Collaboration Applications

Email

Secure Standard Mail Access Protocols

- **POP Access**: Users can download their mail from the server to the Desktop/Mobile using POP email clients such as Mozilla Thunderbird, MS Outlook and Outlook Express.

  Users can set POP Threshold to download mail only after the Threshold date.

  Automatically syncs the sent folder on the mobile or desktop client with Sent Items folder on the server.
- **POPS Access**: POP is available with SSL to secure the channel during access.
- **IMAP Access**: Users can configure their Desktop/Mobile email clients to be in sync with their mailbox on the Connect Xf server using the IMAP protocol. Most of the desktop clients support caching of the email locally allowing offline access of the email messages. IMAP is an efficient and modern protocol, whose biggest benefit is that it allows a mirror view of the mailbox from any of the IMAP clients viz. web, desktop or mobile, allowing you to interchangeability or simultaneously use all three access methods.
- **IMAPS Access**: IMAP is available with SSL to secure the channel during access

  Choosing between POP and IMAP

Secure Standard SMTP protocol

- Configure multiple simultaneous SMTP ports on the server to work in environments where port 25 is blocked.
- Strict reputation and security checks at SMTP layer like valid sender, valid recipient, reverse pointer check, authentication, spoof, etc.
- Secure SMTP communication between Client-Server and Server-Server over TLS.

Automatic Mail Processing tools

- **Auto Forward**: If allowed, users can configure their account to forward all incoming mail to alternate email IDs. This can be useful in case the user has more than one email ID in use.
- **Auto Forward to alternate host:** Administrators can configure a user's account to forward all incoming mail to an alternate host server. This is useful while configuring multi server and/or hybrid setups to integrate with other email systems.

- **Automatic Mail Filters**: The system can automatically match the mail being delivered to the mailbox with predefined rules and perform preset action on these mail. The rules work on mail attributes like sender, recipient, subject etc. The possible actions on the mail, which match the rule sets, can be: Move the mail to a different folder, Copy the mail to a different folder, Forward the mail to another email ID, Forward the mail as an SMS and Discard the mail. Note that these filters are applicable at the server level and will come into force irrespective of the client software used to access the mail.
- **Vacation Reply**: While being away from office for extended periods (touring or on leave), users can configure an automatic reply to every incoming mail with a custom message. The configuration of the automatic reply can be done via the Settings page of Baya (Web client) or via the custom settings page within Thunderbird (Mithi provides a plugin to extend Thunderbird for setting vacation reply and other common attributes)
- **Footers/ Disclaimers:** Administrators can configure a disclaimer message, which will be automatically attached to all outgoing mails. The system provides the choice of separate disclaimers for local and remote recipients. Additionally, the disclaimer messages can have a rich format (HTML) to support formatting and images.

Securing the use of Email

- **Access Rights**: Administrator can define access rights to control which user can use which protocol and from which networks.
- **Mail flow policies**: Administrator can define mail flow policies to define the scope of mail sending and receiving per user and per group of user.
- **Secure protocols**: Access POP, IMAP, SMTP over secure channels using SSL to encrypt the data flow.

Multiple Access Methods

Access your email box from your choice of standards compliant clients like:

- **Baya**: High performance Web client; a single interface for accessing all your applications.
- **Desktop clients:** Thunderbird, Outlook, etc
- **Mobile devices:** Android, iOS based devices, Blackberry, etc.

Calendar

Create and access multiple calendars

Users can organize their activities into different calendars for easier management, e.g. one calendar per project, one personal calendar, etc. Multiple calendars can be viewed in overlap to get a sense of the total agenda for any day.

Calendar Sharing and Subscription

Users can share their calendar for access and use by other members of the team. The sharing can be based on different access rights to different users. Users who have been given access to a shared calendar, can subscribe to these calendars to read and modify them.

Tasks, Events and Meetings

Users can manage their tasks, events and schedule meetings with participants. Check the free busy status of participants to meetings.

Receive email alerts for upcoming calendar events and meetings.

The system can be configured to automatically send out email invites when events/meetings are created or updated using the webclient or CalDAV compliant desktop/mobile clients.

Exchange calendar data with other calendar systems

Export calendar data to a standard iCal file for use by other standard calendar systems. Import calendar data (iCal files) from other standard calendar systems

Securing access to the Calendar by Policy control

Administrator can define, which user can get access to the calendar services

Multiple Access methods

The calendar on Connect Xf can be accessed from your choice of CalDAV compliant client like

- **Baya**: High performance Web client, a single interface for accessing all your applications.
- **Desktop clients**: Thunderbird, Outlook, etc

- **Mobile devices**: Android, iOS based devices etc.

Address Book

Personal Address Book

- **Private Contact list:** Each user has a private address book, which can be used to store personal and frequently used contacts.
- **Maintenance**: The address book can be maintained and modified from Baya (web client)
- **Import/Export**: Insert contacts, which are exported from other systems in a CSV file. The system supports several popular CSV formats, out of the box. Similarly export your contacts to a CSV for insertion into another system. These interfaces are available only via Baya.

Shared Address Book

- **Multiple shared address books**: Administrators can configure the shared address book of a domain, by linking contacts from different sources e.g. the corporate directories of other domains on the server and global address books of other domains.
- **Maintenance**: The Shared address list is maintained automatically for contacts sourced from the corporate directory or from address books of other domains. When users/contacts are added and deleted from the corporate directory or global address books, these automatically reflect in the shared address books where they are included.
- **Custom display name formats**: Display names can be customized by composing them from user attributes like name, designation, location etc

Address Book Access

- **LDAP:** The address books can be accessed from any email client via LDAP and automatically show up during auto complete of user ids in relevant forms.
- **Secure access**: Domain users get secure private access only to relevant address books.

