CIS Okta Identity as a Service (IDaaS) STIG Benchmark

v1.0.0 - 08-21-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

Okta Identity as a Service (IDaaS) Secure Technical Implementation Guide (STIG)
Version: 1 Release: 1 Benchmark
Date: 22 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Okta Identity as a Service (IDaaS) and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Okta Identity as a Service (IDaaS)

Recommendations

1 STIG RULES

Okta IDaaS

Okta Identity as a Service (IDaaS) Secure Technical Implementation Guide (STIG)

Version: 1 Release: 1 Benchmark

Date: 22 Apr 2025

CLASSIFICATION unclassified

1.1 OKTA-APP-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must log out a session after a 15-minute period of inactivity.

```
GROUP ID: V-273186
RULE ID: SV-273186r1098825
```

Rationale:

A session timeout lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their application session prior to vacating the vicinity, applications must be able to identify when a user's application session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled. This is typically at the operating system level and results in a system lock. However, it may be at the application level where the application interface window is secured instead.

Satisfies: SRG-APP-000003, SRG-APP-000190

Audit:

From the Admin Console:

1. Select Security >> Global Session Policy.
2. In the Default Policy, verify a rule is configured at Priority 1 that is not named "Default Rule".
3. Click the edit icon next to the Priority 1 rule.
4. Verify the "Maximum Okta global session idle time" is set to 15 minutes.

If "Maximum Okta global session idle time" is not set to 15 minutes, this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Global Session Policy.
2. Select the Default Policy.
3. In the Rules table, make these updates:
    - Click "Add rule".
    - Set "Maximum Okta global session idle time" to 15 minutes.

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

1.2 OKTA-APP-000025 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Okta Admin Console must log out a session after a 15-minute period of inactivity.

```
GROUP ID: V-273187
RULE ID: SV-273187r1098828
```

Rationale:

A session timeout lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not log out because of the temporary nature of the absence. Rather than relying on the user to manually lock their application session prior to vacating the vicinity, applications must be able to identify when a user's application session has idled and take action to initiate the session lock.

The session lock is implemented at the point where session activity can be determined and/or controlled. This is typically at the operating system level and results in a system lock. However, it may be at the application level where the application interface window is secured instead.

Audit:

From the Admin Console:

1. Select Applications >> Applications >> Okta Admin Console.
2. In the Sign On tab, under "Okta Admin Console session", verify the "Maximum app session idle time" is set to 15 minutes.

If the "Maximum app session idle time" is not set to 15 minutes, this is a finding.

Remediation:

From the Admin Console:

1. Select Applications >> Applications >> Okta Admin Console.
2. In the Sign On tab, under "Okta Admin Console session", set the "Maximum app session idle time" to 15 minutes.

Additional Information:

CCI-000057 Prevent further access to the system by initiating a device lock after organization-defined time period of inactivity; and/or requiring the user to initiate a device lock before leaving the system unattended.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11.1 (ii)
- NIST SP 800-53 Revision 4::AC-11 a
- NIST SP 800-53 Revision 5::AC-11 a

1.3 OKTA-APP-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must automatically disable accounts after a 35-day period of account inactivity.

```
GROUP ID: V-273188
RULE ID: SV-273188r1098831
```

Rationale:

Attackers that are able to exploit an inactive account can potentially obtain and maintain undetected access to an application. Owners of inactive accounts will not notice if unauthorized access to their user account has been obtained. Applications must track periods of user inactivity and disable accounts after 35 days of inactivity. Such a process greatly reduces the risk that accounts will be hijacked, leading to a data compromise.

To address access requirements, many application developers choose to integrate their applications with enterprise-level authentication/access mechanisms that meet or exceed access control policy requirements. Such integration allows the application developer to off-load those access control functions and focus on core application features and functionality.

This policy does not apply to emergency accounts or infrequently used accounts. Infrequently used accounts are local login administrator accounts used by system administrators when network or normal login/access is not available. Emergency accounts are administrator accounts created in response to crisis situations.

Satisfies: SRG-APP-000025, SRG-APP-000163, SRG-APP-000700

Audit:

If Okta Services rely on external directory services for user sourcing, this is not applicable, and the connected directory services must perform this function.
Go to Workflows >> Automations and verify that an Automation has been created to disable accounts after 35 days of inactivity.
If the Okta configuration does not automatically disable accounts after a 35-day period of account inactivity, this is a finding.

