Using JIRA Connect Enterprise with MobileIron

February 27, 2015

Overview

JIRA Connect Enterprise is a iPhone/iPad app to connect to your Atlassian JIRA system (version 5.1 or above). The app requires the "Mobility for JIRA" Add-On from the Atlassian Marketplace. The app includes all premium features such as issue editing and creation, push notifications, and Agile boards.

Bundle ID: net.luethi.ios.JIRAConnectProEnterprise

Check the status of your JIRA projects on your Mobile from anywhere

Are you often in meetings and wished you could quickly pull up details on specific JIRA issues? Ever been in management reviews and needed to know how many enhancements are making the release? Then this app is for you! Receive important updates via Push Notifications. Have piece of mind that the right people get notified and that the update will not get lost in a sea of e-mails.

Use JIRA on a tablet during your Agile Stand-up meetings

Display Agile Boards and Burndown Charts on your iPad. Move issues through the workflow by simple drag-and-drop on your iPhone or iPad. Have your teams always be one tap away from all your Sprint information without having to carry around a laptop.

Comment, edit, prioritize, create whenever something is on your mind

In a creative process thoughts often come to mind randomly. Act on them when they are still fresh in your mind independent of your location.

App availability

The JIRA Connect Enterprise app is available from the Apple App Store. It also requires the Mobility for JIRA add-on from the Atlassian Marketplace to be installed on the JIRA system.

Device compatibility

The app requires iOS version 7.0 or higher. It can connect to JIRA version 5.1 or higher. JIRA OnDemand is not supported by JIRA Connect Enterprise.

App-specific configuration

JIRA Connect Enterprise allows an administrator to preconfigure and push out values that need to be entered on the JIRA Connect Enterprise login screen. They include:

Key	**Description**	**Default if the key-value pair is not configured**
username	A JIRA user name can be pre-set but it is generally typed in by the user	Empty field, to be entered by user
password	A JIRA password can be pre-set but it is generally typed in by the user	Empty field, to be entered by user
server	This is the URL of the JIRA server. For example: https://jira.ourcompany.com:8080	Empty field, to be entered by user

AppTunnel support

JIRA Connect Enterprise supports tunneling

- JIRA Connect Enterprise interacts with your internal JIRA server. The server requires the Mobility for JIRA add-on. The add-on will also send out Push Notifications.
- Your internal JIRA server host name can be configured with app-specific configuration parameters. If it is not configured, users are required to type it in by themselves.
- JIRA Connect Enterprise interacts with your JIRA Server using the REST API, generally on port 80, 8080, or 443

Data loss prevention policy support (iOS SDK apps only)

- the pasteboard DLP policy: not supported
- the print DLP policy: not supported
- the Open In DLP policy: not supported

Secure file I/O support (iOS SDK apps only)

User name and password are stored encrypted in the Keychain. Other than the URL no data is stored locally. Therefore secure file I/O is not supported.

AppConnect and non-AppConnect mode support (iOS SDK apps only)

The application works for users with and without AppConnect. The app does not have to be reinstalled.

Additional sections

JIRA Connect Enterprise requires an on-premise version of Atlassian JIRA.

User features

- Create issues, sub-tasks, and issue links

- Edit, assign, and delete issues

- Ability to enter, edit, and delete your comments

- Transition issue through workflow directly from issue screen

- Receive Push Notifications (Atlassian Marketplace JIRA Plugin needed)

- Support for JIRA Agile/GreenHopper Planning Board, Work Board, Burndown charts

- Renders wiki-markup and HTML fields

- Log your work and include a comment

- View all worklogs, edit and delete your own logs

- View, upload, and delete attachments

- Search by JIRA key, description, summary, project, version, issue type, status, component, and assignee and sort by any field

- Issue details including custom fields, comments, attachments, sub-tasks, and issue links

