [attr1 value1 [attr2 value2]]
```

:: doEditDelegationSettings

```
zxsuite admin doEditDelegationSettings {account} {domain} [attr1 value1 [attr2 value2]]
```

:: doAddDelegationSettings

```
zxsuite admin doAddDelegationSettings {account} {domain} [attr1 value1 [attr2 value2]]
```

:: *doRemoveDelegationSettings

```
zxsuite admin doRemoveDelegationSettings {account} {domain}
```

:: getDomainSettings - Shows all domains' name, account number limit, and max account quota

```
zxsuite admin getDomainSettings
```

:: setDomainSettings - Sets domain max account quota and account limit
zxsuite admin setDomainSettings {domain} [attr1 value1 [attr2 value2]]

:: resetDomainSettings - Resets global account limit, account limit per cos, and domain account quota for the selected domain
zxsuite admin resetDomainSettings {domain}

:: doShowAdminActivity - Shows all recorded admin activity
zxsuite admin doShowAdminActivity [attr1 value1 [attr2 value2]]

:: doEnableDisableAdminLogging - Enables or disables the logging of admin activities
zxsuite admin doEnableDisableAdminLogging {enable|disable}

:: setProperty - Set configuration property
zxsuite adminsetProperty {property_name} {property_value}

:: getProperty - Get configuration properties
zxsuite admin getProperty [attr1 value1 [attr2 value2]]

:: doMonthlyReport - Generate a report of admin activity in the specified month
zxsuite admin doMonthlyReport [attr1 value1 [attr2 value2]]

:: getMonthlyReport - Shows a report of admin activity in the specified *month
zxsuite admin getMonthlyReport [attr1 value1 [attr2 value2]]

:: doSetZimletRights - Fixes the Administration Zimlet rights for all delegated admins.
zxsuite admin doSetZimletRights

:: getAllOperations - Displays all running and queued operations
zxsuite admin getAllOperations

:: doStopAllOperations - Stops all running operations and empties the operations queue
zxsuite admin doStopAllOperations

:: doStopOperation - Stop a single running operation
zxsuite admin doStopOperation {operation_uuid}

:: monitor - Monitor a running operation
zxsuite admin monitor {operation_uuid} [attr1 value1 [attr2 value2]]

Incremental Migration to Zimbra 8.8.0 with Backup NG

Description

- This guide describes how to perform an Incremental Migration using Backup NG.
- It's specifically designed for the migration of a production environment, minimizing the downtime and aiming to be transparent for the users.
 - If correctly planned and executed, your mail system won't suffer any downtime, and the impact on the users will be close to zero.
- The source server of the migration requires either the Zextras Suite or Zimbra Suite Plus.
 - This guide applies for migrations from any Zimbra version supported by either of those to Zimbra 8.8.
- All the CLI commands in this Guide must be executed as the Zimbra user unless otherwise specified.

What Will be Migrated?

- Email and email folders
- Contacts and address books
- Appointments and calendars
- Tasks and task lists
- Files and briefcases
- Share informations
- User preferences
- User settings
- Class of Service settings
- Domain settings

What Will NOT be Migrated?

- Server settings (migrated for reference but not restored)
- Global settings (migrated for reference but not restored)
- Customizations (Postfix, Jetty, etc...).
- Items moved or deleted during the process will not be moved or deleted on the destination server.
- Preferences (e.g. passwords) changed during the process will be reset upon each import.



The incremental migration is not designed to set up a server-to-server mirroring. Using multiple imports to create a mirrored copy of the source server won't create a **mirrored** copy at all, since no deletions are performed by the import process.

Source Data

Data from the source server is obtained through either Zextras Suite or Zimbra Suite Plus.

- Zextras Suite can be obtained on the Zextras Website at <https://www.zextras.com>
- Zimbra Suite Plus can be obtained on the Zimbra website at <https://www.zimbra.com>

Software Installation

Once you obtain either Zextras Suite or Zimbra Suite Plus, follow this installation process:

- Copy the package to your server, in a directory owned by the root user.
- Unpack the package using `tar zxf`.
- Enter the newly created directory called either `zextras_suite-[version]` or `zimbra_suite_plus-[version]`.
- As root, run the installation script `./install.sh all`.
- Follow the installation wizard, accepting the software EULA and installing both the Core and the Zimlet component.
- Once the installation is complete, proceed with the Guide.



Installing Zimbra Suite Plus or Zextras Suite requires a mailboxd service restart, which will be performed during the installation.

Pre-migration Checks

Servers

- Source server: Any Zimbra server can be the source of your migration, provided that it's running Backup NG or Zimbra Suite Plus.
- Destination server: Any Zimbra server can be the destination of your migration, provided that it's running Backup NG.

Storage

- Source server: If Backup NG is not currently enabled on the source server, make sure you have an amount of free disk space *comparable* to the size of the `/opt/zimbra/store/` folder (the exported data is compressed through the gzip algorithm, and all zimbra items are deduplicated, usually reducing the size of exported to the 70% of the original size).
- Destination server: Make sure you have an amount of free space greater than the size of the `/opt/zimbra/store/` and of the `export` folders on the source server combined.

Data Transfer

While you can choose to transfer the data in any way, rsync is our method of choice as it's a good compromise between speed and convenience.

The main data transfer is executed while the source server is still active and functional. However, since the transfer is performed via the network, carefully plan your transfer in advance so that you'll have transferred **all of your data** before migrating.

Alternative Ways to Transfer Your Data

Anything spanning from remote mount to physical move of the drive is ok, as long as it suits your needs.

Never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway.

--Tanenbaum, Andrew S. (1996). Computer Networks. New Jersey: Prentice-Hall.
p. 83. ISBN 0-13-349945-6.

DNS

Set the TTL value of your MX record to 300 on your **real** DNS. This will allow a fast switch between source and destination servers.

Setting up the Migration

Step 1: Coherency Checks

To avoid any possible data-related issues, run the following checks on the source server:

- [zmblobchk](#): Checks the consistency between Zimbra's metadata and BLOBS.
- [zmdbintegrityreport](#): Checks the integrity of the Zimbra's database.

Repair any error found as described in Zimbra's official documentation.

Running a reindex of all mailboxes is also suggested.

Step 2: Network NG Setup

Disable the Real Time Scanner on both servers:

```
zxsuite backup setProperty ZxBackup_RealTimeScanner false
```



A dedicated device for the data export is strongly recommended to improve the export performance and to lower the impact on the performance of the running system.

Any device must be mounted on the `/opt/zimbra/backup/` path, and the Zimbra user must have r/w permissions on it.

Step 3: Data Export (SmartScan)

Run a SmartScan on the source server:

```
zxsuite backup doSmartScan
```

All of your data will be exported to the default backup path (`/opt/zimbra/backup/ng/`).

Pro-Tip: Single Domains Export

You can also choose to only migrate one or more domains instead of all of them. To do so, run the following command **instead** of the SmartScan:

```
zxsuite backup doExport /path/to/export/folder/ domains  
yourdomain.com,yourdomain2.com[...]
```

Mind that if you start with the **SmartScan** method, you'll have to carry on the migration with such method. If you start with the **Single Domains** method ,you'll have to carry on the migration with this one. The two methods cannot be mixed.

Data Export (SmartScan) via the Administration Zimlet

You can also choose to export your data using the Administration Zimlet as follows:

Step 4: Data Synchronization



When you move the exported data to the destination server, make sure that the destination folder is not Backup NG's backup path on the destination server, to avoid any issues if you already use Backup NG or plan to do so on the destination server.

(You can skip this step if you choose to transfer your data by other means than rsync.)

Using `rsync`, copy the data contained in `/opt/zimbra/backup/ng/` to a directory in the destination server (make sure the Zimbra user has r/w permissions on the folder). Use a terminal multiplexer like `screen` or `tmux`. This process command might need A LOT of time depending on network speed and amount of data involved.

```
[run this command as Root]  
rsync -avH /opt/zimbra/backup/ng/ root@desinationserver:/path/for/the/data/
```

Alternate Synchronization Method

While the suggested method is great for high-bandwidth situations, the first synchronization can involve a lot of data. If you feel that the rsync method is too slow, you might consider a physical move of the device (or the proper disk file if running on a virtual environment).

After moving the disk, you can remotely mount it back to the source server (e.g. via SSHFS), as the additional synchronizations needed for the migration will involve much less data. In this case, be sure to remount the device on the source server as `/opt/zimbra/backup/ng/` with all due permissions.

Step 5: First Import

Import all exported data to the destination server:

```
zxsuite backup doExternalRestore /path/for/the/data/
```

Now sit back and relax while Network NG imports your data on the destination server.

"Warning: Do not edit or delete the backup path after this step."

First Import via the Administration Zimlet

You can also choose to import your data using the Administration Zimlet. While importing via the Administration Zimlet, be sure to remove all system accounts (like GalSync, Ham, Spam, Quarantine etc.) from the imported account list.

Step 5 (alternate): First Import for Large Migrations

If you are to migrate a very large infrastructure where an export/import lasts for hours or even days, there is an alternative way to handle the migration from this point forward.

Instead of importing all of your data to the destination server, you can run a **Provisioning Only** import that will only create domains, Classes of Service and accounts on the destination server, skipping all mailbox contents.

```
zxsuite backup doExternalRestore /path/for/the/data/ provisioning_only TRUE
```

After doing this, switch the mailflow to the new server and, when the switch is completed, start the **real** import.

```
zxsuite backup doExternalRestore /path/for/the/data/
```

This way, your users will now connect to the new server where new emails will be delivered while old emails are being restored.

This approach has its pros and cons, namely:

Pros

- Since items are only imported once and never modified or deleted afterwards, using this method will result in less discrepancies than the **standard** incremental migration.
- This is the option that has less impact on the source server (e.g. good if you are in a hurry to decommission it).

Cons

- Depending on the timing of the operation, this method has a higher impact on your users due to the fact that items are restored WHILE they work on their mailbox.
- Since the import is done on a running system, you might notice some slowdowns.

The Situation so Far

Right now, the vast majority of the data has already been imported to the destination server. The source server is still active and functional, and you are ready to perform the actual migration.

The Migration

Step 6: Pre-migration Checks

Before switching the mail flow, **ALWAYS** make sure that the new server is ready to become active (check your firewall, your DNS settings, your security systems etc.).

Step 7: The Switch

This is it, the migration moment has come! At the end of this step the destination server will be active and functional.

- Repeat step 3, step 4 and step 5 (only new data will be exported and synchronized).
- Switch the mail flow to the new server.
- Once NO MORE EMAILS arrive to the source server, repeat step 3, step 4 and step 5.

The Destination server is now active and functional.

Step 8: Post-migration Checks

Run the following command to check for shares inconsistencies:

```
zxsuite backup doCheckShares
```

Should this command report any inconsistency, use the following command to parse the import mapfile used as the first argument and fix any broken shares.

```
zxsuite backup doFixShares
```

Mapfiles can be found in the backup path of the destination server as `map_[source_serverID]`.

Step 9: Galsync

Delete any imported GalSync accounts from the Zimbra Administration Console, then if needed, create new GalSync accounts on all the imported domains and re-sync all the GalSync accounts with the following command:

```
zmgsutil forceSync -a galsync.randomstring@domain.com -n [resourcename]
```

Step 10: Message Deduplication

Running a Volume Deduplication using HSM NG is highly suggested after a migration.

What Now?

- Initialize Backup NG on the new server to make sure all of your data is safe.

Incremental Migration FAQ

Q: Do I need a valid license to perform an incremental migration?

Yes. It can be either a trial License or a purchased one.

Q: What will be migrated?

Everything except for the server configuration. This includes:

- User data
- User preferences
- Classes of Service configuration
- Domain configurations

Q: Will I lose my shares? Will I need to re-configure all my shares?

Absolutely not!

Q: How should I transfer the exported data between my servers?

Again, anything that suits your needs is ok. You just need to be very sure about what your **needs** are.

Do you need to move the data very fast? Physically moving an USB disk between your servers might

not be a good idea.

Do you need to move the data in a very reliable way? Mounting the export folder via SSHFS to the destination server might not be a good idea if your internet connection is sloppy.

Zimbra Chat

About this document

This document is written for system administrators, and it aims to provide both an in-depth view of the product architecture to simplify troubleshooting and the knowledge necessary for solid customizations.

Overview

Zimbra Chat is included in Zimbra starting in version 8.7.6 as Beta software and version 8.8.0 as Stable. Zimbra Chat provides simple and direct text-only chat between Zimbra accounts. It is composed of a Zimlet and a Zimbra extension.

The Zimbra extension exposes an XMPP client so users can chat from a standard XMPP client instead of using the Zimlet through the Zimbra Web Client. Users can use both methods simultaneously.

General Architecture

Zimbra Chat is designed for Zimbra. It runs as a Zimbra Server Extension that implements an XMPP server and handles all the events shared between the clients. The Zimbra Chat Server Extension uses both XMPP and a custom protocol to communicate with the Chat Zimlet.

The server extension can handle multiple sessions for a single user, without limits. Each session has its own delivery queue to ensure that each session has exactly all of the events as any other session of the user.

Sessions are not limited by type (XMPP or Chat Zimlet). A user can use both the Zimbra Web Client and an XMPP client at the same time, without worrying about interferences between the sessions.

Components

Zimbra Chat is composed of two parts:

- Chat Zimlet
- Chat Extension

The Zimbra Chat Extension does not require the Chat Zimlet to work properly. The Chat Zimlet is designed and built to work only with the Zimbra Chat Extension.

Zimlet

The Chat Zimlet is the client component of Chat. It runs on the Zimbra Web Client and is managed like any other Zimlet. It is fully integrated in the Zimbra Web Client and uses the same graphics libraries. The Zimlet can work only with the Chat Extension because the Zimlet and Extension use a specific protocol to send and receive events. The Chat Zimlet is supported on all browsers and versions supported for the Zimbra Web Client.

Features:

- Zimbra Web Client integration.
- Manage the buddy list. Users can add, edit and remove buddies from the buddy list.
- Open each 'chat room' in a separate panel.
- Manage personal status.
- Send/Receive plain messages from users in the buddy list.
- Send presence status to users in the buddy list.
- View presence status of users in the buddy list.
- Support for Emojis (emoticons) on conversations. Emojis are provided free by EmojiOne <http://emojione.com/>.
- Send an entire conversation as email.
- Search conversations in the chat history (if enabled in the Extension options, see [Configuration Keys](#)).
- Get desktop notifications for any incoming message.

Extension

The Zimbra Chat Extension is the core of Zimbra Chat. It is a complete chat server that manages the events between connected clients.

It uses the ZAL to integrate into the mailboxd service of Zimbra.

The Extension can handle two types of connections:

- SOAP connections incoming from the Chat Zimlet, using Zimbra's SOAP infrastructure.
- XMPP connections from compatible clients.

Features:

- Handle events from multiple sessions.
- Handle SOAP connections for Chat Zimlet clients.
- Handle XMPP (plain and SSL) connections for compatible clients through a public port (see [Configuration Keys](#))
- Store the chat history for each conversation in a dedicated 'chat' folder in the user's mailbox (if enabled, see [Configuration Keys](#)).
- Store the relationships between users in the Zimbra database.

Installation

Zimbra Chat comes bundled with all Zimbra packages for version 8.8.0 and higher as a Zimbra package.

No dedicated installation steps are required.



In case the Zimbra Chat package was not installed during the system's installation or upgrade, please refer to the general documentation about package installation to install it.

Upgrade

Zimbra Chat is upgraded with the rest of the Zimbra platform.

No dedicated upgrade steps are needed.

Troubleshooting

This chapter helps the administrator find and solve any issues. If no solution is found, the administrator is guided through the process to report the issue.

Looking for Errors

This process is fundamental to locating the source of an issue and to find a solution or to correctly report it.

Chat Zimlet Error

To locate errors in the source code of the Chat Zimlet, enable developer mode on the Zimbra Web Client by modifying the URL of the Zimbra installation, appending `?dev=1` into the browser URL. Adding the `dev=1` parameter to the URL forces Zimbra to load the entire Web Client with all not minified sources, included the Zimlets. A longer load time should be expected.

During the loading of the Zimbra Web Client, open the browser developer tools.

In the browser developer tools console you will see logs from the Chat Zimlet. If an error occurs, it will be printed into the console.

If no errors are printed, but you see an unwanted behavior, enable the `break on exception` option in the developer tools. With that option enabled, if an error occurs, the execution of the software will be paused on the line where the error is generated.

If an error occurs, please escalate the issue by sending the file, the row and any details about the error through the appropriate channels.

If no errors are detected, please see the "Chat Extension Error" section.

Chat Extension Error

Any exception thrown by the Chat Extension is written into the `mailbox.log`. To check if there are any exceptions, please refer to the appropriate section of this guide.

If you can't find a solution for the exception in the FAQ, please report the issue through the appropriate channels, including the complete exception information.

Tools

Google Chrome Developer Tools

If the user is experiencing unexpected Zimlet behavior in the Zimbra Web Client, use Google Chrome Developer Tools to figure out the source of the issue.

To open the Google Chrome Developer Tools: * Open the main menu. * Find the [Other tools](#) menu option. * Select [Developer Tools](#).

A new panel with many tabs should appear. These tabs are:

- Console:: Like the server console, this tab will display some log information and allow you to interact with the JS Runtime.
- Network:: This tab will show any network activity, and it can be used to identify the requests to the mailbox and the responses from it.

Firefox Developer Tools

To open the Firefox Developer Tools, open the main menu and click the [Developer Tools](#) button.

A new panel with many tabs should appear. These tabs are:

- Console:: Like the server console, this tab will display some log information and you allow to interact with the JS Runtime.
- Network:: This tab will show any network activity, and it can be used to identify the requests to the mailbox and the responses from it.

Gathering System Information

Gathering System information is a vital part of the troubleshooting process. This section helps the administrator collect useful system information required to correctly report an issue (as described in the "How to escalate and issue" section).

Zimbra Version

To see the version of Zimbra, type this command:

```
# As zimbra
zmcontrol -v
```

Extension and Zimlet Version

To see the version of the Extension and the Zimlet, type this command:

```
# As zimbra
java -cp /opt/zimbra/lib/ext/openchat/openchat.jar com.zextras.lib.OpenChat
```

List of the Deployed Zimlets

To see the list of deployed Zimlets, type this command:

```
# As zimbra
zmzimletctl listZimlets
```

List of the Zimlets Enabled for the User

To see the list of Zimlets enabled for a user, type this command:

```
# As zimbra
zmprov getAccount user@domain.tld zimbraZimletAvailableZimlets
```

List of Zimlet User Preferences

To see the list of the preferences for the Zimlets enabled for a user, type this command:

```
# As zimbra
zmprov getAccount user@domain.tld zimbraZimletUserProperties
```

F.A.Q.

Chat Zimlet Issues

The Chat Zimlet is not working after the user login, and I see some JavaScript Errors. What can I do?

This is most commonly caused by caching issues. Refresh all the caches with these commands:

```
# As zimbra
zmprov flushCache -a zimlet com_zextras_chat_open
```

If the problem persists, escalate the issue.

The Chat Zimlet doesn't start at login, and a popup appears informing the user that the server is not available. What can I do?



Remember that the Chat Zimlet will not start if the logged user is using the delegated access feature (e.g. View Mail button from the admin console) to protect the privacy of the user.

Check to see if the Chat Extension is loaded correctly in the `mailbox.log` (see the appropriate section of this guide about how to read the `mailbox.log`).

Loading of the Zimbra Extension is granted by the following lines at the mailbox startup:

```
xxxx-xx-xx xx:xx:xx,xxx INFO [main] [] mailbox - OpenChat starting ...
xxxx-xx-xx xx:xx:xx,xxx INFO [main] [] extensions - OpenChat started
```

If the problem persists, report the issue, including the exception in the report.

Another Zimlet is using the sidebar, and a user cannot see the Chat buddy list. What can I do?

The Chat Zimlet uses a container that can be used by other Zimlets. To avoid collisions, try to detect if that container is used or not.

The Chat Zimlet uses an internal `black list` to detect incompatible Zimlets and disable the sidebar mode, switching to the docked mode.

The detection may fail if the Zimlet using the sidebar container is not indexed in the internal blacklist.

If the problem persists, report the issue, mentioning the name of the conflicting Zimlet.

If a user is stuck in the sidebar mode and another Zimlet has taken control of the sidebar, you can reset the Zimlet user setting to use the docked mode with these commands:

```
# As zimbra
# Reset the involved zimlet user preference:
zmprov modifyAccount user@example.com \
    -zimbraZimletUserProperties "com_zextras_chat_open:zxchat_pref_dockmode:FALSE"
zmprov modifyAccount user@example.com \
    -zimbraZimletUserProperties "com_zextras_chat_open:zxchat_pref_dockmode:TRUE"
# Set the zimlet user preference to dock mode:
zmprov modifyAccount user@example.com \
    +zimbraZimletUserProperties "com_zextras_chat_open:zxchat_pref_dockmode:TRUE"
```

Then reload the Zimbra Web Client to apply the modifications.

If the problem persists, report the issue.

Chat Extension Issues

Server to server messages are not delivered between the two servers. What can I do?

This issue can be caused by connection issues between two mailboxes. Verify that the port **5269** is opened on each server and that the servers can connect to each other.

To verify if the port is opened on the server, a simple check can be done by trying to connect to port **5269** using a telnet client.

If everything seems to work properly, open the **mailbox.log** on both servers and try to send an event (e.g. a text message). If an exception appears, see if it provides a hint on the error. If there is no meaningful exception, report the issue and include the exception in the report.

How to Escalate an Issue

If you found an issue and are not able to fix it, the following information is vital to report:

- A detailed description of the issue: What you are expecting and what is really happening?
- A detailed description of the steps to reproduce the issue.
- A detailed description of the installation and the environment: (see "Gathering System Information" section of this guide)
 - Server information: CPU, RAM, number of servers and for each server:
 - Zimbra Version
 - Chat Version
 - List of the installed Zimlets
 - Client information:
 - Browser name and version
 - Connectivity used between the servers and the client
 - Client Skin (theme)
 - Client Language
 - List of the Zimlets enabled for the user
- Any log involved for the issue:
 - **mailbox.log**

You can remove any personal information to protect users' privacy.

Advanced Topics

Sizing

Stress tests are being performed on Zimbra Chat.

We have noticed an increment of the workload stimabe at most 7% in an Zimbra installation with 20000 users.

The history feature of the Zimbra Chat Extension has the most impact. When a message is sent, a

mime message is either created or updated, meaning few kilobytes are read or written and some database queries are performed.



We suggest disabling history in very large deployments. To edit the configuration see [Configuration Keys](#).

Configuration Keys

The Chat Extension is easily configurable through the Zimbra CLI. All of the configurations are stored in LDAP.

To edit an account configuration, run these commands:

```
# As zimbra
zmprov modifyAccount account@example.tld {propertyName} {value}
```

zimbraChatServiceEnabled

[boolean], Default value: `true`.

Enable the Chat Service.

Can be applied to:

- * Global
- * Server

zimbraChatHistoryEnabled

[boolean], Default value: `true`, requires a mailbox restart to be applied.

Enable the chat history writing inside the chat folder.

Can be applied to:

- * Cos
- * Account

zimbraChatConversationAuditEnabled

[boolean], Default value: `false`.

Enable the dedicated log for the chat conversations.

Can be applied to:

- * Global
- * Domain

zimbraChatXmppSslPortEnabled

[boolean], Default value: **false**, requires a mailbox restart to be applied.

Enable the XMPP legacy SSL port.

Can be applied to:

- * Global
- * Server

zimbraChatAllowUnencryptedPassword

[boolean], Default value: **false**.

Allow unencrypted password login via XMPP.

Can be applied to:

- * Global
- * Server

zimbraChatXmppPort

[port], Default value: **5222**, requires a mailbox restart to be applied.

The XMPP standard port, usually used with StartTLS.

Can be applied to:

- * Global
- * Server

zimbraChatXmppSslPort

[port], Default value: **5223**, requires a mailbox restart to be applied.

The XMPP legacy SSL port.

Can be applied to:

- * Global
- * Server

zimbraChatAllowDlMemberAddAsFriend

[boolean], optional.

Add every member of the distribution list as buddies to each other.

Can be applied to:

- * Distribution list

Logs

mailbox.log

Mailbox log is a standard Log4j log. Here are some sample rows of a [mailbox.log](#):

```
xxxx-xx-xx xx:xx:xx,xxx INFO [qtp1912962767-  
310:https://123.123.123.123:8443/service/soap/ModifyPropertiesRequest]  
[name=user@example.com;mid=6;ip=172.17.0.2;ua=ZimbraWebClient - GC58  
(Linux)/8.6.0_GA_1153;] soap - ModifyPropertiesRequest elapsed=4  
xxxx-xx-xx xx:xx:xx,xxx INFO [qtp1912962767-  
310:https://123.123.123.123:8443/service/soap/ZxChatRequest] [] extensions -  
user@example.com changed status to AVAILABLE  
xxxx-xx-xx xx:xx:xx,xxx INFO [qtp1912962767-  
310:https://123.123.123.123:8443/service/soap/ZxChatRequest] [] soap - ZxChatRequest  
elapsed=24
```

Each row is composed of these elements:

xxxx-xx-xx xx:xx:xx,xxx

Timestamp of the log row.

INFO

The type of the log row.

qtp...ModifyPropertiesRequest

Information on the threads that requested to write the log row, which is usually the handler that triggered the log row.

name=...

Information on the user session.

soap -

Source of the log row.

ModifyPropertiesRequest elapsed=4

The content of the log row.

zmmailboxd.out

Mailbox log is a standard Log4j log. Here are some sample rows of a [zmmailboxd.out](#):

```
xxxx-xx-xx xx:xx:xx.xxx:INFO:oejs.SetUIDListener:main: Opened  
ServerConnector@397fbdb{HTTP/1.1}{0.0.0.0:8080}  
xxxx-xx-xx xx:xx:xx.xxx:INFO:oejs.SetUIDListener:main: Opened  
ServerConnector@36ebc363{SSL-http/1.1}{0.0.0.0:8443}  
xxxx-xx-xx xx:xx:xx.xxx:INFO:oejs.SetUIDListener:main: Opened  
ServerConnector@54d9d12d{SSL-http/1.1}{0.0.0.0:7071}
```

Zimbra Connect

What is Zimbra Connect

New for Zimbra Collaboration 8.8.15, Zimbra Connect integrates a fully fledged corporate instant messaging platform inside the Zimbra WebClient, including Group and Corporate Messaging, File Sharing, Screen Sharing and informal Video Chat capabilities.

Differences with Zimbra Talk V2

The main differences between Zimbra Connect and Zimbra Talk V2 implementation are the following:

Table 60. Back-end

Zimbra Talk V2	Zimbra Connect
Supports XMPP	No XMPP Support
No dedicated API Set	Features a dedicated API set and client protocol
Client/Server communication is SOAP-based	Client/Server communication is based on WebSockets

Table 61. Front-end

Zimbra Talk V2	Zimbra Connect
User interaction is based on a buddy list	User interaction is based on the GAL
Buddy-list-based minimal UI	History-based minimal UI
Bulkier, more crowded UI	Lighter, less cluttered UI
Space settings are defined in the Space itself	Space settings are defined by the Space's "General" channel
User-based video and audio feed control - users can autonomously mute/stop other user's audio and video feed only affecting themselves.	Host-based video and audio feed control - host can mute a participant or stop a video feed affecting all participants. Users can still mute/stop their feeds.

Table 62. Features

Zimbra Talk V2	Zimbra Connect
File exchange is available in Chats, Groups, and Channels	File exchange is available in Chats and Groups starting with Zimbra 8.8.15p3
Instant Meeting is available	Instant Meeting is available starting with Zimbra 8.8.15p1

Frontend Features

Zimbra Connect includes the following front-end features:

- Message delivery and read awareness
- 1-to-1 Instant Messaging
- Group Messaging
- Corporate Messaging (Spaces and Channels)
- Group Video Calls
- Channel Video calls
- File Sharing
- Screen Sharing
- Emojis

Backend Features

Zimbra Connect includes the following backend features:

- COS and User availability
- Built-in TURN server compatibility
- No core installation needed. Zimlet installation through a package manager.
- No configuration required
- Peer-to-Peer WebRTC protocol to avoid server load
- Dedicated audit log

Licensing

Zimbra Connect is licensed on a per-user basis. License information is included in the Network Edition license file just as for any other Zimbra NE feature. Global Admins can enable its Advanced features for any number of users up to the limit allowed by the license, and only "advanced" users count towards any licensing limit.

The total number of users who have the Advanced features active can be seen in the output of the `zxsuite core getLicenseInfo` command under `teamChatActiveCount`:

```
zimbra@129efa51bd95:~$ zxsuite core getLicenseInfo

  dateStart          2019-06-11 00:00:00 UTC
  dateEnd            2019-12-31 17:00:00 UTC
  expired            false
  type               regular - Network Edition
  [...]
  teamchatActiveCount 999
  [...]
```

This count is updated every 15 minutes.

Zimbra Chat and Zimbra Connect

Zimbra Chat and Zimbra Connect are neither compatible nor interoperable, meaning that the two products cannot coexist in any Zimbra NE infrastructure. The Zimbra Chat zimlet gets uninstalled during the installation process of the Zimbra Connect Zimlet package. However, Zimbra Connect includes all *basic* IM features provided by Zimbra Chat, which automatically gets enabled for all users who don't have access to the *advanced* Zimbra Connect features. *Advanced* users can use all of the product's features with other *advanced* users and can use 1-to-1 Instant Messaging with *basic* users. *Basic* users can use 1-to-1 features with all other users.

All users start as *Basic* users. Global and Delegated admins can enable *Advanced* features.

Zimbra Connect Zimlet installation

The Zimbra Connect Zimlet is available in the Zimbra repository and can be easily installed and upgraded through the operating system's package manager.

Zimbra Connect Zimlet installation on Red Hat and CentOS

To install the Zimlet on Red Hat and CentOS, run:

```
yum install zimbra-connect
```

Zimbra Connect Zimlet installation on Ubuntu

To install the Zimlet on Ubuntu, run:

```
apt-get install zimbra-connect
```

Installing the Zimlet removes any Zimbra Chat components from the server automatically.

Migrating from Zimbra Talk to Zimbra Connect

While Zimbra Talk and Zimbra Connect can coexist on a server, as their core components and Zimlets are compatible with each other, this is strongly discouraged as the two share the same Database, and to fully use Connect the database content must be migrated from Talk format to Connect format.

In order to migrate Talk data to Connect, use the `doImportChannels` command:

```
[zimbra@mailserver ~]$ zxsuite connect doImportChannels  
Syntax:  
    zxsuite connect doImportChannels [attr1 value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
delete_destination_before_import(0)	Boolean	true false

(M) == mandatory parameter, (0) == optional parameter

This operation can execute multiple times, but it's a one-way process and cannot be reverted. Once users are switched to Connect (by disabling the Talk Zimlet and enabling the Connect Zimlet), it's not possible to move their Connect data back to Talk.

URLs and Ports

To build URLs and links (e.g., for External Shares) Zimbra Connect uses the default Zimbra settings for the domain of the account in use - the `zimbraPublicServiceHostname` property is used for the URL itself while the `zimbraPublicServicePort` property is used for the port.

Should either of the two not be set up, the system falls back to the `zimbraServiceHostname` and `zimbraMailPort` or `zimbraMailSSLPort` server-level properties.

For Video Chats and Instant Meetings, the following rules apply:

- Zimbra Connect will work through firewalls and NATs as long as the peers can communicate each with the other - either directly or through a TURN server (which together with proper network rules is usually the solution to any WebRTC connection problem).
- When no TURN server is set up is not being used, a default STUN server is used so clients should be able to send outbound traffic to ports 19305/19307. The actual P2P connection is established between the clients on a random port between 0 and 65535 based on the client configuration and network.
- The default handshake/negotiation port used by most TURN servers is 3478 (incoming, UDP), but a different port can be used as long as it is properly set up - on the Zimbra Connect side the port is specified when adding the TURN server and the clients clients will be instructed to connect through it. The default P2P connection range when using a TURN server is 49152-65535 (usually configurable on the TURN side) so clients should be able to send data to that port range to the TURN server.
 - Most TURN servers can also be configured to use TCP instead of UDP.

Zimbra Connect administration

Zimbra Connect features can be enabled and disabled via the `zxsuite config` command line utility:

- Enable Zimbra Connect «Advanced» features
 - Property: `teamChatEnabled`
 - Available in: COS, account
- Enable or disable the chat history
 - Property: `historyEnabled`
 - Available in: global, server, COS, account
- Enable or disable Video Chat
 - Property: `videoChatEnabled`
 - Available in: global, server, COS, account

Browser compatibility

Zimbra Connect features are available on all browsers officially supported by the Zimbra Web Client, with some client-side limitations:

Browser	Quick Access Sidebar	Connect Tab	Videochat	Screen sharing
Internet Explorer 11+	No	No	No	No
Microsoft Edge	Yes	Yes	No	No
Mozilla Firefox	Yes	Yes	Yes	Yes
Google Chrome	Yes	Yes	Yes	Yes (w/ extension)
Safari	Yes	Yes	Yes	No

Google Chrome users must install the "Zextras Companion" extension to use the Screen Sharing feature, publicly available in the Chrome Web Store.

