MindLink

# MindLink Desktop

## *Technical Overview*

Version 17.3

## Table of Contents

# 1 Overview

MindLink Desktop enables MindLink functionality – including Microsoft Skype for Business Instant Messaging (“IM”), Presence and Persistent Chat (“PChat”) – in a web-based HTML 5 app.

## 1.1 Browser Support

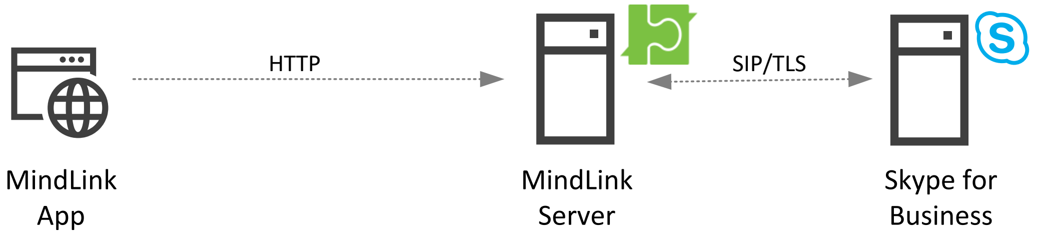
MindLink Desktop is supported in the following browsers:

- Internet Explorer 10
- Internet Explorer 11
- Edge
- Firefox
- Chrome
- Safari – OS X and iOS 9+

Unless otherwise stated, the app will be tested in the latest version of each browser. The app uses various “polyfill” techniques to gracefully degrade feature support in older browsers

## 1.2 High-level Architecture

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



The MindLink Desktop 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.
- Serves the web app assets to the browser.
- Handles connections from the web browser app.
- Brokers between HTTP connection from browser and SIP connection to Skype for Business.
- Maintains session state across network disconnections and acts as an intelligent buffer for updates to be sent to clients.

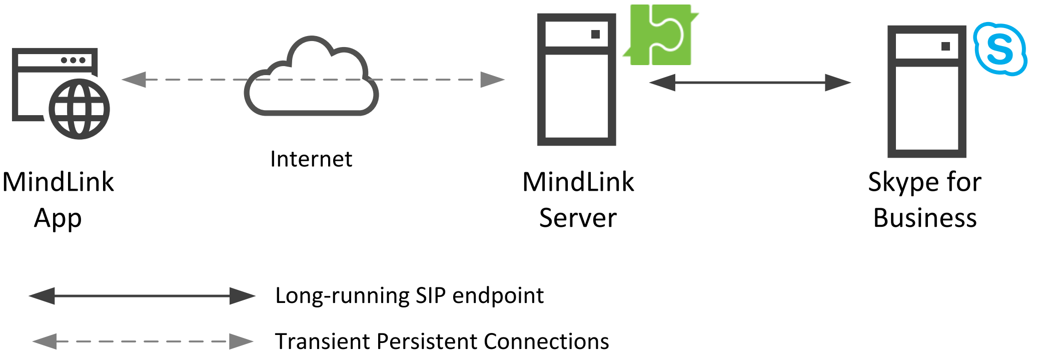
The MindLink Desktop server is a .NET application that runs as a Windows Service. The host Windows Server machine can be virtualized. The server component is installed by running a standalone .MSI executable and then using a graphical management utility application to configure the system.

The MindLink Desktop 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 web-based Skype for Business endpoint. The MindLink Server maintains the Skype for Business endpoint on behalf of the user, throughout the duration of the app being loaded and logged on in the browser – a "session".

The client app establishes a two-way connection with the server and receives updates of new messages immediately.



## 2.1 Configuration Bootstrapping

When the browser navigates to the MindLink URL, the app's static assets – HTML, JavaScript and images – are served from the MindLink Server. The MindLink Server contains an integrated light-weight web server – IIS does not need to be enabled on the host Windows Server.

