mobile:helix™

Administrator’s Basic Guide

LINK 4.1

2025-01A

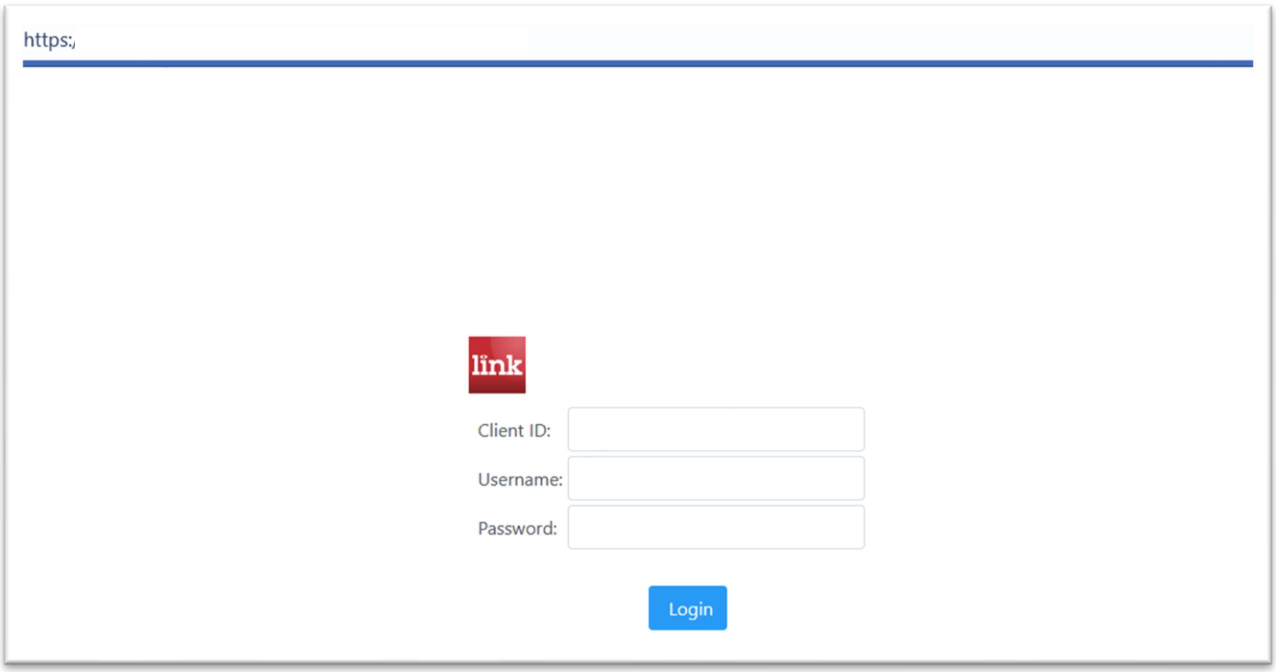
link

Table of Contents

INTRODUCTION

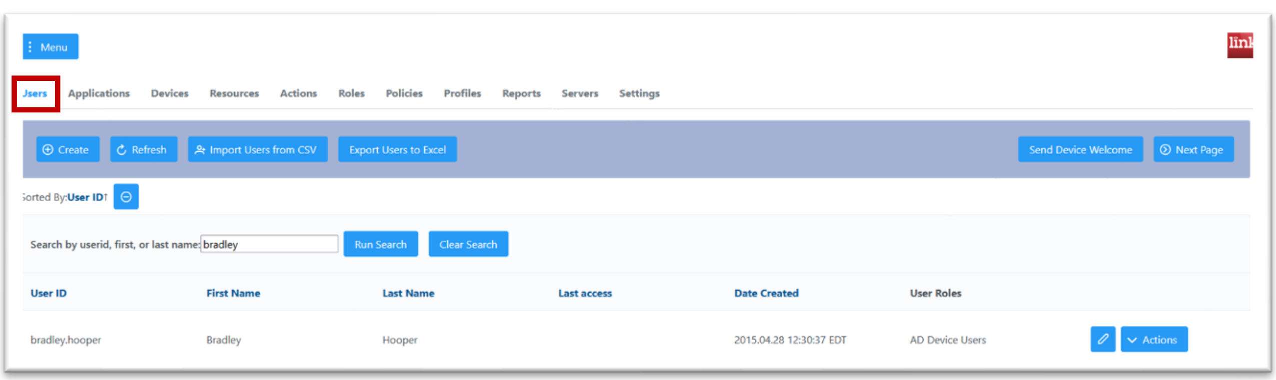
The LINK administration panel provides all control functionality for the Mobile Helix LINK system. This document shows how to use the Controller web interface to manage Users, Applications, Devices, Resources, Actions, Roles, Policies, Profiles, Reports, Servers, and System Settings.

You will need the URL of the LINK Controller and the Client ID. You may use your AD credentials or the Admin credentials to login to the LINK Controller.

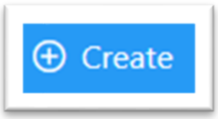


Please contact support@mobilehelix.com if you have not received the URL, Client ID, and Admin credentials.

Logging into the Controller brings you to the Users tab:



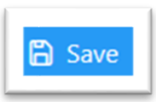
MOBILE HELIX UI SYMBOLS EXPLAINED:



Add (e.g., create a new user, application, etc.)

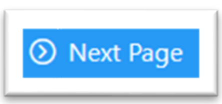
Open item for editing

Delete item

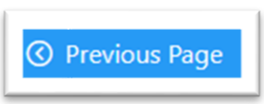


Save item

Go back (without saving) NOTE: do not press the browser back button!



Next page



Previous page

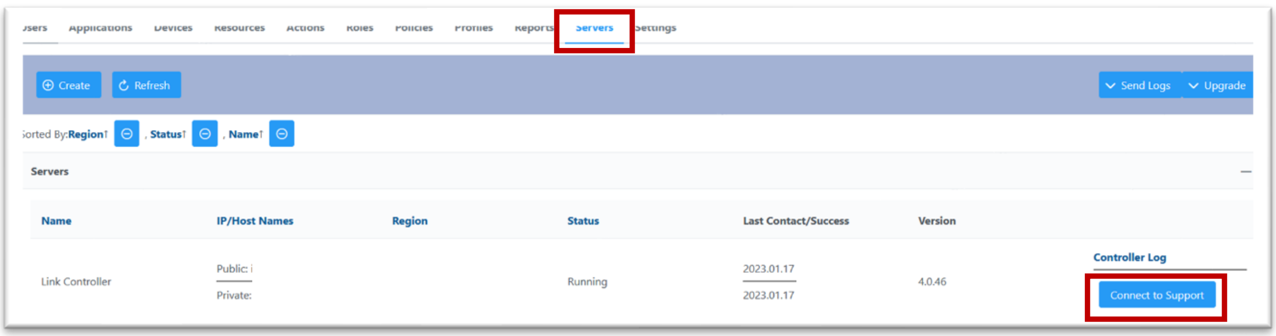
WORKING WITH MOBILE HELIX SUPPORT

The Servers tab provides a portal of support information regarding the Mobile Helix servers, controller logs and support connection to the Mobile Helix support engineer.

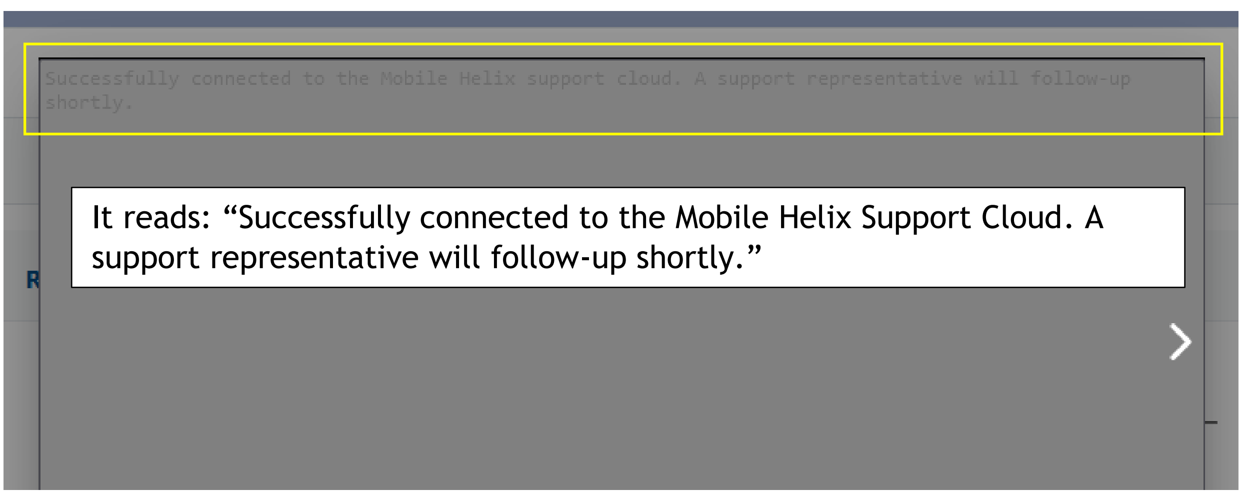
Connect To Support and Send Logs to Support

“Connect to Support” is a feature which allows a Mobile Helix support engineer to temporarily access the Mobile Helix server(s) to perform upgrades or troubleshoot issues remotely. The connection uses SSH and may be started and terminated by the Administrator from the “Servers” tab.

To open a support connection, navigate to the “Servers tab,” scroll to the right if needed, and click the “Connect to Support” button:



If the support connection is successful, Mobile Helix support will receive an email from your system showing the specific SSH port to use to connect remotely:



Click anywhere outside of the message box to return to the “Servers tab” – and note that the button has changed to “Disconnect Support” – use this button to disconnect the support connection when instructed by the Mobile Helix support engineer.

Sending Logs to Support

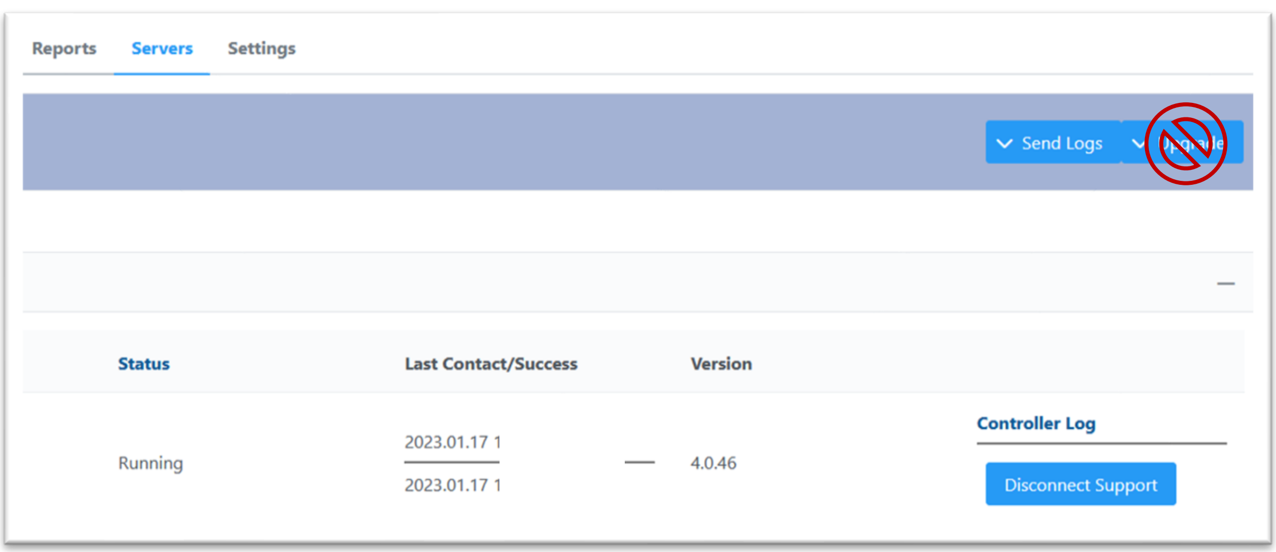
Server logs may be sent to Mobile Helix support from the UI by clicking on the Send Logs button and selecting "All".

Mobile Helix recommends always sending all logs when logs are requested. To select logs for a specific system (the Gateway for example) simply click anywhere on the row being selected. Hold "ctrl" key to select multiple systems (for example Controller and Gateway) although Mobile Helix recommends always sending all logs.

Upgrades

LINK upgrades are conducted via secure remote connection by Mobile Helix Support personnel. The upgrade will be scheduled at your convenience. You will be asked to "Connect to Support" as described above.

Please do not use the Upgrade button in an attempt to perform system upgrades.



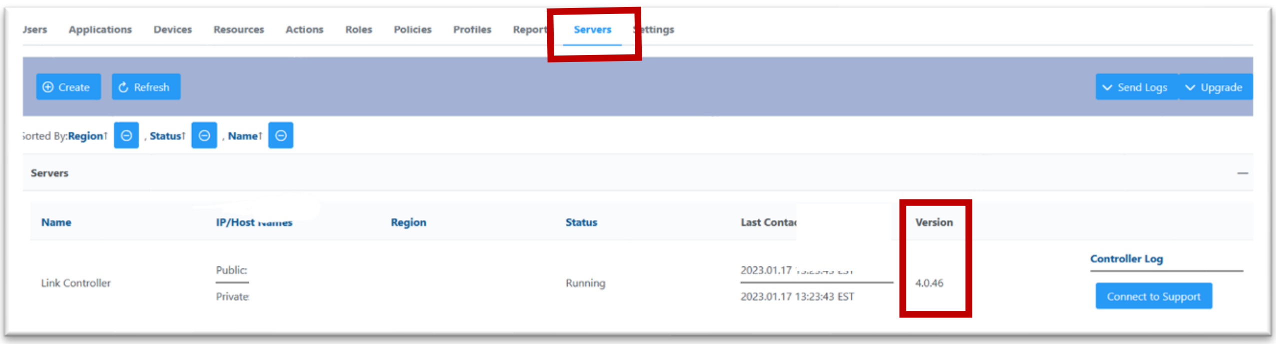
Please contact Mobile Helix support at support@mobilehelix.com, or your named support contact, to discuss upgrades.

