

# Okta + NIST 800-63B



okta

# Table of contents

3	Executive Summary
4	Introduction
5	Determining authentication levels
7	Categorizing applications
8	Maximum Session Duration
9	Maximum idle time
10	Biometrics
12	Conclusion

# Executive Summary

The NIST Special Publication 800-63B Digital Identity Guidelines - Authentication and Lifecycle Management was first published in June of 2017; it's been a critical element of an Identity and Access Management (IAM) program ever since. The guidelines have been revised and augmented with additional documentation over the years, but the primary goal remains the same, to:

**“ ... provide technical requirements for federal agencies implementing digital identity services.”**

Though NIST is a government agency, and the standards a government publication, Okta feels that industry can find applicable guidance and best practices within the document. And as part of the Okta Secure Identity Commitment (OSIC), we would like to highlight the Okta features that support NIST Digital Identity Guidelines.

# Introduction

In this document, we will be sharing NIST guidelines combined with Okta feature sets.

**We have taken the liberty of pulling together NIST requirements around the following topics**

---

**01** Determining authentication levels

---

**02** Categorizing applications

---

**03** Maximum session duration

---

**04** Maximum idle time

---

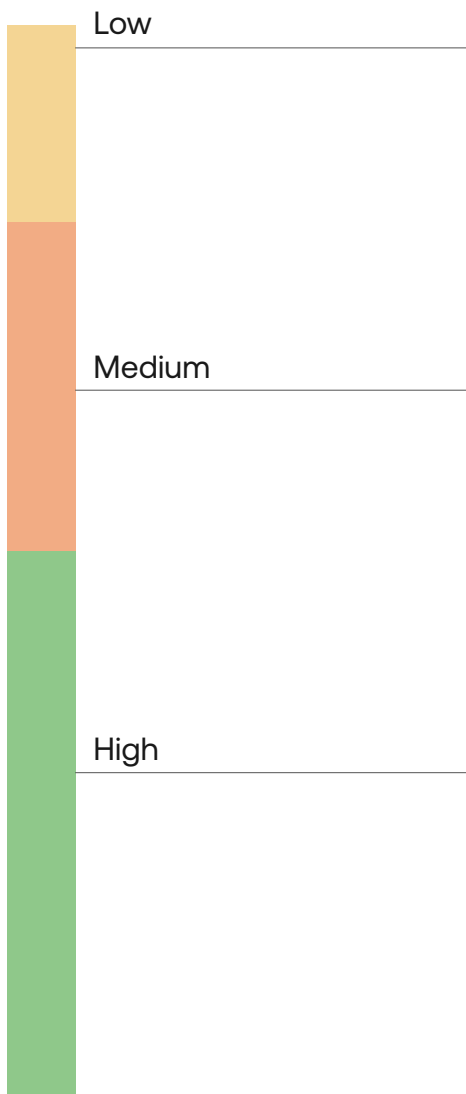
**05** Biometrics

**Let's get started!**

# Determining authentication levels

NIST SP 800-63b (section 4, Authenticator Assurance Levels) provides guidance on determining the proper authentication level for the information you're intending to secure.

The mapping of NIST to Okta assurance levels is as follows:



## Okta Authenticator Assurance Level 1 (Low)

Verify using one or more factors

### Considerations:

This could be any factor “something you have (Okta Verify, security key, etc.)”, “something you know (password/secrets)”, or “something you are” (WebAuthn/FIDO2-capable biometric checks like Face/TouchID, etc.) Reauthentication settings must be set to 30 days to satisfy NIST AAL1 requirements.

## Okta Authenticator Assurance Level 2 (Medium)

Verify using two distinct factors

### Considerations:

This needs to contain two authentication factors, either (1) a physical authenticator and a memorized secret, or (2) a physical authenticator and biometrics linked to that authenticator. An example would be a password + Okta Verify OTP or password + Okta Verify FastPass with Biometric. Reauthentication settings must be set to every 12 hours and idle session time to 30 minutes to satisfy NIST AAL2 requirements.