Firefox users must be sure to be running at least version 66 of the browser to be able to use the Screen Sharing feature.

UI

The Zimbra Connect UI is developed in Preact and seamlessly integrated with the Zimbra Web Client. It is composed of two client-side components: the Quick Access Sidebar and the fully-featured Connect Tab.

The Quick Access Sidebar allows for quick Instant Messaging, both for 1-to-1 and group conversations. Advanced Zimbra Connect features such as File Sharing and Video Chat are available in the IM Pane only for users who have the Zimbra Connect feature set enabled either at an account or COS level.

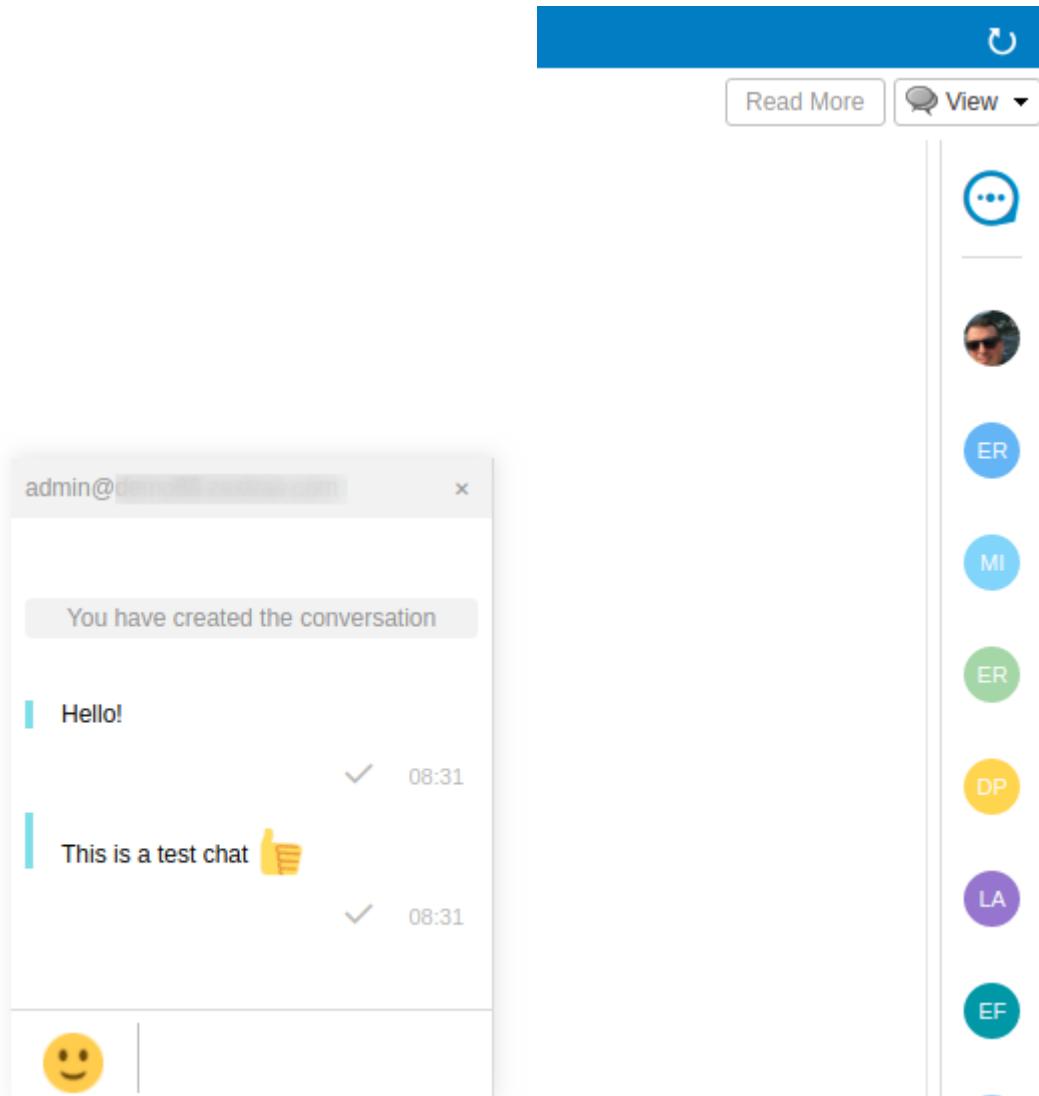
The Connect Tab is the full-sized Zimbra Connect UI, which contains all corporate instant messaging features such as Spaces and Channels. The tab itself is available for both Basic and Advanced users,

but corporate features are only available to Advanced users.

Quick Access Sidebar

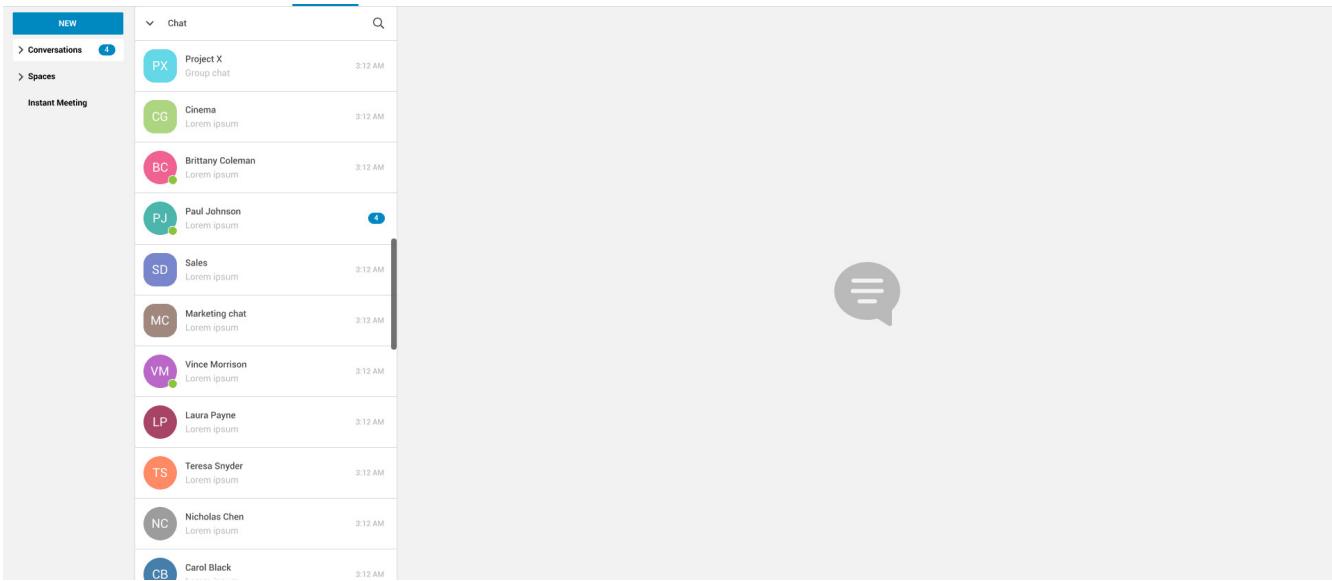
The Quick Access Sidebar displays the last people, groups, and channels the user has interacted with and allows to open a quick chat window with all of those.

It is available for both "Basic" users and "Advanced" users and provides additional features for the latter.



Connect Tab

The Connect Tab is a fully-fledged Zimbra feature tab that behaves similarly to all other feature tabs (e.g., Mail or Calendar).



Instant Messaging and Corporate Communication

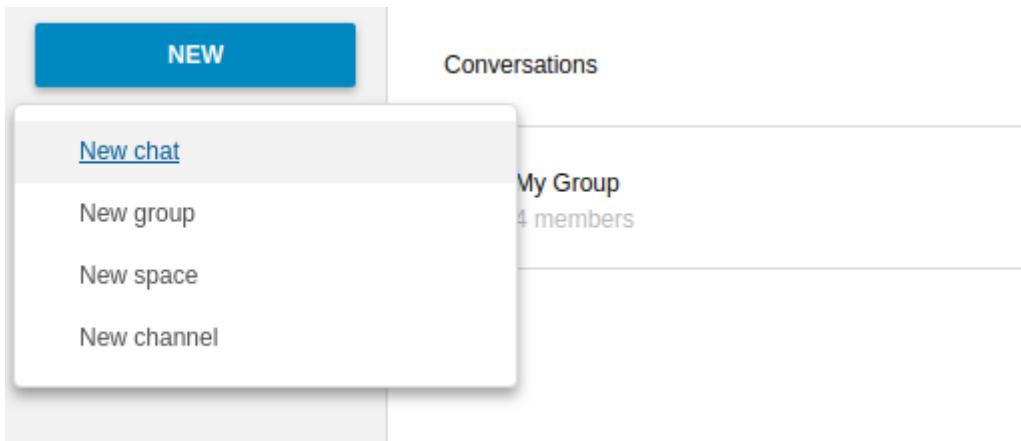
1-to-1 chat

One-to-one Chats can start from either the Quick Access Sidebar or the Connect Tab:

- on the former, select one of the available entries (based on your chat history) and start chatting with that person right away



- on the latter click on "New," then "New Chat" and select the person you want to chat with from the GAL



Recent 1-to-1 chats appear in the "Conversations" section of the Connect Tab and the Quick Access Sidebar (round icon).

Groups

Groups are how users communicate with multiple people at the same time (by default up to 5 total). Those are non-persistent entities not tied to any specific space. Any user can create a group inviting people, and any group member can invite more people in the same way. When all users leave a group, the group itself ceases to exist.

Groups Features

- A user in a Group can add more users to the Group itself up to the allowed limit.
- A user in a Group can chat with all of the others. All members of that Group can view all messages sent to the Group.
- A user in a Group can send files to all of the others. Files sent in a Group are available to all members of that Group.
- An user in a Group can start a video chat with all of the others. Group video chats can be joined at any time by all members of the Group.

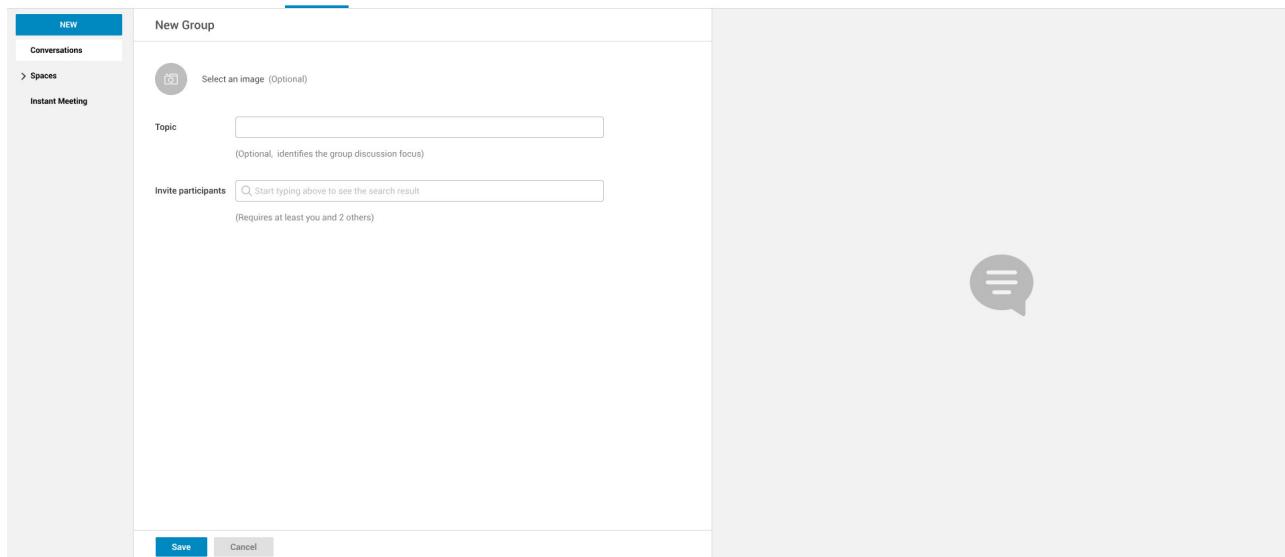
Global Administrators can change the allowed maximum number of group members in the Zimbra Connect section of the Global Settings in the Admin Console.

Groups UI

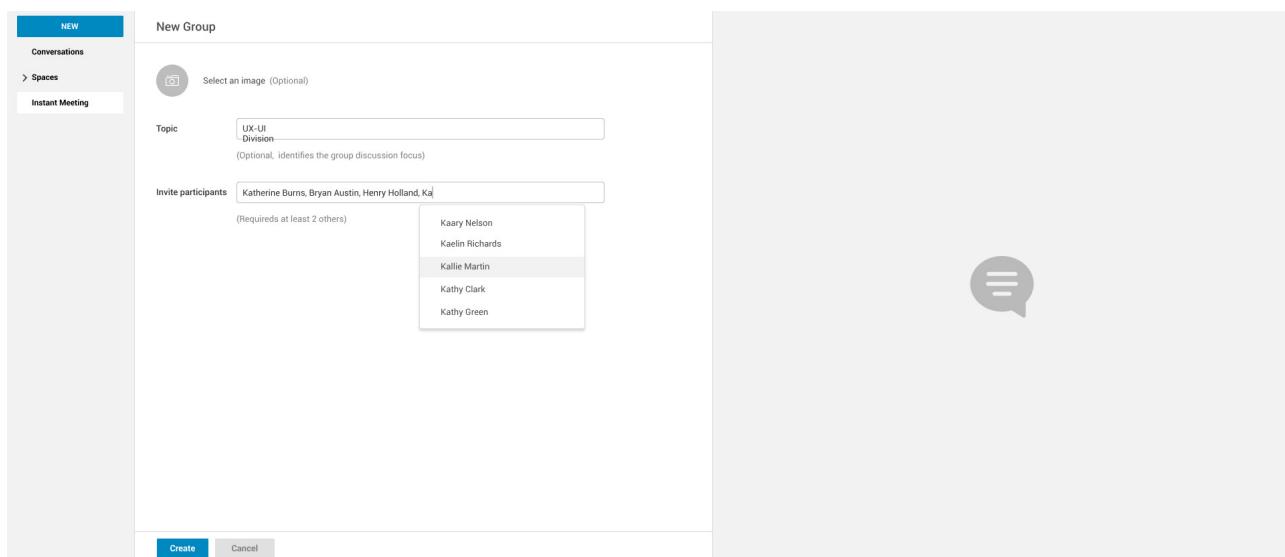
Recent Group chats appear in the "Conversations" section of the Connect Tab and the Quick Access Sidebar (rounded square icon).

- Creating a Group

To create a new Group, click on the "New" button in the Connect Tab, and select "New Group."

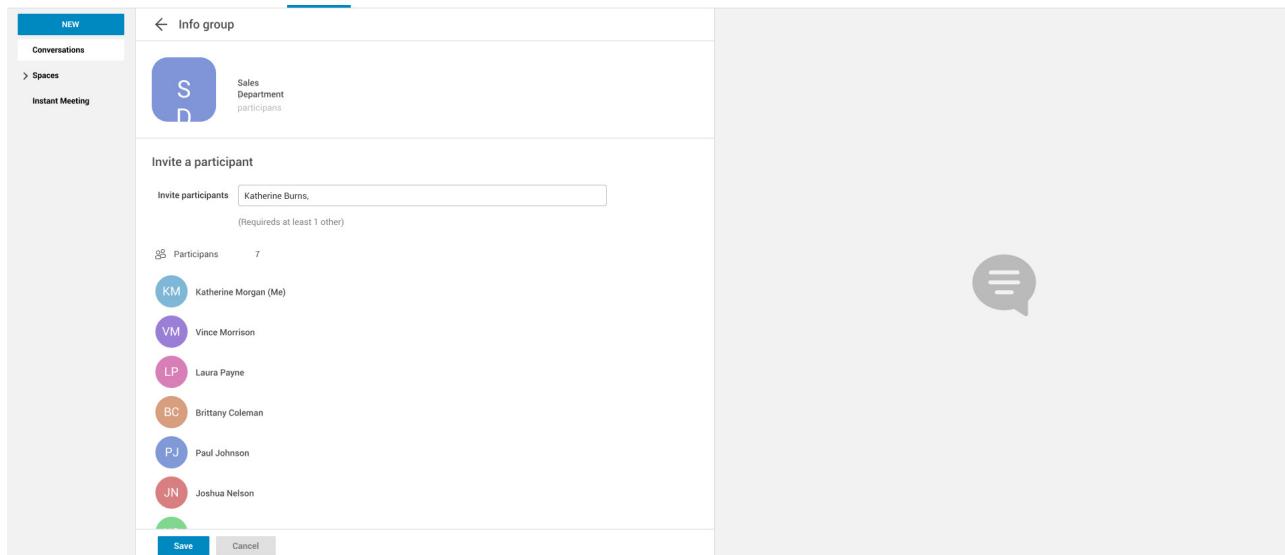


then, add the Group's title, select the buddies you wish to invite and click on "Create."



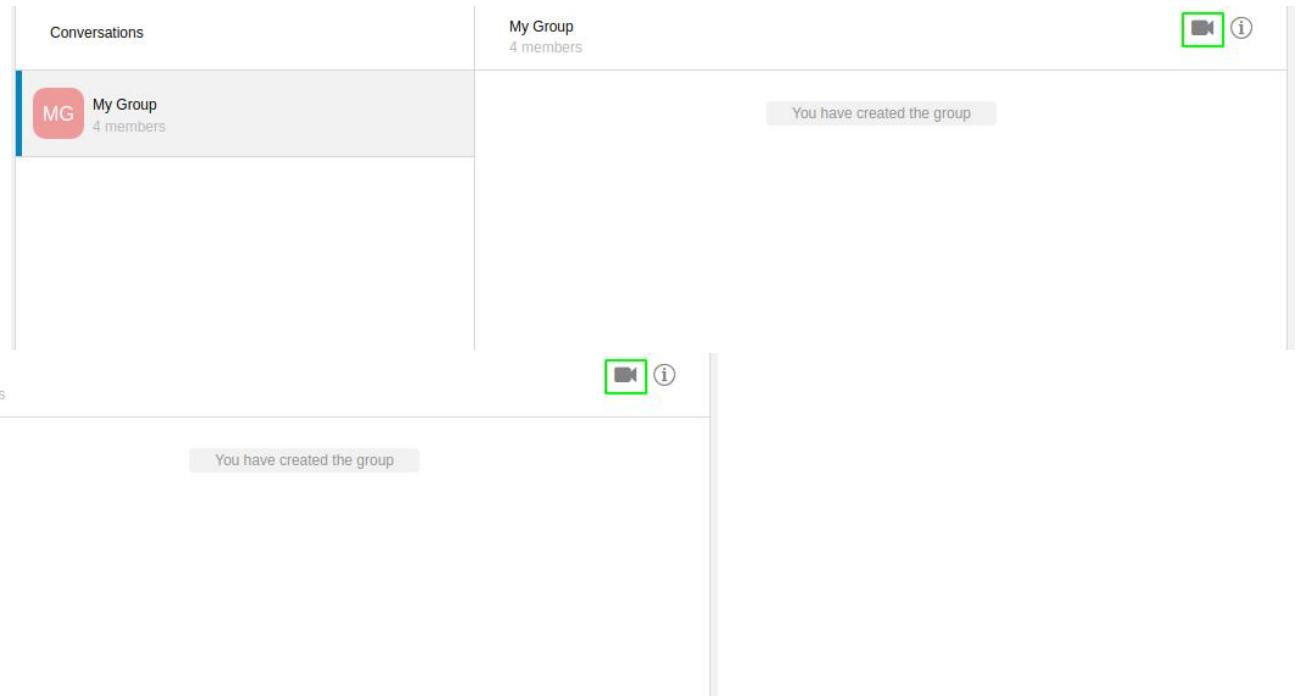
- Inviting a participant to a Group

To invite one or more buddies to a Group expand the Group's Info, select the users to be added and click on "Save."



- Starting a Group Video Chat

To start a Group video chat, click on the "Camera" icon on the top of the Group's chat window.



Any member of the Group can join the call at any time by clicking on the same button.

- Leaving a Group

To leave a Group, first, click on "Leave Group" in the Group's Info



My Group

Add participants

Leave group



Participants

4



test1@example.com

Last seen Today at 12:43 PM



test2@example.com

Last seen Today at 12:43 PM



test3@example.com

Last seen Today at 12:43 PM

then, click on "Yes" under the warning message.

Leave group

X

Are you sure to leave the group?

Yes

No

Spaces

Spaces are a themed container that can hold any number of Channels. Think of a Space as a community center where people gather to discuss different topics in dedicated areas (named Channels).

Spaces Features

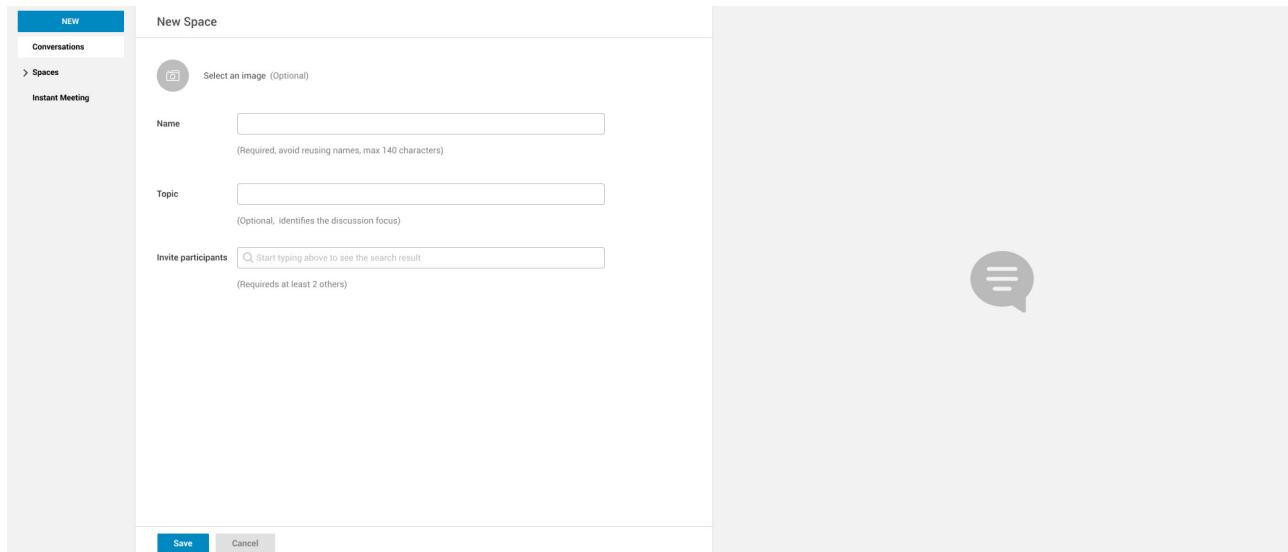
- Each space has a unique name and topic. You may change both the name and the Topic by clicking on the relevant field in the Space's settings.
- Members can leave a space at any time.
- Space Administrators can create new channels and invite new people to the space using the appropriate buttons.

Spaces UI

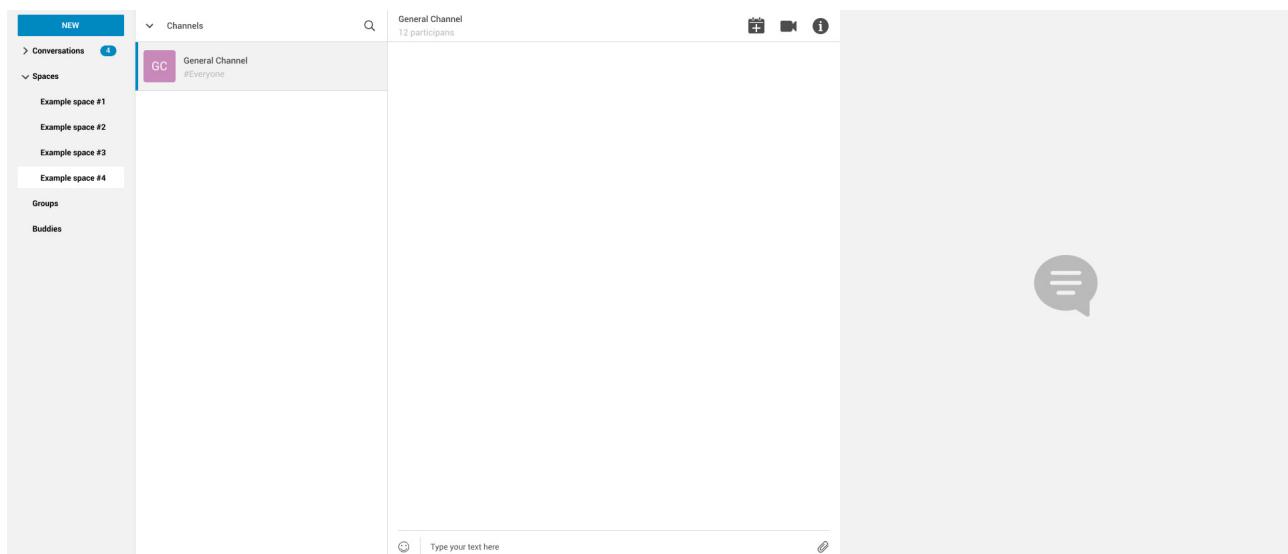
Spaces appear in a dedicated section of the Connect Tab, which gives access to all Space-related features:

- Creating a Space

To create a new Space, click on the "New" button in the Connect Tab, and select "New Space."



then, enter the Space's name and topic, select any users to invite and finally, click on "Save."



- Leaving a Space

To leave a Space, click on the "Leave Space" in the Space's General Channel Info.

Participants can leave a space at any time, while a Space Administrator can only leave a space if there is at least one other Space Administrator.

Both need to be invited to join the space again, and former Space Administrators get invited as regular participants but can be granted Administrator rights again.

Space Settings

The General Channel Info in each Space defines its settings (see below).

The Space's creator is also the first Space Administrator and can grant the same rights to any other user by clicking on the crown icon in the appropriate entry of the participant list.

The screenshot shows a participant list with four entries:

- Participants:** 4
- test1@example.com** (Last seen Today at 1:31 PM) - Has a red profile icon with 'TE' and green edit/crown icons.
- test2@example.com** (Last seen Today at 1:31 PM) - Has a green profile icon with 'TE' and blue edit/crown icons.
- test3@example.com** (Last seen Today at 1:31 PM) - Has a pink profile icon with 'TE' and blue edit/crown icons.
- admin@[REDACTED]** (Online) - Has a blue profile icon with 'AD' and a blue 'Administrator's Space' badge.

Only Space Administrators can invite new participants, create new channels, kick people, and delete channels within the space.

Channels

Channels are topic-defined areas inside of the same space. Those can contain any number of users, and unlike Groups, users can autonomously join any Channel in a Space they are in instead of being invited to it by a member.

Each new Space has a "General" channel automatically created within it, which defines the space's properties (e.g., Title and Topic) and which all users automatically join when they join the Space.

Channels Features

- A user in a Channel can chat with all of the others. All members of that channel can view all

messages sent on the Channel.

- A user in a Channel can start a video chat with all of the others. Channel video chats can be joined at any time by all members of the Channel.

Channels UI

Channels appear in Spaces within the Connect Tab, and all of the Channel-related features are managed there, by:

- Creating a Channel

To create a new Channel, click on the "New" button, and select "New Channel."

The screenshot shows a user interface for creating a new channel. On the left, a sidebar has a 'NEW' button at the top, followed by sections for 'Conversations', 'Spaces' (which is expanded), and 'New Space'. In the main area, the title 'New channel' is displayed above input fields for 'Name' and 'Topic'. Below these fields is a note: 'Select a space to create a channel Required. Channels are always linked to a space'. At the bottom of the form is a blue button labeled 'NS' and 'New Space'.

then select:

1. the Space that should contain the Channel (*mandatory*)
2. the Channel's name (*mandatory*)
3. the Channel's topic (*optional*)

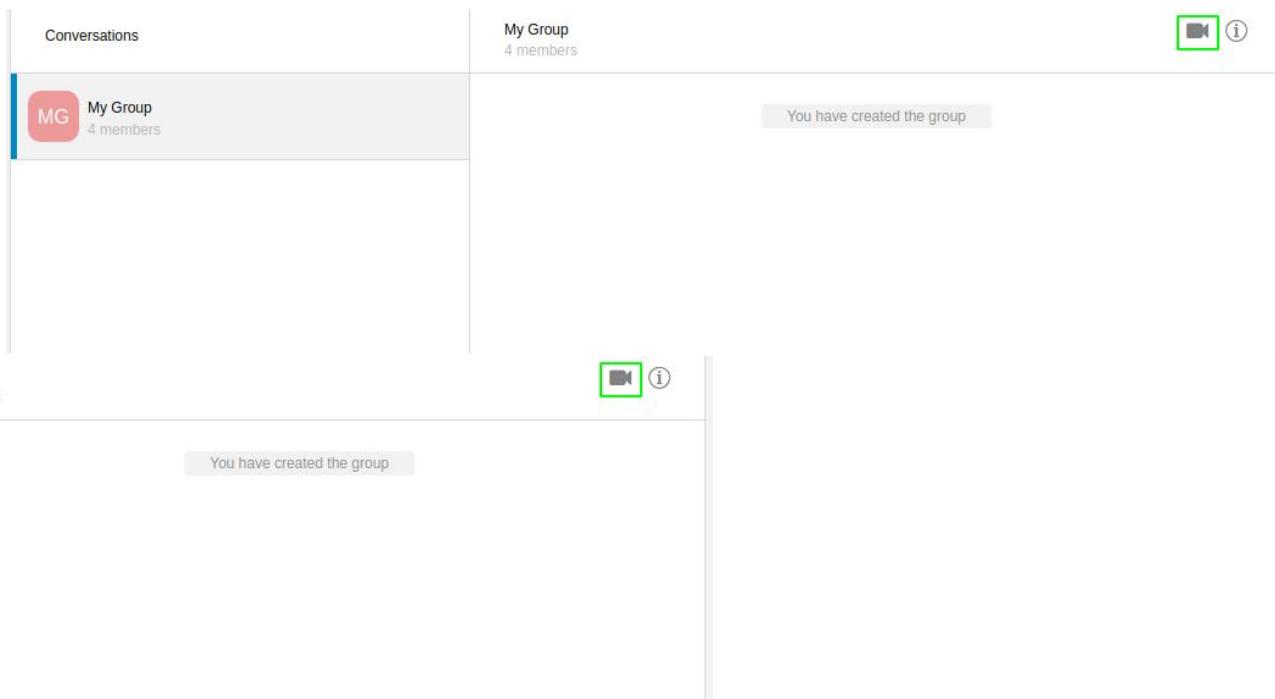
finally, click on "Save."

- Joining a Channel

To join a Channel, click on the Channel label and then on "Join Channel."

- Starting a Channel video chat

To start a Channel video chat, click on the "Camera" icon on the Channel's chat window.



Any member of the Channel can join the call at any time by clicking on the same button.

- Leaving a Channel

To leave a Channel, first, click on the red "Leave Channel" entry in the Channel's Info

◀ Channel Info



Frontend
The best team ever!

➡ Leave this channel

Participants

3

Both normal users and Space Admins can leave a channel at any time and join it afterward.

File sharing

Users can easily share files via Connect to Chats and Groups by dragging and dropping the files directly into the chat interface (both in the minichat and in the Connect tab) or by clicking the "paperclip" icon on the right of the message input field. Multiple files can be uploaded at once, and image files will show a preview of the file while other common filetypes will display a custom icon.

Clicking on a file within a chat window will download it to the local client using the browser's own download interface.

Files shared via Connect will be stored inside a protected folder the sender's Drive, thus counting towards the sender's mailbox quota, and will remain available for download in the chat window for all participants until deleted from Drive by the sender.

Video Chat

Video Chat features are available in 1-to-1 chats, Groups, and Channels, allowing multiple people to communicate in real-time using a webcam and a headset, as well as allowing them to share their screen with all other attendees.

The WebRTC protocol is the foundation for this feature. WebRTC is a peer-to-peer auto-adaptive technology that allows clients to communicate directly without overloading the server. Call quality is automatically tweaked based on the available bandwidth, with the maximum quality being *Full HD* for both video and audio. When starting their first video chat, users need to grant their browser access permissions to their camera and microphone.

Video Chat UI



The video chat UI has three main areas:

- The center displays video streams with a single (main) stream on the top and multiple secondary streams on the bottom. The total number depends on the screen's resolution and window size.

- On the left is the Group's or Channel's instant messaging chat. This chat is visible and entirely usable, and its history gets retained in the group's or channel's chat history.
- On the bottom left appear the user's video feed and controls (disable video, mute microphone, and share screen).