Software Version Numbers

LINK Server Software Version - LINK Controller

Go to:

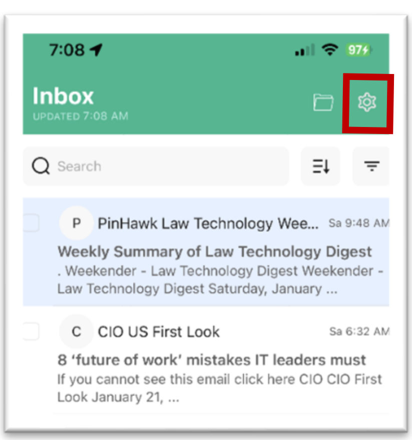
- Servers tab
- Version column – displays version per software component

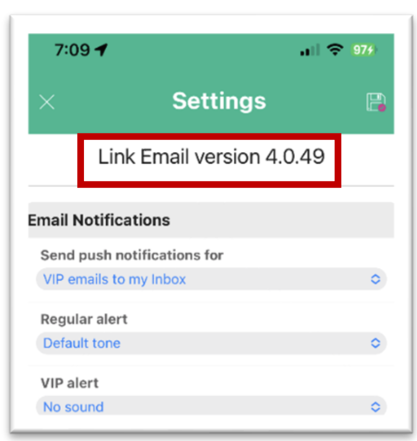


LINK Server Software Version - LINK Client/App

The LINK administrator or support desk may have occasion to verify with the user the version number of the server software being used on the client/LINK app.

Go to the LINK Email Inbox and tap the Gear icon. The version number is at the top of the Settings screen.



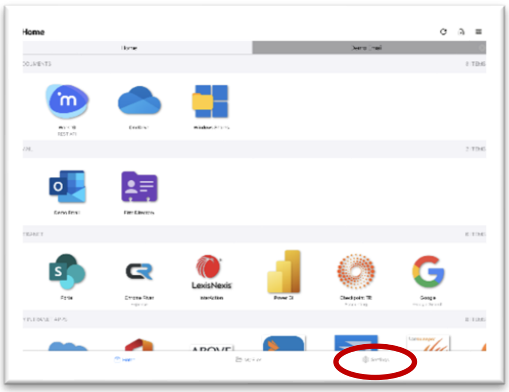


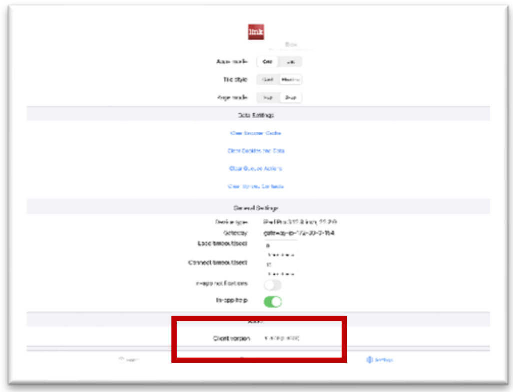
LINK App Client Version

From the LINK home screen, tap Settings.

Scroll to the bottom, to Client Version.

In most cases, this version number should be the version in the App Store.





MANAGING AND ADDING USERS

The default system installation creates only the admin user. Additional users must be added to the system on the **"Users tab"**. Each user must be assigned one or more roles. Three roles are pre-configured in each Mobile Helix installation:

- Administrator, which is reserved for "super users" whose primary responsibility is administering LINK through the Controller.
- Device Users, which is intended for all mobile users provisioned in LINK.
- Installers, which is used internally by other server components to run upgrades with the Controller. This role should not be changed.

LINK uses roles to associate users with a group of applications and a policy. The group of applications defines the user's mobile view. The policy defines the authentication behavior for those users (primary and second factors, authentication timeouts, etc.). In addition, policy profiles are associated with policies to assign app-specific policies to a user session. LINK is preconfigured with sensible policies and profiles that you can configure as needed.

How to Setup AD Sync

Configure the connection with an Active Directory (AD) Group and LINK

1. Login to the LINK Controller
2. Click on the **Applications** tab
3. Search for the application configured with the **'Type' = 'AD Domain Server'**
    a. Usually named appropriately, like 'ADDS', etc.
4. Under the **Active Directory Advanced Settings:**
    a. Provide credentials for a read-only account that can be used to access AD and query the group's membership:
        i. Bind DN for selecting all users/groups or creating users (optional; should include the bind domain e.g., binduser@mobilehelix.com)
        ii. Bind Password for the bind DN
    b. Click the button to **"Enable synchronization between AD groups and LINK roles"**
    c. In the **"Number of minutes in between queries to AD to synchronize groups with LINK roles"** field, configure the amount of time between queries to AD in increments of 5 minutes (the default is set to 30 minutes).

d. Next, find the field titled **'Mapping from AD roles to LINK roles specified as AD Role Full DN (lookup in the attribute editor for the group): LINK Role Name'**

   i. In this field add the Fully Qualified Domain Name (FQDN) of your Active Directory group that has been created for provisioning users in LINK, followed by a colon, and the appropriate LINK role for users in this group.

   ii. **Example:** CN=MobileHelixUsers,OU=Groups,DC=mobilehelix,DC=com : Users

e. **"Mapping from AD roles to LINK roles (specified as above) whose only purpose is to determine group membership. Role mappings in this box will *NOT* trigger user adds or deletes."** This box allows you to specify that, for example, all attorneys in the firm are going to be in a role called Attorneys, but this will not cause all attorneys in the firm to be added to Link. Entries in this box do not trigger adds or deletes, just changes in role membership.

f. To automate the delivery of a launch link to new users, check the box **"Send a launch link automatically when a new user is added by an A-D sync"**

g. To protect against mistakenly moved or deleted AD groups, the number of changes allowed in one sync can be configured by adding a value to the **"Maximum count of changes to allow in any one sync. Syncs exceeding this max are aborted and an email is sent to the Monitor email address. Specify -1 to place no limit"** field.

h. Email addresses can be added to allow administrators to be notified of user adds/deletes.

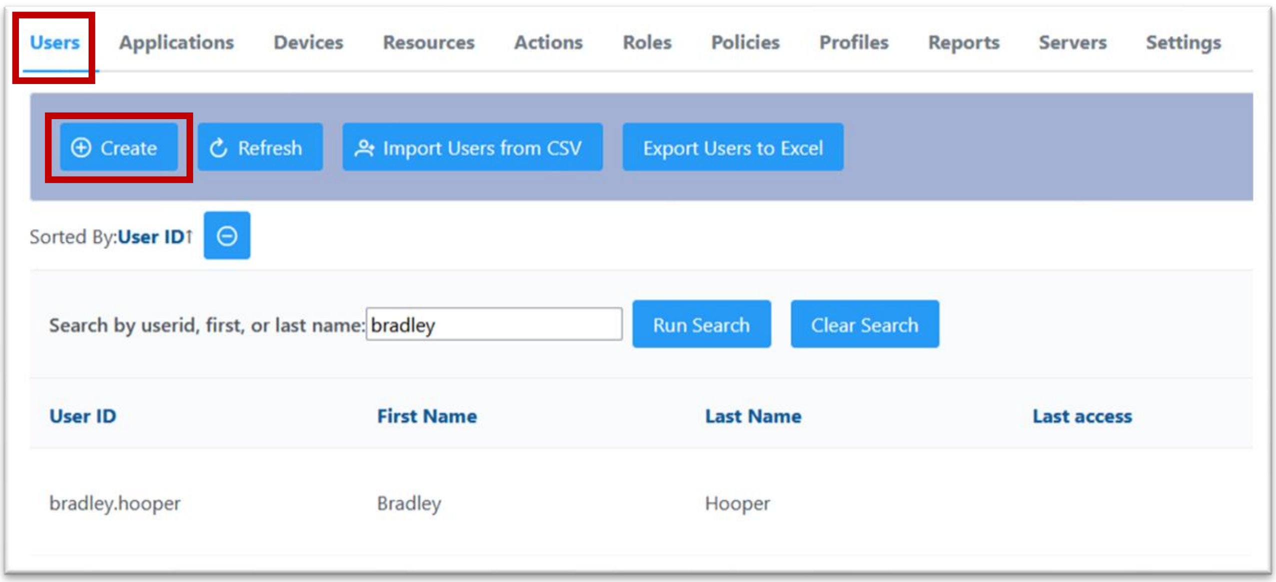
i. The templates for these emails are also customizable in the text areas below.

5. Click **Save**

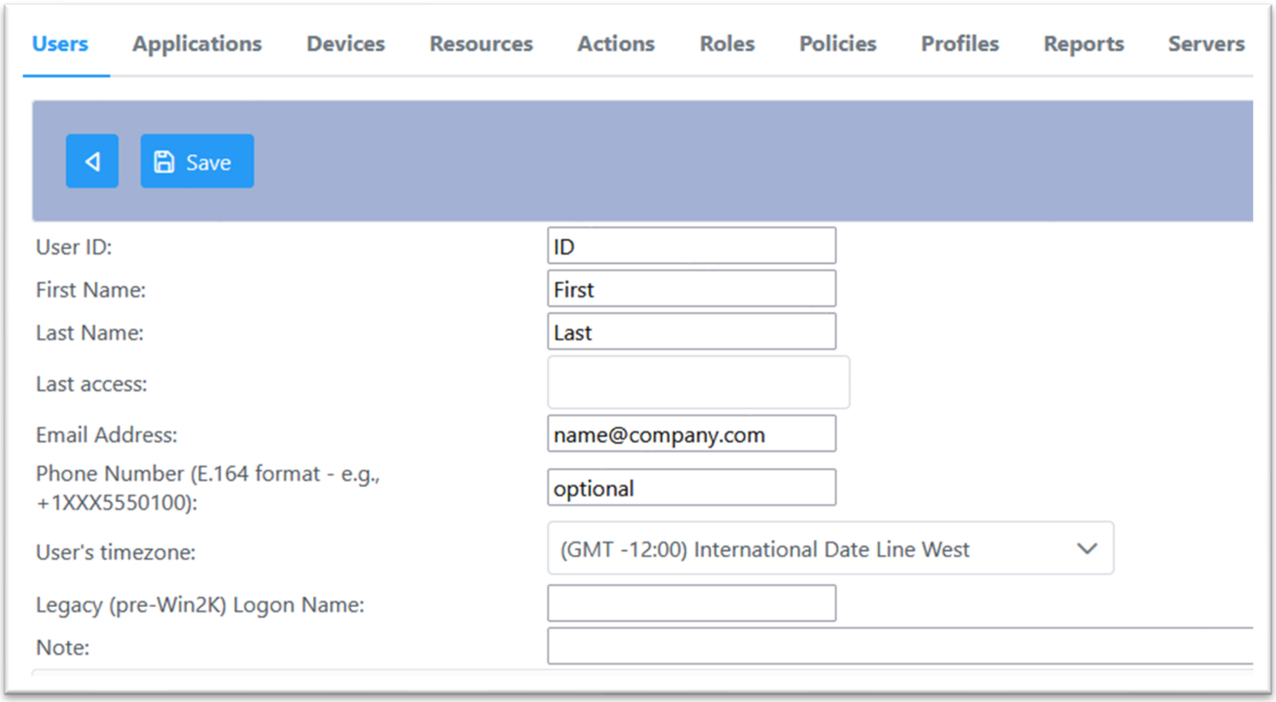
Creating New Users Manually

1. Add the new users to the Active Directory Security Group
2. Based on the sync interval time specified above, the new user will be added to **Users** tab in the LINK Controller with the appropriate role.
3. A launch link will be sent to the user, if configured to do so.

To add a user manually, in the Users tab, click the "+ Create" button.

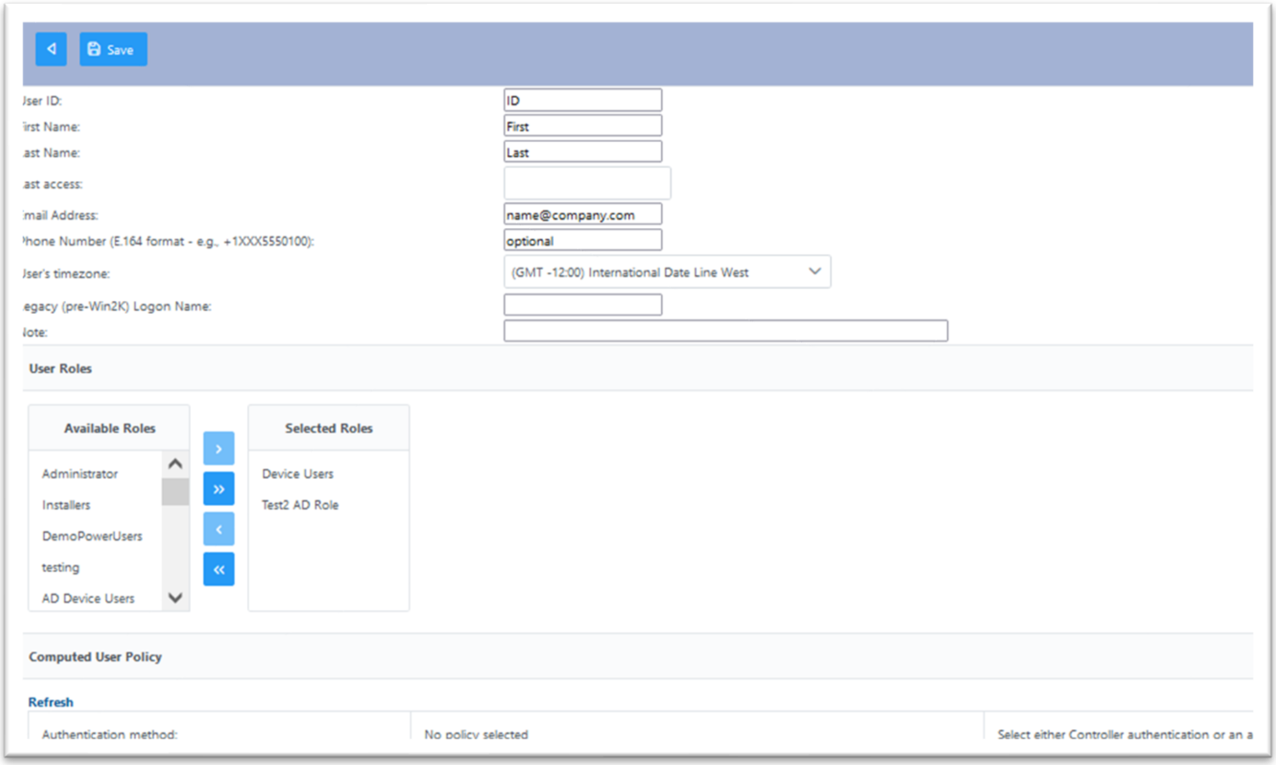


Adding users who authenticate with AD is easy: specify the AD username, first and last name, and work email address.