## Okta Authenticator Assurance Level 3 (High)

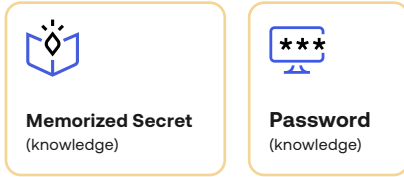
Verify using Smartcard or Password with a phishing-resistant authenticator

### Considerations:

The only way to satisfy the NIST AAL3 requirement is through password + FIPS Yubikey/ FIDO2/WebAuthn or CAC/PIV Authentication. More options may become available as NIST releases further updates to the SP 800-63-3 Digital Identity Guidelines. An example would be password + FIDO2 (WebAuthn) Reauthentication settings must be set to every 12 hours and idle session time to 15 minutes to satisfy NIST AAL3 requirements.

<p><b>Low assurance requirements apps</b></p> <ul style="list-style-type: none"> <li>• General information portal, order lunch</li> <li>• Non sensitive information or processes</li> </ul>	<p><b>Medium assurance requirements apps</b></p> <ul style="list-style-type: none"> <li>• Regular business apps</li> <li>• Non sensitive collaboration</li> </ul>	<p><b>High assurance requirements apps</b></p> <ul style="list-style-type: none"> <li>• Critical customer data or financial data apps</li> <li>• Intellectual property related Apps</li> </ul>
---	---	--

**Any one possession or knowledge factor type**



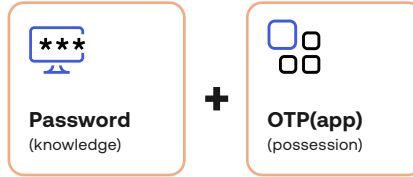
**Authentication methods**

- Password or security question,
- SMS OTP or Email,,
- Okta Verify Push (no biometric)

**Context**

- Any network
- Any device
- Any user

**(Possession + Knowledge) & Registered device (optional)**



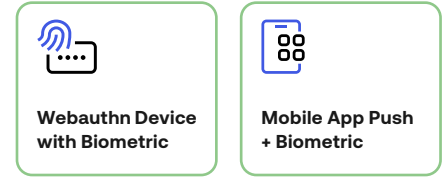
**Authentication methods**

- Password + Okta Verify OTP,
- Password + Okta Verify Push (no biometric)
- Webauthn only
- Okta Fastpass (no biometrics)

**Context**

- Any network
- Registered, not Managed device Employees or approved 3rd parties only

**Inherence + (Possession or Knowledge) Factor Types**



**Authentication methods**

- Okta Verify push with Biometric,
- Okta Verify OTP + WebAuthn Okta Fastpass with prompt/biometrics

**Context**

- Corporate network only
- Registered and Managed Device
- Employees only

# Categorizing applications

Next up, NIST SP 800-63-3 (section 6.2) provides a sample decision tree on categorizing apps, “Group applications by risk to simplify policy creation (e.g. AAL1, AAL2, AAL3).”

Okta allows customers to classify apps based on their risk profile to determine requirements related to MFA frequency and assurance strength. Policies are configured in the Okta Admin Console at Security > Authentication Policies

**1 AAL1 Rule**

**IF** Any request

**THEN** Access: Allowed with any 1 factor type

Your org's authenticators that satisfy this requirement:

1 factor type

Duo Security or Email or Google Authenticator or Okta Verify or Password or Phone or FIDO2 (WebAuthn) or Spoke1 - Factor (IdP)

**If Okta FastPass is used:**  
The user must approve a prompt in Okta Verify or provide biometrics

**Re-authentication frequency is:** Every 30 days

Priority	Rule	Status	Actions
1	<b>Okta Authenticator Assurance Level 2 (Medium)</b>	ENABLED	Actions
	<b>IF</b> Group: Office Workers, Remote Workers Expression: Yes Device: Registered, Managed Device Assurance: Compliant Mac Device, Compliant Windows Device	<b>THEN</b> Access: Allowed with any 2 factor types	
		Your org's authenticators that satisfy this requirement: Knowledge / Biometric factor types Okta Verify <sup>1,3</sup> or Password or FIDO2 (WebAuthn) <sup>1,3</sup> AND Additional factor types Okta Verify <sup>1,3</sup> or FIDO2 (WebAuthn) <sup>1,3</sup> <sup>1</sup> Authenticator that may satisfy multiple factor requirements <sup>3</sup> Phishing resistance may vary based on combinations of apps, browser, operating system, and more. <a href="#">Learn more.</a>	
		<b>If Okta FastPass is used:</b> The user must approve a prompt in Okta Verify or provide biometrics	
		<b>Re-authentication frequency is:</b> Every 2 hours	
2	<b>Deny All if OAAAL2 is not met</b>	ENABLED	Actions
	<b>IF</b> Any request	<b>THEN</b> Access: Denied	