Users can disconnect from an ongoing video chat by pressing the "Hang up" button in their video stream's frame on the bottom left of the screen. Whenever a video chat is on, users belonging to the Group or Channel of the video chat see a "Call in progress" message below the name of the Group or Channel and may join by clicking on the "Camera" icon in the chat.

Video Stream Control

Video streams are displayed in a "first come, first served" basis according to the connection order between the peers.

Every participant can mute their audio stream or stop their video stream.

Screen Sharing



When clicking on the Screen Share button, a pop-up window appears asking the user whether to share their entire screen or just a specific window. After choosing, the screen sharing feed replaces the user's webcam feed for all participants.

Instant Meetings

Instant Meetings are one-shot Video Chats that can be attended by external users as well as internal users. Only users with the Advanced Connect features enabled can start Instant Meetings, but any internal or external user can attend.

To create an Instant Meeting, click on the "New" button in the Connect Tab, and select Instant Meeting.

Then, fill in the attendee list by entering any internal or external email address in the text box and pressing enter to add it to the list. Once all attendees are added, press "Save" to send an email

notification to all participants and start the Instant Meeting.

Instant Meeting URLs

Both external and internal users can join an Instant Meetings through a dedicated URL that can be found both in the invitation email and in the information section of the Instant Meeting itself.

Such URLs are uniquely generated for each Instant Meeting and expire 10 minutes after the host leaves the meeting.

Instant Meeting UI

The Instant Meeting feature uses the very same UI as any internal Video Chat session.

Presence

Presence is managed automatically in Zimbra Connect: whenever a user logs in, regardless of whether the Connect Tab has the focus, they appear as **online**.

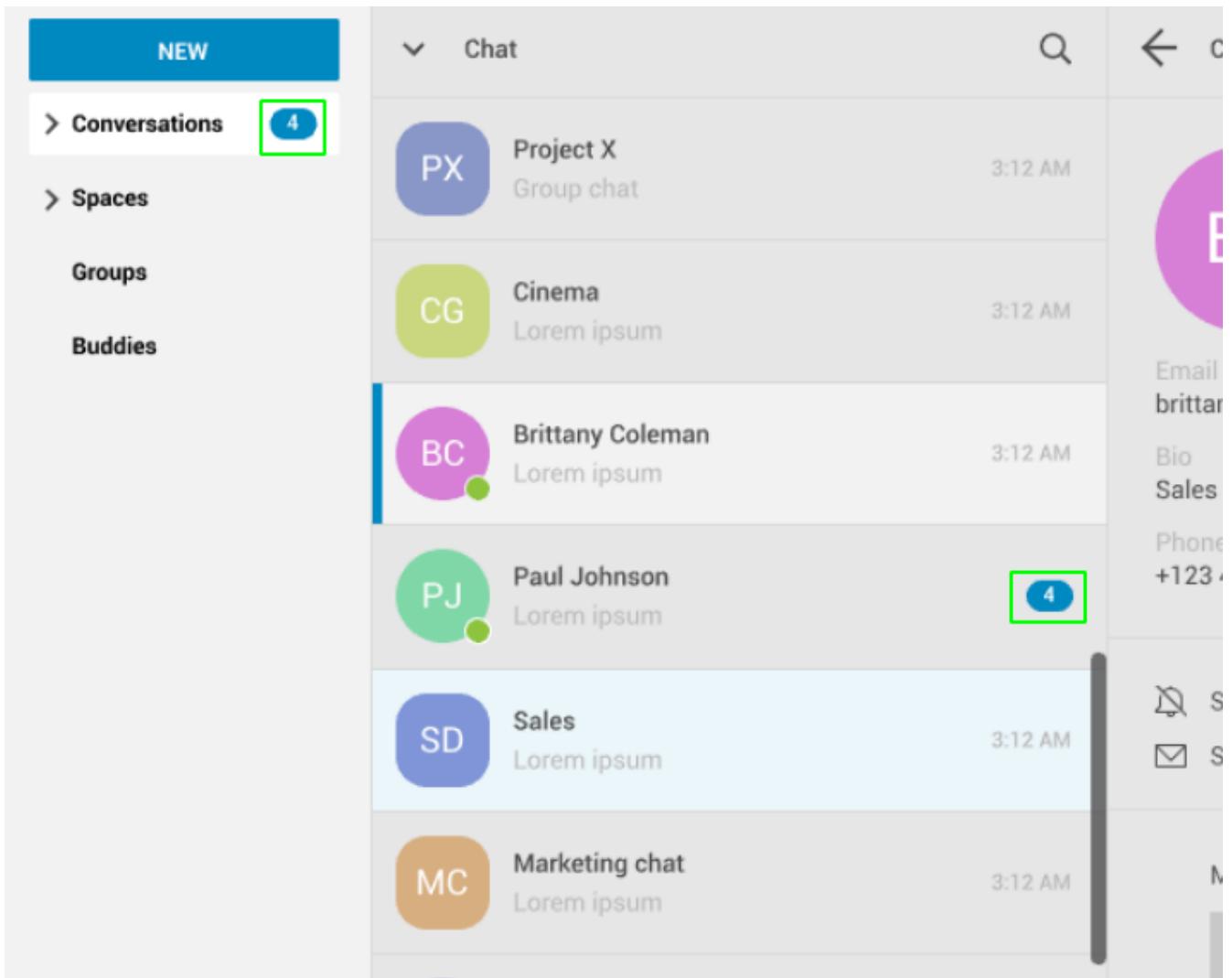
As part of the user presence system, all messages get displayed with a variable number of check symbols:



- 0 checks, message not delivered to the server
- 1 check, message delivered to the server
- 2 checks, message viewed by all users

Unread Messages

The number of unread messages in any conversation, Group or Channel appears on the right side of the conversation, Group, or Channel.



Chat History

Chat History for each 1-to-1 Chat, Group, and Channel is available in the very same window (e.g., enter a Channel to see all of that channel's history) and messages delivered to offline users appear in the appropriate IM conversation, Group or Channel.

STUN/TURN Server

Since WebRTC is a peer-to-peer protocol, all users in a video chat must be able to reach each other's client for the connections to get established.

Should this not be possible, because of NAT rules on the network or because of a Service Provider's policy, using a TURN server ensures proper communication between all peers. Zimbra Connect is designed to allow using a STUN/TURN server out of the box by simply adding the TURN server's URL and login information in the zimlet configuration.

Setting up Zimbra Connect to use a TURN server

A dedicated set of TURN configuration tools is available via CLI through the `zxsuite connect iceServer` command:

```
zimbra@mailserver:~$ zxsuite connect iceServer
```

Edit the list of ICE servers used to establish connections for video calls.
Configuration scope can be global(default), cos, or account.

```
add           - add ice server candidates using global (default), cos or
account

remove        - remove ice server candidates using global (default), cos
or account

get           - get ice server candidates using global (default), cos or
account

{turn:turn.example.com:3478?transport=udp} [attr1 value1 [attr2 value2...]]
```

```
zxsuite connect iceServer add
zxsuite connect iceServer remove
zxsuite connect iceServer get [attr1 value1 [attr2 value2...]]
```

The "add" subcommand is used to add a new TURN server:

Syntax:

```
zxsuite connect iceServer add {turn:turn.example.com:3478?transport=udp} [attr1
value1 [attr2 value2...]]
```

PARAMETER LIST

NAME	TYPE	EXPECTED VALUES
url(M)	String	turn:turn.example.com:3478?transport=udp
username(0)	String	myuser
credential(0)	String	mysecretkey
account(0)	String	user@example.com
cos(0)	String	default

(M) == mandatory parameter, (0) == optional parameter

Usage example:

```
zxsuite connect iceServer add turn:turn.example.com credential mysecret username
myuser
zxsuite connect iceServer add turn:turn.example.com credential mysecret username
myuser account testaccount@example.com
```

Multiple TURN servers can be added to handle different users or Classes of Service (defined through the **user** and **cos** optional parameters of the command above).

On the TURN-server side, it is strongly recommended to have a single user, authenticated with a

username and secret key, for ease-of-use reasons as a 1:1 correspondence between Zimbra users and TURN users is not necessary.

Zimbra Open Drive

Zimbra Open Drive is a client that interfaces Zimbra to third party products and services.



Prior to version 8.8.11, Zimbra Open Drive was known as Zimbra Drive.

Zimbra Open Drive currently works with:

- Nextcloud
- ownCloud



Data on Zimbra Open Drive is not hosted on the Zimbra server or on any other Zimbra product. Likewise, the data is not managed by Zimbra or any incorporated service. Therefore, Zimbra Support does not support issues related to Nextcloud and ownCloud servers.

About this Document

This document is written for system administrators, and it aims to provide an in-depth view of the product architecture and the knowledge necessary for solid customizations.

Zimbra Open Drive is included in Zimbra starting in version 8.7.6 as Beta software and version 8.8.0 as Stable. Zimbra Open Drive is provided as an included package of Zimbra Collaboration Suite, so Zimbra Open Drive can be installed during the Zimbra installation process.

The [Installation](#) and [Configuration](#) chapters cover the installation and the configuration of the product in the supported environments respectively.

The upgrade process and compatibility information is covered in the [Upgrade](#) chapter.

The [Uninstallation](#) chapter contains the procedure to uninstall Zimbra Open Drive. Advanced topics, such as how to build the software from the sources, are in the [Advanced Topics](#) chapter.



Backups, archiving, access security and user management is not done by or within Zimbra.

Malfunctions, data and access security as well as storage management and data archiving on any third party product is not managed by Zimbra or through Zimbra software nor falls under any Zimbra Support contract as stated in section 2.4(a) of Zimbra's "Maintenance & Support Terms and Conditions".

Overview

General Architecture

The purpose of Zimbra Open Drive is to connect the Zimbra end user to a cloud service, external to Zimbra.

Zimbra Open Drive has three parts: Zimbra Extension, Zimlet and Cloud App. These parts integrate

external storage services and an authentication mechanism into the Zimbra Web Interface. Each Zimbra account will be linked to the external storage service account.

Components

Zimbra Open Drive includes the following components:

1. Zimbra Open Drive Extension
2. Zimlet
3. Cloud App

Each component is mandatory and requires careful configuration. However, errors in installation or configuration won't affect Zimbra usability.

Extension

The Zimbra Open Drive extension is installed in the `mailboxd` component. The extension acts between the Zimbra Open Drive Zimlet and the Cloud App, providing services like authentication and item actions to the Zimlet.

Zimlet

The Zimbra Open Drive Zimlet adds a new *Open Drive* tab to the user Zimbra interface, before the Preferences tab. With the Zimlet, user can search in the linked cloud.

The Zimlet component is contained in the package `com_zextras_drive_open.zip`. The Zimlet name is `com_zextras_drive_open`.

Cloud App

The external services of cloud storage need a specific app with a dedicated API to communicate with the Zimbra Open Drive Extension. Zimbra Open Drive provides an app for each of the services supported.

Nextcloud/ownCloud

The Nextcloud/ownCloud app is a specific application for Nextcloud and ownCloud. It provides transparent authentication in ownCloud and Nextcloud using Zimbra credentials and a layer of compatibility that abstracts the version of ownCloud and Nextcloud for the extension.

Installation

This chapter guides the administrator through the manual installation of Zimbra Open Drive.

Requirements

- Root-level access to the underlying operating system.
- Administrative access to an external cloud supported service (see [Cloud App](#)).
Supported versions:

- Nextcloud 9, 10, 11
- ownCloud 9.0, 9.1, 10

Zimbra Packages Installation

This section describes how to install the Zimbra Open Drive Extension and the Zimbra Open Drive Zimlet.

Both the Zimbra Open Drive Extension and the Zimlet are installed through the official Zimbra installer. The Zimbra installer prompts you as follows:

```
Use Zimbra's package repository [Y] Yes  
...  
Install zimbra-drive [Y] Yes
```

Zimbra Already Installed

The Zimbra installation adds the Zimbra repositories to apt sources list, so Zimbra Open Drive can be installed through the following command:

```
# As root, when apt-get is available  
apt-get update  
apt-get install zimbra-drive  
# As root, when yum is available  
yum update  
yum install zimbra-drive
```

Hereafter, the Zimbra Open Drive Extension will be enabled with the zimlet deploy command and a mailbox restart:

```
# As zimbra  
zmzimletctl deploy /opt/zimbra/zimlets/com_zextras_drive_open.zip  
zmmailboxd restart
```

Cloud App Installation

Here are the steps to install the Zimbra Open Drive Cloud App to the specific supported cloud.

The cloud services currently supported are Nextcloud and ownCloud with the archive **zimbradrive.tar.gz**.

Nextcloud/ownCloud

Nextcloud and ownCloud require the same following installation steps.

The placeholder **PATHTO CLOUD** is the path of the Nextcloud/ownCloud service in server:

1. Copy `zimbradrive.tar.gz` in Nextcloud/ownCloud drive:
`scp zimbradrive.tar.gz root@cloud:/tmp`
2. In Nextcloud/ownCloud server, extract `zimbradrive.tar.gz` in `PATHTO CLOUD/apps`:
`tar -xvzf zimbradrive.tar.gz -C PATHTO CLOUD/apps`
3. Change permissions of the extracted folder `PATHTO CLOUD/apps/zimbradrive` with the user owner of Nextcloud/ownCloud (E.g.: www-data):
`chown -R www-data:www-data PATHTO CLOUD/apps/zimbradrive/`
4. Enable Zimbra Open Drive App from Nextcloud/ownCloud Admin Interface or with command:
`sudo -u www-data php PATHTO CLOUD/occ app:enable zimbradrive`

At this point, the Nextcloud/ownCloud Zimbra Open Drive App is installed and requires configuration.

On Apache Web Server, Zimbra Open Drive doesn't work if the server is not correctly configured. Refer to these instructions for *Apache Web Server Configuration* in the Nextcloud manual: [Nextcloud installation](#) or in the ownCloud manual: [ownCloud installation](#).

Configuration

Zimbra Open Drive configuration is split into the Zimbra side and the Cloud side. The Zimbra Open Drive Zimlet doesn't need more than standard Zimlet configuration, so the Zimbra side requires only Zimbra Open Drive Extension configuration. On the Cloud side, each supported cloud service configuration will be shown later. These are independent, and you need only configure for your desired cloud service.

Zimbra Extension Configuration

The Zimbra Extension setup requires the URL of the cloud service that will be paired. This URL has to be set in the domain attribute `zimbraDriveOwnCloudURL`, and it is common to all users belonging the same domain. Different domains may have different cloud service URLs.

The command to set the cloud service URL is:

```
# As zimbra
zmprov md domainExample.com zimbraDriveOwnCloudURL CLOUD_URL
```

The cloud service URL (`CLOUD_URL`) has to be in the form: `protocol://cloudHost/path`.

- `protocol`: can be `http` or `https`
- `cloudHost`: hostname of the server with the cloud service
- `path`: path in server of the targeted cloud service

Each cloud service has its entry point.

In Nextcloud/ownCloud, the URL has to target `index.php protocol://cloudHost/path/index.php`

Cloud App Configuration

Nextcloud/ownCloud

When everything is correctly configured, the Zimbra end user creates a private account in the cloud service that will be paired with the Zimbra user account. This new cloud account inherits the Zimbra user credentials and appears in the user's list of Nextcloud/ownCloud interface; however this account is not active until the Zimbra Open Drive app is enabled.

Nextcloud and ownCloud have the same following configuration entries. In the Nextcloud/ownCloud administration panel, it must appear as a new **Zimbra Open Drive** entry in the left sidebar that redirect to the configuration view. There are the following configurations:

- (CheckBox) **Enable Zimbra authentication back end**
(Mandatory checked) On check, adds a configuration in config.php that lets Nextcloud/ownCloud use Zimbra Open Drive App class. On uncheck, removes this configuration.
- (CheckBox) **Allow Zimbra's users to log in**
(Mandatory checked) Allows Zimbra users to use Nextcloud/ownCloud with their Zimbra credentials.
- (InputField) **Zimbra Server**
(Mandatory) Zimbra webmail host or ip.
- (InputField) **Zimbra Port**
(Mandatory) Zimbra webmail port.
- (CheckBox) **Use SSL**
Check if the Zimbra webmail port uses SSL certification.
- (CheckBox) **Enable certification verification**
Disable only if Zimbra has an untrusted certificate.

- (InputField) **Domain Preauth Key**

After the Zimbra end user creates a private account with the first successful access in Zimbra Open Drive, he can log into the Nextcloud/ownCloud web interface using Zimbra credentials. In the Nextcloud/ownCloud web interface, he will find a Zimbra icon in the Apps menu that opens a new Zimbra webmail tab without a login step.

This feature works only if the Zimbra Domain PreAuth Key is copied. In Zimbra, run the following command to show the desired Zimbra Domain PreAuth Key:

```
# As zimbra
zmprov getDomain example.com zimbraPreAuthKey
# If response is empty, generate with
zmprov generateDomainPreAuthKey domainExample.com
```

Upgrade

This chapter guides administrators through the manual upgrade of Zimbra Open Drive. It's important to pay attention to the version of each component: the compatibility is granted only if each component has the same version.

The Zimbra Open Drive Zimlet and extension can be upgraded with Zimbra upgrade, but the Zimbra Open Drive App must be manually updated.

Zimbra Extension and Zimlet Upgrade

When Zimbra is upgraded, Zimbra Open Drive can be installed directly from the installation. Zimbra Open Drive can be kept upgraded in the same Zimbra major.minor versions with apt-get or yum:

```
# As root, when apt-get is available  
apt-get update; apt-get install zimbra-drive  
# As root, when yum is available  
yum update; yum install zimbra-drive
```

Cloud App Upgrade

Unlike the Zimbra Open Drive Zimlet and the Extension, the Zimbra Open Drive Cloud app has to be manually upgraded on every version change.

The upgrade of Zimbra Open Drive App in Nextcloud/ownCloud requires that files are replaced. Perform these steps at installation([Nextcloud/ownCloud](#)):

1. Copy `zimbradrive.tar.gz` in Nextcloud/ownCloud drive
`scp zimbradrive.tar.gz root@cloud:/tmp`
2. In the Nextcloud/ownCloud server, extract `zimbradrive.tar.gz` in `PATHTOCLOUD/apps`:
`tar -xvzf zimbradrive.tar.gz -C PATHTOCLOUD/apps/apps`
3. Change permissions of the extracted folder `PATHTOCLOUD/apps/zimbradrive` with the user owner of Nextcloud/ownCloud (E.g.: www-data):
`chown -R www-data:www-data PATHTOCLOUD/apps/zimbradrive/`

On upgrade from version 0.0.1, remove the table `oc_zimbradrive_users` that are no longer used. In mysql, execute the following command:

```
DROP TABLE oc_zimbradrive_users;
```

Uninstallation

This chapter guides the administrator through the manual uninstallation of Zimbra Open Drive and cleanup of the system.

Disable Zimbra Open Drive Packages

Since the Zimbra Open Drive Extension and the Zimbra Open Drive Zimlet are installed as Zimbra packages, their uninstallation is unexpected. To disable Zimbra Open Drive, disable the Zimbra Open Drive Zimlet from the desired user, domain or class of service.

Remove Cloud App

Nextcloud/ownCloud

The removal of the Nextcloud/ownCloud App has two steps: clean up and app uninstall.

The clean up step deletes all Zimbra users' data from Nextcloud/ownCloud and is not reversible. It **requires** that Zimbra Open Drive is installed and enabled.

However, this clean up step can be skipped. The Zimbra Open Drive App can be uninstalled without removing the Zimbra users' data.

Clean Up

Before starting clean up, it's recommended to disable Zimbra users' access: the configuration **Allow Zimbra's users to log in** should be unchecked.

The following commands delete the users created by the Zimbra Open Drive App and clean up the table containing references to Zimbra users (replace correctly `mysql_pwd` and `occ_db`):

```
cd /var/www/cloud          # Go to the OCC path
mysql_pwd='password'       # database password
occ_db='cloud'              # database name for the Nextcloud / ownCloud

# In ownCloud
user_id_column='user_id'    # column name in table oc_accounts of ownCloud
# In Nextcloud
user_id_column='uid'        # column name in table oc_accounts of Nextcloud

mysql -u root --password="${mysql_pwd}" "${occ_db}" -N -s \
-e 'SELECT uid FROM oc_group_user WHERE gid = "zimbra"' \
| while read uid; do \
    sudo -u www-data php ./occ user:delete "${uid}"; \
    mysql -u root --password="${mysql_pwd}" "${occ_db}" \
    -e "DELETE FROM oc_accounts WHERE ${user_id_column} = '${uid}' LIMIT 1"; \
done
```

App Uninstall

The Zimbra Open Drive App can be removed from the Nextcloud/ownCloud Admin Interface. The configuration should be restored by unchecking **Enable Zimbra authentication back end**, then the Zimbra Open Drive App must be disabled from the **Enabled Apps**' tab and **uninstalled from the Disabled Apps`**.

With the previous steps, the Zimbra Open Drive App folder (`PATHTOCLLOUD/apps/zimbradrive`) is deleted but all the users' files still remain in the cloud service drive: any configuration or file that was not previously cleaned up is retrieved on reinstallation of the Zimbra Open Drive App.

Advanced Topics

Build from Sources

This section describes the steps to build the Zimbra Open Drive components. The official Zimbra Open Drive source repository is hosted on [GitHub.com/ZeXtras/zimbra-drive](https://github.com/ZeXtras/zimbra-drive).

The build system uses a relative path. The following example assumes that the working path is

/tmp/, but it can be changed at will.

```
# Clean the folder that will be used for the build
rm -rf /tmp/ZimbraDrive && cd /tmp/

# Clone the source repository
git clone --recursive git@github.com:ZeXtras/ZimbraDrive.git

# Jump into the source folder
cd ZimbraDrive

# Checkout the correct branch for the Zimbra release (assuming Zimbra 8.8.0 )
git checkout release/8.8.0

# Build the whole package, setting the target Zimbra (can take some minutes)
make clean && make ZAL_ZIMBRA_VERSION=8.8.0
```

The final artifact **zimbra_drive.tgz** will be placed in the folder **/tmp/zimbradriver/dist**.

The **dist** folder:

The archive zimbra_drive.tgz contains all components of Zimbra Open Drive:

Manual Installation

Manual installation is not supported.

The Zimbra Open Drive Zimlet and the Extension are installed during the Zimbra installation. Any modification to the installed Zimbra packages may lead to a fail during the Zimbra upgrade.

Extension

The files **zimbradriver-extension.jar** and **zal.jar** must be copied in the right place; then a mailbox restart is required to load the extension.

```
# As root
mkdir -p /opt/zimbra/lib/ext/zimbradriver
cp zimbradriver-extension.jar /opt/zimbra/lib/ext/zimbradriver/
cp zal.jar /opt/zimbra/lib/ext/zimbradriver/

# As zimbra
mailboxdctl restart
```

Everything is successfully done only if the extension starts correctly. The following string should be logged in **ZIMBRA_HOME/log/mailbox.log** at the moment of the last mailbox restart:

```
Initialized extension Zimbra Abstraction Layer for: zimbradriver
```

Zimlet

Deploy the Zimbra Open Drive Zimlet with the following command:

```
# As zimbra
zmzimletctl deploy com_zextras_drive_open.zip
```

By default, the Zimlet is enabled for the ‘default’ COS. The Zimlet can be enabled on any required COS from the administration console.

Manual Upgrade

Manual upgrade is not supported.

The Zimbra Open Drive Zimlet and the Extension are upgraded during the the Zimbra upgrade. Any modification to the installed Zimbra packages may lead to a fail during the Zimbra upgrade.

Extension

The Zimbra Open Drive Extension can be upgraded replacing the `zimbra-extension.jar` and `zal.jar` files in `/opt/zimbra/lib/ext/zimbradrive/` and performing a mailbox restart.

```
# As root
cp zimbradrive-extension.jar /opt/zimbra/lib/ext/zimbradrive/
cp zal.jar /opt/zimbra/lib/ext/zimbradrive/

# As zimbra
mailboxdctl restart
```

Zimlet

The Zimbra Open Drive Zimlet can be upgraded by deploying the newest version and flushing cache:

```
# As zimbra
zmzimletctl deploy com_zextras_drive_open.zip
zmprov fc zimlet
```

Manual Uninstall

Manual uninstallation is not supported.

Please consider disabling Zimbra Open Drive (see: [Disable Zimbra Open Drive Packages](#)) instead of uninstalling it. Any modification to the installed Zimbra packages may lead to a fail during the Zimbra upgrade.

The manual uninstallation process of the Zimbra Open Drive Zimlet and the Zimbra Open Drive extension requires you to undeploy the Zimlet and clean the extension folder from zimbra.

To remove the Zimbra Open Drive Zimlet:

```
# As zimbra
zmzimletctl undeploy com_zextras_drive_open
```

To remove the Zimbra Open Drive extension:

```
# As root
rm -rf /opt/zimbra/lib/ext/zimbradrive/
# As zimbra
zmmailboxdctl restart
```

The last, but not necessary, step is to clean the domain attribute with the command
`zmprov md domainExample.com zimbraDriveOwnCloudURL`

How to Report an Issue

If an issue is found, Zimbra Support requires the following information:

- A detailed description of the issue: What you are expecting and what is really happening.
- A detailed description of the steps to reproduce the issue.
- A detailed description of the installation and the environment: (see "Gathering System Information" section of this guide)
 - Cloud information:
 - Server information: CPU, RAM, number of servers and for each server:
 - Zimbra version
 - Zimbra Open Drive version
 - List of the installed Zimlets
 - Client information:
 - Browser name and version
 - Connectivity used between the servers and the client
 - Client skin (theme)
 - Client language
 - List of the Zimlets enabled for the user
- Any log involved in the issue:
 - **mailbox.log**

Any personal information can be removed to protect the privacy.

Gathering System Information

This section helps the administrator to collect useful system information that is required to escalate an issue to Zimbra Support.

Zimbra Version

To see the version of Zimbra, type this command:

```
# As zimbra
zmcontrol -v
```

List of Deployed Zimlets

To see the list of deployed Zimlets, type this command:

```
# As zimbra
zmzimletctl listZimlets
```

List of Zimlets Enabled for the User

To see the list of Zimlets enabled for a user, type this command:

```
# As zimbra
zmprov getAccount user@domain.tld zimbraZimletAvailableZimlets
```

List of Zimlet User Preferences

To see the list of preferences for the Zimlets enabled for a user, type this command:

```
# As zimbra
zmprov getAccount user@domain.tld zimbraZimletUserProperties
```

Extension and Zimlet Versions

To see the version of the extension and the Zimlet, type this command:

```
# As zimbra
java -cp /opt/zimbra/lib/ext/zimbradrive/zimbradrive-extension.jar \
com.zextras.lib.ZimbraDrive
```

Zimbra Drive

Introduction

Zimbra Drive v2 is a new Zimbra component that provides both a fully fledged file storage system integrated with the Zimbra WebClient and a replacement to the old "Briefcase" component.

Features

Frontend

- Upload, manage and download files
- Organize files within navigable folders
- Preview files
- Mark files as "preferred" for quick access
- Add custom notes (descriptions) to files
- Share files to internal users
- Share files to external users (NYI)
- Integration with Zimbra Docs
- File search
- Folder-based navigation
- Quick "stateful" navigation

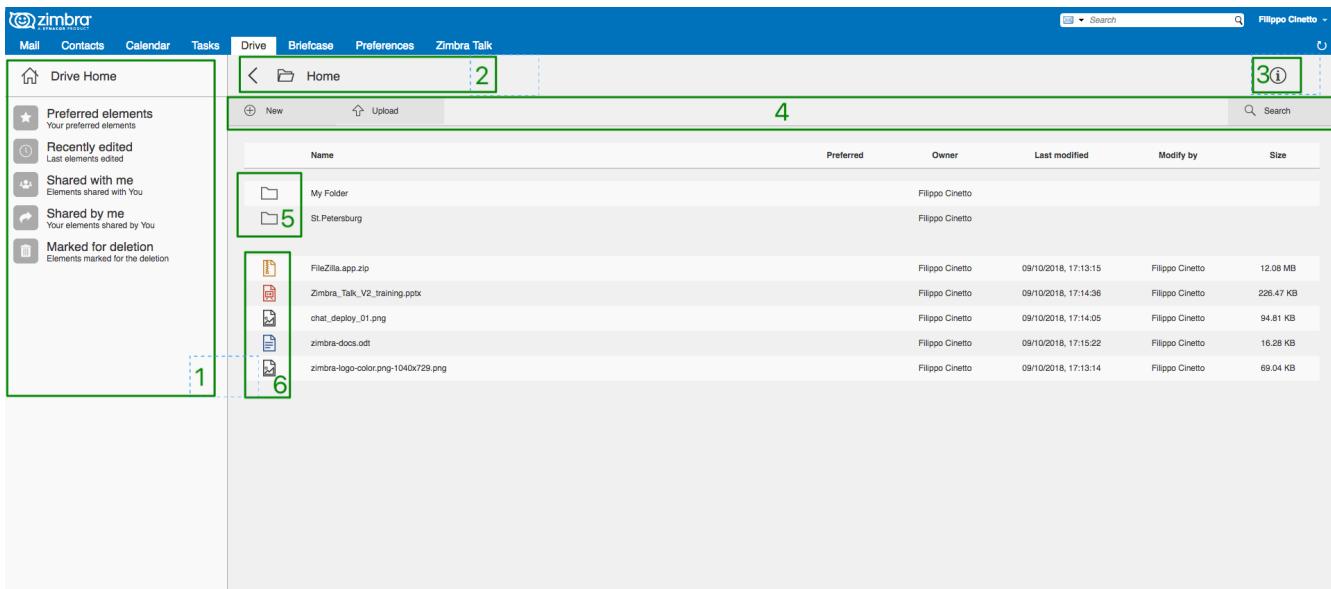
Backend

- Option to store files on dedicated Zimbra volumes
- `zxsuite drive` CLI

Differences between Briefcase and Drive

Zimbra Drive v2 does not follow the usual mailbox-driven behaviors when it comes to file storage, navigation, sharing, and item deletion. See each feature's dedicated paragraph for a complete explanation of the differences and of the features themselves.

Drive V2 UI

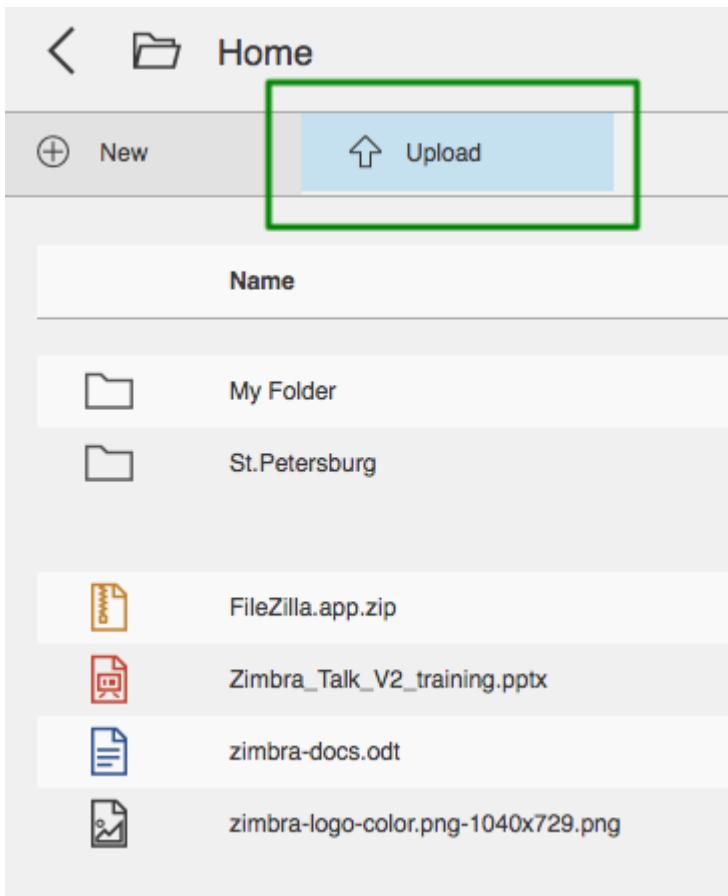


1. Quick Access navigation panel;
2. Folder navigation panel;
3. InfoBox control;
4. New, Upload and Search features;
5. Folder list;
6. File list;

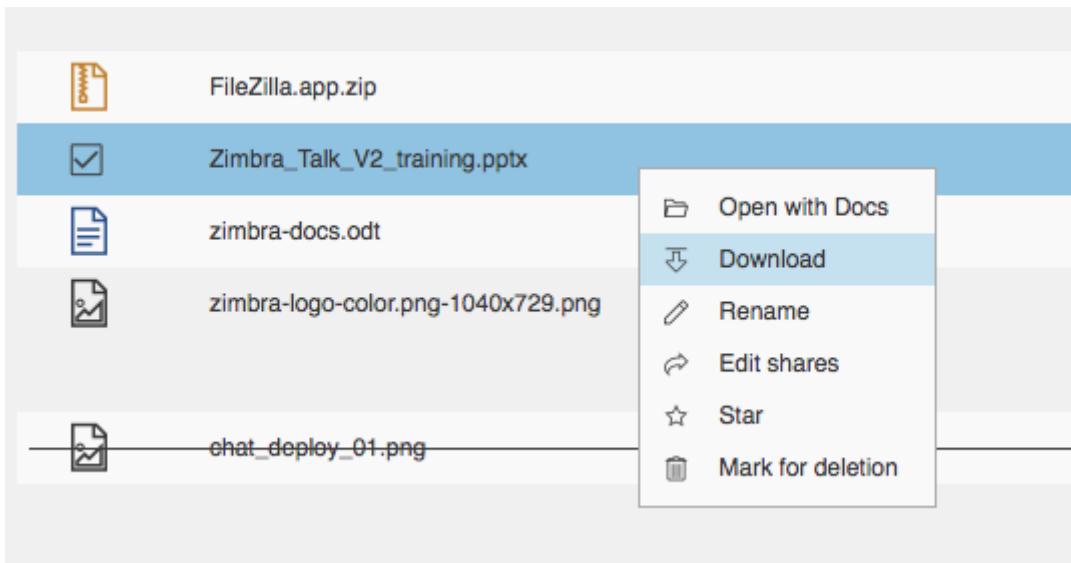
Feature Description

Upload and Download

To upload a file to Drive v2, either click on the "Upload" button above the file list or drag and drop any number of files from your computer to the main Drive window.



