



Protecting Your Zimbra Collaboration Environment

Zimbra Security and Privacy White Paper





Table of Contents

The Zimbra Approach to Security and Data Privacy	1
Open Source Commitment	1
Adherence to Open Standards	2
Flexible, Open Architecture	3
Tour of the Security Life Cycle	4
<i>Identity and Access Management</i>	4
<i>Information Security and Privacy</i>	6
<i>Administration</i>	9
Zimbra Partner Ecosystem	10
<i>MTA-Level Integration</i>	11
<i>Zimlets</i>	11
Conclusion	11
Acronyms	12

The Zimbra Approach to Security and Data Privacy

With the rise of mobile and cloud computing, sacrificing user experience for improvements to security is no longer an option. Normal modes of business communication have shifted from personal computers to mobile devices. With this shift, organizations must update legacy messaging and collaboration systems to better address the changing threat and technology landscape.

As a messaging and collaboration platform, Zimbra Collaboration is at the core of business communication, a mission-critical component of the organization's information infrastructure. Since no two organizations are the same, the need for flexible, extensible software is critical to the success of any information security and technology program.

This paper explores the native security and privacy features of Zimbra Collaboration. As organizations look to create comprehensive compliance and governance practices, and proactively mitigate malicious activity, Zimbra's approach to security and privacy will help guide evaluations of Zimbra Collaboration as a cornerstone of your information infrastructure.

Open Source Commitment

As a commercial open source vendor, Zimbra offers customers and partners accountability as well as transparency. The open source community reinforces visibility into the software code, while Zimbra ensures that the software meets ongoing requirements for deployments within enterprise and service provider infrastructure environments. This combination results in joint innovation that benefits user experience, security and data privacy.

Zimbra Collaboration is built on established and trusted open source components, including the Linux file system (message store), Jetty (Web server and Java servlet container), MariaDB (database), Postfix (mail transfer agent), OpenLDAP (configuration data and user directory) and others. Each draws from its own open source community, which further improves software quality and thus software security.

What is open source software?

Software licensed with a copyright license compliant with the Open Source Definition.

Software is distributed with its source code in a human readable format.

Software is developed in an open and collaborative way by groups of developers.

Source: Open Software Initiative

As an active participant in the open source community, Zimbra contributes code to open source projects. Not only does this give back to the community that provides so much value—it helps Zimbra Collaboration by validating, enhancing and streamlining the architecture through community input. Commitment to open source provides business continuity, which protects your messaging and collaboration technology investment by ensuring that the core product has a strong, diverse and developer-led open source community.

Adherence to Open Standards

Zimbra Collaboration uses widely adopted industry standards:

- Lightweight Directory Access Protocol (LDAP)
- Secure Sockets Layer/Transport Layer Security (SSL/TLS)
- Simple Mail Transfer Protocol (SMTP)
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Security Assertion Markup Language (SAML) 2.0

