# CIS Apache Server 2.4 Windows Server Security Technical Implementation Guide STIG Benchmark

v1.0.0 - 09-10-2025

# 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

Apache Server 2.4 Windows Server Security Technical Implementation Guide Secure Technical Implementation Guide (STIG)
Version: 3 Release: 3 Benchmark
Date: 02 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 Apache Server 2.4 Windows Server Security Technical Implementation Guide 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

The Rule Title from the STIG

## 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

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

## 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 Apache Server 2.4 Windows Server Security Technical Implementation Guide

# Recommendations

## 1 STIG RULES

Apache HTTP Server 2.4

Apache Server 2.4 Windows Server Security Technical Implementation Guide Secure Technical Implementation Guide (STIG)

Version: 3 Release: 3 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

## *1.1 AS24-W1-000010 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must limit the number of allowed simultaneous session requests.

```
GROUP ID: V-214306
RULE ID: SV-214306r960735
```

**Rationale:**

Apache web server management includes the ability to control the number of users and user sessions that utilize an Apache web server. Limiting the number of allowed users and sessions per user is helpful in limiting risks related to several types of denial-of-service (DoS) attacks.

Although there is some latitude concerning the settings, they should follow DoD-recommended values, but the settings should be configurable to allow for future DoD direction. While the DoD will specify recommended values, the values can be adjusted to accommodate the operational requirement of a given system.

**Audit:**

With an editor, open the configuration file:
\Apache24\conf\extra\httpd-default
Search for the following directive:
MaxKeepAliveRequests
Verify the value is "100" or greater.
If the "MaxKeepAliveRequests" directive is not "100" or greater, this is a finding.

**Remediation:**

With an editor, open the configuration file:
\conf\extra\httpd-default
Search for the following directive:
MaxKeepAliveRequests
Set the "MaxKeepAliveRequests" directive to a value of "100" or greater. Add the "MaxKeepAliveRequests" directive if it does not exist.
It is recommended that the "MaxKeepAliveRequests" directive be explicitly set to prevent unexpected results if the defaults change with updated software.

**Additional Information:**

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

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

## *1.2 AS24-W1-000020 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must perform server-side session management.

```
GROUP ID: V-214307
RULE ID: SV-214307r960735
```

**Rationale:**

Session management is the practice of protecting the bulk of the user authorization and identity information. Storing of this data can occur on the client system or on the server.

When the session information is stored on the client, the session ID, along with the user authorization and identity information, is sent along with each client request and is stored in a cookie, embedded in the uniform resource locator (URL), or placed in a hidden field on the displayed form. Each of these offers advantages and disadvantages. The biggest disadvantage to all three is the possibility of the hijacking of a session along with all of the user's credentials.

When the user authorization and identity information is stored on the server in a protected and encrypted database, the communication between the client and Apache web server will only send the session identifier, and the server can then retrieve user credentials for the session when needed. If, during transmission, the session were to be hijacked, the user's credentials would not be compromised.

**Audit:**

In a command line, navigate to "<'INSTALLED PATH'>\bin". Run "httpd -M" to view a list of installed modules.
If "mod_session" module and "mod_usertrack" are not enabled, this is a finding.
session_module (shared)
usertrack_module (shared)

**Remediation:**

Uncomment the "usertrack_module" module line and the "session_module" module in the <'INSTALL PATH'>\conf\httpd.conf file.
Restart the Apache service.
Additional documentation can be found at:
https://httpd.apache.org/docs/2.4/mod/mod_usertrack.html
https://httpd.apache.org/docs/2.4/mod/mod_session.html

**Additional Information:**

CCI-000054 Limit the number of concurrent sessions for each organization-defined account and/or account type to an organization-defined number.

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

## *1.3 AS24-W1-000030 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must use encryption strength in accordance with the categorization of data hosted by the Apache web server when remote connections are provided.

```
GROUP ID: V-214308
RULE ID: SV-214308r1067789
```

**Rationale:**

The Apache web server has several remote communications channels. Examples are user requests via http/https, communication to a backend database, and communication to authenticate users. The encryption used to communicate must match the data that is being retrieved or presented.

Methods of communication are "http" for publicly displayed information, "https" to encrypt when user data is being transmitted, VPN tunneling, or other encryption methods to a database.

Satisfies: SRG-APP-000014-WSR-000006, SRG-APP-000015-WSR-000014, SRG-APP-000033-WSR-000169, SRG-APP-000179-WSR-000110, SRG-APP-000179-WSR-000111, SRG-APP-000439-WSR-000152, SRG-APP-000439-WSR-000154, SRG-APP-000439-WSR-000188, SRG-APP-000442-WSR-000182

**Audit:**

In a command line, navigate to "<'INSTALLED PATH'>\bin". Run "httpd -M" to view a list of installed modules.
If the "ssl_module" is not enabled, this is a finding.
Review the <'INSTALL PATH'>\conf\httpd.conf file to determine if the "SSLProtocol" directive exists and looks like the following:
SSLProtocol -ALL +TLSv1.2 -SSLv2 -SSLv3
If the directive does not exist or exists but does not contain "-ALL +TLSv1.2 -SSLv2 -SSLv3", this is a finding.

**Remediation:**

Ensure the "ssl_module" is loaded in the httpd.conf file (not commented out).
Ensure the "SSLProtocol" is added and looks like the following in the <'INSTALL PATH'>\conf\httpd.conf file:
SSLProtocol -ALL +TLSv1.2
Restart the Apache service.

**Additional Information:**

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-000213 Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

- NIST SP 800-53::AC-3
- NIST SP 800-53A::AC-3.1
- NIST SP 800-53 Revision 4::AC-3
- NIST SP 800-53 Revision 5::AC-3

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

## *1.4 AS24-W1-000065 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

System logging must be enabled.

```
GROUP ID: V-214309
RULE ID: SV-214309r961863
```

**Rationale:**

The server error logs are invaluable because they can also be used to identify potential problems and enable proactive remediation. Log data can reveal anomalous behavior such as "not found" or "unauthorized" errors that may be an evidence of attack attempts. Failure to enable error logging can significantly reduce the ability of Web Administrators to detect or remediate problems. The CustomLog directive specifies the log file, syslog facility, or piped logging utility.

**Audit:**

In a command line, navigate to "<'INSTALLED PATH'>\bin\conf".
Edit the "httpd.conf" file and search for the directive "CustomLog".
If the "CustomLog" directive is missing or does not look like the following, this is a finding:
CustomLog "Logs/access_log" common

**Remediation:**

Edit the httpd.conf file and enter the name, path, and level for the CustomLog.

**Additional Information:**

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

## *1.5 AS24-W1-000070 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must generate, at a minimum, log records for system startup and shutdown, system access, and system authentication events.

```
GROUP ID: V-214310
RULE ID: SV-214310r960879
```

**Rationale:**

Log records can be generated from various components within the Apache web server (e.g., httpd, plug-ins to external backends, etc.). From a web server perspective, certain specific Apache web server functionalities may be logged as well. The Apache web server must allow the definition of what events are to be logged. As conditions change, the number and types of events to be logged may change, and the Apache web server must be able to facilitate these changes.

The minimum list of logged events should be those pertaining to system startup and shutdown, system access, and system authentication events. If these events are not logged at a minimum, any type of forensic investigation would be missing pertinent information needed to replay what occurred.

Satisfies: SRG-APP-000089-WSR-000047, SRG-APP-000092-WSR-000055

**Audit:**

In a command line, navigate to "<'INSTALLED PATH'>\bin". Run "httpd -M" to view a list of installed modules.
If the "log_config_module" is not enabled, this is a finding.

**Remediation:**

Uncomment the "log_config_module" module line in the <'INSTALL PATH'>\conf\httpd.conf file.
Restart the Apache service.

**Additional Information:**

CCI-000169 Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2 a on organization-defined information system components.

- NIST SP 800-53::AU-12 a
- NIST SP 800-53A::AU-12.1 (ii)
- NIST SP 800-53 Revision 4::AU-12 a

- NIST SP 800-53 Revision 5::AU-12 a

CCI-001464 Initiates session audits automatically at system start-up.

- NIST SP 800-53::AU-14 (1)
- NIST SP 800-53A::AU-14 (1).1
- NIST SP 800-53 Revision 4::AU-14 (1)
- NIST SP 800-53 Revision 5::AU-14 (1)

## *1.6 AS24-W1-000090 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must produce log records containing sufficient information to establish what type of events occurred.

```
GROUP ID: V-214311
RULE ID: SV-214311r962395
```

**Rationale:**

Web server logging capability is critical for accurate forensic analysis. Without sufficient and accurate information, a correct replay of the events cannot be determined.

Ascertaining the correct type of event that occurred is important during forensic analysis. The correct determination of the event and when it occurred is important in relation to other events that happened at that same time.

Without sufficient information establishing what type of log event occurred, investigation into the cause of event is severely hindered. Log record content that may be necessary to satisfy the requirement of this control includes but is not limited to time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, file names involved, access control, and flow control rules invoked.

Satisfies: SRG-APP-000095-WSR-000056, SRG-APP-000096-WSR-000057, SRG-APP-000097-WSR-000058, SRG-APP-000098-WSR-000059, SRG-APP-000099-WSR-000061, SRG-APP-000100-WSR-000064

**Audit:**

Items to be logged are as shown in this sample line in the <'INSTALL PATH'>\conf\httpd.conf file:
LogFormat "%a %A %h %H %l %m %s %t %u %U "%{Referer}i" " combined
If the web server is not configured to capture the required audit events for all sites and virtual directories, this is a finding.

**Remediation:**

Configure the "LogFormat" in the "httpd.conf" file to look like the following:
LogFormat "%a %A %h %H %l %m %s %t %u %U "%{Referer}i" " combined
Restart the Apache service.
NOTE: Your log format may be using different variables based on your environment, however, it should be verified to be producing the same end result of logged elements.