On loading up, the MindLink app will make a request to fetch bootstrap configuration data from the server. 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

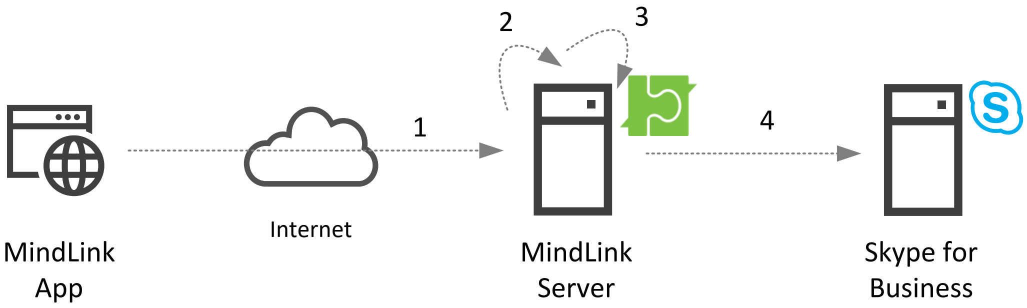
The logging on process happens once at the start of the MindLink session. Once logged on, the server issues the client app with a one-time token, which it subsequently uses to identify itself to the server in requests.

To log on, the user must supply their credentials. See section 2.3 for more information about the supported types of credentials.

These 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 will first authenticate these credentials, and then resolve the corresponding SIP address. This may involve an Active Directory LDAP query or other interactions.

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, no additional credentials are sent to Skype for Business directly.



1) Client sends credentials to server.
2) Server authenticates credentials.
3) Server resolves corresponding SIP address for credentials.
4) Server establishes Skype for Business endpoint with SIP address using trusted connection.

## 2.3 Authentication

MindLink supports multiple authentication mechanisms out of the box. The administrator may configure which authentication mechanism(s) are enabled.

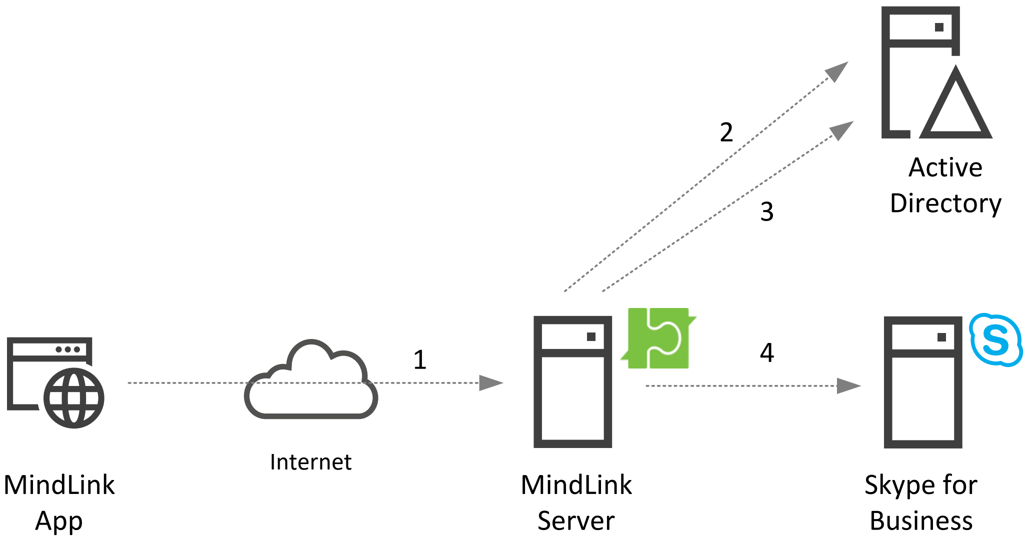
If multiple mechanisms are available, the administrator can either let the user select which mechanism they want to use, or the client will try each mechanism in turn until one succeeds. The administrator may configure URLs to which the user is redirected if all mechanisms fail, or on logging off.

In addition to the standard authentication mechanisms outlined below, custom adaptor code may be injected into the authentication pipeline to form a custom authentication, authorization and account resolution workflow.

### 2.3.1 Password Authentication

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.

