MindLink

MindLink Mobile

Technical Overview

Version 3.11

Table of Contents

1 Overview

MindLink Mobile enables MindLink functionality – including Microsoft Skype for Business Instant Messaging ("IM") Presence and Persistent Chat ("PChat") – on a range of cross-platform mobile devices, and inside a number of Mobile Application Management ("MAM") containers.

1.1 Mobile Platform Support

MindLink Mobile clients are available for the following devices:

- Android – phone and tablet
- Apple iOS – iPad and iPhone
- BlackBerry 10 – inside BES work perimeter

The application is offered in a version that runs natively and unmanaged on each of the above devices – referred to in this documentation as the "vanilla" version of the application.

In addition, versions of the application are offered that run inside the following MAM containers:

- Good Dynamics – iOS only
- SECTOR-based enterprise workspaces – iOS, Android
    - BlackBerry Secure Workspace
    - AT&T Toggle
    - Deustche Telekon SAMBA!
- MobileIron – iOS only
- Citrix Worx – iOS only

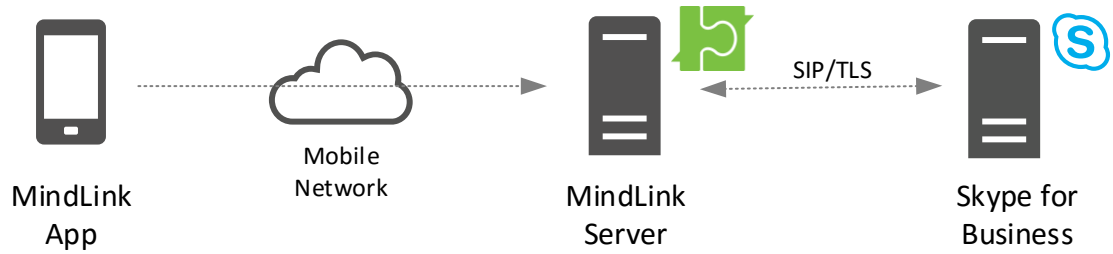
All versions of the application follow the same core architecture and offer the same set of features, unless otherwise indicated.

This document describes this core architecture and highlights differences for each mobile OS and MAM container where appropriate. For brevity, we will discuss the BlackBerry Secure Workspace implementation of the SECTOR secure workspace platform only.

1.2 High-level Architecture

To enable connectivity to the on-premise Skype for Business components, an organization must deploy the MindLink Mobile server within their internal IT infrastructure.

A single MindLink Server can serve clients connecting from all supported device platforms.



The MindLink Mobile server performs the following responsibilities:

- Hosts the MindLink Foundation, which coordinates the core MindLink functionality and communicates with Microsoft Skype for Business as the underlying backend.
- Handles connections from mobile clients.

- Maintains session state across mobile network disconnections and acts as an intelligent buffer for updates to be sent to clients.
- Sends push notifications to mobile devices.

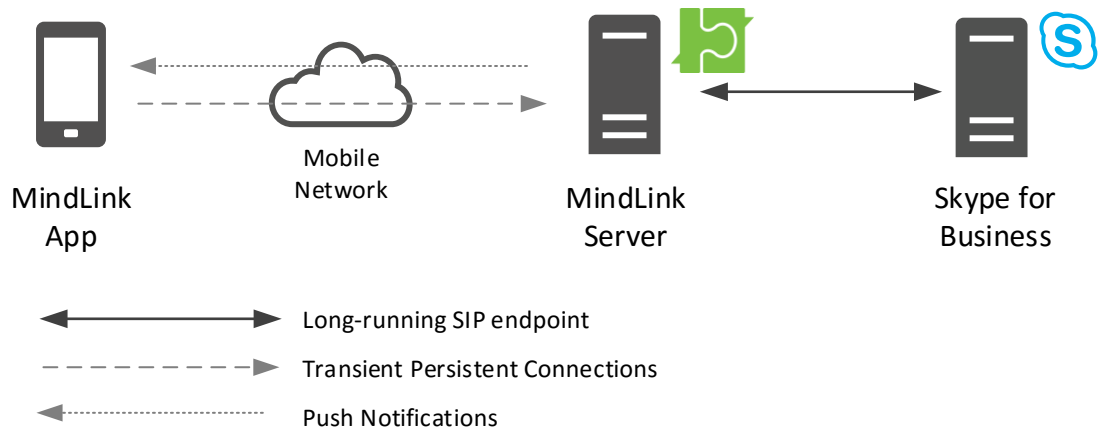
The MindLink Mobile server is a .NET application that runs as a Windows Service. The host Windows Server machine can be virtualized. The server component is installed by running a standalone .MSI executable and then using a graphical management utility application to configure the system.

The MindLink Mobile server exposes a number of performance counters with which to monitor its load and network traffic.

2 Application Lifecycle

MindLink provides the user with an always-on mobile Skype for Business endpoint. The MindLink Server maintains the Skype for Business endpoint on behalf of the user, even when the user is not actively using the client application. This allows the user to receive push notifications of new messages when not using the application.

When the user is actively using the application, the application establishes a two-way connection with the server and receives updates of new messages immediately.



2.1 Configuration Bootstrapping

When the application starts up without a pre-existing session, it makes a one-time HTTP call to the MindLink server web address. The user is prompted to enter this server address upon opening the app for the first time, and is able to change the address between sessions.

The MindLink server responds with basic configuration about how further connectivity will be managed, and the capabilities enabled by the administrator. Having received this configuration, the app displays the log on screen.

2.2 Logging On

The logging on process happens once at the start of the MindLink session. Since MindLink sessions are long-running and persist across application or device restarts, this process happens relatively infrequently.

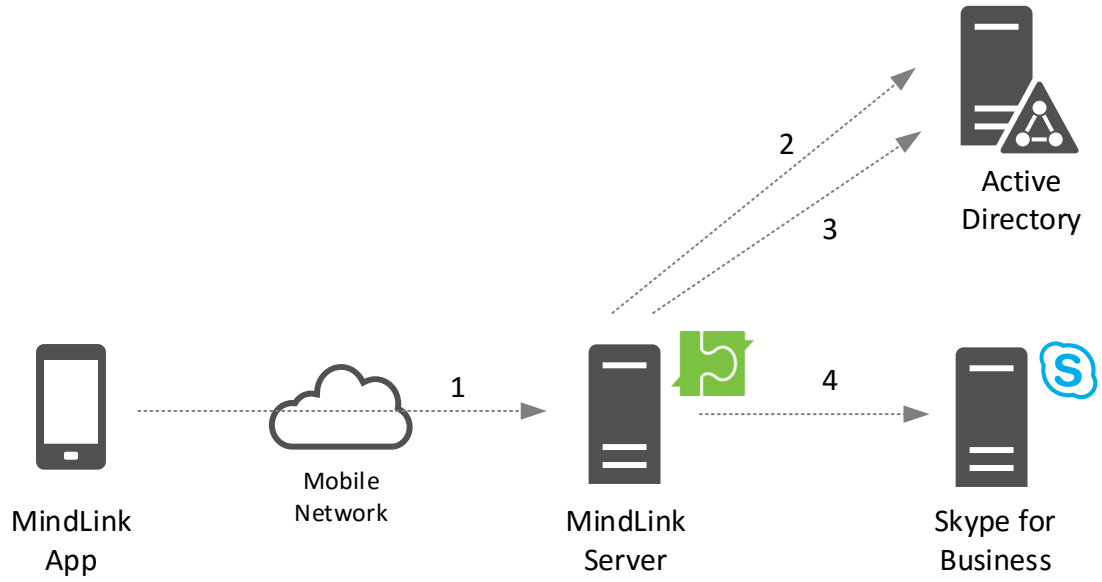
Once logged on, the client application is issued by the server with a one-time token which it subsequently uses to re-establish the session when required.

To log on, a user must manually enter their Active Directory credentials – the account name (in down-level or UPN format), and the password. Explicit UPNs with UPN suffixes are supported for accounts in the same forest as the MindLink Server. The credentials are sent over a secure connection to the MindLink Server.

The entered credentials should correspond to the user's enabled user account. In a "resource" or "central" forest Skype for Business deployment, the credentials of the linked user account should be entered.

The MindLink Server authenticates these credentials with Active Directory by performing a fast bind with an LDAP server in the user account's domain. Active Directory in the Skype for Business forest is then queried via the Global Catalog to obtain the user's SIP address.

The SIP address is then used to establish the connection with Skype for Business. Since the MindLink Server is trusted by the Skype for Business infrastructure, neither the user name nor password is forwarded to Skype for Business directly.



1) Client sends user name/password to server
2) Server authenticates with fast concurrent bind to Active Directory LDAP server.
3) Server queries for SIP address from Active Directory Global Catalog
4) Server establishes Skype for Business endpoint with SIP address using trusted connection.