Remediation:

From the Admin Console:

1. Go to Workflow >> Automations and select "Add Automation".
2. Create a name for the Automation (e.g., "User Inactivity").
3. Click "Add Condition" and select "User Inactivity in Okta".
4. In the duration field, enter 35 days and click "Save".
   5 Click the edit button next to "Select Schedule".
5. Configure the "Schedule" field for "Run Daily" and set the "Time" field to an organizationally defined time to run this automation. Click "Save".
6. Click the edit button next to "Select group membership".
7. In the "Applies to" field, select the group "Everyone" by typing it into the field. Click "Save".
8. Click "Add Action" and select "Change User lifecycle state in Okta".
9. In the "Change user state to" field, select "Suspended" and click "Save".
10. Click the "Inactive" button near the top of the section screen and select "Activate".

Additional Information:

CCI-000017 Disable accounts when the accounts have been inactive for the organization-defined time-period.

- NIST SP 800-53::AC-2 (3)
- NIST SP 800-53A::AC-2 (3).1 (ii)
- NIST SP 800-53 Revision 4::AC-2 (3)
- NIST SP 800-53 Revision 5::AC-2 (3) (d)

CCI-000795 The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53::IA-4 e
- NIST SP 800-53A::IA-4.1 (iii)
- NIST SP 800-53 Revision 4::IA-4 e

CCI-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5::AC-2 (3) (a)

1.4 OKTA-APP-000170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must enforce the limit of three consecutive invalid login attempts by a user during a 15-minute time period.

```
GROUP ID: V-273189
RULE ID: SV-273189r1098834
```

Rationale:

By limiting the number of failed login attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Satisfies: SRG-APP-000065, SRG-APP-000345

Audit:

If Okta Services rely on external directory services for user sourcing, this check is not applicable, and the connected directory services must perform this function.
From the Admin Console:

1. Go to Security >> Authenticators.
2. Click the "Actions" button next to "Password" and select "Edit".
3. For each Password Policy, verify the "Lock Out" section has the following values:
    - "Lock out after 3 unsuccessful attempts" is checked.
    - The value is set to "3".

If Okta Services are not configured to automatically lock user accounts after three consecutive invalid login attempts, this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Authenticators.
2. Click the "Actions" button next to "Password" and select "Edit".
3. For each Password Policy, ensure the "Lock Out" section has the following values:
    - "Lock out after 3 unsuccessful attempts" is checked.
    - The value is set to "3".

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

1.5 OKTA-APP-000180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Okta Dashboard application must be configured to allow authentication only via non-phishable authenticators.

```
GROUP ID: V-273190
RULE ID: SV-273190r1099763
```

Rationale:

Requiring the use of non-phishable authenticators protects against brute force/password dictionary attacks. This provides a better level of security while removing the need to lock out accounts after three attempts in 15 minutes.

Audit:

From the Admin Console:

1. Go to Security >> Authentication Policies.
2. Click the "Okta Dashboard" policy.
3. Click the "Actions" button next to the top rule and select "Edit".
4. In the "Possession factor constraints are" section, verify the "Phishing resistant" box is checked. This will ensure that only phishing-resistant factors are used to access the Okta Dashboard.

If in the "Possession factor constraints are" section the "Phishing resistant" box is not checked, this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Authentication Policies.
2. Click the "Okta Dashboard" policy.
3. Click the "Actions" button next to the top rule and select "Edit".
4. In the "Possession factor constraints are" section, ensure the "Phishing resistant" box is checked.

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

1.6 OKTA-APP-000190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Okta Admin Console application must be configured to allow authentication only via non-phishable authenticators.

```
GROUP ID: V-273191
RULE ID: SV-273191r1099764
```

Rationale:

Requiring the use of non-phishable authenticators protects against brute force/password dictionary attacks. This provides a better level of security while removing the need to lock out accounts after three attempts in 15 minutes.

Audit:

From the Admin Console:

1. Go to Security >> Authentication Policies.
2. Click the "Okta Admin Console" policy.
3. Click the "Actions" button next to the top rule and select "Edit".
4. In the "Possession factor constraints are" section, verify the "Phishing resistant" box is checked. This will ensure that only phishing-resistant factors are used to access the Okta Dashboard.