**Additional Information:**

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

CCI-000131 Ensure that audit records containing information that establishes when the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 b

CCI-000132 Ensure that audit records containing information that establishes where the event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 c

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

CCI-000134 Ensure that audit records containing information that establishes the outcome of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 e

CCI-001487 Ensure that audit records containing information that establishes the identity of any individuals, subjects, or objects/entities associated with the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1

- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 f

## *1.7 AS24-W1-000130 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

An Apache web server, behind a load balancer or proxy server, must produce log records containing the client IP information as the source and destination and not the load balancer or proxy IP information with each event.

```
GROUP ID: V-214312
RULE ID: SV-214312r960900
```

**Rationale:**

Apache web server logging capability is critical for accurate forensic analysis. Without sufficient and accurate information, a correct replay of the events cannot be determined.

Ascertaining the correct source, e.g., source IP, of the events is important during forensic analysis. Correctly determining the source will add information to the overall reconstruction of the logable event. By determining the source of the event correctly, analysis of the enterprise can be undertaken to determine if the event compromised other assets within the enterprise.

Without sufficient information establishing the source of the logged event, investigation into the cause of event is severely hindered. Log record content that may be necessary to satisfy the requirement of this control includes but is not limited to time stamps, source and destination IP addresses, user/process identifiers, event descriptions, application-specific events, success/fail indications, file names involved, access control, and flow control rules invoked.

**Audit:**

Interview the System Administrator to review the configuration of the Apache web server architecture and determine if inbound web traffic is passed through a proxy.
If the Apache web server is receiving inbound web traffic through a proxy, the audit logs must be reviewed to determine if correct source information is being passed through by the proxy server.
View Apache log files as configured in "httpd.conf" files.
When the log file is displayed, review source IP information in log entries and verify the entries do not reflect the IP address of the proxy server.
If the log entries in the log file(s) reflect the IP address of the proxy server as the source, this is a finding.

**Remediation:**

Access the proxy server through which inbound web traffic is passed and configure settings to pass web traffic to the Apache web server transparently.

**Additional Information:**

CCI-000133 Ensure that audit records containing information that establishes the source of the event.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 d

## *1.8 AS24-W1-000160 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must use a logging mechanism that is configured to alert the (ISSO) and System Administrator (SA) in the event of a processing failure.

```
GROUP ID: V-214313
RULE ID: SV-214313r960912
```

**Rationale:**

Reviewing log data allows an investigator to recreate the path of an attacker and to capture forensic data for later use. Log data is also essential to system administrators in their daily administrative duties on the hosted system or within the hosted applications.

If the logging system begins to fail, events will not be recorded. Organizations must define logging failure events, at which time the application or the logging mechanism the application uses will provide a warning to the ISSO and SA at a minimum.

**Audit:**

Work with the SIEM administrator to determine if an alert is configured when audit data is no longer received as expected.
If there is no alert configured, this is a finding.

**Remediation:**

Work with the SIEM administrator to configure an alert when no audit data is received from Apache based on the defined schedule of connections.

**Additional Information:**

CCI-000139 Alert organization-defined personnel or roles within an organization-defined time period in the event of an audit logging process failure.

- NIST SP 800-53::AU-5 a
- NIST SP 800-53A::AU-5.1 (ii)
- NIST SP 800-53 Revision 4::AU-5 a
- NIST SP 800-53 Revision 5::AU-5 a

## *1.9 AS24-W1-000180 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server log files must only be accessible by privileged users.

```
GROUP ID: V-214314
RULE ID: SV-214314r960930
```

**Rationale:**

Log data is essential in the investigation of events. If log data were to become compromised, competent forensic analysis and discovery of the true source of potentially malicious system activity would be difficult, if not impossible, to achieve. In addition, access to log records provides information an attacker could potentially use to their advantage since each event record might contain communication ports, protocols, services, trust relationships, user names, etc.

The web server must protect the log data from unauthorized read, write, copy, etc. This can be done by the web server if the web server is also doing the logging function. The web server may also use an external log system. In either case, the logs must be protected from access by non-privileged users.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file to determine the location of the logs. Determine permissions for log files. From the command line, navigate to the directory where the log files are located and enter the following command:
icacls <'Apache Directory'>\logs*
ex: icacls c:\Apache24\logs*
Only the Auditors, Web Managers, Administrators, and the account that runs the web server should have permissions to the files.
If any users other than those authorized have read access to the log files, this is a finding.

**Remediation:**

To maintain the integrity of the data that is being captured in the log files, ensure that only the members of the Auditors group, Administrators, and the user assigned to run the web server software are granted permissions to read the log files.

**Additional Information:**

CCI-000162 Protect audit information from unauthorized access.

- NIST SP 800-53::AU-9

- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## *1.10 AS24-W1-000200 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The log information from the Apache web server must be protected from unauthorized deletion and modification.

```
GROUP ID: V-214315
RULE ID: SV-214315r960936
```

**Rationale:**

Log data is essential in the investigation of events. The accuracy of the information is always pertinent. Information that is not accurate does not help in the revealing of potential security risks and may hinder the early discovery of a system compromise. One of the first steps an attacker will undertake is the modification or deletion of log records to cover his tracks and prolong discovery.

The web server must protect the log data from unauthorized modification. This can be done by the web server if the web server is also doing the logging function. The web server may also use an external log system. In either case, the logs must be protected from modification by non-privileged users.

Satisfies: SRG-APP-000120-WSR-000070, SRG-APP-000119-WSR-000069

**Audit:**

Query the System Administrator (SA) to determine who has update access to the web server log files.
The role of auditor and the role of SA should be distinctly separate. An individual functioning as an auditor should not also serve as an SA due to a conflict of interest.
Only management-authorized individuals with a privileged ID or group ID associated with an auditor role will have access permission to log files that are greater than read on web servers he or she has been authorized to audit.
Only management-authorized individuals with a privileged ID or group ID associated with either an SA or Web Administrator role may have read authority to log files for the web servers he or she has been authorized to administer.
If an account with roles other than auditor has greater than read authority to the log files, this is a finding.
Obtain the log location by reviewing the <'INSTALL PATH'>\conf\httpd.conf file.
Click the "Browse" button and navigate to the directory where the log files are stored.
Right-click the log file name to review and click "Properties".
Click the "Security" tab.
If an account associated with roles other than auditors, SAs, or Web Administrators has any access to log files, this is a finding.
If an account with roles other than auditor has greater than read authority to the log files, this is a finding.
This check does not apply to service account IDs used by automated services necessary to process, manage, and store log files.

**Remediation:**

Obtain the log location by reviewing the <'INSTALL PATH'>\conf\httpd.conf file.
Click the "Browse" button and navigate to the directory where the log files are stored.
Right-click the log file name to review and click "Properties".
Click the "Security" tab.
Set the log file permissions for the appropriate group(s).
Click "OK".
Select "Apply" in the "Actions" pane.

**Additional Information:**

CCI-000163 Protect audit information from unauthorized modification.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1
- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

CCI-000164 Protect audit information from unauthorized deletion.

- NIST SP 800-53::AU-9
- NIST SP 800-53A::AU-9.1

- NIST SP 800-53 Revision 4::AU-9
- NIST SP 800-53 Revision 5::AU-9 a

## *1.11 AS24-W1-000210 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The log data and records from the Apache web server must be backed up onto a different system or media.

```
GROUP ID: V-214316
RULE ID: SV-214316r960948
```

**Rationale:**

Protection of log data includes ensuring log data is not accidentally lost or deleted. Backing up log records to an unrelated system or onto separate media than the system the web server is actually running on helps to ensure that, in the event of a catastrophic system failure, the log records will be retained.

**Audit:**

Interview the Information System Security Officer (ISSO), System Administrator (SA), Web Manager, Webmaster, or developers as necessary to determine whether a tested and verifiable backup strategy has been implemented for web server software as well as all web server data files.
Proposed Questions:
Who maintains the backup and recovery procedures?
Do you have a copy of the backup and recovery procedures?
Where is the off-site backup location?
Is the contingency plan documented?
When was the last time the contingency plan was tested?
Are the test dates and results documented?
If there is not a backup and recovery process for the web server, this is a finding.

**Remediation:**

Document the web server backup procedures.

**Additional Information:**

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)

## *1.12 AS24-W1-000240 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must not perform user management for hosted applications.

```
GROUP ID: V-214318
RULE ID: SV-214318r960963
```

**Rationale:**

User management and authentication can be an essential part of any application hosted by the web server. Along with authenticating users, the user management function must perform several other tasks such as password complexity, locking users after a configurable number of failed logons, and management of temporary and emergency accounts. All of this must be done enterprise-wide.

The web server contains a minimal user management function, but the web server user management function does not offer enterprise-wide user management, and user management is not the primary function of the web server. User management for the hosted applications should be done through a facility that is built for enterprise-wide user management, such as LDAP and Active Directory.

**Audit:**

Interview the System Administrator (SA) about the role of the Apache web server.
If the web server is hosting an application, have the SA provide supporting documentation on how the application's user management is accomplished outside of the web server.
If the web server is not hosting an application, this is Not Applicable.
If the web server is performing user management for hosted applications, this is a finding.
If the web server is hosting an application and the SA cannot provide supporting documentation on how the application's user management is accomplished outside of the Apache web server, this is a finding.

**Remediation:**

Reconfigure any hosted applications on the Apache web server to perform user management outside the web server.
Document how the hosted application user management is accomplished.

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

## *1.13 AS24-W1-000250 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must only contain services and functions necessary for operation.

```
GROUP ID: V-214319
RULE ID: SV-214319r960963
```

**Rationale:**

A web server can provide many features, services, and processes. Some of these may be deemed unnecessary or too unsecure to run on a production DoD system.

The web server must provide the capability to disable, uninstall, or deactivate functionality and services that are deemed to be non-essential to the web server mission or can adversely impact server performance.

**Audit:**

Verify the document root directory and the configuration files do not provide for default index.html or welcome page.
Verify the Apache User Manual content is not installed by checking the configuration files for manual location directives.
Verify the Apache configuration files do not have the Server Status handler configured.
Verify that the Server Information handler is not configured.
Verify that any other handler configurations such as perl-status is not enabled.
If any of these are present, this is a finding.