Multiple Access methods

The address book on Connect Xf can be accessed from your choice of LDAP compliant clients like

- **Baya**: High performance Web client, a single interface for accessing all your applications.
- **Desktop clients**: Thunderbird, Outlook, etc

- **Mobile devices**: Android, iOS based devices etc.

Chat

Standard XMPP access protocol

Configure and access the chat/IM services over the XMPP protocol to collaborate with buddies on the enterprise network. XMPP allows you to use a variety of different chat client applications on different platforms.

Collaborate over Chat

- **One-on-One Chat:** Have private conversations with colleagues.
- **Multi User Chat:** Use group chat for communication amongst departments, teams, or projects. Rooms can be open for anyone to join, or private for only invited members, can be persistent and available across sessions or available only for the session and can be password protected.
- **History:** Use Chat History to track all your One-to-One and multi-user conversations and access them on demand.

Easy to use and manage

- **Presence Management:** Update your presence status for other users of your roster to see.
- **Emoticons**: Express yourself by using emoticons.
- **Roster Management**: Manage a Roster of chat contacts (buddies) with whom you communicate frequently. Add buddies to your roster by using the auto-complete feature to look up the corporate directory for colleagues.
- **Spell Check:** Avoid embarrassing mistakes by using the online spell check.
- **Notifications**: Get notified when a buddy comes online or goes off line and when a new message arrives.
- **Preferences**: Customize the chat application as per your needs
- **Pin-out chat window**: Use Pin-out the chat window to see more of the conversations.

Security of the conversations

- **Access Rights**: Connect Xf allows you to enable or disable One-to-One and Group Chat at an

individual level.

- **Scope of Communication**: The administrator can define the scope for a user (i.e. with who all can this user initiate a conversation)
- **Archive all chat transcripts:** Connect Xf can be configured to convert transcripts of One-to-One and multi-user chats into email, which are then delivered to the mailboxes of the participants. The email archive system will capture these transcripts (sent as email) and retain them for compliance.
- **Secure Transmission**: Secure message transmission using secure XMPP to ensure that there is no data theft during transmission.

Strong Management capabilities

- **Manage the Enterprise Chat App easily**: The command line and GUI interfaces of Connect Xf make managing the Chat application easy.
- **Generate Activity Reports:** Use the reporting engine to get reports on users who have logged in to use the chat service.
- **Authenticate using External Directories:** Use the "authservice" of Connect Xf to authenticate users with external directory servers such as ADS.
- **Backup of User and Roster Data:** The native backup scripts secure all user configuration and roster data to ensure no data loss.
- **Quickly Diagnose Problems:** Use the diagnostic framework to quickly identify problems.

Multiple Access methods

The chat/IM service on Connect Xf can be accessed from your choice of XMPP compliant clients like:

- **Baya**: High performance Web client, a single interface for accessing all your applications.
- **Desktop clients**: Thunderbird, Pidgin, Exodus, etc.
- **Mobile devices**: Android, iOS based devices, Blackberry (third party client) etc.

SMS

Introduction

With a near ubiquitous presence of the mobile phones, it forms a very important, indeed essential means by which people connect and communicate with their personal and professional network.

Extending the email network to the mobile phone therefore makes imminent sense. However, most approaches to enable email access on the mobile phone have been constrained by the need for

special devices and services.

The SMS integration in Connect Xf however breaks through this constraint enabling users to access their mail message through SMS.

This approach therefore offers a lower cost, faster, easier way to extend the enterprise email network to include the mobile phones, with immediate benefit to productivity and responsiveness of an enterprise. The SMS integration enables the following benefits for the user and the administrator.

Interesting use cases of the email to SMS capability

This platform enables a whole new set of applications and also increases the efficiency of the work force. Below are a few examples of how the integrated SMS feature can be used by organizations:

- The organization has uploaded all the key customer information in the Global Address Book along with the mobile numbers.
- The marketing team has also defined separate distribution lists or mailing groups based on cities and regularly sends SMS updates to its customers.
- Alert about new offering are sent to the traveling sales force using SMS, asking them to refer to the web site for details.
- Account managers have configured SMS alerts from key customers.
- I am sending a very important mail to a team lead and need to be sure that he gets alerted of it right away. The quickest way is to deliver this via SMS

Alert recipients of an important email sent

Using the Email to SMS feature, send SMS messages from your email account. While sending an email, also send a summary of that as an SMS to the recipients. This serves to alert the recipients immediately about an important message sent

Receive SMS alerts for important email messages

Users can configure SMS alerts to be sent to their mobile phones, based on mail filter rules, e.g. send an alert with a summary of the mail, whenever the user receives a mail from ravi@mycustomer.com.

View presentation on Email to SMS Integration

Alert members of a Distribution list of an important email sent

The user (if allowed to use this feature) can send an email to a group and also send a summary of the same email as an SMS to the same group. The system would send the email to the members and also send an SMS to each member of the group. It would take the phone numbers from the directory

and address books.

Track/Archive all the SMSes sent and received by every user

A single message store, ensures that communication via SMS or email are archived in a single location and easily searchable

Use from Baya (web client) or Desktop clients like Thunderbird or MS Outlook

Baya integrates the capability to send SMS alerts for select emails, right into the compose page. While sending the email, you can choose the SMS recipients for the shortened message from the address book, or enter the mobile numbers directly. You can also choose the fields of your email, which should compose the shortened message to be sent as an SMS alert. While sending from a desktop client, you would need to mark a bcc to a predefined system id, which will capture the recipient ids from the mail and transport a summary to them via SMS. It would take the phone numbers from the directory and address books.

Control who can use the SMS feature

Administrators can define which users have access to this feature of Email to SMS.

Can connect to standard SMS gateways over HTTP

For the SMSes to be transported, you would need to purchase bulk SMS credits from an aggregator, who will provide you with an HTTP URL, user id and password of your account. By invoking the loaded URL, the SMS gateway will transport the SMS to the specified mobile number.