If in the "Possession factor constraints are" section the "Phishing resistant" box is not checked, this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Authentication Policies.
2. Click the "Okta Admin Console" policy.
3. Click the "Actions" button next to the top rule and select "Edit".
4. In the "Possession factor constraints are" section, ensure the "Phishing resistant" box is checked.

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

1.7 OKTA-APP-000200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must display the Standard Mandatory DOD Notice and Consent Banner before granting access to the application.

```
GROUP ID: V-273192
RULE ID: SV-273192r1098843
```

Rationale:

Display of the DOD-approved use notification before granting access to the application ensures that privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via login interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060. Use the following verbiage for applications that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read & consent to terms in IS user agreem't."
```

Satisfies: SRG-APP-000068, SRG-APP-000069, SRG-APP-000070

Audit:

Attempt to log in to the Okta tenant and verify the DOD-approved warning banner is in place.
If the required warning banner is not present and complete, this is a finding.

Remediation:

Follow the supplemental instructions in the "Okta DOD Warning Banner Configuration Guide" provided with this STIG package.

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-000050 Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (i)
- NIST SP 800-53 Revision 4::AC-8 c 1
- NIST SP 800-53 Revision 5::AC-8 c 1

CCI-001385 For publicly accessible systems, displays references, if any, to monitoring that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001386 For publicly accessible systems, displays references, if any, to recording that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001387 For publicly accessible systems, displays references, if any, to auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (ii)
- NIST SP 800-53 Revision 4::AC-8 c 2
- NIST SP 800-53 Revision 5::AC-8 c 2

CCI-001388 For publicly accessible systems, includes a description of the authorized uses of the system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (iii)
- NIST SP 800-53 Revision 4::AC-8 c 3
- NIST SP 800-53 Revision 5::AC-8 c 3

1.8 OKTA-APP-000560 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Okta Admin Console application must be configured to use multifactor authentication.

```
GROUP ID: V-273193
RULE ID: SV-273193r1098846
```

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include: (i) something a user knows (e.g., password/PIN); (ii) something a user has (e.g., cryptographic identification device, token); or (iii) something a user is (e.g., biometric).

A privileged account is defined as an information system account with authorizations of a privileged user.

Network access is defined as access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, or the internet).

Satisfies: SRG-APP-000149, SRG-APP-000154

Audit:

From the Admin Console:

1. Go to Security >> Authentication Policies.
2. Click the "Okta Admin Console" policy.
3. Click the "Actions" button next to the top rule and select "Edit".
4. In the "User must authenticate with" field, verify that either "Password/IdP + Another factor" or "Any 2 factor types" is selected.

If either of these settings is incorrect, this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Authentication Policies.
2. Click the "Okta Admin Console" policy.
3. Click the "Actions" button next to the top rule and select "Edit".
4. In the "User must authenticate with" field, select either "Password/IdP + Another factor" or "Any 2 factor types".

Additional Information:

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5::IA-2 (6) (a)

1.9 OKTA-APP-000570 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Okta Dashboard application must be configured to use multifactor authentication.

```
GROUP ID: V-273194
RULE ID: SV-273194r1098849
```

Rationale:

To ensure accountability and prevent unauthenticated access, nonprivileged users must use multifactor authentication to prevent potential misuse and compromise of the system.

Multifactor authentication uses two or more factors to achieve authentication.

Factors include: (i) Something you know (e.g., password/PIN); (ii) Something you have (e.g., cryptographic identification device, token); or (iii) Something you are (e.g., biometric).

A nonprivileged account is any information system account with authorizations of a nonprivileged user.

Network access is any access to an application by a user (or process acting on behalf of a user) where the access is obtained through a network connection.

Applications integrating with the DOD Active Directory and using the DOD CAC are examples of compliant multifactor authentication solutions.

Satisfies: SRG-APP-000150, SRG-APP-000155

Audit:

From the Admin Console:

1. Go to Security >> Authentication Policies.
2. Click the "Okta Dashboard" policy.
3. Click the "Actions" button next to the top rule and select "Edit".
4. In the "User must authenticate with" field, verify that either "Password/IdP + Another factor" or "Any 2 factor types" is selected.

If either of these settings is incorrect, this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Authentication Policies.
2. Click the "Okta Dashboard" policy.
3. Click the "Actions" button next to the top rule and select "Edit".
4. In the "User must authenticate with" field, select either "Password/IdP + Another factor" or "Any 2 factor types".

Additional Information:

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-004046 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.

- NIST SP 800-53 Revision 5::IA-2 (6) (a)

1.10 OKTA-APP-000650 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must enforce a minimum 15-character password length.