2.3 Connection Lifecycle

When a session has been established it continues to persist (including maintaining the connection to Skype for Business) until:

- The user manually logs off.
- The user manually logs on as a different user on the same device, or uninstalls and reinstalls the application.
- The Skype for Business endpoint is disconnected due to an unrecoverable error with the Skype for Business infrastructure.
- The user is disabled on the Skype for Business system.
- The administrator has configured a session expiration interval and the user has not been active on the app for that interval.

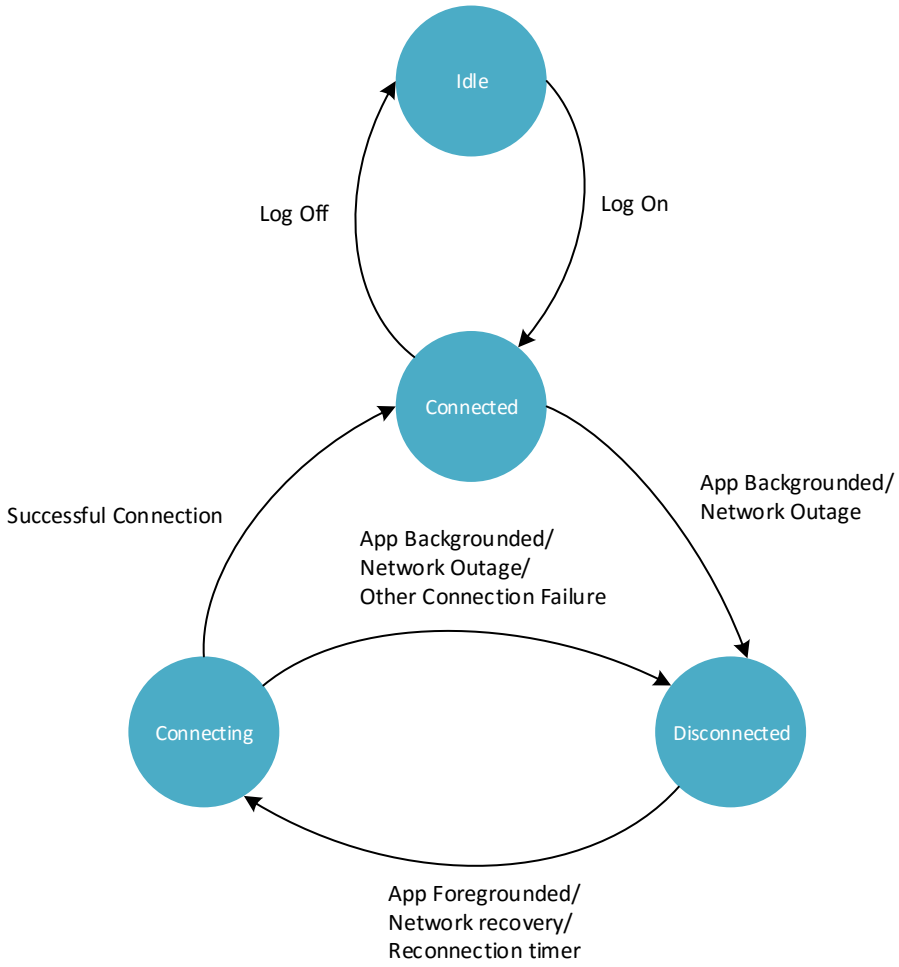
The session is always in one of two modes:

- **Connected to the client via a persistent connection**
  - The application will attempt to establish a two-way "persistent" connection to the server whenever it is in the foreground on the device screen.
  - The application will report itself as "connected" when in this state.

    - The user will be able to interact with the application including changing their profile, loading new messages, searching for content, and changing their presence.
    - The user will receive new messages and updates (e.g. presence state) immediately.
    - The client and server minimize data usage by using a subscription-based "client virtualization" protocol to negotiate only sending the data that is actually required on the device
- **Disconnected from the client**
    - The application will report itself as "disconnected" in this state.
    - The session will transition to this state when in the background on the device, the device is locked, or the application is forcefully "closed" by the user.
    - The client application uses no network data and no CPU time in this state.
    - The user will receive a push notification when a new message in a chat room or IM conversation is received.
    - The MindLink Server acts as buffer to any new messages or updates that are received in this time, ready to send them down to the device when it next reconnects.

Management of this lifecycle is automatic. The client disconnects when put into the background on the device and will immediately reconnect when brought into the foreground. The user will see a "Reconnecting…" message while the client reconnects to the server when the app is opened or brought into the foreground. Disconnection of the client when not in use saves battery and network usage.

The server records the last time that a user was connected. The administrator can define a policy such that sessions that have not been connected for a given amount of time are automatically disconnected.



2.4 Persistent Connectivity

When the client reports itself as connected, it is maintaining a continuous two-way "persistent" connection to the server. This connection allows the device to send and receive real time updates. If the connection is dropped due to bad network connectivity, then automatic reconnection will take place. A connection attempt is made every 1 second with a timeout of 4 seconds.

2.5 Push Connectivity

When the client is not connected – but the server is maintaining the user's session – new messages will be sent to the device as a push notification.

The notification signals to the user that new messages are available and that they should open the MindLink application to fetch and read them. The information sent with the notification is enough to indicate in which conversation new messages are available, but does not contain the full message text.

Notifications are sent via the native push notification infrastructure for the corresponding device OS. On the device, notifications are added to the native OS notification center/hub and may trigger a sound of vibration (depending on the operating system).

The user can configure which types of messages will trigger a notification by setting the notification settings inside the app. In addition, they have the option to completely disable push notifications.

2.6 Stored Data

MindLink Mobile has been designed as a thin, or “stateless” client. This means that the application only holds session state – including message content – in memory, and only while the application is running.

When the application is opened, it connects to the server and downloads the necessary session state fresh from the cached data that the server is holding. This data persists in memory on the device while the application is open (foreground or background) and is purged when the application is closed or the device reboots.

When not running, the application will only store the following data at-rest on the device’s permanent storage:

- One-time session token – Used to reconnect to the long-running server-side session between application or device restarts.
- Log-on user settings – Used to store user preferences as selected on the log-on screen.
- User journey state – Used to store the progress of the user through the tutorial workflow that appears when the application is first used.

Message data is not stored on the device at any time.

3 Skype for Business Integration

MindLink uses Skype for Business as the engine for the core functionality. Messages sent on MindLink can be received by Skype for Business users using any compatible client, and vice versa.

3.1 Supported Versions

MindLink requires an on-premise Skype for Business Server deployment. Hybrid and Skype for Business Online deployments are not supported.

In addition, Group Chat (prior to Lync 2013) or Persistent Chat servers must be deployed within the topology. For Lync 2013 and later, users who need to log in to MindLink must be enabled for Persistent Chat via the Persistent Chat Policy.

The following versions of Skype for Business Server are supported:

- Microsoft Office Communications Server 2007 R2 – with Group Chat servers deployed.
- Microsoft Lync 2010 – with Group Chat servers deployed.
- Microsoft Lync 2013 – with Persistent Chat deployed and users enabled for Persistent Chat.
- Microsoft Skype for Business Server 2015 – with Persistent Chat deployed and users enabled for Persistent Chat.

A mixed version topology is also supported – for instance using a Lync 2010 Group Chat server in a Skype for Business 2015 topology.

3.2 Connectivity

The MindLink Server connects to the Skype for Business infrastructure via SIP as a trusted application.

The trusted connection allows the Skype for Business infrastructure to treat the MindLink Server as an equal peer and enables efficient routing of SIP traffic to and from the MindLink Server. The establishment of this trust requires that the Skype for Business servers be able to resolve the DNS name of the MindLink Server.

