Use Case: Secure Naval Operations Using Confluence - Part 2

Background: Within the Navy's strategic operations, security and data integrity are paramount. Confluence is utilized for secure communications and operations planning. Given the sensitive nature of these activities, the management of OAuth access tokens, user themes for optimal data visualization, and email visibility settings are critical for operational security and personal ease of use in varying light conditions during naval operations.

Objective: This document provides instructions for Navy personnel in managing OAuth tokens for secure data access, customizing Confluence's visual interface for environment-adaptive use, and setting email visibility for communication confidentiality.

Instructions:

1. Managing OAuth Access Tokens:

Viewing OAuth Access Tokens: a. Click your profile picture in the Confluence navigation bar, and select "Settings." b. Find and select "View OAuth Access Tokens" to see a list of tokens and their properties.

Revoking OAuth Access Tokens: a. Follow the steps above to view your tokens. b. Locate the specific access token you wish to revoke under the "Consumer" column. c. Click "Revoke OAuth Access Token." Confirm the action if necessary. Note: After revocation, gadgets on external platforms will lose access to private Confluence data.

2. Adapting Confluence Theme for Naval Environments:

a. Navigate to the navigation bar and click on your profile picture, then select "Theme." b. Choose from the following options per your operational environment: - "Light": Use in well-lit control rooms or during the day. - "Dark": Ideal for low-light environments or night operations to reduce glare. - "Match Browser": Automatically adapts based on your system settings; useful for seamless integration with other on-board systems. c. Exit the settings; Confluence will save your preference automatically. Note: If the "Dark" theme is not rendering correctly, it may be due to admin-level customizations. Please report the issue to your IT department.

3. Configuring Email Visibility for Operational Security:

a. Click on your profile picture at the right of the navigation bar and choose "Settings." b. From the left sidebar, select "Profile and visibility." c. Navigate to the "Contact" section. d. Adjust your email visibility according to the desired confidentiality level: - "Anyone": Select when on joint operations where broader

visibility is required. - "Your organization": Restricts visibility to internal personnel; suitable for most operations. - "Only you and admins": For classified operations where utmost confidentiality is required. e. Your settings will save automatically; exit the menu afterward.

Conclusion: Proper management of OAuth tokens is crucial for preventing unauthorized data access, especially when using Confluence gadgets on external systems during joint operations or collaborations. Adapting the Confluence theme assists personnel in data readability during various naval operations, ensuring that crucial information is always visible and clear. Lastly, setting appropriate email visibility levels helps maintain operational security and personal privacy. Regular review and adjustment of these settings are advised, in line with current operational parameters and security protocols.

Optional / Additional Information

Lab: Manage your account - Part 2

Manage OAuth access tokens

OAuth access tokens allow you to use a Confluence gadget on an external web application or website (also known as the 'consumer') *and* grant this gadget access to Confluence data which is restricted or privy to your Confluence user account.

OAuth access tokens will only appear in your user profile if the following conditions have been met:

1. Your Confluence administrator has established an OAuth relationship between your Confluence site and the consumer.
2. You've accessed a Confluence gadget on the consumer and have completed the following tasks:

a. Logged in to your Confluence user account via the gadget
b. Clicked the **Approve Access** button to allow the gadget access to data that's privy to your Confluence user account

Confluence will then send the consumer an OAuth 'access token', which is specific to this gadget. You can view the details of this access token from your Confluence site's user account.

An OAuth access token acts as a type of 'key'.

As long as the consumer is in possession of this access token, the Confluence gadget on the consumer will be able to access Confluence data that's both publicly available and privy to your Confluence user account.

As a Confluence user, you can revoke this access token at any time.

All access tokens expire after seven days. Once the access token is revoked or has expired, the Confluence gadget will only have access to publicly available Confluence data.

View your OAuth Access Tokens

To view all of your Confluence user account's OAuth access tokens:

1. Choose your profile picture at the right side of the navigation, then choose **Settings**
2. Click **View OAuth Access Tokens**

OAuth Access Token Details

Your list of OAuth access tokens is presented in a table, with a row for each access token and a column for each property:

Column Name	Description
Consumer	The name of the Confluence gadget that was added on the consumer.
Consumer Description	A description of this consumer application. This information would have been obtained from the consumer's own OAuth settings when an OAuth relationship was established between Confluence and that consumer. If the consumer is another Atlassian application, this information is obtained from the Consumer Info tab's **Description** field of the OAuth Administration settings. The application's administrator can customize this Consumer Info detail.
Issued On	The date on which the OAuth access token was issued to the consumer by Confluence. This would have occurred immediately after you approved this gadget access to your Confluence data (privy to your Confluence user account).
Expires On	The date when the OAuth access token expires. This is seven days after the "Issued On" date. When this date is reached, the access token is automatically removed from this list.
Actions	For revoking the access token.