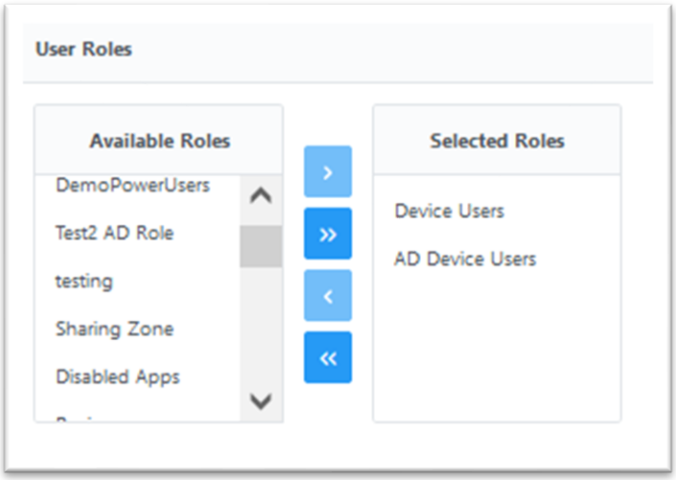


NOTE: __DO__ __NOT__ specify passwords if you intend to use Active-Directory credentials for logon. Most law firms should NOT specify passwords.

First, add this user to the “Device Users” role, which will trigger the “New User Password” panel to disappear.



Now select the appropriate role(s) for this user and click the move to Selected Roles arrow:

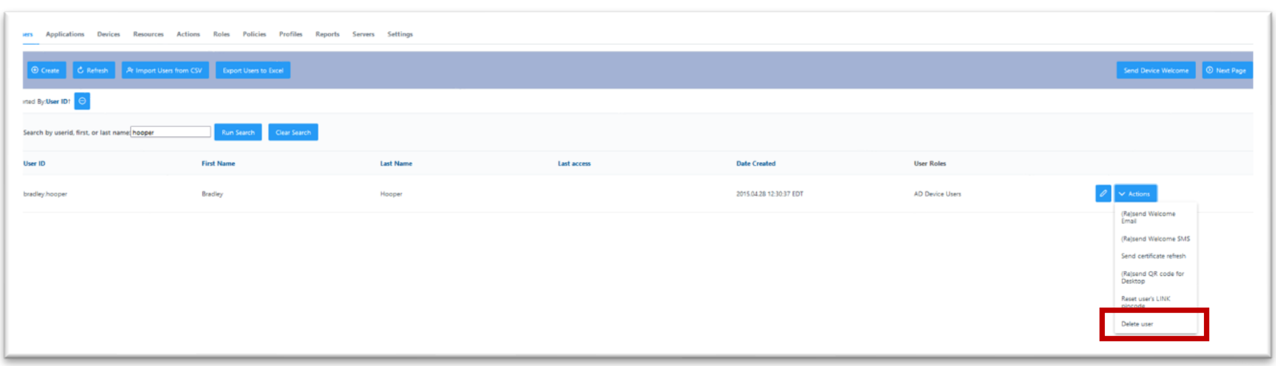


Save the user record by tapping the Save button in the upper left. It can be viewed or edited later.

Delete User

This action item will delete the user account from LINK.

Also ask us about using Active Directory sync, where users will be added or deleted via AD sync.



WAYS TO ACTIVATE LINK

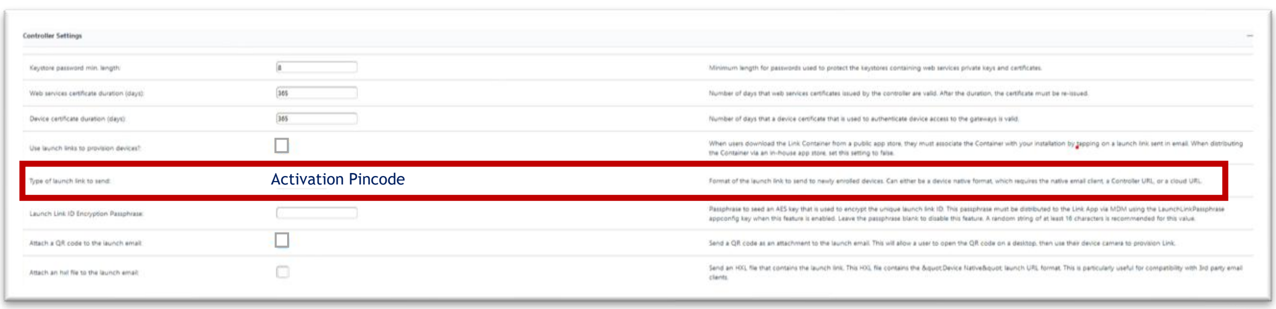
When a new user is first added to LINK, that user's device(s) must be provisioned in LINK. This process is known as "activation," and it involves send the requisite data to the new device to:

1. Tell the device how to find the LINK Gateway
2. Store a controller-signed certificate on the device, which is required to access the Gateway

Activation data can be transmitted to a user via an MDM "App Configuration Policy." This policy is used to send the gateway location and an activation certificate to each MDM-enrolled mobile device. MDM-enrolled devices can then activate Link with a 6-character activation code.

Configuring Code-Based Activation in the Link Controller

Code-based activation is configured in the LINK Controller on the "Settings" tab. The first step is to change the launch link type to be "Activation Pincode" in the "Controller Settings" pane on the "Settings" tab. To do so, change the link type using the dropdown pictured here:



Please make sure that the "Attach a QR code …" and "Attach an hxl file …" are both toggled off.

Configuring Code-Based Activation in MDM

The next step is to create the required "App Configuration Policy" in your MDM solution. The instructions provided here are generic and may be adapted to any MDM solution.

LINK must be distributed via MDM, so the first step is to add the LINK app to your MDM configuration and to distribute LINK from the iOS App Store or the Google Play store. Define the group of users who should receive the LINK app and ensure that this user group matches the group that you have configured as users in the LINK Controller.

Next, create an app configuration profile for the LINK app. The profile parameters are generally specified in XML (on iOS) or in JSON (on Android) as name/value pairs.

For example, the following configuration structure is used for iOS devices:

```
<dict>
   <key>LaunchLinkPassword</key>
   <string>ENTER PASSWORD</string>
   <key>LaunchLinkGateway</key>
   <string>10.0.0.32</string>
   <key>LaunchLinkProxy</string>
   <string>demo.mobilehelix.com</string>
   <key>LaunchLinkPort</string>
   <string>443</string>
   <key>LaunchLinkKey</key>
   <string>-----BEGIN RSA PRIVATE KEY-----
…
-----END RSA PRIVATE KEY-----</string>
 <key>LaunchLinkCert</key>
 <string>-----BEGIN CERTIFICATE-----
…
-----END CERTIFICATE-----</string>
<key>LaunchLinkCACert</key>
<string>-----BEGIN CERTIFICATE-----
…
-----END CERTIFICATE-----</string>
</dict>
```

And the following configuration structure is used on Android devices:

```
{
  "kind": "androidenterprise#managedConfiguration",
  "productId": "app:com.mobilehelix.link",
  "managedProperty": [
    {
      "key": "LaunchLinkPassword",
      "valueString": "ENTER PASSWORD"
    },
    {
      "key": "LaunchLinkGateway",
      "valueString": "10.0.0.32"
    },
    {
      "key": "LaunchLinkProxy",
      "valueString": " demo.mobilehelix.com "
    },
    {
      "key": "LaunchLinkPort",
      "valueString": "443"
```

```
    },
    {
      "key": "LaunchLinkKey",
            "valueString": ">-----BEGIN RSA PRIVATE KEY-----
      …
-----END RSA PRIVATE KEY-----"
    },
    {
      "key": "LaunchLinkCert",
            "valueString": ">-----BEGIN CERTIFICATE-----
      …
-----END CERTIFICATE-----"
    },
    {
      "key": "LaunchLinkCACert",
            "valueString": ">-----BEGIN CERTIFICATE-----
      …
-----END CERTIFICATE-----"
    }
  ]
}
```

For Android, many MDM providers (such as Intune) also provide a user interface for entering individual key/value pairs and generating the JSON configuration. You may use the GUI method for creating the configuration JSON as well.

The parameters to be supplied here are as follows:

1. “LaunchLinkPassword” - Generate a unique password. This should be a long, complex password. Enter the same value in this MDM XML configuration that you enter on the Settings tab in the LINK Controller in the box titled “Launch Link ID Encryption Passphrase” in the LINK Controller.
2. “LaunchLinkGateway” - Enter the public IP address or DNS name of your gateway.
3. “LaunchLinkProxy” – If you are using a DMZ proxy, enter the public DNS name that is routed to the DMZ proxy here.
4. “LaunchLinkPort” – Enter the public port of the proxy here. This will generally be port 443.
5. “LaunchLinkKey” – on the Settings tab in the Controller, scroll down to the Downloads pane. Click on the hyperlink titled “Download a PEM text file with a private key and certificate pair to use as MDM settings for provisioning”. Open this file in a text editor. Copy the RSA Private key portion into the XML configuration.
6. “LaunchLinkCert” – using the same file downloaded in step 5, copy the certificate here.
7. “LaunchLinkCACert” – on the Settings tab, downloads pane, click on the hyperlink titled “Download a PEM text file with the Root CA Cert for this LINK Controller”. Open this file in a text editor, and copy the encoded certificate here.

This configuration profile should be pushed to all users of the LINK app.

Activation by Email

The most common way to activate the LINK app is with an email. This email can be sent to any email account that the user can access, including a webmail (Outlook Web Application) email client. This email contains a 6-character activation code.

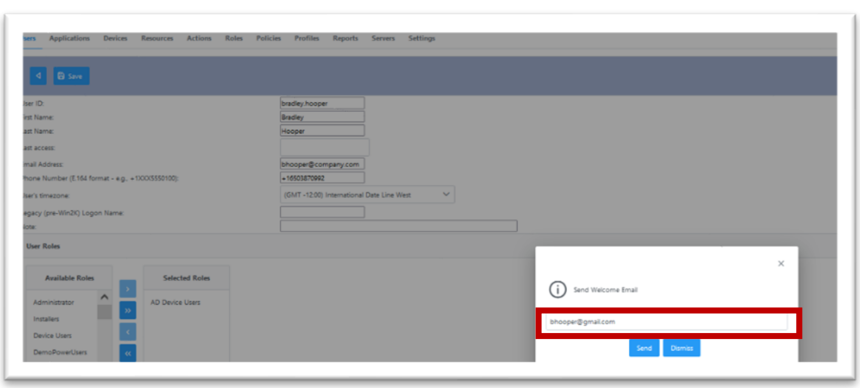
To customize the contents of the email, edit the email template on the Settings tab of the Controller in the pane titled “Provisioning Email”. The “Any Device, Delegated Login” email template is the correct one to edit. The activation code will replace “{0}” in the template email that you write. **This template must be modified, as the default template is designed for hyperlinks not activation code.**

After making any changes to the launch email template, click the “Save” button to ensure that your changes are saved.

Sending Activation Emails to a Personal Address

In general, activation emails are sent to the email address configured in a User’s record on the Users tab in LINK. Selecting “Resend Activation Email” from the “Actions” menu will do exactly this.

However, an activation email can be sent to an alternative address. To do so, simply edit the user record with the pencil icon, then use the “Send Device Welcome” button at the top-right of the screen. This will present a dialog box that allows you to enter an email address. Click send. This email address will not be stored permanently in the user’s record – it is intended as a one-time opportunity to change where an activation email is sent.

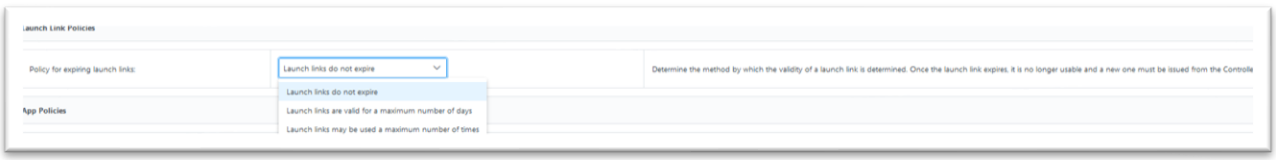


Launch Link Policies

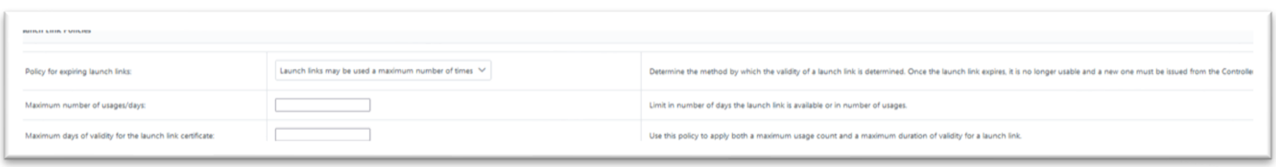
Launch link policies are configured as part of a user's login policies on the Policies tab in the LINK Controller (see first screen shot below). The main policies governing launch links are:

1) Number of permitted usages (i.e., how many times can the user tap on the launch link to activate a device). A launch link that permits multiple usages ***can*** be used on multiple devices. If this is not desired, the usage count should be limited to 1. This usage count limit can be combined with a day limit by setting the expiration of the embedded certificate in a launch link (see second screen shot below).
2) Length of time before the launch link expires. Expired launch links are no longer valid.