**Remediation:**

Review all pre-installed content and remove content that is not required. In particular, look for the unnecessary content that may be found in the document root directory, a configuration directory such as conf/extra directory, or as a UNIX/Linux package
Remove the default index.html or welcome page if it is a separate package. If the default welcome page is part of the main Apache httpd package as it is on Red Hat Linux, comment out the configuration as shown below. Removing a file such as the "welcome.conf" is not recommended as it may be replaced if the package is updated.

## This configuration file enables the default "Welcome"

**page if there is no default index page present for**

**the root URL. To disable the Welcome page, comment**

**out all the lines below.**

##<LocationMatch "^/+$">

*Options -Indexes*

*ErrorDocument 403 /error/noindex.html*

##</LocationMatch>
Remove the Apache User Manual content or comment out configurations referencing the manual:

**yum erase httpd-manual**

Remove or comment out any Server Status handler configuration:

**Allow server status reports generated by mod_status,**

**with the URL of http://servername/server-status**

**Change the ".example.com" to match your domain to enable.**

##<Location /server-status>

*SetHandler server-status*

*Order deny,allow*

*Deny from all*

*Allow from .example.com*

##</Location>
Remove or comment out any Server Information handler configuration:

**Allow remote server configuration reports, with the URL of**

**http://servername/server-info (requires that mod_info.c be loaded).**

**Change the ".example.com" to match your domain to enable.**

##<Location /server-info>

*SetHandler server-info*

*Order deny,allow*

*Deny from all*

*Allow from .example.com*

##</Location>
Remove or comment out any other handler configuration such as perl-status:

**This will allow remote server configuration reports, with the URL of**

**http://servername/perl-status**

**Change the ".example.com" to match your domain to enable.**

##<Location /perl-status>

*SetHandler perl-script*

*PerlResponseHandler Apache2::Status*

*Order deny,allow*

*Deny from all*

*Allow from .example.com*

##</Location>
The default source build provides extra content available in the /usr/local/apache2/conf/extra/ directory, but the configuration of most of the extra content is commented out by default. In particular, the inclusion of conf/extra/proxyhtml.conf is not commented out in "httpd.conf":

## Server-pool management (MPM specific)

#Include conf/extra/httpd-mpm.conf

## Multi-language error messages

#Include conf/extra/httpd-multilang-errordoc.conf

## Fancy directory listings

#Include conf/extra/httpd-autoindex.conf

## Language settings

#Include conf/extra/httpd-languages.conf

## User home directories

#Include conf/extra/httpd-userdir.conf

## Real-time info on requests and configuration

#Include conf/extra/httpd-info.conf

## Virtual hosts

#Include conf/extra/httpd-vhosts.conf

## Local access to the Apache HTTP Server Manual

#Include conf/extra/httpd-manual.conf

## Distributed authoring and versioning (WebDAV)

#Include conf/extra/httpd-dav.conf

## Various default settings

#Include conf/extra/httpd-default.conf

## Configure mod_proxy_html to understand HTML4/XHTML1

For applications developed in-house, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software or accessible in the production environment.

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

## *1.14 AS24-W1-000260 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must not be a proxy server.

```
GROUP ID: V-214320
RULE ID: SV-214320r1051286
```

**Rationale:**

A web server should be primarily a web server or a proxy server but not both, for the same reasons that other multiuse servers are not recommended. Scanning for web servers that will also proxy requests into an otherwise protected network is a very common attack, making the attack anonymous.

**Audit:**

If the server has been approved to be a proxy server, this requirement is Not Applicable.
Open the <'INSTALL PATH'>\conf\httpd.conf file with an editor and search for the following directive:
ProxyRequests
If the ProxyRequests directive is set to "On", this is a finding.

**Remediation:**

Open the <'INSTALL PATH'>\conf\httpd.conf file with an editor and search for the following directive:
ProxyRequests
Set the directive to a value of "off".
Restart the Apache service.

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

## *1.15 AS24-W1-000270 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

The Apache web server must provide install options to exclude the installation of documentation, sample code, example applications, and tutorials.

```
GROUP ID: V-214321
RULE ID: SV-214321r960963
```

**Rationale:**

Web server documentation, sample code, example applications, and tutorials may be an exploitable threat to a web server because this type of code has not been evaluated and approved. A production web server must only contain components that are operationally necessary (e.g., compiled code, scripts, web-content, etc.).

Any documentation, sample code, example applications, and tutorials must be removed from a production web server. To ensure that the documentation and code are not installed or uninstalled completely, the web server must offer an option as part of the installation process to exclude these packages or to uninstall the packages if necessary.

Satisfies: SRG-APP-000141-WSR-000077, SRG-APP-000141-WSR-000080

**Audit:**

If the site requires the use of a particular piece of software, the Information System Security Officer (ISSO) will need to maintain documentation identifying this software as necessary for operations. The software must be operated at the vendor's current patch level and must be a supported vendor release.
If programs or utilities that meet the above criteria are installed on the web server, and appropriate documentation and signatures are in evidence, this is not a finding.
Determine whether the web server is configured with unnecessary software.
Determine whether processes other than those that support the web server are loaded and/or run on the web server.
Examples of software that should not be on the web server are all web development tools, office suites (unless the web server is a private web development server), compilers, and other utilities that are not part of the web server suite or the basic operating system.
Check the directory structure of the server and verify that additional, unintended, or unneeded applications are not loaded on the system.
If, after review of the application on the system, there is no justification for the identified software, this is a finding.

**Remediation:**

Remove any unnecessary applications.

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

## *1.16 AS24-W1-000280 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

Apache web server application directories, libraries, and configuration files must only be accessible to privileged users.

```
GROUP ID: V-214322
RULE ID: SV-214322r960963
```

**Rationale:**

When accounts used for web server features such as documentation, sample code, example applications, tutorials, utilities, and services are created even though the feature is not installed, they become an exploitable threat to a web server.

These accounts become inactive, are not monitored through regular use, and passwords for the accounts are not created or updated. An attacker, through very little effort, can use these accounts to gain access to the web server and begin investigating ways to elevate the account privileges.

The accounts used for web server features not installed must not be created and must be deleted when these features are uninstalled.

Satisfies: SRG-APP-000141-WSR-000078, SRG-APP-000211-WSR-000031, SRG-APP-000380-WSR-000072

**Audit:**

Obtain a list of the user accounts for the system, noting the privileges for each account.
Verify with the System Administrator (SA) or the Information System Security Officer (ISSO) that all privileged accounts are mission essential and documented.
Verify with the SA or the ISSO that all non-administrator access to shell scripts and operating system functions are mission essential and documented.
If undocumented privileged accounts are present, this is a finding.
If undocumented access to shell scripts or operating system functions is present, this is a finding.

**Remediation:**

Ensure non-administrators are not allowed access to the directory tree, the shell, or other operating system functions and utilities.

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

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

## *1.17 AS24-W1-000300 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must have resource mappings set to disable the serving of certain file types.

```
GROUP ID: V-214323
RULE ID: SV-214323r960963
```

**Rationale:**

Resource mapping is the process of tying a particular file type to a process in the web server that can serve that type of file to a requesting client and to identify which file types are not to be delivered to a client.

By not specifying which files can and cannot be served to a user, the web server could deliver to a user web server configuration files, log files, password files, etc.

The web server must only allow hosted application file types to be served to a user, and all other types must be disabled.

Satisfies: SRG-APP-000141-WSR-000081, SRG-APP-000141-WSR-000083

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
If "Action" or "AddHandler" exist and they configure .exe, .dll, .com, .bat, or .csh, or any other shell as a viewer for documents, this is a finding.

**Remediation:**

Disable MIME types for .exe, .dll, .com, .bat, and .csh programs.
If "Action" or "AddHandler" exist and they configure .exe, .dll, .com, .bat, or .csh, remove those references.
Restart the Apache service.

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

## *1.18 AS24-W1-000310 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must allow the mappings to unused and vulnerable scripts to be removed.

```
GROUP ID: V-214324
RULE ID: SV-214324r960963
```

**Rationale:**

Scripts allow server-side processing on behalf of the hosted application user or as processes needed in the implementation of hosted applications. Removing scripts not needed for application operation or deemed vulnerable helps to secure the web server.

To ensure scripts are not added to the web server and run maliciously, script mappings that are not needed or used by the web server for hosted application operation must be removed.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
Locate cgi-bin files and directories enabled in the "Script", "ScriptAlias" or "ScriptAliasMatch", or "ScriptInterpreterSource" directives.
If any script is not needed for application operation, this is a finding.

**Remediation:**

Remove any scripts in cgi-bin directory if they are not needed for application operation.

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

## *1.19 AS24-W1-000330 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must have Web Distributed Authoring (WebDAV) disabled.

```
GROUP ID: V-214325
RULE ID: SV-214325r960963
```

**Rationale:**

A web server can be installed with functionality that, just by its nature, is not secure. WebDAV is an extension to the HTTP protocol that, when developed, was meant to allow users to create, change, and move documents on a server, typically a web server or web share. Allowing this functionality, development, and deployment is much easier for web authors.

WebDAV is not widely used and has serious security concerns because it may allow clients to modify unauthorized files on the web server.

**Audit:**

In a command line, navigate to "<'INSTALLED PATH'>\bin". Run "httpd -M" to view a list of installed modules.
If any of the following modules are present, this is a finding:
dav_module
dav_fs_module
dav_lock_module

**Remediation:**

Edit the <'INSTALL PATH'>\conf\httpd.conf file and remove the following modules:
dav_module
dav_fs_module
dav_lock_module
Restart the Apache service.

**Additional Information:**

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

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

## *1.20 AS24-W1-000360 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must be configured to use a specified IP address and port.

```
GROUP ID: V-214326
RULE ID: SV-214326r1043177
```

**Rationale:**

The web server must be configured to listen on a specified IP address and port. Without specifying an IP address and port for the web server to use, the web server will listen on all IP addresses available to the hosting server. If the web server has multiple IP addresses, i.e., a management IP address, the web server will also accept connections on the management IP address.