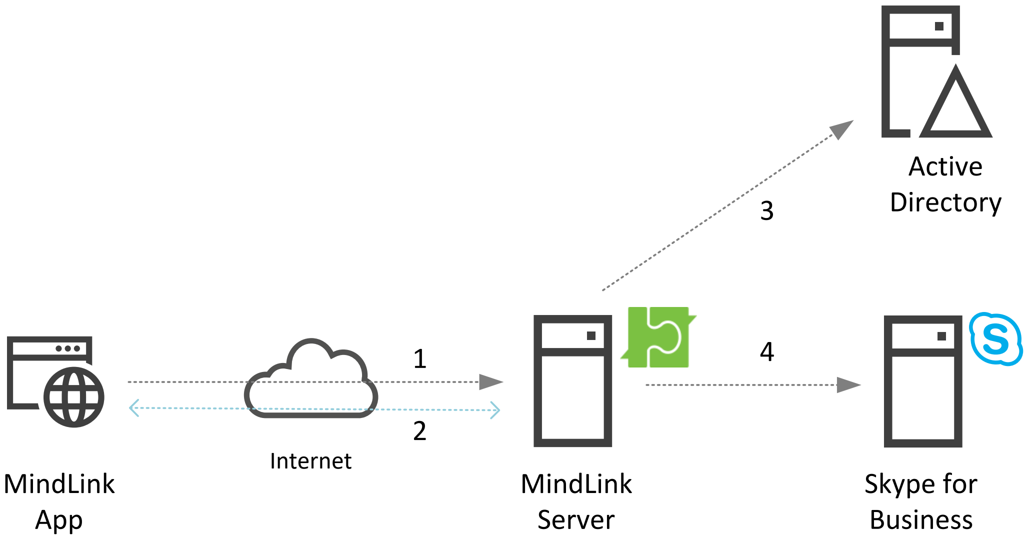
The MindLink Server authenticates these credentials with Active Directory by performing a fast bind with an LDAP server in the user account's domain. Active Directory in the Skype for Business forest is then queried via the Global Catalog to obtain the user's SIP address.



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.

### 2.3.2 Integrated Windows Authentication

The MindLink Server challenges the web browser for the current user's identity, which is negotiated over NTLM or Kerberos protocols. The user must be running the web browser as an account that maps to their SIP-enabled identity. If the browser security settings are configured to negotiate the security context without prompting, this enables a "zero-sign-on" experience.



1) Client makes HTTP request to MindLink Server
2) Server challenges browser for Windows identity. Browser communicates this over NTLM or Kerberos.
3) Server queries for SIP address from Active Directory Global Catalog.

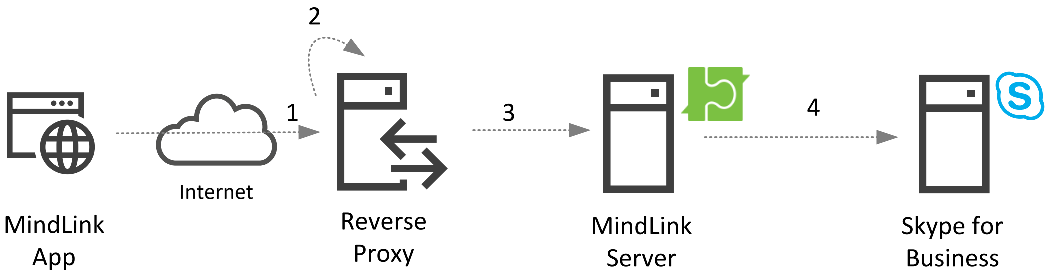
4) Server establishes Skype for Business endpoint with SIP address using trusted connection.

### 2.3.3 Pre-Authenticated HTTP Header Authentication

To enable decoupling of the authentication mechanism – and deployment of custom or more elaborate multi-factor authentication workflows – the MindLink Server can be configured to accept the user's identity as an HTTP Header included in incoming requests from the browser.

The MindLink Server is typically published behind a pre-authenticating reverse proxy in this scenario. The reverse proxy deals with authenticating and authorizing the user, and then forwards the resolved identity on as an HTTP header injected into the original request. The proxy should inject the value of the user's SIP address into the HTTP Header.

This mechanism assumes that unauthenticated requests cannot be made to the MindLink Server, protected by virtual or physical network security constructs.



1) Client makes HTTP request to MindLink Server address.
2) Reverse proxy intercepts request and pre-authenticates user. Skype for Business SIP address is resolved by proxy authentication flow.
3) Reverse proxy forwards browser request, with SIP address injected as additional HTTP header.
4) Server establishes Skype for Business endpoint with SIP address using trusted connection.

## 2.4 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 closes the browser tab.
- 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 app is disconnected from the server for 2 minutes.

