Administering Jive Mobile Apps

Contents

Administering Jive Mobile Apps

Setting up the Jive side of the apps may not require any configuration at all. However, there are some configuration options including a choice of authentication modes, and you can also enable and disable connections from Jive's mobile apps to your site.

Configuring Jive for Android and iOS

No Jive-side configuration is required to use the apps, unless you can't or don't want to use your Jive installation's SSO setup to authenticate Mobile users.

Fastpath: Admin Console: Mobile

In general, if you have licensed Jive Mobile, you don't need to do anything to let your users download the Mobile app from the App Store and get started. By default, the Mobile app will use whatever authentication method you've set up for your Jive site, and you can use the default settings for push notifications. Here are some situations where you might want to do further configuration:

- You have an SSO configuration for your Jive site that you can't or don't want to use with Mobile. For example, if your sign-in page for SSO is on a VPN (and not accessible to mobile devices), or SSO timeout policy is mobile-unfriendly, you should read the section on Authenticating with Mobile Apps and consider your options.
- You want to distribute a customized or wrapped version of the app.

Enabling and Disabling App Connections

You can enable and disable access from the current generation of native apps with Mobile 3, and you can also decide whether you want users who try to access Jive through their mobile device's browser to be automatically redirected to the app.

Note: Previous versions of the Jive native apps, which were compatible with Jive 6.x, are not supported for Jive versions after Jive 7, and people with these apps installed will need to uninstall them and install the current Jive for iOS or Jive for Android app

To control access to your community using the Jive native apps:

1. To disable or grant access from users via the mobile app, clear or select **Allow access from standard Jive Mobile apps (versions 3.0+) published by Jive**. Note that users will still be able to use your community from a mobile device using the responsive web interface.
2. To make sure users are prompted to use the native app instead of the browser when they try to log in from the browser on a mobile device that supports it, select **Prompt web users on compatible mobile devices to launch the native Jive Mobile app**. Users who haven't yet downloaded the app will be prompted to install it.

Authentication with Mobile Apps

With Jive 7 and Mobile 3, Jive Mobile apps support OAuth 2 as both an Authorization Server and a Resource Server. This enables several new authentication methods. Basic authentication is no longer supported.

Authenticating with Standard OAuth

When you have the Jive for iOS or Jive for Android add-on installed through the Jive Add-ons interface, standard OAuth is the default configuration.

In previous versions, Jive used basic auth as an authentication option for mobile apps. As of Jive 7, we use OAuth2 with the username/password grant. When users enter a username and password on the mobile device, all subsequent API calls go through OAuth instead of basic auth. This authentication method is much more secure, because the username and password are never stored on the mobile device.

If you also have SAML SSO enabled on the instance, and you prefer to use OAuth rather than SAML for mobile authentication only, please refer to "Forced OAuth for Mobile Only," below. If you want Mobile users to authenticate through SAML SSO, but you prefer different timeout settings for mobile devices, see "Initial Authentication Through SAML Followed by OAuth."

1. Under your name or avatar, select **Add-Ons**.
2. Make sure the Jive for iOS or Jive for Android app add-on is installed and enabled. `If you are using an on-premise version earlier than 7.0.1, or your instance isn't connected to the Internet, you may need to contact Jive Support to install this add-on.`
3. Next to the app listing, click the gear icon and select **Settings**. Then click **Advanced**.
4. If necessary, adjust the **Access Token** and **Refresh Token** timeout settings. The default settings are 48 hours for the Access Token and 15 years for the Refresh Token.

Authenticating with SAML SSO

When your Jive instance is configured with SAML SSO, Jive's Mobile apps will follow the same authentication flow as the regular web UI.

Mobile detects whether SAML SSO is enabled by making a call to *yourcommunity*/api/version as shown in the following example:

```
       throw 'allowIllegalResourceCall is false.';
                {
                "jiveVersion" : "7.0.0.0 ",
                "jiveCoreVersions" : [ {
                "version" : 2,
                "revision" : 3,
                "uri" : "/api/core/v2",
                "documentation" : "https://developers.jivesoftware.com/api/v3/
rest"
                }, {
                "version" : 3,
                "revision" : 4,
                "uri" : "/api/core/v3",
```

```
                "documentation" : "https://developers.jivesoftware.com/api/v3/
rest"
                } ],
                "instanceURL" : "https://yourcommunity.com",
                "ssoEnabled" : [ "saml" ],
                }
```

Implementing SAML SSO for your Jive site extends the functionality to Jive Mobile. However, use the following steps to ensure that the SAML SSO timeout behaves correctly on a mobile device:

1. Check the value of the `auth.lifetime` system property in the Jive admin console.
2. Make sure this value is the same as the SAML SSO timeout.

