Configuring Okta for FedRAMP Compliance

For agencies that require FedRAMP Moderate, FedRAMP High, and FedRAMP+ with IL4 controls met, Okta's compliance offering is easy to set up for your regulated environment. In order to take advantage of Okta's Authority To Operate (ATO) and ensure your own FedRAMP compliance, we have included below a detailed list of the required controls and settings you are responsible to set in Okta.

More information on how to comply with FedRAMP+ IL4 is available at: "Using Okta to Protect IL4 data".

Note: This is intended to serve as an overview of the minimum settings for your new Okta org to meet your FedRAMP requirements. The full detailed customer responsibility matrix, or Control Implementation Summary (CIS) is available in our FedRAMP package.

Considerations

Before you start configuring your Okta tenant, please make sure you review and take any necessary actions on the following:

- **SIEM Configuration for Monitoring**: Configure your SIEM to consume the Okta logs to ensure monitoring is sufficient for your regulated environment.
- **Okta Basic Settings**:
    - Set up unique usernames for all users.
    - When setting up multi-factor authentication (MFA), the following all meet FedRAMP requirements: Okta Verify, FIPS-validated MFA/U2F keys, PIV/CAC credentials, and other FIPS-validated authenticators.
        - Note: You are responsible for ensuring that the registration process to receive all hardware/biometric (multi-factor authenticators) be conducted in person and with an organization-defined registration authority having authorization.
- **Document Security Policies**: Ensure your policies and procedures around account creation, modification, deletion of all user identification and authentication credentials, as well as roles and groups, are written to include Okta.
- **Okta and Okta Verify meet FICAM requirements as follows**:
    - IAL: Okta does not verify identity verification, complying with level 1, 2 or 3 is the customer's responsibility.
    - AAL: Okta with Okta Verify is level 3 compliant.
    - FAL: Okta is level 2 compliant.

Considerations

Please see https://help.okta.com/en/prod/Content/Topics/Security/Administrators.htm for a description of the various account types in Okta.

Control	Okta for FedRAMP Moderate	Changes for IL4 or FedRAMP High if needed	Where is this setting?
AC-2 (3)	Enable the available automation to automatically disable inactive accounts after 90 days of non-use.	Enable the available automation to automatically disable inactive accounts after 35 days of non-use.	Please see https://help.okta.com/en/prev/Content/Topics/Directory/automations.htm
AC-2 (5)	The session timeout shall be configured to 15 minutes or less in the Okta Admin panel.		In the Okta Admin panel Security => Authentication => Sign On Create a rule for Session Lifetime and assign it to the group(s) in FedRAMP scope.
AC-7	In the Okta Admin panel set the invalid attempt threshold to 3 or less and enforcing a lockout duration of at least 30 minutes.		In the Okta Admin panel Security => Authentication => Password Create a rule for Lockout after 3 unsuccessful attempts and set Account is automatically unlocked after 30 minutes, then assign it to the group(s) in FedRAMP scope.
AC-8	The Okta Admin panel allows configuring an access banner and notifications, this shall be done.		In the Okta Admin panel Org Settings => Appearance for custom logo => Customization for Customize Sign In Page => Email and SMS for configuring email notifications
AC-11 and AC-12	The session timeout shall be configured to 15 minutes or less in the Okta Admin panel.		In the Okta Admin panel Security => Authentication => Sign On Create a rule for Session Lifetime and assign it to the group(s) in FedRAMP scope.
IA-2 controls	MFA (hardware MFA or Okta Verify is required for AAL level 3) must be configured and strong password rules (15 or more characters, including alphanumeric, lower case, capitalization, and symbols) are needed.		In the Okta Admin panel Security => Authentication => Password Create a rule for password complexity requirements and assign it to the group(s) in FedRAMP scope. If using Okta Verify as your MFA, contact your CSM to verify your org is set up for FIPS compliant communications.
IA-4	Enable the available automation to automatically disable inactive accounts after 90 days of non-use.	Enable the available automation to automatically disable inactive accounts after 35 days of non-use.	Please see https://help.okta.com/en/prev/Content/Topics/Directory/automations.htm

Control	Okta for FedRAMP Moderate	Changes for IL4 or FedRAMP High if needed	Where is this setting?
IA-5 controls	MFA (hardware MFA or Okta Verify is required for AAL level 3) must be configured and strong password rules (15 or more characters, including alphanumeric, lower case, capitalization, and symbols) are needed, set password expiration at 60 days or less, set minimum password age to at least 1 day, enforce password history for last 24 passwords.		In the Okta Admin panel Security => Authentication => Password Create a rule for password complexity requirements, set password expiration to 60 days or less, set minimum password age to at least 1 day, enforce password history for last 24 passwords, and assign it to the group(s) in FedRAMP scope. In the Okta Admin panel Security => Authentication => Sign On Create a rule for require MFA (select factors) and assign it to the group(s) in FedRAMP scope. If using Okta Verify as your MFA, contact your CSM to verify your org is set up for FIPS compliant communications.
SC-10	The session timeout shall be configured to 15 minutes or less in the Okta Admin panel.		In the Okta Admin panel Security => Authentication => Sign On Create a rule for Session Lifetime and assign it to the group(s) in FedRAMP scope.

For more information about Okta's comprehensive approach to security and compliance, visit Okta.com/Security.