- Scans QR Codes with encoded JIRA key

- Activity stream and details

- Responsive and fast UI, utilizing lazy loading, and asynchronous calls

For more information

http://www.mobilityforjira.com

http://www.mobilityforjira.com/instructions

https://marketplace.atlassian.com/plugins/net.luethi.plugins.jira.apn4jiraconnect

https://itunes.apple.com/us/app/jira-connect-enterprise/id898500641?ls=1&mt=8

Configuration tasks

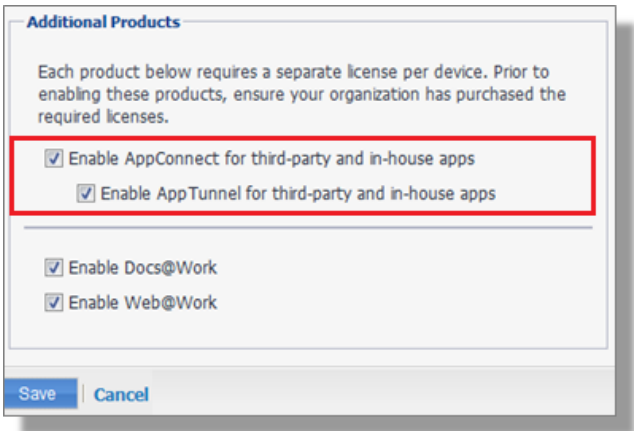
Use the following high-level steps to configure AppConnect for the app.

1. Enable AppConnect.
2. Configure an AppConnect global policy.
3. Configure a new AppConnect app configuration for the app.
4. Configure a new AppConnect container policy for the app.

Enable AppConnect

Before enabling AppConnect on your VSP, confirm that your organization has purchased the required AppConnect licenses. Contact your MobileIron representative if you require additional details on AppConnect license purchases.

To enable AppConnect and AppTunnel functionality on the VSP, navigate to the Settings page on the VSP Admin Portal and check the boxes as shown below.



1. Select the option for “Enable AppConnect for third-party and in-house apps”.

5. Select the option of “Enable AppTunnel for third-party and in-house apps”.

Configure an AppConnect global policy

An AppConnect global policy configures the security settings for all AppConnect apps, including:

- Whether AppConnect is enabled for the devices that the policy is applied to
- AppConnect passcode requirements.

  Note: The AppConnect passcode is not the same as the device passcode.
- out-of-contact timeouts
- the app check-in interval

  Note: The app check-in interval is independent of the MDM check-in timer and controls, and apps cannot be forced to check-in before the interval expires. The recommended configuration for the app check-in interval is 60 minutes.
- the default end-user message for when an app is not authorized by default
- whether AppConnect apps with no AppConnect container policy are authorized by default
- data loss prevention settings

To modify an existing AppConnect global policy:

1. On the VSP Admin Portal, go to Policies & Configs > Policies.
6. Select an AppConnect global policy.
7. Click Edit.
8. Edit the AppConnect global policy based on your requirements.

   See the AppConnect chapter of the VSP Administration Guide for details about each field.

Configure a new AppConnect app configuration

The AppConnect app configuration defines the app-specific parameters that are automatically pushed down to the app, as well as configurations for establishing and authenticating an AppTunnel associated with the app. See the AppConnect chapter of the VSP Administration Guide for details about each field.

Also, for more on AppTunnel configuration, see “Adding AppTunnel Support” in the AppConnect chapter of the VSP Administration Guide.

Use the following steps to configure the app-specific configuration:

1. On the VSP Admin Portal, go to Apps > Configurations > Add New > AppConnect > Configuration.

9. Edit the AppConnect app configuration with the Name, Description, Application, AppTunnel configuration including the identity certificate, and App-specific key-value pair configurations required for the app.

   Note: For the Application field, choose an application from the app distribution library, or for iOS apps, specify the iOS bundle ID. You can find the bundle ID by going to Apps > App Distribution Library, and clicking to edit the app. The field Inventory Apps displays the bundle ID in parenthesis.

10. AppTunnel: Click on the “+” button and enter the AppTunnel details. The AppTunnel service for this app must be pre-configured in order to use it here.

11. App Specific Configuration: Click on the “+” button to enter the key-value pair information.

Configure a new AppConnect container policy

An AppConnect container policy specifies data loss protection policies for the app. The AppConnect container policy is required for an app to be authorized unless the AppConnect global policy allows apps without a container policy to be authorized. Such apps get their data loss protection policies from the AppConnect global policy.

Details about each field are in the AppConnect chapter of the VSP Administration Guide.

To configure an AppConnect container policy:

1. On the VSP Admin Portal, go to Policies & Configs > Configurations > Add New > AppConnect > Container Policy.

12. Enter the Name, Description, and Application.

Note: For the Application field, choose an application from the app distribution library, or for iOS apps, specify the iOS bundle ID. You can find the bundle ID by going to Apps > App Distribution Library, and clicking to edit the app. The field Inventory Apps displays the bundle ID in parenthesis.

13. Configure the data loss protection policies according to your requirements.