```
GROUP ID: V-273195
RULE ID: SV-273195r1098852
```

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Audit:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy, verify the "Minimum Length" field is set to at least "15" characters.

If any policy is not set to at least "15", this is a finding.

Remediation:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy:
    - Click "Edit".
    - Set the "Minimum Length" field to at least "15" characters.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.11 OKTA-APP-000670 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must enforce password complexity by requiring that at least one uppercase character be used.

```
GROUP ID: V-273196
RULE ID: SV-273196r1098855
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password is, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy, verify "Upper case letter" is checked.

For each policy, if "Upper case letter" is not checked, this is a finding.

Remediation:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy:
   - Click "Edit".
   - Set "Upper case letter" to checked.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.12 OKTA-APP-000680 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must enforce password complexity by requiring that at least one lowercase character be used.

```
GROUP ID: V-273197
RULE ID: SV-273197r1098858
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy, verify "Lower case letter" is checked.

For each policy, if "Lower case letter" is not checked, this is a finding.

Remediation:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy:
   - Click "Edit".
   - Set "Lower case letter" to checked.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.13 OKTA-APP-000690 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must enforce password complexity by requiring that at least one numeric character be used.

```
GROUP ID: V-273198
RULE ID: SV-273198r1098861
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy, verify "Number (0-9)" is checked.

For each policy, if "Number (0-9)" is not checked, this is a finding.

Remediation:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy:
    - Click "Edit".
    - Set "Number (0-9)" to checked.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.14 OKTA-APP-000700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must enforce password complexity by requiring that at least one special character be used.

```
GROUP ID: V-273199
RULE ID: SV-273199r1098864
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor in determining how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Special characters are not alphanumeric. Examples include: ~ ! @ # $ % ^ *.

Audit:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy, verify "Symbol (e.g., !@#$%^&*)" is checked.

For each policy, if "Symbol (e.g., !@#$%^&*)" is not checked, this is a finding.

Remediation:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy:
    - Click "Edit".
    - Set "Symbol (e.g., !@#$%^&*)" to checked.

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.15 OKTA-APP-000740 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must enforce 24 hours/one day as the minimum password lifetime.

```
GROUP ID: V-273200
RULE ID: SV-273200r1098867
```

Rationale:

Enforcing a minimum password lifetime helps prevent repeated password changes to defeat the password reuse or history enforcement requirement.

Restricting this setting limits the user's ability to change their password. Passwords must be changed at specific policy-based intervals; however, if the application allows the user to immediately and continually change their password, it could be changed repeatedly in a short period of time to defeat the organization's policy regarding password reuse.

Satisfies: SRG-APP-000173, SRG-APP-000870

Audit:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy, verify "Minimum password age is XX hours" is set to at least "24".

For each policy, if "Minimum password age is XX hours" is not set to at least "24", this is a finding.

Remediation:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy:
    - Click "Edit".
    - Set "Minimum password age is XX hours" to at least "24".

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.16 OKTA-APP-000745 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must enforce a 60-day maximum password lifetime restriction.

```
GROUP ID: V-273201
RULE ID: SV-273201r1098870
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords must be changed at specific intervals.

One method of minimizing this risk is to use complex passwords and periodically change them. If the application does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the system and/or application passwords could be compromised.

This requirement does not include emergency administration accounts, which are meant for access to the application in case of failure. These accounts are not required to have maximum password lifetime restrictions.

Audit:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy, verify "Password expires after XX days" is set to "60".

For each policy, if "Password expires after XX days" is not set to "60", this is a finding.

Remediation:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy:
   - Click "Edit".
   - Set "Password expires after XX days" to "60".

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

1.17 OKTA-APP-001430 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Okta must off-load audit records onto a central log server.

```
GROUP ID: V-273202
RULE ID: SV-273202r1099766
```

Rationale:

Information stored in one location is vulnerable to accidental or incidental deletion or alteration.

Off-loading is a common process in information systems with limited audit storage capacity.