Access Devices

Configuring Mobile devices with Connect Xf

Email

Configure Email on these popular Mobile Devices to experience features like Search, IMAP Push Email, Multi-folder Sync, Flagging, etc.

Calendar

Use built-in CalDAV settings in iOS devices and use 'CalDAV-Sync' Calendar application for Android devices to setup your Calendar account and share your calendar with your colleagues.

Contacts/Address Books

Use the built-in LDAP application in iOS devices and use the 'Contacts In Line' application for Android devices to setup your Address Book and to create, manage and share your contact list.

Chat

Use 'JabberB' application on iOS devices, 'Xabber' application on Android devices and 'BeejiveIM' application on BlackBerry to setup your Chat account and to start chatting with your colleagues.

Compatibility of the Connect Xf collaboration applications with various mobile clients

Applications / **Devices**	**Email**	**Calendar**	**Contacts**	**Chat**
Android	* Access email account and Folders * Access over secured channels * POP/IMAP protocol	* Sync Calendar Events and meetings * Access over secured channels * CalDAV Protocol	* Look up Shared Contacts * Import Contacts * Access over secured channels * LDAP Protocol	* Send/receive text messages * Access over secured channels * XMPP Protocol
IOS	* Access email account and Folders * Access over secured channels * POP/IMAP protocol	* Sync Calendar Events and meetings * Access over secured channels * CalDAV Protocol	* Look up Shared Contacts * Import Contacts * Access over secured channels * LDAP Protocol	* Send/receive text messages * Access over secured channels * XMPP Protocol

Desktop Collaboration Suit

Connect Xf helps you further lower your licensing costs with free Desktop Email clients like Mozilla Thunderbird for Email, Address Book, Chat and Calendar. Thunderbird has native built in support for an XMPP based chat client and also supports a plugin called “Lightning” for Calendar sync.

For desktop chat clients, you can opt for free clients like Neos, Pidgin, Exodus, etc. You can further save cost using Open Office which is a free Open Source based Office Productivity Package.

Compatibility of the Connect Xf collaboration applications with the various desktop clients

Application Desktop Client	Email	Shared Calendar	Contacts	Chat
Thunderbird	* Access email account and Folders * Access over secured channels * POP/IMAP protocol	* Sync Calendar Events and meetings * Access over secured channels * CalDAV protocol * Using Lightning plugin	* Look up Shared Contacts * Import Contacts * Access over secured channels * LDAP Protocol	* Send/receive text messages * Access over secured channels * XMPP Protocol
Outlook	* Access email account and Folders * Access over secured channels * POP/IMAP protocol	Unavailable * You can use the personal calendar	* Look up Shared Contacts * Import Contacts * Access over secured channels * LDAP Protocol	Unavailable
Apple Mac	* Access email account and Folders * Access over secured channels * POP/IMAP protocol	* Sync Calendar Events and meetings * Access over secured channels * CalDAV protocol	* Look up Shared Contacts * Import Contacts * Access over secured channels * LDAP Protocol	Unavailable
Outlook Express	* Access email account and Folders * Access over secured channels * POP/IMAP protocol			

Eudora	* Access email account and Folders * Access over secured channels * POP/IMAP protocol	Unavailable	Unavailable	Unavailable
Windows Live Mail	* Access email account and Folders * Access over secured channels * POP/IMAP protocol	Unavailable * You can use the personal calendar	* Look up Shared Contacts * Import Contacts * Access over secured channels * LDAP Protocol	Unavailable
Neos	Unavailable	Unavailable	Unavailable	* Send/receive text messages * Access over secured channels * XMPP Protocol
Pidgin	Unavailable	Unavailable	Unavailable	* Send/receive text messages * Access over secured channels * XMPP Protocol
Miranda	Unavailable	Unavailable	Unavailable	* Send/receive text messages * Access over secured channels * XMPP Protocol

Working of Email

- Desktop clients like Thunderbird need to be configured to connect to your account on the Connect Xf server. The information requested here would be the SMTP/POP/IMAP server and the necessary authentication information pertaining to the user's mailbox on the Mithi Connect Xf server
- To send an email, the user would compose a mail using the email client and send. The email client would then connect to the specified SMTP server (Connect Xf in your setup) and send the mail.
- To receive mail for the user, the email client would periodically poll the user's account on the

POP/IMAP server (the Connect xf in your setup) for new messages. It would then download the messages and alert the user.

- Using IMAP on all email clients (mobile and desktop), can provide the user with a uniform view of the mailbox from the mobile device, desktop client and Baya (web client). This means that any mail sent from the mobile client is also seen in the sent items of the desktop client or web client (since each of the clients is showing a view of and modifying the same mailbox on the server). Similar behavior is observed for deletion of mail, moving mail between folders, saving to drafts, and for reading/marking of mail.

  Note: MS Outlook is capable of connecting to a mail server like Connect Xf over SMTP/POP and IMAP

Working of Calendar

You would need to deploy a plugin called "Lightning" into Thunderbird to make it connect to the CalDAV service on Connect xf, the open protocol for accessing calendar services. This implies that the clients update and sync calendar information from the Connect Xf server. This presents a uniform view of the calendar data via any of the clients, i.e. any changes made on the calendar using the smart phone, or Baya (web client), or Thunderbird (desktop email client) are in sync.

Note: Since MS Outlook was designed to support the MS Exchange calendar service over MAPI, it is currently incapable of working with the CalDAV server of Connect Xf. This means that if you use MS Outlook with Connect Xf, you will be able to work with your personal calendar (add, modify, delete events and schedule meetings and reminders), but will not be able to share it or work with the group calendars.

