CIS Arista MLS EOS 4.X NDM STIG Benchmark

v1.0.0 - 08-28-2025

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

Arista MLS EOS 4.X NDM Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 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 Arista MLS EOS 4.X NDM and are looking to comply with the STIG guidance

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

The Rule Title from the STIG.

Rationale Statement

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

Audit Procedure

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

Remediation Procedure

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

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

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

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

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

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

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

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

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

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

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for Arista MLS EOS 4.X NDM.

Recommendations

1 STIG RULES

Arista Cloud EOS

Arista MLS EOS 4.X NDM Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 ARST-ND-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must limit the number of concurrent sessions to an organization-defined number for each administrator account and/or administrator account type.

```
GROUP ID: V-255947
RULE ID: SV-255947r960735
```

Rationale:

Device management includes the ability to control the number of administrators and management sessions that manage a device. Limiting the number of allowed administrators and sessions per administrator based on account type, role, or access type is helpful in limiting risks related to denial-of-service (DoS) attacks.

This requirement addresses concurrent sessions for administrative accounts and does not address concurrent sessions by a single administrator via multiple administrative accounts. The maximum number of concurrent sessions must be defined based upon mission needs and the operational environment for each system. At a minimum, limits must be set for SSH, HTTPS, account of last resort, and root account sessions.

Audit:

Verify the device is configured to limit the number of concurrent management sessions with the following commands:

```
switch#sh run | section management ssh
management ssh
   connection limit 5
!
```

If the Arista network device is not configured to limit the number of SSH concurrent sessions, this is a finding.

Remediation:

Configure the switch to limit SSH concurrent connections to the device with the following commands:

```
switch#configure
switch(config)#management ssh
switch(config-mgmt-ssh)#connection limit 5
switch(config-mgmt-ssh)#exit
switch#wr
!
```

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 ARST-ND-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must enforce approved authorizations for controlling the flow of management information within the network device based on information flow control policies.

```
GROUP ID: V-255948
RULE ID: SV-255948r991781
```

Rationale:

A mechanism to detect and prevent unauthorized communication flow must be configured or provided as part of the system design. If management information flow is not enforced based on approved authorizations, the network device may become compromised. Information flow control regulates where management information is allowed to travel within a network device. The flow of all management information must be monitored and controlled so it does not introduce any unacceptable risk to the network device or data.

Application-specific examples of enforcement occur in systems that employ rule sets or establish configuration settings that restrict information system services or message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics).

Applications providing information flow control must be able to enforce approved authorizations for controlling the flow of management information within the system in accordance with applicable policy.

Audit:

Verify the Arista network device is configured with access control lists to control the flow of management information.

Step 1: Verify SSH has an inbound ACL applied as shown in the example below.

```
sh run | sec management ssh
 ip access-group MGMT_NETWORK in
```

Step 2: Verify the ACL permits only hosts from the management network to access the device.

```
sh run | sec access-list MGMT_NETWORK
 ip access-list MGMT_NETWORK
   10 permit ip 10.1.12.0/24 any
   20 deny ip any any log
```

If the Arista network device is not configured to enforce approved authorizations for controlling the flow of management information within the device based on control policies, this is a finding.

Remediation:

Step 1: Configure an ACL for SSH access using the following commands:

```
switch(config)#ip access-list MGMT_NETWORK
switch(config-acl-MGMT_NETWORK)#10 permit ip 10.1.12.0/24 any
switch(config-acl-MGMT_NETWORK)#20 deny ip any any log
switch(config-acl-MGMT_NETWORK)#exit
```

Step 2: Apply the ACL to management ssh.

```
switch(config)#management ssh
switch(config-mgmt-ssh)#ip access-group MGMT_NETWORK in
switch(config-mgmt-ssh)#exit
```

Additional Information:

CCI-001368 Enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.

- NIST SP 800-53::AC-4
- NIST SP 800-53A::AC-4.1 (iii)
- NIST SP 800-53 Revision 4::AC-4
- NIST SP 800-53 Revision 5::AC-4

CCI-004192 Protect nonlocal maintenance sessions by separating the maintenance session from other network sessions with the system by logically separated communications paths.