Accessing the hosted application through an IP address normally used for non-application functions opens the possibility of user access to resources, utilities, files, ports, and protocols that are protected on the desired application IP address.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file and search for the following directive: Listen
For any enabled "Listen" directives, verify they specify both an IP address and port number.
If the "Listen" directive is found with only an IP address or only a port number specified, this is finding.
If the IP address is all zeros (i.e., 0.0.0.0:80 or [::ffff:0.0.0.0]:80), this is a finding.
If the "Listen" directive does not exist, this is a finding.

**Remediation:**

Edit the <'INSTALL PATH'>\conf\httpd.conf file and set the "Listen" directive to listen on a specific IP address and port.
Restart the Apache service.

**Additional Information:**

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b

- NIST SP 800-53 Revision 5::CM-7 b

## *1.21 AS24-W1-000370 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must encrypt passwords during transmission.

```
GROUP ID: V-214327
RULE ID: SV-214327r961029
```

**Rationale:**

Data used to authenticate, especially passwords, needs to be protected at all times, and encryption is the standard method for protecting authentication data during transmission. Data used to authenticate can be passed to and from the web server for many reasons.

Examples include data passed from a user to the web server through an HTTPS connection for authentication, the web server authenticating to a backend database for data retrieval and posting, and the web server authenticating to a clustered web server manager for an update.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
Ensure SSL is enabled by looking at the "SSLVerifyClient" directive.
If the value of "SSLVerifyClient" is not set to "require", this is a finding.

**Remediation:**

Edit the <'INSTALL PATH'>\conf\httpd.conf file and set the value of "SSLVerifyClient" to "require".
Restart the Apache service.

**Additional Information:**

CCI-000197 For password-based authentication, transmit passwords only over cryptographically-protected channels.

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

## *1.22 AS24-W1-000380 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must perform RFC 5280-compliant certification path validation.

```
GROUP ID: V-214328
RULE ID: SV-214328r961038
```

**Rationale:**

A certificate's certification path is the path from the end entity certificate to a trusted root certification authority (CA). Certification path validation is necessary for a relying party to make an informed decision regarding acceptance of an end entity certificate. Certification path validation includes checks such as certificate issuer trust, time validity, and revocation status for each certificate in the certification path. Revocation status information for CA and subject certificates in a certification path is commonly provided via certificate revocation lists (CRLs) or online certificate status protocol (OCSP) responses.

**Audit:**

Review the <'INSTALL PATH'>/conf/extra/httpd-ssl.conf file.
Look for the "SSLCACertificateFile" directive.
Review the path of the "SSLCACertificateFile" directive.
Review the contents of <'path of cert'>\ca-bundle.crt.
Examine the contents of this file to determine if the trusted CAs are DoD approved. If the trusted CA that is used to authenticate users to the website does not lead to an approved DoD CA, this is a finding.
NOTE: There are non-DoD roots that must be on the server for it to function. Some applications, such as antivirus programs, require root CAs to function. DoD-approved certificate can include the External Certificate Authorities (ECA), if approved by the AO. The PKE InstallRoot 3.06 System Administrator Guide (SAG), dated 08 Jul 2008, contains a complete list of DoD, ECA, and IECA CAs.

**Remediation:**

Configure the web server's trust store to trust only DoD-approved PKIs (e.g., DoD PKI, DoD ECA, and DoD-approved external partners).
Restart the Apache service.

**Additional Information:**

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

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

## *1.23 AS24-W1-000430 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Apache web server accounts accessing the directory tree, the shell, or other operating system functions and utilities must only be administrative accounts.

```
GROUP ID: V-214329
RULE ID: SV-214329r961095
```

**Rationale:**

As a rule, accounts on a web server are to be kept to a minimum. Only administrators, web managers, developers, auditors, and web authors require accounts on the machine hosting the web server. The resources to which these accounts have access must also be closely monitored and controlled. Only the system administrator needs access to all the system's capabilities, while the web administrator and associated staff require access and control of the web content and web server configuration files.

**Audit:**

Review the web server documentation and configuration to determine what web server accounts are available on the hosting server.
Review permissions in the web and Apache directories.
If the files are owned by anyone other than the Apache user set up to run Apache, this is a finding.
If non-privileged web server accounts are available with access to functions, directories, or files not needed for the role of the account, this is a finding.

**Remediation:**

Limit the functions, directories, and files that are accessible by each account and role to administrative accounts and remove or modify non-privileged account access.

**Additional Information:**

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

## *1.24 AS24-W1-000450 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must separate the hosted applications from hosted Apache web server management functionality.

```
GROUP ID: V-214330
RULE ID: SV-214330r961095
```

**Rationale:**

The separation of user functionality from web server management can be accomplished by moving management functions to a separate IP address or port. To further separate the management functions, separate authentication methods and certificates should be used.

By moving the management functionality, the possibility of accidental discovery of the management functions by non-privileged users during hosted application use is minimized.

**Audit:**

Review the web server documentation and deployed configuration to determine whether hosted application functionality is separated from web server management functions. If the functions are not separated, this is a finding.

**Remediation:**

Configure Apache to separate the hosted applications from web server management functionality.

**Additional Information:**

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

## *1.25 AS24-W1-000460 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must invalidate session identifiers upon hosted application user logout or other session termination.

```
GROUP ID: V-214331
RULE ID: SV-214331r1043179
```

**Rationale:**

Captured sessions can be reused in "replay" attacks. This requirement limits the ability of adversaries from capturing and continuing to employ previously valid session IDs.

Session IDs are tokens generated by web applications to uniquely identify an application user's session. Unique session IDs help to reduce predictability of said identifiers. When a user logs out, or when any other session termination event occurs, the web server must terminate the user session to minimize the potential for an attacker to hijack that particular user session.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
Search for the following directive:
SessionMaxAge
Verify the value of "SessionMaxAge" is set to "600" or less.
If "SessionMaxAge" does not exist or is set to more than "600", this is a finding.

**Remediation:**

Open the <'INSTALL PATH'>\conf\httpd.conf file.
Set the "SessionMaxAge" directive to a value of no more than "600".
Add the directive if it does not exist.
Restart the Apache service.

**Additional Information:**

CCI-001185 Invalidate session identifiers upon user logout or other session termination.

- NIST SP 800-53::SC-23 (1)
- NIST SP 800-53A::SC-23 (1).1
- NIST SP 800-53 Revision 4::SC-23 (1)
- NIST SP 800-53 Revision 5::SC-23 (1)

## *1.26 AS24-W1-000470 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Cookies exchanged between the Apache web server and client, such as session cookies, must have security settings that disallow cookie access outside the originating Apache web server and hosted application.

```
GROUP ID: V-214332
RULE ID: SV-214332r1043180
```

**Rationale:**

Cookies are used to exchange data between the web server and the client. Cookies, such as a session cookie, may contain session information and user credentials used to maintain a persistent connection between the user and the hosted application since HTTP/HTTPS is a stateless protocol.

When the cookie parameters are not set properly (i.e., domain and path parameters), cookies can be shared within hosted applications residing on the same web server or to applications hosted on different web servers residing on the same domain.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
If "HttpOnly;secure" is not configured, this is a finding.
Review the code. If when creating cookies, the following is not occurring, this is a finding:
function setCookie() { document.cookie = "ALEPH_SESSION_ID = $SESS; path = /; secure"; }

**Remediation:**

Add this line to "httpd.conf" file:
Header always edit Set-Cookie ^(.*)$ $1;HttpOnly;secure
Add the secure attribute to the JavaScript set cookie:
function setCookie() { document.cookie = "ALEPH_SESSION_ID = $SESS; path = /; secure"; }
HttpOnly cannot be used since by definition this is a cookie set by JavaScript.
Restart the Apache service.

**Additional Information:**

CCI-001664 Recognize only session identifiers that are system-generated.

- NIST SP 800-53::SC-23 (3)

- NIST SP 800-53A::SC-23 (3).1 (ii)
- NIST SP 800-53 Revision 4::SC-23 (3)
- NIST SP 800-53 Revision 5::SC-23 (3)

## *1.27 AS24-W1-000480 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must accept only system-generated session identifiers.

```
GROUP ID: V-214333
RULE ID: SV-214333r1043180
```

**Rationale:**

Communication between a client and the web server is done using the HTTP protocol, but HTTP is a stateless protocol. To maintain a connection or session, a web server will generate a session identifier (ID) for each client session when the session is initiated. The session ID allows the web server to track a user session and, in many cases, the user, if the user previously logged on to a hosted application.

When a web server accepts session identifiers that are not generated by the web server, the web server creates an environment where session hijacking, such as session fixation, could be used to access hosted applications through session IDs that have already been authenticated. Forcing the web server to only accept web server-generated session IDs and to create new session IDs once a user is authenticated will limit session hijacking.

Satisfies: SRG-APP-000223-WSR-000145, SRG-APP-000224-WSR-000135, SRG-APP-000224-WSR-000137, SRG-APP-000224-WSR-000138

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
Verify the "mod_unique_id" is loaded.
If it does not exist, this is a finding.

**Remediation:**

Edit the <'INSTALL PATH'>\conf\httpd.conf file and load the "mod_unique_id" module.
Restart the Apache service.

**Additional Information:**

CCI-001188 Generate a unique session identifier for each session with organization-defined randomness requirements.

- NIST SP 800-53::SC-23 (4)
- NIST SP 800-53A::SC-23 (4).1 (ii)
- NIST SP 800-53 Revision 4::SC-23 (3)
- NIST SP 800-53 Revision 5::SC-23 (3)

CCI-001664 Recognize only session identifiers that are system-generated.