Working of the Address book

Typically the desktop clients have a built in address book/contact application, which supports connections to an LDAP server (the Connect xf in your setup), which can sync contacts from the server over the LDAP protocol. This allows a one way sync of the global address book contacts for the company to the mobile device. This means that when employees are added, deleted or their information modified, the same is synced to the mobile device.

Note: MS Outlook is capable of connecting to an LDAP server.

Working of Chat

You can use any XMPP based chat client like pidgin, neos, etc or the inbuilt chat application in Thunderbird, which can connect to an open XMPP server (the Connect Xf in your setup). Since the roosters are provided by the XMPP server, the user will see a uniform view of the chat rooster and presence indicators when working with chat from different access points (Baya, desktop chat clients and mobile chat clients).

Note: If you are using MS Outlook as your primary client, you would need to use an extra XMPP chat

client on your desktop to access the chat service or you may use the web chat facility of Baya.

Configuring Desktop clients with Connect Xf

- **Email**

  Configure Email on these popular desktop clients to experience features like Search, IMAP Push Email, Multi-folder Sync, Flagging, etc.

- **Calendar**

  Use the CalDAV client (via the Lightning plugin) in Thunderbird to setup your Calendar account and share your calendar with your colleagues.

- **Contacts/Address Books**

  Use the built-in LDAP application to setup your Address Book and to create, manage and share your contact list.

- **Chat**

  Use these XMPP chat clients to setup your Chat account and to start chatting with your colleagues.

Baya

Web Mail

While composing a message in Baya, you can send it as an Email and/or SMS via the same interface without having to switch between multiple windows.

User's can efficiently manage their email using context- sensitive menus, infinite scroll-bar, faster sorting and incremental searching for quick results.

The AutoComplete feature saves you the hassle of remembering the contact info. Soon as you start typing the recipient email/ phone number, it auto-suggests a list of related contacts.

You can organise your mailbox very easily with Folders. Simply create mail-filters to divert incoming messages to different folders or receive them as text messages on your mobile.

Attachment handling includes features such as multiple files attachment on a single click, preview

attachments prior downloading them on machine, or review, add and share comments to attachments without downloading them on machine using Framebench connector.

Web Calendar

With a few clicks, you can keep track of your tasks, events, meetings and share the calendar with

anyone in your Address Book, keeping them in sync during meetings and other events. Once the members have given access of their calendars, it is very convenient to view their schedules and avoid overlaps.

You can also import and export calendars to Baya Webmail using iCal Calendar protocol.

Contacts

Connect Xf provides a Personal Address Book to let you manage a personal list of contacts while a Shared Address Book gives access to the Global Address Book and Corporate Directory. The Shared Address Book automatically syncs with Connect Xf Server via LDAP, thus eliminating the need to duplicate the entries manually. The Address Book can also be used to send email/ SMS to multiple contacts from your directory.

Web Chat

Baya makes chatting really convenient with the integrated Chat feature. You can engage in individual and group chats, create private chat rooms, etc. All the chat exchanges are archived in a folder to be accessed for later reference.

Presentation on Benefits of Baya chat

Baya Security

Captcha on Login page restricts the entry for robots.

Last Login details in the user panel helps users in monitoring the illegal access to their account.

Management

System

Easy and intuitive admin panel for user and group management

- Intuitive Cross Browser Admin panel interface: Easier day-to-day management of users and groups.
- Bulk user addition/deletion: Add users one at a time, in small groups or import from a CSV file
- Easily locate users: See a sorted list of users and Search through a large list of users
- Easily modify user information: Update frequently used properties through an intuitive interface
- Export the selected list of users into a CSV file (also select the fields to be exported.)
- Delete one or more users, groups from a domain
- Define and Update group membership easily
- Add groups and their memberships one at a time, or in bulk
- See a sorted list of groups and Search for groups
- Export groups and their membership data
- Configure password policies, expiry and account lockout features

Advanced management for granular control over entities

- The browser based secure Application Manager enables advanced management which gives granular control in managing the system with extreme flexibility
- Manage class of services, define roles, define mail policies and password policies, provide access control, ability to export entity details etc.
- Switch to the advanced command line interface to manipulate properties of entities in bulk, configure server properties, manage services and operating system level configurations.

Secure role based Administration Console

- Define administrator roles to have a limited view of the system, once they log into the administration console. This allows you to define levels of administration like super administrator with all rights, a junior administrator who can only add users and reset passwords, etc.
- These roles apply even to operations performed from the command line, allowing you to provide secured and audited command line access to the administrator.

Manage the server operations

- Using the advanced command line interface and the dense knowledge base, the super administrator has access to configuring the server properties (timeouts, thresholds, global block rules, etc), start/stop/restart services, tune the services and components, power off and power on the server, manage mail queues, storage, perform backups, etc. Each activity is tracked in logs for audits and review if required.

Provisioning and Managing Domains, Users and Groups

- Using the Application Manager interface, the administrator can provision domains, users, groups and also configure their properties.
- The provisioning can be done in bulk (typically done during migrations) from the command line.
- The Application Manager interface offers two perspectives of the entities, viz. the Entity view to see all the properties of a single entity and the Application view, which gives a spreadsheet like interface to see related properties for multiple users.
- The interchangeable use of these two interfaces and the granular attribute control allows the administrator tremendous flexibility when configuring the properties of the entities.
- Export user, group, COS and domain details from the Admin Console.
- Intuitive interface to define group membership while adding users/groups, View the list of groups the user/group belongs to, Export the list of group members, Import a list of group members

Class of Service (COS)

- To manage large sets of users, typically organizations group the users into types/classes like managers, sales team, HR team, etc and assign properties like quota, mail policies, access rights etc to the sets so that each user in the set receives the same properties.
- This makes the provisioning very easy, since a newly added user is simply attached to the

appropriate classs to inherit the properties of that class/type. Connect Xf provides an easy way to manage classes of users by providing a Class of Service (COS) entity, which is an easy way to specify the default behavior for a set of users. The administrator creates COSes as per the required types/classes in the organization and classifies each user with the relevant COS.