Configuring launch link policies on the Policies tab in the Controller:

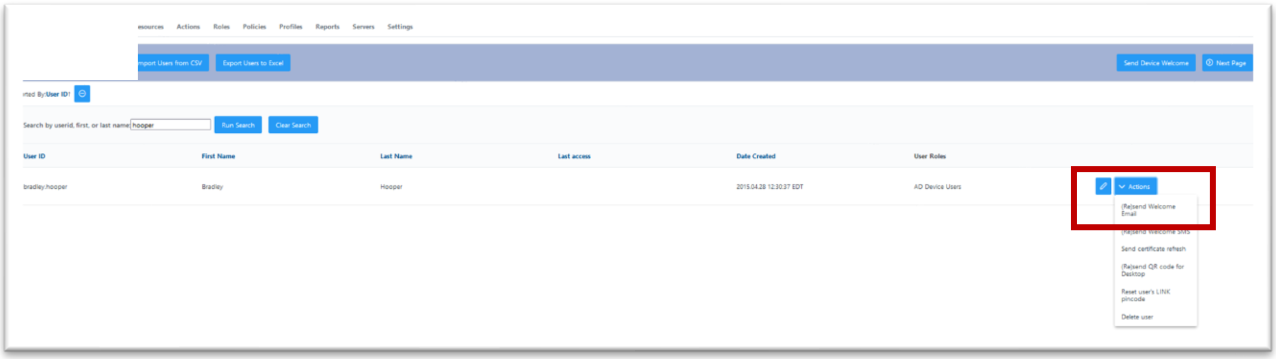


Limiting usages (first text box) and days (second text box):



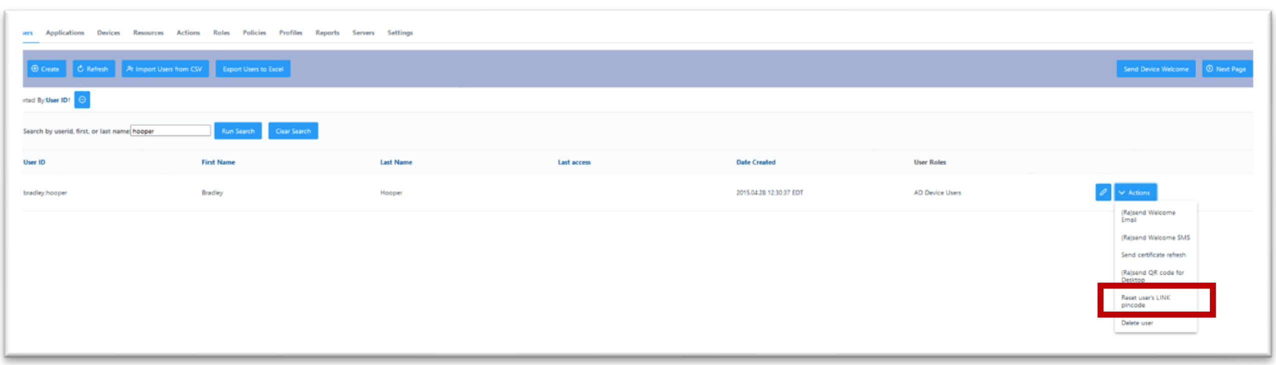
RESEND DEVICE WELCOME EMAIL (LAUNCH LINK)

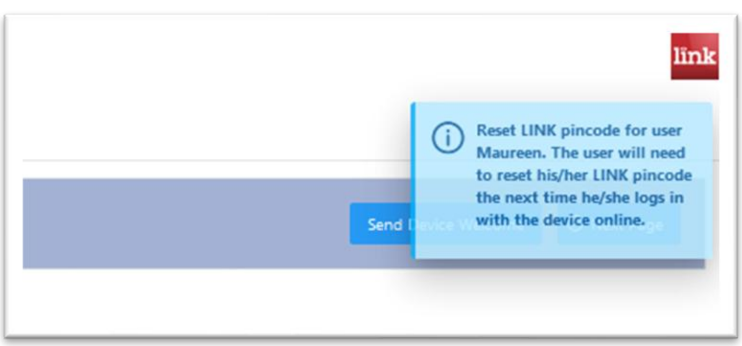
If the user is already correctly set up as above, go to the User ID, click the Actions button, select **"Resend Welcome Email"** button to send the Device Welcome email with launch link to the email in the user's record.



RESET USER'S LINK PIN CODE

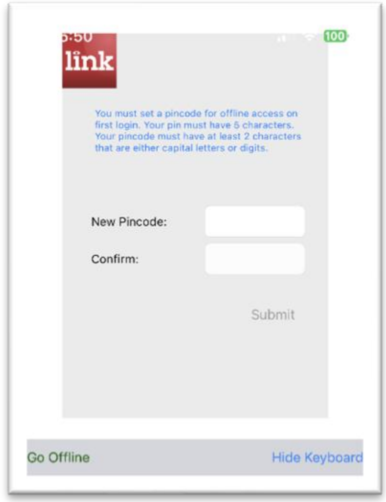
This option is used when a user forgets or would like to reset the pin code assigned to a particular device to access the LINK app. Resetting the PIN code will ask the user to reset the PIN code once they have logged off of their session.





Pincode Reset – User Experience

User is prompted to do an AD Login.



User is prompted to input new Pincode, twice. The Pincode requirement rules are displayed.

CONFIGURING AN INTRANET APPLICATION IN LINK

LINK allows you to mobilize your Intranet by mapping Intranet URLs to tiles that appear on the home screen in the LINK app. Through this mechanism, you can either mobilize an internal site (e.g., your Intranet) or 1 or more important pages within a larger site (e.g., the search page and the directory page in your Intranet).

The LINK browser is generally compatible with any modern web application that does not use any of the legacy “rich-client” web technologies (i.e. Flash, Silverlight). However, LINK’s method for proxying web traffic through the LINK gateway can, in some cases, introduce compatibility issues with some web applications. If you run into any such issues, please consult with Mobile Helix Support as we have a variety of configuration options available to resolve such issues.

All tiles in LNK are role-based, meaning that different groupings of users can see different subsets of the configured tiles. Through this mechanism, you can customize the user’s experience in the LINK app based on his or her role in your organization.

Prerequisites

Mobilizing a web application in LINK requires 3 pieces of information:

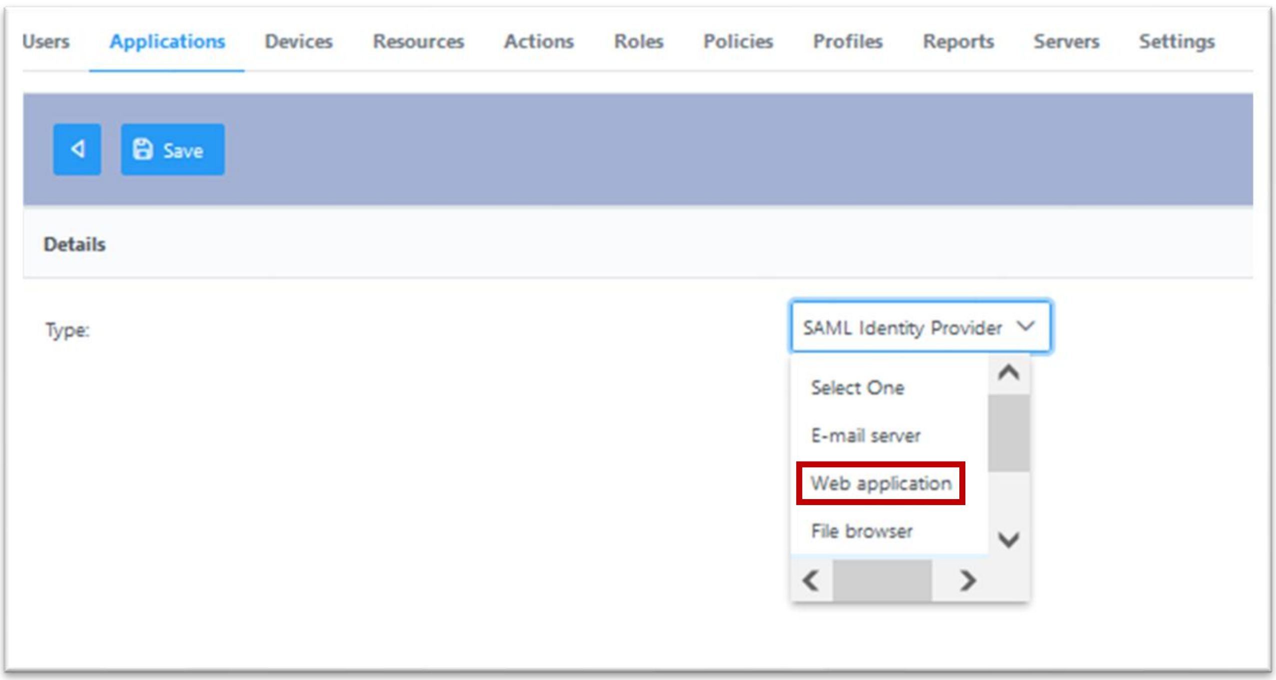
1. The start URL of the application – this is the URL that you want the LINK app to load when the user taps on the tile that you create for this application.
2. A name for this application and any additional descriptive text. This must be concise as space is limited, but it should clearly indicate to the user what the tile mobilizes.
3. An icon, which is used as a simple visual indicator to help the user identify each tile.

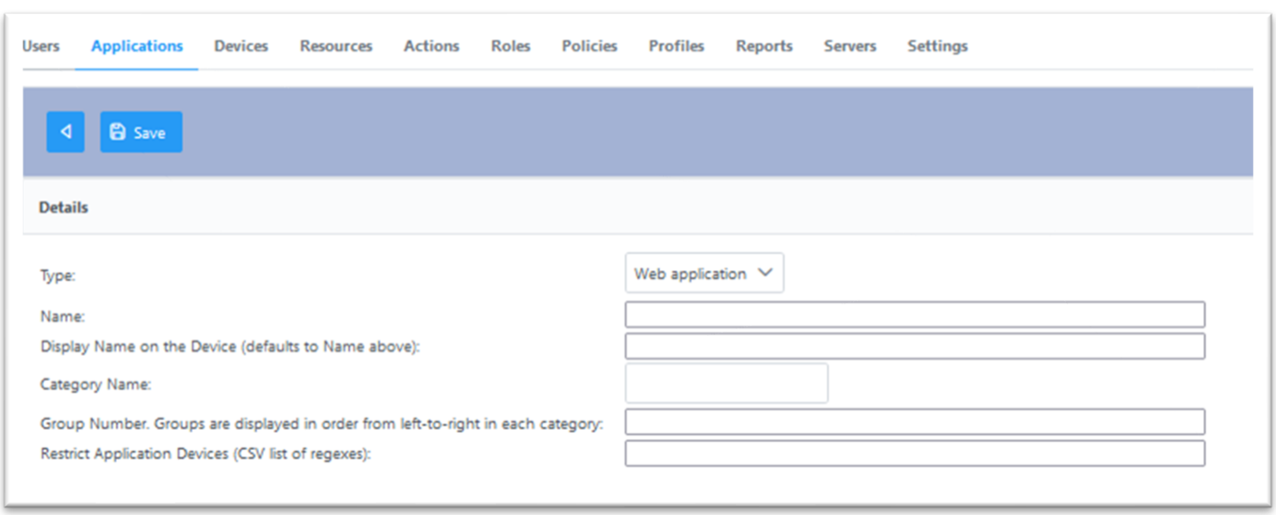
Creating a new Application in the LINK Controller

Application Basics

On the Applications tab in the LINK Controller, click the “+ Create” button.

Select the type as “Web Application”.





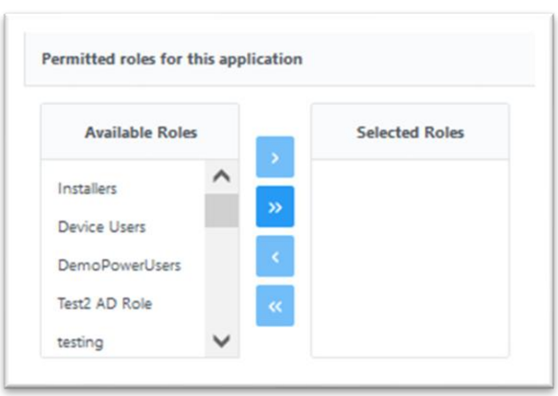
Enter a name for this application, which must be unique within the Controller. If the name you would like to appear at the top of the tile in the LINK app differs from the unique name, enter that in the “Display Name …” field. The “Category Name” (typically row name) is required, and it is used to separate tiles in the LINK app into groupings (with a header in between them). This field will auto-complete to existing categories within the Controller, but you can type a new value here to create a new category (row).

The “Group Number” is used to order this tile relative to other tiles in the same category. Categories are ordered by group number primarily, then alphabetically within each group.

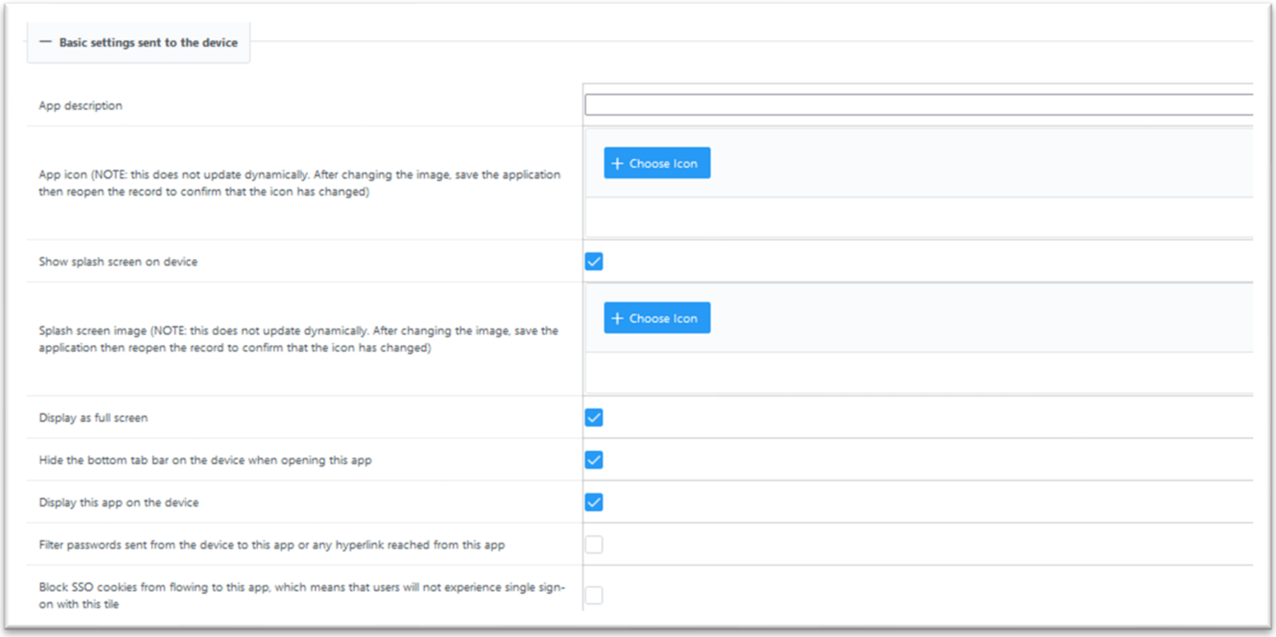
The last field, “Restrict Application Devices”, would be used to introduce restrictions like only displaying a device on iOS vs. Android, or iPhone vs. iPad. Consult Mobile Helix Support if you would like to enable this functionality.

