Slack's Secure Configuration Guide for FedRAMP Moderate

Introduction

This guide provides required recommendations for configuring a Slack instance to align with the security controls and best practices supporting a FedRAMP Moderate authorization.

NOTE: It is the customer's responsibility to set up their Slack instance in compliance with FedRAMP and other security regulations. This document provides suggestions on how to utilize some of the key functionality in Slack that helped support Slack's FedRAMP Moderate package. The full package can be requested by federal agencies, while commercial customers can request Slack's customer responsibility matrix.

Required FedRAMP Moderate Settings

The following points are critical for maintaining a FedRAMP Moderate authorization and are based on the guidance provided during Slack's authorization process:

FedRAMP Moderate is only supported on the Slack Enterprise or Enterprise+ plan. Lower Slack plans do not provide support for FedRAMP Moderate.

Implement multi-factor authentication for privileged accounts and non-privileged accounts through the use of single sign-on (SSO)

- If the customer chooses to use delegated authority SSO then the customer should ensure that the authentication mechanism they are being delegated to requires two factor authentication.
- If the customer chooses to use SAML SSO, the customer should work with the SAML provider to require multi-factor authentication at login.
- Slack accepts SAML 2.0 which is able to federate with personal identity verification (PIV) credentials.
- If personal identity verification (PIV) credentials are being used for SSO, the customer may need to identify a solution to enable mobile access (e.g. mobile derived credentials).
- For guest accounts required by your organization, ensure two-factor authentication is enabled.
- Access the full Slack SAML guide, here.

Utilize Slack's Custom Terms of Service

The customer can configure a system use banner with the necessary requirements to notify users they are accessing a government information system. Prior to authentication, no sensitive data is displayed. Access the full Custom Terms of Service guide, here.

Utilize Slack's Mobile Device Management known as Enterprise Mobility Management (EMM)

- Slack provides EMM to customer allowing them to implement strict controls when using the Slack mobile clients
- Slack provides our customers with the ability to perform concurrent session control via identity providers and/or mobile device management partners (integrations).
- (optional) Slack recommends blocking file downloads and data copies to the mobile device.
- Access the full EMM guide, here.

Utilize Slack's Audit Log API to ingest log data and audit account actions

- Slack provides customers with an API to ingest audit logs into their own SIEM tool for all account actions within their environment, commensurate with the requirements outlined in the AU family.
- Customers are responsible for auditing account actions within their own instance of Slack.
- NOTE: An out of the box Splunk Integration & Add On are available.
- Access the full audit log API how-to article, here.

Ensure all Apps are FedRAMP authorized before approving in Slack

- Slack makes available a host of APIs that are able to interact with the service offering.
- Slack does not incorporate any of the third-party applications within the application directory inside the boundary.
- Slack integrations are merely API connectors from Slack's platform to a third-party's environment.
- When a customer uses a FedRAMP authorized version of a service and connects it to Slack through the Slack app, that connection is considered compliant with FedRAMP requirements.

If desired, Admins can lock Slack display names and add indicators for contractors and guests

- Customers are able to configure the display name(s) for users in their environment.
- Customers are able to define their own parameters to ensure contractors and foreign nationals are able to be identified by other government employees.

Slack recommends the customer review minimum requirements for accessing Slack here

Customers should configure their browser to only accept connections via TLS 1.2/3. If customers configure their browsers to support TLS 1.2/3, Slack's servers will always establish a connection over TLS 1.2/3. Slack has configured TLS_SCV_Downgrade to ensure that connections can't be negotiated down from TLS 1.2/3 to a lesser version.

Recommended Settings for Security (Optional)

The following suggestions provide additional security tips and role guidance for managing your Slack workspace.

Slack has an Add On capability to enable Enterprise Key Management (EKM) if revoking access to data is required. EKM reduces the risk of data spills in Slack – whether from uploading the wrong file or inadvertently discussing Secret or Covered Defense Information.