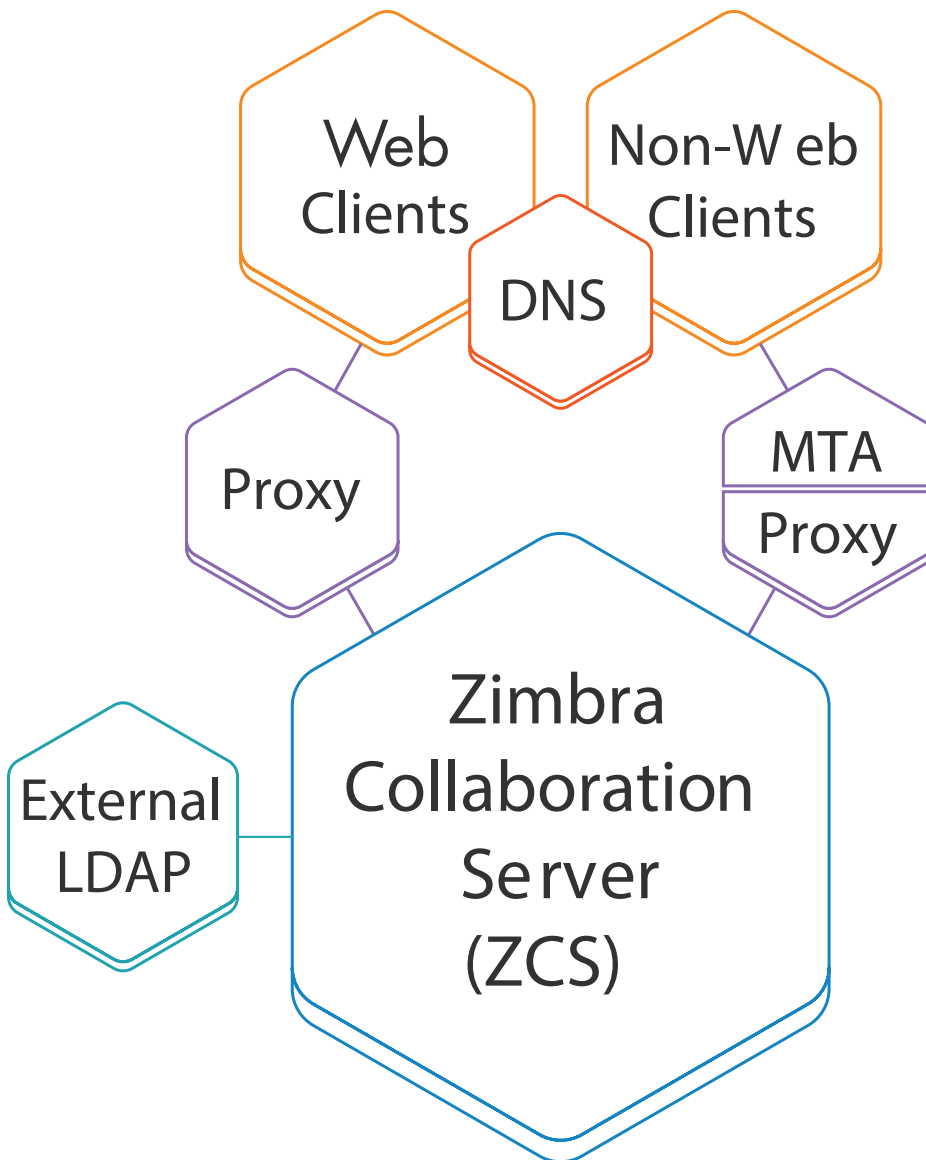
Commitment to standards improves interoperability across mobile, desktop and cloud environments, as well as ensures partners are making calls into a consistent set of APIs. By using open standards, sophisticated users can create their own security and privacy tools or layer in a third-party solution.

An **open standard** is a standard that is publicly available and has various rights to use associated with it, and may also have various properties of how it was designed (e.g. open process). There is no single definition and interpretations vary with usage.

Source: Wikipedia

Flexible, Open Architecture

Zimbra Collaboration uses a modular architecture that supports flexible, secure deployments and helps organizations easily fit the software into their unique information infrastructure. Additionally, the use of a modular platform allows organizations to use existing components of their infrastructure, limiting the need to rip and replace.



Web Client Protocols

- HTTPS
- IMAPS/IMAP+STARTTLS
- POP3S/POP3+STARTTLS

Non-Web Client Protocols

- SMTP
- LMTP+STARTTLS

MTA Components

- AS/AV
- DKIM
- DMARC

ZCS Components

- ActiveSync
- Databases
- Message Store
- OpenLDAP
- Zimbra Web Clients (ZWC)
 - APIs
 - Admin UI
- REST/SOAP/DAV
- Extensions
- Zimlets

Tour of the Security Life Cycle

Defense in depth, the coordinated use of multiple security measures to increase the security of the system as a whole, is still considered one of the best approaches to securing your information infrastructure. Identity and information security are central to Zimbra Collaboration, and by exposing rich interfaces to administrators, organizations can dramatically improve their security posture.

Identity and Access Management

Identity Lifecycle Management

The first step to ensuring organizational security is understanding your users and their rights and privileges. Zimbra Collaboration leverages a native **Lightweight Directory Access Protocol** (LDAP) Directory for all Create, Read, Update and Delete (CRUD) functionality related to user administration specific to Zimbra Collaboration. The use of an external LDAP Directory is optional; however, all attributes specific to Zimbra Collaboration are stored and managed through the native LDAP Directory.

First-factor Authentication

The primary authentication method into mail clients (Zimbra Collaboration or third-party) is username and password. The user store, whether Zimbra Collaboration or external, is used to store the appropriate login credentials. When the native directory is leveraged, all authentication takes place within Zimbra Collaboration, which ships with OpenLDAP.