Satisfies: SRG-APP-000358, SRG-APP-000080, SRG-APP-000125

Audit:

From the Admin Console:

1. Go to Reports >> Log Streaming.
2. Verify that a Log Stream connection is configured and active.

Alternately, interview the information system security manager (ISSM) and verify that an external Security Information and Event Management (SIEM) system is pulling Okta logs via an Application Programming Interface (API).
If either of these is not configured, this is a finding.

Remediation:

From the Admin Console:

1. Go to Reports >> Log Streaming.
2. Select either "AWS EventBridge" or "Splunk Cloud" and click "Next".
3. Complete the necessary fields and click "Save".

If Log Streaming is not an option because the SIEM required is not an option, customers can use the Okta Log API to export system logs in real time.

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

CCI-000166 Provide irrefutable evidence that an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

- NIST SP 800-53::AU-10
- NIST SP 800-53A::AU-10.1
- NIST SP 800-53 Revision 4::AU-10
- NIST SP 800-53 Revision 5::AU-10

CCI-001348 Store audit records on an organization-defined frequency in a repository that is part of a physically different system or system component than the system or component being audited.

- NIST SP 800-53::AU-9 (2)
- NIST SP 800-53A::AU-9 (2).1 (iii)
- NIST SP 800-53 Revision 4::AU-9 (2)
- NIST SP 800-53 Revision 5::AU-9 (2)

1.18 OKTA-APP-001665 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must be configured to limit the global session lifetime to 18 hours.

```
GROUP ID: V-273203
RULE ID: SV-273203r1099958
```

Rationale:

Without reauthentication, users may access resources or perform tasks for which they do not have authorization.

When applications provide the capability to change security roles or escalate the functional capability of the application, it is critical the user reauthenticate.

In addition to the reauthentication requirements associated with session locks, organizations may require reauthentication of individuals and/or devices in other situations, including (but not limited to) the following circumstances.

(i) When authenticators change; (ii) When roles change; (iii) When security categories of information systems change; (iv) When the execution of privileged functions occurs; (v) After a fixed period of time; or (vi) Periodically.

Within the DOD, the minimum circumstances requiring reauthentication are privilege escalation and role changes.

Audit:

From the Admin Console:

1. Select Security >> Global Session Policy.
2. In the Default Policy, verify a rule is configured at Priority 1 that is not named "Default Rule".
3. Click the "Edit" icon next to the Priority 1 rule.
4. Verify "Maximum Okta global session lifetime" is set to 18 hours.

If the above is not set, this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Global Session Policy.
2. Select the Default Policy.
3. In the Rules table, make these updates:
    - Click "Add rule".
    - Set "Maximum Okta global session lifetime" to 18 hours.

Additional Information:

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

1.19 OKTA-APP-001670 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must be configured to accept Personal Identity Verification (PIV) credentials.

```
GROUP ID: V-273204
RULE ID: SV-273204r1098879
```

Rationale:

The use of PIV credentials facilitates standardization and reduces the risk of unauthorized access.

DOD has mandated the use of the common access card (CAC) to support identity management and personal authentication for systems covered under HSPD 12, as well as a primary component of layered protection for national security systems.

Satisfies: SRG-APP-000391, SRG-APP-000402, SRG-APP-000403

Audit:

From the Admin Console:

1. Go to Security >> Authenticators.
2. Verify that "Smart Card Authenticator" is listed and has "Status" listed as "Active".

If "Smart Card Authenticator" is not listed or is not listed as "Active", this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Authenticators.
2. In the "Setup" tab, click "Add authenticator".
3. Select the configured Smart Card Identity Provider and finish configuration.

Additional Information:

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-002009 Accept Personal Identity Verification-compliant credentials from other federal agencies.

- NIST SP 800-53 Revision 4::IA-8 (1)
- NIST SP 800-53 Revision 5::IA-8 (1)

CCI-002010 Electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

- NIST SP 800-53 Revision 4::IA-8 (1)
- NIST SP 800-53 Revision 5::IA-8 (1)

1.20 OKTA-APP-001700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Okta Verify application must be configured to connect only to FIPS-compliant devices.

```
GROUP ID: V-273205
RULE ID: SV-273205r1098882
```

Rationale:

Without device-to-device authentication, communications with malicious devices may be established. Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk. Currently, DOD requires the use of AES for bidirectional authentication because it is the only FIPS-validated AES cipher block algorithm.