- Migrating users from one department to another or one region to another, is simply a matter of reassigning the relevant COS to the user.
- Changing properties for the entire set/class of users is as simple as changing the properties of the COS, which is automatically inherited by the users belonging to that COS.

Subscription Manager

- The Subscription manager component tracks your purchased user count, and the subscription end date. As you use the system and approach the threshold, the administrative interface throws up alerts to enable you to refresh the subscription certificate by purchasing extra users or renewing the same.

Backup for server recovery

- The administrator can configure scheduled jobs to perform regular backups of the entire configuration data (LDAP, database and configuration files) as a single zip file, which can be stored offline to support a full server rebuild if required.
- The backup operation is capable of copying the backup file to the selected destination or media like a mounted remote drive or tape. Typically these jobs run once a day during off peak hours and capture a snap shot of the system state.

Mail store backup

- This is separate from the configuration data backup and exclusively includes only the mail store. This job compresses and zips the entire mailstore either as a single zip file or individual zip files (per user) and transfers them to the medium of choice.
- Owing to the very nature of the job, where the entire mail data is compressed and zipped using the Linux tar utility, this method of backup is best suited for mail stores smaller than 50 GB.
- For anything larger than 50 GB, Mithi recommends deploying a specialized backup tool, which will support incremental backups and an interface to restore granular parts of the backup (even a single mail).

Automation

- **Automatically sends a Welcome mail to every new user** created on the domain which contains
  - Instructions for new users on how to use the web client Baya for the collaboration applications, update their profiles and other settings.
  - Guidelines to the help wizard where the user can find information on configuring a mobile and desktop clients for application access.
- Automatically clean the unused mailstores of deleted users

Security

The security framework in Connect Xf is built over multiple layers, right from hardening the OS upto the perimeter of the system.

Hardening the core to reduce vulnerabilities

Using best practices for securing the OS, the server is hardened during deployment, to reduce risks that arise from having a larger surface of vulnerability i.e. a server doing more than it is supposed to do. These include but are not limited to turning off/blocking unnecessary services, resources and access points, running a firewall on the server, providing a role based command line access control with audit logs to trace each and every action taken on the server, etc.

Besides this, the Mithi back-end team regularly scans for new found vulnerabilities and publishes customer advisories with patches to mitigate the risks posed by these.

Securing User Access

- **Limiting Access to trusted networks with Access control**

  Administrators can setup policies on each service and for each user or group of users to restrict the use of services from un-trusted networks. The same control allows the administrator to choose, which services should be available to which users, allowing the organization the flexibility to define the use of the services.

- **Secure authentication with strong Password Policies**

  Passwords are the single weakest link to the security of any system. To reduce risks from leaked and weak passwords, Administrators can enforce password policies like minimum password length, password complexity (rules to define the mix of characters in a password like minimum 1 special character, 2 numbers and the rest can be alphabets), password expiry

(forcing a password change at the end of a defined period) for users and groups of users and password history to prevent users from reusing the same password in a defined period.

- **Keep out intruders with Account lockout**

  Baya can automatically block repeated attempts to login with a wrong password and alert the administrator of the failed attempts.

- **Self help for forgotten passwords**

  Users can help themselves to reset their password securely.

- **Use Authorization to limit use of services and features for different users**

  Typically it is not needed to provide all services/features to all users. It's generally a good practice to segregate users into their classes of use and limit their access only to the relevant services/features. This approach is akin to hardening at the Application layer to further reduce risk from exposing unnecessary services and also helps to optimize server resource utilization.

- **Eliminate risk of sniffing and tapping by Encrypting the client-server communication**

  The POP, IMAP, SMTP, XMPP and HTTP services are setup with TLS/SSL (Transport level security) **by default** to secure the channel of communication between the client (mobile, desktop or Baya (web)) and the server, thus eliminating the risk of anybody snooping in on the conversation and stealing information.

- **Reduce risk of scripting attacks with Mail Sanitization**

  The Administrator can enable strict HTML mail sanitization to prevent cross scripting attacks by removing code in email, which may redirect users to rogue sites.

Securing Mail flow

- **Encrypt server to server communication to eliminate risk of snooping**

  The MTAs are equipped to transport mail over TLS to encrypt the mail data in transit, thus reducing risk of data theft by wire sniffing.

- **Control Mail traffic, Information theft and Resource overuse with extensive and granular Mail Flow Policies**

  It has been observed that a lot of security threats come from an unharnessed mail system, which allows all and sundry to send any kind of mail to anybody (internal or external). It is a good practice to establish a corporate mail policy framework, which prescribes for each user and group of users, what type of mail they can send, and to whom. Connect Xf is equipped with a strong mail policy framework, that allows the administrator to encode such corporate policies and control the mail flow.

The policies can be defined based on parameters such as sender, recipient, mail size, subject, contents, and attachments and can be used to control mail flow to/from users, and to distribution lists, e.g. the "testing team" can send mail ONLY to the internal users and the mail should be without any kind of attachments, ONLY the management team can send mail to the "everyone" distribution list, etc.

The solution provides an easy and intuitive way to define the policies for each entity:

Allow universe and deny few (exceptions) or deny universe and allow few (exceptions).

- **Detect and Control internal spam/DOS attacks**

  Typically when client PCs get infected with certain types of viruses, they become spam generation agents. The virus hijacks the desktop mail client (typically MS Outlook) and pumps large volumes of mail to the configured outbound SMTP server using the authentication information remembered in the mail client. All this typically happens without the user's knowledge.

  To reduce impact of such attacks from within the network, the administrator can configure IP rate control to enable auto blocking of client IPs if they cross their allowed number of connections in a day and the administrator can also configure email id rate control to disable users automatically if they cross their threshold of sending mail in a day.