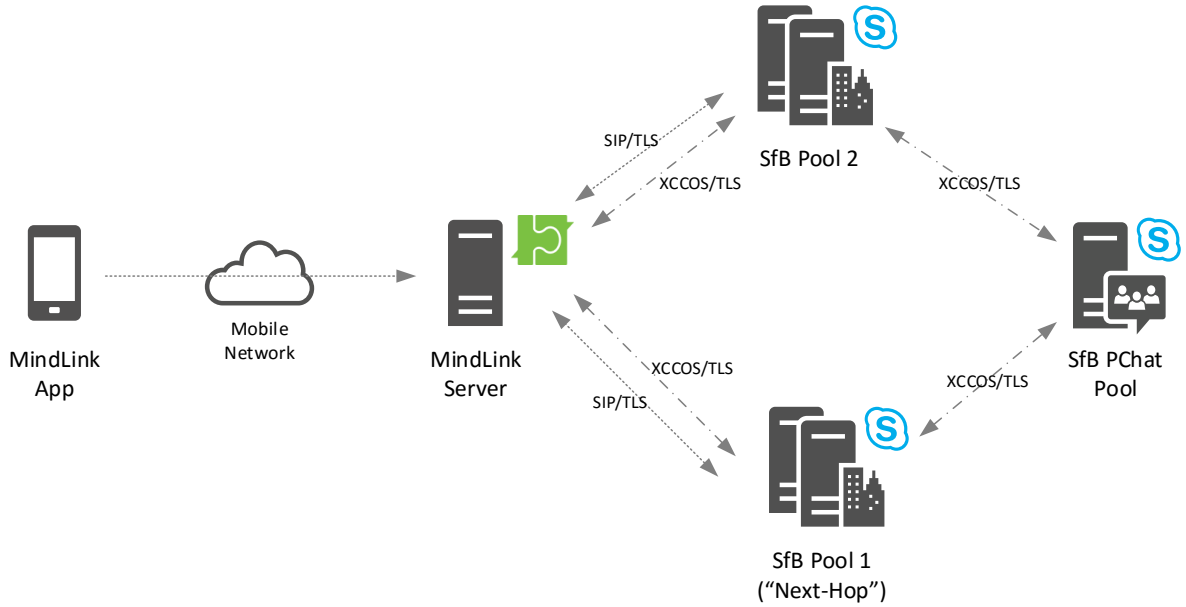
Configuration of this involves:

- Creating a trusted application pool containing the MindLink Windows host machine in the Skype for Business Topology.
- Adding MindLink as a trusted application on the pool.
- Creating and assigning a certificate to the MindLink Server to establish trust with the Skype for Business servers.

A Skype for Business trusted application – in this case, the MindLink Server – must be configured with a “next-hop” Frontend pool. This is the Skype for Business frontend pool to which any initial connection will be made.

A MindLink user may be homed on any frontend pool in the Skype for Business infrastructure – the MindLink Server will subsequently connect directly to the necessary home pool to register each user. As such, a single MindLink Server may serve any Skype for Business user in the topology, subject to

scale and geolocation decisions. It is generally recommended that the MindLink Server be located as physically close to the end users as possible.



However, a single MindLink installation can only support one Persistent Chat pool. If there are multiple Persistent Chat pools, multiple MindLink Servers must be deployed.

3.3 Compliance

The MindLink Server acts a stateless proxy between the MindLink client and the Skype for Business infrastructure - no additional message data is stored in the MindLink infrastructure.

Any message sent via MindLink is routed through the Skype for Business system – even IM messages sent between two users both on the MindLink client. As such, all messages sent to or from MindLink will be captured by the Skype for Business IM and PChat compliance engines, or third-party products that filter frontend traffic.

3.4 User Profile

A user configures their MindLink client with a set of chat rooms to be permanently joined to, and a "contact list" of users that they wish to see the presence of and may want to message frequently.

These lists are separate to the joined chat rooms and contact list of the desktop Skype for Business client. Typically a user will only require updates from only the most important chat rooms when mobile, and will only need to communicate with a subset of users. Maintaining a separate "mobile" user profile allows the user to filter the information they actually require when away from the desktop.

The MindLink client allows a user to see their desktop chat rooms and contacts and pull items from these lists to configure their mobile profile.

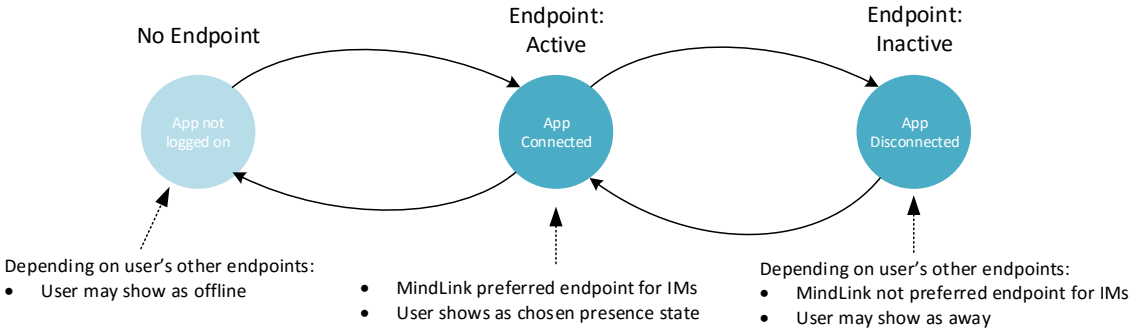
3.5 Lifecycle

A user may choose to use MindLink for Persistent Chat and IM communication, or only Persistent Chat communication. In addition, IM communication can be disabled for all MindLink users by the administrator.

When using MindLink with IM enabled, MindLink automatically participates in the Skype for Business multiple-points-of-presence (MPOP) system to ensure that IM messages are delivered to the most appropriate endpoint.

When the user opens the application, the application will report the user as active on the MindLink endpoint to the Skype for Business presence engine. When the user backgrounds the application or the application gets disconnected for any other reason, the MindLink Server reports the user as inactive on the MindLink endpoint to the Skype for Business presence engine.

The aggregation system inside the Skype for Business presence engine uses this information to intelligently update the user's presence state and to rank the user's available endpoints in preference order for consumption of incoming IM messages.



When IM is not enabled, the MindLink endpoint does not publish presence information to the Skype for Business presence system and hence has no effect on the user's presence state.

3.6 Active Directory

MindLink supports Skype for Business deployments in single or multi (resource or central) forest topologies.

The MindLink Server must have read access to Active Directory via the Global Catalog or LDAP server such that it can look-up users' Skype for Business SIP addresses in the Skype for Business forest.

In addition, the MindLink Server must be able to connect to an LDAP server in each of the authentication forests to pre-authenticate users using a fast-concurrent LDAP bind. This requires that auto-discovery of Active Directory infrastructure via DNS is working correctly.

3.7 User Access

A user must be enabled on Skype for Business to log on to MindLink. Conversely, disabling a user on Skype for Business will disable them on MindLink, including terminating any active MindLink sessions.

There are no additional provisioning steps required to allow a user access to MindLink. However, user access to MindLink can be restricted to a subset of Skype for Business users by assigning MindLink users to an Active Directory group.

4 iOS

MindLink Mobile for iOS is a universal application that supports iPhone, iPod Touch and iPad devices.

It is also available in flavours that integrate with the following MAM containers:

- MindLink for Good (Good Dynamics)
- MindLink for SECTOR (SECTOR-based workspaces e.g. BlackBerry Secure Workspace)
- MindLink for MobileIron
- MindLink for Citrix Worx

4.1 Persistent Connectivity

The application connects by making a TLS connection and an HTTP connection on two different ports to the MindLink Server.

These connections must be routed from the external mobile network to the MindLink Server, which must be installed on the internal network. The application has been designed to be agnostic as to how this routing occurs so that organisations can leverage their existing network infrastructure.

Various strategies are available:

- Direct connection through external firewall – the organisation opens the external firewall so that devices on the external firewall can connect directly to the MindLink Server
- Proxied connection via a network security gateway – the organisation routes the connection via a security gateway deployed in the DMZ. E.g. using a F5 Big-IP or Citrix NetScaler.
- VPN connection – the connection is tunnelled via a VPN appliance to the internal network. The MindLink client supports iOS manual VPN, VPN on-demand, and per-app VPN.

4.1.1 MindLink for Good

The MindLink for Good application connects to the server using the Good Dynamics infrastructure. The connection is tunnelled securely via the Good Network Operations Center and Good Proxy server directly to the MindLink Server on the internal network.

4.1.2 MindLink for SECTOR

The MindLink for SECTOR application connects to the server using the secure workspace connection. For BlackBerry Secure Workspace, the connection is tunnelled via the BlackBerry Enterprise Server's secure BCP connection directly to the MindLink Server on the internal network.

4.1.3 MindLink for MobileIron

The MindLink for MobileIron application can be configured to use the integrated the MobileIron AppTunnel proxy. In this configuration, "persistent" connections are made over HTTP. The application will issue continuous "pending-GET" HTTP requests to the server to simulate a two-way connection. The use of HTTP is required due to limitations in the MobileIron AppTunnel/Proxy platform.

Alternatively the MobileIron Tunnel per-app VPN client may be used to proxy all traffic, which leverages the same MobileIron Sentry and Core components as the AppTunnel system.

4.1.4 MindLink for Citrix Worx

The MindLink for Citrix application may leverage the Worx implicit VPN, provided by a NetScaler appliance associated with the XenMobile instance.

4.2 Push Connectivity

Push notifications are sent to the device using the Apple Push Notification Service (APNs).

The MindLink Server connects to the APNs infrastructure by making an outbound TLS connection. The ability to make this connection is a pre-requisite for starting the server. The connection is a TLS connection and hence cannot be made using a standard HTTP proxy.