To download a file from Drive v2, right-click on it and select "Download":



Any file and folder in Drive v2 can be renamed by right-clicking on it and selecting the "Rename" option in the context menu.

Navigation

Briefcase items are part of the mailbox's folder and item hierarchy, while Drive v2 has its own internal folder structure and navigation. Navigating through Drive v2 folders is done through the Navigation Bar on top of the UI instead of through a tree view and folders are visible in the main section of the UI above files.

The screenshot shows the Drive v2 user interface. On the left, there's a "Quick Access" sidebar with five categories: "Preferred elements" (marked with a star), "Recently edited" (marked with a clock), "Shared with me" (marked with a person icon), "Shared by me" (marked with a circular arrow), and "Marked for deletion" (marked with a trash bin). The main area shows a folder structure: Home / My Folder / A Subfolder. At the top, there are "New" and "Upload" buttons. Below them is a table listing files and folders. The table has columns for "Name" and "Pre". One folder is listed: "Yet Another Subfolder". Below it is a list of eight files, each with a small thumbnail icon: "agriculture-alternative-energy-clouds-414837.jpg", "agriculture-bright-clouds-440731.jpg", "agriculture-close-up-cultivation-1002703.jpg", "agriculture-environment-flower-33044.jpg", "animal-avian-beak-679598.jpg", "animal-bloom-blossom-1310182.jpg", "autumn-boulder-creek-230629.jpg", and "autumn-business-daylight-296085.jpg".

On top of the standard folder-based navigation, a "Quick Access" menu is available on the left side of the UI, which allows to quickly view the following types of items:

- "Preferred Items" – items marked with the "Star" option available in the right-click context menu;
- "Recently Edited" – items edited recently, sorted from the most recently edited;
- "Shared with me" – items shared by other users
- "Shared by me" – items shared to other users
- "Marked for deletion" – items marked for deletion

Folder Creation

To create a folder in Drive v2, click on the "New" button above the file list and select "Folder":

This screenshot shows the "New" button highlighted in blue, indicating it is selected. The other buttons, "Upload" and "New Folder", are in their normal grey state.

File and Folder naming

The following characters cannot be used in Drive folders and files:

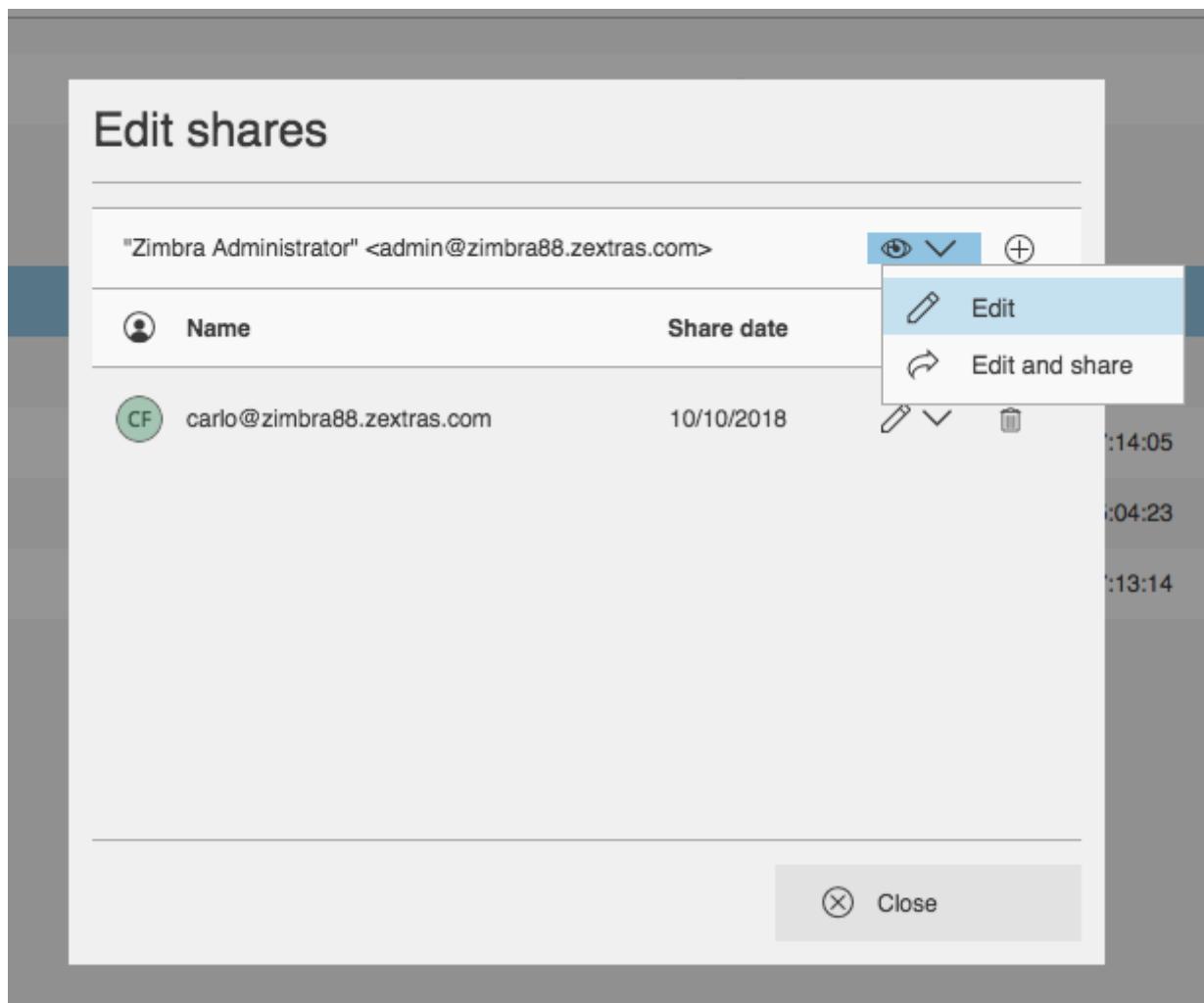
- Slash - /
- Backslash - \
- Semicolon - :
- Question Mark - ?

- Plus sign - +
- Asterisk - *
- Percent sign - %

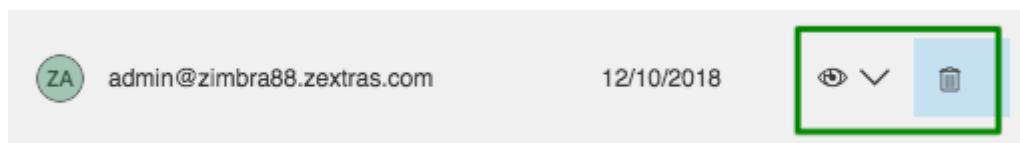
Sharing

Being separated from the mailbox's item hierarchy, Drive v2 files and folders can be shared independently. Sharing permissions can be chosen among 3 options: "View", "Edit" and "Edit and Share" – the latter two options include the "View" right by default.

To share a file or a folder, right-click on it and select "Edit Shares". After entering the email address of the destination user and selecting the sharing permissions, click the (+) button to add the share to the list:



To edit or delete a share, simply click on the dropdown permission selector to change the sharing permissions of the file/folder or click the trash bin icon to delete the share:

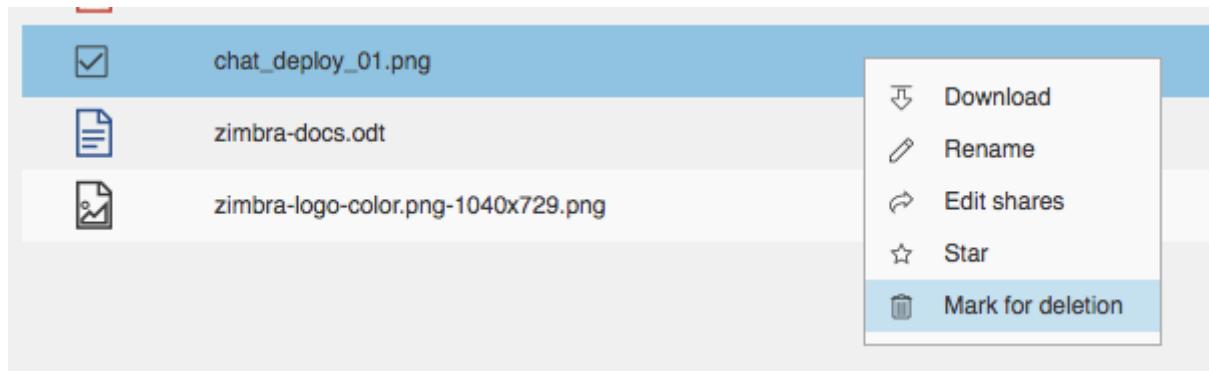


In Drive v2 sharing rights are only "positive", so it's not possible to share an item with a lower permission than its parent, e.g. if a folder is shared with "Edit" permissions it's not possible to share

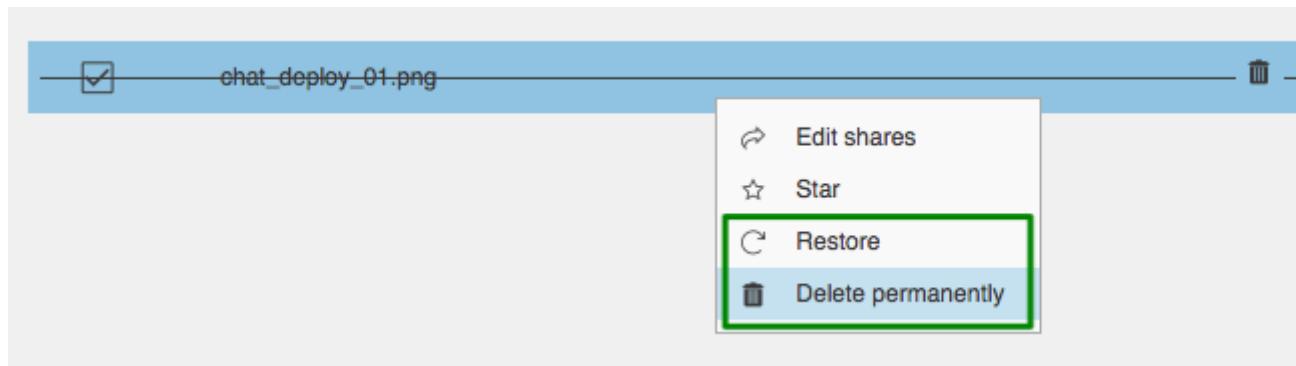
one of its items with "View" rights with the same person.

Item Deletion

When deleted, Drive v2 items are not put into the Trash like every other item type in Zimbra, as such items are marked for deletion instead. To mark a file or a folder for deletion, right-click on it and select "Mark for Deletion":



Items marked for deletion are displayed on the bottom of the file list with a strikethrough line and can be deleted permanently clicking on the "Delete Permanently" entry within the right-click context menu of a file marked for deletion while the "Restore" entry will unmark the file:



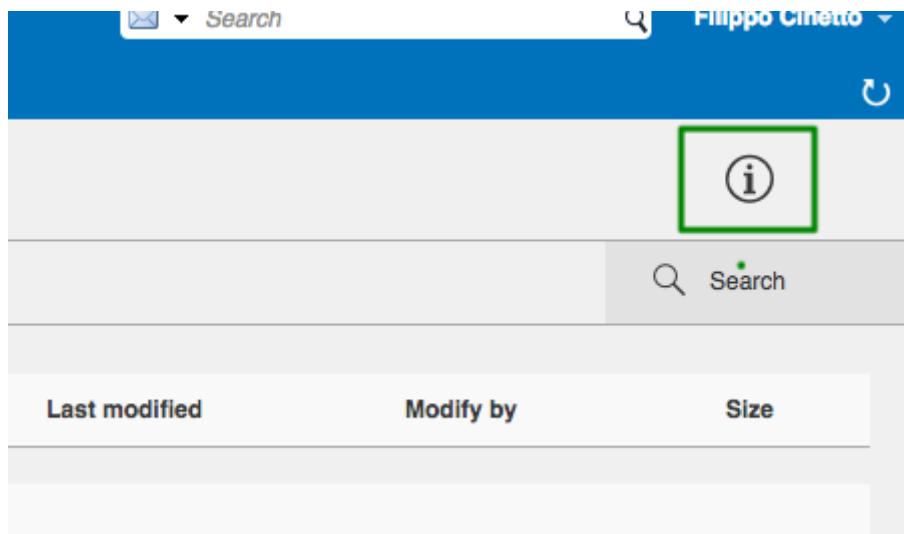
While any user with "Edit" or "Edit and Share" rights on an item or folder can mark it for deletion, only the original owner can delete it permanently.

Items marked for deletion cannot be accessed, so should a user try to do so a pop-up message will ask whether to restore the item and access it or to stop the attempt and leave it as marked for deletion.

InfoBox

The InfoBox is a collapsible element that contains all information and controls for the selected file or folder, as well as a preview of the file itself if in a compatible format (pictures, PDFs and more).

To display the Infobox, click on the "(i)" button on the top-right of the Drive v2 UI:



The infobox will appear on the right side of the screen:

A screenshot of a file info dialog for a file named "agriculture-environment-flower-33044.jpg". The dialog shows a thumbnail image of a sunflower in a field at sunset. Below the image are several actions: "Download", "Rename", "Edit shares", "Star", and "Mark for deletion". A section titled "Shared with nobody" follows. At the bottom, detailed metadata is listed:

Created by	Filippo Cinetto
On date	12/10/2018, 14:53:49
Modify by	Filippo Cinetto
On date	12/10/2018, 14:53:49

Below the metadata is a "Description" section with the text "Click here to add a description."

Top-to-bottom, the InfoBox contains:

- The name of the selected file
- The preview of the file (or a format icon for unsupported formats)
- All action items available in the right-click context menu
- Share information
- Creation and edit information
- A customizable "Description" field

Technical information

File Storage

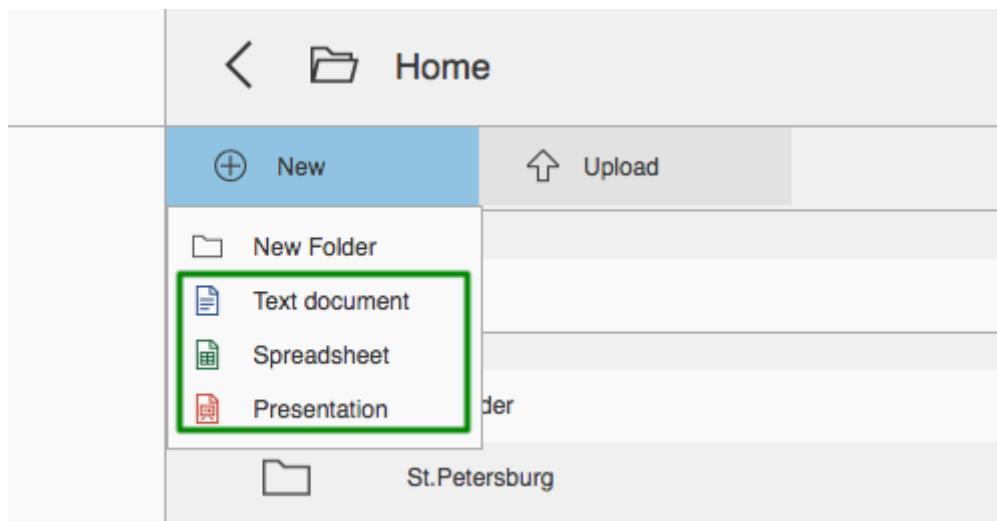
While Briefcase files are stored as mail-like items within the mailbox's folder tree, Drive v2 features a detached folder hierarchy based on nodes: thus, Drive v2 folders do not appear as mailbox folders (e.g. in the output of `zmmailbox getAllFolders`). Drive v2 metadata are stored in a dedicated HSQL Database while all files (including previous file versions and file previews) are stored in a dedicated folder within a volume's root. File naming is now hash-based instead of id-based to achieve native deduplication, compression rules follow the volume's settings

e.g. Filesystem path for a briefcase file: /opt/zimbra/store/0/[mID]/msg/0/[itemid]-[revision].msg
Filesystem path for a Drive v2 file: /opt/zimbra/store/drive/[hash]-[revision].[extension]

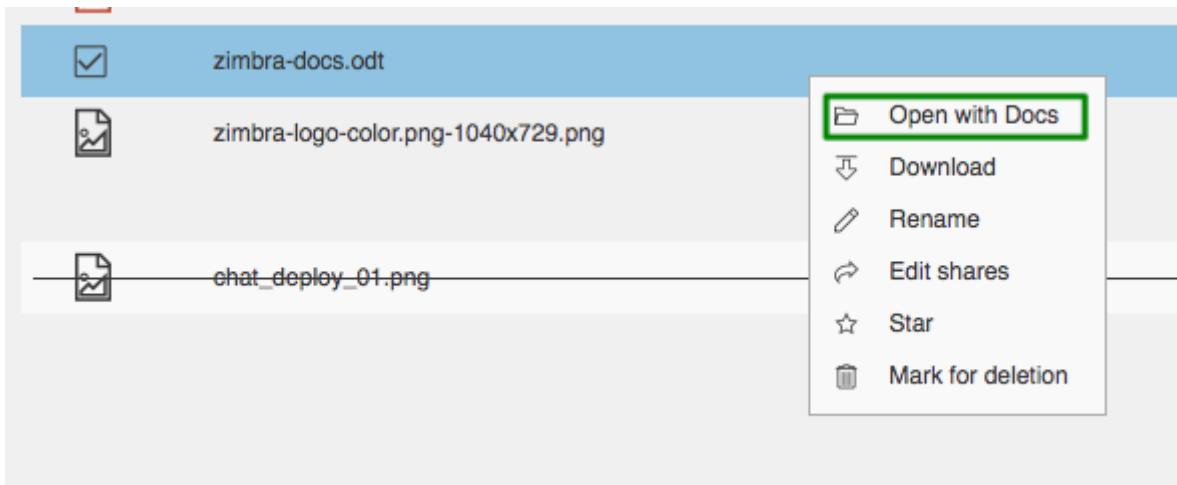
Volumes

As of this release, Drive v2 files are stored in the Current Primary volume as any other item.

Integration with Zimbra Docs If the Zimbra Docs zimlet is correctly installed, dedicated document options will appear in the "New" button above the file list:



When right-clicking on a compatible file, an "Open with Docs" option will also appear:



Furthermore, Zimbra Docs will also allow for previews of compatible document formats to be displayed in the InfoBox.

URLs and Ports

To build URLs and links (e.g. for External Shares) Zimbra Drive uses the default Zimbra settings for the domain of the account in use - the `zimbraPublicServiceHostname` property is used for the URL itself while the `zimbraPublicServicePort` property is used for the port.

Should any of the two not be set up, the system will always fall back to the `zimbraServiceHostname` and `zimbraMailPort` or `zimbraMailSSLPot` server-level properties.

Zimbra Drive Backup and HSM

Backup NG

Drive V2 files are included in Backup NG, and both the RealTime Scanner and the SmartScan are aware of those and no additional actions must be taken in order to ensure the files' safety.

The Restore on New Account and External Restore modes will also restore Drive V2 files, while other restore modes such as the Undelete Restore do not operate on such files.

HSM NG

Drive V2 can store its data on a different volume than the default Current Primary one, and HSM policies can move Drive V2 files onto a different volume than the Current Secondary one, thus effectively allowing independent storage management for Drive V2 files.

When an HSM policy is applied, Drive V2 files will be handled under the "document" item type.

This setting is applied at the server level so that different mailbox servers can use different volumes.

Setting the Drive Primary volume

To set the Drive Primary volume, first find out the volumeID of the target volume by running

```
zxsuite hsm getAllVolumes.
```

Once the volumeID has been identified, simply run

```
zxsuite config server set 'zmhostname' attribute driveStore value [volumeID]
```

(where [volumeID] is the ID found with the previous command)

Setting the Drive Secondary volume

To set the Drive Secondary volume, find out the volumeID of the target volume as described in the previous paragraph and then run the following command

```
zxsuite config server set 'zmhostname' attribute driveSecondaryStore value [volumeID]
```

Briefcase Migration

Briefcase data can be migrated to Drive v2 using the dedicated [doImport](#) CLI command:

```
zimbra@test:~$ zxsuite drive doImport
```

Syntax:

```
zxsuite drive doImport {john@example.com,test.com[,...]} [attr1 value1 [attr2 value2...]]
```

The command accepts a comma-separated list of targets to migrate, which can be either mailboxes or domains, and different target types can be used on the same command.

The following attributes can be used to customize the migration:

NAME	TYPE	EXPECTED VALUES	DEFAULT	DESCRIPTION
targets(M)	String[...]	john@example.co m,test.com[...]		Comma separated list of targets to migrate
dryRun(O)	Boolean	true or false	false	Only perform a test run without affecting the data
allVersions(O)	Boolean	true or false	false	Migrate all versions of every file
deleteSources(O)	Boolean	true or false	false	Delete migrated files from the Briefcase

NAME	TYPE	EXPECTED VALUES	DEFAULT	DESCRIPTION
overwrite(O)	Boolean	true or false	false	Overwrite existing files
showIgnoredAccounts(O)	Boolean	true or false	false	
ignoreQuota(O)	Boolean	true or false	false	Ignore mailbox quota when migrating

Zimbra Docs

Introduction

Zimbra Docs is based on a heavily customized LibreOffice online package allowing for collaborative editing of documents, spreadsheets and presentations straight from the Zimbra WebClient.

Components

Zimbra Docs Server

The Zimbra Docs server is the heart of the service. The service hosts each document opened through a LibreOffice engine and responds to the client via an image upon every keystroke and change in the document.



This component must be installed on one or more dedicated nodes running Ubuntu 16.04 LTS, Ubuntu 18.04 LTS or Red Hat Centos 7.

Zimbra Docs Extension

The extension is the key component which coordinates everything. Its main tasks are:

- Select which Docs server the next document will be opened on.
- Redirect the client when it needs to open a document.
- Read and write documents to and from system storage on behalf of the Docs server.
- Connect to each Docs server via an administrative websocket and keep track of the availability and the resource usage of each.
- Orchestrate concurrent user connections to the same document in the same server. (document sharing)

The Zimbra Docs Extension is contained within the NG modules package together with the NG Core.

Zimbra Docs Zimlet

A Zimbra Docs Zimlet handles the integration with briefcase and with email attachments. It is a thin web client which connects to a native server instance via websocket, renders a document and only sends changes to the client in order to keep the fidelity of the document on par with a desktop client while at the same time reducing the bandwidth to the bare minimum.

Documents in preview and attachments are shown in read-only mode with a simplified interface, while edit mode has a full interface.

Its main tasks are:

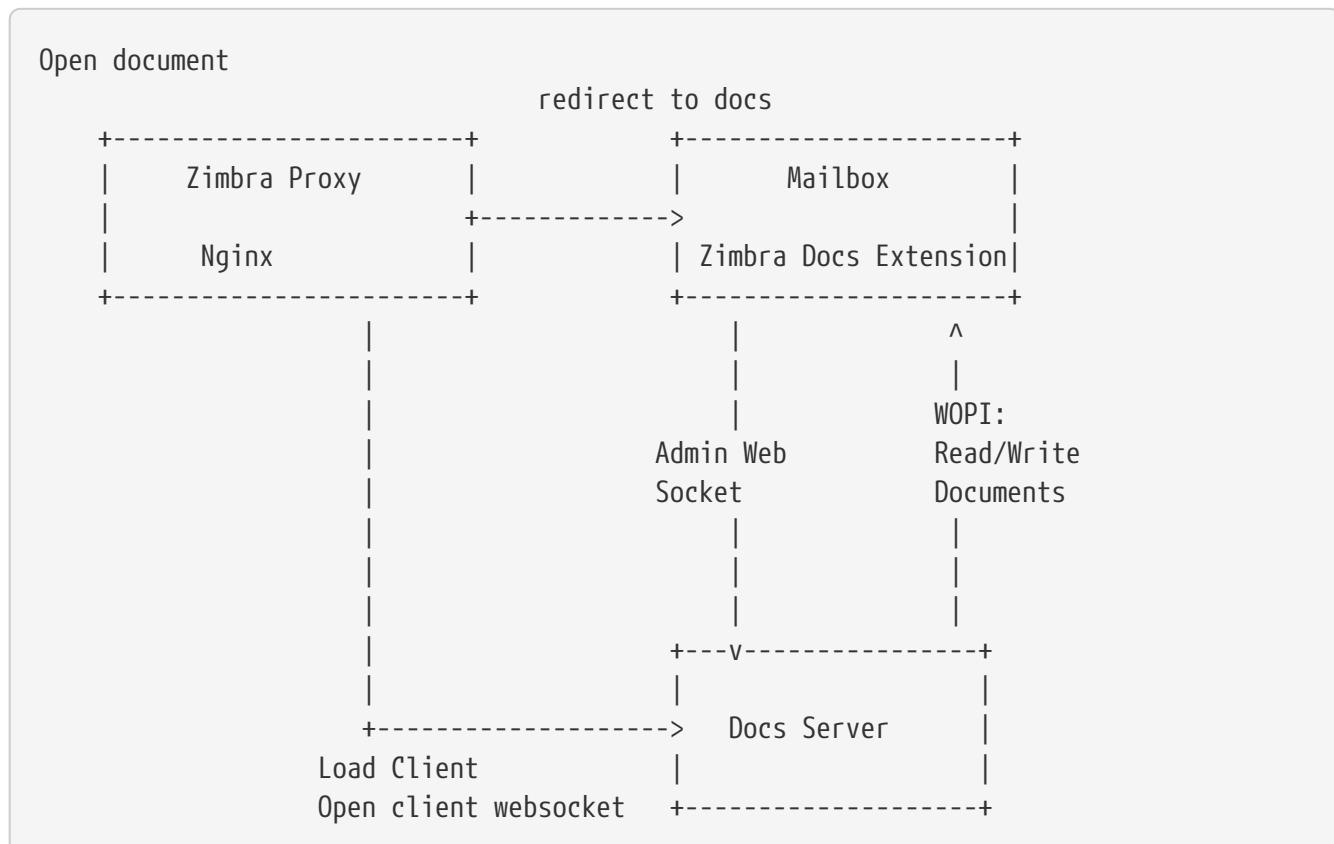
- Change the "create" button in the ZWC to the related Docs feature.

- Change the preview feature to use Docs.
- Allow the preview of documents.

Document Management Flow

This is what happens "behind the scenes" when a user creates a new document:

1. The Zimlet prompts the Extension to create a new empty document
2. The Extension creates the document and returns the document's ID to the client
3. The Zimlet opens a new Zimbra tab containing an iframe pointing towards '/service/extension/wopi-proxy'
4. The extension receives the request from the client, creates a new token for the needed document, and replies with a new url
5. The new url points toward `/docs/[docs-node-id]/[token]`, which will be proxied by nginx to the specific Docs Server node
6. The Docs Server will respond with the web application in Javascript
7. The web application opens a websocket connection, going through the nginx
8. Docs Server receives the websocket connection along with a token, sends a `read wopi` command towards the mailbox url indicated in the parameters (the url is validated against allowed nodes)
9. The Extension validates the token and replies with information and content
10. The Docs Server node parses the document, renders it and sends it back to the client.
11. The document is fully opened and editable.



Networking and ports

All mailbox servers will need to be able to directly communicate with the Docs Server over port 8443 (HTTPS Backend), which must be open on both ends.

The Docs Server communicates with the Extension through port 9980, so incoming traffic from all mailbox and proxy servers to that port must be allowed. The Docs Server component must also be able to directly communicate with the master LDAP server as well as with all Mailbox servers.

Installation and Configuration

Docs Nodes

Download the `zimbra-docs.tgz` standalone installer, extract it and as the `root` user execute the `install.sh` script contained in the package.

The script will install the Zimbra Docs package and then ask the information about the master ldap, url, username and password, which will be used to add a new server in the LDAP with just the 'docs' service installed/enabled. Every Docs Server will be visible by every node, and will read the LDAP in order to write the configuration in `/opt/zimbra/conf/docs/loolwsd.xml`.

Once the setup is completed no other configuration is needed.

Adding Custom Fonts to the Docs Server

To add Custom Fonts to your Docs Server, simply copy the `.ttf` font files in the `/opt/zimbra/docs/zimbra-docs-core/share/fonts/custom/` directory, then generate the new font cache and restart the docs server running `zdocs restart` as `root`.

To generate the new font cache, run the following command based on the Docs Server's Operating System:

Ubuntu 16 and Ubuntu 18

```
dpkg-reconfigure zimbra-docs-server
```

CentOS 7

```
fc-cache /opt/zimbra/docs/zimbra-docs-core/share/fonts
```



The server will briefly be unavailable during the restart, and clients will need to close and open again any open document to see the new fonts in the list.

Mailbox Nodes

While the Zimbra Docs extension is already contained within the NG modules, the `com_zextras_docs` Zimlet needs to be deployed on the server and enabled on all users and COS that need to have access to the Zimbra Docs features.

The `com_zextras_docs` Zimlet is available in the Zimbra repository, so it can be easily downloaded and deployed by running `apt-get install zimbra-docs`.

No configuration on the mailboxd side is needed after the Zimlet has been deployed and enabled.

Proxy Nodes

The proxy configuration must be re-generated after adding one or more Zimbra Docs Servers to the infrastructure: to do so, run `/opt/zimbra/libexec/zmproxyconfig` as the `zimbra` user and then restart the proxy service running `zmproxyctl restart` as the same user.

The new docs nodes will be read from ldap and no manual configuration is needed.

Licensing

Zimbra Docs will be available on every NG for the same amount users allowed by the Network Edition license.

The standalone installer is released under the MPLv2 license while the extension and Zimlet are released under a proprietary license.

Removal

Before uninstalling the software the node must be removed form LDAP either from the docs node via command

`zdocs remove-local-server`

or via the zmprov command from any zimbra node

`zmprov deleteServer {servername}`

Commands

Zimbra Docs Server CLI - zdocs

On Docs server zdocs (/usr/local/bin/zdocs as root) command can generate the config for lool (it's already on cron), add/remove the docs server from ldap, test configuration and manage the service.

`zdocs command`

```
usage: zdocs [-h] [--auto-restart] [--ldap-dn LDAP_DN] [--ldap-pass LDAP_PASS]
              [--ldap-url LDAP_URL] [--hostname HOSTNAME] [--debug][--cron]
```

```
{genkey,write-local-server,remove-local-server,generate-config,ldap-write-config,ldap-
test,start,stop,restart,status,setup}
```

Manage Zimbra Docs service.