  While it is doing the above automatically, the system also continually scans for any threshold overflows in normal usage patterns and sends out early warning alerts to the administrator if any anomaly is observed.

- **Disable automatic mail forwarding**

  Users may or may not be allowed to configure an auto-forward option for all inbound mail to their mailbox. This can be configured granularly for a set of users, or the entire domain. Controlling this can go a long way in preventing data theft.

- **Disable masquerading with domain and email id Spoof check**

  In a normal insecure mail system, it has been observed that once a user authenticates, he can now relay mail with the from id/envelop id as something different from the authentication id, making it appear to the receiver that the mail came from another person. This means that technically one user can send mail on behalf of another (masquerade).

  To prevent this, Connect Xf is equipped with 2 types of spoof check viz. domain spoof check which ensures that mail originating from a trusted IP address (typically a branch email server or a mail gateway server) can only be from amongst a trusted list of domains, and second, email id spoof check to ensure that the from id in the envelop, the from id in the message (mime) construct and the authentication id must all match for the mail to be accepted for relaying.

- **Automatically isolate Virus infected mail**

  The product has a built-in Anti-virus tool, to ensure that all mail traffic flowing through the servers is checked for virus. Infected mail are automatically quarantined to prevent spread of the virus through the system, and an alert is sent out to the recipient. The administrator can view the quarantine folder to review the filtered mail.

  Automatic and Periodic signature updates for the virus detection tool, ensure that the tool is

aware of the latest threats, almost as they happen.

- **Automatically detect and mark Spam mail**

  The Connect Xf Server incorporates reputation and content based technologies to detect, control and mark spam on incoming channels, giving more than 98% spam detection accuracy. The reputation based technologies in play are Greylist, RBL, reverse PTR checks, return MX checks, Blacklists & Whitelists, etc.

  The content based scanning is implemented using Spam Assassin, an open source spam detection tool, which scans the contents of the mail for objectionable words and known patterns matched to spam signature databases and marks the mail as spam. The marked mail are automatically filtered into the spam folder of each user for their review.

- **Easy Spam Management**

  The end users can manage their own spam by analyzing a digest (report) of spam sent to them daily or by browsing the spam folder where the mail marked as spam are deposited. This they can do from any client (web or desktop).

  The report and the Baya interface allows the user to release a mail falsely marked as spam (false positive), Whitelist a sender such that in future mail from that sender will not be scanned for spam, blacklist a sender to block all further mail from that sender, or mark a mail as spam (false negative).

- **Mail Archival for Compliance and Recovery**

  Personal archival for securing a user's mail to retrieve on demand

  Connect Xf allows you to configure archival for a select set of users, where a copy of every mail sent and received is deposited into a parallel read only mailbox for that user. This can be used to retrieve the entire mailbox for the user on demand or only seek out a few specific mail and forward them to the original account. The system can configure the retention period for mail in each of these personal archive accounts.

- **Compliance archival: Retain, Search, Comply**

  Keeping in line with government regulations and compliance policies, most enterprises are required to retain a copy of all mails sent and received for a defined period. With the Compliance Mail Archival feature, retaining, storing and searching for a copy of mails exchanged by users or a set of users becomes very easy.

  The mails are stored in a compressed and encrypted format, which only the Administrators can access through the web based interface. They are stored and indexed on a separate partition of the server for the defined period and can be retrieved quickly for audit purpose.

Secure Administration

- **Multi-level administration with Role based access**

  The administration console via the GUI is secured with role based access to allow multiple levels of administration (concept of least privileges). Using the roles, the super administrator can define granular control over entities, fields/attributes of entities and operations. The same

roles apply for operations done via the command line.

- **Trace changes with Activity Logging**

  The system maintains audit trails for each operation done by the administrators, and a trace of all the transactions and configurations done by the end users.

Storage

Manage Account Storage using Quota and Quota policies

- ***Integration with Expandable or Elastic Cloud Storage***

  System administrator can deploy the mailstore of a server on the AWS S3 service. This improves the availability of the storage.

- **Automatically manage mailbox size with Quota**

  The administrator can limit the storage available per user or set of users, which helps the organization manage the available storage resources. As the users approach their allocated thresholds for storage of mail data, the system sends them alerts to prompt them to clean their mailbox. The system allows the administrator to define multiple threshold points, where alerts can be sent to users.

- **Flexible Quota overflow policy**

  If a user's mailbox usage crosses the allocated quota, the administrator can configure the system to disallow the user from Sending mail (Block Sending) or reject mail being delivered to the user's mail box (Block receiving)

- **Time based Quota**

  The administrator can configure the system to automatically delete mail of selected users based on retention period (E.g. For a specified user, retain mail only for the last 3 months)

- **Monitor Mailbox usage with reports**

  The system can be configured to send mailbox usage reports to the administrator for monitoring the use and taking corrective action if necessary.

- **Optimize Storage use with SISA (Single Instance Attachment Storage)**

  Define user level policies to automatically strip attachments larger than a defined threshold from the mail, store them in a central repository and send hyperlinks instead. For mail sent to multiple users, this results in immense savings on storage, since only a single copy of the attachments are stored. The policies are flexible and can be applied per user for inbound and local mail.

Reports

Reports available to the Users

- **Mail marked as virus (quarantined)**

  The built in virus detection engine, automatically quarantines a mail if it contains a known virus and sends an alert to the end user (recipient) about this event. If the sender is a known contact, the user can alert the sender to resend the cleaned mail.

- **Users manage their own spam with a daily digest/report of all the Spam received by them.**

  The users get a daily digest of all the spam they have received and which was detected, marked and moved to their "spam" folder. Via the report, the user is presented options to release the mail (in case it is a false positive) and whitelist the sender (so that in future mails from this user will not be scanned for viruses)(**)

  The report frequency is configurable by the end users themselves via their application manager consoles from Baya.