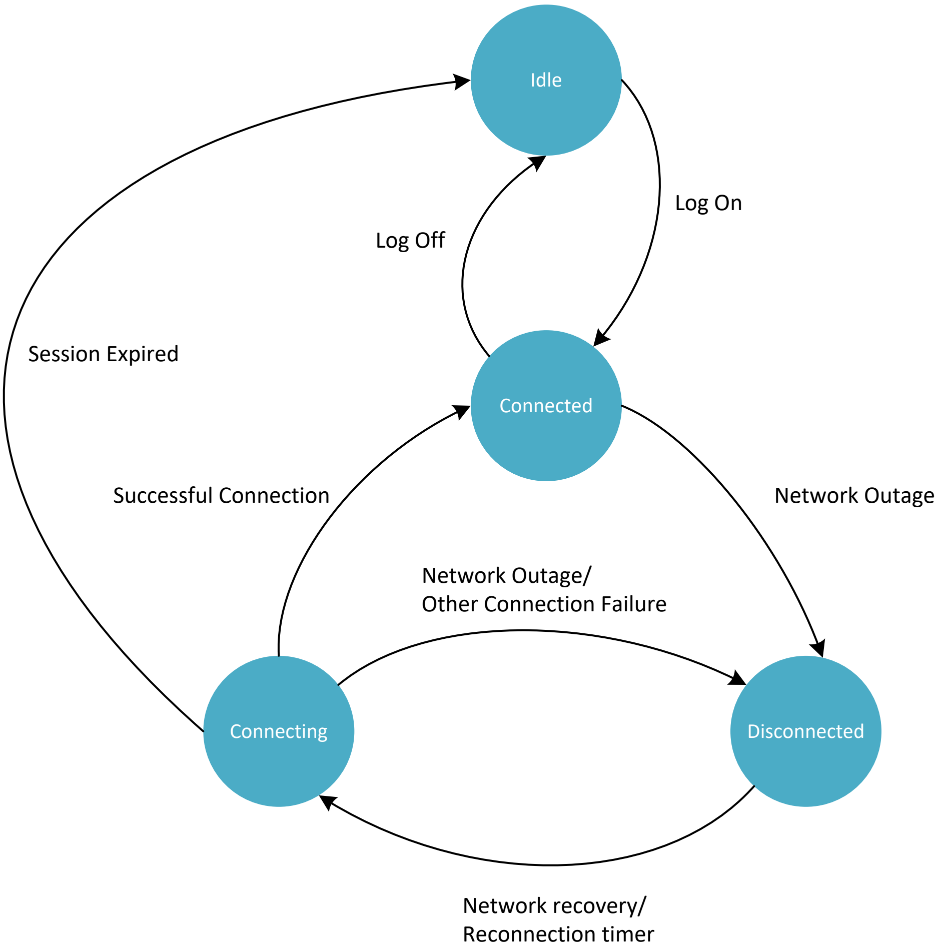
The session is always in one of two modes:

- **Connected**
  - The app will attempt to establish a two-way "persistent" connection to the server.
  - The app will report itself as "connected" when in this state.

    - The user will be able to interact with the app 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.
- **Disconnected from the client**
    - The app will report itself as "disconnected" in this state.
    - The session will transition to this state if network connectivity to the server is lost.
    - The app will attempt to reconnect to the server during this period.

Management of this lifecycle is automatic. The user will see a "Reconnecting…" message while the client reconnects to the server.

The server records the last time that a user was connected. Sessions that have not been connected to the client for 2 minutes are automatically destroyed, and the underlying Skype for Business endpoint disconnected.



## 2.5 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 client to send and receive real time updates.

This "two-way" connection over HTTP is achieved via a "long-poll" (aka. "pending-GET") mechanism whereby the client issues consecutive long-running HTTP GET requests:

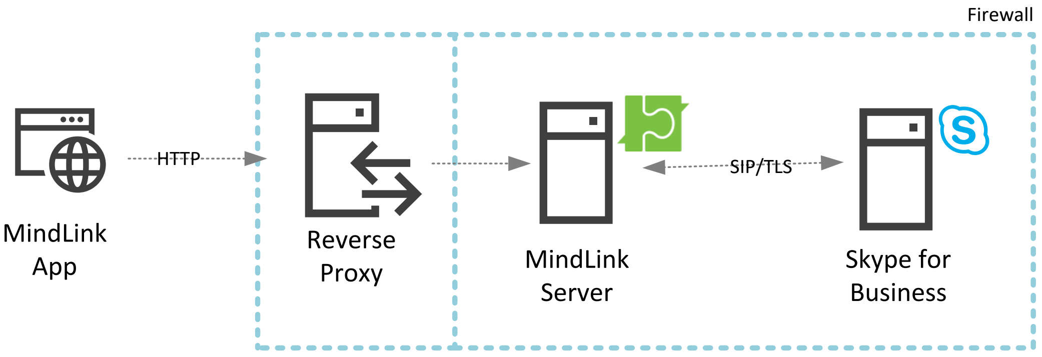
- A GET request will be issued by the app to wait for new events from the server.
- If events are ready – e.g. a new message is received – the GET request is completed by the server immediately, with the HTTP response containing the event data.
- To prevent long-running requests being terminated as idle by network infrastructure, if no events are received within 30 seconds then the GET request is completed immediately with an empty response.
- In either case, on completion, a new GET request is issued immediately by the client to wait for future events.