Authenticating with Activity-Based OAuth

You can choose to extend users' OAuth access tokens based on continued activity. By default, users will be required to re-authenticate after 15 minutes of inactivity on the device.

The activity-based OAuth method works like a very basic application lock. You set it up by setting the Refresh Token to time out earlier than the Access Token, which ensures that the Access Token is not refreshed before the Refresh Token has expired.

1. Under your name or avatar, select **Add-Ons**.
2. Make sure the Jive for iOS or Jive for Android app add-on is installed and enabled. `If you are using an on-premise version earlier than 7.0.1, or your instance isn't connected to the Internet, you may need to contact Jive Support to install this add-on.`
3. Next to the iOS app listing, click the gear icon and select **Settings**. Then click **Advanced**.
4. Set the **Access Token** and **Refresh Token** timeout settings to very short intervals. The Refresh Token timeout setting should be at least 1 minute shorter than the Access Token timeout setting.
5. Select **Automatically extend access token expiration upon activity**.

First-Time Only Authentication with SAML

With this method, a user authenticates initially through SAML SSO. Then Jive Mobile converts the session to a longer-lived OAuth session.

Note: This option is not available for versions earlier than Jive 7.0.1.

This method is achieved by setting the Access Token and Refresh Token timeouts for the Add-on to an interval greater than the timeout settings of SAML SSO, thereby circumventing the timeout settings of both auth.lifetime (the Jive authentication session) and the SAML SSO session. Keep in mind that if you use the default values for the Access Token timeout (48 hours) and the Refresh Token timeout (15 years), the user will not need to log in again on mobile unless the device's authentication is revoked or the values are changed.

This method has the following advantages:

- The user can revoke a device authenticated through SAML SSO, a feature that is not available by using regular SAML SSO login alone.
- Users who authenticated through the mobile clients and the regular web UI can have different timeout settings, while using the same authentication login flow and the same IdP.

To configure this method:

1. Make sure SAML SSO is enabled.
2. Make sure the Jive for iOS or Jive for Android app add-on is installed and enabled. `If you are using an on-premise version earlier than 7.0.1, or your instance isn't connected to the Internet, you may need to contact Jive Support to install this add-on.`
3. Next to the app listing, click the gear icon and select **Settings**. Then click **Advanced**.
4. Set the **Access Token** and **Refresh Token** timeout settings to interval greater than the timeout settings of SAML SSO.
5. Enable **Allow this add-on to obtain an access token using an authenticated session**. (Enabling this setting returns a 200 status code when /api/addons/*extensionUUID*/session-grant-allowed is passed. Otherwise, this call returns a 403 error.)

Forced OAuth for Mobile Only

You can enforce OAuth as the authentication method for Mobile users only, even if the instance is configured with SAML SSO.

Note: This option is not available for versions earlier than Jive 7.0.1.

If this setting is enabled, users accessing Jive on a mobile device will not use the SAML SSO login flow but instead enter a username and password. They will then use an OAuth token for all subsequent API calls.

1. Make sure a directory server such as LDAP is configured on the community.
2. In the admin console, add the system property `jive.coreapi.force.oauth` and set it to true.
3. Verify that the setting has been applied. If it's working correctly, `"ssoEnabled": ["saml"]` should be removed when making a call to `/api/version`.

Troubleshooting OAuth Errors

If you see an OAuth error when you try to connect using the Jive for iOS or Jive for Android app, the most likely cause is that the correct add-on is not installed.

Jive for iOS and Jive for Android rely on mobile add-ons that are added to your site via the Jive Add-ons Registry. Cloud and Hosted sites should have these add-ons installed by default. However, in rare cases, a site may require the add-ons to be installed. If you see the "Unable to initiate OAuth login" error when trying to connect from a mobile app, this is the likely cause.

Use the following steps to ensure your site can connect to the Add-ons Registry and then install the add-on(s) you need:

1. In the admin console, click **Add-Ons** > **Add-on Services Settings** and verify that Connections to Add-on Services is set to **Allow**. (If you don't have system admin privileges, you'll need Support to access this setting.)
2. Click your avatar in the top right of your site and select **Add-ons**.
3. From the Add-Ons tab, select **All Add-ons** > **Available**
4. Select the Jive for Android or Jive for iOS add-on, and click **Install**.