The connection to the APNs service is secured using a certificate that the server must present to APNs to identify itself. This certificate will be provided by MindLink as part of the installation delivery, and must be updated every year.

On launching the app for the first time, the user is prompted to accept whether push notifications can be sent by the application. The user can configure how notifications should be shown on the device using the standard iOS notification settings system in the iOS Settings application.

Push notifications are sent according to the standard APNs Quality of Service implementation. If a push notification is sent when a device is out of coverage, then the push notification will be stored and delivered when the device is back in coverage. Only the latest push notification will be stored for delivery, however.

4.3 Storage

The MindLink app stores very little information in the at-rest device storage.

The following data is classed as “sensitive”:

- The one-time session token, used to reconnect to the current session.
- The user’s user name, if the “remember me” checkbox was checked when logging on.

The above data is stored encrypted in the device keychain using keys only known to the MindLink application. This is enforced by the iOS security model.

All other data, which tracks the non-sensitive state of the application, is stored in the application’s sandbox storage area.

4.3.1 MindLink for Good

All data is stored securely in the Good Dynamics storage container.

4.3.2 MindLink for SECTOR

All data is stored securely in the SECTOR storage container.

4.3.3 MindLink for MobileIron

All sensitive data is stored in a file that is encrypted using the MobileIron secure storage system.

4.3.4 MindLink for Citrix Worx

All sensitive data is stored securely encrypted by the Citrix Worx container.

4.4 Access Rights

On start-up, the application will ask the user whether it should be allowed to send push notifications. This permission is enforced by the iOS app security model. The user will still be able to log in and use MindLink regardless of whether push notifications are enabled or disabled.

When the app is installed, it asks the operating system for permission to use the device keychain to store secure values. iOS sandboxes this access to an area that can only be used by that particular app.

The app does not access any personal information stored on the device – the iOS security model enforces that this is the case.

4.5 File Download

Files sent in chat rooms can be downloaded by the user to the device. The app farms the actual downloading process off to Safari, from where the file can be opened.

4.5.1 MindLink for Good

The download is farmed off to the Good Access browser, if installed. Otherwise the download will be farmed off to Safari.

4.5.2 MindLink for SECTOR

The download is farmed off to a SECTOR-enabled browser e.g. the BlackBerry Workspace Browser, if installed. Otherwise the download will be farmed off to Safari.

4.5.3 MindLink for MobileIron

The download is farmed off to the MobileIron Web@Work browser, if installed. Otherwise the download will be farmed off to Safari.

4.5.4 MindLink for Citrix Worx

The download is processed according to the URL rules configured by the XenMobile App Policy. This includes the ability to farm the download off to the Worx Web browser.

4.6 Data-Loss Prevention

In addition to the data-loss prevention mechanisms described elsewhere, the application does not allow copy/paste of message data outside of the application.

4.7 Deployment

The application is deployed to the user's device as a publically distributed app from the iTunes store.

An enterprise-app store system may be used to advertise the availability of the application to the user, but the actual delivery of the app binary is from iTunes.

4.7.1 MindLink for Good

The application must be assigned to the user via the Good Control console, and the user must be provisioned with an activation key. The MindLink application definition is made available to the Good Control instance as a Partner app via the Good Marketplace.

4.7.2 MindLink for SECTOR

The user's device must have an enabled SECTOR workspace e.g. BlackBerry Secure Workspace, and the application must be configured as an allowed application via the workspace configuration.

4.7.3 MindLink for MobileIron

The user's device must have a MobileIron AppConnect container – i.e. they must have deployed the MobileIron Mobile@Work application and be registered and enabled in the MobileIron Core console. The application must be authorized via the policy settings.

4.7.4 MindLink for Citrix Worx

The user's device must have a Citrix Worx container – i.e. they must have deployed the Worx Home application and be registered and enabled in the XenMobile console. The application must be authorized via the policy settings.

In addition to the publically-available app, delivered via the iTunes store, we also support in-house self-wrapping via the MDX Toolkit. In this scenario, MindLink will deliver the "vanilla" application IPA file which can then be wrapped and deployed directly from the XenMobile console.

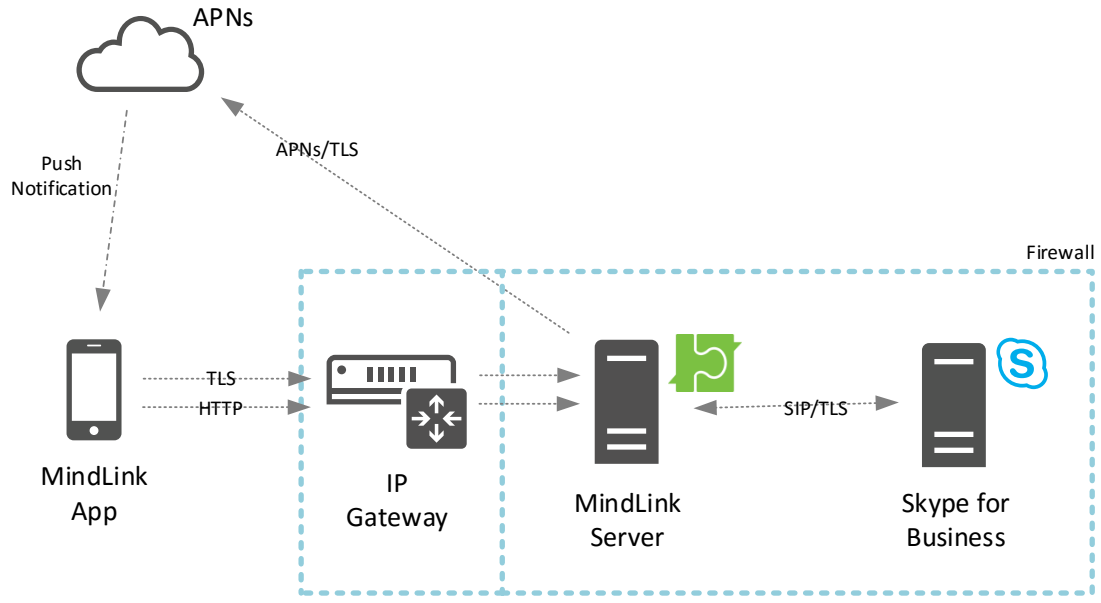
The application metadata MDX file for the public iTunes app is available from the Citrix Marketplace.

4.8 On-Boarding

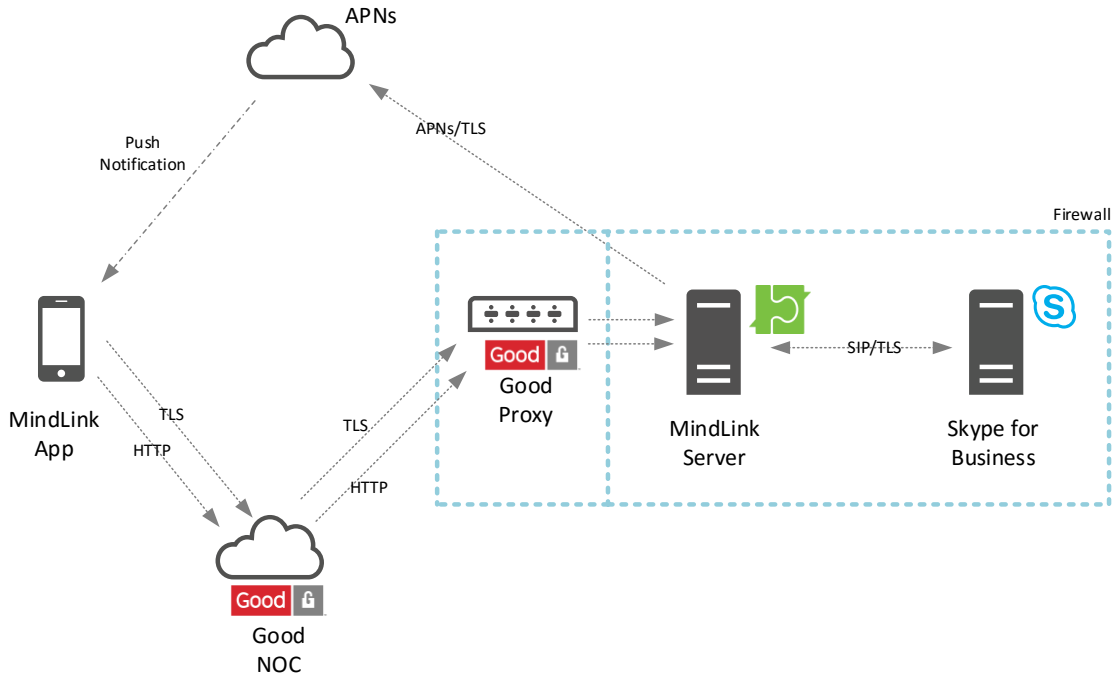
The user must configure the application to talk to the MindLink Server. On first installation, the application will ask for the address of the server to connect to – the DNS name of the MindLink Server, plus the port on which the web service is configured to listen.