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.

## 2.6 External Connectivity

All communication between the browser and server is over HTTP. This connectivity can be secured over HTTPS, and the port used for communication is configurable.

The MindLink Server must be deployed to a domain-joined server on the internal network, but the app may be published to external users via an HTTP reverse proxy or other network security gateway.



## 2.7 Stored Data

MindLink Desktop 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 in the browser.

The application will only store the following data at-rest in the browser’s “Local Storage” cache:

- Log-on user settings – Used to store user preferences as selected on the log-on screen.
- View state – The size of the resizable UX elements, and the collapsed state.

Message data and authentication tokens are not stored in the browser’s cookies or local storage, and user preferences are persisted to the server so they can be shared between endpoints.

## 2.8 Endpoints

A user may log on simultaneously to MindLink in any number of browser tabs, across any number of PCs or devices. Each browser tab creates a new MindLink session on the MindLink Server, and a corresponding Skype for Business endpoint.

Authentication and session state are not shared between concurrent sessions.

# 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. Skype for Business Online deployments are not supported.

For Hybrid topologies, MindLink must be deployed in the on-premise topology and may be utilized only by users homed on-premise. This includes both the users logging on via MindLink, and other users who appear on the MindLink user's contact list or chat with the MindLink user over IM.

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 on 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.

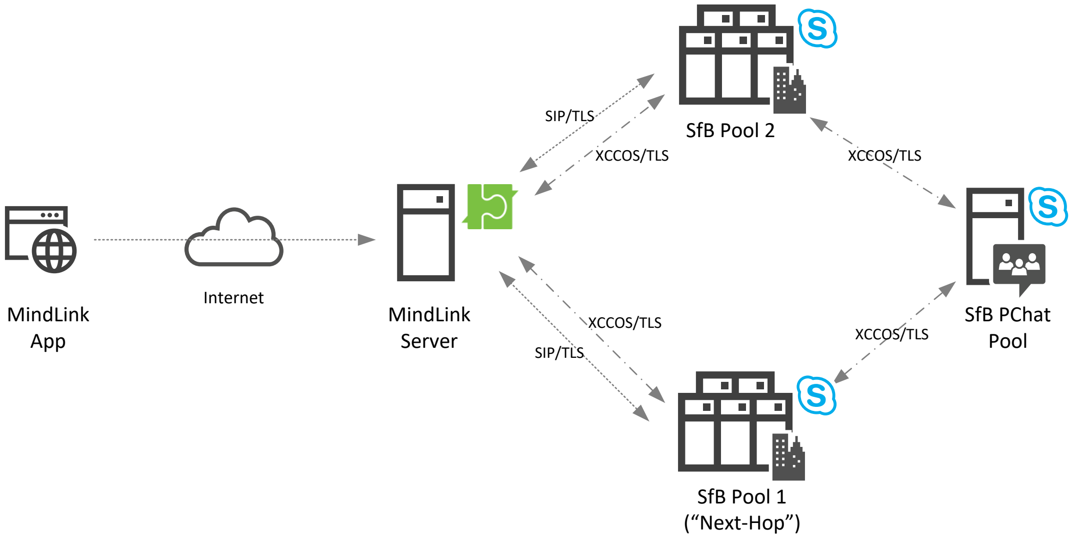
The trusted connection allows the Skype for Business infrastructure to treat the MindLink Server as an equal peer and enables efficient routing of SIP traffic to and from the MindLink Server. The establishment of this trust requires that the Skype for Business servers be able to resolve the DNS name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

The MindLink client displays a set of chat rooms that the user is 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 drawn directly from the user's desktop Skype for Business profile. Adding or removing groups or contacts in MindLink will propagate the change to Skype for Business client. Propagating in the reverse direction occurs when the user re-logs in to the MindLink client.