Available commands:

genkey	Generate a private key needed for authentication between docs and mailbox servers.
write-local-server	Add or update in LDAP the necessary server entry for this

server in order to be reachable from other servers.

remove-local-server	Remove local server entry in LDAP.
generate-config	Populate the config template with ldap values and write a new configuration file.
ldap-write-config	Write new configuration about the ldap access needed to generate the docs configuration file.
ldap-test	Check the ldap connection.
start	Start the service.
stop	Stop the service.
restart	Restart the service.
status	Print service status.
setup	Start the initial setup.

positional arguments:

{genkey,write-local-server,remove-local-server,generate-config,ldap-write-config,ldap-test,start,stop,restart,status,setup}

Command to execute

optional arguments:

-h, --help	show this help message and exit
--auto-restart	Automatically restart the service if configuration is changed (to be used with generate-config)
--ldap-dn LDAP_DN	Ldap dn (distinguish name) to bind to (to be used with ldap-test and ldap-settings)
--ldap-pass LDAP_PASS	Ldap password used of the DN (to be used with ldap-test and ldap-settings)
--ldap-url LDAP_URL	Ldap url completed with schema (ex.: ldaps://ldap.example.com, to be used with ldap-test and ldap-settings)
--hostname HOSTNAME	Hostname of this server (to be used with add-local-server)
--debug	Show complete errors when things go bad.
--cron	Start in cron mode, avoid any output unless there is an error (to be used with generate-config).

examples:

```
#regenerate the config and restart the server if config changed
zdocs --auto-restart generate-config
#restart the service
zdocs restart
#check ldap connection availability using current settings
zdocs ldap-test
#check ldap connection using custom settings
zdocs --ldap-url ldaps://ldap.example.com/ --ldap-dn
'uid=zimbra,cn=admins,cn=zimbra' --ldap-pass password ldap-test
#change the ldap connection settings
zdocs --ldap-url ldap://ldap2.example.com/ --ldap-dn
'uid=zimbra,cn=admins,cn=zimbra' --ldap-pass password
ldap-write-config
#add the local server
zdocs write-local-server
#add the local server with a custom hostname in LDAP, this command should be already
invoked during setup.
```

```
zdocs --hostname myhostname write-local-server
#remove the local server from LDAP, useful when destroying the server, you can also
use 'zmprov deleteServer' from a mailbox server.
zdocs remove-local-server
```

Zimbra Docs Extension CLI - zxsuite docs

On a Mailbox server, the `zxsuite docs` command is available. This command allows to check and control the Docs service's status, to force a configuration reload and to see the Docs Servers' status.

`zxsuite docs`

```
zxsuite docs
```

Commands regarding docs module

`doReloadConfig` - reload docs configuration from ldap, which would happen once a minute.

```
zxsuite docs doReloadConfig
```

`doRestartService` - restart a given service

```
zxsuite docs doRestartService
```

```
{service_name}
```

`doStartService` - start a given service

```
zxsuite docs doStartService {service_name}
```

`doStopService` - stop a given service

```
zxsuite docs doStopService {service_name}
```

`getServices` - show current status of all services for this module

```
zxsuite docs getServices
```

`status` - show zimbra docs servers status with their resource usage (if connected).

```
zxsuite docs status
```

Troubleshooting

[Nothing happens when opening a document / extension requests returns 503.](#)

This is most likely due to a connection issue between the mailbox server and the Docs server. Check the `mailbox.log` and see the reason for the connection failure. If there are no connection errors, check the Docs server with `zdocs status` on the docs node.

The mailbox will log every connection and disconnection for each Docs server.

[404 error code instead of docs](#)

The proxy configuration needs to be re-generated and the proxy restarted.

[*Docs opens but a message “this is embarrassing...” appears instead of the document.*](#)

This happens if the Docs server cannot connect back to the mailbox server to read and write the document. Check name resolution and SSL certificate of mailboxd which must be valid for the Docs server that does not inherit Zimbra certificate management.

Appendix A: Command Line Utilities

Command Line Interface (CLI) can be used to create, modify and delete certain features and functions of the Zimbra Collaboration. The Administration Console is the main tool for maintaining the Zimbra Collaboration, but some functions can only be changed from CLI utilities.

The CLI utilities can be used for the following purposes:

- Provisioning accounts
- Backup and Restore
- Starting and stopping a service
- Move mailboxes
- Cross-mailbox searches
- Installing self-signed certificates
- Local configuration



In general, provisioning and managing accounts should be performed from the Administration Console.

General Tool Information

The Zimbra Collaboration command-line utilities follow standard UNIX command-line conventions. Use the following general guidelines with the CLI:

- CLI commands are run as the `zimbra` user:
`su - zimbra`
- The CLI commands are case-sensitive. You must type them in lower case.
- Press **ENTER** after you type a command.
- To display usage information about a command, type the CLI command with `-h`.

Example: `zmprov -h` lists all the options available for the `zmprov` utility.

- Each operation is invoked through command-line options. Many have a long name and a short name. For example, these two commands are equivalent:

```
zmprov createAccount joe@domain.com test123  
zmprov ca joe@domain.com test123
```

Syntax Conventions

When demonstrating the syntax of each tool, the following conventions indicate required, optional, and alternate values:

- {attribute} in curly brackets is required information.
- [attribute] in square brackets are optional arguments or information.
- {a|b|c} or [a|b|c] options separated by the pipe character | means "a" OR "b" OR "c"
- For attribute names that may contain spaces, surround the name with double quotes.

Location of Command-Line Utilities

The command-line tools available for administrators are all located in the `/opt/zimbra/bin` folder on the Zimbra Collaboration server.

Zimbra CLI Commands

```
[zimbra@... bin]$ cd /opt/zimbra/bin
[zimbra@... bin]$ ls
antispam-mysql      zmcertmgr      zmlocalconfig   zmrestoreldap
antispam-mysqldadmin zmclamdctl    zmloggerctl    zmrestoreoffline
antispam-mysql.server zmconfigdctl  zmloggerhostmap zmsaslauthdctl
ldap                 zmcontrol     zmlogswatchctl zmschedulebackup
mysql                zmconvertctl  zmmailbox       zmshutil
mysqldadmin          zmdedupe     zmmailboxdctl zmskindeploy
mysql.server          zmdevicesstats zmmailboxmove  zmsoap
postconf              zmdhparam    zmmboxmovequery zmspellctl
postfix               zmdnscachectl zmmboxsearch   zmsshkeygen
qshape                zmdumpenv    zmmemcachedctl zmstat-chart
zmaccts              zmfixcalendtime zmmetadump    zmstat-chart-config
zmamavisdctl         zmfixcalprio zmmilterctl   zmstatctl
zmantispamctl        zmfreshclamctl zmmtactl     zmstorectl
zmantispamdbpasswd  zmgdcutil    zmmypasswd   zmswatchctl
zmantivirusctl      zmgsautil   zmmysqlstatus zmsyncreverseproxy
zmapachectl          zhactl      zmmytop      zmthrdump
zmarchiveconfig      zhhostname  zmopendkimctl zmtlsctl
zmarchivectl         zhsm        zmplayredo   zmtotp
zmarchivesearch      zminnotop   zmprov       zmtrainsa
zmauditwatchctl     zmitemdatafile zmproxyconf  zmtzupdate
zmbackup              zmjava      zmproxyctl   zmupdateauthkeys
zmbackupabort         zmjavaext   zmpurgeoldmbox zmvolume
zmbackupquery         zmldapasswd zmpython     zmzimletctl
zmblobchk            zmladupupgrade zmredodump
zmcaldebug           zmlicense   zmresolverctl
zmcbpolicydctl      zmlmtpinject zmrestore
```

The table below lists the CLI commands in `/opt/zimbra/bin`.

CLI	Description
<code>antispam-mysqldadmin</code>	anti-spam SQL server admin utility
<code>antispam-mysql</code>	anti-spam SQL client
<code>antispam-mysql.server</code>	Start, stop the anti-spam SQL instance
<code>ldap</code>	Start, stop, or find the status of Zimbra LDAP
<code>ldapsearch</code>	Perform a search on an LDAP server
<code>logmysqldadmin</code>	Send mysqladmin commands to the logger SQL instance

CLI	Description
<code>mysql</code>	Enters interactive command-line for the mailbox SQL instance
<code>mysql.server</code>	Start, stop the mailbox SQL instance
<code>mysqladmin</code>	Send admin commands to the mailbox SQL instance
<code>postconf</code>	Postfix command to view or modify the postfix configuration
<code>postfix</code>	Start, stop, reload, flush, check, upgrade-configuration of postfix
<code>qshape</code>	Examine postfix queue in relation to time and sender/recipient domain
<code>zmaccts</code>	Lists the accounts and gives the status of accounts on domain
<code>zmamavisdctl</code>	Start, stop, restart, or find the status of the Amavis-D New
<code>zmantispamctl</code>	Start, stop, reload, status for anti-spam service
<code>zmantivirusctl</code>	Start, stop, reload, status for the anti-virus service
<code>zmantispamdbpasswd</code>	Changes anti-spam SQL database password
<code>zmapachectl</code>	Start, stop, reload, or check status of Apache service (for spell check)
<code>zmarchiveconfig</code>	Command to view, modify, or configure archiving
<code>zmarchivectl</code>	Start, stop, reload, status for archiving
<code>zmarchivesearch</code>	Search archives on the account
<code>zmauditswatchctl</code>	Start, stop, restart, reload, status of the auditswatch
<code>zmbackup</code>	Performs full backups and incremental backups for a designated mail host.
<code>zmbackupabort</code>	Stops a backup that is in process.
<code>zmbackupquery</code>	Find a specific full backup set
<code>zmblobchk</code>	Check consistency of the Zimbra blob store
<code>zmcalchk</code>	Check consistency of appointments and attendees in the Zimbra calendar
<code>zmcbpolicyctl</code>	Start, stop, and restart the cluebringer policyd service, if enabled
<code>zmconfigctl</code>	Start, stop, kill, restart status of the MTA configuration daemon.
<code>zmcertmgr</code>	Manage self-signed and commercial certificates
<code>zmclamdctl</code>	Start, stop, or find the status of Clam AV
<code>zmcleaniplanetics</code>	Clean iPlanet ICS calendar files
<code>zmcontrol</code>	Start, stop, restart, status of the Zimbra servers. Also can use to find the Zimbra version installed
<code>zmconvertctl</code>	Start, stop, the conversion server or find the status of the converted attachments conversion/indexing
<code>zmdevicesstats</code>	Number of unique ActiveSync device IDs per server
<code>zmgdutil</code>	(get devices count) gives the total devices system wide without the need of specifying individual servers.

CLI	Description
<code>zmdumpenv</code>	General information about the server environment is displayed
<code>zmgsautil</code>	Global Address Book (GAL) synchronization utility. Create, delete the GAL sync account and initiate manual syncs.
<code>zmhostname</code>	Find the hostname of the Zimbra server
<code>zmhsm</code>	Start, stop and status of a HSM session.
<code>zmitemdatafile</code>	Extracts and packs tgz files that ZCS uses for REST import/export
<code>zmjava</code>	Execute Java with Zimbra-specific environment settings
<code>zmjavaext</code>	Execute Java and Zimbra-specific environment settings including extension based jars.
<code>zmldappasswd</code>	Changes the LDAP password
<code>zmlicense</code>	View and install your Zimbra license
<code>zmlmtpinject</code>	Testing tool
<code>zmlocalconfig</code>	Used to set or get the local configuration of a Zimbra server
<code>zmloggerctl</code>	Start, stop, reload, or find the status of the Zimbra logger service
<code>zmloggerhostmap</code>	Used to manually map a DNS hostname to a zmhostname.
<code>zmlogswatchctl</code>	Start, stop, status of the swatch that is monitoring logging.
<code>zmmailbox</code>	Performs mailbox management tasks
<code>zmmailboxdctl</code>	Start, stop, reload, or find the status of the mailbox components (zmmailboxd, MariaDB, convert)
<code>zmmboxsearch</code>	(Cross Mailbox Search) Search across mailboxes to find messages and attachments
<code>zmmboxmove</code>	7.1.3 and later. Used to move selected mailboxes from one Zimbra server to another.
<code>zmmboxmovequery</code>	7.1.3 and later. Used to query ongoing mailbox moves on a server
<code>zmpurgeoldbox</code>	7.1.3 and later. Purges a mailbox from the old server after a mailbox move
<code>zmemcachedctl</code>	Start, stop, and restart
<code>zmetadump</code>	Support tool that dumps an item's metadata in a human-readable form
<code>zmfilterctl</code>	Start, stop, and restart the Zimbra milter server if enabled
<code>zmtaconfigdctl</code>	Beginning in ZCS 7.0, this command is not used. Use <code>zmconfigdctl</code> .
<code>zmtactl</code>	Start, stop, or find the status of the MTA
<code>zmmypasswd</code>	Change SQL passwords
<code>zmmysqlstatus</code>	Status of mailbox SQL instance
<code>zmnginxconf</code>	Output the reverse proxy configuration
<code>zmnginxctl</code>	Start, stop, and restart the Zimbra reverse proxy

CLI	Description
<code>zmplayredo</code>	Performs data restore using backed up snapshots taken periodically. Users who use snapshots to backup and restore their information from a standby site use this command.
<code>zmprov</code>	Performs all provisioning tasks in Zimbra LDAP, including creating accounts, domains, distribution lists and aliases
<code>zmproxyconfgen</code>	Generates configuration for the nginx proxy
<code>zmproxyctl</code>	Start, stop, restart, and find the status of the IMAP proxy service
<code>zmproxypurge</code>	Purges POP/IMAP routing information from one or more memcached servers
<code>zmpython</code>	Ability to write Python scripts that access Zimbra Java libraries. It sets the Zimbra class path and starts the Jython interpreter.
<code>zmredodump</code>	Support tool for dumping contents of a redolog file for debugging purposes
<code>zmrestore</code>	Performs full restores and incremental restores for a designated mail host
<code>zmrestoreldap</code>	Restore accounts from the LDAP backup
<code>zmrestoreoffline</code>	(Offline Restore) Performs full restore when the Zimbra server (i.e., the <code>mailboxd</code> process) is down
<code>zmsaslauthdctl</code>	Start, stop, or find the status of saslauthd (authentication)
<code>zmschedulebackup</code>	Schedule backups and add the command to your cron table
<code>zmshutil</code>	Used for other zm scripts, do not use
<code>zmskindeploy</code>	Deploy skins
<code>zmsoap</code>	Print mail, account, and admin information in the SOAP format
<code>zmspellctl</code>	Start, stop, or find the status of the spell check server
<code>zmsshkeygen</code>	Generate Zimbra's SSH encryption keys
<code>zmstat-chart</code>	Generate charts from zmstat data collected in a directory
<code>zmstat-chart-config</code>	Outputs an XML configuration that describes the current state of the data gathered from zmstat-chart to generate charts on the Administration Console.
<code>zmstatctl</code>	Start, stop, check status, or rotate logs of zmstat data collectors
<code>zmstorectl</code>	Start, stop, or find the status of Zimbra store services
<code>zmwatchctl</code>	Start, stop, or find the status of the Swatch process, which is used in monitoring
<code>zmsyncreverseproxy</code>	Decodes the sync request/responses and logs them when verbose mode is turned on.
<code>zmthrdump</code>	Initiate a thread dump and save the data to a file with a timestamp

CLI	Description
<code>zm tlsctl</code>	Set the Web server mode to the communication protocol options: HTTP, HTTPS or mixed
<code>zm trainsa</code>	Used to train the anti-spam filter to recognize what is spam or ham
<code>zm tzupdate</code>	Provides mechanism to process time zone changes
<code>zm updateauthkeys</code>	Used to fetch the ssh encryption keys created by <code>zm sshkeygen</code>
<code>zm volume</code>	Manage storage volumes on your Zimbra Mailbox server
<code>zm zimletctl</code>	Deploy and configure Zimlets

Using non-ASCII Characters in CLIs

If you use non-ASCII characters in the CLI, in order for the characters to display correctly, you must change this setting to the desired UTF-8 before running the CLI command. To change this, type

```
export LC_ALL=<UTF_locale>
```



The default locale on the zimbra user system account is LANG=C. This setting is necessary for starting ZCS services. Changing the default LANG=C setting may cause performance issues with amavisd-new.

zmprov (Provisioning)

The `zmprov` tool performs all provisioning tasks in Zimbra LDAP, including creating accounts, aliases, domains, COS, distribution lists, and calendar resources. Each operation is invoked through command-line options, each of which has a long name and a short name.

The syntax is `zmprov [cmd] [argument]`.

The syntax for modify can include the prefix "+" or "-" so that you can make changes to the attributes affected and do not need to reenter attributes that are not changing.

- Use `+` to add a new instance of the specified attribute name without changing any existing attributes.
- Use `-` to remove a particular instance of an attribute.

The following example would add the attribute `zimbraZimletUserProperties` with the value "blue" to user 1 and would not change the value of any other instances of that attribute.

```
zmprov ma user1 +zimbraZimletUserProperties "com_company_testing:favoriteColor:blue"
```

The attributes for the tasks zmprov can be used with are listed when you type `zmprov -h`. The task area divided into the following sections:

Long Name	Short Name	Syntax, Example, and Notes
<code>--help</code>	<code>-h</code>	display usage

Long Name	Short Name	Syntax, Example, and Notes
--file	-f	use file as input stream
--server	-s	{host}[:{port}] server hostname and optional port
--ldap	-l	provision via LDAP instead of SOAP
--logpropertyfile	-L	log4j property file, valid only with -l
--account {name}	-a	account name to auth as
--password {pass}	-p	password for account
--passfile {file}	-P	read password from file
--zadmin	-z	use Zimbra admin name/password from localconfig for admin/password
--authtoken {authtoken}	-y	use auth token string (has to be in JSON format) from command line
--authtokenfile {authtoken-file}	-Y	use auth token string (has to be in JSON format) from a file
--verbose	-v	verbose mode (dumps full exception stack trace)
--debug	-d	debug mode (dumps SOAP messages)
--master	-m	use LDAP master. This only valid with -l
--replace	-r	allow replacement of safe-guarded multi-value attribute configured in localconfig key <code>zmprov_saveguarded_attrs</code>

The commands are categorized and briefly described in the following topics:

- [Account Provisioning Commands](#)
- [Calendar Resource Provisioning Commands](#)
- [Free Busy Commands](#)
- [Domain Provisioning Commands](#)
- [COS Provisioning Commands](#)
- [Server Provisioning Commands](#)
- [Config Provisioning Commands](#)
- [Distribution List Provisioning Commands](#)
- [Mailbox Commands](#)
- [Logs Commands](#)
- [Search Commands](#)
- [Share Provisioning Commands](#)
- [Unified Communication Service Commands](#)
- [IMAP/POP Proxy Commands](#)

Account Provisioning Commands

Table 63. `zmprov` — Account Provisioning Commands

Command	Syntax	Example/Notes
<code>addAccountAlias (aaa)</code>	<code>{name@domain id adminName} {alias@domain}</code>	<pre>zmprov aaa joe@domain.com joe.smith@engr.domain.com</pre>
<code>checkPasswordStrength (cps)</code>	<code>{name@domain id} {password}</code>	<pre>zmprov cps joe@domain.com test123</pre> <p>i This command does not check the password age or history.</p>
<code>createAccount (ca)</code>	<code>{name@domain} {password} [attr1 value1]..</code>	<pre>zmprov ca joe@domain.com test123 displayName JSmith</pre>
<code>createDataSource (cds)</code>	<code>{name@domain} {ds-type} {ds-name} zimbraDataSourceEnabled {TRUE FALSE} zimbraDataSourceFolderId {folder-id} [attr1 value1 [attr2 value2]]..</code>	
<code>createIdentity (cid)</code>	<code>{name@domain} {identity-name} [attr1 value1 [attr2 value2]]..</code>	
<code>createSignature (csig)</code>	<code>{name@domain} {signature-name} [attr1 value1 [attr2 value2]]..</code>	
<code>deleteAccount (da)</code>	<code>{name@domain id adminName}</code>	<pre>zmprov da joe@domain.com</pre>
<code>deleteDataSource (dds)</code>	<code>{name@domain id} {ds-name ds-id}</code>	
<code>deleteIdentity (did)</code>	<code>{name@domain id} {identity-name}</code>	
<code>deleteSignature (dsig)</code>	<code>{name@domain id} {signature-name}</code>	
<code>getAccount (ga)</code>	<code>{name@domain id adminName}</code>	<pre>zmprov ga joe@domain.com</pre>
<code>getAccountMembership (gam)</code>	<code>{name@domain id}</code>	

Command	Syntax	Example/Notes
getAllAccounts (gaa)	[-v] [domain]	Must include -l/--ldap zmprov -l gaa zmprov -l gaa -v domain.com
getAllAdminAccounts (gaaa)		zmprov gaaa
getDataSources (gds)	{name@domain id} [arg1 [arg2]]	
getIdentities (gid)	{name@domain id} [arg1 [arg2]]	
getSignatures (gsig)	{name@domain id} [arg1 [arg2]]	
modifyAccount (ma)	{name@domain id adminName} [attr1 value1]	zmprov ma joe@domain.com zimbraAccountStatus maintenance
modifyDataSource (mds)	{name@domain id} {ds-name ds-id} [attr1 value1 [attr2 value2]]	
modifyIdentity (mid)	{name@domain id} {identity-name} [attr1 value1 [attr2 value 2]]	
modifySignature (msig)	{name@domain id} {signature-name signature-id} [attr1 value1 [attr2 value2]]	
removeAccountAlias (raa)	{name@domain id adminName} {alias@domain}	zmprov raa joe@domain.com joe.smith@engr.domain.com
renameAccount (ra)	{name@domain id} {newname@domain}	zmprov ra joe@domain.com joe23@domain.com
		<p> After you rename an account, you should run a full backup for that account.</p> <pre>zmbackup -f -s <servername.com> -a <newaccountname@servername.com></pre>

Command	Syntax	Example/Notes
setAccountCOS (sac)	{name@domain id adminName} {cos-name cos-id}	<pre>zmprov sac joe@domain.com FieldTechnician</pre>
setPassword (sp)	{name@domain id adminName} {password}	<pre>zmprov sp joe@domain.com test321</pre> <p>i Passwords cannot include accented characters in the string. Example of accented characters that cannot be used: ã, é, í, ú, ü, ñ.</p>

Calendar Resource Provisioning Commands

Table 64. `zmprov` — Calendar Resource Provisioning Commands

Command	Syntax
createCalendarResource (ccr)	{name@domain} [attr1 value1 [attr2 value2]...]
deleteCalendarResource (dcr)	{name@domain id}
getAllCalendarResources (gacr)	[-v] [domain]
getCalendarResource (gcr)	{name@domain id}
modifyCalendarResource (mcr)	{name@domain id} [attr1 value1 {attr2 value2}...]
purgeAccountCalendarCache (pacc)	{name@domain} [...]
renameCalendarResource (rcr)	{name@domain id} {newName@domain}

Free Busy Commands

Table 65. `zmprov` — Free Busy Commands

Command	Syntax
getAllFbp (gafbp)	[-v]
getFreebusyQueueInfo (gfbqi)	[{provider-name}]
pushFreebusy (pfb)	{domain account-id} [account-id...]
pushFreebusyDomain (pfbd)	{domain}
purgeFreebusyQueue (pfbg)	[{provider-name}]

Domain Provisioning Commands

Table 66. zmprov — Domain Provisioning Commands

Command	Syntax	Example/Notes
countAccount (cta)	{domain id}	This lists each COS, the COS ID and the number of accounts assigned to each COS
createAliasDomain (cad)	{alias-domain-name} {local-domain-name id} [attr1 value1 [attr2 value2]…]	
createDomain (cd)	{domain} [attr1 value1]…	<pre>zmprov cd mktng.domain.com zimbraAuthMech zimbra</pre>
deleteDomain (dd)	{domain id}	<pre>zmprov dd mktng.domain.com</pre>
getDomain (gd)	{domain id}	<pre>zmprov gd mktng.domain.com</pre>
getDomainInfo (gdi)	name id virtualHostname {value} [attr1 [attr2]…]	
getAllDomains (gad)	[-v]	
modifyDomain (md)	{domain id} [attr1 value1]…	<pre>zmprov md domain.com zimbraGalMaxResults 500</pre> <p> Do not modify <code>zimbraDomainRenameInfo</code> manually. This is automatically updated when a domain is renamed.</p>
renameDomain (rd)	{domain id} {newDomain}	<p></p> <p><code>renameDomain</code> can only be used with <code>zmprov -l/--ldap</code></p>

COS Provisioning Commands

Table 67. zmprov — COS Provisioning Commands

Command	Syntax	Example/Notes
copyCos (cpc)	{src-cos-name id} {dest-cos-name}	
createCos (cc)	{name} [attr1 value1]	<pre>zmprov cc Executive zimbraAttachmentsBlocked FALSE zimbraAuthTokenLifetime 60m zimbraMailQuota 100M zimbraMailMessageLifetime 0</pre>
deleteCos (dc)	{name id}	<pre>zmprov dc Executive</pre>
getCos (gc)	{name id}	<pre>zmprov gc Executive</pre>
getAllCos (gac)	[-v]	<pre>zmprov gac -v</pre>
modifyCos (mc)	{name id} [attr1 value1]	<pre>zmprov mc Executive zimbraAttachmentsBlocked TRUE</pre>
renameCos (rc)	{name id} {newName}	<pre>zmprov rc Executive Business</pre>

Server Provisioning Commands

Table 68. `zmprov` — Server Provisioning Commands

Command	Syntax	Example/Notes
createServer (cs)	{name} [attr1 value1]	
deleteServer (ds)	{name id}	<pre>zmprov ds domain.com</pre>
getServer (gs)	{name id}	<pre>zmprov gs domain.com</pre>
getAllServers (gas)	[-v]	<pre>zmprov gas</pre>

Command	Syntax	Example/Notes
modifyServer (ms)	{name id} [attr1 value1]…	<pre>zmprov ms domain.com zimbraVirusDefinitionsUpdateFrequency 2h</pre>
getAllMtaAuthURLs (gamau)		Used to publish into <code>saslauthd.conf</code> what servers should be used for <code>saslauthd.conf</code> MTA auth
getAllMemcachedServers (gamcs)		Used to list memcached servers (for nginx use).

Config Provisioning Commands

Table 69. `zmprov` — Config Provisioning Commands

Command	Syntax	Example/Notes
getAllConfig (gacf)	[-v]	All LDAP settings are displayed
getConfig (gcf)	{name}	
modifyConfig (mcf)	attr1 value1	Modifies the LDAP settings.
createXMPPComponent (csc)	{short-name} {domain} {server} {classname} {category} {type} [attr1 value1 [attr2 value2]…]	
deleteXMPPComponent (dxc)	{xmpp-component-name}	
getXMPPComponent (gxc)	{name@domain} [attr1 [attr2]…]	
modifyXMPPComponent (mxc)	{name@domain} [attr1 value1 [attr2 value2]…]	

Distribution List Provisioning Commands

Table 70. `zmprov` — Distribution List Provisioning Commands

Command	Syntax	Example/Notes
createDistributionList (cdl)	{list@domain}	<pre>zmprov cdl needlepoint-list@domain.com</pre>

Command	Syntax	Example/Notes
addDistributionListMember (adlm)	{list@domain id} {member@domain}	zmprov adlm needlepoint-list@domain.com singer23@mail.free.net
removeDistributionListMember (rdlm)	{list@domain id}	zmprov rdlm needlepoint-list@domain.com singer23@mail.free.net
getAlldistributionLists (gadl)	[-v]	
getDistributionListmembership (gdlm)	{name@domain id}	 gdlm can not be used for dynamic groups, as dynamic groups cannot be nested.
getDistributionList (gdl)	{list@domain id}	zmprov gdl list@domain.com
modifyDistributionList (mdl)	{list@domain id} attr1 value1 [attr2 value2]	zmprov md list@domain.com
deleteDistributionList (ddl)	{list@domain id}	
addDistributionListAlias (adla)	{list@domain id} {alias@domain}	
removeDistributionListAlias (rdla)	{list@domain id} {alias@domain}	
renameDistributionList (rdl)	{list@domain id} {newName@domain}	

Mailbox Commands

Table 71. `zmprov` — Mailbox Commands

Command	Syntax	Example/Notes
getMailboxInfo (gmi)	{account}	
getQuotaUsage (gqu)	{server}	

Command	Syntax	Example/Notes
recalculateMailboxCounts (rmc)	{name@domain id}	When unread message count and quota usage are out of sync with the data in the mailbox, use this command to immediately recalculate the mailbox quota usage and unread messages count. ! Recalculating mailbox quota usage and message count should be scheduled to run in off peak hours and used on one mailbox at a time.
reIndexMailbox (rim)	{name@domain id} {start status cancel} [type id]	
compactIndexMailbox (cim)	{name@domain id} {start status}	
verifyIndex (vi)	{name@domain id}	
getIndexStats (gis)	{name@domain id}	
selectMailbox (sm)	{account-name} [{zmmailbox commands}]	
unlockMailbox (ulm)	{name@domain id} [hostname]	Only specify the hostname parameter when unlocking a mailbox after a failed move attempt.

Miscellaneous Provisioning Commands

Table 72. `zmprov` — Miscellaneous Provisioning Commands

Command	Syntax	Example/Notes
countObjects (cto)	{type} [-d {domain id}]	<code>countObjects</code> can only be used with <code>zmprov -l/--ldap</code>
createBulkAccounts (cabulk)	{domain} {namemask} {number of accounts to create}	
describe (desc)	[[-v] [-ni] [{entry-type}]] [-a {attribute-name}]	Prints all attribute names (account, domain, COS, servers, etc.).
flushCache (fc)	[-a] {acl locale skin uistrings license all account config glo balgrant cos domain galgroup group mime server zimlet <extension-cache-type>} [name1 id1 [name2 i d2]]	Flush cached LDAP entries for a type. See Zimbra LDAP Service .

Command	Syntax	Example/Notes
generateDomainPreAuth Key (gdpak)	{domain id}	Generates a pre-authentication key to enable a trusted third party to authenticate to allow for single-sign on. Used in conjunction with <code>GenerateDomainPreAuth</code> .
generateDomainPreAuth (gdpa)	{domain id} {name} {name id foreignPrincipal} {timestamp 0} {expires 0}	Generates preAuth values for comparison.
syncGal (syg)	{domain} [{token}]	
getAccountLogger (gal)	[-s /--server hostname] {name@domain id}	

Logs Commands

Table 73. `zmprov` — Logs Commands

Command	Syntax	Example/Notes
addAccountLogger (aal)	{name@domain id} {logging-category} {debug info warn error}	Creates custom logging for a single account.
getAccountLoggers (gal)	[-s /--server hostname] {name@domain id} {logging-category} {debug info warn error}	
getAllAccountLoggers (gaal)	[-s /--server hostname]	Shows all individual custom logger account.
removeAccountLogger (ral)	[-s / --server hostname] {name@domain id} {logging-category}	When name@domain is specified, removes the custom logger created for the account otherwise removes all accounts all account loggers from the system.
resetAllLoggers (rlog)	[-s /--server hostname]	This command removes all account loggers and reloads <code>/opt/zimbra/conf/log4j.properties</code> .

See the [zmprov Log Categories](#) for a list of logging categories.

Search Commands

Table 74. `zmprov` — Search Commands

Command	Syntax	Example/Notes
searchGAL (sg)	{domain} {name}	<code>zmprov sg joe</code>

Command	Syntax	Example/Notes
autoCompleteGal (acg)	{domain} {name}	
searchAccounts (sa)	[-v] {ldap-query} [limit] [offset] [sortBy {attribute}] [sortAscending 0 1] [domain {domain}]	
searchCalendarReso urces (scr)	[-v] domain {attr op value} [attr op value]	

Share Provisioning Commands

Table 75. `zmprov` — Share Provisioning Commands

Command	Syntax	Example/Notes
getShareInfo (gsi)	{owner-name owner-id}	

Unified Communication Service Commands

Table 76. `zmprov` — Unified Communication Service Commands

Command	Syntax	Example/Notes
createUCService (cucs)	{name} [attr1 value1 [attr2 value2]]	
deleteUCService (ducs)	{name id}	
getAllUCServices (gaucs)	[-v]	
getUCService (guucs)	[-e] {name id} [attr1 [attr2]]	
modifyUCService (mucs)	{name id} [attr1 value1 [attr2 value2]]	
renameUCService (ruucs)	{name id} {newName}	

IMAP/POP Proxy Commands

Table 77. `zmprov` — IMAP/POP Proxy Commands

Command	Example/Notes
getAllReverseProxyURLs (garpu)	Used to publish into nginx.conf the servers that should be used for reverse proxy lookup.
getAllReverseProxy Backends (garpb)	Returns the list of servers that have <code>zimbraReverseProxyLookupTarget=TRUE</code> . Indicates whether a mailbox server is available for lookup requests from the proxy.

Command	Example/Notes
<code>getAllReverseProxyDomains (garpd)</code>	Returns a list of all domains configured with <code>ZimbraSSLCertificate</code> <code>zimbraVirtualHostname</code> and <code>zimbraVirtualIPAddress</code> configured. This allows the proxy to configure a list of domains to serve customized/domain certificates for.

Examples — using zmprov

Example 44. Creating an account with a password that is assigned to the default COS

```
zmprov ca name@domain.com password
```

Example 45. Creating an account with a password that is assigned to a specified COS

You must know the COS ID number. To find a COS ID:

```
zmprov gc <CO$name>
zmprov ca name@domain.com password zimbraCOS cosIDnumberstring
```

Example 46. Creating an account when the password is not authenticated internally

```
zmprov ca name@domain.com ''
```

The empty single quote is required and indicates that there is no local password.

Example 47. Using a batch process to create accounts

See [Provisioning User Accounts](#) for the procedure.

Example 48. Bulk provisioning

See the Zimbra wiki page [Bulk_Provisioning](#).