- NIST SP 800-53::SC-23 (3)
- NIST SP 800-53A::SC-23 (3).1 (ii)
- NIST SP 800-53 Revision 4::SC-23 (3)
- NIST SP 800-53 Revision 5::SC-23 (3)

## *1.28 AS24-W1-000500 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must generate unique session identifiers that cannot be reliably reproduced.

```
GROUP ID: V-214334
RULE ID: SV-214334r1043181
```

**Rationale:**

Communication between a client and the Apache web server is done using the HTTP protocol, but HTTP is a stateless protocol. To maintain a connection or session, a web server will generate a session identifier (ID) for each client session when the session is initiated. The session ID allows the Apache web server to track a user session and, in many cases, the user, if the user previously logged on to a hosted application.

Unique session IDs are the opposite of sequentially generated session IDs, which can be easily guessed by an attacker. Unique session identifiers help to reduce predictability of generated identifiers. Unique session IDs address man-in-the-middle attacks, including session hijacking or insertion of false information into a session. If the attacker is unable to identify or guess the session information related to pending application traffic, the attacker will have more difficulty in hijacking the session or otherwise manipulating valid sessions.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
Check to see if the "mod_unique_id" is loaded.
If it does not exist, this is a finding.

**Remediation:**

Edit the <'INSTALL PATH'>\conf\httpd.conf file and load the "mod_unique_id" module.
Restart the Apache service.

**Additional Information:**

CCI-001188 Generate a unique session identifier for each session with organization-defined randomness requirements.

- NIST SP 800-53::SC-23 (4)
- NIST SP 800-53A::SC-23 (4).1 (ii)
- NIST SP 800-53 Revision 4::SC-23 (3)
- NIST SP 800-53 Revision 5::SC-23 (3)

## *1.29 AS24-W1-000530 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must generate unique session identifiers with definable entropy.

```
GROUP ID: V-214335
RULE ID: SV-214335r1043181
```

**Rationale:**

Generating a session identifier (ID) that is not easily guessed through brute force is essential to deter several types of session attacks. By knowing the session ID, an attacker can hijack a user session that has already been user authenticated by the hosted application. The attacker does not need to guess user identifiers and passwords or have a secure token since the user session has already been authenticated.

Random and unique session IDs are the opposite of sequentially generated session IDs, which can be easily guessed by an attacker. Random session identifiers help to reduce predictability of said identifiers. The session ID must be unpredictable (random enough) to prevent guessing attacks, where an attacker is able to guess or predict the ID of a valid session through statistical analysis techniques. For this purpose, a good Pseudo Random Number Generator (PRNG) must be used.

Unique session IDs address man-in-the-middle attacks, including session hijacking or insertion of false information into a session. If the attacker is unable to identify or guess the session information related to pending application traffic, they will have more difficulty in hijacking the session or otherwise manipulating valid sessions.

At least half of a session ID must be created using a definable source of entropy (PRNG).

**Audit:**

Review the <'INSTALLED PATH'>\conf\httpd.conf file.
Verify the "ssl_module" is loaded.
If it does not exist, this is a finding.
If the "SSLRandomSeed" directive is missing or does not look like the following, this is a finding:
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin

**Remediation:**

Edit the <'INSTALLED PATH'>\conf\httpd.conf file and load the "ssl_module" module.
Set the "SSLRandomSeed" directives to the following:
SSLRandomSeed startup builtin
SSLRandomSeed connect builtin
Restart the Apache service.

**Additional Information:**

CCI-001188 Generate a unique session identifier for each session with organization-defined randomness requirements.

- NIST SP 800-53::SC-23 (4)
- NIST SP 800-53A::SC-23 (4).1 (ii)
- NIST SP 800-53 Revision 4::SC-23 (3)
- NIST SP 800-53 Revision 5::SC-23 (3)

## *1.30 AS24-W1-000550 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must be built to fail to a known safe state if system initialization fails, shutdown fails, or aborts fail.

```
GROUP ID: V-214336
RULE ID: SV-214336r961122
```

**Rationale:**

Determining a safe state for failure and weighing that against a potential DoS for users depends on what type of application the web server is hosting. For an application presenting publicly available information that is not critical, a safe state for failure might be to shut down for any type of failure, but for an application that presents critical and timely information, a shutdown might not be the best state for all failures.

Performing a proper risk analysis of the hosted applications and configuring the web server according to what actions to take for each failure condition will provide a known fail safe state for the web server.

Satisfies: SRG-APP-000225-WSR-000140, SRG-APP-000225-WSR-000074

**Audit:**

Interview the System Administrator for the Apache 2.4 web server.
Ask for documentation on the disaster recovery methods tested and planned for the Apache 2.4 web server in the event of the necessity for rollback.
If documentation for a disaster recovery has not been established, this is a finding.

**Remediation:**

Prepare documentation for disaster recovery methods for the Apache 2.4 web server in the event of the necessity for rollback.
Document and test the disaster recovery methods designed.

**Additional Information:**

CCI-001190 Fail to an organization-defined known-system state for the list of organization-defined types of system failures on organization-defined system components on the indicated components while preserving organization-defined system state information in failure.

- NIST SP 800-53::SC-24
- NIST SP 800-53A::SC-24.1 (iv)
- NIST SP 800-53 Revision 4::SC-24

- NIST SP 800-53 Revision 5::SC-24

## *1.31 AS24-W1-000580 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server document directory must be in a separate partition from the Apache web servers system files.

```
GROUP ID: V-214337
RULE ID: SV-214337r961131
```

**Rationale:**

A web server is used to deliver content on the request of a client. The content delivered to a client must be controlled, allowing only hosted application files to be accessed and delivered. To allow a client access to system files of any type is a major security risk that is entirely avoidable. Obtaining such access is the goal of directory traversal and URL manipulation vulnerabilities. To facilitate such access by misconfiguring the web document (home) directory is a serious error. In addition, having the path on the same drive as the system folder compounds potential attacks such as drive space exhaustion.

**Audit:**

Determine whether the public web server has a two-way trusted relationship with any private asset located within the network. Private web server resources (e.g., drives, folders, printers, etc.) will not be directly mapped to or shared with public web servers.
If sharing is selected for any web folder, this is a finding.
If private resources (e.g., drives, partitions, folders/directories, printers, etc.) are shared with the public web server, this is a finding.

**Remediation:**

Configure the public web server to not have a trusted relationship with any system resource that is also not accessible to the public. Web content is not to be shared via Microsoft shares or NFS mounts.

**Additional Information:**

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53::SC-3
- NIST SP 800-53A::SC-3.1 (ii)
- NIST SP 800-53 Revision 4::SC-3
- NIST SP 800-53 Revision 5::SC-3

## *1.32 AS24-W1-000590 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must restrict the ability of users to launch denial-of-service (DoS) attacks against other information systems or networks.

```
GROUP ID: V-214338
RULE ID: SV-214338r961152
```

**Rationale:**

Apache web server can limit the ability of the web server being used in a DoS attack through several methods. The methods employed will depend upon the hosted applications and their resource needs for proper operation.

An example setting that could be used to limit the ability of the web server being used in a DoS attack is bandwidth throttling.

**Audit:**

Review the <'INSTALLED PATH'>\conf\httpd.conf file.
Verify the "Timeout" directive is specified in the "httpd.conf" file to have a value of "10" seconds or less.
If the "Timeout" directive is not configured or set for more than "10" seconds, this is a finding.

**Remediation:**

Review the <'INSTALLED PATH'>\conf\httpd.conf file.
Add or modify the "Timeout" directive in the Apache configuration to have a value of "10" seconds or less.

```
"Timeout 10"
```

Restart the Apache service.

**Additional Information:**

CCI-001094 Restrict the ability of individuals to launch organization-defined denial of service attacks against other systems.

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

## *1.33 AS24-W1-000620 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Warning and error messages displayed to clients must be modified to minimize the identity of the Apache web server, patches, loaded modules, and directory paths.

```
GROUP ID: V-214339
RULE ID: SV-214339r961167
```

**Rationale:**

Information needed by an attacker to begin looking for possible vulnerabilities in a web server includes any information about the web server, backend systems being accessed, and plug-ins or modules being used.

Web servers will often display error messages to client users, displaying enough information to aid in the debugging of the error. The information given back in error messages may display the web server type, version, patches installed, plug-ins and modules installed, type of code being used by the hosted application, and any backends being used for data storage.

This information could be used by an attacker to blueprint what type of attacks might be successful. The information given to users must be minimized to not aid in the blueprinting of the Apache web server.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
If the "ErrorDocument" directive is not being used, this is a finding.

**Remediation:**

Edit the <'INSTALL PATH'>\conf\httpd.conf file and use the "ErrorDocument" directive to enable custom error pages.
ErrorDocument 500 "Sorry, our script crashed. Oh dear"
ErrorDocument 500 /cgi-bin/crash-recover
ErrorDocument 500 http://error.example.com/server_error.html
ErrorDocument 404 /errors/not_found.html
ErrorDocument 401 /subscription/how_to_subscribe.html
The syntax of the ErrorDocument directive is:
ErrorDocument <3-digit-code>
Restart the Apache service.
Additional Information:
https://httpd.apache.org/docs/2.4/custom-error.html

**Additional Information:**

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a
- NIST SP 800-53 Revision 5::SI-11 a

## *1.34 AS24-W1-000630 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Debugging and trace information used to diagnose the Apache web server must be disabled.

```
GROUP ID: V-214340
RULE ID: SV-214340r961167
```

**Rationale:**

Information needed by an attacker to begin looking for possible vulnerabilities in a web server includes any information about the web server and plug-ins or modules being used. When debugging or trace information is enabled in a production web server, information about the web server, such as web server type, version, patches installed, plug-ins and modules installed, type of code being used by the hosted application, and any backends being used for data storage may be displayed. Since this information may be placed in logs and general messages during normal operation of the web server, an attacker does not need to cause an error condition to gain this information.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
For any enabled "TraceEnable" directives, verify they are part of the server=level configuration (i.e., not nested in a "Directory" or "Location" directive).
Also verify the "TraceEnable" directive is set to "Off".
If the "TraceEnable directive is not part of the server-level configuration and/or is not set to "Off", this is a finding.
If the directive does not exist in the conf file, this is a finding because the default value is "On".

**Remediation:**

Edit the <'INSTALL PATH'>\conf\httpd.conf file and add or set the value of "TraceEnable" to "Off".
Restart the Apache service.