- NIST SP 800-53 Revision 5::MA-4 (4) (b) (2)

1.3 ARST-ND-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must be configured to enforce the limit of three consecutive invalid logon attempts, after which time it must block any login attempt for 15 minutes.

```
GROUP ID: V-255949
RULE ID: SV-255949r960840
```

Rationale:

By limiting the number of failed login attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute-forcing, is reduced.

Audit:

Verify the Arista device is configured to enforce the limit of three consecutive invalid logon attempts with the following command:

```
switch#show running-config | section aaa

aaa authentication policy lockout failure 3
duration 900
```

If the Arista device is not configured to enforce the limit of three consecutive invalid logon attempts, this is a finding.

Remediation:

Configure the account lockout policy using the following commands:

```
switch(config)#aaa authentication policy lockout failure 3
switch(config)#duration 900
switch(config)#exit
```

Additional Information:

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

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

1.4 ARST-ND-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must display the Standard Mandatory DOD Notice and Consent Banner before granting access to the device.

```
GROUP ID: V-255950
RULE ID: SV-255950r960843
```

Rationale:

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

System use notifications are required only for access via logon interfaces with human users.

Satisfies: SRG-APP-000068-NDM-000215, SRG-APP-000069-NDM-000216

Audit:

Verify the Arista network device is configured to present a DOD-approved banner that is formatted in accordance with DTM-08-060.

Verify the Arista device uses the following verbiage for applications that can accommodate banners of 1300 characters by using the following command:

switch#show configuration | section banner

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

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

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

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

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

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

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

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

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

If the Arista device does not display such a banner, this is a finding.

Remediation:

Configure the Arista network device to display the Standard Mandatory DOD Notice and Consent Banner before granting access to the device.

```
switch(config)#banner login
Enter TEXT message.
<Insert banner here>
Type 'EOF' on its own line to end.
```

Additional Information:

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

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

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

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

1.5 ARST-ND-000150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must be configured to audit all administrator activity.

```
GROUP ID: V-255951
RULE ID: SV-255951r960777
```

Rationale:

This requirement supports non-repudiation of actions taken by an administrator and is required in order to maintain the integrity of the configuration management process. All configuration changes to the network device are logged, and administrators authenticate with two-factor authentication before gaining administrative access. Together, these processes will ensure the administrators can be held accountable for the configuration changes they implement.

Satisfies: SRG-APP-000026-NDM-000208, SRG-APP-000027-NDM-000209, SRG-APP-000028-NDM-000210, SRG-APP-000029-NDM-000211, SRG-APP-000080-NDM-000220, SRG-APP-000091-NDM-000223, SRG-APP-000101-NDM-000231, SRG-APP-000319-NDM-000283, SRG-APP-000343-NDM-000289, SRG-APP-000495-NDM-000318, SRG-APP-000499-NDM-000319, SRG-APP-000503-NDM-000320, SRG-APP-000504-NDM-000321, SRG-APP-000506-NDM-000323

Audit:

Verify the Arista network device is configured to audit all administrator activity.

Verify the AAA logging settings in the configuration file with the following example:

```
switch#show running-config | section aaa

aaa authentication policy on-success log
aaa authentication policy on-failure log
aaa accounting exec default start-stop group radius logging
aaa accounting system default start-stop group radius logging
aaa accounting commands all default start-stop logging group radius
```

If the Arista network device is not configured to audit all administrator activity, this is a finding.

Remediation:

Configure the Arista network device to audit all administrator activity.

Configure the AAA settings to capture administrator activity events.

```
switch(config)#aaa authentication policy on-success log
switch(config)#aaa authentication policy on-failure log
switch(config)#aaa accounting exec default start-stop group radius logging
switch(config)#aaa accounting system default start-stop group radius logging
switch(config)#aaa accounting commands all default start-stop logging group
radius
```

Additional Information:

CCI-000018 Automatically audit account creation actions.