Example 49. Adding an alias to an account

```
zmprov aaa accountname@domain.com aliasname@domain.com
```

Example 50. Creating a distribution list

```
zmprov cdl listname@domain.com
```

The ID of the distribution list is returned.

Example 51. Adding a member to a distribution list

```
zmprov adlm listname@domain.com member@domain.com
```



You can add multiple members to a list from the Administration Console.

Example 52. Changing the administrator's password

Use this command to change any password. Enter the address of the password to be changed.

```
zmprov sp admin@domain.com password
```

Example 53. Creating a domain that authenticates against Zimbra LDAP

```
zmprov cd marketing.domain.com zimbraAuthMech zimbra
```

Example 54. Setting the default domain

```
zmprov mcf zimbraDefaultDomain domain1.com
```

Example 55. Listing all COSS and their attribute values

```
zmprov gac -v
```

Example 56. Listing all user accounts in a domain (domain.com)

```
zmprov gaa domain.com
```

Example 57. Listing all user accounts and their configurations

```
zmprov gaa -v domain.com
```

Example 58. Enabling logger on a single server

```
zmprov ms server.com +zimbraServiceEnabled logger
```

Then type zmloggerctl start, to start the logger.

Example 59. Querying a value for a multi-valued attribute

```
zmprov gs server.com attribute=value
```

For example, `zmprov gs example.com zimbraServiceEnabled=ldap` to find out if the ldap service is enabled.

Example 60. Modify the purge interval

To modify the purge interval, set `zimbraMailPurgeSleepInterval` to the duration of time that the server should "sleep" between every two mailboxes.

```
zmprov ms server.com zimbraMailPurgeSleepInterval <Xm>
```

`X` is the duration of time between mailbox purges; `m` represents minutes. You could also set `<xh>` for hours.

Example 61. Customize the notification email

Modify `zimbraNewMailNotification` to customize the notification email template. A default email is sent from Postmaster notifying users that they have received mail in another mailbox. To change the template, you modify the receiving mailbox account. The variables are

- `${SENDER_ADDRESS}`
- `${RECIPIENT_ADDRESS}`
- `${RECIPIENT_DOMAIN}`
- `${NOTIFICATION_ADDRESSES}`
- `${SUBJECT}`
- `${NEWLINE}`

You can specify which of the above variables appear in the **Subject**, **From**, or **Body** of the email. The following example is changing the appearance of the message in the body of the notification email that is received at **name@domain.com**. You can also change the template in a class ofservice, use `zmprov mc`. The command is written on one line.

```
zmprov ma name@domain.com zimbraNewMailNotificationBody 'Important message from  
${SENDER_ADDRESS}.${NEWLINE}Subject:${SUBJECT}'
```

Example 62. Enable the SMS notification by COS, account or domain

```
zmprov mc <default> zimbingaFeatureCalendarReminderDeviceEmailEnabled TRUE  
zmprov ma <user1> zimbraFeatureCalendarReminderDeviceEmailEnabled TRUE  
zmprov md <domain> zimbraFeatureCalendarReminderDeviceEmailEnabled TRUE
```

Example 63. Enable the Activity Stream feature for a COS or set of users

```
zmprov mc <default> zimbraFeaturePriorityInboxEnabled TRUE  
zmprov ma <user1> zimbraFeaturePriorityInboxEnabled TRUE
```

Configure Auto-Grouped Backup from the CLI

Set the backup method in the global configuration, and you can override the configuration on a per server basis if you do not want a server to use the auto-grouped backup method.

To set up auto-grouped backup, you modify LDAP attributes using the `zmprov` CLI. Type the command as

```
zmprov mcf <ldap_attribute> <arg>
```

You can also set the attributes at the server level using `zmprov ms`.

The following LDAP attributes are modified:

- `zimbraBackupMode` — Set it to be `Auto-Grouped`. The default is `Standard`.
- `zimbraBackupAutoGroupedInterval` — Set this to the interval in either days or weeks that backup sessions should run for a group. The default is `'1d`. Backup intervals can be 1 or more days, entered as `xd (1d)`; or 1 or more weeks, entered as `xw (1w)`.
- `zimbraBackupAutoGroupedNumGroups` — This the number of groups to spread mailboxes over. The default is 7 groups.

Changing Conversations Thread Default

Messages can be grouped into conversations by a common thread. The default is to thread messages in a conversation by the `References` header. If there is no `References` header, the `Subject` is used to determine the conversation thread. The default options can be changed from the COS or for individual accounts.

```
zmprov mc [cosname] zimbraMailThreadingAlgorithm [type]
```

The types include:

- **none** — no conversation threading is performed.
- **subject** — the message will be threaded based solely on its normalized subject.
- **strict** — only the threading message headers (`References`, `In-Reply-To`, `Message-ID`, and `Resent-Message-ID`) are used to correlate messages. No checking of normalized subjects is performed.
- **references** — the same logic as "strict" with the constraints slightly altered so that the non-standard `Thread-Index` header is considered when threading messages and that a reply message lacking `References` and `In-Reply-To` headers will fall back to using subject-based threading.
- **subjrefs** — the same logic as "references" with the further caveat that changes in the normalized subject will break a thread in two.

Detecting Corrupted Indexes

Run `zmprov verifyIndex` as a sanity check for the specified mailbox index. Diagnostic information is written to `stdout`. If problems are detected, a failure status is returned.

`verifyIndex` locks the index while it's running, and checks every byte in the index. Therefore, it's not recommended to run this on a regular basis such as in a cron job. The `zmprov verifyIndex` command should be used only when you need to make a diagnosis.

```
zmprov verifyIndex <user@example.com>
```

If `verifyIndex` reports that the index is corrupted, you can repair the mailbox index by running `reIndexMailbox (rim)`.

```
zmprov rim <user@example.com> start
```

Table 78. zmprov — Log Categories

<code>zimbra.account</code>	Account operations
<code>zimbra.acl</code>	ACL operations
<code>zimbra.backup</code>	Backup and restore
<code>zimbra.cache</code>	Inmemory cache operations
<code>zimbra.calendar</code>	Calendar operations
<code>zimbra.dav</code>	DAV operations
<code>zimbra.dbconn</code>	Database connection tracing
<code>zimbra.extensions</code>	Server extension loading
<code>zimbra.filter</code>	Mail filtering
<code>zimbra.gal</code>	GAL operations
<code>zimbra.imap</code>	IMAP protocol operations
<code>zimbra.index</code>	Index operations
<code>zimbra.io</code>	Filesystem operations
<code>zimbra.ldap</code>	LDAP operations
<code>zimbra.lmtp</code>	LMTP operations (incoming mail)
<code>zimbra.mailbox</code>	General mailbox operations
<code>zimbra.misc</code>	Miscellaneous
<code>zimbra.op</code>	Changes to mailbox state
<code>zimbra.pop</code>	POP protocol operations
<code>zimbra.redolog</code>	Redo log operations
<code>zimbra.security</code>	Security events
<code>zimbra.session</code>	User session tracking
<code>zimbra.smtp</code>	SMTP operations (outgoing mail)
<code>zimbra.soap</code>	SOAP protocol
<code>zimbra.sqltrace</code>	SQL tracing
<code>zimbra.store</code>	Mail store disk operations
<code>zimbra.sync</code>	Sync client operations

<code>zimbra.system</code>	Startup/shutdown and other system messages
<code>zimbra.wiki</code>	Wiki operations
<code>zimbra.zimlet</code>	Zimlet operations

zmaccts

Use `zmaccts` to run a report that lists all the accounts, their status, when they were created and the last time anyone logged on. The domain summary shows the total number of accounts and their status.

Syntax

```
zmaccts
```

zmarchiveconfig

Use `zmarchiveconfig` for configuring the archiving mailbox. It has the option of using short commands or full names for commands that lead to the same function being carried out.

Syntax

```
zmarchiveconfig [args] [cmd] [cmd-args]...
```

Description

Long Name	Short Name	Description
<code>--help</code>	<code>-h</code>	Displays the usage options for this command
<code>--server</code>	<code>-s</code>	(host)[:(port)] Displays the server hostname and optional port
<code>--account</code>	<code>-a</code>	(name) Returns the value of the account name to be authorized
<code>--ldap</code>	<code>-l</code>	Allows archiving to be provisioned via LDAP
<code>--password</code>	<code>-p</code>	(pass) Returns the password for auth account
<code>--passfile</code>	<code>-P</code>	(file) Allows password to be read from file
<code>--zadmin</code>	<code>-z</code>	Allows use of Zimbra admin/password from local
<code>--debug</code>	<code>-d</code>	Activates debug mode (dumps SOAP messages)
Command in		

Long Name	Short Name	Description
enable <account>		[archive-address <aaddr> [archive-cos <cos>] [archive-create <TRUE/FALSE>] [archive-password <pa [zimbraAccountAttrName <archive-attr-value]>+]
disable <account>		

zmarchivectl

Use `zmarchivectl` to start, stop, reload, or check the status of the Zimbra account archive.

Syntax

```
zmarchivectl start|stop|reload|status
```

zmarchivesearch

Use `zmarchivesearch` to search across account archives. You can search for archives that match specific criteria and save copies to a directory.

Syntax

```
zmarchivesearch {-m <user@domain.com>} {-q <query_string>} [-o <offset>] [-l <limit>] [-d <output_directory>]
```

Description

Long Name	Short Name	Description
--dir	-d	<arg> Folder to write messages to. If none is specified, then only the headers are fetched. Filenames are generated in the form <code>RESULTNUM_ACCOUNT-ID_MAILITEMID</code>
--help	-h	Displays help messages
--limit	-l	<arg> Sets the limit for the number of results returned. The default is 25
--mbox	-m	<arg> Name of archive account to search
--offset	-o	<arg> Specifies where the hit list should begin. The default is 0
--query	-q	<arg> The query string for archive search
--server	-s	<arg> Mail server hostname. Default is localhost
--verbose	-v	Allows printing of status messages while the search is being executed

Example 64. Search archives on a specified server and put a copy of the archive in a specified directory

```
zmarchivesearch -m user1@yourdomain.com -q "in:sent" -o 0 -l 30 -d /var/tmp
```

zmbackup

Use **zmbackup** to perform full backups and incremental backups for a designated mail host.

This utility has short option names and full names. The short option is preceded by a single dash, while the full option is preceded by a double dash. For example, **-f** is the same as **--fullBackup**.

Syntax

One of **-f**, **-i**, or **-del** must be specified.

```
zmbackup {-f | -i | del} {-a <arg>} [options]
```

Description

Long Name	Short Name	Description
--account	-a	<arg> Account email addresses separated by white space or all for all accounts. This option is not specified for auto-grouped backups since the system knows which accounts to backup every night.
--debug	-d	Display diagnostics for debugging purposes.
--delete	-del	<arg> Deletes the backups including and prior to the specified label, date (YYYY/MM/DD[hh:mm:ss]) or period (nn(d m y)).
--excludeBlobs		Exclude blobs from full backup. If unspecified, use server config
--excludeHsmBlobs		Exclude blobs on HSM volumes from full backup; if unspecified, use server config
--excludeSearchIndex		Exclude search index from full backup; if unspecified, use server config
--fullBackup	-f	Starts a full backup. In auto-grouped backup mode, this option also copies the redologs since the last backup (which is the main function of an incremental backup).
--help	-h	Displays the usage options for this command.
--incrementalBackup	-i	Starts an incremental backup. This option is not available in the auto-grouped backup mode.

Long Name	Short Name	Description
--includeBlobs		Include blobs in full backup. If this is unspecified, the server config is used.
--includeHsmBlobs		Include blobs on HSM volumes in full backup. If this is unspecified, the server config is used.
--includeSearchIndex		Include search index in full backup. If this is unspecified, the server config is used.
--noZip		Backs up blobs as individual files rather than in zip files.
--server	-s	<arg> Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name.
--sync	-sync	Runs full backup synchronously.
--target	-t	<arg> Specifies the target backup location. The default is /opt/zimbra/backup.
--zip	-z	Backs up blobs in compressed zip files. Ignored if --zipStore is specified.
--zipStore		Backup blobs in zip file without compression. (default)

Examples

In these examples, the server (**-s**) is `server1.domain.com`. The (**-t**) is not required if the target is the default directory, (`/opt/zimbra/backup`).

*Example 65. Perform a full backup of all mailboxes on **server1***

```
zmbbackup -f -a all -s server1.domain.com
```

*Example 66. Perform incremental backup of all mailboxes on **server1** since last full backup*

```
zmbbackup -i -a all -s server1.domain.com
```

*Example 67. Perform full backup of only **user1**'s mailbox on **server1**.*

```
zmbbackup -f -a user1@domain.com -s server1
```



Hostname does not need full domain if account is used.

Example 68. Perform incremental backup of user1's mailbox on server1

```
zmbbackup -i -a user1@domain.com -s server1
```

zmblobchk

Use **zmblobchk** to check the consistency of the Zimbra blob store ([/opt/zimbra/store](#)). This command checks and records notes of files without matching database metadata. It also checks to make sure that size information is correct for the files.

Syntax

```
zmblobchk [options] start
```

The start command is required to avoid unintentionally running a blob check. The ID values are separated by commas.

Description

Long Name	Short Name	Description
--export-dir		<path> Target directory for database export files.
--help	-h	Displays help messages
--mailboxes	-m	<mailbox-ids> Specify which mailboxes to check. If not specified, check all mailboxes.
--missing-blob-delete		Delete any items that have a missing blob.
-item		
--no-export		Delete items without exporting
--skip-size-check		Skip blob size check
--unexpected-blob-list		<path> Write the paths of any unexpected blobs to a file
--verbose	-v	Display verbose output; display stack trace on error
--volumes		<volume-ids> Specify which volumes to check. If not specified, check all volumes

zmcalchk

Use **zmcalchk** to check the consistency of appointments on the Zimbra calendar and sends an email notification regarding inconsistencies. For example, it checks if all attendees and organizers of an event on the calendar agree on start/stop times and occurrences of a meeting.

See the output of `zmmailbox help appointment` for details on time-specs.

Syntax

```
zmcalchk [-d] [-n <type>] <user> <start-time-spec> <end-time-spec>
```

Description

Short Name	Description
<code>-d</code>	Debugs verbose details
<code>-m</code>	Allows the user to specify the maximum number of attendees to check. The default value is 50.
<code>-n</code>	<code>-n none user organizer attendee all</code> Send email notifications to selected users if they are out of sync for an appointment

zmschedulebackup

Use `zmschedulebackup` to schedule backups and add the command to your cron table.

The default schedule is as follows:

- Full backup, every Saturday at 1:00 a.m. (`0 1 * * 6`)
- Incremental backup, Sunday through Friday at 1:00 a.m. (`0 1 * * 0-5`)

Each crontab entry is a single line composed of five fields separated by a blank space. Specify the fields as follows:

- minute — 0 through 59
- hour — 0 through 23
- day of the (month) — 1 through 31
- month — 1 through 12
- day of the (week) — 0 through 7 (0 or 7 is Sunday, or use names)

Type an asterisk (*) in the fields you are not using.

This command automatically writes the schedule to the crontab.

Syntax

```
zmschedulebackup {-q|-s|-A|-R|-F|-D}[f|i|d] ["schedule"]
```

Description

Name	Command Name	Description
help	-h	Displays the usage options for this command.
query	-q	Default command. Displays the existing Zimbra backup schedule.
save	-s	Save the schedule. Allows you to save the schedule command to a text file so that you can quickly regenerate the backup schedule when the system is restored.
flush	-F	Removes the current schedule and cancels all scheduled backups.
append	-A	Adds an additional specified backup to the current schedule.
replace	-R	Replaces the current schedule with the specified schedule.
default	-D	Replaces the current schedule with the default schedule.

Options that will be passed to zmbackup

no compression	-n	Backs up blobs as individual files rather than in zip files
compress	-z	Backs up blobs in compressed zip files. Ignored if --zipStore is specified.
--zipStore		Backs up blobs in zip file without compression.
target	-t	<p>Can be used only to designate a full back target location. The default is /opt/zimbra/backup.</p> <div style="display: flex; align-items: center;"> i <p>You cannot designate a target for incremental backups. If a target (-t) location is added for incremental scheduled backups, it is ignored.</p> </div>
account	-a	Account specific. The default is all accounts.

Name	Command Name	Description
--mail-report		Send an email report to the admin user.
--server		server - Mail server hostname. Default is localhost.
--sync		Runs full backup synchronously.
--excludeBlobs		Exclude blobs from full backup. If unspecified, server config is used.
--includeBlobs		Include blobs in full backup. If unspecified, the server config is used.
--excludeHsmBlobs		Exclude blobs on HSM volumes from full backup. If unspecified, the server config is used.
--includeHsmBlobs		Include blobs on HSM volumes in full backup. If unspecified, the server config is used.
--excludeSearchIndex		Exclude search index form full backup. If unspecified, the server config is used.
--includeSearchIndex		Include search index in full backup. If unspecified, the server config is used.

Cron schedule `zmschedulebackup-type: <i | f | d arg>`

incremental backup	i	<time specifier> Incremental backup. Incremental backup is not used with the auto-grouped backup mode.
full backup	f	Full backup
delete	d <arg>	Delete backups. <arg> is n(d m y)

Backup Scheduling Examples

Example 69. Schedule the default full and incremental backup

```
zmschedulebackup -D
```

Example 70. Replace the existing schedule with a new schedule

```
zmschedulebackup -R f ["schedule"]
```

Example 71. Add an additional full backup to the existing schedule

```
zmschedulebackup -A f ["schedule"]
```

Example 72. Add an additional incremental backup to the existing schedule

```
zmschedulebackup -A i ["schedule"]
```

Example 73. Display the existing schedules

```
zmschedulebackup -q
```

Example 74. Display the schedules on one line

Display the schedules on one line as a command, so that they can be copied to a text file and saved to be used if the application needs to be restored.

```
zmschedulebackup -s
```

zmbackupabort

Use **zmbackupabort** to stop a backup process. Before you can abort an account you must know its backup label. This label is displayed after you start the backup procedure. If you do not know the label, use **zmbackupquery** to find the label name.

To stop the restore process:

The **zmbackupabort -r** interrupts an ongoing restore. The restore process is stopped after the current account is restored. The command displays message showing which accounts were not restored.

Syntax

```
zmbackupabort [options]
```

Description

Long Name	Short Name	Description
--debug	-d	Display diagnostics for debugging purposes
--help	-h	Displays the usage options for this command
--label	-lb	<arg> Label of the full backup to be aborted. Use <code>zmbackupquery</code> , to find the label name.
--restore	-r	Abort the restore in process
--server	-s	<arg> Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name.
--target	-t	<arg> Specifies the target backup location. The default is <code>/opt/zimbra/backup</code> .

zmbackupquery

Use `zmbackupquery` to find full backup sets. The command can be used to find a specific full backup set or full backup sets since a specific date, or all backup sets in the backup directory.

To find out the best full backup to use as the basis for point-in-time restore of an account, run a command like this:

```
zmbackupquery -a <account email> --type full --to <restore-to time>
```

Syntax

```
zmbackupquery [options]
```

Description

Long Name	Short Name	Description
--account	-a	<arg> Account email addresses separated by white space or all for all accounts
--debug	-d	Display diagnostics for debugging purposes
--help	-h	Displays the usage options for this command
--from		<arg> List backups whose start date/time is at or after the date/time specified here.

Long Name	Short Name	Description
--label	-lb	<arg> The label of the full backup session to query. An example of a label is <code>backup200507121559510</code> .
--server	-s	<arg> Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name.
--target	-t	<arg> Specifies the backup target location (The default is <code>/opt/zimbra/backup</code> .)
--to		<arg> List backups whose start date/time is at or before the date/time specified here.
--type		<arg> Backup set type to query. "full" or "incremental", both are queried if one is not specified.
--verbose	-v	Returns detailed status information

Specify date/time in one of these formats:

`2008/12/16 12:19:23`

`2008/12/16 12:19:23 257`

`2008/12/16 12:19:23.257`

`2008/12/16-12:19:23-257`

`2008/12/16-12:19:23`

`20081216.121923.257`

`20081216.121923`

`20081216121923257`

`20081216121923`

Specify year, month, date, hour, minute, second, and optionally millisecond.

Month/date/hour/minute/second are 0-padded to 2 digits, millisecond to 3 digits.

Hour must be specified in 24-hour format, and time is in local time zone.

zmrestore

Use `zmrestore` to perform full restores and incremental restores for a designated mail host. You can either specify specific accounts, or, if no accounts are specified, all accounts in the backup are restored. In addition, you can restore to a specific point in time.

This utility has short option names and full names. The short option is preceded by a single dash, the full option is proceeded by a double dash. For example, `-rf` is the same as `--restorefullBackupOnly`.

Syntax

```
zmrestore [options]
```

Description

Long Name	Short Name	Description
--account	-a	<arg> Specifies the account email addresses. Separate accounts with a blank space or type all to restore all accounts.
--backedupRedologs	-br	Replays the redo logs in backup only, which Only excludes archived and current redo logs of the system.
--continueOnError	-c	Continue to restore other accounts when an error occurs.
--createAccount	-ca	Restores accounts to target accounts whose names are prepended with prefix. (Can only be used in commands that use the -pre option.)
--debug	-d	Display diagnostics for debugging purposes.
--excludeBlobs		Do not restore blobs (HSM or not).
--excludeHsmBlobs		Do not restore HSM blobs.
--excludeSearchIndex		Do not restore search index.
--help	-h	Displays the usage options for this command.
--label	-lb	<arg> The label of the full backup to restore. Restores to the latest full backup if this is omitted.
--prefix	-pre	<arg> The prefix to pre-pend to the original account names.
--restoreAccount	-ra	Restores the account in directory service.
--restoreToIncrLabel		<arg> Replay redo logs up to and including this incremental backup
--restoreToredoSeq		<arg> Replay up to and including this redo log sequence.
--restoreToTime		<arg> Replay redo logs until this time.
--restorefullBackupOnly	-rf	Restores to the full backup only, not any incremental backups since that backup.

Long Name	Short Name	Description
--server	-s	<arg> Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name.
--skipDeletes		If true, do not execute delete operation during redo log replay.
--skipDeletedAccounts		Do not restore if named accounts were deleted or did not exist at backup time. (This option is always enabled with -a all)
--systemData	-sys	Restores global tables and local config.
--target	-t	<arg> Specifies the backup target location. The default is /opt/zimbra/backup.

Examples

Example 75. Perform complete restore of all accounts on server1

Perform complete restore of all accounts on **server1**, including last full backup and any incremental backups since last full backup.

```
zmrestore -a all -s server1.domain.com
```

Example 76. Perform restore only to last full backup

Perform restore only to last full backup, excluding incremental backups since then, for all accounts on **server1**.

```
zmrestore -rf -a all -s server1.domain.com
```

Example 77. Create a new account from a backup of the target account

The name of the new account will be new_user1@domain.com.

```
zmrestore -a user1@domain.com -ca -pre new_
```

zmrestoreoffline (Offline Restore)

zmrestoreoffline requires that the following is true:

- **mailboxd** IS NOT running

- SQL database IS RUNNING
- LDAP directory IS RUNNING

Pre-requisites

Syntax

```
zmrestoreoffline [options]
```

Description

Long Name	Short Name	Description
--account	-a	<arg> Specifies the account email addresses. Separate accounts with a blank space or state all for restoring all accounts. Required .
--backedupRedoLogsOnly	-br	Replays the redo logs in backup only, which excludes archived and current redo logs of the system.
--continueOnError	-c	Continue to restore other accounts when an error occurs.
--createAccount	-ca	Restores accounts to new target accounts whose names are pre-pended with prefix.
--debug	-d	Display diagnostics for debugging purposes.
--help	-h	Displays the usage options for this command.
--ignoreRedoErrors		If true, ignore all errors during redo log replay.
--label	-lb	<arg> The label of the full backup to restore. Type this label to specify a backup file other than the latest.
--prefix	-pre	<prefix> The prefix to pre-pend to the original account names.
--restoreAccount	-ra	Restores the account in directory service.
--restoreToIncrLabel		<arg> Replay redo logs up to and including this incremental backup.
--restoreToredoSeq		<arg> Replay up to and including this redo log sequence.
--restoreToTime		<arg> Replay redo logs until this time.
--restoreFullBackupOnly	-rf	Restores to the full backup only, not any incremental backups since that backup.

Long Name	Short Name	Description
--server	-s	<arg> Mail server host name. For format, use either the plain host name or the server.domain.com name. The default is the localhost name. If -s is specified, this must be localhost.
--skipDeletedAccounts	-skipDeletedAccounts	Do not restore if named accounts were deleted or did not exist at backup time. (This option is always enabled with -a all)
--systemData	-sys	Restores global tables and local config.
--target	-t	<arg> Specifies the backup target location. The default is /opt/zimbra/backup.

Examples

Before you begin `zmrestoreoffline`, the LDAP directory server must be running.

Example 78. Perform a complete restore of all accounts on server1

Perform a complete restore of all accounts on **server1**, including last full backup and any incremental backups since last full backup.

```
zmrestoreoffline -s server1.domain.com
```

zmrestoreldap

Use `zmrestoreldap` to restore accounts from the LDAP backup.

Syntax

```
zmrestoreldap {-lb <arg>} {-t <arg>} [options]
```

Description

Short Name	Description
-lb	<arg> Session label to restore from. For example, <code>full20061229182113</code> .
-t	<arg> Specifies the backup target location. The default is /opt/zimbra/backup.
-lbs	Lists all session labels in backup.
-l	Lists accounts in file.
-a	<arg> Restores named account(s). List account names separated by white space.

zmcontrol (Start/Stop/Restart Service)

Use **zmcontrol** to start, to stop, or to restart services. You can also find which version of the Zimbra Collaboration is installed.

Syntax

```
zmcontrol [ -v -h ] command [args]
```

Description

Long Name	Short Name	Description
	-v	Displays ZCS software version.
	-h	Displays the usage options for this command.
	-H	Host name (localhost).

Command in

maintenance	Toggle maintenance mode.
restart	Restarts all services and manager on this host.
shutdown	Shutdown all services and manager on this host. When the manager is shutdown, you cannot query that status.
start	Startup manager and all services on this host.
startup	Startup manager and all services on this host.
status	Returns services information for the named host.
stop	Stop all services but leaves the manager running.

zmmboxsearch (Cross Mailbox Search)

Use **zmmboxsearch** is used to search across mailboxes. You can search across mailboxes to find messages and attachments that match specific criteria and save copies of these messages to a directory.

Syntax

```
zmmboxsearch {-m <arg>} {-q <arg>} [-o <arg>] [-l <arg>] [-d <arg>] [options]
```

Description

Long Name	Short Name	Description
--dir	-d	<arg> Folder to write the messages to. If none is specified, then only the headers are fetched. Files names are generated in the form RESULTNUM_ACCOUNT-ID_MAILITEMID .
--help	-h	Displays help information.
--limit	-l	Sets the limit for the number of results returned. The default is 25.
--mbox	-m	<arg> Comma-separated list of mailboxes to search. UIDs or email-address or /SERVER/MAILBOXID or * .
--offset	-o	<arg> Specify where the hit list should start. The default is 0.
--query	-q	<arg> The query string for the search.
--server	-s	<arg> Mail server hostname. default is the localhost
--verbose	-v	Request that the status message print while the search is being executed.

Example

The following example performs a cross-mailbox search in the inbox folder of two different mailboxes on the specified server and puts a copy of the found messages in to the specified directory.

Example 79. Cross-mailbox search

```
zmmboxsearch -m user1@yourdomain.com,user2@yourdomain.com -q "in:inbox" -d
/var/tmp
```

zmmboxmove

Use **zmmboxmove** to move mailboxes. The destination server manages the overall move process. Using the **zmmboxmove** command significantly reduces the account lockout time.

The CLI command **zmmboxmove** is used to move mailboxes from one Zimbra server to another. Mailboxes can be moved between Zimbra servers that share the same LDAP server. All the files are copied to the new server and the LDAP is updated. After the mailbox is moved to a new server a copy still remains on the older server, but the status of the old mailbox is **closed**. Users cannot log on and mail is not delivered. You should check to see that all the mailbox content was moved successfully before purging the old mailbox.

Syntax

```
zmmboxmove -a <email> --from <src> --to <dest> [--sync]
```

Description

Long Name	Short Name	Description
--account	-a	<arg> Email address of account to move.
--help	-h	Displays the usage options for this command.
--from	-f	<arg> Mail server hostname. Server where the --account mailbox is located.
--to	-t	<arg> Destination server.
--sync	-sync	Run synchronously

zmmboxmovequery

Use `zmmboxmovequery` to query ongoing mailbox moves on a server, both move-ins and move-outs.

Syntax

```
zmmboxmovequery -a <account email> [-s <server to query>]
```

zmpurgeoldmbox

Use `zmpurgeoldmbox` to purge the mailbox from the older server after a mailbox move.

Syntax

```
zmpurgeoldmbox -a <account email> [-s <server to purge>]
```

Description

Long Name	Short Name	Description
--account	-a	<arg> Email address of account to purge.
--help	-h	Displays the usage options for this command
--server	-s	<arg> Mail server hostname. Old server where the account existed

zmgsutil

Use `zmgsutil` to create or delete the GAL sync account, and to force syncing of the LDAP data to the GAL sync account.

A GAL sync account is created when the GAL is configured on a domain. This account is created and the polling interval for performing a full sync is managed from the Administration Console.

To see attributes and settings for a GAL sync account, run `zmprov gds` against the account.

Long Name	Description
<code>createAccount</code>	<p>Creates the GAL sync account. This should be done from the Administration Console.</p> <p>The parameter "server" is required.</p> <pre>-a {account-name} -n {datasource-name} --domain {domain-name} -t zimbra ldap -s {server} [-f {folder-name}] [-p {polling-interval}]</pre>
<code>addDataSource</code>	<p>When configuring a datasource for a server, specify a folder name other than <code>/Contacts</code>. The datasource folder name must be unique.</p> <pre>-a {account-name} -n {datasource-name} --domain {domain-name} -t zimbra ldap [-f {folder-name}] [-p {polling-interval}]</pre>
<code>deleteAccount</code>	<p>Deletes the GAL sync account and the references to the LDAP server. The account can also be deleted from the Administration Console.</p> <pre>deleteAccount [-a {galsyncaccountname}] -i {account-id}]</pre>
<code>trickleSync</code>	<p>This syncs new and updated contact data only.</p> <pre>[-a {galsyncaccountname}] -i {account-id}] [-d {datasource-id}] [-n {datasource-name}]</pre> <p>The datasource ID the LDAP datasource ID. The datasource name is the name of the address book (folder) in the GAL account created to sync LDAP to.</p> <p>A cron job can be set up to run <code>trickleSync</code>.</p>
<code>fullSync</code>	<p>This syncs all LDAP contact data. You can also set this from the Administration Console.</p> <pre>[-a {galsyncaccountname}] -i {account-id}] [-d {datasource-id}] [-n {datasource-name}]</pre>

Long Name	Description
<code>forceSync</code>	<p>This should be used to reload the entire GAL if there is change in the filter, attribute mapping or LDAP server parameters.</p> <p><code>[-a {galsyncaccountname}] [-i {account-id}]</code> <code>[-d {datasource-id}] [-n {datasource-name}]</code></p>

zmldappasswd

Use `zmldappasswd` to change the LDAP password on the local server. In multi node environments, this command must be run on the LDAP master server only.

This CLI command used with options changes other passwords.

For better security and audit trails the following passwords are generated in ZCS:

- **LDAP Admin password.** This is the master LDAP password.
- **LDAP Root password.** This is used for internal LDAP operations.
- **LDAP Postfix password.** This is the password used by the `postfix` user to identify itself to the LDAP server and must be configured on the MTA server to be the same as the password on the LDAP master server.
- **LDAP Amavis password.** This is the password used by the `amavis` user to identify itself to the LDAP server and must be configured on the MTA server to be the same as the password on the LDAP server.
- **LDAP Replication password.** This is the password used by the `LDAPreplication` user to identify itself to the LDAP master and must be the same as the password on the LDAP master server.

Syntax

```
zmldappasswd [-h] [-r] [-p] [-l] new-password
```

Description

Name	Syntax, Example, Notes
<code>-h</code>	Displays the help.
<code>-a</code>	Changes <code>ldap_amavis-password</code> .
<code>-b</code>	Changes <code>ldap_bes_searcher_password</code> .
<code>-l</code>	Changes <code>ldap_replication_password</code> .
<code>-p</code>	Changes <code>ldap_postfix_password</code> .
<code>-n</code>	Changes <code>ldap_nginx_password</code> .
<code>-r</code>	Changes <code>ldap_root_passwd</code> .

Name	Syntax, Example, Notes
-c	Updates the password in the config database on replicas. Must be used with -1 and must be run on a replica after changing the password on the master. Only one of a, l, p, or r can be specified. If options are not included, the zimbra_ldap_password is changed.

zmlocalconfig

Use `zmlocalconfig` to set or get the local configuration for a Zimbra server. Use `zmlocalconfig -i` to see a list of supported properties that can be configured by an administrator.