**Additional Information:**

CCI-001312 Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited.

- NIST SP 800-53::SI-11 b
- NIST SP 800-53A::SI-11.1 (iii)
- NIST SP 800-53 Revision 4::SI-11 a

- NIST SP 800-53 Revision 5::SI-11 a

## *1.35 AS24-W1-000640 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must set an absolute timeout for sessions.

```
GROUP ID: V-214341
RULE ID: SV-214341r1043182
```

**Rationale:**

Leaving sessions open indefinitely is a major security risk. An attacker can easily use an already authenticated session to access the hosted application as the previously authenticated user. By closing sessions after an absolute period of time, the user is forced to reauthenticate, guaranteeing the session is still in use. Enabling an absolute timeout for sessions closes sessions that are still active. Examples would be a runaway process accessing the Apache web server or an attacker using a hijacked session to slowly probe the Apache web server.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
Search for the following directive:
SessionMaxAge
Verify the value of "SessionMaxAge" is set to "600" or less.
If the "SessionMaxAge" does not exist or is set to more than "600", this is a finding.

**Remediation:**

Open the <'INSTALL PATH'>\conf\httpd.conf file.
Set the "SessionMaxAge" directive to a value of "600" or less; add the directive if it does not exist.
Restart the Apache service.

**Additional Information:**

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

## *1.36 AS24-W1-000650 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must set an inactive timeout for completing the TLS handshake

```
GROUP ID: V-214342
RULE ID: SV-214342r1043182
```

**Rationale:**

Leaving sessions open indefinitely is a major security risk. An attacker can easily use an already authenticated session to access the hosted application as the previously authenticated user.

Timeouts for completing the TLS handshake, receiving the request headers and/or the request body from the client. If the client fails to complete each of these stages within the configured time, a 408 REQUEST TIME OUT error is sent.

For SSL virtual hosts, the handshake timeout values is the time needed to do the initial SSL handshake. If the user's browser is configured to query certificate revocation lists and the CRL server is not reachable, the initial SSL handshake may take a significant time until the browser gives up waiting for the CRL. Therefore the handshake timeout should take this possible overhead into consideration for SSL virtual hosts (if necessary). The body timeout values include the time needed for SSL renegotiation (if necessary).

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
Verify the "mod_reqtimeout" is loaded.
If it does not exist, this is a finding.
If the "mod_reqtimeout" module is loaded and the "RequestReadTimeout" directive is not configured, this is a finding.
Note: The "RequestReadTimeout" directive must be explicitly configured (i.e., not left to a default value) to a value compatible with the organization's operations.

**Remediation:**

Edit the <'INSTALL PATH'>\conf\httpd.conf file and load the "mod_reqtimeout" module.
Set the "RequestReadTimeout" directive to a value compatible with the organization's operations.
Restart the Apache service.

**Additional Information:**

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

## *1.37 AS24-W1-000670 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must restrict inbound connections from nonsecure zones.

```
GROUP ID: V-214343
RULE ID: SV-214343r961278
```

**Rationale:**

Remote access to the Apache web server is any access that communicates through an external, non-organization-controlled network. Remote access can be used to access hosted applications or to perform management functions.

A web server can be accessed remotely and must be capable of restricting access from what the DoD defines as nonsecure zones. Nonsecure zones are defined as any IP, subnet, or region that is defined as a threat to the organization. The nonsecure zones must be defined for public web servers logically located in a DMZ, as well as private web servers with perimeter protection devices. By restricting access from nonsecure zones, through the internal Apache web server access list, the Apache web server can stop or slow denial-of-service (DoS) attacks on the Apache web server.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
If "IP Address Restrictions" are not configured or IP ranges configured to be "Allow" are not restrictive enough to prevent connections from nonsecure zones, this is a finding.

**Remediation:**

Configure the "http.conf" file to include restrictions.
Example:

Restart the Apache service.

**Additional Information:**

CCI-002314 Employ automated mechanisms to control remote access methods.

- NIST SP 800-53 Revision 4::AC-17 (1)
- NIST SP 800-53 Revision 5::AC-17 (1)

## *1.38 AS24-W1-000680 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must be configured to immediately disconnect or disable remote access to the hosted applications.

```
GROUP ID: V-214344
RULE ID: SV-214344r961281
```

**Rationale:**

During an attack on the Apache web server or any of the hosted applications, the system administrator may need to disconnect or disable access by users to stop the attack.

The Apache web server must be configured to disconnect users to a hosted application without compromising other hosted applications unless deemed necessary to stop the attack. Methods to disconnect or disable connections are to stop the application service for a specified hosted application, stop the Apache web server, or block all connections through the Apache web server access list.

The Apache web server capabilities used to disconnect or disable users from connecting to hosted applications and the Apache web server must be documented to make certain that, during an attack, the proper action is taken to conserve connectivity to any other hosted application if possible and to make certain log data is conserved for later forensic analysis.

**Audit:**

Interview the System Administrator and Web Manager.
Ask for documentation for the Apache web server administration.
Verify there are documented procedures for shutting down an Apache website in the event of an attack. The procedure should, at a minimum, provide the following steps:
Determine the respective website for the application at risk of an attack.
Stop the Apache service.
If the web server is not capable of or cannot be configured to disconnect or disable remote access to the hosted applications when necessary, this is a finding.

**Remediation:**

Prepare documented procedures for shutting down an Apache website in the event of an attack.
The procedure should, at a minimum, provide the following step:
Stop the Apache service.

**Additional Information:**

CCI-002322 Provide the capability to disconnect or disable remote access to the system within the organization-defined time period.

- NIST SP 800-53 Revision 4::AC-17 (9)
- NIST SP 800-53 Revision 5::AC-17 (9)

## *1.39 AS24-W1-000690 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

Non-privileged accounts on the hosting system must only access Apache web server security-relevant information and functions through a distinct administrative account.

```
GROUP ID: V-214345
RULE ID: SV-214345r961353
```

**Rationale:**

By separating Apache web server security functions from non-privileged users, roles can be developed that can then be used to administer the Apache web server. Forcing users to change from a non-privileged account to a privileged account when operating on the Apache web server or on security-relevant information forces users to only operate as a Web Server Administrator when necessary. Operating in this manner allows for better logging of changes and better forensic information and limits accidental changes to the Apache web server.

**Audit:**

Determine which tool or control file is used to control the configuration of the web server.
If the control of the web server is done via control files, verify who has update access to them. If tools are being used to configure the web server, determine who has access to execute the tools.
If accounts other than the System Administrator (SA), the Web Manager, or the Web Manager designees have access to the web administration tool or control files, this is a finding.

**Remediation:**

Restrict access to the web administration tool to only the System Administrator, Web Manager, or the Web Manager designees.

**Additional Information:**

CCI-002235 Prevent non-privileged users from executing privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (10)
- NIST SP 800-53 Revision 5::AC-6 (10)

## *1.40 AS24-W1-000700 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

An Apache web server that is part of a web server cluster must route all remote management through a centrally managed access control point.

```
GROUP ID: V-214346
RULE ID: SV-214346r985884
```

**Rationale:**

A web server cluster is a group of independent Apache web servers that are managed as a single system for higher availability, easier manageability, and greater scalability. Without having centralized control of the web server cluster, management of the cluster becomes difficult. It is critical that remote management of the cluster be done through a designated management system acting as a single access point.

**Audit:**

Review the <'INSTALL PATH'>\conf\httpd.conf file.
Verify the "mod_proxy" is loaded.
If it does not exist, this is a finding.
If the "mod_proxy" module is loaded and the "ProxyPass" directive is not configured, this is a finding.

**Remediation:**

Edit the <'INSTALL PATH'>\conf\httpd.conf file and load the "mod_proxy" module.
Set the "ProxyPass" directive.
Restart the Apache service.

**Additional Information:**

CCI-000154 Provide the capability to centrally review and analyze audit records from multiple components within the system.

- NIST SP 800-53::AU-6 (4)
- NIST SP 800-53A::AU-6 (4).1
- NIST SP 800-53 Revision 4::AU-6 (4)
- NIST SP 800-53 Revision 5::AU-6 (4)

## *1.41 AS24-W1-000710 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must use a logging mechanism that is configured to allocate log record storage capacity large enough to accommodate the logging requirements of the Apache web server.

```
GROUP ID: V-214347
RULE ID: SV-214347r961392
```

**Rationale:**

To make certain that the logging mechanism used by the web server has sufficient storage capacity in which to write the logs, the logging mechanism needs to be able to allocate log record storage capacity.

The task of allocating log record storage capacity is usually performed during initial installation of the logging mechanism. The System Administrator will usually coordinate the allocation of physical drive space with the web server administrator along with the physical location of the partition and disk. Refer to NIST SP 800-92 for specific requirements on log rotation and storage dependent on the impact of the web server.

**Audit:**

Work with SIEM administrator to determine log storage capacity.
If there is no setting within a SIEM to accommodate enough a large logging capacity, this is a finding.

**Remediation:**

Work with the SIEM administrator to determine if the SIEM is configured to allocate log record storage capacity large enough to accommodate the logging requirements of the Apache web server.

**Additional Information:**

CCI-001849 Allocate audit log storage capacity to accommodate organization-defined audit log retention requirements.

- NIST SP 800-53 Revision 4::AU-4
- NIST SP 800-53 Revision 5::AU-4

## *1.42 AS24-W1-000720 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must not impede the ability to write specified log record content to an audit log server.

```
GROUP ID: V-214348
RULE ID: SV-214348r961395
```

**Rationale:**

Writing events to a centralized management audit system offers many benefits to the enterprise over having dispersed logs. Centralized management of audit records and logs provides for efficiency in maintenance and management of records, enterprise analysis of events, and backup and archiving of event records enterprise-wide. The web server and related components are required to be capable of writing logs to centralized audit log servers.

**Audit:**

Work with the SIEM administrator to determine current security integrations.
If the SIEM is not integrated with security, this is a finding.

**Remediation:**

Work with the SIEM administrator to integrate with an organizations security infrastructure.