This value is then stored and re-used for subsequent sessions. The iOS Settings app can be used to change the value.

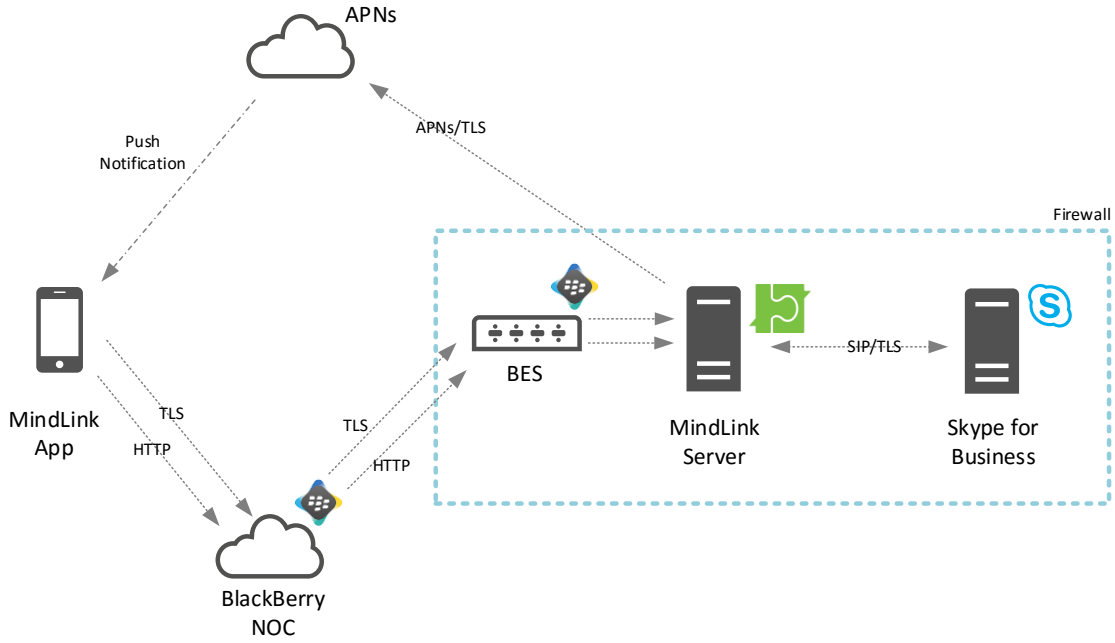
4.9 Reference Deployment



4.9.1 MindLink for Good

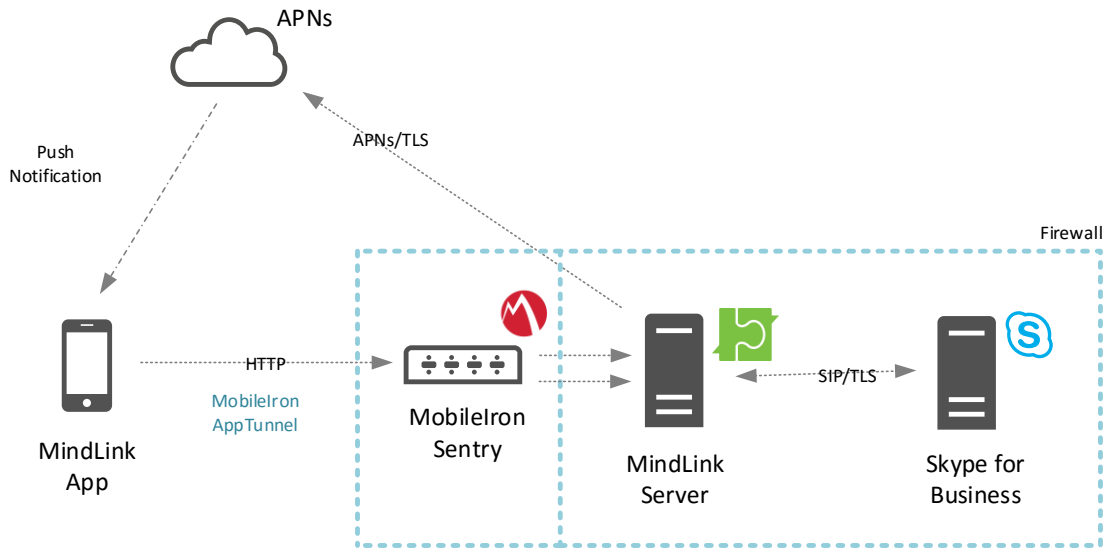


4.9.2 MindLink for SECTOR

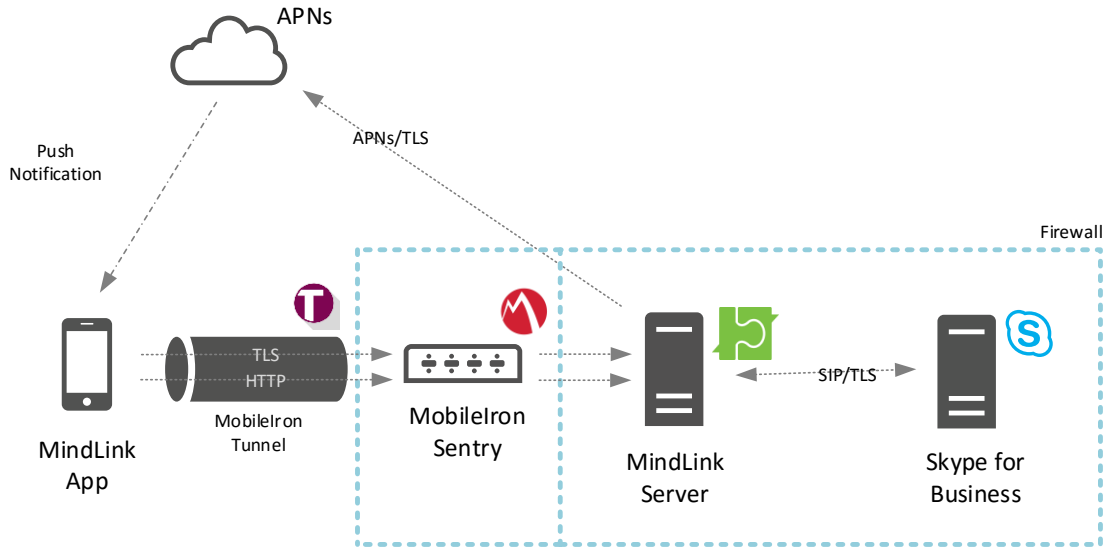


4.9.3 MindLink for MobileIron

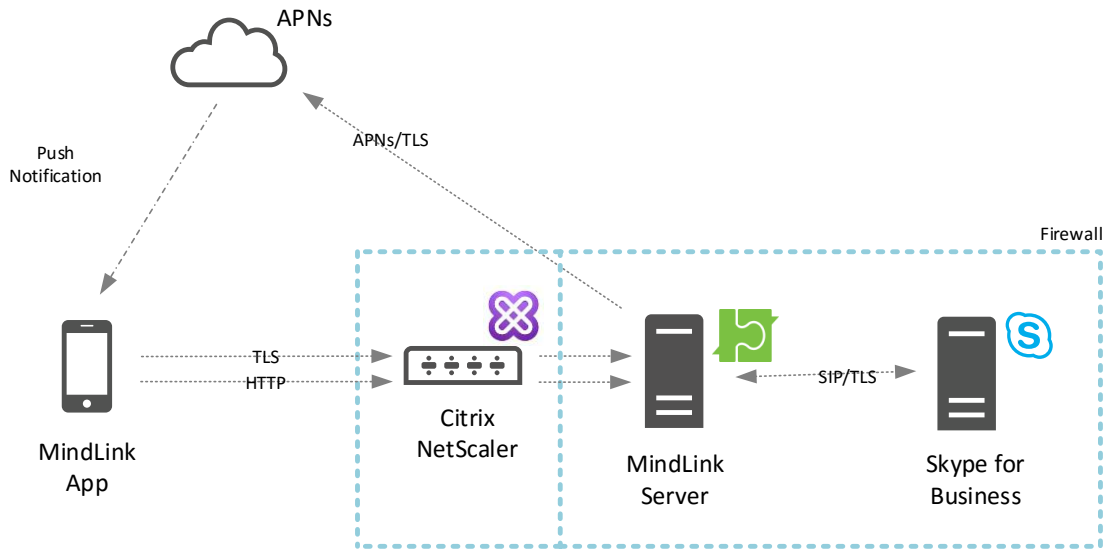
Leveraging MobileIron AppTunnel:



Leveraging MobileIron Tunnel:



4.9.4 MindLink for Citrix Worx



5 Android

MindLink Mobile for Android supports Android phone and tablet devices with any screen size.