Zimbra Collaboration automatically stores a salted hash of the password. The hash is used for comparison against the entered password's salted hash, which is then rejected or accepted for login.

If an external directory (LDAP or Active Directory) is preferred, the appropriate login credentials can be stored within this external LDAP directory, or similar. Additional attributes, specific to Zimbra Collaboration, are maintained within the native OpenLDAP Directory.

For setting up external user stores or customer external authentication, refer to Section 5 (Zimbra LDAP Service) of the **Zimbra Collaboration Administrator Guide**.

The **Lightweight Directory Access Protocol** (LDAP) is an Internet protocol for accessing distributed directory services that act in accordance with X.500 data and service models.

Source: IETF

Mobile Device Authentication

For certain mobile devices, Zimbra Collaboration can ensure that the device complies with ActiveSync mobile security policies before allowing access. These policies might include timeouts, personal identification numbers (PINs) and local device wipe. For example, the user must enter a PIN to unlock the device; if a preconfigured number of incorrect PINs are entered, the device performs a local wipe.

Identity Federation and Single Sign-On (SSO)

To help organizations reduce user identity proliferation, Zimbra Collaboration can be set up as a Relying Party (RP) in a federated identity ecosystem, as well as streamline the user login process through SSO.

As an RP, Zimbra Collaboration can consume identity assertions from SAML (including Shibboleth), OAuth and Connect ID Identity Providers (IDP). The IDP and Zimbra Collaboration mutually authenticate. Once a secure, trusted connection is established, the IDP will pass an identity assertion through to Zimbra Collaboration, which will allow or reject access.

To reduce friction for users, Zimbra Collaboration can pass through authenticated credentials to connected services that rely on the same credentials. To achieve SSO, Zimbra Collaboration uses Kerberos (and an associated Kerberos5 service) or an LDAP pre-authentication key.

For setting up a Kerberos service or becoming an RP (custom authentication), refer to Section 5 (Zimbra LDAP Service) of the [Zimbra Collaboration Administrator Guide](#).

Two-factor Authentication

For organizations looking to augment their security, an additional layer of identity security can be overlaid onto Zimbra Collaboration via custom authentication. In this scheme, the username and password act as the “something you know” with the second factor performing the function of a “something you have,” which is the traditional approach in a two-factor scheme.

Authorized Access

After users connect to Zimbra Collaboration, authorization processes control what data they can see and which functions they can perform. For example, most users can use their own email and calendars, while some may be able to check someone else’s calendar.



Federated identity management enables identity information to be developed and shared among several entities and across trust domains. Tools and standards permit identity attributes to be transferred from one trusted identifying and authenticating entity to another for authentication, authorization and other purposes, thus providing “single sign-on” convenience and efficiencies to identified individuals, identity providers and relying parties.

Source: Gartner, Inc.

Zimbra Collaboration supports highly granular authorization frameworks. Attributes, permissions and policies drive everything in Zimbra (including accounts, domains, mail folder, contacts, calendar, tasks and briefcase folder). Administrators can easily create groups and assign access permissions to support specific business objectives.

Permissions

Zimbra Collaboration offers flexible permissions for shared mail folders, contacts, calendars, tasks lists and briefcase folders. You can grant internal users or groups permission to view, edit or share folders. You can also grant external users read-only or password-based access to shared objects. For example, you might give a colleague the permission to create, accept or delete meetings for your calendar but not to share your calendar with other users.

Delegated, Role-Based Administration

Zimbra Collaboration lets you delegate administrative tasks with highly configurable permissions. An administrator's role can be as simple as managing a distribution list or resetting forgotten passwords for a specific group of users. You can create roles from a plethora of attributes and for a number of tasks in Zimbra Collaboration. It also provides predefined roles for domain administrators and distribution-list managers.

Information Security and Privacy

The next layer to our defense-in-depth approach is to ensure that the information generated by users remains secure and private. Zimbra has taken several steps to ensure the privacy and security of user information, including shipping the product with security and privacy-enhancing mechanisms and protocols enabled as the default.

Message Security, Integrity and Privacy

By using cryptographic services, specifically public key or asymmetric cryptography, users can ensure message security, integrity and privacy, as well as sender authentication. To perform these functions, Zimbra Collaboration supports the use of S/MIME certificates, which can be provided by a publicly trusted Certification Authority (CA). Alternatively, an internal PKI may be used if public trust is not required.



Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries).

Public Key Cryptography

Public key cryptography, also known as asymmetric cryptography, is a class of cryptographic algorithms, which requires two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plaintext or to verify a digital signature, whereas the private key is used to decrypt ciphertext or to create a digital signature.

Source: Wikipedia

An S/MIME certificate can provide message authentication, integrity and non repudiation through a digital signature, as well as message confidentiality through encryption. In addition, many nations have digital signature laws, which equate a digital signature to a physical signature and provide non-repudiation for digitally signed emails, transactions or documents.

Additional message authenticity methods available in Zimbra Collaboration:

- DomainKeys Identified Mail (DKIM) signatures can be added to email headers to verify the sender's domain.
- Domain-based Message Authentication, Reporting and Conformance (DMARC) expands on DKIM capabilities to provide message authentication and includes explicit guidance on message handling if DKIM signatures aren't present.

Amavisd-new leverages the integration with the Zimbra Collaboration OpenLDAP directory for domain attribute validation, including DKIM keys. Amavisd-new is housed in the Mail Transfer Agent (MTA) and manages the incoming and outgoing DMARC policies.

In-Transit Encryption

Zimbra recommends the use of, and defaults to, secure alternatives of all mail protocols and communications channels between Zimbra Collaboration services and endpoints. In fact, to further improve security and privacy, Zimbra provides the option to use opportunistic TLS or to require encrypted communications. For supported versions of Zimbra Collaboration, OpenSSL's cryptographic library is embedded into the product.

Secure connections between endpoints/services use TLS; additional security is protocol specific:

- SMTP
- LMTP+STARTTLS
- HTTPS
- IMAPS/IMAP+STARTTLS
- POP3S/POP3+STARTTLS

S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a consistent way to send and receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures), and data confidentiality (using encryption). As a supplementary service, S/MIME provides for message compression.

Source: IETF

At-Rest Encryption

When S/MIME is used for end-to-end encryption, the data stored in the Zimbra Collaboration message store is encrypted until decryption takes place with the appropriate private key.

Antivirus and Antispam

Email-based malware remains a prominent threat for businesses, and while usually not as insidious, spam clogs email systems and increases user frustration. Zimbra addresses malware and spam through both native functionality and third-party plugins.

Amavisd-new is the interface for information exchange between MTA, ClamAV and SpamAssassin.

ClamAV is open source antivirus software with traditional signature-based matching and heuristics. The rules and signatures are updated daily.

SpamAssassin is open source antispam software that supports ongoing spam-filter training (i.e., teaching the filter what is spam and what isn't), enabling organizations to optimize performance in their own environments. Users can train spam filters by moving messages in and out of their junk folders.

Disaster Recovery and High Availability

Though disaster recovery is not often considered a security feature, the assurance that your data is intact is beneficial for organizations. Also, as your user base grows, the need to ensure uptime and the timely delivery of data will increasingly put demands on the infrastructure. Zimbra is developing an active-active architecture to help ensure your information is delivered on time, every time.



According to the AV-TEST Institute, over 390,000 new malicious programs are registered by their systems daily. By the end of 2014, there were over 300 million malicious programs (total), with 140 million of those being new malware as of 2014.

Source: AV-TEST Institute

Administration

While the user is busy sending and receiving email, scheduling appointments and collaborating with others, Zimbra Collaboration is logging activity. Based on your audit and compliance needs, you can set different levels of logging.

Zimbra Collaboration logs a wide range of activities:

- User and administrator activity
- Login failures
- Slow queries
- Mailbox activity
- Mobile synchronization activity
- Database errors

Zimbra Collaboration supports the syslog format and Simple Network Management Protocol (SNMP). Log events, alerts and traps can be forwarded to log-management and event correlation systems to create centralized policies and notifications based on your security and compliance requirements.

These logs can support forensic analysis, which is useful for our next step: incident response.

Incident Response

Even with the layers of security we've defined so far, you may need to take action to respond to a problem or mitigate risk. For example:

- A user's account credentials have been stolen.
- An executive left his or her smartphone in a taxicab.
- Log analysis reveals problematic activity on an administrator account.

Zimbra supports incident response in several ways.