**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)

## *1.43 AS24-W1-000730 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must be configurable to integrate with an organizations security infrastructure.

```
GROUP ID: V-214349
RULE ID: SV-214349r961395
```

**Rationale:**

A web server will typically use logging mechanisms for maintaining a historical log of activity that occurs within a hosted application. This information can then be used for diagnostic purposes, forensics purposes, or other purposes relevant to ensuring the availability and integrity of the hosted application.

While it is important to log events identified as being critical and relevant to security, it is equally important to notify the appropriate personnel in a timely manner so they are able to respond to events as they occur.

Manual review of the web server logs may not occur in a timely manner, and each event logged is open to interpretation by a reviewer. By integrating the web server into an overall or organization-wide log review, a larger picture of events can be viewed, and analysis can be done in a timely and reliable manner.

**Audit:**

Work with the SIEM administrator to determine current security integrations.
If the SIEM is not integrated with security, this is a finding.

**Remediation:**

Work with the SIEM administrator to integrate with an organizations security infrastructure.

**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)

## *1.44 AS24-W1-000740 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must use a logging mechanism that is configured to provide a warning to the Information System Security Officer (ISSO) and System Administrator (SA) when allocated record storage volume reaches 75 percent of maximum log record storage capacity.

```
GROUP ID: V-214350
RULE ID: SV-214350r961398
```

**Rationale:**

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process logs as required. Log processing failures include software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded.

If log capacity were to be exceeded, then events subsequently occurring would not be recorded. Organizations must define a maximum allowable percentage of storage capacity serving as an alarming threshold (e.g., web server has exceeded 75 percent of log storage capacity allocated), at which time the Apache web server or the logging mechanism the web server uses will provide a warning to the ISSO and SA at a minimum.

This requirement can be met by configuring the Apache web server to use a dedicated log tool that meets this requirement.

**Audit:**

Work with the SIEM administrator to determine if an alert is configured when audit data is no longer received as expected.
If there is no alert configured, this is a finding.

**Remediation:**

Work with the SIEM administrator to configure an alert when no audit data is received from Apache based on the defined schedule of connections.

**Additional Information:**

CCI-001855 Provide a warning to organization-defined personnel, roles, and/or locations within an organization-defined time period when allocated audit log storage volume reaches an organization-defined percentage of repository maximum audit log storage capacity.

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

## *1.45 AS24-W1-000760 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must generate log records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) with a minimum granularity of one second.

```
GROUP ID: V-214351
RULE ID: SV-214351r961446
```

**Rationale:**

If time stamps are not consistently applied and there is no common time reference, it is difficult to perform forensic analysis across multiple devices and log records.

Time stamps generated by the Apache web server include date and time. Time is commonly expressed in UTC, a modern continuation of GMT, or local time with an offset from UTC.

Without sufficient granularity of time stamps, it is not possible to adequately determine the chronological order of records.

Time stamps generated by the Apache web server include date and time and must be to a granularity of one second.

Satisfies: SRG-APP-000375-WSR-000171, SRG-APP-000374-WSR-000172

**Audit:**

Review the web server documentation and configuration to determine the time stamp format for log data.
In a command line, navigate to "<'INSTALLED PATH'>\bin". Run "httpd -M" to view a list of installed modules.
If "log_config_module" is not listed, this is a finding.
In a command line, navigate to "<'INSTALLED PATH'>\bin". Determine the location of the "httpd.conf" file by running the following command:
httpd -V
Review the "HTTPD_ROOT" path.
Navigate to the "HTTPD_ROOT"/conf directory.
Edit the "httpd.conf" file.
Verify the "LogFormat" directive exists.
If it does not exist, this is a finding.
Verify the "LogFormat" line contains the "%t" flag.
If "%t" flag is not present, time is not mapped to UTC or GMT time, and this is a finding.

**Remediation:**

In a command line, navigate to "<'INSTALLED PATH'>\bin". Run "httpd -M" to view a list of installed modules.
If "log_config_module" is not listed, enable this module.
In a command line, navigate to "<'INSTALLED PATH'>\bin". Determine the location of the "httpd.conf" file by running the following command:
httpd -V
Review the "HTTPD_ROOT" path.
Navigate to the "HTTPD_ROOT"/conf directory.
Edit the "httpd.conf" file.
Determine if the "LogFormat" directive exists. If it does not exist, ensure the "LogFormat" line contains the "%t" flag.

**Additional Information:**

CCI-001890 Record time stamps for audit records that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

- NIST SP 800-53 Revision 4::AU-8 b
- NIST SP 800-53 Revision 5::AU-8 b

## *1.46 AS24-W1-000800 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must only accept client certificates issued by DoD PKI or DoD-approved PKI Certification Authorities (CAs).

```
GROUP ID: V-214352
RULE ID: SV-214352r965407
```

**Rationale:**

Non-DoD-approved PKIs have not been evaluated to ensure they have security controls and identity vetting procedures in place that are sufficient for DoD systems to rely on the identity asserted in the certificate. PKIs lacking sufficient security controls and identity vetting procedures risk being compromised and issuing certificates that enable adversaries to impersonate legitimate users.

**Audit:**

Review the "ssl.conf" file.
Look for the "SSLCACertificateFile" directive.
Review the path of the "SSLCACertificateFile" directive.
Review the contents of <'path of cert'>\ca-bundle.crt.
Examine the contents of this file to determine if the trusted CAs are DoD approved.
If the trusted CA that is used to authenticate users to the website does not lead to an approved DoD CA, this is a finding.
NOTE: There are non-DoD roots that must be on the server for it to function. Some applications, such as antivirus programs, require root CAs to function. DoD-approved certificate can include the External Certificate Authorities (ECA), if approved by the AO. The PKE InstallRoot 3.06 System Administrator Guide (SAG), dated 08 Jul 2008, contains a complete list of DoD, ECA, and IECA CAs.

**Remediation:**

Configure the web server's trust store to trust only DoD-approved PKIs (e.g., DoD PKI, DoD ECA, and DoD-approved external partners).

**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)

## *1.47 AS24-W1-000820 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must be protected from being stopped by a non-privileged user.

```
GROUP ID: V-214353
RULE ID: SV-214353r961620
```

**Rationale:**

An attacker has at least two reasons to stop a web server. The first is to cause a denial of service (DoS), and the second is to put in place changes the attacker made to the web server configuration.

To prohibit an attacker from stopping the Apache web server, the process ID (pid) of the web server and the utilities used to start/stop it must be protected from access by non-privileged users. By knowing the "pid" and having access to the Apache web server utilities, a non-privileged user has a greater capability of stopping the server, whether intentionally or unintentionally.

**Audit:**

Right-click <'Install Path'>\bin\httpd.exe.
Click "Properties" from the "Context" menu.
Select the "Security" tab.
Review the groups and user names.
The following account may have Full control privileges:
TrustedInstaller
Web Managers
Web Manager designees
The following accounts may have read and execute, or read permissions:
Non Web Manager Administrators
ALL APPLICATION PACKAGES (built-in security group)
SYSTEM
Users
Specific users may be granted read and execute and read permissions.
Compare the local documentation authorizing specific users against the users observed when reviewing the groups and users.
If any other access is observed, this is a finding.

**Remediation:**

Restrict access to the web administration tool to only the Web Manager and the Web Manager's designees.

**Additional Information:**

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

## *1.48 AS24-W1-000830 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must be tuned to handle the operational requirements of the hosted application.

```
GROUP ID: V-214354
RULE ID: SV-214354r1067792
```

**Rationale:**

A denial of service (DoS) can occur when the Apache web server is so overwhelmed that it can no longer respond to additional requests. A web server not properly tuned may become overwhelmed and cause a DoS condition even with expected traffic from users. To avoid a DoS, the Apache web server must be tuned to handle the expected traffic for the hosted applications.

**Audit:**

Verify the "Timeout" directive is specified in the Apache configuration files to have a value of "60" seconds or less.
If the "Timeout" directive is not configured or set for more than "60" seconds, this is a finding.

**Remediation:**

Add or modify the "Timeout" directive in the Apache configuration to have a value of "60" seconds or less.

```
"Timeout 60"
```

Restart the Apache service.

**Additional Information:**

CCI-002385 Protect against or limit the effects of organization-defined types of denial-of-service events.

- NIST SP 800-53 Revision 4::SC-5
- NIST SP 800-53 Revision 5::SC-5 a

## *1.49 AS24-W1-000860 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server cookies, such as session cookies, sent to the client using SSL/TLS must not be compressed.

```
GROUP ID: V-214355
RULE ID: SV-214355r961632
```

**Rationale:**

A cookie is used when a web server needs to share data with the client's browser. The data is often used to remember the client when the client returns to the hosted application at a later date. A session cookie is a special type of cookie used to remember the client during the session. The cookie will contain the session identifier (ID) and may contain authentication data to the hosted application. To protect this data from easily being compromised, the cookie can be encrypted.

When a cookie is sent encrypted via SSL/TLS, an attacker must spend a great deal of time and resources to decrypt the cookie. If, along with encryption, the cookie is compressed, the attacker can now use a combination of plaintext injection and inadvertent information leakage through data compression to reduce the time needed to decrypt the cookie. This attack is called Compression Ratio Info-leak Made Easy (CRIME).

Cookies shared between the Apache web server and the client when encrypted should not also be compressed.

**Audit:**

Search the Apache configuration files for the "SSLCompression" directive.
If the "SSLCompression" directive does not exist, this is a not a finding.
If the "SSLCompression" directive exists and is not set to "Off", this is a finding.

**Remediation:**

Perform the following to implement the recommended state:
Search the Apache configuration files for the "SSLCompression" directive. If the directive is present, set it to "Off".
Restart the Apache service.