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

CCI-000135 Generate audit records containing the organization-defined additional information that is to be included in the audit records.

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

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

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

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001403 Automatically audit account modification actions.

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

CCI-001404 Automatically audit account disabling actions.

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

CCI-001405 Automatically audit account removal actions.

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

CCI-002130 Automatically audit account enabling actions.

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

CCI-002234 Log the execution of privileged functions.

- NIST SP 800-53 Revision 4::AC-6 (9)
- NIST SP 800-53 Revision 5::AC-6 (9)

1.6 ARST-ND-000340 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Arista network device must be configured to prohibit the use of all unnecessary and/or nonsecure functions, ports, protocols, and/or services.

```
GROUP ID: V-255952
RULE ID: SV-255952r1043177
```

Rationale:

To prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling (i.e., embedding of data types within data types), organizations must disable unused or unnecessary physical and logical ports/protocols on information systems.

Network devices are capable of providing a wide variety of functions and services. Some of the functions and services provided by default may not be necessary to support essential organizational operations. Additionally, it is sometimes convenient to provide multiple services from a single component (e.g., email and web services); however, doing so increases risk over limiting the services provided by any one component.

To support the requirements and principles of least functionality, the network device must support the organizational requirements providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved. Some network devices have capabilities enabled by default; if these capabilities are not necessary, they must be disabled. If a particular capability is used, then it must be documented and approved.

Audit:

Verify the Arista network device has telnet and https disabled.

Step 1: Determine if telnet is disabled with the following command:

```
switch#show management telnet

Telnet status for Default VRF is disabled
Telnet session limit is 20
Telnet session limit per host is 20
```

If telnet is enabled, this is a finding.

Step 2: Determine if https is disabled with the following command:

```
switch#show management http-server

SSL Profile:        none
FIPS Mode:          No
QoS DSCP:           0
LogLevel:           none
CSP Frame Ancestor: None
TLS Protocols:      1.0 1.1 1.2
   VRF           Server Status         Enabled Services
---------------------------------------------------------
   default       HTTPS: port 443       http-commands
```

If Enabled Services in the output shows http-commands, this is a finding.

Remediation:

Configure the Arista network device to prohibit the use of all unnecessary and/or nonsecure functions, ports, protocols, and/or services.

Step 1: Disable telnet with the following command:

```
switch#config
switch(config)#management telnet
switch(config-mgmt-telnet)#shutdown
switch(config-mgmt-telnet)#exit
switch(config)#exit
```

Step 2: Disable https with the following command:

```
switch#config
switch(config)#management api http-commands
switch(config-mgmt-api-http-commands)#shutdown
switch(config-mgmt-api-http-commands)#exit
switch(config)#exit
```

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

1.7 ARST-ND-000350 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must be configured with only one local account to be used as the account of last resort in the event the authentication server is unavailable.

```
GROUP ID: V-255953
RULE ID: SV-255953r1051115
```

Rationale:

Authentication for administrative (privileged level) access to the device is required at all times. An account can be created on the device's local database for use when the authentication server is down or connectivity between the device and the authentication server is not operable. This account is referred to as the account of last resort since it is intended to be used as a last resort and when immediate administrative access is absolutely necessary.

The account of last resort logon credentials must be stored in a sealed envelope and kept in a safe. The safe must be periodically audited to verify the envelope remains sealed. The signature of the auditor and the date of the audit should be added to the envelope as a record. Administrators should secure the credentials and disable the root account (if possible) when not needed for system administration functions.