Syntax

```
zmlocalconfig [options]
```

To see the local config type `zmlocalconfig`.

Description

Long Name	Short Name	Description
--config	-c	<arg> File in which the configuration is stored.
--default	-d	Show default values for keys listed in [args].
--edit	-e	Edit the configuration file, change keys and values specified. The [args] is in the key=value form.
--force	-f	Edit the keys whose change is known to be potentially dangerous.
--help	-h	Shows the help for the usage options for this tool.
--info	-i	Shows the list of supported properties.
--format	-m	<arg> Shows the values in one of these formats: plain (default), xml, shell, nokey.
--changed	-n	Shows the values for only those keys listed in the [args] that have been changed from their defaults.
--path	-p	Shows which configuration file will be used.
--quiet	-q	Suppress logging.
--random	-r	This option is used with the edit option. Specified key is set to a random password string.
--show	-s	Forces the display of the password strings.

Long Name	Short Name	Description
--unset	-u	Remove a configuration key. If this is a key with compiled-in defaults, set its value to the empty string.
--expand	-x	Expand values.
--zimbraAmavisMaxServers		Allows control of the concurrency of Amavisd (default 10).
--zimbraClamAVMaxThreads		Allows control of the concurrency of ClamAV (default 10).

zmmailbox

Use `zmmailbox` for mailbox management. The command can help administrators provision new mailboxes along with accounts, debug issues with a mailbox, and help with migrations.

You can invoke the `zmmailbox` command from within the `zmpprov` command. You enter `selectMailbox` within `zmpprov` to access the `zmmailbox` command connected to that specified mailbox. You can then enter `zmmailbox` commands until you type exit. Exit returns you to `zmpprov`. This is useful when you want to create accounts and also pre-create some folders, tags, or saved searches at the same time.

Syntax

```
zmmailbox [args] [cmd] [cmd-args]...
```

Description

Short Name	Long Name	Syntax, Example, and Notes
-h	--help	Display usage.
-f	--file	Use file as input stream.
-u	--url	<code>http[s]://{host}[:{port}]</code> server hostname and optional port. Must use admin port with <code>-z/-a</code> .
-a	--account	Account name to auth as <code>{name}</code> .
-z	--zadmin	Use zimbra admin name/password from localconfig for admin/password.
-y	--authtoken <code>{authtoken}</code>	Use authtoken string (has to be in JSON format) from command line.
-Y	--authtoken <code>{authtoken-file}</code>	Use authtoken string (has to be in JSON format) from a file.
-m	--mailbox <code>{name}</code>	Mailbox to open. Can be used as both authenticated and targeted unless other options are specified.

Short Name	Long Name	Syntax, Example, and Notes
	--auth {name}	Account name to authorize as. Defaults to --mailbox unless --admin-priv is used.
-A	--admin-priv	Execute requests with admin privilege.
-P	--password {pass}	Password for admin account and or mailbox.
-P	--passfile {file}	Read password from file.
-t	--timeout	Timeout (in seconds).
-v	--verbose	Verbose mode (dumps full exception stack trace)
-d	--debug	Debug mode (dumps SOAP messages)

Specific CLI tools are available for the different components of a mailbox. Usage is described in the CLI help for the following.

<code>zmmailbox help admin</code>	Help on admin-related commands.
<code>zmmailbox help commands</code>	Help on all <code>zmmailbox</code> commands.
<code>zmmailbox help appointment</code>	Help on appointment-related commands.
<code>zmmailbox help contact</code>	Help on contact-related commands (address book).
<code>zmmailbox help conversation</code>	Help on conversation-related commands.
<code>zmmailbox help filter</code>	Help on filter-related commands.
<code>zmmailbox help folder</code>	Help on folder-related commands.
<code>zmmailbox help item</code>	Help on item-related commands.
<code>zmmailbox help message</code>	Help on message-related commands.
<code>zmmailbox help misc</code>	Help on miscellaneous commands.
<code>zmmailbox help right</code>	Help on right commands.
<code>zmmailbox help search</code>	Help on search-related commands.
<code>zmmailbox help tag</code>	Help on tag-related commands.

Examples

Example 80. Create tags and folders

When you create an account, you may want to pre-create some tags and folders. You can invoke `zmmailbox` inside of `zmprov` by using `selectMailbox(sm)`.

```
$ zmprov  
prov> ca user10@domain.example.com test123  
9a993516-aa49-4fa5-bc0d-f740a474f7a8  
prov> sm user10@domain.example.com  
mailbox: user10@domain.example.com, size: 0 B, messages: 0, unread: 0  
mbox user10@domain.example.com> createFolder /Archive  
257  
mbox user10@domain.example.com> createTag TODO  
64  
mbox user10@domain.example.com> createSearchFolder /unread "is:unread"  
258  
mbox user10@domain.example.com> exit  
prov>
```

Example 81. Find the mailbox size for an account

```
zmmailbox -z-m user@example.com gms
```

Example 82. Send requests to a mailbox using the admin auth token

This is required when using the command `emptyDumpster`. Use `--admin-priv` to skip delegated auth as the target mailbox.

```
zmmailbox -z --admin-priv -m foo@example.com emptyDumpster
```

Example 83. Use `--admin-priv` with select Mailbox command

```
zmmailbox -z  
mbox> sm --admin-priv foo@domain.com
```

Example 84. Authenticate as a delegated admin user

This lets one user login to another user's mailbox. The authenticating user must be a delegated admin account and must have the `adminLoginAs` right on the target mailbox. This auth option uses a non-admin auth token. Use the `--auth` option to specify the authenticating account. To login as user `bar` and open mailbox `foo`:

```
$ zmmailbox --auth bar@example.com -p password -m foo@example.com
```

Example 85. Find the mailbox size for an account

```
zmmailbox -z -m user@example.com gms
```

Example 86. Backup mailbox content in a `zip` file

When you use `zmmailbox` to backup individual mailboxes, you can save the file as either a `zip` file or a `tgz` file. The default settings for the information that is saved in these formats is different.

File	TGZ	ZIP
Briefcase	X	X
Calendar		X
Conversations		X
Contacts	X	X
Deleted Messages	X	X
Emailed Contacts		X
Inbox	X	X
Sent	X	X
Sent Messages	X	X
Tasks		X

To include all the mailbox content in a `zip` file, you must enable the meta data. Type as:

```
zmmailbox -z -m user@example.com gru "?fmt=zip&meta=1" > <filename.zip>
```

zmtlsctl

Use `zmtlsctl` to set the Web server `zimbraMailMode` to the communication protocol options: HTTP, HTTPS, Mixed, Both and Redirect. The default setting is HTTPS.

The `zmtlsctl` setting also impacts the ZCO's **Use Secure Connection** setting. ZCO users in a self-signed environment will encounter warnings about connection security unless the root CA certificate is added to Window Certificate Store. See the Zimbra Wiki article [ZCO Connection Security](#) for more information.

- **HTTP.** HTTP only, the user would browse to <http://zimbra.domain.com>.
- **HTTPS.** HTTPS only (default), the user would browse to <https://zimbra.domain.com>. `http://` is denied.
- **Mixed** If the user goes to `http://` it will switch to `https://` for the login only, then will revert to `http://` for normal session traffic. If the user browses to `https://`, then the user will stay `https://`
- **Both** A user can go to `http://` or `https://` and will keep that mode for the entire session.
- **Redirect** Like mixed if the user goes to `http://` it will switch to `https://` but they will stay `https://` for their entire session.

All modes use TLS encryption for back-end administrative traffic.

Only `zimbraMailMode` **HTTPS** can ensure that no listener will be available on HTTP/port 80, that no client application will try to auth over HTTP, and that all data exchanged with the client application will be encrypted.

Note, `mailboxd` has to be stopped and restarted for the change to take effect.

If you switch to HTTPS, you use the self-signed certificate generated during ZCS installation in `/opt/zimbra/ssl/zimbra/server/server.crt`. For ZCO users, secure ZCO profiles will display Certificate Trust dialogs unless the root CA certificate is deployed to the server. For more information about ZCO certificates, see the Zimbra Wiki page [ZCO Connection Security](#).

Syntax

```
zmtlsctl [mode]
```

`mode = http, https, mixed, both, redirect`

Steps to run

1. Type `zmtlsctl [mode]` and press **ENTER**.
2. Type `zmmailboxdctl stop` and press **ENTER**.
3. When `mailboxd` is stopped, type `zmmailboxdctl start` and press **ENTER**.

Limitations When Using Redirect

- Many client applications send an auth request in the initial HTTP request to the Server ("blind auth"). The implications of this are that this auth request is sent in the clear/unencrypted prior to any possible opportunity to redirect the client application to HTTPS.

- Redirect mode allows for the possibility of a man-in-the-middle attack, international/unintentional redirection to a non-valid server, or the possibility that a user will mis type the server name and not have certificate-based validity of the server.
- In many client applications, it is impossible for users to tell if they have been redirected (for example, ActiveSync), and therefore the users continue to use HTTP even if the auth request is being sent unencrypted.

zmhsms

Use **zmhsms** to start, stop (abort), and see the status of a HSM session. The threshold for when messages are moved to a storage volume is configured from the Administration Console, **Servers > Volumes** page.

Syntax

```
zmhsms {abort|start|status} {server} <name>
```

Description

Long Name	Short Name	Description
--abort	-a	Aborts the current HSM session. If all the messages in a mailbox being processed were not moved before you clicked Abort , no messages from that mailbox are moved from the primary volume. Messages for mailboxes that have completed the move to the secondary volume are not moved back to the primary volume.
--help	-h	Shows the help for the usage options for this tool.
--server	-s	<arg> The mail server host name. The default is the localhost [args].
--start	-t	Manually starts the HSM process.
--status	-u	The status of the last HSM session is displayed.

zmlicense

Use **zmlicense** to view and install your Zimbra license. The license can be viewed and installed from the Administration Console, **Global Settings > License** page.

Syntax

```
zmlicense [options]
```

Description

Long Name	Short Name	Description
--check	-c	Check to see if a valid license is installed.
--help	-h	Shows the help for the usage options for this tool.
--install	-i	<arg> Installs the specified license file.
--ldap	-l	Install on LDAP only.
--print	-p	Displays the license information.

zmmetadump

The `zmmetadump` command is a support tool that dumps the contents of an item's metadata in a human readable form.

Syntax

```
zmmetadump -m <mailbox id/email> -i <item id>
```

or

```
zmmetadump -f <file containing encoded metadata>
```

zmmypasswd

Use `zmmypasswd` to change `zimbra_mysql_password`. If the `--root` option is specified, the `mysql_root_passwd` is changed. In both cases, MariaDB is updated with the new passwords. Refer to the MariaDB documentation to see how you can start the MariaDB server temporarily to skip grant tables, to override the root password.



This requires a restart for the change to take effect.

Syntax

```
zmmypasswd [--root] <new_password>
```

zmplayredo

Users who maintain a backup and restore mechanism using the snapshot facility of the storage layer use `zmplayredo` to restore backed up data. This command brings all backed up data to the current state so that there is no loss of information during the restore process.

Syntax

```
zmplayredo <option>
```

Description

Long Name	Short Name	Description
--fromSeq		<arg> Replays snapshots from the specified redolog sequence.
--fromTime		<arg> Replays snapshots from the specified time.
--help	-h	Shows the help information for this command.
--logfiles		<arg> Replays the specified logfiles in order.
--mailboxId		<arg> Replays snapshots for the specified mailbox.
--queueCapacity		<arg> Used for specifying the queue capacity per player thread. The default value is 100.
--stopOnError		Stops the replay on occurrence of any error.
--threads		<arg> Specifies the number of parallel redo threads. The default value is 50.
--toSeq		<arg> Replays snapshots to the specified redolog sequence.
--toTime		<arg> Replays snapshots to the specified time.

Time is specified in the local time zone. The year, month, date, hour, minute, second, and optionally millisecond should be specified. Month/date/hour/ minute/second are 0-padded to 2 digits, millisecond to 3 digits. The hour must be specified in a 24-hour format.

zmproxyconfgen

Use **zmproxyconfgen** to generate the Nginx proxy configuration files. It reads LDAP settings to replace template variables and generates the final Nginx configuration.

Syntax

```
ProxyConfGen [options]
```

Description

Long Name	Short Name	Description
--config	-c	<arg> Overrides a config variable. The <arg> format should be <code>name=value</code> . To see a list of names, use <code>-d</code> or <code>-D</code> .

Long Name	Short Name	Description
--defaults	-d	Prints the default variable map.
--definitions	-D	Prints the Definitions variable map after loading LDAP configuration and processing overrides.
--help	-h	Displays help information.
--include-dir	-i	<arg> Displays the directory path (relative to \$workdir/conf), where included configuration files are written.
--dry-run	-n	Specifies not to write configuration and only display the files that would be written.
--prefix	-p	<arg> Displays the config file prefix. The default value is nginx.conf
--template-prefix	-P	<arg> Displays the template file prefix. The default value is \$prefix.
--server	-s	<arg> Specifies a valid server object. Configuration is generated based on the specified server's attributes. The default is to generate configuration based on global configuration values.
--templatelocation	-t	<arg> Specifies the proxy template directory. The default value is \$workdir/conf/nginx/templates.
--verbose	-v	Displays verbose data.
--workdir	-w	<arg> Specifies the proxy working directory. The default value is /opt/zimbra.

zmproxypurge

Use `zmproxypurge` to purge POP/IMAP proxy routing information from one or more memcached servers. Available memcached servers are discovered by the `zmprov gamcs` function. Others can be specified if necessary using the server port.

Syntax

```
ProxyPurgeUtil [-v] [-i] -a account [-L accountlist] [cache1] [cache2]...
```

Description

Long Name	Short Name	Description
--help	-h	Shows the help for the usage options for this tool.

Long Name	Short Name	Description
--verbose	-v	Displays verbose data.
--info	-i	Displays account routing information.
--account	-a	Displays account name.
--list	-L	Displays file containing list of accounts, one per line.
--output	-o	Specifies the format to be used for printing routing information with information. The fields that display by default are <ul style="list-style-type: none"> • cache server • account name • route information
cacheN		(optional command) Specifies additional memcache server in the form of server:port.

zmredodump

Use `zmredodump` for debugging purposes and to dump the contents of a redolog file. When users are debugging a problem, Zimbra support might ask them to run `zmredodump` with specific options.

Multiple log files/directories can be specified with all redolog files under each directory being sorted in ascending order and processed.

Syntax

```
zmredodump [options] <redolog file/directory> [...]
```

Description

Long Name	Short Name	Description
--help	-h	Displays help messages.
	-m	Specifies the mailbox ids separated by a comma or a space. The entire list of mailbox ids must be quoted if using space as a separator. To dump contents of all the redolog files, omit this option.

Long Name	Short Name	Description
--no-offset		Specifies if file offsets and size for each redolog dump should not be shown.
--quiet	-q	Activates the quiet mode. Used to only print the log filename and errors, if any. Useful for verifying integrity of redlogs with minimal output.
--show-blob		Shows blob content. The specified item's blob is printed with <START OF BLOB> and <END OF BLOB> marking the start and end of the blob.

zmskindeploy

Use **zmskindeploy** to simplify the process of deploying skins in ZWC. This tool processes the skin deployment, enables the skin for all users of the ZWC deployment, and restarts the web server so that it recognizes the new skin.

Syntax

```
zmskindeploy <path/to/skin/dir/or/zipfile>
```

zmsoap

Use **zmsoap** to print mail, account, and admin information in the SOAP format.

Syntax

```
zmsoap [options] {path1} [path2]...
```

Description

Long Name	Short Name	Description
--help	-h	Prints usage information.
--mailbox	-m	<name> Displays mailbox account name. Mail and account requests are sent to this account. This attribute is also used for authentication if -a and -z are not specified.
--target		<name> Displays the target account name to which the requests are sent. Used only for non-admin sessions.
--admin name	-a	<name> Displays the admin account name to authenticate as.

Long Name	Short Name	Description
--zadmin	-z	Displays the Zimbra admin name and password to authenticate as.
--password	-p	<pass> Displays account password.
--passfile	-P	<path> Reads password from a file.
--element	-e	<path> Displays the root element path. If specified, all path arguments that do not start with a slash (/) are relative to this element.
--type	-t	<type> Displays the SOAP request type. Can either be <code>mail</code> , <code>account</code> , or <code>admin</code> .
--url	-u	<http[s]://> Displays the server hostname and optional port value.
--verbose	-v	Prints the SOAP request and other status information.
path		<[path]> Displays the element or attribute path and value. Roughly follows the XPath syntax as: [/]element1[/element2][/@attr][=value].

zmstat-chart

Use `zmstat-chart` to collect statistical information for the CPU, IO, `mailboxd`, MTAqueue, MariaDB, and other components and to run a script on the csv files to display the usage details in various charts. These csv files are saved to `/opt/zimbra/zmstat/`.

You must enable `zmstat` to collect the performance charts data:

1. Enter `zmprov ms {hostname} zimbraServerEnable stats`.
2. Restart the server, Enter:

```
zmcontrol stop
zmcontrol start
```

Syntax

```
zmstat-chart -s <arg> -d <arg> [options]
```

Description

Long Name	Short Name	Description
--aggregate-end-at		<arg> If this is specified, the aggregate computation ends at this timestamp. Usage is <code>MM/dd/yyyy HH:mm:ss</code> .

Long Name	Short Name	Description
--aggregate-start-at		<arg> If this is specified, the aggregate computation starts at this timestamp. Usage is MM/dd/yyyy HH:mm:ss.
--end-at		<arg> If this is specified, all samples after the specified timestamp are ignored. Usage is MM/dd/yyyy HH:mm:ss.
--start-at		<arg> If this is specified, all samples before this timestamp are ignored.
--title		<arg> This gives the chart a title that displays. Defaults to the last directory name of srccdir.
--no-summary		Summary data generation is not included.
--conf	-c	<arg> Chart the configuration xml files.
--destdir	-d	<arg> The directory where the generated chart files are saved.
--srccdir		One or more directories where the csv files are located. The csv files are moved to directories listed by date under zmstat/.

zmstat-chart-config

Use **zmstat-chart-config** to generate an xml file `/opt/zimbra/conf/zmstat-chart.xml` from a template, taking into account the server setup including the LDAP node and the processes run, among other specifications.

zmstatctl

Use **zmstatctl** to run a control script for checking **zmstat** data collectors. This instruction starts or stops monitoring processes, and checks status or rotates logs.

Syntax

```
zmstatctl start|stop|status|rotate
```

zmthrdump

Use **zmthrdump** to invoke a thread dump in the ZCS server process and print the output file. This command also gives the option of saving the thread dump to a file and inserts a timestamp on the logfile.

Syntax

```
zmthrdump [-h] [-i] [-t <timeout seconds>] [-p <pid file>] [-f <file>] [-o <out-file>]
```

Description

Short Name	Description
-h	Displays help messages.
-i	Appends the timestamp to the LOGFILE before invoking SIGQUIT.
-p	Returns the PID to send SIGQUIT. The default value can be found in <code>zmmailboxd_java.pid</code>
-f	Specifies the LOGFILE to save the thread dump output in. The default value is <code>zmmailbox.out</code> .
-o	Specifies the output file of the thread dump. The default value is stdout.
-t	Specifies the timeout value (in seconds) to exit if the process becomes unresponsive. The default value is 30 seconds.

zmtrainsa

Use `zmtrainsa` to train the anti-spam filter. This command is run automatically every night to train the SpamAssassin filter from messages users mark as "junk" / "not junk" from their mailbox. See [SpamAssassin's sa-update tool](#), which is included with SpamAssassin. This tool updates SpamAssassin rules from the SA organization. The tool is installed into `/opt/zimbra/common/bin`.

The `zmtrainsa` command can be run manually to forward any folder from any mailbox to the spam training mailboxes. If you do not enter a folder name when you manually run `zmtrainsa` for an account, for spam, the default folder is Junk. For ham, the default folder is Inbox.

Syntax

```
zmtrainsa <user> <spam|ham> [folder]
```

zmtzupdate

Use `zmtzupdate` to update time zone changes in existing appointments for specific users or all users. An `.ics` rule file should first be created to run with this command. A rule file lists a series of rules to match a time zone and the replacement time zone definitions. More information about this command can be found at: https://wiki.zimbra.com/wiki/Changing_ZCS_Time_Zones.

Syntax

```
zmtzupdate --rulefile <rule file> -a <"all" or list of specific email addresses> [--sync] [--after <date/time stamp>]
```

Description

Long Name*	Short Name	Description
--account	-a	<arg> account email addresses separated by a white space. Use "all" for all accounts to be updated.
--after		<arg> Appointments occurring after the specified date/time in this field are updated. The default cut off time is January 1st, 2008.
--help	-h	Displays help information.
--rulefile		Specifies the .ics XML file that should be used to update time zone definitions.
--server	-s	<arg> Specifies the mail server hostname. The default value is localhost.
--sync		If specified, this option causes the <code>zmtzupdate</code> command to block till the server processes all requested accounts. The default value is no.

zmvolume

Use `zmvolume` to manage storage volumes from the CLI. Note that volumes can be managed from the Administration Console, **Server > Volumes** page.

Syntax

```
zmvolume {-a|-d|-l|-e|-dc|-sc} [options]
```

Description

Long Name	Short Name	Description
--add	-a	Adds a volume.
--compress	-c	<arg> Compress BLOBs; "true" or "false".
--compressionThreshold	-ct	Compression threshold; default 4KB.
--delete	-d	Deletes a volume.
--displayCurrent	-dc	Displays the current volume.
--edit	-e	Edits a volume.
--help	-h	Shows the help for the usage options for this tool.
--id	-id	<arg> Volume ID.
--list	-l	Lists volumes.
--name	-n	<arg> Volume name.
--path	-p	<arg> Root path.

Long Name	Short Name	Description
--server	-s	<arg> Mail server hostname. Default is localhost.
--setCurrent	-sc	Sets the current volume.
--type	-t	<arg> Volume type (primaryMessage, secondaryMessage, or index)
--turnOffSecondary	-ts	Turns off the current secondary message volume.

zmzimletctl

Use **zmzimletctl** to manage Zimlets and to list all Zimlets on the server. Additional information is provided in [Zimlets](#). Most Zimlet deployment can be completed from the Zimbra Administration Console.

Syntax

```
zmzimletctl [-l] {command} [<zimlet.zip>|<config.xml>|<zimlet>]
```

Description

Long Name	Description
deploy	<zimlet.zip> Creates the Zimlet entry in the LDAP server, installs the zimlet files on the Server, grants, access to the members of the default COS, and turns on the Zimlet.
undeploy	<zimlet> Uninstall a zimlet from the Zimbra server.
install	<zimlet.zip> Installs the Zimlet files on the host.
ldapDeploy	<zimlet> Adds the Zimlet entry to the LDAP.
enable	<zimlet> Enables the Zimlet.
disable	<zimlet> Disables the Zimlet.
acl	<zimlet> <cos1> {grant deny} [<cos2> {grant deny}] Sets the access control, grant deny, to a COS.
listAcls	<zimlet> Lists the ACLs for the Zimlets.
listZimlets	View details about all Zimlets on the server.
getConfigTemplate	<zimlet.zip> Extracts the configuration template from the Zimlet.zip file.
configure	<config.xml> Installs the configuration.
listPriority	Shows the current Zimlet priorities (0 is high, 9 is low)
setPriority	<zimlet> Sets the Zimlet priority.

zmproxyconfig

Use `zmproxyconfig` to manage Zimbra proxy and should only be used when you have to make changes to Zimbra proxy after it has been installed. See [Zimbra Proxy Server](#).



Previous to ZCS 6.0, this command was called `zmproxyinit`.

Syntax

```
/opt/zimbra/libexec/zmproxyconfig [-h] [-o] [-m] [-w] [-d [-r] [-s] [-a w1:w2:w3:w4] [-i p1:p2:p3:p4] [-p p1:p2:p3:p4] [-x mailmode]] [-e [-a w1:w2:w3:w4] [-i p1:p2:p3:p4] [-p p1:p2:p3:p4] [-x mailmode]] [-f] -H hostname
```

Description

Short Name	Description
<code>-h</code>	Displays help messages.
<code>-H</code>	Hostname of the server on which enable/disable proxy functionality.
<code>-a</code>	Colon separated list of Web ports to use. Format: HTTP-STORE:HTTP-PROXY:HTTPS-STORE:HTTPS-PROXY (Ex: 8080:80:8443:443)
<code>-d</code>	Disable proxy.
<code>-e</code>	Enable proxy.
<code>-f</code>	Full reset on memcached port and search queries and POP/IMAP throttling.
<code>-i</code>	Colon separated list of IMAP ports to use. Format: IMAP-STORE:IMAP-PROXY:IMAPS-STORE:IMAPS-PROXY (Ex: 7143:143:7993:993)
<code>-m</code>	Toggle mail proxy portions.
<code>-o</code>	Override enabled checks.
<code>-p</code>	Colon separated list of POP ports to use. Format: POP-STORE:POP-PROXY:POPS-STORE:POPS-PROXY (Ex: 7110:110:7995:995)
<code>-r</code>	Run against a remote host. Note that this requires the server to be properly configured in the LDAP master.
<code>-s</code>	Set Cleartext to FALSE (secure mode) on disable.
<code>-t</code>	Disable reverse proxy lookup target for the store server. Only valid with <code>-d</code> . Make sure that you intend for all proxy functions for the server to be disabled.
<code>-w</code>	Toggle Web proxy portions.
<code>-x</code>	<code>zimbraMailMode</code> to use on disable (Default is HTTP)

`hostname` is the value of the `zimbra_server_hostname` LC key for the server being modified.

Required options are **-f** by itself, or **-f** with **-d** or **-e**.

Note that

- **-d** or **-e** require one or both of **-m** and **-w**.
- **-i** or **-p** require **-m**.
- **-a** requires **-w**.
- **-x** requires **-w** and **-d** for store.
- **-x** requires **-w** for proxy.

The following are the defaults for **-a**, **-i**, **-p**, and **-x** if they are not supplied as options.

-a	default on enable: 8080:80:8443:443	default on disable: 80:0:443:0
-i	default on enable: 7143:143:7993:993	default on disable: 143:7143:993:7993
-p	default on enable: 7110:110:7995:995	default on disable: 110:7110:995:7995
-x	default on store disable: http	default on proxy enable/disable: http

zmsyncreverseproxy

Use **zmsyncreverseproxy** to reverse proxy mobile sync HTTP traffic between the source and forwarding server and port. Decodes the sync requests/responses and logs them when verbose mode is turned on.

Syntax

```
zmsyncreverseproxy [-v] [-d] [-L log4j.properties] -p <port number> -fs <fwd server>
-fp <fwd port> [-sv syncversions]
```

Description

Long Name	Short	Description
--help	-h	Displays help.
--verbose	-v	Verbose mode, dumps full exception stack trace.
--debug	-d	Debug mode, dumps decoded sync messages.
--port	-p	The port this service listens on.
--forwardserver	-fs	The server host to forward requests to.
--forwardport	-fp	The server port to forward requests to.
--syncversions	-sv	Active sync versions supported.
--logpropertyfile	-L	log4j property file, valid only with -l .

Appendix B: Configuring SPNEGO Single Sign-On

The SPNEGO protocol mechanism can be configured on ZCS for single sign-on authentication to the Zimbra Web Client and to the Zimbra Connector for Outlook (ZCO). For ZCO configuration see [Setting Up Single Sign-On Options for ZCO](#).

From ZWC, when users log on to their Intranet through Active Directory, they can enter their ZWC mailbox without having to re-authenticate to Zimbra.

The ZCS server is configured to redirect users attempting to log on to ZWC to a URL under SPNEGO protection. The server asks for authentication with Kerberos through SPNEGO and users are redirected to their ZWC mailbox. When users log out, they are redirected to a logout URL that displays a Launch button. When users click **Launch**, they are directed to the ZWC entry page.



When users log on to their ZWC accounts from the Internet, the ZWC log in page displays and they must enter their ZWC password to log on.



If SPNEGO SSO is enabled on a domain, the browsers must be configured correctly. See [Configure Your Browser](#). Improperly configured browsers may pop up a user/pass dialog and if a user enters his correct AD domain username/password, he can still log into the Zimbra mailbox, and some browsers may display a "401 Unauthorized" error.

Configuration Process

1. Create the Kerberos keytab file.
 - Create an Active Directory service account. This account is used to generate the Kerberos keytab file.
 - Add the service Principal Names (SPN) directory property for an Active Directory service account.
 - Create the keytab file.
2. Enable and configure the SPNEGO protocol on the ZCS server.
3. Configure browsers

Create the Kerberos Keytab File

An Active Directory service account is created in Domain for each mailstore server.

1. Create an Active Directory service account. This is the account used to generate the Kerberos keytab file that is added to the Zimbra server.
 - a. Go to the Active Directory **Start > Programs > Administrative Tools > Active Directory Users and Computers** console.

- b. To create the service account, click the AD Domain name and from the expanded content right-click **Users** and select **New > User**. Complete the New Object – User dialog.
 - **Full name:** Enter the user display name for the AC service account. Recommend that the full name be the ZCS mailbox server name.
Example: **mail1**
 - **User Logon Name:** This name is the value that is set for the `zimbraSpnegoAuthTargetName` server attribute in LDAP. Write it down.
Example: **HTTP/mail1.example.com**
 - **User Logon Name (pre-Windows2000):** This name is used for the `\mapUser` parameter in the `setspn` and `ktpass` commands.
Example: **mail1**
 - Click **Next**.
 - c. Enter and confirm the password. This password is used for the `\pass {AD-user-password}` parameter in the `ktpass` command, configured below.
 - d. Check **Password never expires** and **User cannot change password**, and click **Next**.
 - e. Click **Finish** to create the user. The service account name displays in the Users directory.
2. Use the `setspn` command to map the mailbox server name as the service Principal Names (SPN) to the user account. The SPN is used in the process of mutual authentication between the client and the server hosting particular service.
- a. From the command prompt, type `setspn \a {userlogonname} {serviceaccountname}`

Example 87. Map mailbox server name as servie Principal Names to user account

```
setspn \a HTTP/mail1.example.com mail1
```

- b. To verify that the SPN is registered, type `C:\>setspn \l {accountname}`
A list of registered SPNs is displayed.
3. Create the keytab file used when signing into the Kerberos domain. Use the `ktpass` tool from the Windows Server toolkit to create the Kerberos keytab.



A Kerberos keytab file contains a list of keys that are analogous to user passwords. Restrict and monitor permissions on any keytab files you create.

The command to type follows:

```
ktpass -out {keytab-file-to-produce} -princ {Service-Principal-Name}@{the-kerberos-realm} -mapUser {AD-user} -mapOp set -pass {AD-user-password} -crypto RC4-HMAC-NT -pType KRB5_NT_PRINCIPAL
```

<code>ktpass -out</code>	The key is written to this output file. Enter the directory location and keytab file name. The keytab file name is jetty.keytab . For example, <code>C:\Temp\spengo\jetty.keytab</code>
<code>-princ</code>	This is the principal name. Enter the service Principal Name as used in Step 2 in Setting up the Microsoft Windows Active Directory Domain Controller section. For example, <code>HTTP/mail1.example.com@COMPANY.COM</code>
<code>-mapUser</code>	This maps <code>princ</code> value to this user account. Enter the AD service account user name entered in the User Logon Name (pre-Windows2000) set in Step 1.b in Setting up the Microsoft Windows Active Directory Domain Controller section.
<code>-mapOp</code>	This sets the mapping. The value for this parameter is set
<code>-pass</code>	This is the password to use. Enter the password entered in the User Logon Name (pre-Windows2000) set in Step 1.c in Setting up the Microsoft Windows Active Directory Domain Controller section.
<code>-crypto</code>	This is the cryptosystem to use. Enter RC4-HMAC-NT
<code>-pType</code>	Enter KRB5_NT_PRINCIPAL To avoid warning messages from the toolkit enter this value.

Example 88. Using `ktpass` to create a `jetty.keytab` file

```
ktpass -out C: \Temp\spengo\jetty.keytab -princ
HTTP/mail1.example.com@COMPANY.COM -mapUser mail1 -mapOp set - pass password123
-crypto RC4-HMAC-NT -pType KRB5_NT_PRINCIPAL
```

The command is confirmed with something similar to the example below.

Targeting domain controller: □

```
Using legacy password setting method
Successfully mapped HTTP/mail1.example.com to mail1.
Key created.
Output keytab to c:\Temp\spengo\jetty.keytab:
Keytab version: 0x502
```

```
keysize 71 HTTP HTTP/mail1.example.com@COMPANY.COM ptype 1
(KRB5_NT_PRINCIPAL) vno3 etype 0x17 (RC4-HMAC) keylength 16
(0xc383f6a25f1e195d5aef495c980c2bfe)
```

- Transfer the keytab file (jetty.keytab) to the Zimbra server. Copy the file created in step 3 to the following Zimbra server location: `/opt/zimbra/data/mailboxd/spnego/jetty.keytab`.