Roles

Next, select the user roles that should be permitted to see this application. Move roles that should see the application from the left to the right box on the page by double-clicking on the role or using the buttons to move list items from “Available Roles” to “Selected Roles.”



Web Application Basics



This section focuses entirely on the display of this application on the device:

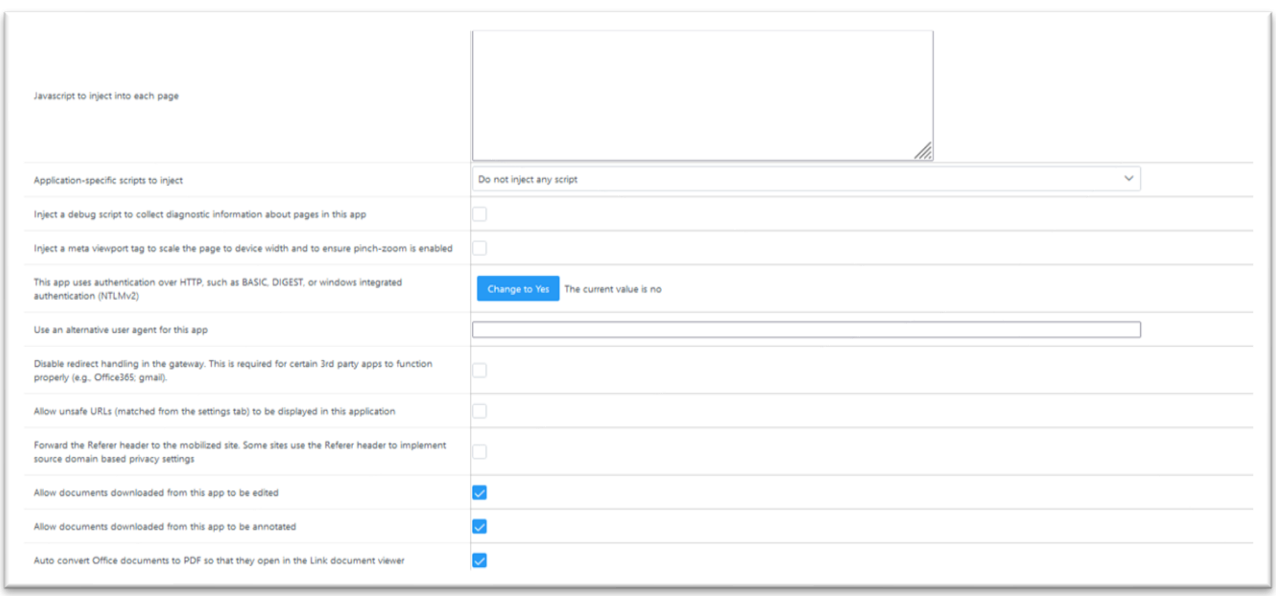
- “App description” is the grey text at the bottom of the app tile in tiles mode, or to the right side of the list in list mode.
- “App icon” is the icon used in the tile or in the list entry in the LINK app. Upload a .png file; recommended 150 X 150 pixels.
- “Show splash screen on device” displays an icon on the loading screen when the app is loading from the network.
- “Splash screen image” is the image to show during loading
- “Display as full screen” should be generally toggled **OFF**. Leaving this toggle on hides the header bar of the LINK Browser, removing the exit button and the back/forward/refresh/stop buttons.
- “Hide the bottom tab bar …” – this is a legacy option. Ignore.
- “Display this app on the device” – toggle this off to hide this app from display on the device without otherwise changing this application record. This is useful when you are testing various tiles and want to temporarily toggle a tile on/off.
- “Filter passwords …” is a security feature that attempts to block users from sending a password to this web application. This feature has limited use cases. Please use in consultation with Mobile Helix Support.

URL

This section specifies what LINK loads when the user taps on the tile for this Application:

- “Full URL …” is the URL to load when the user taps on the tile. Load this page in a desktop browser first and confirm that it is the page that you want a user to see upon tapping the tile.
- “URL filter…” is a feature to allow you to exclude certain parts of an intranet site from mobile access. Contact Mobile Helix Support for more detail.
- “Show address bar …” determines whether a text box is shown in the LINK browser with the URL that the user is currently browsing. Users can also type a new address in the address bar to browse to a different address.

Advanced Settings



These settings are used to customize the load behavior of a web application or to modify the load behavior of that application:

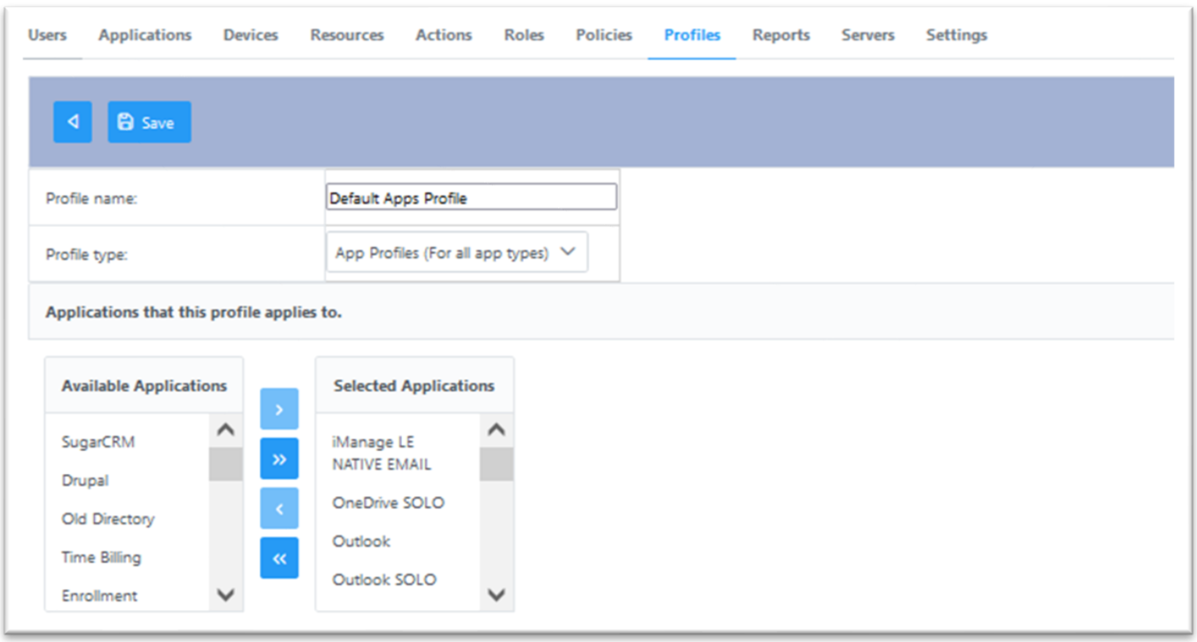
- “Javascript to inject …” allows for the injection of custom javascript into a web application page. Consult Mobile Helix support before using this option.
- “Application-specific scripts to inject …” allow for the injection of scripts that are shipped with LINK to enhance the compatibility of specific web applications. Again, consult with Mobile Helix support before using this option.
- “Inject a debug script …” is a useful way to debug web applications when you are working with a support representative.
- “Inject a meta viewport tag …” tells the browser to scale the width of a loaded page to the device width. Most applications already include this viewport tag, so leave this option off unless you have consulted with support first.
- “This app uses authentication over HTTP …” toggle this to “on” for IIS applications that use “Windows Integrated Authentication” to automatically authenticate users without any additional sign-on.
- “Use the newer …” this is a legacy option for older versions of the LINK app. Ignore.
- “Use an alternative user agent …” is useful for applications that reject the user agent sent to the application by the LINK app. In such a case, open the desktop web browser that you normally use to access this web application. Browse to google.com, and enter the search query “my user agent”. Copy the value in the “Your user agent” box into this text box in the Controller.
- “Disable redirect handling …” is an option that you can use to try to fix an application that is not loading correctly in LINK. Use in consultation with support.
- “Forward the Referer …” by default LINK does not forward the Referer header to mobilized sites. Turn this on only in the case that a mobilized site requires it.
- “Allow documents downloaded from this app to be edited” allows an Office Document downloaded from this app to then be edited using LINK’s local “Open In” edit method.
- “Allow documents downloaded from this app to be annotated” allows a PDF or a converted Office Document downloaded from this app to be annotated with LINK’s PDF tools.
- “Auto convert Office documents to PDF …” enables the automatic conversion of all Office Documents and text files to PDF so that they open as annotatable PDFs in the LINK Documents viewer. This toggle must be “on” for the “Allow documents …” toggles to work correctly.

When you are done working through all options in the Application record, click “Save” in the blue header bar to save this application record.

Assign the New Application to a Profile

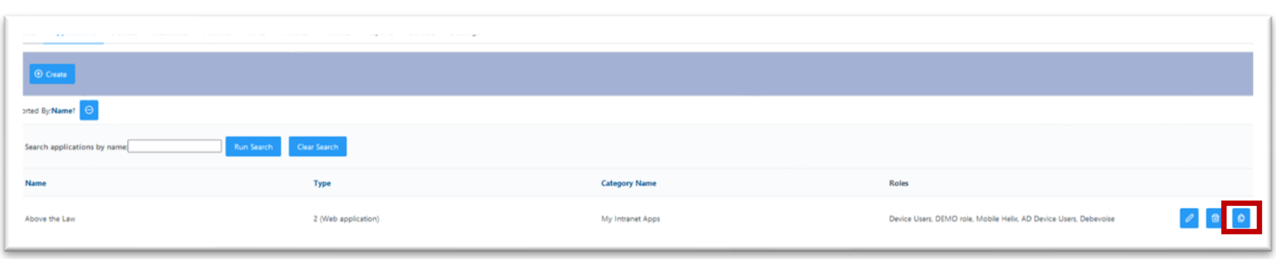
After creating an Application in the LINK Controller, the final step is to assign this application to the “Default Apps Profile” profile on the “Profiles” tab in LINK. Profiles apply an additional set of feature restrictions to an app. In advanced configurations, profiles may be customized to different user roles.

Edit the “Default Apps Profile” and move the app that you just created from the “Available Applications” to “Selected Applications” by double-clicking on it, or by using the arrow buttons.



Copy An Application Setup

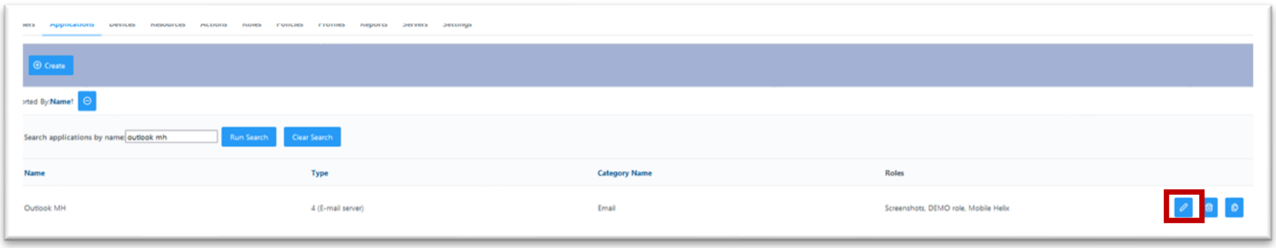
From the Applications tab page, identify another web application. Use the copy button, right-most in the application listing, to duplicate your Application record.



How to change an application tile image

This pertains to the Applications tiles on the LINK Home Screen

1. Login to the LINK Controller
2. Go to the Application Tab
3. To the right of the target application, click the Pencil to edit.



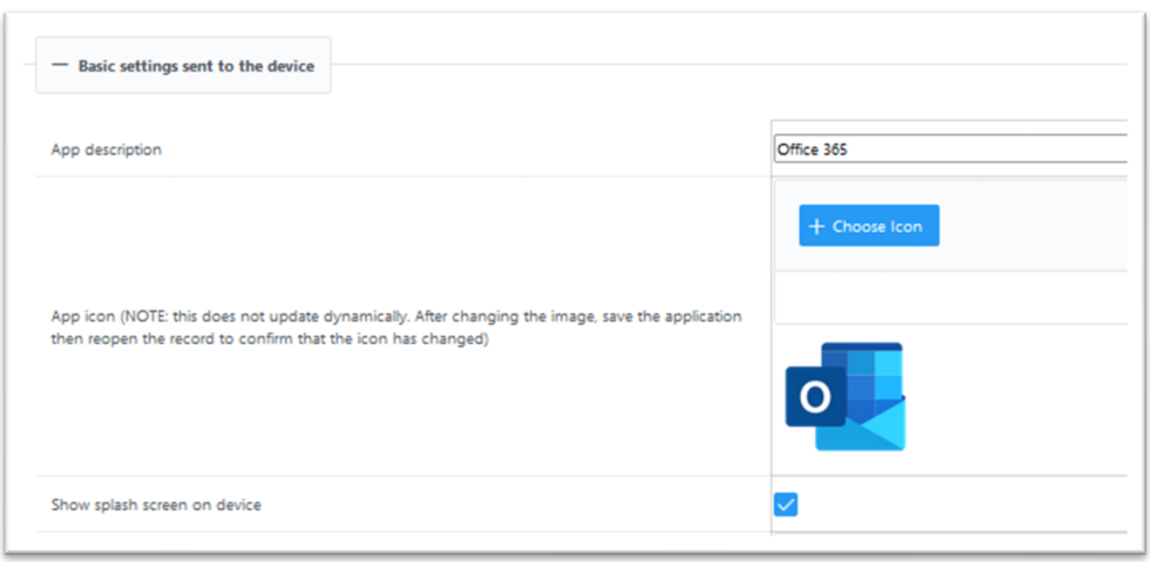
4. In Basic Settings, App Description, Click "+Choose icon"
5. Upload .png image.

Ideally choose a file in the range of 150 X 150 pixels.

Transparent .png files are recommended to achieve the floating look.

Note, you may not see the image change in the LINK Controller after uploading.

You must Save first. Use the button in the upper left.