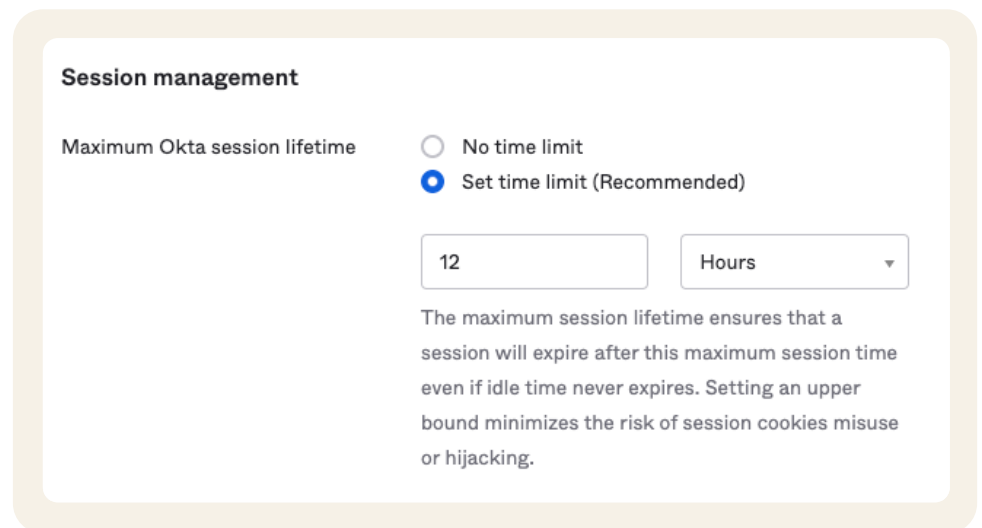
# Maximum Session Duration

NIST SP 800-63B (4.1.3 Reauthentication) also provides guidance on maximum session duration that states:

Periodic reauthentication of subscriber sessions SHALL be performed as described in Section 7.2. At AAL1, reauthentication of the subscriber SHOULD be repeated at least once per 30 days during an extended usage session, regardless of user activity. The session SHOULD be terminated (i.e., logged out) when this time limit is reached.

**Note: At AAL2 & AAL3 reauthentication is recommended every 12 hours.**

Okta recommends regular session reauthentication as a security best practice. Session Management options are configured in the Okta Admin Console at Security > Global Session Policy (see below):



The screenshot shows the 'Session management' configuration page in the Okta Admin Console. It features a section titled 'Maximum Okta session lifetime' with two radio button options: 'No time limit' (unselected) and 'Set time limit (Recommended)' (selected). Below the selected option, there is a text input field containing the number '12' and a dropdown menu set to 'Hours'. A descriptive paragraph below the form states: 'The maximum session lifetime ensures that a session will expire after this maximum session time even if idle time never expires. Setting an upper bound minimizes the risk of session cookies misuse or hijacking.'

Configuring a maximum session lifetime for your Okta session helps minimize the risk of session hijacking.



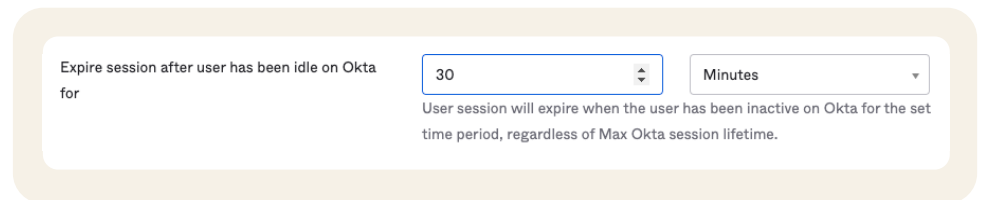
## Maximum idle time

NIST SP 800-63B (4.2.3 Reauthentication) provides guidance on idle timeouts, including:

At AAL2 ... reauthentication of the subscriber SHALL be repeated following any period of inactivity lasting 30 minutes or longer. The session SHALL be terminated (i.e., logged out) when either of these time limits is reached.