For distributed architectures (e.g., service-oriented architectures), the decisions regarding the validation of authentication claims may be made by services separate from the services acting on those decisions. In such situations, it is necessary to provide authentication decisions (as opposed to the actual authenticators) to the services that need to act on those decisions.

A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area or wide area network; the internet). A remote connection is any connection with a device communicating through an external network (e.g., the internet).

Because of the challenges of applying this requirement on a large scale, organizations are encouraged to apply the requirement only to those limited number (and type) of devices that truly need to support this capability.

Audit:

From the Admin Console:

1. Go to Security >> Authenticators.
2. From the "Setup" tab, select "Edit Okta Verify".
3. Review the "FIPS Compliance" field.

If FIPS-compliant authentication is not enabled, this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Authenticators.
2. From the "Setup" tab, select "Edit Okta Verify".
3. In the "FIPS Compliance" field, choose whether users enrolling in Okta Verify can use FIPS-compliant devices only or any device.
4. Click "Save" after making any changes.

Additional Information:

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

1.21 OKTA-APP-001710 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must be configured to disable persistent global session cookies.

```
GROUP ID: V-273206
RULE ID: SV-273206r1098885
```

Rationale:

If cached authentication information is out of date, the validity of the authentication information may be questionable.

Satisfies: SRG-APP-000400, SRG-APP-000157

Audit:

From the Admin Console:

1. Select Security >> Global Session Policy.
2. In the Default Policy, verify a rule is configured at Priority 1 that is not named "Default Rule".
3. Click the "Edit" icon next to the Priority 1 rule.
4. Verify "Okta global session cookies persist across browser sessions" is set to "Disabled".

If the above it not set, this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Global Session Policy.
2. Select the Default Policy.
3. In the "Rules" table, make these updates:
    - Click "Add rule".
    - Set "Okta global session cookies persist across browser sessions" to Disable.

Additional Information:

CCI-002007 Prohibit the use of cached authenticators after an organization-defined time period.

- NIST SP 800-53 Revision 4::IA-5 (13)
- NIST SP 800-53 Revision 5::IA-5 (13)

CCI-001942 The information system implements replay-resistant authentication mechanisms for network access to non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (9)

1.22 OKTA-APP-001920 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must be configured to use only DOD-approved certificate authorities.

```
GROUP ID: V-273207
RULE ID: SV-273207r1098888
```

Rationale:

Untrusted Certificate Authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DOD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not DOD approved, trust of this CA has not been established.

The DOD will accept only PKI certificates obtained from a DOD-approved internal or external CA. Reliance on CAs for the establishment of secure sessions includes, for example, the use of Transport Layer Security (TLS) certificates.

This requirement focuses on communications protection for the application session rather than for the network packet.

This requirement applies to applications that use communications sessions. This includes, but is not limited to, web-based applications and Service-Oriented Architectures (SOA).

Satisfies: SRG-APP-000427, SRG-APP-000910

Audit:

From the Admin Console:

1. Select Security >> Identity Providers (IdPs).
2. Review the list of IdPs with "Type" as "Smart Card".

If the IdP is not listed as "Active", this is a finding.

3. Select Actions >> Configure.
4. Under "Certificate chain", verify the certificate is from a DOD-approved CA.

If the certificate is not from a DOD-approved CA, this is a finding.

Remediation:

From the Admin Console:

1. Go to Security >> Identity Providers.
2. Click "Add identity provider."
3. Click "Smart Card IdP". Click "Next".
4. Enter the name of the identity provider.
5. Build a certificate chain:
    - Click "Browse" to open a file explorer. Select the certificate file to add and click "Open".
    - To add another certificate, click "Add Another" and repeat step 1.
    - Click "Build certificate chain". On success, the chain and its certificates are shown. If the build failed, correct any issues and try again.
    - Click "Reset certificate chain" if replacing the current chain with a new one.
6. In "IdP username", select the "idpuser.subjectAltNameUpn" attribute. This is the attribute that stores the Electronic Data Interchange Personnel Identifier (EDIPI) on the CAC.
7. In the "Match Against" field, select the Okta Profile Attribute in which the EDIPI is to be stored.