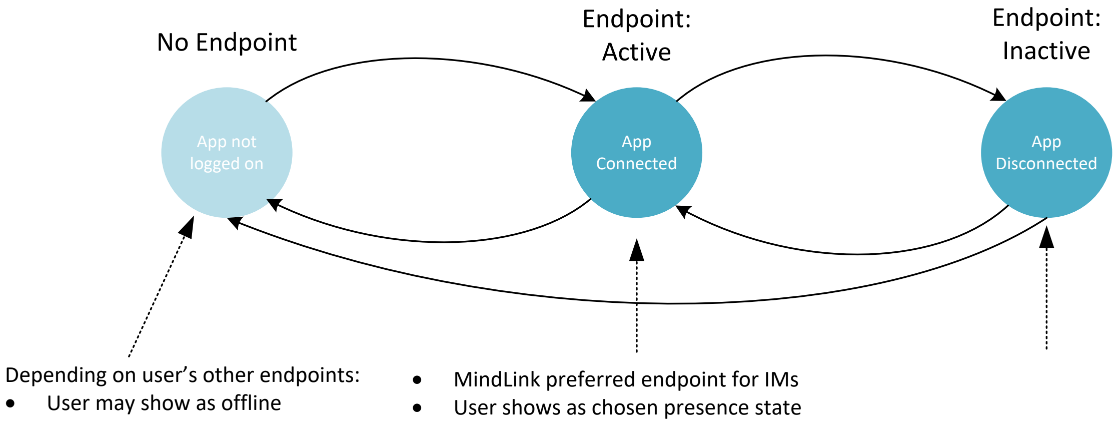
## 3.5 Lifecycle

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. The endpoint is maintained as an active endpoint until the client logs out. If the client is disconnected from the server due to a network outage or otherwise, the endpoint is reported as inactive 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.


No Endpoint
Endpoint: Active
Endpoint: Inactive
App not logged on
App Connected
App Disconnected
Depending on user's other endpoints:
• User may show as offline
• MindLink preferred endpoint for IMs
• User shows as chosen presence state

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.

## 3.8 Monitoring

MindLink endpoints are registered against the Skype for Business registrar in the standard way. Post-mortem MindLink usage can be identified by querying the Skype for Business registration monitoring report logs, filtering by a MindLink User-Agent string.

Similarly, MindLink IM activity is recorded in the Skype for Business monitoring reports.

## 3.9 Conversation History

MindLink endpoints may optionally integrate with the Skype for Business Server "Conversation History" system, whereby IM messages are saved to the user's "Conversation History" folder in their Exchange mailbox. MindLink will additionally retrieve previous messages from this folder when a conversation is re-opened at a later time.

The MindLink Server coordinates saving and retrieval of history messages against all Skype for Business backend versions, independent of the "Server-Side Conversation History" (SSCH) platform managed by Skype for Business itself. Furthermore, conversation history for MindLink endpoints can be enabled/disabled independently of SSCH and conversation history in the Microsoft SfB desktop client.

The following versions of Exchange Server are supported, independent of the backend Skype for Business version:

- Exchange 2010 SP2
- Exchange 2013
- Exchange 2016

## 3.10 Exchange Integration

The MindLink Server will connect to Exchange to access the user's mailbox in the following circumstances:

- When conversation history is enabled on the MindLink Server.
- When the user is enabled for the Unified Contact Store (Lync 2013 and later)

In any of these cases the MindLink Server will use Exchange Autodiscover to locate the appropriate Exchange server, and then connect to Exchange on behalf of the user via Exchange Web Services.

This integration requires:

- Correct DNS configuration to support Exchange AutoDiscovery, given the user's primary email address.
- Exchange ApplicationImpersonation rights assigned to the MindLink Server's service account.

# 4 Group Chat Add-ins

MindLink Desktop 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.

