

Zimbra Collaboration 8.7

Open Source Messaging and Collaboration



What Is Zimbra Collaboration?

Zimbra Collaboration is the world's leading open source messaging and collaboration solution, trusted by more than 5,000 companies and public sector customers, and over 500 million end users, in over 140 countries. Zimbra includes complete email, contacts, calendar, file-sharing and tasks, and can be accessed from the Zimbra Web client via any device. You can deploy Zimbra as a traditional on-prem install or through a Zimbra hosting provider.

Key 8.7 Features

The Zimbra Collaboration 8.7 release is specifically enhanced for global enterprises and service providers, including Two-Factor Authentication (2FA), a new Zimbra Packaging System, SSL Server Name Identification (SNI) and Zimbra Postscreen, all combined to deliver a low total cost of ownership (TCO).

And there is still more to come. Zimbra's active and vibrant Partner Community continues to leverage the Zimbra platform to extend Zimbra products through Zimlets and APIs. Zimbra Partners have integrated Zimbra with Plone, BroadSoft, ThinkFree, Alfresco, ownCloud and other open source products to create rich end-user experiences. We will be offering some of these valuable integrations as Zimbra add-on packages in 2016 and beyond.

2-Factor Authentication (2FA)

Two-factor authentication provides identification of users with the combination of two different components. These components may be something that the user knows (like a password, UserID, etc.) and something that the user possesses (good examples are a smartphone, USB-key, etc.).

The use of 2FA to prove your users' identity is based on the premise that an unauthorized user is unlikely to be able to supply both factors required for access.

The 2FA feature must be enabled in the Admin Console, and it can be enabled at the User or Class-of-service levels. This allows precise security control. Once the Admin has enabled 2FA, users set up the feature using the new option under Preferences > Accounts, called Two Factor Authentication.

For more information about Zimbra 2FA, [click here](#).

KEY BENEFITS

- **2-Factor Authentication**
- **Zimbra Packaging System**
- **SSL SNI**
- **Postscreen**

ZIMBRA PRODUCT OVERVIEW
ZIMBRA COLLABORATION

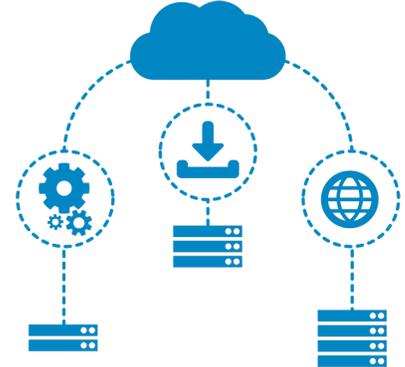




Zimbra Packaging System

With the new Zimbra Packaging System in Zimbra 8.7, you can apply security patches and Zimbra updates easier than ever before. When a new vulnerability comes up, simply update individual Zimbra components instead of the entire Zimbra package (typically a full upgrade).

When the next vulnerability is released, how quickly can you update your infrastructure for protection? With Zimbra's new packaging, you can update the effected component as soon as the update is available, whether the software is openssl, Nginx, PostFix or some other open source component used by Zimbra. Zimbra has already leveraged this capability to apply performance updates to individual package components within our internal 8.7 infrastructure. For more information, [click here](#).



SSL SNI

If you are hosting multiple Zimbra domains, Zimbra 8.7 now supports Multiple SSL domains on a single server for HTTPS connections. You can now publish multiple SSL Certificates using one single IPv4 with Server Name Indication (SNI).

With SNI, a server can present multiple certificates on the same IP address and TCP port number, allowing multiple hostnames to be served over HTTPS from the same IP address without requiring all those sites to use the same certificate.

[Click here](#) for more information about Zimbra SSL SNI.

Postscreen

Zimbra Postscreen is an additional Anti-Spam strategy at the MTA level. The postscreen daemon provides protection against mail server overload. One postscreen process handles multiple inbound SMTP connections and decides which clients may talk to a Postfix SMTP server process.

In a typical scenario, good connections, bots and zombies talk with Postscreen. Postscreen does basic checks and denies the connection if the message is from a bot or zombie. If the connection is not in the temporary whitelist, Postscreen will pass the email to the local Anti-SPAM and Anti-Virus engines, who can accept it or deny it as usual.

For more information about Zimbra Postfix, [click here](#).



About Zimbra

Zimbra, a Synacor brand, connects people and information with unified collaboration software that includes email, calendaring, file sharing, chat and video chat. Zimbra is trusted by more than 5,000 companies and government customers, as well as by service providers who manage Zimbra in the cloud for more than 200,000 businesses. Zimbra is the largest provider of open source collaboration software in the world. For more information, visit Zimbra.com or connect with us on [Twitter](#), [Facebook](#) and [LinkedIn](#).