Additional Information:

CCI-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

CCI-004909 Include only approved trust anchors in trust stores or certificate stores managed by the organization.

- NIST SP 800-53 Revision 5::SC-17 b

1.23 OKTA-APP-002980 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must validate passwords against a list of commonly used, expected, or compromised passwords.

```
GROUP ID: V-273208
RULE ID: SV-273208r1099769
```

Rationale:

Password-based authentication applies to passwords regardless of whether they are used in single-factor or multifactor authentication.

Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten.

Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

Audit:

From the Admin Console:

1. Navigate to Security >> Authenticators.
2. Click the "Actions" button next to the Password authenticator and select "Edit".
3. Under the "Password Settings" section, verify the "Common Password Check" box is checked.

If "Common Password Check" is not selected, this is a finding.

Remediation:

From the Admin Console:

1. Navigate to Security >> Authenticators.
2. Click the "Actions" button next to the Password authenticator and select "Edit".
3. Under the "Password Settings" section, check the "Common Password Check" box.

Additional Information:

CCI-004058 For password-based authentication, maintain a list of commonly used, expected, or compromised passwords on an organization-defined frequency.

- NIST SP 800-53 Revision 5::IA-5 (1) (a)

1.24 OKTA-APP-003010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Okta must prohibit password reuse for a minimum of five generations.

```
GROUP ID: V-273209
RULE ID: SV-273209r1098894
```

Rationale:

Password-based authentication applies to passwords regardless of whether they are used in single-factor or multifactor authentication.

Long passwords or passphrases are preferable over shorter passwords. Enforced composition rules provide marginal security benefits while decreasing usability. However, organizations may choose to establish certain rules for password generation (e.g., minimum character length for long passwords) under certain circumstances and can enforce this requirement in IA-5(1)(h). Account recovery can occur, for example, in situations when a password is forgotten.

Cryptographically protected passwords include salted one-way cryptographic hashes of passwords. The list of commonly used, compromised, or expected passwords includes passwords obtained from previous breach corpuses, dictionary words, and repetitive or sequential characters. The list includes context-specific words, such as the name of the service, username, and derivatives thereof.

Audit:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password row" and select "Edit".
3. For each listed policy, verify "Enforce password history for last XX passwords" is set to "5".

If any policy is not set to at least "5", this is a finding.

Remediation:

From the Admin Console:

1. Select Security >> Authenticators.
2. Click the "Actions" button next to the "Password" row and select "Edit".
3. For each listed policy:
    - Click "Edit".
    - Set "Enforce password history for last XX passwords" to "5".

Additional Information:

CCI-004061 For password-based authentication, verify when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5 (1) (a).

- NIST SP 800-53 Revision 5::IA-5 (1) (b)

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	OKTA-APP-000020 (Manual)	□	□
1.2	OKTA-APP-000025 (Manual)	□	□
1.3	OKTA-APP-000090 (Manual)	□	□
1.4	OKTA-APP-000170 (Manual)	□	□
1.5	OKTA-APP-000180 (Manual)	□	□
1.6	OKTA-APP-000190 (Manual)	□	□
1.7	OKTA-APP-000200 (Manual)	□	□
1.8	OKTA-APP-000560 (Manual)	□	□
1.9	OKTA-APP-000570 (Manual)	□	□
1.10	OKTA-APP-000650 (Manual)	□	□
1.11	OKTA-APP-000670 (Manual)	□	□
1.12	OKTA-APP-000680 (Manual)	□	□
1.13	OKTA-APP-000690 (Manual)	□	□
1.14	OKTA-APP-000700 (Manual)	□	□
1.15	OKTA-APP-000740 (Manual)	□	□
1.16	OKTA-APP-000745 (Manual)	□	□
1.17	OKTA-APP-001430 (Manual)	□	□
1.18	OKTA-APP-001665 (Manual)	□	□
1.19	OKTA-APP-001670 (Manual)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	OKTA-APP-001700 (Manual)	□	□
1.21	OKTA-APP-001710 (Manual)	□	□
1.22	OKTA-APP-001920 (Manual)	□	□
1.23	OKTA-APP-002980 (Manual)	□	□
1.24	OKTA-APP-003010 (Manual)	□	□

Appendix: Change History

Date	Version	Changes for this version
Aug 19, 2025	1.0.0	Initial CIS Release