- EKM adds a layer of object level encryption to your data with your own keys.
- If a user uploads information that is not permitted in Slack, they should follow their organization's internal data spill policy. Once that process is complete, the final step is to delete the message within Slack.
- With EKM, the customer can prevent access to the specific messages or file after revoking the specific AWS KMS key. Administrators can revoke Slack's access to the customer's keys on a granular basis in order to render specific data unavailable. These granular levels include:
    - The entire organization
    - Each workspace
    - Each channel
    - Every hour of messages within a channel
    - Each file
- In the event the customer is using the Enterprise Key Management Feature, the production databases will be encrypted with a key derived from the customer's AWS KMS Master Key, which is a FIPS 140-2 validated key.
- Access the full EKM guide, here.

Limit Access to your workspace. Slack allows for transparency, and sometimes that means sharing proprietary information or sensitive data. Here are some tips to ensure only the right people have access to information in your workspace:

- Only invite people you know. By default, Workspace owners, Workspace Admins and members can send invitations. To control who's invited, you can require admin approval for all invitations. If you do allow members to send invites, review pending and accepted invitations periodically.
- Verify email domains. Workspace owners and workspace admins can set a signup mode for your workspace to allow anyone with an approved email domain to automatically join their workspace. Verify that you own any email domains you've approved for your workspace.
- Deactivate members accounts who no longer need access. Change is constant, and people come and go. Don't forget to deactivate a member's account when they leave. Workspace owners can streamline deactivation with an identity provider using SCIM provisioning.
- Use Slack Connect to work with external people. To work with external people who don't need access to all the information in your workspace, you can use Slack Connect. This lets your collaborate securely in channels and direct messages, each from your own workspaces.
- Use guest accounts and limit the channels they're invited to. Some members of your Slack workspace (like contractors, interns, or clients) may only need access to certain channels. Guest accounts are a great way to manage who has access to the information they need in your workspace.
- Manage email display. Members can find each others' email addresses in their profiles, but

some people may prefer to keep this info private. Workspace Owners and Admins can choose if members' email addresses are displayed in their Slack profiles.

Set Session Duration

Workspace owners and admins on all plans can limit how long their members are signed into Slack by setting a session duration. More information on session durations can be found here.

Understand Slack usage

Workspace owners can view analytics and usage for insights into how members use Slack. More details can be found here.

Understand the Primary Owner Role

The primary owner is the most powerful administrative role in your Slack workspace. You can become a Primary owner by creating your own workspace, or if a primary owner chooses to transfer ownership of a workspace or Enterprise organization to you. The primary owner has the ultimate authority capabilities and represents the customer in administering the workspace. There can only be one person in this role at a time, so it's important to make sure it's the right person. Some recommendations are:

- An executive or senior level manager
- Someone from the IT department who provisions licenses or handles account administration
- If within the policy guidelines of your organization, use a shared service/administrative email account on your company's domain that is managed by authorized personnel.
- More information about this can be found here.

Best Practices for Primary Owners

- Promote Owners and Admins to help with day-to-day administrative tasks, like managing invitations or channels. Or, assign members to system roles.
- Add billing contacts like people from the accounting department, to keep them informed on billing activity.

Keep administrative accounts on the corporate domain

- Make sure all of your owners and admins use their company email addresses to join your Slack workspace or Enterprise org.
- If your company's email domain changes, the primary owner - and any other affected members - should update their email address in Slack.

Workspace organization and setup

- Slack allows unlimited workspaces within your organization's tenant. Slack recommends organizing workspaces by department and use cases. This allows customers to keep workspace channels segmented by use case.
- Slack recommends creating a separate workspace for your Slack connect channels with external partners.

Outdated Slack Clients

- Slack provides workspace administrators with a dashboard that displays any users currently using unsupported client versions of Slack.
- Slack recommends engaging with these users to update their software

Message Restrictions

- Determine who in the organization can use the @here or @channel when sending messages, options include:
    - All members and guests (default)
    - All members but not guests
    - Workspace admins and owners only
    - Workspace owners only
- @channel will notify all members in that channel, @here will only notify those members online in that channel

Channel Management and Restrictions

- For channels with broad amounts of users, Slack allows administrators to restrict who can post messages to those channels.
- Slack allows administrators to control who can create public channels and private channels
- Slack allows administrators to control who can archive channels

Document Control

Update Date	Summary of Changes	Version
2026-02-15	First draft	0.01
2026-02-24	Finalized first draft	0.02