It is also available in flavours that integrate with the following MAM containers:

- MindLink for SECTOR (SECTOR-based workspaces e.g. BlackBerry Secure Workspace)

5.1 Persistent Connectivity

The application connects by making a TLS connection and an HTTP connection on two different ports to the MindLink Server.

These connections must be routed from the external mobile network to the MindLink Server, which must be installed on the internal network. The application has been designed to be agnostic as to how this routing occurs so that organisations can leverage their existing network infrastructure.

Various strategies are available:

- Direct connection through external firewall – the organisation opens the external firewall so that devices on the external firewall can connect directly to the MindLink Server
- Proxied connection via a network security gateway – the organisation routes the connection via a security gateway deployed in the DMZ. E.g. using a F5 Big-IP or Citrix NetScaler.

5.1.1 MindLink for SECTOR

The MindLink for SECTOR application connects to the server using the secure workspace connection. For BlackBerry Secure Workspace, the connection is tunnelled via the BlackBerry Enterprise Server's secure BCP connection directly to the MindLink Server on the internal network.

5.2 Push Connectivity

Push notifications are sent to the device using Google Cloud Messaging (GCM).

The MindLink Server connects to the GCM infrastructure by making outbound HTTP requests. The server must be able to communicate with GCM for push notifications to be received. The server can be configured to use an HTTP proxy to make this connection.

A user can choose whether push notifications are sent to the device by configuring a setting inside the application. When push notifications are received, they are added to the Android notification drawer. If a new message is received while the app is in the background (before it has automatically disconnected), then a notification of this new message will also be added to the notification drawer. The Android Settings application may also be used to configure how MindLink notifications are added to the notification drawer.

If a push notification is sent when a device is out of coverage, then the push notification will be stored and delivered when the device is back in coverage. Only the latest push notification will be stored for delivery, however.

5.3 Storage

The MindLink app stores very little information in the at-rest device storage, and no message content.

The data that is stored is saved on the device's internal storage in "private" mode, such that the operating system restricts access to the application itself.

5.3.1 MindLink for SECTOR

All data is stored securely in the SECTOR storage container.

5.4 Access Rights

The application requests the following permissions from the operating system on installation:

- Network access
  - To communicate with the MindLink Server
- Inspect network connections
  - To coordinate the connection to the MindLink Server
- Control vibration
  - To insert notifications into the notification drawer
- Prevent the phone from sleeping
  - To momentarily clean-up network resources when disconnecting.

The app does not access any personal information stored on the device – the Android security model enforces that this is the case.

Android 6.0+ devices

Android will prompt the user for permission to access external storage the when the user enables logging for the first time.

Pre-Android 6.0 devices

On installation, Android will prompt the user to accept that the application can perform the following actions:

- Access Identity
  - This is required to identify the device to the GCM infrastructure
- Access External Storage
  - This is required to write log files to the SD Card when logging is enabled.

5.5 File Download

Files sent in chat rooms can be downloaded by the user to the device. The app farms the actual downloading process off to the device browser, from where the file can be opened.

5.5.1 MindLink for SECTOR

The download is farmed off to a SECTOR-enabled browser e.g. the BlackBerry Workspace Browser, if installed.

5.6 Data-Loss Prevention

In addition to the data-loss prevention mechanisms described elsewhere, the application does not allow copy/paste of message data outside of the application.

5.7 Deployment

The application is deployed to the user's device as a publically distributed app from the Google Play store.

An enterprise-app store system may be used to advertise the availability of the application to the user, but the actual delivery of the app binary is from Google Play.

5.7.1 MindLink for SECTOR

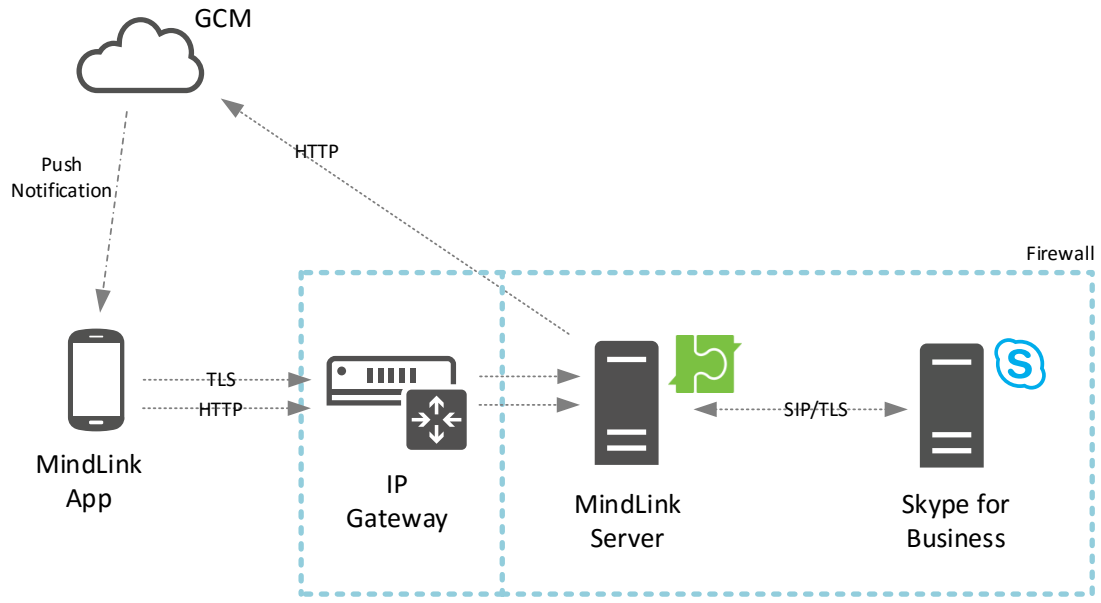
The user's device must have an enabled SECTOR workspace e.g. BlackBerry Secure Workspace, and the application must be configured as an allowed application via the workspace configuration.

5.8 On-Boarding

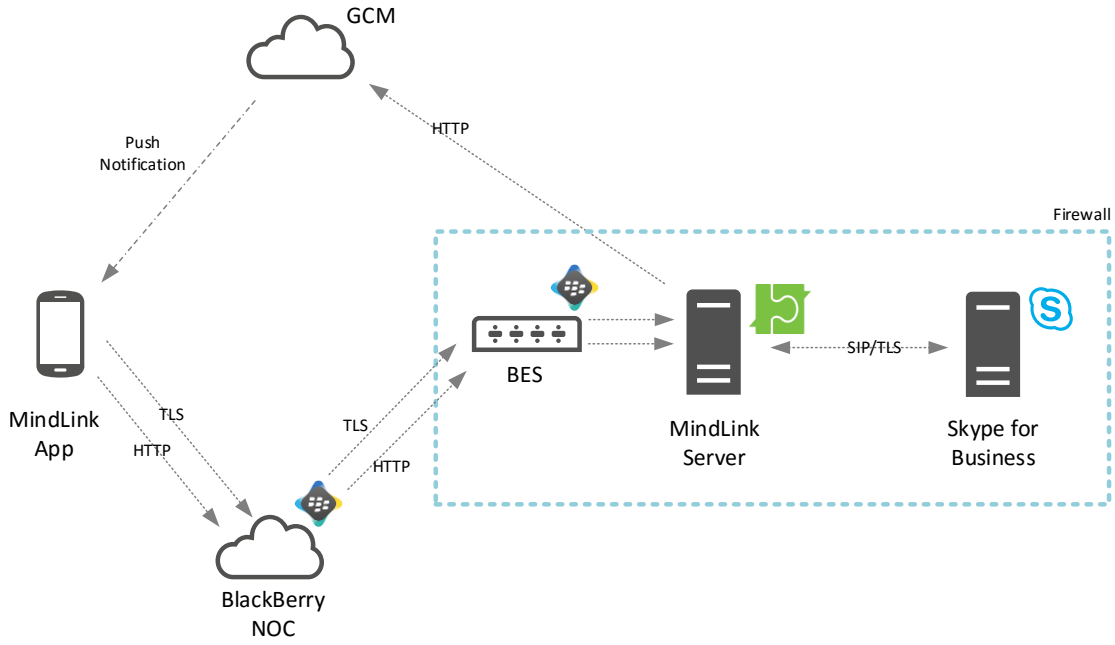
The user must configure the application to talk to the MindLink Server. On first installation, the application will ask for the address of the server to connect to – the DNS name of the MindLink Server, plus the port on which the web service is configured to listen.

This value is then stored and re-used for subsequent sessions. The server settings view inside app can be used to change the value.

5.9 Reference Deployment



5.9.1 MindLink for SECTOR



6 BlackBerry 10

MindLink Mobile for BlackBerry 10 supports any BlackBerry 10 device that has been activated against a BlackBerry Enterprise Server (BES). The application is designed to be deployed to and used in the “work” side of the device.