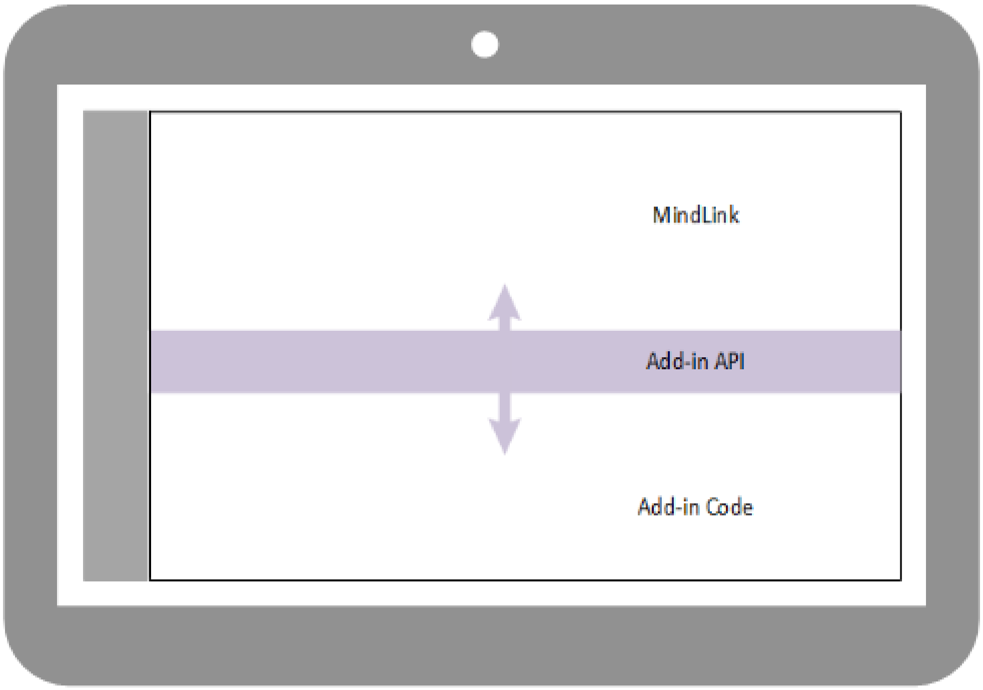
An Add-in can be any web page. The system administrator configures which panel appears in which chat room using the Persistent Chat administration tools.

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 consists of following components:

- A standard web page, which contains code and content.
- A browser frame which hosts the Add-in page and manages the 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.



## 5 Scale Out and High Availability

With the minimum hardware requirements, a single MindLink Server instance will support 2000 concurrent sessions. Each logged-on browser tab represents a single session.

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

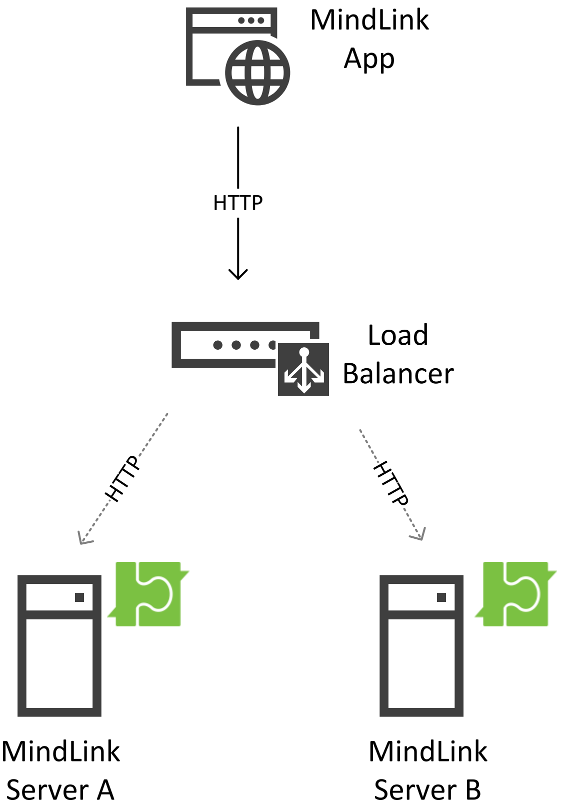
- Scaling out the number of concurrent sessions:
  - Deploy more servers to linearly scale the supported number of sessions.
  - Session load is distributed throughout the pool.
- Fault tolerance during server failure:
  - Deploy ***f*** additional servers to support ***f*** server failures.
- Cross-site high-availability:
  - Deploy MindLink Servers in a cross-site stretched pool for site-level active/active HA.

### 5.1 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 – an HTTP load balancer with session affinity support.

The clustering mechanism is implemented at the application level and does not require Windows Server clustering or other OS-level configuration.



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.

When a user logs on, the servicing node establishes a Skype for Business session on behalf of the client app. This process creates an affinity between the client and the server maintaining the SIP endpoint. Hence, the load balancer must support session affinity, via cookies or otherwise. This is to ensure that subsequent HTTP requests are serviced by the same node that processed the initial log on request.

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.

## 5.2 Scale Out

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

Each session is managed by exactly one member of the MindLink Server pool. This affinity is assigned and managed by the load balancer.

## 5.3 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, sessions are load balanced evenly across all nodes. When a server fails, the long-running sessions managed by the node are ended.