  (**) This is applicable for setups that use the Spam protection and management engine of Connect Xf.

- **Non delivery report (bounce alert)**

  If a user sends a mail, which cannot be delivered for any reason, the user would receive a bounce alert or a mail non-delivery report, which will indicate the reason for the bounce. Based on that report and in consultation with the administrator of the system, the user can take corrective action before resending the mail.

Reports for the Administrator

- **User Activity Reports**

  Connect Xf has incorporated more than 25 types of reports to assist the administrator to understand and act on user activity patterns. Some of the available reports help to answer queries like:

  1. How many users are actively using the collaboration platform?
  2. Conversely, how many people are not using the collaboration platform at all?
  3. Which users are using which services on the platform (like how many and which users are using POP, IMAP etc)?
  4. When did each user last login to the system on each of the protocols (along with full history of all logins)?

- **Mail Traffic reports**

  Learn about the top users of your collaboration platform with the statistics reports on mail usage across the Users and Domain. Some of the available reports help to answer queries like:

  1. Top senders (local and external) by number of mail sent, size of mail sent, number of recipients in each mail etc.
  2. Top recipients (local and external), by number of mail received, size of mail received, etc
  3. User mail flow statistics, to understand the total number and total size of all the unique mail sent and received by the user.

4. Number of mail archived and the volume size of the archival store.

- **Server Statistics Reports**

  Keep a tab on the health of your collaboration setup by reviewing some key information like:

  1. What is the status of the Backup jobs?
  2. What is the data replication status between multiple servers in an enterprise?
  3. What is the status on the resource utilization of the servers in terms of CPU, memory, disk, server load?

System Performance

Performance

Connect Xf has been designed to deliver more performance for the same resource utilization, when compared to traditional systems.

Our engineers worked hard to design a system, which delivers more performance and scale for the same resource utilization, when compared to any other collaboration system. Our product incorporates our vision of being able to do more with less

Adaptive Mail routing

Speed of mail delivery is crucial for effective collaboration. To ensure that there are no bottlenecks within the system, the Connect Xf engineers designed multiple ways to route mail such that each mail has the shortest path to the destination, being extremely stingy with hops.

In addition it is easily possible to configure parallel paths for mail flow by adding queues to ensure that the queues never pile up due to a problem with one of the recipient system. With the introduction of such innovative features over the OSS MTAs, we were able to get more than a 300% jump in mail delivery times with a high level of consistency.

Learn more about the Adaptive Mail Routing features.

SISA (Single Instance Storage of Attachments)

Besides the server capacity, one of the biggest enemies of high performance is choking within the network leading upto the server or in the last mile to the client. The network capacities can be easily consumed when large mail are transported between servers or downloaded by clients.

We realized that one big problem causing the network bottle-necking was mail with large attachments sent to multiple people (groups or distribution lists) within the network, and then each client downloading these large mail to their clients. By stripping mail of large attachments and storing them at a central place, we observed a reduction in 60 % on the network utilisation. Not to mention the savings in storage due to retaining only one copy of the original large mail (Application level DE-

duplication).

To enhance performance for large sets of users having a large mail flow (10,000+ users) the attachments are stored in sub folders which saves time in saving or reading attachment from the folders as the size of each folder is small.

Aggressive Caching

The Connect Xf engineers identified another point, where even excessive use of high performance components like LDAP and Database (which have inbuilt caches) can degrade performance substantially. While letting the application developers have the flexibility to write code as they want, they built in a strong caching layer in between, which holds frequently accessed data from different parts of the system in the memory which reduces the calls to the database, LDAP and mail store.

Enhanced end user usability leading to higher system performance

Right from bringing out frequently used applications and options in easily usable interface options, to intelligently searching only the minimum data to get the required results, to painstakingly designing the system to reduce clicks or eliminate them during any user operation, Baya, the collaboration web client within Connect Xf, has been specifically designed to reduce the operating path for the users, to allow them to access and view information with minimal clicks. This in turn has an impact on server performance since the server now has so much less to do.

Scale only on demand and do it with ease

The Simple High Availability architecture and the ability to setup distributed site servers, makes it very easy to scale the system on demand. As you grow vertically (more users at one site), you can simply add or consolidate servers within the server farm to achieve more capacity and as you grow horizontally (more sites), you can easily add servers the enterprise tree to allow users to be located remotely.

Minimize data movement across servers

Connect Xf has been designed to optimize the movement of data across enterprise servers to reduce delays in data replication and also to optimize server and network performance. The simple philosophy is that if you need it frequently replicate it else access from where it is, e.g. your mailbox is never replicated across distributed site servers or even on the server farm at a single site, thus if you temporarily access your mailbox from any site (other than your own), the system will connect remotely and show you the mailbox.

Monitoring out of Tune components

Typically during deployment the system is tuned to the specified work load. However as the system is used over time, the work load may vary (up or down) and it may be necessary re-tune some of the components and sub-systems to work optimally with the new loading patterns. You don't have to worry about this since the system automatically monitors the usage and sends alerts when a re-tuning is required.

Nip DOS attacks and system overuse in the bud

Connect Xf allows you to define system usage policies like mail flow controls, system access controls, availability of specific features to user sets, etc to ensure that users only consume resources commensurate to what has been allowed to them. In addition, Connect Xf has strong attack detection, mitigation and prevention features to keep the server resources from being locked up dealing with a DOS attack.

Faster user access and optimized IO

With the dovecot-director service integrated in Connect Xf, a system architect has the option to have a separate Front end and a separate mail box server. Also when migrating users from Courier & Qmail IMAP and POP servers to the Dovecot IMAP and POP servers, administrators have the control to migrate a user or domain at a time using the Proxy server. An IMAP & POP servers from Dovecot results in faster user access and optimized IO.