The BES server is deployed on the internal network alongside the MindLink Server. BES 10 and BES 12 are both supported.

6.1 Persistent Connectivity

The application connects by making a TLS connection and an HTTP connection on two different ports to the MindLink Server.

These connections are tunnelled via the BlackBerry Enterprise Server’s secure MDS-CS connection directly to the MindLink Server on the internal network.

6.2 Push Connectivity

Push notifications are sent to the device via the MDS-CS service on the BlackBerry Enterprise Server. The MindLink Server sends push notifications by making HTTP requests to the MDS-CS push web service.

A user can choose whether push notifications are sent to the device by configuring a setting inside the application. When push notifications are received, they are added to the device’s Notification Hub. If a new message is received while the app is in the background (before it has automatically disconnected), then a notification of this new message will also be added to the Notification Hub. The BlackBerry 10 Settings application can be used to configure the sound and vibration behaviour when MindLink notifications are added to the notification hub.

If a push notification is sent when a device is out of coverage, then the push notification will be stored by the MDS-CS server and delivered when the device is back in coverage. The MDS-CS server will store the notification for a maximum of 10 minutes before it is discarded.

6.3 Storage

The MindLink app stores very little information in the at-rest device storage, and no message content.

The data that is stored is saved inside the secure work perimeter container and encrypted by the operating system to the standard level.

6.4 Access Rights

On installation, Android will prompt the user to accept that the application can perform the following actions:

- Access device identifying information
    - This is required to identify the device to the GCM infrastructure
- Access Shared Storage
    - This is required to write log files to the SD Card when logging is enabled.

The application also requests the following permissions from the operating system on installation:

- Post Notifications
    - Required to add notifications to the Notification Hub.

The app does not access any personal information stored on the device – the BlackBerry 10 security model enforces that this is the case.

6.5 File Download

Files sent in chat rooms can be downloaded by the user to the device. The app farms the actual downloading process off to the device browser, from where the file can be opened.

6.6 Data-Loss Prevention

All application data is containerised inside the BlackBerry Work perimeter.

6.7 Deployment

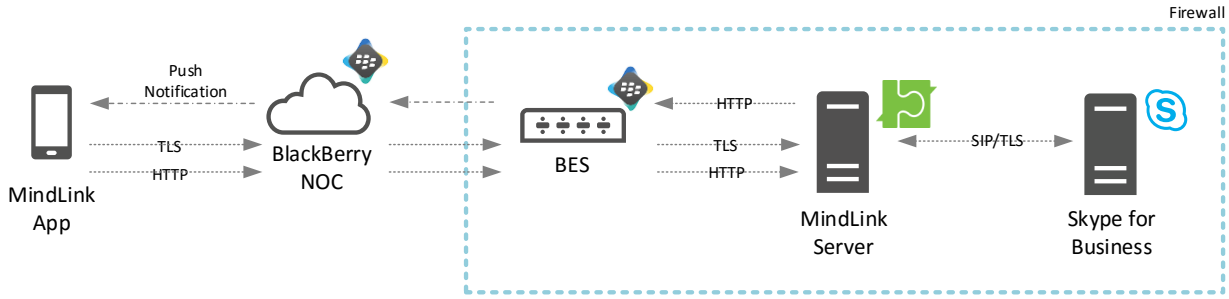
The application is deployed to the user's device from the BES administration console. The application is delivered by MindLink as a .bar file which should then be uploaded as a software configuration and pushed out via policy to the device.

6.8 On-Boarding

The user must configure the application to talk to the MindLink Server. On first installation, the application will ask for the address of the server to connect to – the DNS name of the MindLink Server, plus the port on which the web service is configured to listen.

This value is then stored and re-used for subsequent sessions. The server settings view inside app can be used to change the value.

6.9 Reference Deployment



7 Scale Out and High Availability

With the minimum hardware requirements a single MindLink Server instance will support 2000 devices.

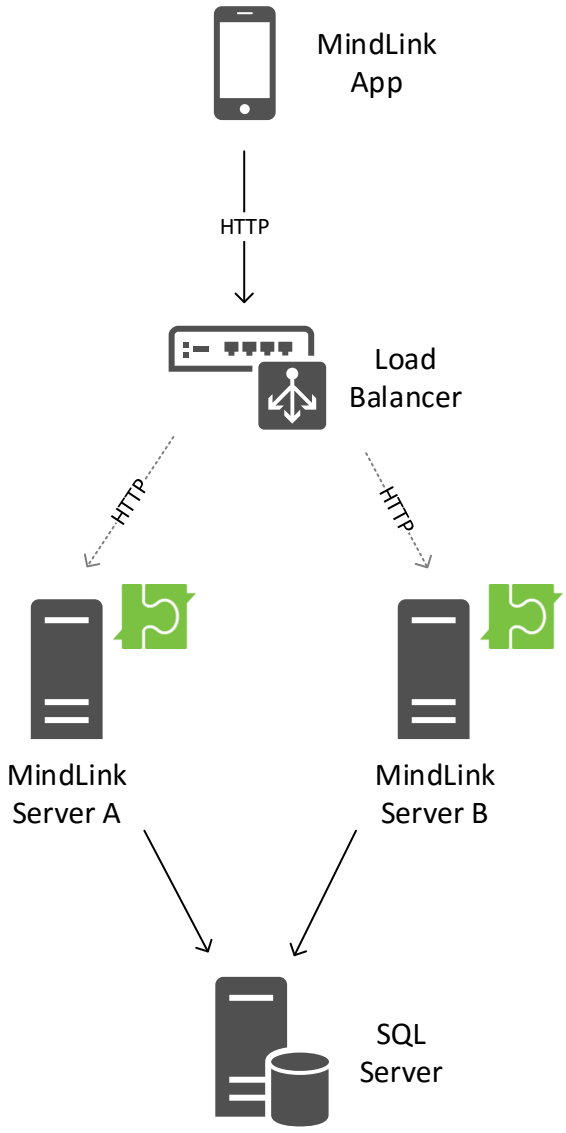
MindLink Servers can be deployed in a pooled cluster for the purpose of:

- Scaling out the number of devices:
  - Deploy more servers to linearly scale the supported number of devices.
  - Session load is distributed throughout the pool
- Fault tolerance during server failure:
  - Deploy f additional servers to support f server failures

7.1 Infrastructure Requirements

Deployment of a standalone MindLink Server requires no additional infrastructure outside of the host Windows Server.

However, deployment of multiple MindLink Servers in a pooled cluster requires additional infrastructure components – a Microsoft SQL server and an HTTP Load Balancer. The clustering mechanism is implemented at the application level and does not require Windows Server clustering or other OS-level configuration.



7.1.1 Load Balancer

The load balancer's role is to distribute new session logons across the available servers. Any standard HTTP load balancer implementing a round-robin balancing algorithm is supported, and no client affinity mechanism is required.

Only the initial bootstrapping HTTP request is made via the load balancer. This establishes an association between a specific node in the pool and the device. The chosen node then coordinates the Skype for Business session on behalf of the device as usual. Subsequent TLS connections throughout the lifetime of the session are made directly from the device to the specific node as usual.

The load balancer is aware of which servers are active in the pool by periodically pinging an HTTP health-check service exposed by each MindLink Server.

7.1.2 SQL Server

The role of the SQL server is to allow the servers in the pool to coordinate amongst themselves as to which node is responsible for which device.

SQL Mirroring, AlwaysOn Failover Cluster and AlwaysOn Availability Groups are all supported high-availability solutions for the SQL layer.

7.2 Scale Out

Adding more servers to a MindLink Server pool will add capacity to serve more devices. Each server is responsible for maintaining the long-running Skype for Business server for a subset of the connected devices.

Each device session is managed by exactly one member of the MindLink Server pool. This affinity is assigned by the load balancer when each session is initiated.

7.3 High Availability

Deploying MindLink Servers in a clustered pool with extra server capacity allows service to be maintained even when a server fails. An extra node should be deployed for every server failure that should be tolerated.

In normal operation, device sessions are load balanced evenly across all nodes. When a server fails, the long-running sessions managed by the node are ended.

When the device next tries to re-connect to the failed server to resume its session, the app will prompt the user that their session cannot be resumed. At this point, the app will then create a new session which will be assigned a new remaining live node by the load balancer.

Sessions for devices homed on other nodes are not affected by the node failure and will continue as normal.

8 Group Chat Add-ins

MindLink for iPad and MindLink for Android on Android tablet devices supports Chat Room Add-ins. An add-in is a panel that is displayed alongside the chat room message content for the purposes of displaying related or relevant information. The Add-in can be used to enhance the productivity and usefulness of the conversation within the chat room.