When the app 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 and they must re-logon. On log on, the app will then create a new session which will be assigned a new remaining live node by the load balancer.

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

## 5.4 Cross-Site High Availability

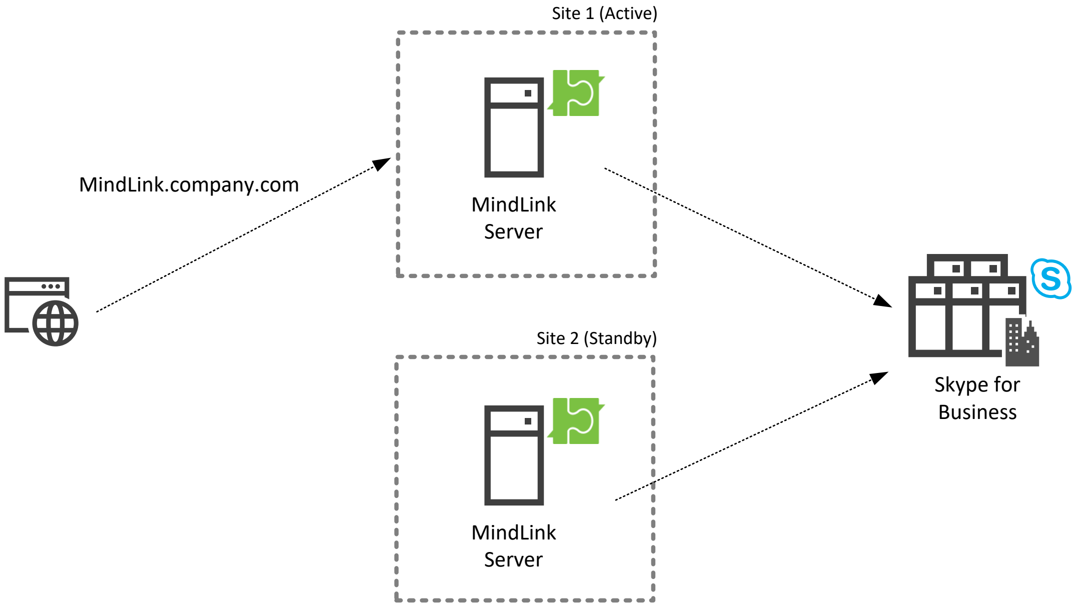
MindLink Servers may be deployed in a cross-site pool for active/active site-level resilience. In normal operation, sessions are load balanced evenly across the two sites. When an entire site fails, the end-user experience is as described above.

The network connection between datacentres must have a latency of less than 5ms.

# 6 Failover

For failover at the site-level in an active/passive configuration, a mirror-image MindLink deployment should be configured at another site.

On failover, the HTTP URL 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 Desktop server pool has been configured as MindLink.company.com, and users are accessing the app by navigating 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.

### 6.1.1 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.

### 6.1.2 Pooled Failover

If the MindLink Servers are deployed in a pooled cluster, an identical pool should be defined in each site.

# 7 Deployment

MindLink Desktop is distributed as a self-contained MSI. The MSI contains the server components, the Management Center (a graphical configuration utility), and the web app client.

The installation process consists of:

1) Extracting the MSI.
2) Configuring the system via the Management Center – including Skype for Business connectivity and frontend app settings.
3) Starting the MindLink Server Windows Service.

Updates are made available on roughly a 6-week cadence. Upgrades are installed in-place and will migrate existing configuration. Users will experience an outage while the MindLink Server service is restarted after the upgrade.

# 8 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 Center interface. The license will either allow an unlimited number of users to connect, or will specify a maximum capacity.

If a maximum capacity is specified, the licensed capacity is applied up front against the number of users that are “enabled” for MindLink – i.e. able to log on to MindLink given an enabled Skype for Business account and the MindLink Active Directory settings. An enabled user will be able to log on an unlimited number of sessions across any PCs or devices.

On start-up, the MindLink Server will survey the Skype for Business user base via Active Directory and reconcile the number of enabled users against the licensed capacity. If the number of enabled MindLink users exceeds the licensed capacity, the MindLink Server will prevent users from logging on.

The MindLink Server subsequently performs this check periodically. If the number of enabled users exceeds the licensed capacity, the MindLink Server will prevent future sessions from being established, until corrective action is taken.

A specific subset of Skype for Business users can be enabled for MindLink by assigning an Active Directory group, partitioning via an OU, or configuring some other custom LDAP query.