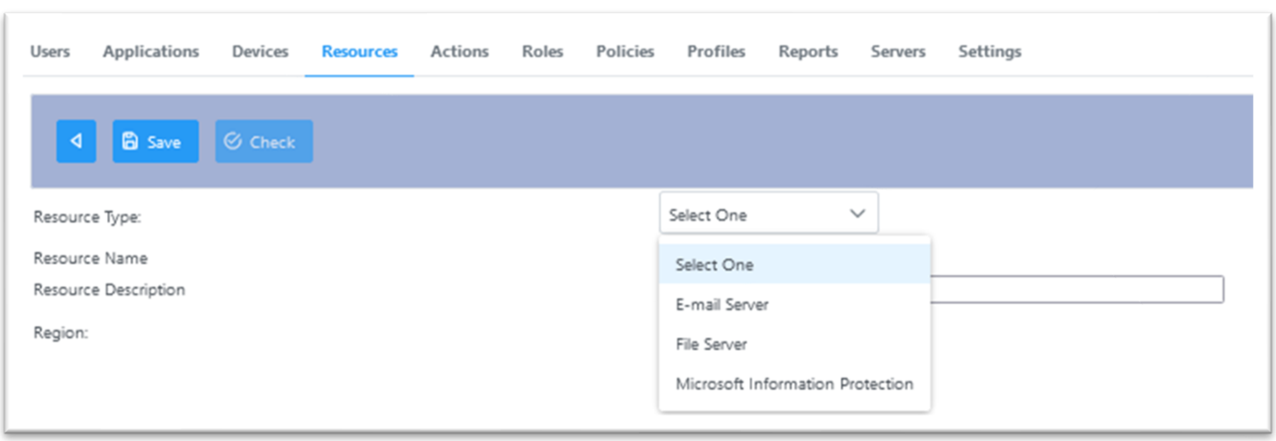
EMAIL AND FILE ACCESS

In addition to proxying Intranet applications, LINK allows users to access their company email and a variety of file repositories from a mobile device. Supported email servers include both M365, cloud-based Exchange, and on-prem Exchange 2013+. Supported file repositories include:

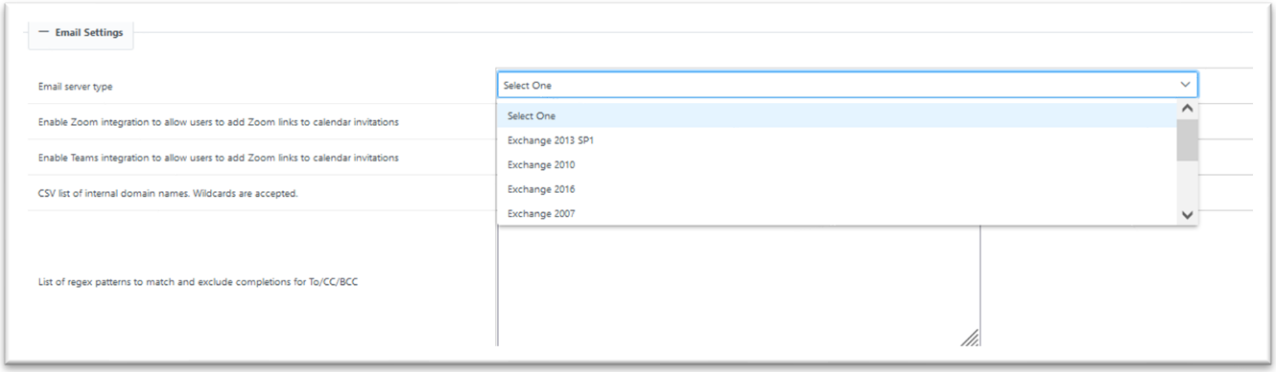
- iManage Work
- NetDocuments
- OpenText eDocs
- Microsoft Windows File Shares
- Microsoft OneDrive
- Amazon S3

Mobile Helix is an official partner of iManage®, NetDocuments, and OpenText to provide licensed, API-based access to documents stored in those repositories via our LINK app.

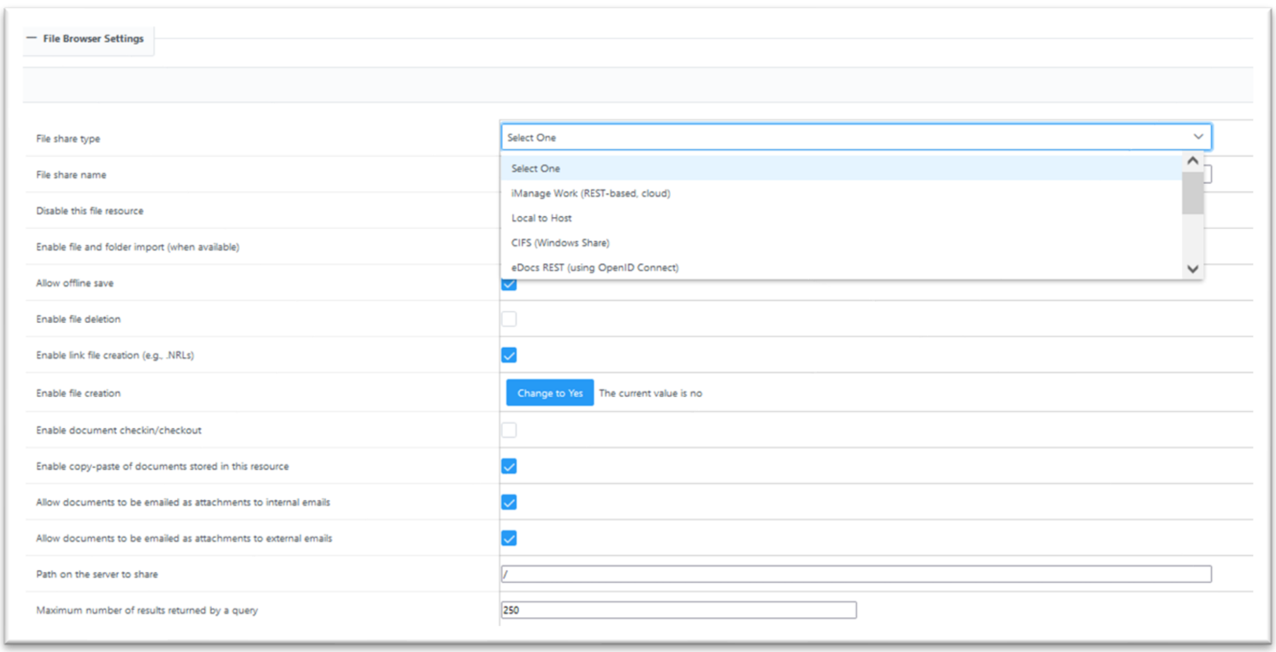
To configure email or file access in LINK, the first step is to create a resource on the Resources tab corresponding to the external service that LINK is connecting to. Click the "+" on the Resources tab, and select from the options in the image below:



After choosing “E-mail Server”, select the target Email server from the available options:



After choosing “File Server”, select from the following options:

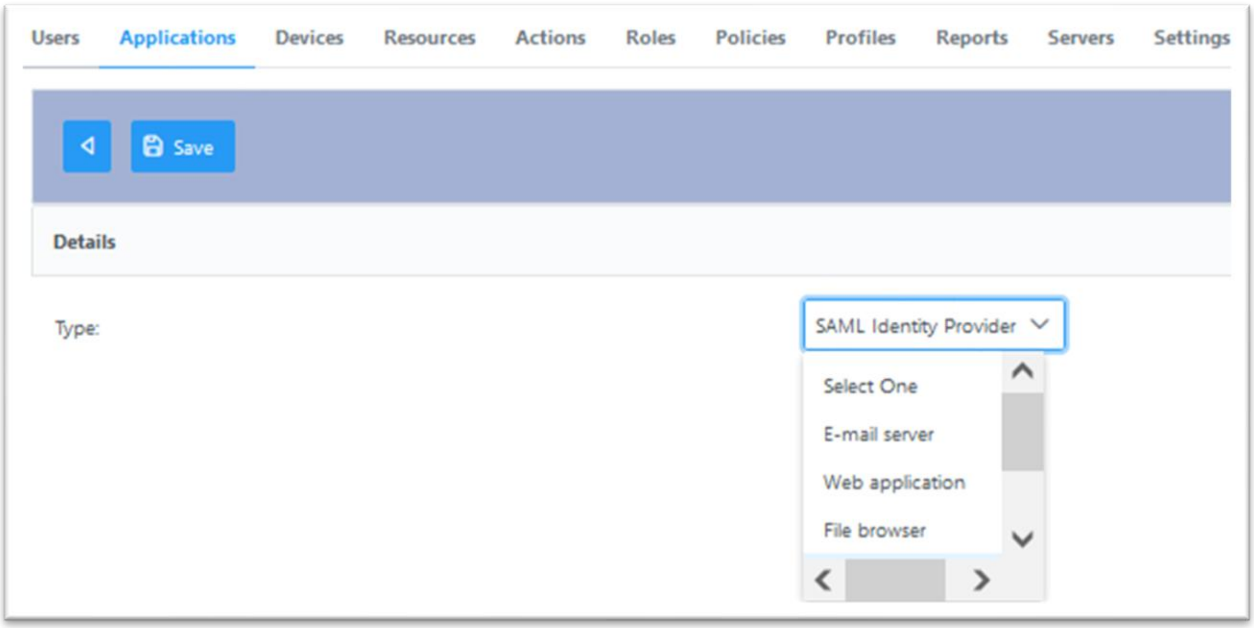


Once the resource type is selected, the remainder of the page will populate with options that are specific to the setup requirements of that external resource. A full documentation of those options is outside the scope of this document.

After a resource is created for the external email or file server, the next step is to create an Application that will correspond to a tile that appears in the LINK app. This tile will be assigned a name, an (optional) description, and an icon to determine how it renders in the LINK app. Tiles are also grouped by Category.

Application configuration is specified on the Applications tab, and the "+ Create" button in the upper left initiates the creation of a new Application record.

After clicking on the create button, select the type of application to create from the available options:



Choose either "E-mail server" or "File browser." Then assign this application to one or more Roles, which determines the subset of LINK users who will see this tile in the LINK app. Application records must also be assigned a name and a category so that LINK knows how to render them in the app. Finally, assign the resource for the appropriate external service to this application. All other settings should be left with their default values unless specified otherwise in a conversation with Mobile Helix Support.

The final step in configuring an email or file browsing tile is to assign this tile to the appropriate profiles on the Profiles tab. Profiles are used to provide role-specific overrides to the default behaviors of a given Resource. For example, editing can be disabled for a specific group of users by using a Profile, or push notifications in email can be enabled/disabled for a specific user group.

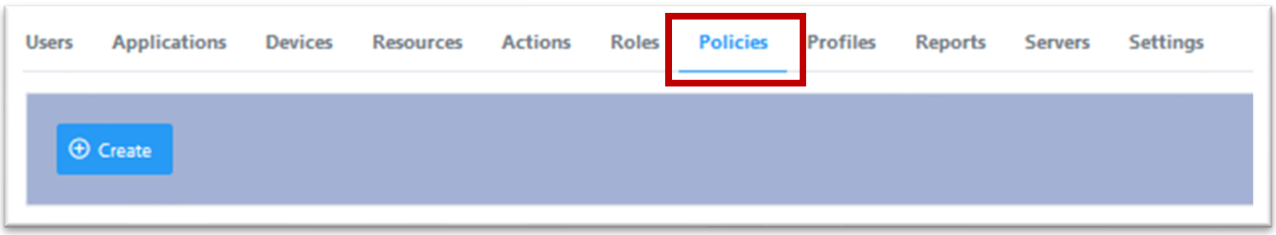
Profiles are specified on the profiles tab. There are 4 profile types:

1. Profiles that apply to all applications
2. Profiles that apply to all devices
3. Profiles that apply only to email applications
4. Profiles that apply to file browsing applications

Depending on the type of application created, either assign the new application to profiles of types 1 and 3 or types 1 and 4. This assignment will ensure that all of the appropriate settings are specified for the new application tile.

ONLINE POLICIES

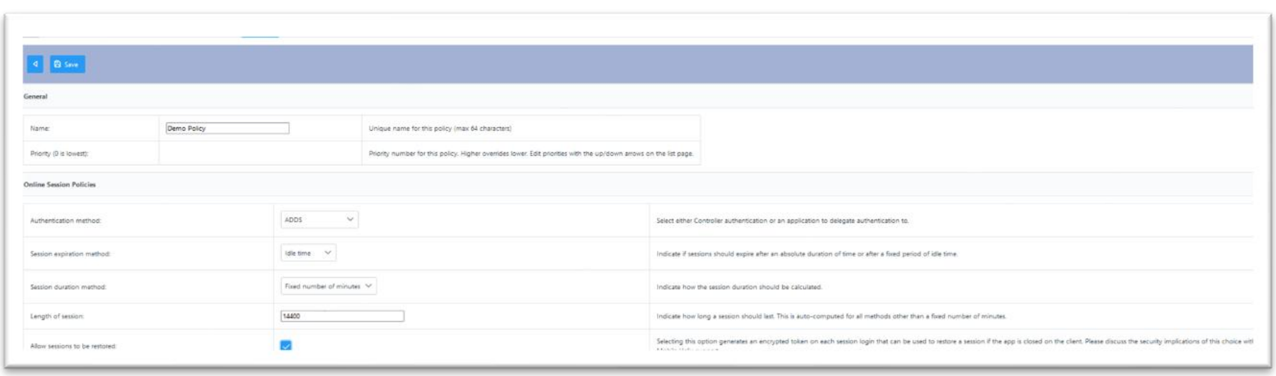
In the LINK Controller, go to the Policies tab.



First Factor Authentication

When a user signs into LINK from a completely signed out state, the Controller creates a server session for that user. When that session terminates, the user must log in again with AD credentials as well as a second factor, if one is configured. The server session may terminate if the server is upgraded or restarted, if the user selects to log out from the LINK app, or if the session expires based on the policy. See brief tutorial below, “Full First Factor Tutorial.”

Change AD login frequency: **Browse to the box entitled "Length of session:" This field indicates the number of minutes a user will be idle before they are forced to login again with their AD credentials. Input number of minutes and SAVE.**



Full First Factor Tutorial

Refer to image immediately above.

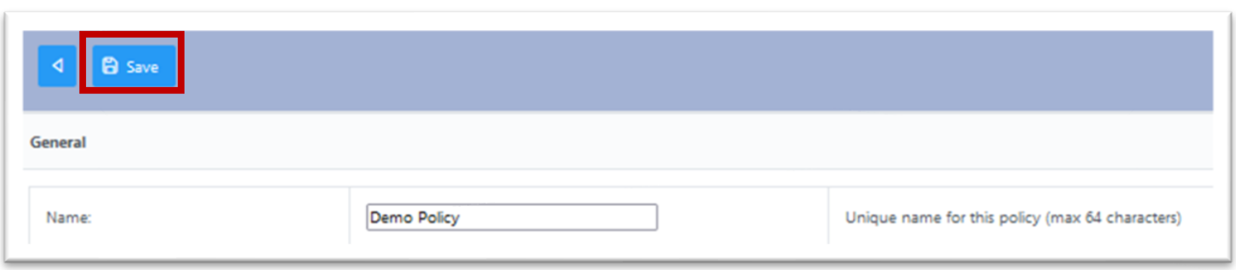
Authentication method: Setting should be LDAP/ADDS. In rare instances, the Controller may be asked to authenticate users – only use this with guidance from Mobile Helix Support.