Integration

Connect Xf was designed to work on open and standard protocols and store data in standard well understood formats such as Maildir for mail data, LDAP for directory information, etc. to support easy integration with external backup solutions, external security gateways, varied mobile devices, desktop clients, etc.

Connect Xf can be deployed on Bare metal or Virtualized environments with ease, thus giving you the option to choose the most cost effective environment for your requirement.

Support for bi-directional connectors with other business applications

Connect Xf exposes web services and standard secure services to allow business applications like portals, HRMS, ERP, CRMs to use the services of the collaboration solution. Common uses include accessing the directory of users over LDAP, treating the LDAP directory on Connect Xf as a central directory, using the email interface to dispatch alerts to users, providing a single sign on for the collaboration applications to the users of the corporate portal via an authentication connector and so on.

Co-exist with other mailing systems to create a hybrid solution

Connect Xf can comfortably co-exist with other mailing solutions like MS Exchange, Lotus Notes, etc to allow user mailboxes to be divided across the two systems, while maintaining the same domain name, synchronized address books and replication of relevant properties to create a powerful option for cost saving without any compromise for special users on the system. The co-existence comes in the form of a single point authentication to maintain a common password, seamless mail flow connectors and processes to maintain the address books in sync.

Open directory to support easy integration and distributed setups

Having an open standard directory based on LDAP (integrated LDAP directory holds the domain, user, group and contact information), allows flexible multi-server configurations within a single site or across distributed sites. This means that when more than one Connect Xf Server is deployed as a part of the solution architecture, the directory content has to be same across all the servers. This can be easily achieved by creating a single directory server such that all other servers use the LDAP service on it or setting the systems in a Master-Slave farm to have the directory replicated across all slaves. This flexibility allows the solution designers the flexibility to define different topologies to best meet the requirements and available infrastructure.

External applications can also refer to the Connect Xf for accessing the entity information and for authentication to maintain a single password.

Integrating with External directories like MS ADS, RHDS, etc

Typically most organizations have a central directory, which lists all the corporate resources and their properties, that includes the users' authentication credentials. Connect Xf can be configured to have all its services directly authenticate with this central directory over LDAP (single password the collaboration Apps as well).

In addition, the external directory connector on Connect Xf can also periodically sync selected user

attributes such as user personal information from the external central directory to be made available to the collaboration applications.

Secure Attachment Vault

The capability allows you to capture all inbound and outbound attachments into a central secure reliable storage (accessible via FTP) as an Asset repository. This frees up the user to freely create and exchange the documents, without worrying about securing them someplace.

Read more about Saving Costs, Securing Critical Information Assets using the new Attachment Vault

Integration with Expandable or Elastic Cloud Storage

A system administrator can now deploy the mailstore of a server on the AWS S3 service. This improves the availability of the storage.

Integration with AWS Elastic Search and Kibana service

An admin can now configure central logging using the newly integrated logstash service. Integration with AWS Elastic Search and Kibana service will allow the local support team to revert quickly on requests to trace mail.

Availability

Mithi understands the market need for cost effective no compromise solutions and hence the Mithi engineers designed multiple options for availability to suite various budgets. Using any of these options makes the system extremely reliable, only varying the uptime.

Automatic remote backups for mail store and system data

A daily backup to a remote device/storage is the most important activity for the system to ensure a reliable setup. Connect Xf has built in tools to perform automatic backups of the configuration and system data to enable a server rebuild if required. Multiple such backup jobs can be scheduled during the day to take a system dump onto a defined media (tape, external storage or remote machine).

Connect Xf also has built in tools for backups of the mail data, which can be scheduled to take backups of the mail store of all or selected users onto the defined media.

For incremental backups and more refined control over the mail store backup and restore process, Mithi recommends using a dedicated third party backup tool for the mail store. Since the mail is stored in a regular files and folder structure, most popular backups tools working on Linux, will easily integrate with Connect Xf.

Automated domain migration

Allows system admins to reduce down time when migrating domains from one setup to another and also eliminates human errors.

Fully hosted, Fully Managed Cloud based collaboration setup - 99.9% uptime

Mithi provides a SaaS service (Mithi SkyConnect) based on the Connect Xf platform, which is fully hosted and managed by Mithi at a carrier grade data center. No servers to setup, No team to manage this, Get started in a day - simply connect to our cloud and use the service.

Hybrid setup of a hosted setup (SaaS) and an In-premise gateway server - 99.3% uptime

Most organizations don't have the carrier grade infrastructure to host a mail landing point in premise, due to the high availability demands from MX handling servers. This solution provides the flexibility for these type of organizations to have a highly available SaaS setup for the entry and exit point for all inbound and outbound mail, while giving them a local mail server in-premise to optimally handle local mail traffic. This saves on Internet bandwidth since only clean mail land on the in-premise mail server and all user access to their mailboxes is via the local network (bypassing the Internet link)

Additionally the cloud infrastructure retains a copy of the inbound mail in each user's mailbox for a period of 7 days, making this a functional DR (Disaster recovery) site in case the primary site or server is unavailable.

In-premise Connect Xf servers in Active-Passive mode with auto failover - 99.9% uptime

A Hot standby server can be configured for the mail server to ensure minimum downtime in case of a primary server failure. The system and mail store data on the Hot Standby server is automatically synchronized with the primary server, continuously. Real time synchronization of mail store and the system data ensures that there is no loss of data in case of a switch over to the secondary server.

In-premise Load balanced Connect Xf servers in Active-Active mode for extreme highly availability- 99.95% uptime

A cluster of Connect Xf Servers can be set-up in an Active-Active mode for easy scalability, hands free high availability and minimal performance degradation during peak loads. The server farm is load

balanced to ensure that there is zero downtime in case of any component failure.