**Additional Information:**

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8

- NIST SP 800-53 Revision 5::SC-8

## *1.50 AS24-W1-000930 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must install security-relevant software updates within the configured time period directed by an authoritative source (e.g., IAVM, CTOs, DTMs, and STIGs).

```
GROUP ID: V-214356
RULE ID: SV-214356r961683
```

**Rationale:**

Security flaws with software applications are discovered daily. Vendors are constantly updating and patching their products to address newly discovered security vulnerabilities. Organizations (including any contractor to the organization) are required to promptly install security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling must also be addressed expeditiously.

The Apache web server will be configured to check for and install security-relevant software updates from an authoritative source within an identified time period from the availability of the update. By default, this time period will be every 24 hours.

**Audit:**

Determine the most recent patch level of the Apache web server 2.4 software, as posted on the Apache HTTP Server Project website.
In a command line, type "httpd -v".
If the version is more than one version behind the most recent patch level, this is a finding.

**Remediation:**

Install the current version of the web server software and maintain appropriate service packs and patches.

**Additional Information:**

CCI-002605 Install security-relevant software updates within an organization-defined time period of the release of the updates.

- NIST SP 800-53 Revision 4::SI-2 c
- NIST SP 800-53 Revision 5::SI-2 c

## *1.51 AS24-W1-000940 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

All accounts installed with the Apache web server software and tools must have passwords assigned and default passwords changed.

```
GROUP ID: V-214357
RULE ID: SV-214357r961863
```

**Rationale:**

During installation of the Apache web server software, accounts are created for the Apache web server to operate properly. The accounts installed can have either no password installed or a default password, which will be known and documented by the vendor and the user community.

The first things an attacker will try when presented with a logon screen are the default user identifiers with default passwords. Installed applications may also install accounts with no password, making the logon even easier. Once the Apache web server is installed, the passwords for any created accounts should be changed and documented. The new passwords must meet the requirements for all passwords, i.e., upper/lower characters, numbers, special characters, time until change, reuse policy, etc.

Service accounts or system accounts that have no logon capability do not need to have passwords set or changed.

**Audit:**

Access "Apps" menu. Under "Administrative Tools", select "Computer Management".
In left pane, expand "Local Users and Groups" and click on "Users".
Review the local users listed in the middle pane.
If any local accounts are present and are used by Apache Web Server, verify with System Administrator that default passwords have been changed.
If passwords have not been changed from the default, this is a finding.

**Remediation:**

Access "Apps" menu. Under "Administrative Tools", select "Computer Management".
In left pane, expand "Local Users and Groups" and click on "Users".
Change passwords for any local accounts that are present and are used by Apache Web Server.
Develop an internal process for changing passwords on a regular basis.

**Additional Information:**

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

## *1.52 AS24-W1-000950 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT III

**Description:**

The Apache web server must be configured in accordance with the security configuration settings based on DoD security configuration or implementation guidance, including STIGs, NSA configuration guides, CTOs, and DTMs.

```
GROUP ID: V-214358
RULE ID: SV-214358r961863
```

**Rationale:**

Configuring the Apache web server to implement organization-wide security implementation guides and security checklists guarantees compliance with federal standards and establishes a common security baseline across the DoD that reflects the most restrictive security posture consistent with operational requirements.

Configuration settings are the set of parameters that can be changed that affect the security posture and/or functionality of the system. Security-related parameters are parameters impacting the security state of the Apache web server, including the parameters required to satisfy other security control requirements.

**Audit:**

Review the website to determine if "HTTP" and "HTTPS" are used in accordance with well-known ports (e.g., 80 and 443) or those ports and services as registered and approved for use by the DoD Ports, Protocols, and Services Management (PPSM). Verify that any variation in PPS is documented, registered, and approved by the PPSM. If it is not, this is a finding.

**Remediation:**

Ensure the website enforces the use of IANA well-known ports for "HTTP" and "HTTPS".

**Additional Information:**

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

## *1.53 AS24-W1-000960 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT I

**Description:**

The Apache web server software must be a vendor-supported version.

```
GROUP ID: V-214359
RULE ID: SV-214359r961863
```

**Rationale:**

Many vulnerabilities are associated with older versions of web server software. As hot fixes and patches are issued, these solutions are included in the next version of the server software. Maintaining the web server at a current version makes the efforts of a malicious user to exploit the web service more difficult.

**Audit:**

Determine the version of the Apache software that is running on the system.
In a command line, navigate to "<'INSTALLED PATH'>\bin". Run "httpd -v" to view the Apache version.
If the version of Apache is not at the following version or higher, this is a finding:
Apache 2.4 (February 2012)

**Remediation:**

Install the current version of the web server software and maintain appropriate service packs and patches.

**Additional Information:**

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

## *1.54 AS24-W1-000970 (Manual)*

**Profile Applicability:**

- SEVERITY: CAT II

**Description:**

The Apache web server must alert the ISSO and SA (at a minimum) in the event of an audit processing failure.

```
GROUP ID: V-214360
RULE ID: SV-214360r961863
```

**Rationale:**

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without this notification, the security personnel may be unaware of an impending failure of the audit capability and system operation may be adversely affected.

Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

This requirement applies to each audit data storage repository (i.e., distinct information system component where audit records are stored), the centralized audit storage capacity of organizations (i.e., all audit data storage repositories combined), or both.

**Audit:**

Work with the SIEM administrator to determine if an alert is configured when audit data is no longer received as expected.
If there is no alert configured, this is a finding.

**Remediation:**

Work with the SIEM administrator to configure an alert when no audit data is received from Apache based on the defined schedule of connections.

**Additional Information:**

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

# Appendix: Summary Table

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| **1** | **STIG RULES** | | |
| 1.1 | AS24-W1-000010 (Manual) | ☐ | ☐ |
| 1.2 | AS24-W1-000020 (Manual) | ☐ | ☐ |
| 1.3 | AS24-W1-000030 (Manual) | ☐ | ☐ |
| 1.4 | AS24-W1-000065 (Manual) | ☐ | ☐ |
| 1.5 | AS24-W1-000070 (Manual) | ☐ | ☐ |
| 1.6 | AS24-W1-000090 (Manual) | ☐ | ☐ |
| 1.7 | AS24-W1-000130 (Manual) | ☐ | ☐ |
| 1.8 | AS24-W1-000160 (Manual) | ☐ | ☐ |
| 1.9 | AS24-W1-000180 (Manual) | ☐ | ☐ |
| 1.10 | AS24-W1-000200 (Manual) | ☐ | ☐ |
| 1.11 | AS24-W1-000210 (Manual) | ☐ | ☐ |
| 1.12 | AS24-W1-000240 (Manual) | ☐ | ☐ |
| 1.13 | AS24-W1-000250 (Manual) | ☐ | ☐ |
| 1.14 | AS24-W1-000260 (Manual) | ☐ | ☐ |
| 1.15 | AS24-W1-000270 (Manual) | ☐ | ☐ |
| 1.16 | AS24-W1-000280 (Manual) | ☐ | ☐ |
| 1.17 | AS24-W1-000300 (Manual) | ☐ | ☐ |
| 1.18 | AS24-W1-000310 (Manual) | ☐ | ☐ |
| 1.19 | AS24-W1-000330 (Manual) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 1.20 | AS24-W1-000360 (Manual) | ☐ | ☐ |
| 1.21 | AS24-W1-000370 (Manual) | ☐ | ☐ |
| 1.22 | AS24-W1-000380 (Manual) | ☐ | ☐ |
| 1.23 | AS24-W1-000430 (Manual) | ☐ | ☐ |
| 1.24 | AS24-W1-000450 (Manual) | ☐ | ☐ |
| 1.25 | AS24-W1-000460 (Manual) | ☐ | ☐ |
| 1.26 | AS24-W1-000470 (Manual) | ☐ | ☐ |
| 1.27 | AS24-W1-000480 (Manual) | ☐ | ☐ |
| 1.28 | AS24-W1-000500 (Manual) | ☐ | ☐ |
| 1.29 | AS24-W1-000530 (Manual) | ☐ | ☐ |
| 1.30 | AS24-W1-000550 (Manual) | ☐ | ☐ |
| 1.31 | AS24-W1-000580 (Manual) | ☐ | ☐ |
| 1.32 | AS24-W1-000590 (Manual) | ☐ | ☐ |
| 1.33 | AS24-W1-000620 (Manual) | ☐ | ☐ |
| 1.34 | AS24-W1-000630 (Manual) | ☐ | ☐ |
| 1.35 | AS24-W1-000640 (Manual) | ☐ | ☐ |
| 1.36 | AS24-W1-000650 (Manual) | ☐ | ☐ |
| 1.37 | AS24-W1-000670 (Manual) | ☐ | ☐ |
| 1.38 | AS24-W1-000680 (Manual) | ☐ | ☐ |
| 1.39 | AS24-W1-000690 (Manual) | ☐ | ☐ |
| 1.40 | AS24-W1-000700 (Manual) | ☐ | ☐ |
| 1.41 | AS24-W1-000710 (Manual) | ☐ | ☐ |

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 1.42 | AS24-W1-000720 (Manual) | ☐ | ☐ |
| 1.43 | AS24-W1-000730 (Manual) | ☐ | ☐ |
| 1.44 | AS24-W1-000740 (Manual) | ☐ | ☐ |
| 1.45 | AS24-W1-000760 (Manual) | ☐ | ☐ |
| 1.46 | AS24-W1-000800 (Manual) | ☐ | ☐ |
| 1.47 | AS24-W1-000820 (Manual) | ☐ | ☐ |
| 1.48 | AS24-W1-000830 (Manual) | ☐ | ☐ |
| 1.49 | AS24-W1-000860 (Manual) | ☐ | ☐ |
| 1.50 | AS24-W1-000930 (Manual) | ☐ | ☐ |
| 1.51 | AS24-W1-000940 (Manual) | ☐ | ☐ |
| 1.52 | AS24-W1-000950 (Manual) | ☐ | ☐ |
| 1.53 | AS24-W1-000960 (Manual) | ☐ | ☐ |
| 1.54 | AS24-W1-000970 (Manual) | ☐ | ☐ |

# Appendix: Change History

| Date | Version | Changes for this version |
|---|---|---|
| Sep 10, 2025 | 1.0.0 | Initial CIS Release |