Session expiration method: Commonly select "Idle Time." Sessions may be expired based on idle time (how long has the LINK app not been in use) or absolute time (timer counts down whether the app is in use or not)

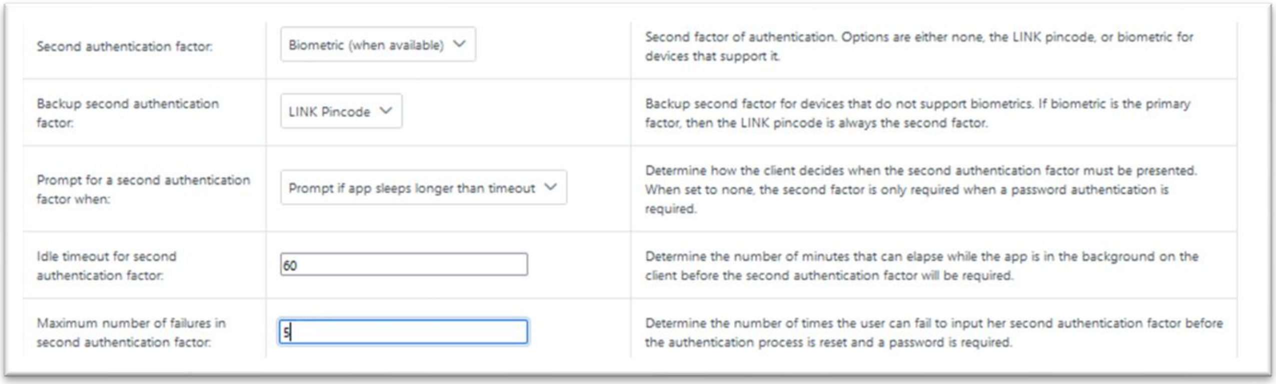
Session duration: Commonly select "Fixed number of minutes." Fixed number of minutes/seconds or end of each day is repeatable and predictable. End of the week or month is not – consider what happens if a new user is activated on a Friday – they will have to re-enter their password 2 days later, and then every 7 days. Select whichever setting makes sense for your organization and user base.

Allow sessions to be restored: Commonly check this box. While the server session will be active as specified in the above settings, the local device session will terminate when the app is removed from memory by the underlying OS. Allowing sessions to be restored will enable the client to seamlessly restore the session from the server without prompting the user – again this is governed by the settings specified above, so if the client attempts to restore a session but the server session has terminated because of the session duration settings, then accordingly the user will be prompted to log in again.

Save: Tap the Save button.



Second Factor Authentication



LINK supports Touch ID, or Face ID, or PIN code as second factor authentication settings. If enabled, the biometric ID or PIN code must be provided each time the user provides their AD credentials. However, the recommended approach is to create a long online session time, and then use the biometric ID or PIN code to log into LINK without having to always enter the AD password.

Change Second Factor login frequency: Browse to the box entitled "Idle timeout for second factor authentication." This field indicates the number of minutes a user will be idle before they are forced to login again with their Second Factor credentials. Input number of minutes and SAVE.

Consider this example: set the first factor online session to expire after 60x24x7 = 10080 minutes (one-week absolute time) but have the second factor session expire when the app sleeps for longer than 30 minutes.

The user will have to enter their AD credentials and biometric ID (or PIN code) once a week. However, during that week, if LINK is inactive for more than 30 minutes they will only have to provide their biometric ID (or enter a short PIN code) to get to their email, DMS, etc.

Save: Tap the diskette icon.

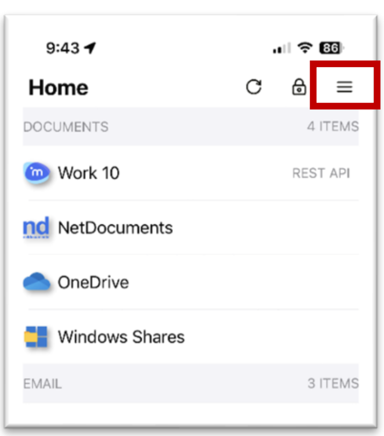
NOTE:

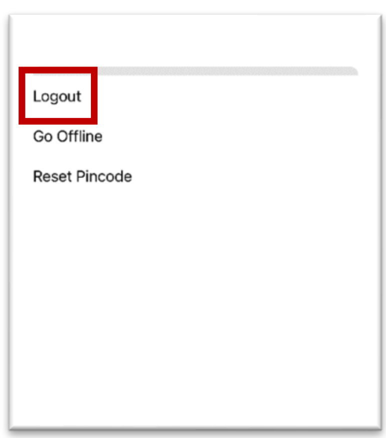
Any Changes to Authentication Policies Require a Full User A-D Logout

For authentication policy changes to take effect users must logout. Users must be in a new server session to receive new session policies. There are two options for this logout.

1. **"Logout All"**
   Force all users to logout. Do this from the Devices tab. See image below.

2. **Full AD Logout**
   An individual user may log out from their device. From the LINK app home screen, tap the 3 bars menu in the upper right. Select logout. Now, fully login with first and second factors.



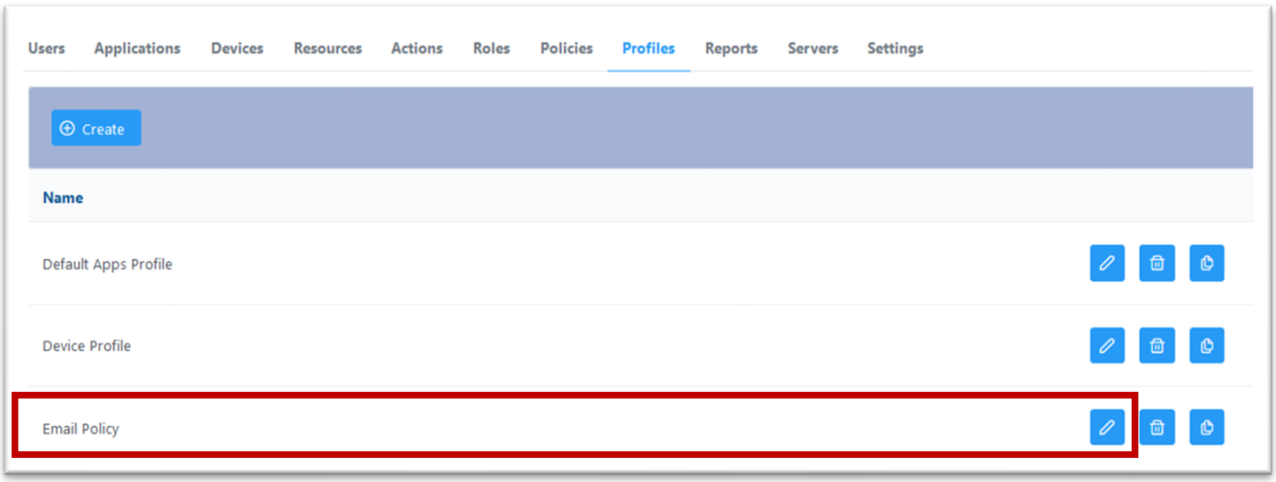


Email push notifications & settings

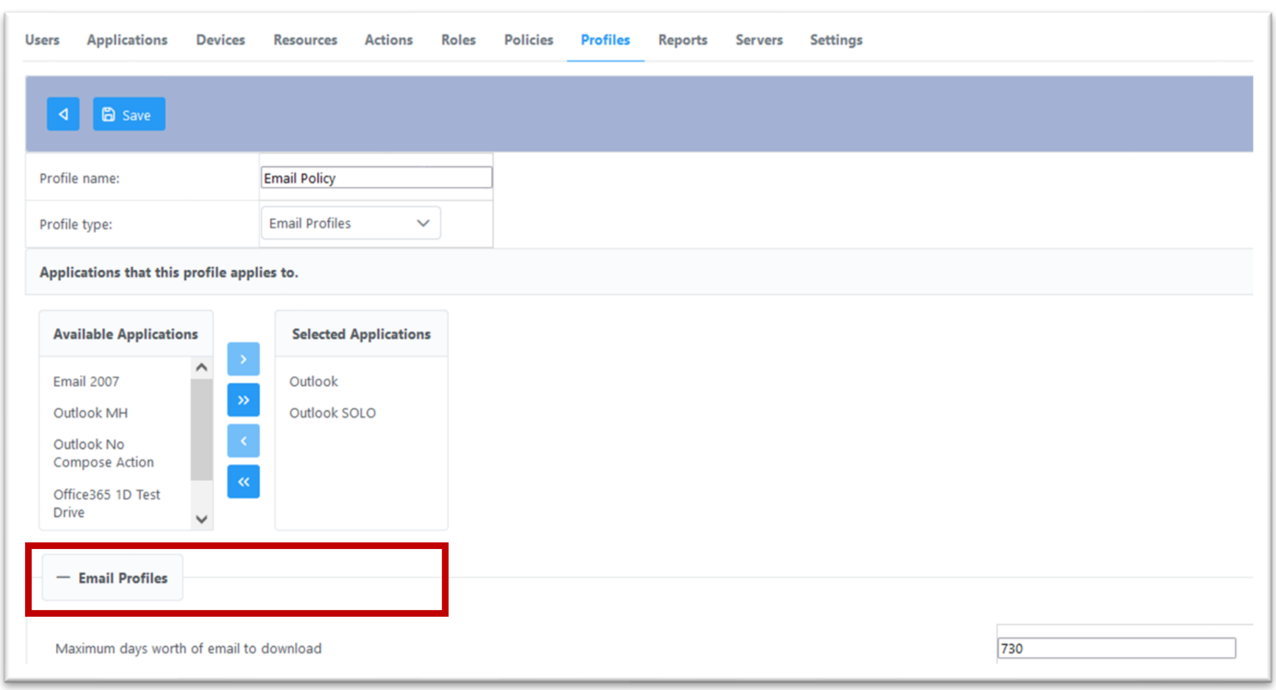
LINK can be set to provide email push notifications and 6 options. As these settings have a security policy ramification, they are set by the LINK admin in the LINK controller.

To configure email push notifications:

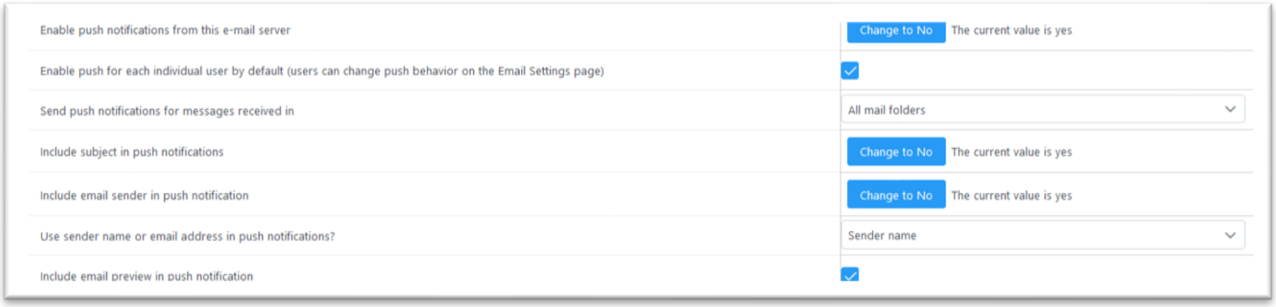
- Go to the Profiles tab in the LINK Controller
- Select Email Policy. Tap Pencil.



Go to "Email Profiles" section.



Go to “Enable push notifications from this e-mail server” and set it to, “The current value is yes or no.”



When push notifications are set to yes, there are six options:

1. Enable push for each individual user by default: Check as on/off.
2. Send push notifications for messages received in: Select from dropdown menu either “All mail folders” or “Inbox only.”
   Note: Users can change push behavior on the Email Settings page. See below.
3. Include subject in push notifications (Yes/No)
4. Include email sender in push notifications (Yes/No)
5. Use email address or sender name in push notifications? Select from dropdown menu either “Email address” or “Sender name.”
6. Include email preview in push notifications: Check as On or Off.

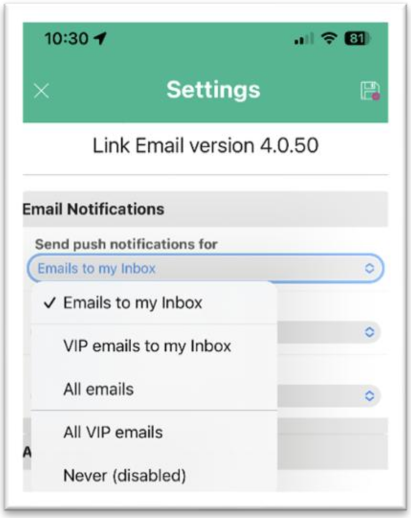
Set options as preferred.

Tap the Diskette icon to Save.

User Action to View Controller Option Change

For the user to see this change, the user the user must do a “Full AD Logout” from the three bars menu in the upper right on the LINK home screen. Then log in again.

User Options for Push Notifications from the Device



If Push Notifications are set to “On” in the LINK Controller, the user can further manage their personal push notification settings.