Revoke your OAuth Access Tokens

To revoke one of your OAuth access tokens:

1. View your Confluence user account's OAuth access tokens (described above).
2. Click **Revoke OAuth Access Token** for the OAuth access token you want to revoke.

The gadget's access token is revoked and the Confluence gadget on the consumer will only have access to publicly available Confluence data.

Change your theme

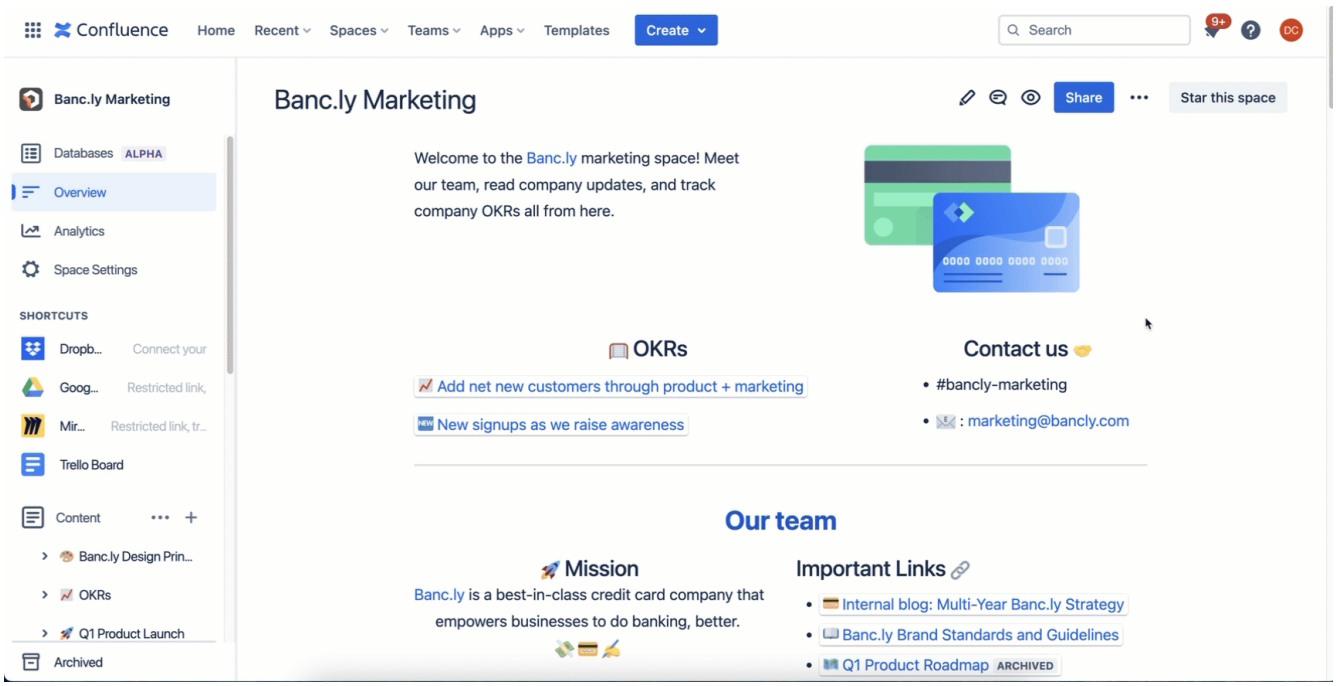
You can set a theme to change how Confluence looks.

To change your theme:

1. Select your profile avatar at the right of the navigation bar, then select **Theme**.
2. Select one of the theme options:

- **Light:** Sets Confluence to display in lighter colors. This is the default theme.
- **Dark:** Sets Confluence to display in darker colors.
- **Match Browser:** This will match the theme you set in your browser. If you don't have this set, you will see the default theme.

The theme you select will be saved to your account, so your choice will apply even if you use Confluence on another device.



Themes change your current view of Confluence and don't impact how a reader sees your page.

Admin-driven themes

If you switch to Dark theme and your top navigation bar doesn't look right, your admin may have set custom colors that don't work well with Dark theme. Contact your admin to update the colors.

Set your email visibility

On your Atlassian account settings, you can control who can see your email address.

To set your email visibility:

1. Tap your profile picture at the right of the navigation, then select **Settings**.
2. Select **Profile and visibility** on the left sidebar.
3. Scroll down to the **Contact** section.
4. Choose one of the options from the **Who can see this?** dropdown:

a. **Anyone**: visible to anyone who can view your content, including people outside of the Atlassian organization. Accessible by installed apps.
b. **Your organization**: only visible to people who have access to your organization.
c. **Only you and admins**: only visible to you and admins. To manage access to Atlassian products and services, admins need to view your email address too.

Note: setting options can vary by type of account.

Your new settings will be saved automatically.