**Note: At AAL3, the most stringent level, the inactive timeout should be set to 15 minutes.**

Session idle timeouts can be an effective way to prevent session hijacking. Session idle timeout are configured in the Okta Admin Console at Security > Global Session Policy (see below):



Expire session after user has been idle on Okta for

User session will expire when the user has been inactive on Okta for the set time period, regardless of Max Okta session lifetime.

After a defined period of inactivity from first party Okta applications or Okta single sign-on to target applications, Okta will terminate the user session.

# Biometrics

NIST SP 800-63b (section 5.1.5.1 Multi-Factor One-time password (OTP) Authenticators) provides guidance on MFA with OTP, including:

Multi-factor OTP authenticators operate in a similar manner to single-factor OTP authenticators, except that they require the entry of either a memorized secret or the use of a biometric to obtain the OTP from the authenticator. Each use of the authenticator SHALL require the input of the additional factor.

The form of Okta Verify that can satisfy multiple factor requirements is FastPass and push notification with Biometrics.

The screenshot shows a configuration interface for multi-factor authentication. It includes several sections:

- AND User must authenticate with:** A dropdown menu set to "Any 2 factor types". Below it is a link: "Learn more about authentication scenarios".
- AND Possession factor constraints are:** Three checkboxes:
  - Phishing resistant
  - Hardware protected
  - Exclude phone and email authenticators
- AND Smart Card is:** A checkbox for "Required" which is currently unchecked.
- AND If Okta FastPass is used:** Two radio buttons:
  - The user must approve a prompt in Okta Verify or provide biometrics
  - The user is not required to approve a prompt in Okta Verify or provide biometrics

Below these sections is a box titled "Your org's authenticators that satisfy this requirement:" containing:

- Knowledge / Biometric factor types: Okta Verify<sup>1</sup> or Password or FIDO2 (WebAuthn)
- AND
- Additional factor types: Okta Verify<sup>1</sup>

A red box highlights the footnote: <sup>1</sup> Authenticator that may satisfy multiple factor requirements

**Note: For Okta Verify to satisfy multiple factor requirements it will need to satisfy the Additional factor types (Possession factor) and Biometric factor types .**

Below is a comparison between when a user authenticates with Okta Verify FastPass, Okta Verify Push and Okta Verify One Time Passcode (OTP). For Okta Verify FastPass, the authentication has the USER\_VERIFYING properties that are considered biometrics factor type.

MethodTypeUsed	Use Okta FastPass
MethodUsedVerifiedProperties	[DEVICE_BOUND, PHISHING_RESISTANT, USER_VERIFYING, USER_PRESENCE, HARDWARE_PROTECTED]
DisplayName	Okta Verify
ID	[REDACTED]
Type	AuthenticatorEnrollment

In the case of Okta Verify Push notification, the USER\_VERIFYING properties are considered biometrics factor type only if the user has biometrics enabled on the Okta Verify application.

MethodTypeUsed	Get a push notification
MethodUsedVerifiedProperties	[USER_PRESENCE, DEVICE_BOUND, USER_VERIFYING, HARDWARE_PROTECTED]
DisplayName	Okta Verify
ID	[REDACTED]
Type	AuthenticatorEnrollment

**Note: When factor properties don't include USER\_VERIFYING, it will not satisfy multiple factors requirements, so the user will be prompted for a second factor.**

## Conclusion

Awareness of the NIST SP 800-63B Digital Identity Guidelines is helpful for organizations striving to secure their digital environments effectively. Okta's solutions provide a robust framework for meeting these guidelines, ensuring that authentication processes are aligned with industry standards and best practices. By mapping NIST's authentication assurance levels to Okta's authenticator options, organizations can confidently implement secure, compliant authentication mechanisms across their user base.

The alignment of Okta's features with NIST guidelines not only supports federal agencies but also provides a strong foundation for any industry looking to enhance their security posture. With Okta's comprehensive approach to authentication, including the use of MFA, session management, and biometric verification, organizations are well-equipped to manage digital identities securely.

### About Okta

Okta is the leading independent Identity provider. We enable organizations to securely connect the right people to the right technologies at the right time. We provide simple and secure access to people and organizations everywhere, giving them confidence to reach their full potential. Learn more at [okta.com](https://okta.com).