Do not rename the `jetty.keytab` file. This file name is referenced from various configuration files.

Repeat steps 1 to 4 to create an create the keytab file (`jetty.keytab`) for each Zimbra mailstore server.

Configure ZCS

SPNEGO attributes in Global Config and on each Zimbra server are configured and pre-authentication is set up for the domain. Use the `zmprov` commands to modify the Zimbra server.



Only one Kerberos REALM is supported per ZCS installation.

- Modify the following global config attributes, with the `zmprov mcf` command.

<code>zimbraSpnegoAuthEnabled</code>	Set to TRUE.
<code>zimbraSpnegoAuthErrorURL</code>	This is the URL users are redirected to when spnego auth fails. Setting it to <code>/zimbra/?ignoreLoginURL=1</code> will redirect user to the regular Zimbra login page, where user will be prompted for their zimbra user name and password.
<code>zimbraSpnegoAuthRealm</code>	The Kerberos realm in the domain controller. This is the domain name in the Active Directory. (COMPANY.COM)

To modify the global config attributes, type:

- `zmprov mcf zimbraSpnegoAuthEnabled TRUE`
 - `zmprov mcf zimbraSpnegoAuthErrorURL '/zimbra/?ignoreLoginURL=1'`
 - `zmprov mcf zimbraSpnegoAuthRealm <COMPANY.COM>`
- On each Zimbra server, modify the following global config attributes with the `zmprov ms` command.

<code>zimbraSpnegoAuthTargetName</code>	This is the user logon name from Step 1 B, User Logon Name.
<code>zimbraSpnegoAuthPrincipal</code>	Enter the user logon name set in <code>zimbraSpnegoAuthTargetName</code> and the address set in global config <code>zimbraSpnegoAuthRealm</code> Type as <code>zimbraSpnegoAuthTargetName@zimbraSpnegoAuthRealm</code> For example, <code>HTTP/mail1.example.com@COMPANY.COM</code>

To modify the server global config attributes, type:

- a. zmprov ms mail1.example.com zimbraSpnegoAuthTargetName HTTP/mail1.example.com
 - b. zmprov ms mail1.example.com zimbraSpnegoAuthPrincipal HTTP/mail1.example.com@COMPANY.COM
3. The following is set up on the domain.

- Kerberos Realm
- Virtual host
- Web client login URL and UAs
- Web client logout URL and UAs
 - a. Set up Kerberos Realm for the domain. This is the same realm set in the global config attribute **zimbraSpnegoAuthRealm**. Type `zmprov md {domain} zimbraAuthKerberos5Realm {kerberosrealm}`
 - b. Set up the virtual hosts for the domain. Virtual-hostname-* are the hostnames you can browse to for the Zimbra Web Client UI. Type:

```
zmprov md {domain} +zimbraVirtualHostname {virtual-hostname-1}
+zimbraVirtualHostname {virtual-hostname-2}
...
```

- c. Setup the web client log in URL and UAs allowed for the login URL on the domain.
- Set the login URL. The login URL is the URL to redirect users to when the Zimbra auth token is expired. `zmprov md {domain} zimbraWebClientLoginURL '.../service/spnego'`
 - Honor only supported platforms and browsers.

zimbraWebClientLoginURLAllowedUA is a multi-valued attribute, values are regex. If this is not set, all UAs are allowed. If multiple values are set, an UA is allowed as long as it matches any one of the values.

```
zmprov md {domain} +zimbraWebClientLoginURLAllowedUA {UA-regex-1}
+zimbraWebClientLoginURLAllowedUA {UA-regex-2} ...
```

For example, to honor **zimbraWebClientLoginURL** only for Firefox, Internet Explorer, Chrome, and Safari on computers running Windows, and Safari on Apple Mac computers, type the following commands.

```
zmprov md {domain} +zimbraWebClientLoginURLAllowedUA
'._Windows._Firefox/3.*'
zmprov md {domain} +zimbraWebClientLoginURLAllowedUA '._MSIE._Windows.*'
zmprov md {domain} +zimbraWebClientLoginURLAllowedUA
'._Windows._Chrome.*'
zmprov md {domain} +zimbraWebClientLoginURLAllowedUA
'._Windows._Safari.*'
zmprov md {domain} +zimbraWebClientLoginURLAllowedUA
'._Macintosh._Safari.*'
```

d. Setup the web client logout URL and UAs allowed for the logout URL on the domain.

- Set the logout URL. The logout URL is the URL to redirect users to when users click Logout.

```
zmprov md {domain} zimbraWebClientLogoutURL '.../?sso=1'
```

- Honor only supported platforms and browsers. `zimbraWebClientLogoutURLAllowedUA` is a multi-valued attribute, values are regex. If this is not set, all UAs are allowed. If multiple values are set, an UA is allowed as long as it matches any one of the values.

```
zmprov md {domain} +zimbraWebClientLogoutURLAllowedUA {UA-regex-1}  
+zimbraWebClientLogoutURLAllowedUA {UA-regex-2} ...
```

For example, to honor `zimbraWebClientLogoutURL` only for Firefox, Internet Explorer, Chrome, and Safari on computers running Windows, and Safari on Apple Mac computers, type the following commands.

```
zmprov md {domain} +zimbraWebClientLogoutURLAllowedUA  
'._Windows._Firefox/3.*'  
zmprov md {domain} +zimbraWebClientLogoutURLAllowedUA '._MSIE._Windows.*'  
zmprov md {domain} +zimbraWebClientLogoutURLAllowedUA  
'._Windows._Chrome.*'  
zmprov md {domain} +zimbraWebClientLogoutURLAllowedUA  
'._Windows._Safari.*'
```

Configure Your Browser

When the SPNEGO SSO feature is enabled on your domain, user's browsers must be configured properly. Improperly configured browsers will behave differently depending on the browser.

The following browsers are supported:

- For computers running Windows: Internet Explorer 10.0 or later, Edge, Firefox 52 or later, Chrome, Safari
- Apple Mac computer: Safari
 1. Firefox browser for computers running Windows
 - a. In Firefox browse to **about:config**. In the Firefox browser address field, type **about:config**. The warning — **This might void your warranty**, is now displayed.
 - b. Click **I'll be careful, I promise!**
 - c. Search in Filters, type **network.n**. Enter a comma-delimited list of trusted domains or URLs.

Double-click **network.negotiate-auth.delegation-uris**. Enter <http://,https://>

Double-click **network.negotiate-auth.trusted-uris**. Enter <http://,https://>

Or, to set specific URLs,

Double-click **network.negotiate-auth.delegation-uris**. Enter the domain addresses. For example, <http://mail1.example.com,https://> mail2.example.com

Double-click **network.negotiate-auth.trusted-uris**. Enter the domain addresses. For example, <http://mail1.example.com,https://> mail2.example.com

2. Internet Explorer, Chrome, and Safari for computers running Windows
 - a. In these browsers, go to **Tools > Internet Options > Security > Local Intranet > Sites**. On the Sites dialog make sure all items are checked.
 - b. Select **Advanced**. Add the domain server (hostname) URL, both http:// and https://
 - c. Click **OK** to close the file.
 - d. Go to **Tools > Options > Advanced > Security**. Locate and check **Enable Integrated Windows Authentication**.
 - e. Click **OK** and close the browser.
3. Safari for Apple Mac computers. No configuration is necessary.

Test your setup

1. On a Windows computer or an Apple Mac computer, log in to the computer as a domain user.

Your ticket as a domain user will be saved on the computer. The token will be picked up by the spnego-aware browser and sent in the Authorization header to the Zimbra server.

2. Browse to the Zimbra Web Client log on page. You should be redirected to your ZWC inbox without being prompted for user name and password.

If spnego auth fails, the user is redirected to an error URL.

Troubleshooting setup

Make sure the following are true.

- The browser is in the Intranet zone.
- The user is accessing the server using a Hostname rather than IP address.
- Integrated Windows authentication in Internet Explorer is enabled, and the host is trusted in Firefox.
- The server is not local to the browser.
- The client's Kerberos system is authenticated to a domain controller.
- If the browser display the "401 Unauthorized", it's most likely that the browser either did not send another request with Authorization in response to the 401, or had sent an Authorization

which is not using the GSS-API/SPNEGO scheme.

Check your browser settings, and make sure it is one of the supported browsers/platforms

- If you are redirected to the error URL specified in `zimbraSpnegoAuthErrorURL`, that means The SPNEGO authentication sequence does not work.

Take a network trace, make sure the browser sends Authorization header in response to the 401. Make sure the Negotiate is using GSS-API/ SPNEGO, not NTLM (use a network packet decoder like Wireshark).

After verifying that the browser is sending the correct Negotiate, if it still does not work, turn on the following debug and check Zimbra logs:

- ADD “`-DDEBUG=true -Dsun.security.spnego.debug=all`” (note, not replace) to localconfig key `spnego_java_options`
- Add `log4j.logger.org.mortbay.log=DEBUG` in `log4j`

Then restart the mailbox server.

Browse to the debug snoop page: <http://{server}:{port}/spnego/snoop.jsp>. See if you can access the snoop.jsp

Check `zmmailboxd.out` and `mailox.log` for debug output.

- One of the errors at this stage could be because of clock skew on thejetty server. If this is the case, it should be shown in `zmmailboxd.out`. Fix the clock skew and try again.

Configure Kerberos Auth with SPNEGO Auth

Kerberos auth and SPNEGO can co-exists on a domain. Use case is using Kerberos as the mechanism for verifying user principal/password against a KDC, instead of the native Zimbra LDAP, when user cannot get in by SPNEGO.

When SPNEGO auth fails, users are redirected to the Zimbra sign in page if the browser is configured properly. Users can enter their Zimbra username and password on the sign in page to sign in manually. The Domain attribute `zimbraAuthMech` controls the mechanism for verifying passwords. If `zimbraAuthMech` is set to "kerberos5", The user name the user enters is usedto first identify a valid Zimbra user (users must be provisioned in the Zimbra LDAP), then from Zimbra user is mapped to a Kerberos principal, the Kerberos principal + password is then validated against a KDC. This KDC could be different from, or the same as, the KDC that the Active Directory domain controller (for SPNEGO auth) is running as.



Every Microsoft Active Directory domain controller acts as Kerberos KDC. For SPNEGO auth, KDC is not contacted from the mailbox server. The Kerberos token sent from the Authorization http header along with jetty's keytab file can identify/authenticate the user.

For kerberos auth (`zimbraAuthMech*="kerberos5"`), the mailbox server needs to contact KDC to validate principal+password. For the java kerberos client (i.e. Zimbra mailbox server), the default

realm and KDC for the realm is specify in a Kerberos config file. The location of this config file can be specified in JVM argument `java.security.krb5.conf`. If it is not specified, the default is `/etc/krb5.conf`. When SPNEGO is enabled in Zimbra, `java.security.krb5.conf` for the mailbox server is set to `/opt/zimbra/jetty/etc/krb5.ini`. Therefore, that is the effective file for configuring kerberos auth.

`/opt/zimbra/jetty/etc/krb5.ini` is rewritten from `/opt/zimbra/jetty/etc/krb5.ini.in` each time when the mailbox server restarts. To configure, you need to modify the `/opt/zimbra/jetty/etc/krb5.ini.in` file, not `/opt/zimbra/jetty/etc/krb5.ini`.

Under [realms] section, kdc and admin_server are not set for SPNEGO auth, but they are required for kerberos auth.

To configure:

1. Edit `/opt/zimbra/jetty/etc/krb5.ini.in`

2. Change:

```
[realms]
%%zimbraSpnegoAuthRealm%% = {
    default_domain = %%zimbraSpnegoAuthRealm%%
}
```

to

```
%%zimbraSpnegoAuthRealm%% = {
    kdc = YOUR-KDC
    admin_server = YOUR-ADMIN-SERVER
    default_domain = %%zimbraSpnegoAuthRealm%%
}
```

1. Replace YOUR-KDC and YOUR-ADMIN-SERVER to the hostname on which the kdc/admin_server for kerberos auth is running.
2. Save the file and restart mailbox server.

The restriction is the realm for SPNEGO and Kerberos auth must be the same. For SPNEGO auth, the Kerberos principal in the Authorization header is mapped to a unique Zimbra account. For Kerberos auth, the Zimbra account is mapped to a unique Kerberos principal. The mapping (by domain attribute `zimbraAuthKerberos5Realm`) is the same for both.

Setting Up Single Sign-On Options for ZCO



To use SSO, SPNEGO must be configured on the ZCS server to use this option.

The single sign-on option works with a specific server. The server name used in the ZCO profile must match that in the SPNEGO configuration. Make sure that the server name is incorporated into

the **.msi** file prior to installation.

To set up the single sign-on option in the **.msi** customization script:

1. Set the server name to be the server name configured for SPNEGO, enter **-sn <spnegoserver.example.com>**.
2. Set the password rule, enter **-pw 0**

```
ecscript ZmCustomizeMsi.js <path/msi-filename> -sn <spnegoserver.example.com> -pw 0
```

Appendix C: ZCS Crontab Jobs

The crontab is used to schedule commands to be executed periodically on the Zimbra servers.

How to read the crontab

Each entry in a crontab file consists of six fields, specified in the following order: minute, hour, day, month, weekday, command

The fields are separated by blank spaces or tabs.

Field	Description
minute	0 through 59
hour	0 through 23
day of the (month)	1 through 31
month	1 through 12
day of the (week)	0 through 7 (0 or 7 is Sunday, 1 is Monday, etc., or use names)
command	This is the complete sequence of commands to be executed for the job

When an asterisk (*) is displayed, it means all possible values for the field. For example, an asterisk in the hour time field would be equivalent to "every hour".

ZCS Cron Jobs

You can view the ZCS crontab by logging on as zimbra and typing `crontab -l`.

Scheduled jobs

The following cron jobs are scheduled to run for ZCS:

Log pruning

The log pruning deletes logs from `/opt/zimbra/log` that are over eight days old. The job runs at 2:30 a.m.

Status logging

`zmstatuslog` calls `zmcontrol status` and outputs its data into syslog.

This is primarily so that logger can read the data and keep the administration console status up-to-date.

Status logging job runs every 2 minutes.

Backups

Full and increment backups are scheduled to run according to the schedule defined by `zmschedulebackup` command. By default the full backup is scheduled for 1:00 a.m., every Saturday. The incremental backups are scheduled for 1:00 a.m., Sunday through Friday.

By default, backups older then a month are deleted on the first of each month at 12 a.m.

Jobs for crontab.store

Log pruning

The log pruning deletes logs from `/opt/zimbra/mailboxd/logs` that are over eight days old. The job runs at 2:30 a.m.

Clean up the quarantine dir

Mail identified with a virus or spam are not dropped immediately, but are put in quarantine. Messages older than seven days are deleted at 1:00 a.m daily.

Table maintenance

The `ANALYZE TABLE` statement is run on all tables in the database to update the statistics for all indexes. This is done to make sure that the SQL query optimizer picks the correct indexes when executing SQL statements. This script is run 1:30 a.m. on Sunday.

Report on any database inconsistencies

`zmdbintegrityreport` is run weekly to check the SQL database for corruption and will notify the administrator if any corruption is found. When this is run, it may consume a significant amount of I/O. If you find that it is an issue, you may want to change the frequency with which `zmdbintegrityreport` is run by editing the ZCS crontab entry. This report runs at 11:00 p.m. Sundays.

Large sites may opt to disable this by setting:

```
zmlocalconfig -e zmdbintegrityreport_disabled=TRUE
```

If you choose to disable this, it is recommended that the integrity report be run by hand during the normal maintenance windows and prior to running any ZCS upgrades.

Monitor for multiple mysqld to prevent corruption

A script is executed to see if mysqld process is running to detect cases where corruption is likely to be caused. An email is generated if it finds more than 1 mysqld process running. The script runs every 5 minutes.

Jobs for crontab.logger

process logs

`zmlogprocess` runs every 10 minutes to parse logs and produce MTA metrics (as/av, volume, count, etc).

Daily reports

When the `logger` package is installed, a daily mail report is automatically scheduled in the crontab. The report runs every morning at 11:30 and is sent to the administrator's email address.

Jobs for crontab.mta

Queue logging

The `zmqueue` report status via the syslog is reviewed. This is logger data. The status is updated every 10 minutes.

Spam training

The `zmtrainsa` script is enabled to feed mail that has been classified as spam or a non-spam to the SpamAssassin application. SpamAssassin learns what signs are likely to mean spam or ham. This job should run only on one Zimbra MTA. The job runs at 11:00 p.m.

Spam training cleanup

`zmtrainsa` empties the spam and ham mailboxes each day. The job runs at 11:45 p.m.

Spam Bayes auto-expiry

Spam bayes auto-expiry maintains the SpamAssassin Bayes database. This keeps the database to manageable size ensuring spam processing remains as quick as possible. This runs every day at 11:20 p.m.

Clean up amavisd/tmp

This job is used to clean up the amavisd temp files. It runs at 5:15 a.m. and at 8:15 p.m.

Single Server Crontab -l Example

Example 89. Output of `crontab -l`

```
# ZIMBRASTART -- DO NOT EDIT ANYTHING BETWEEN THIS LINE AND ZIMBRAEND
#
# Log pruning
#
30 2 * * * find /opt/zimbra/log/ -type f -name *.log* -mtime +8 -exec rm {} \; >
/dev/null 2>&1
35 2 * * * find /opt/zimbra/log/ -type f -name *.out.?????????? -mtime +8 -exec
rm {} \; > /dev/null 2>&1
#
# Status logging
#
*/2 * * * * /opt/zimbra/libexec/zmstatuslog
#
# Backups
#
# BACKUP BEGIN
# BACKUP END
#
# crontab.ldap
#
#
#
# crontab.store
#
# Log pruning
#
30 2 * * * find /opt/zimbra/mailboxd/logs/ -type f -name \*log\* -mtime +8 -exec
rm {} \; > /dev/null 2>&1
30 2 * * * find /opt/zimbra/log/ -type f -name stacktrace.\* -mtime +8 -exec rm {}
\; > /dev/null 2>&1
#
# Table maintenance
#
30 1 * * 7 /opt/zimbra/libexec/zmmaintainables >> /dev/null 2>&1
#
#
# # Report on any database inconsistencies
#
0 23 * * 7 /opt/zimbra/libexec/zmdbintegrityreport -m
#
# Monitor for multiple mysqld to prevent corruption
#
*/5 * * * * /opt/zimbra/libexec/zmcheckduplicatemyqld -e > /dev/null 2>&1
#
# crontab.logger
#
# process logs
#
```

```

00,10,20,30,40,50 * * * * /opt/zimbra/libexec/zmlogprocess > /tmp/logprocess.out
2>&1
#
# Graph generation
#
10 * * * * /opt/zimbra/libexec/zmgengraphs >> /tmp/gengraphs.out 2>&1
#
# Daily reports
10 1 * * * /opt/zimbra/libexec/zmdailyreport -m
#
#
# crontab.mta
#
#
# Queue logging
#
0,10,20,30,40,50 * * * * /opt/zimbra/libexec/zmqueuelog
#
# Spam training
0 23 * * * /opt/zimbra/bin/zmtrainsa >> /opt/zimbra/log/spamtrain.log 2>&1
#
# Spam training cleanup
#
45 23 * * * /opt/zimbra/bin/zmtrainsa --cleanup >> /opt/zimbra/log/spamtrain.log
2>&1
#
# Dspam cleanup
#
0 1 * * * [ -d /opt/zimbra/data/dspam/data/z/i/zimbra/zimbra.sig ] && find
/opt/zimbra/dspam/var/dspam/data/z/i/zimbra/zimbra.sig/ -type f -name \*sig -mtime
+7 -exec rm {} \; > /dev/null 2>&1
8 4 * * * [ -f /opt/zimbra/data/dspam/system.log ] &&
/opt/zimbra/dspam/bin/dspam_logrotate -a 60 -l /opt/zimbra/data/dspam/system.log
8 8 * * * [ -f /opt/zimbra/data/dspam/data/z/i/zimbra/zimbra.log ] &&
/opt/zimbra/dspam/bin/dspam_logrotate -a 60 -l
/opt/zimbra/data/dspam/data/z/i/zimbra/zimbra.log
#
# Spam Bayes auto-expiry
#
20 23 * * * /opt/zimbra/libexec/sa-learn -p /opt/zimbra/conf/salocal.cf --dbpath
/opt/zimbra/data/amavisd/.spamassassin --siteconfigpath
/opt/zimbra/conf/spamassassin --force-expire --sync > /dev/null 2>&1
#
# Clean up amavisd/tmp
#
15 5,20 * * * find /opt/zimbra/data/amavisd/tmp -maxdepth 1 -type d -name 'amavis-'
* -mtime +1 -exec rm -rf {} \; > /dev/null 2>&1
#
# Clean up the quarantine dir
#

```

```
0 1 * * * find /opt/zimbra/data/amavisd/quarantine -type f -mtime +7 -exec rm -f  
{} \; > /dev/null 2>&1
```

ZIMBRAEND -- DO NOT EDIT ANYTHING BETWEEN THIS LINE AND ZIMBRASTART

Appendix D: ABQ - SOAP API

Introduction

The "Allow/Block/Quarantine" feature allows for granular access control of mobile devices connecting to the server. For more details about the feature, refer to the [ABQ Service documentation](#).

This appendix introduces the SOAP API support for the ABQ service.

Zimbra SOAP

Zimbra implements the Simple Object Access Protocol (SOAP) for integration with clients. For more information:

- [SOAP API Reference Material beginning with Zimbra Collaboration 8.0](#)
- and [here are](#) a couple of libraries that simplify access to that API.

Zimbra's SOAP implementation comprises a `soap:Header` and a `soap:Body`, as in this example of a SOAP request:

```
<?xml version="1.0" encoding="utf-8" ?>
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <context xmlns="urn:zimbra">
      <authToken>$token</authToken>
      <format type="xml"/>
    </context>
  </soap:Header>
  <soap:Body>
    $xml
  </soap:Body>
</soap:Envelope>
```

Here `$xml` should be replaced with the SOAP request that we want to issue, and `$token` should be a valid token granted by Zimbra after the client has successfully authenticated.

Login

To get access to Zimbra, first authenticate yourself and obtain a valid token. Here is the XML request to do so:

```
<AuthRequest xmlns="urn:zimbraAdmin">
  <account by="name">"user@example.com"</account>
  <password>password</password>
</AuthRequest>
```

Here an example of a reply:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <context xmlns="urn:zimbra">
      <change token="699"/>
    </context>
  </soap:Header>
  <soap:Body>
    <AuthResponse xmlns="urn:zimbraAdmin">

      <authToken>0_2ebb6bdada2b1987c4fa625f95862d2a299b2e4c_69643d33363a34623065356237342d36
      6135612d343435372d393032662d6630313833343131386666363b6578703d31333a313532393335333836
      373330303b61646d696e3d313a313b747970653d363a7a696d6272613b753d313a613b7469643d31303a31
      3031323636373733383b76657273696f6e3d31333a382e382e385f47415f323030393b</authToken>
      <lifetime>43199998</lifetime>
    </AuthResponse>
  </soap:Body>
</soap:Envelope>
```

After we have a valid token we can use it in subsequent calls placing it into the `<authToken>$token</authToken>` of `soap:Header`.

ABQ API

All ABQ calls have a common XML:

```
<zextras xmlns="urn:zimbraAdmin">
  <module>ZxMobile</module>
  <action>$action</action>
</zextras>
```

where `$action` can be: `getDeviceControlList`, `getDeviceStatus` or `setDeviceStatus` followed by a parameter if needed. Here is an example of a reply:

```

<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope">
  <soap:Header>
    <context xmlns="urn:zimbra">
      <change token="699"/>
    </context>
  </soap:Header>
  <soap:Body>
    <response content='{"response":{"devices":[{"device_id":"device4","status":"device1=allowed;device2=quarantined;device3=Blocked"}]}, "ok":true}'/>
  </soap:Body>
</soap:Envelope>

```

All ABQ replies are standard and they are placed into a `<response>` tag with a `content` attribute. Content is formatted as JSON with only one `JSONObject`: `"response"` and `Boolean`: `"ok"`. The former contains the reply and the latter indicates if the request succeeded or not.

getDeviceControlList

Returns a list of all ABQ devices filtered by status: "all", "allowed", "quarantined" or "blocked" (case insensitive)

```

<zextras xmlns="urn:zimbraAdmin">
  <module>ZxMobile</module>
  <action>getDeviceControlList</action>
  <status>all</status>
</zextras>

```

getDeviceStatus

Returns a list of ABQ devices status given a device list (semicolon separated)

```

<zextras xmlns="urn:zimbraAdmin">
  <module>ZxMobile</module>
  <action>getDeviceStatus</action>
  <device>device01;device02</device>
</zextras>

```

The reply contains a JSON array called `devices`, each with a pair of string attributes : `"device_id"` and `"status"`. Here is an example:

```
{"response":{"devices":[{"device_id":"device1","status":"Allowed"}]}},"ok":true}
```

If the requested device is not found in ABQ, it is simply omitted from the response.

setDeviceStatus

Sets the device status for a given device or list of devices. The list is semicolon separated and each element is composed of `device_id = $status` where `$status` can be `Allowed`, `Quarantined` or `Blocked` (case insensitive). Returns a list of failed devices.

```
<zextras xmlns="urn:zimbraAdmin">
  <module>ZxMobile</module>
  <action>setDeviceStatus</action>
  <deviceStatus>device01=allowed;device02=blocked</deviceStatus>
</zextras>
```

The reply contains a JSON array called `devices`, each with a pair of string attributes : `"device_id"` and `"status"`. Here is an example:

```
{"response": {"devices": [{"device_id": "device4", "status": "wrong"}]}, "ok": true}
```

Example

AbqClient is a simple java example to show access to ABQ api. It's self contained and can be build with ant:

```
$ ant build
```

and executed by:

```
$ ant run
```

Glossary

The Glossary lists terms and acronyms used in this document, and includes both industry terms and application-specific terms. If a general industry concept or practice has been implemented in a specific way within the product, that is noted as well.

A record

A (Address) records map the hostname to the numeric IP address. For Zimbra, the A record is the IP address for the Zimbra server.

ABQ

The Allow/Block/Quarantine function provided by the NG Modules gives system administrators control over which devices are allowed to sync via ActiveSync.

Account Policy

Class of Service as exposed in Zimbra administration console.

AD

Microsoft Active Directory Server. Used in Zimbra Collaboration as an optional choice for authentication and GAL, along with OpenLDAP for all other Zimbra Collaboration functions.

Alias

An “also known as” email address, which should be routed to a user at a different email address.

Attribute

Contains object-related data for directory server entries. Attributes store information such as a server host name or email forwarding address.

Authentication

Process by which user-supplied login information is used to validate that user's authority to enter a system.

Blacklist

Anti-spam term, indicates a known bad IP address. This could be one that has been hijacked by spammers, or also one from a poorly maintained but legitimate site that allows mail relaying from unauthorized parties.

BLOB

Binary Large Object.

Class of Service (COS)

Describes an object in the Zimbra Collaboration LDAP data schema, which contains settings for things like user mail quotas. Each Zimbra Collaboration account includes a COS, and the account inherits all the settings from the selected COS.

CLI

Command-Line Interface. Used to refer to the collective set of Zimbra Collaboration command-line tools, such as [zmprov](#).

Cluster

A type of network configuration for high availability, using clusters of servers (nodes). If one server fails or drops off the network, a spare takes over.

Contacts

Within Zimbra Collaboration, Contacts are a user-interface feature listing that user's personal collection of address and contact information.

Conversation

Within Zimbra Collaboration, Conversations are a user-interface feature that presents email threads (emails sharing the same subject line) as a single Conversation listing. Users can expand the Conversation to view all emails within it.

DHTML

Dynamic HTML. A technology employed in the Zimbra Web Client.

DNS

Domain Name System is an Internet directory service. DNS is how domain names are translated into IP addresses and DNS also controls email delivery. Correctly configured DNS is required for Postfix to route messages to remote destinations

Edge MTA

Generic term used to refer to any mail transfer agent that is the first line of defense in handling incoming email traffic. Functions that may occur on the Edge MTA include spam filtering.

Entry

An item in the directory server, such as an account or mail host.

Ephemeral Data

Data which is short lived or fast changing in nature. Login timestamps, authentication tokens, etc.

Failover

Takeover process where a spare server machine detects that a main server is unavailable, and the spare takes over processing for that server.

FQDN

Fully qualified domain name. The hostname and the path to the host. For example, www.zimbra.com is a fully qualified domain name where www is the host, zimbra is the second-level domain, and [.com](http://com) is the top level domain.

GAL

Global Address List, the Outlook version of a company directory. Lists contact information, including email addresses, for all employees within an organization.

Global Configuration

A Zimbra Collaboration object containing default settings for servers and Class of Service.

High Availability

Abbreviated as HA, high availability refers to the availability of resources in a computer system in the wake of component failures in the system.

HTTP

HyperText Transfer Protocol, used along with SOAP for UI integration.

IMAP

Internet Message Access Protocol is a method of accessing mail from a remote message store as if the users were local.

Store

Within Zimbra Collaboration, a directory area that stores all the indexing information for mail messages on a particular mailbox server.

Indexing

The process of parsing incoming email messages for search words.

Java

Java is an industry standard object-oriented programming language. Used for the core Zimbra Collaboration application server.

JavaScript

Scripting largely developed by Netscape that can interact with HTML source code. Technology used in the Zimbra Web Client.

LDAP

Lightweight Directory Access Protocol, an industry standard protocol used for authentication.

Zimbra administration console

The Zimbra Collaboration administrator interface.

Zimbra Web Client

The Zimbra Collaboration end-user interface.

LMTP

Local Mail Transfer Protocol, used for transferring messages from Postfix MTA to the Zimbra Collaboration server for final delivery.

Mailbox Server

Alternative term for Zimbra Collaboration server.

MAPI

Messaging Application Programming Interface. A system built into Microsoft Windows to enable different email applications to work together.

Message Store

Within Zimbra Collaboration, a directory area that stores the mail messages on a particular

mailbox server.

MDA

Mail Delivery Agent, sometimes known as a mail host. The Zimbra Collaboration server functions as an MDA.

Metadata

Data that describes other data, rather than actual content. Within Zimbra Collaboration, metadata consists of user folders, threads, message titles and tags, and pointers.

MIME

Multipurpose Internet Mail Extensions, a specification for formatting non-ASCII Internet message content such as image files. Format used to store messages in Message Store.

MTA

Message Transfer Agent. MTA is a program that delivers mail and transports it between machines. A Zimbra Collaboration deployment assumes both the Postfix MTA and an edge MTA.

MX Record

Mail eXchange. An MX record is an entry in a domain name database that identifies the mail server that is responsible for handling emails for that domain name. The email system relies on DNS MX records to transmit emails between domains. When mail is processed, the MX record is checked before the A record for the destination address.

OOTO

Common shorthand for “out of the office”, used when sending vacation messages.

Open Source

Refers to software created by groups of users for non-commercial distribution, where source code is published rather than proprietary.

OS

Operating system, such as Linux, UNIX, or Microsoft Windows.

POP

Post Office Protocol is used to retrieve email from a remote server over TCP/IP and save it to the local computer.

Provisioning

The process of creating accounts or other data, usually in batch or automated fashion.

RBH

Real-time black hole. Usually refers to web sites that, as a public service, provide lists of known bad IP addresses from which mail should be blocked, because the servers are either known to be spammers, or are unsecured and exploited by spammers.

Redo Logs

Detailed transaction log for the Zimbra Collaboration server, used for replay and replication.

SAN

Storage Array Network. A high-availability data storage area.

Schema

Describes the data structures in use for by directory services at a particular organizational site.

SMTP

Simple Mail Transfer Protocol. Used in Zimbra Collaboration deployments between the Edge MTA and the Postfix MTA.

SNMP

Simple Network Monitoring Protocol. Used by monitoring software to pick up critical errors from system logs.

SOAP

Simple Object Access Protocol, an XML-based messaging protocol used for sending requests for Web services. The Zimbra Collaboration servers use SOAP for receiving and processing requests, which can come from Zimbra Collaboration command-line tools or Zimbra Collaboration user interfaces.

Spam

Unsolicited commercial email. Spammers refer to their output as “bulk business email”.

SQL

Structured Query Language, used to look up messages in the Message Store.

SSL

Secure Sockets Layer.

Tags

A Zimbra Web Client feature. Users can define tags and apply them to mail messages for searching.

TCO

Total Cost of Ownership. Zimbra Collaboration reduces total cost of ownership (TCO) by reducing requirements for server hardware, OS licensing fees, supporting application license fees, disk storage requirements, and personnel (IT, help desk, consulting).

TLS

Transport Layer Security.

UCE

Unsolicited commercial email, also known as spam.

Virtual Alias

A type of mail alias recognized in the Postfix MTA.

Whitelist

Anti-spam term for a known good mail or IP address. Mail coming from such an address may be “automatically trusted”.

XML

eXtended Markup Language.