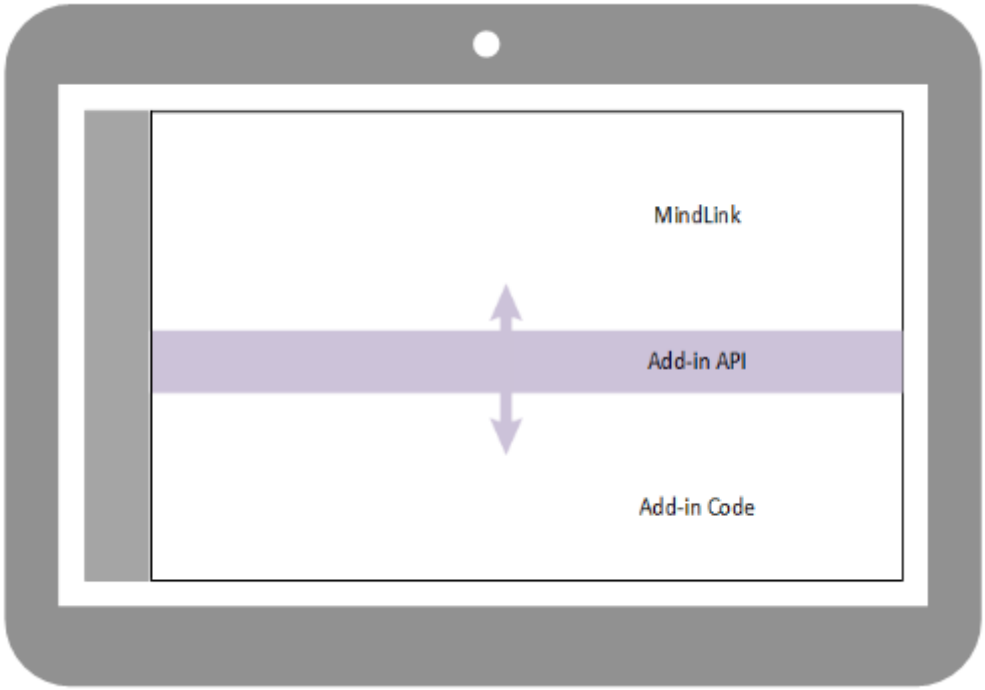
An Add-in can be any web page. The system administrator configures which panel appears in which chat room using the Persistent Chat administration tools.

The MindLink application hosts the Add-in content and also exposes an API with which the Add-in can interact with the conversation in the chat room. Whilst any static web page content can be shown as an Add-in, specially designed Add-ins can be implemented to interact with the rest of the application using the API. For example, the Add-in may be written to interact with the chat room messages when a condition is met – such as an Add-in hosting a live data stream from a third-party line of business system which then posts relevant information to the chat room in the parent pane.

The Add-In architecture consist of following components:

- A standard web page which contains code and content
- The page is contained within the Add-In wrapper which essentially sits inside a browser frame with an API – “MindLink JavaScript Add-In API”
- The JavaScript API, which provides the capability to support interaction between the Add-In and the parent panes

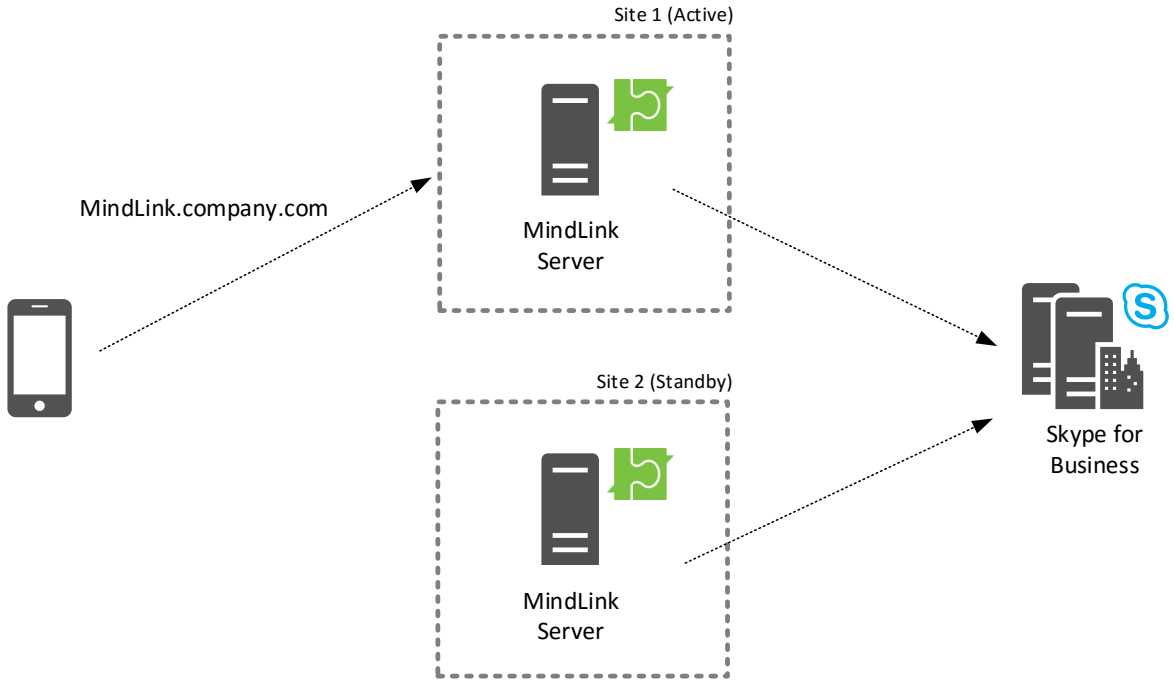
More information is available within the Add-In developer guide.



9 Failover

Failover strategy at the site-level is achieved by an active/passive configuration. A mirror-image MindLink deployment should be configured at another site.

On failover, the address of the MindLink Server (or the address of the load balancer when deployed as a pool) as configured on the client should be switched to point to the secondary installation via DNS or otherwise.



In the above diagram the address of the MindLink Mobile server pool has been configured as MindLink.company.com, and all devices have been configured to connect to that address. MindLink.company.com is currently resolving via DNS to the IP of the MindLink Server in Site 1.

On failover to Site 2, the DNS configuration will be changed such that MindLink.company.com resolves to the IP of the MindLink Server in Site 2.

9.1.1 Skype for Business

Failover of the MindLink components can happen independently of the Skype for Business frontend and Persistent Chat pools.

Similarly, as the MindLink components in the standby site should already be defined as trusted application servers in the Skype for Business topology, no additional Skype for Business configuration changes are required to failover the MindLink tier.

9.1.2 Pooled Failover

If the MindLink Servers are deployed in a pooled cluster, an identical pool should be defined in each site. The data stored in the SQL server used by the pool relates only to the member server nodes in

the pool, and as such does not need to be synchronized between sites – the active and standby SQL databases can be completely decoupled.

10 Versioning

This section applies to the MindLink apps that are publically distributed, as it deals with the versioning concerns of having regularly updated public-store client apps connecting against customers' on-premise MindLink Server deployments. It does not apply to the BlackBerry 10 client apps, which is deployed in lock-step with the corresponding server version.

On release of a new MindLink Mobile version (currently scheduled at monthly), MindLink Software will update the download available in the iTunes store and Google Play store to the latest version, so that the iTunes and Google Play client apps always match the latest server version available from MindLink Software.

10.1 Backwards Compatibility

As such, it will be likely that eventually the client version available in the iTunes or Play store will be a newer version than that of the MindLink Server which an organization has deployed. For example, new MindLink users will be downloading version 4 of MindLink from iTunes, when their organization may have version 2 deployed.

This backwards-compatibility of new client versions will be supported by MindLink Software for server versions up to a year old.

10.1.1 BlackBerry 10

The corresponding version of the client is pushed out to user devices via the BES when the MindLink Server is upgraded. A newer version of the application is only pushed out when the MindLink Server is upgraded.

10.2 Forwards Compatibility

Conversely, on upgrade of an organization's MindLink Server, existing users will potentially still have an older version of the MindLink Mobile client installed on their devices.

In this case, the MindLink client will show a message informing the user to upgrade their installed application to the latest version from the iTunes or Play store, and prevent them from logging in to the app.

10.2.1 BlackBerry 10

When the MindLink Server is upgraded, the new corresponding version of the client application is pushed out to all user devices via the BES.

11 Licensing

The MindLink Server requires a license to run. This will be provided to you by MindLink and must be applied to the installation via the Management interface. The license will either allow an unlimited number of devices to connect, or will specify a maximum capacity.

If a maximum capacity is specified, devices will be allowed to start sessions up until the number of sessions on the server (or across the pool) reaches the capacity limit. At this point, further device logons will be denied. This will occur until existing sessions are ended – the user logs out, the session expires, etc.