Custom App Wrapping for iOS

With Mobile 3, we are introducing a program to enable custom enterprise distribution of the iOS app, including wrapping with MDM tools like Good Dynamics or MobileIron.

If you participate in this program, you will be provided access to iOS binaries (.ipa files) for the Jive app, and will be able to perform some customizations, as well as app signing and wrapping. You can also contract with Jive professional services for app wrapping with Good Dynamics or MobileIron. Contact your Jive account representative for more information.

Jive internally tests a wrapped version with Good Dynamics and Mobile Iron. However, we cannot provide technical support for app wrapping outside of a Jive Professional Services engagement. We recommend that if you do imple ment wrapping without our Professional Services team, you assign this task to a mobile expert within your company. To verify success, we recommend testing the iOS app outside MDM, then wrapping and testing again. If you have a problem with Jive functionality after the app is wrapped, the problem can be isolated to the wrapped app, and you will need to reach out to your MDM vendor for assistance.

Note: App wrapping is not yet available for the Android app.

Native App Caching: Android

Caching behavior is designed to balance security and convenience.

Table 1: Data That Can Be Cached or Stored on the Device

Item	Description
User Avatars	--
Content Creation Activities	The most recently mentioned users and recently selected places for content creation will be cached.
Community URL	--
SSO Authentication Cookies	These cookies are stored only if the main instance is using SAML SSO.

Item	Description
Downloaded Attachments	Attachments are stored in the private application data folder.
oAuth token	The oAuth token is only stored if the main Jive instance is using oAuth.
Inbox items	Inbox items are stored in the private application data folder.

Table 2: Data That Cannot be Cached or Stored on the Device

Item	Description
Core API Responses	The core application API returns instance-specific data about the community, such as user profiles and content.

Native App Caching: iOS

Caching behavior is designed to balance security and convenience.

Table 3: Data That Can Be Cached or Stored on the Device

Item	Description
User Avatars	--
Content Creation Activities	The most recently mentioned users and recently selected places for content creation will be cached.
Username, password, and community URL	This information is stored securely in the keychain. Username and password are only stored if the main instance is using Basic Authentication.
SSO Authentication Cookies	These cookies are stored only if the main instance is using SAML SSO.
Downloaded Attachments	Attachments are stored using Data Protection.
oAuth token	The oAuth token is only stored if the main Jive instance is using oAuth.
Inbox items	Inbox items are stored using Data Protection.

Table 4: Data That Cannot be Cached or Stored on the Device

Item	Description
Core API Responses	The core application API returns instance-specific data about the community, such as user profiles and content.

Native Apps and Push Notifications

You can use the Native Apps settings to disable push notifications if you don't want to use them. Or, if you have a custom distribution of the native app, you can configure Jive to use an Apple or Android certificate to send push notifications.

Fastpath: Admin Console: Mobile

Push Notification Defaults

By default, push notifications are on, and are relayed through the Jive Push Service. If you want to shut them off, click **None - disable push notifications**.

Push notifications continue to send data through the Jive Push Service securely via HTTPS, but do not require authentication. To ensure Jive can send push notifications, you'll need to enable outbound traffic from your Jive instance to the following IP address on port 443:

- 204.93.84.65

Due to iOS and Android security restrictions on which credentials are needed to push to an application, push notifications must go through Jive's push notification gateway to reach the standard Jive Mobile application. If you don't like this behavior, you can disable push notifications, or you can do a custom app distribution and configure custom push directly through Google's and Apple's servers, as described below.

Custom Push Notifications

Custom push notifications go directly from the Jive server to the appropriate notification services (GCM from Android and APNS for iOS). For security, Android and iOS require that the credentials used to send push notifications to an app match the credentials used to sign the distributed app. Therefore, to use custom push notifications, you must have a customized version of the app that is signed by your organization's appropriate credentials. You can upload your organization's APNS credentials and/or GCM key on the **Mobile** page of the Admin Console.

Android	If you enable custom push notifications for Android, be sure the Jive server allows POSTs to `https://android.googleapis.com/gcm/send`. For more information about Android push notifications, you might want to check out their documentation.
iOS	To read more about how iOS push notifications work, the Mac Developer Library describes the provisioning process at length here. For a more detailed discussion of iOS app customization, you may want to ask your account manager for the following article in the Jive Community: How

To: Configure the Jive iOS App for Enterprise Distribution.