Zimbra Collaboration uses log4j, a Java logging package, as the log manager for mailboxd. By default, the Zimbra Collaboration server has log4j configured to log to the local file system, but log4j can be configured to direct output to a variety of other locations. For more, visit the Zimbra Wiki.

[Visit the Zimbra Wiki](#)

Remote Device Wiping

If a tablet or smartphone that uses Zimbra Collaboration is lost or stolen, the administrator can wipe the data from the device remotely. This mitigates the risk of someone accessing the Zimbra Collaboration data remotely. It also reduces the risk of the data on the device being compromised.

Account Lockout

You can configure a policy that automatically locks an account after a specific number of failed login attempts. The administrator can also immediately disable any account at any time.

An administrator with appropriate access privileges can also view the email messages of the suspect account to help determine if the account has been compromised.

If you are using a federated identity management solution or an internal directory with Zimbra Collaboration to implement SSO, you can disable access from the central directory or identity store to prevent authentication to the Zimbra Collaboration account.

Archiving and Discovery

Zimbra Archiving and Discovery is an optional feature of Zimbra Collaboration. With this integrated solution, you can select which users' email messages to archive and set retention policies for both archived and live mailboxes. Zimbra Archiving and Discovery offers powerful search indexing in a simple, cost-effective platform. You can also integrate third-party archiving solutions with Zimbra Collaboration.

Zimbra Partner Ecosystem

As part of a broader information and identity security infrastructure, Zimbra Collaboration can integrate with additional security and privacy solutions. Zimbra's reliance on open-based standards helps make integrations and inter-application communications easy.

Zimbra Collaboration supports two types of third-party integrations:

- MTA-level integration
- Zimlets



Zimbra partners with hosting providers to provide in-region hosting of Zimbra Collaboration. By relying on in-region hosting, customers and end users are ensured their data is under the auspices of only the most directly applicable regulations, legislations and jurisdictions.

MTA-Level Integration

Through its support for SMTP protocols, Zimbra Collaboration offers gateway-level integration with a wide range of third-party solutions. For example, Zimbra Collaboration can be configured to send all messages to an SMTP-enabled gateway, which can then provide email archiving, content filtering, data-loss prevention, etc.

Zimlets

Zimlets makes it easy to customize and extend Zimbra Collaboration to suit your needs, allowing you to add new features to suit your particular requirements. Zimlets are a mechanism for integrating with and extending the functionality of Zimbra Collaboration. Zimlets enable the “mash-up” of web-based technologies with enterprise messaging (e.g. email, IM, voice) and collaboration systems. With Zimlets, message content and collaboration objects can be made live by dynamically linking to web content and third-party services.

Visit Zimbra.com to view the Zimbra Gallery of community-contributed Zimlets. Please note that this is not an exhaustive list of available Zimlets, as many Zimbra partners create and deploy their own.

Conclusion

Messaging and collaboration solutions are business-critical applications and should be put through the same risk assessments and considerations as other critical applications. The best defense remains defense in depth, which has multiple layers of security. This approach should properly balance the needs for administrative control, information and identity security, privacy and the user experience.

As security paradigms shift and the threat landscape evolves, leveraging open source and open standards will define best-in-class software. Community-driven innovation will ensure that Zimbra Collaboration meets the constantly changing business needs of organizations. By building around an open source core, Zimbra Collaboration provides a robust platform for organizations to offer secure, private messaging and collaboration, whether mobile, desktop or in the cloud.

If you are interested in more information on the Zimbra Security Vulnerability Disclosure and Response Program, visit the below links.

[Security Center](#)

[Security Response Policy](#)

[Vulnerability Rating Classification](#)

[Responsible Disclosure Policy](#)

[Reporting Vulnerabilities to Zimbra](#)

Acronyms



Antispam



Antivirus



Domain Keys
Identified Mail



Domain-based Message
Authentication, Reporting
and Conformance



Identity Provider



Lightweight Directory
Access Protocol



Message Transfer Agent



Relying Party



Security Assertion
Markup Language



Secure Multipurpose
Internet Mail Extensions



Simple Mail Transfer
Protocol



Secure Socket Layer



Single Sign-On



Transport Layer Security



Zimbra 3000 Internet Blvd., Suite 200 Frisco, Texas 75034 Tel +1 (972) 407-0688 www.zimbra.com

Copyright © 2015 Synacor. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. Zimbra is a registered trademark or trademark of Synacor in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.