okta

Inheriting from Okta's FedRAMP Authorization

Private companies looking to work with government agencies will need to explore FedRAMP certification in order to meet compliance requirements for their government customers. For organizations planning on pursuing FedRAMP Moderate, High, or FedRAMP+ IL4, there are hundreds of controls and considerations that must be met in order to achieve an authority to operate (ATO).

A benefit of leveraging Okta as your identity provider is that you may be able to inherit controls from Okta's ATO for your FedRAMP audit. Below is the full list of controls as well as details for your FedRAMP documentation. Out of the box, Okta offers a FedRAMP Moderate compliant solution that organizations and agencies can leverage for their identity needs; to comply with FedRAMP IL4, visit our "Using Okta to Protect IL4 Data" whitepaper for additional details and guidance on how to protect FedRAMP High or IL4 data.

Control Details

Below is the full list of FedRAMP controls you can inherit using Okta. Use the table when filling out your FedRAMP documentation to guide you through how Okta assists with the controls. Every architecture is unique so review yours thoroughly with your FedRAMP assessor to verify any controls inherited from Okta, or other Cloud Service Providers.

Control	Okta for FedRAMP Moderate	Changes for IL4 or FedRAMP High if needed
AC-2	Your accounts are entirely or at least partially in Okta. Ensure your policies and procedures reflect the processes accurately.	
AC-2 (1)	The appropriate Okta logs can be used for monitoring and imported to a SIEM for combination with other system logs. Okta can be mastered from your HR system where appropriate to automate provisioning and deprovisioning.	
AC-2 (3)	Okta has automation available to automatically disable inactive accounts after 90 days of non-use.	Okta has automation available to automatically disable inactive accounts after 35 days of non-use.
AC-2 (4)	The appropriate Okta logs can be used for monitoring and imported to a SIEM for combination with other system logs.	
AC-2 (5)	The session lifetime can be set in the Okta Admin panel to an appropriate value.	
AC-2 (7)	Roles and groups can be created as appropriate in the Okta Admin panel	

Control	Okta for FedRAMP Moderate	Changes for IL4 or FedRAMP High if needed
AC-7	The Okta Admin panel allows setting invalid attempt threshold to 3 or less and enforcing a lockout duration of at least 30 minutes.	
AC-8	The Okta Admin panel allows configuring an access banner and notifications.	
AC-11 and AC-12	The session timeout shall be configured to 15 minutes or less in the Okta Admin panel.	
AC-12	The session timeout shall be configured to 15 minutes or less in the Okta Admin panel.	
AU-2	The appropriate Okta logs can be used for monitoring and imported to a SIEM for combination with other system logs.	
AU-3	The appropriate Okta logs can be used for monitoring and imported to a SIEM for combination with other system logs.	
AU-6	The appropriate Okta logs can be used for monitoring and imported to a SIEM for combination with other system logs.	
IA-2	Unique usernames are required in Okta.	
IA-2 (1)	MFA shall be enabled.	
IA-2 (2)	MFA shall be enabled.	
IA-2 (5)	Okta can be used for the individual login authenticator.	
IA-2 (8)	Okta is replay resistant.	
IA-2 (11)	MFA shall be enabled.	
IA-2 (12)	Okta supports Personal Identity Verification (PIV) or Common Access Card (CAC) credentials via inbound SAML or IWA.	
IA-4	Your Okta tenant will manage using your existing policies for assigning identifiers. Okta has automation available to automatically disable inactive accounts after 90 days of non-use.	Okta has automation available to automatically disable inactive accounts after 35 days of non-use.
IA-4 (4)	Your Okta tenant will manage using your existing policies for uniquely assigning identifiers.	
IA-5	Your Okta tenant will manage using your existing policies, ensure to set password expiration at 60 days or less.	
IA-5 (1)	Your Okta tenant will manage these, follow current FedRAMP guidance for settings.	
IA-5 (4)	Okta controls complexity of users passwords.	

Control	Okta for FedRAMP Moderate	Changes for IL4 or FedRAMP High if needed
IA-5 (6)	Okta is FedRAMP Moderate and can be used to protect data accordingly.	Do not put data more sensitive than allowed by FedRAMP Moderate into your Okta tenant and ensure you use the more strict control settings if accessing more sensitive data.
IA-5 (7)	All information stored in Okta is encrypted.	
IA-6	Okta obscures the authenticator.	
IA-7	Okta uses FIPS 140-2 level 2 or higher validated cryptography to store data.	
IA-8 (1)	Okta supports Personal Identity Verification (PIV) or Common Access Card (CAC) credentials via inbound SAML or IWA.	
IA-8 (2)	Okta meets 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 is level 3 compliant. FAL: Okta is level 2 compliant.	
IA-8 (3)	Okta meets 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 is level 3 compliant. FAL: Okta is level 2 compliant.	
IA-8 (4)	Okta meets 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 is level 3 compliant. FAL: Okta is level 2 compliant.	
IR-4	The appropriate Okta logs can be used for monitoring and imported to a SIEM for combination with other system logs.	
IR-5	The appropriate Okta logs can be used for monitoring and imported to a SIEM for combination with other system logs.	
PS-4	Okta can be mastered from several HR systems and automatically disable accounts. Okta can also be used manually to meet account disabling timelines.	
SI-4	The appropriate Okta logs can be used for monitoring and imported to a SIEM for combination with other system logs.	
SI-4 (1)	The appropriate Okta logs can be used for monitoring and imported to a SIEM for combination with other system logs.	

For further information on using the Okta admin console to find and adjust settings for your FedRAMP documentation, visit: https://help.okta.com/en/prod/Content/