To access user options for push notifications:

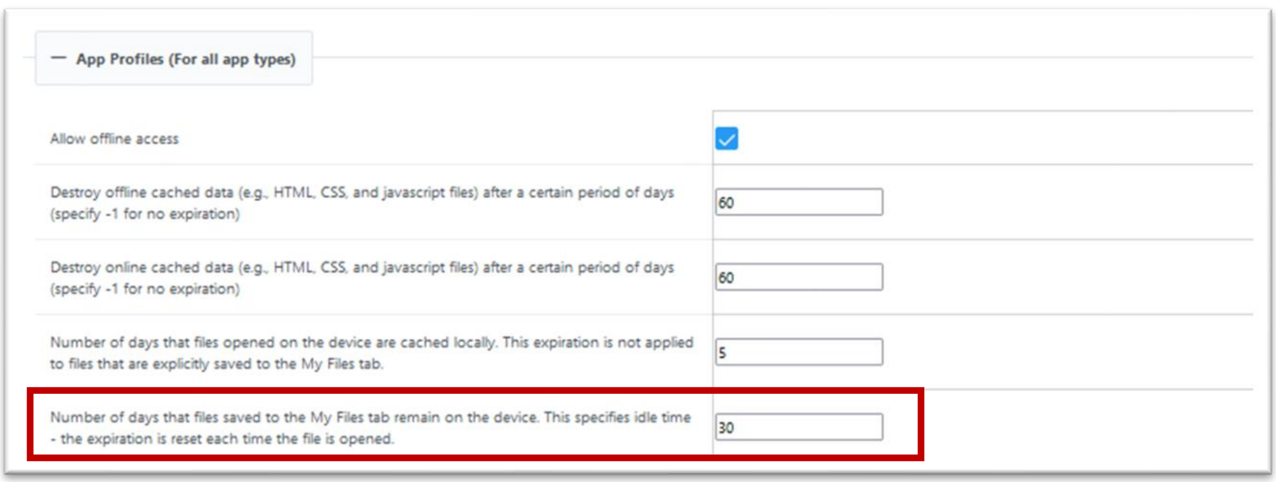
- From the Email Inbox
- Tap the Gear icon
- At “Send push notifications for” tap the up/down carat
- Select one of the options displayed
- Tap the Diskette icon to save

To be clear, the individual user may also go to the device OS Settings to manage LINK app notifications (if they are turned on in the LINK Controller). The user can turn off notifications for LINK as with any other app.

CHANGE EXPIRATION FOR FILES IN “MY FILES”

“My Files” provides encrypted local storage of files within the LINK secure container. The default setting for file expiration is 30 days. This is 30 days of *idle* time, which means that every time the user opens the doc and does something with it, the 30 day counter resets. Hence, the document only expires after 30 straight days of not touching it at all.

You can change the global policy (or you can assign different policies to different user groups, if appropriate) on the "Profiles" tab in your Controller. You should have a profile usually called "Offline Profile." Edit that profile (with the pencil button to the far right), and you will see a field labelled "Number of days that files saved to the My Files tab remain on the device. This specifies idle time - the expiration is reset each time the file is opened." This is the setting that determines the expiration period.



Note: When you change this setting and save your change, users will not see this change until: (i) they login to a fresh session by entering their A-D password in the LINK app, and (ii) they download a new file. This policy change is not applied retroactively to files that are already downloaded, and we do not dynamically change the policies of existing user sessions.

CHANGE DOWNLOAD FILE SIZE

Downloading large documents may take a long time or fail on a poor network. This may create a poor user experience.

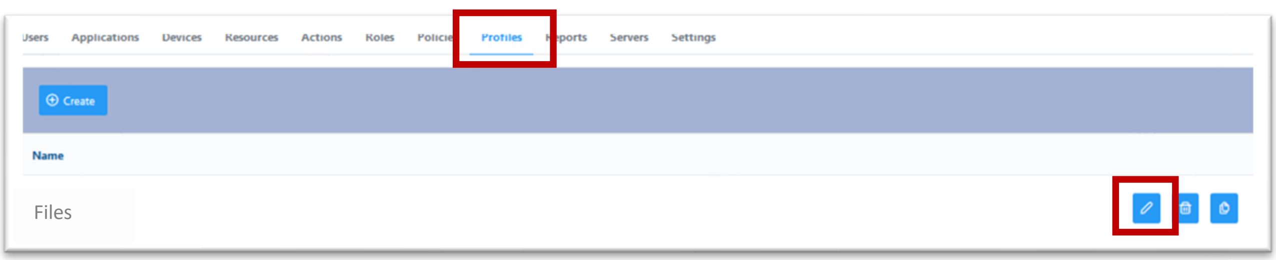
LINK provides a warning when a user tries to open/download a large file.

There are two pertinent settings which you can change in the Controller.

1. Warn user when they try to download files greater than this size (in MB).
2. Do not allow users to download files greater than this size (in MB).

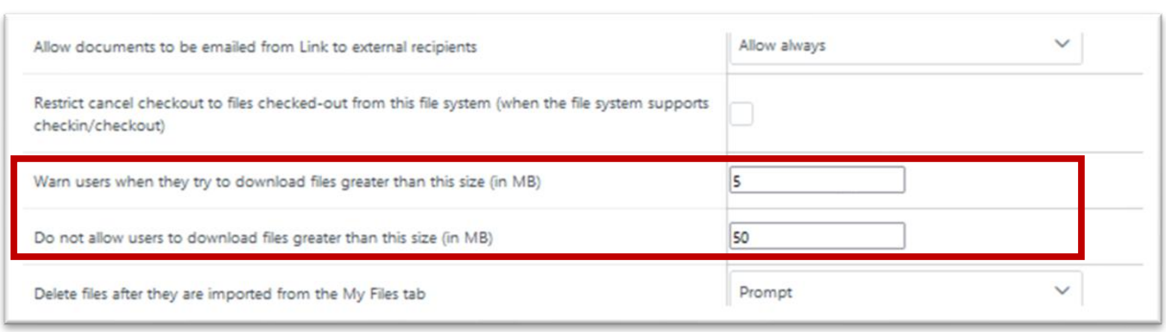
To change these settings, go to the Profiles tab.

At Files, tap the pencil icon.



Change settings as shown below. Tap the Diskette icon to save.

Users will have to logout via the three bars menu in the upper right in the LINK app to start a new session with the changes active.



USER SUMMARY REPORTS

This guide shows how to generate the most commonly used report – number of users.

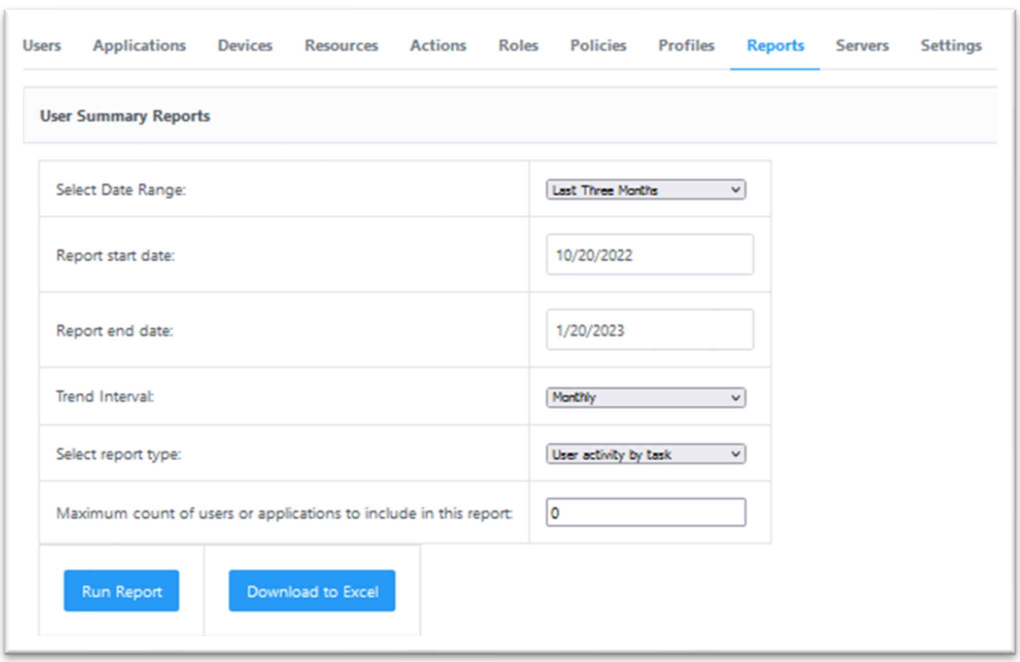
You can generate many more reports from this screen as well.

Start in the LINK Controller.

- Go to the Reports tab.
- Date Range: Set for the period you want to measure active users. We suggest using either 3 months from the drop down, or manually set to 6 months.
- Trend interval: Monthly
- Select report type: “User activity by task”
- Maximum number of users to include in this report: Don’t change
- Select: “Download to Excel”

You can readily tally the number of users in Excel.

Example of settings:



MICROSOFT AZURE MIP INTEGRATION WITH LINK

Create an App Registration in Azure

Login to your Azure portal at https://portal.azure.com. To create a new App Registration, search for “App Registrations” and click on the service when it appears. Once you have opened the “App Registrations” panel:

1. Select “New registration” in the top-right of the screen.
2. Select “Accounts in this organizational directory only” for the account types.
3. Choose “Public client(mobile & desktop)” as the redirect URI type.
4. Enter mobilehelix://auth in the input box.
5. Click “Register”

After clicking Register, you are redirected to the page for your new App Registration. On this page, you must add an additional redirect URI, create a client secret, and add the required API permissions.

Before proceeding further, capture the “Application (client) ID” and the “Directory (tenant) ID” from this page. Both will be used as configuration parameters in the LINK Controller.

Add an Additional Redirect URI

From the app registration page for your new app, add a new redirect URI by clicking the link next to “Redirect URIs:”.   Toggle on the checkbox next to https://login.microsoftonline.com/common/oauth2/nativeclient for the redirect URI.

Click “Save” at the bottom of the screen.

Add Required API Permissions

Next, add API permissions to your app registration. To do so, click “API Permissions” in the “Manage” section on the left panel of the page.

(See https://github.com/Azure-Samples/MipSdk-Dotnet-File-ServicePrincipalAuth for the original source):

Azure Rights Management Services

1. Click API permissions.
2. Click Add a permission.
3. Select Microsoft APIs.
4. Select Azure Rights Management Services.

Permission Type	Permissions Required
Application permissions	1. Content.DelegatedWriter 2. Content.Writer

Microsoft Information Protection Sync Service

1. Select Add permissions.
2. Again, Select Add a permission.
3. Select APIs my organization uses.
4. In the search box, type Microsoft Information Protection Sync Service then select the service.

Permission Type	Permissions Required
Application permissions	1. UnifiedPolicy.Tenant.Read

Grant Admin Consent

1. Select Add permissions.
2. In the API permissions blade, Select Grant admin consent for and confirm.

Add a Client Secret

Finally, click “Certificates & Secrets” in the “Manage” section of the left panel of the page. Click “+ New client secret” to create a new client secret. Add a descriptive name for this secret and select an expiration. **NOTE: you will be responsible for creating a new secret before the current secret expires, and for updating the LINK Controller configuration accordingly.**

Before you leave this page, click the copy button to the right of the secret value that is shown in the second to last column. Capture this value as you will need it in your LINK Controller configuration.

Configure LINK to use MIP

Browse to the Resources tab in LINK and edit the file resource for which you would like to enable information protection. Scroll down until you find the option that says “Enable Azure MIP protection when editing files”. Click “Change to yet” to enable Azure MIP integration. Doing so will reveal the following configuration parameters:

Parameter	**Description of Value**
Azure Tenant ID	Directory (Tenant) ID captured during the app registration
Email address of a tenant administrator (e.g., admin@mobilehelix.com)	As described. This email is used as the sign-in identity when LINK authenticates with Azure using the client secret
App ID for the Azure MIP App Registration	App (Client) ID captured during the app registration
Client secret for MIP service access	Client secret used for authentication with the MIP REST APIs
Email address of the owner for MIP-encrypted files	To protect files while they are being edited with Office for iOS, LINK applies MIP encryption using the owner email address provided here, and grants Read/Write permission to the signed-in LINK user. This allows the user to manipulate the document in Office for iOS without granting the user the ability to alter the permissions in any way.

After these parameters are entered, click the “Save” button in the blue bar in the LINK Controller. Tap the refresh button on your device to ensure that these changes are propagated into your active LINK session.

Once enabled, checkout-and-edit should trigger the encryption of this document. The checkin process should strip away these MIP protections on the server side.

DEPLOYING THE LINK APP WITH MICROSOFT INTUNE

The LINK app can be distributed to your users via the Intune Mobile Device Management system. To do so involves the following steps:

1. Add LINK as an app in Intune and deploy it to your target user group
2. Ensure that LINK can share documents with the Office apps for iOS
3. Ensure that only Intune Managed Devices can register with your LINK installation

Add LINK as an app in Intune and deploy it to your target user group

Login to https://endpoint.microsoft.com, your Intune management console. Under "All Services" or "Favorites", select "Apps". Click "All Apps", "Add" … and select the following:

- iOS Store App for the App Type
- Search the App Store for "Mobile Helix LINK"
- Set "iOS 13.0" as the "Minimum Operating System"
- Determine which groups will be required to install LINK, and which will have LINK available on enrolled devices
- Review and create the app

LINK should now be deployed along with all other MDM Managed Apps to your Intune Company Portal. For groups that are "Required" to deploy LINK, the LINK app should be installed automatically on those devices.

Ensure that LINK can share documents with the Office apps for iOS

To edit documents and to import documents authored in the Office apps for iOS, LINK must be able to share documents with the Office apps for iOS. When using an Intune App Protection policy to add additional policy restrictions to the Office apps for iOS, the "Send org data to other apps" must allow document sharing to LINK in order to permit users to author documents in Office for iOS, then upload them to DMS or email them via LINK. Because LINK is not specifically integrated with Intune, this setting should be "Policy managed apps with OS sharing".

In addition, the setting "Receive data from other apps" must allow LINK to send data to apps governed by an App Protection policy. Choosing "All apps" or "Any app with incoming org data" for this setting should enable LINK to share files with the Office for iOS apps.

Ensure that only Intune Managed Devices can register with your LINK installation

To prevent users from downloading LINK from the public app store and using a registration email to configure LINK on an unmanaged device, LINK can deploy an encryption secret to your

MDM managed devices that is also used to encrypt a unique identifier placed in each launch link. Only managed devices will then be able to unlock that unique identifier and authenticate it with your LINK installation.

To create such a shared secret, first generate a random string that is at least 16 characters long. A convenient way to do so is with a password manager or secret server. Login to the LINK Controller, and on the settings tab add this secret into the field that says “Launch LINK ID Encryption Passphrase:”

Next, create an “App configuration policy” in Intune to deploy this secret to all managed devices. Select “Add … Managed Devices”. After selecting iOS and LINK on the basic settings page, enter the configuration settings as XML:

```
<dict>
   <key>LaunchLinkPassword</key>
   <string>yourpasswordhere</string>
</dict>
```

In the XML above, replace “yourpasswordhere” with the 16-character random string that is also placed in the Controller on the Settings tab. Ensure that the “Assignments” for this app configuration match the assignments that are selected for the LINK app.

After entering this password on the Settings tab in the LINK Controller, launch emails will only be valid on Intune-enrolled devices.