Audit:

Step 1: Verify on the Arista network device that an account of last resort is configured using the following command:

```
switch#sh running-config | section username
username Emergency-Admin privilege 15 role network-admin secret sha512
$6$ObuWg.Eu7DwGD8k/$EgT0uI.hLrStrmxUvJijecxDXr.Zy.imi1UrDzDP38q8Erqgkfe0IhHzI
hYmR3ekW74XdAFf7I6SgzAoUFd0
```

Step 2: Verify the Arista network device default account has been overwritten with the local account of last resort.

```
switch#sh running-config | section username
username Emergency-Admin privilege 15 role network-admin secret sha512
$6$ObuWg.Eu7DwGD8k/$EgT0uI.hLrStrmxUvJijecxDXr.Zy.imi1UrDzDP38q8Erqgkfe0IhHzI
hYmR3ekW74XdAFf7I6SgzAoUFd0
```

If one local account on the Arista network device does not exist for use as the account of last resort in the event the authentication server is unavailable, this is a finding.

If the default admin account exists on the device, this is a finding.

Remediation:

Step 1: Configure the Arista network device for a username "Emergency-Admin" account of last resort using the following command:

```
switch#configure
switch(config)#username Emergency-Admin privilege 15 role network-admin
secret 0  <plain-text password>
```

Step 2: Ensure the Arista network device default account has been overwritten with the local account of last resort.

```
switch#sh running-config | section username
username Emergency-Admin privilege 15 role network-admin secret sha512
$6$ObuWg.Eu7DwGD8k/$EgT0uI.hLrStrmxUvJijecxDXr.Zy.imi1UrDzDP38q8Erqgkfe0IhHzI
hYmR3ekW74XdAFf7I6SgzAoUFd0
!
```

Use the following command to remove the default admin account if necessary:

```
switch(config)#no username admin
```

Step 3: As a final step in the case all administrative accounts are locked out of the device, ensure the username and password created for the account of last resort is contained within a sealed envelope and kept in a safe or secure network location.

Additional Information:

CCI-001358 Establish privileged user accounts in accordance with a role-based access scheme; or an attribute-based access scheme.

- NIST SP 800-53::AC-2 (7) (a)
- NIST SP 800-53A::AC-2 (7).1 (i)
- NIST SP 800-53 Revision 4::AC-2 (7) (a)
- NIST SP 800-53 Revision 5::AC-2 (7) (a)

CCI-002111 The organization identifies and selects the organization-defined information system account types of information system accounts which support organizational missions/business functions.

- NIST SP 800-53 Revision 4::AC-2 a

1.8 ARST-ND-000380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must enforce a minimum 15-character password length.

```
GROUP ID: V-255954
RULE ID: SV-255954r1015710
```

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password.

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised. Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Audit:

Review the Arista device configuration "show management security" to determine the minimum 15-character password length.

```
 switch#show run | section management security
management security
   password minimum length 15
!
```

If the Arista network device does not enforce a minimum 15-character password length, this is a finding.

Remediation:

Configure the Arista device to enforce a minimum password 15-character length.

```
 switch#configure
switch(config)#management security
switch(config-mgmt-security)#password minimum length 15
switch(config-mgmt-security)#exit
switch(config)#
!
```

Additional Information:

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

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

CCI-000205 The information system enforces minimum password length.

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

1.9 ARST-ND-000470 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Arista network device must use FIPS 140-2 approved algorithms for authentication to a cryptographic module.

```
GROUP ID: V-255955
RULE ID: SV-255955r961050
```

Rationale:

Unapproved mechanisms used for authentication to the cryptographic module are not validated and therefore cannot be relied upon to provide confidentiality or integrity, and DOD data may be compromised.

Network devices utilizing encryption are required to use FIPS-compliant mechanisms for authenticating to cryptographic modules.

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules utilize authentication that meets DOD requirements. However, authentication algorithms must configure security processes to use only FIPS-approved and NIST-recommended authentication algorithms.

Audit:

Determine if the Arista network device uses FIPS 140-2 approved algorithms for authentication to a cryptographic module.

Step 1: Review the Arista network device configuration to verify hardware or software entropy is enabled and FIPS restrictions are used in accordance with NIST-specified validated cryptographic requirements.

```
switch# show management security
CPU Model: AMD GX-424CC SOC with Radeon(TM) R5E Graphics
Security Chip: N313X
Crypto Module: Arista EOS Crypto Module v2.0
Forwarding ASIC: Jericho0 Model: Jericho
Blocked client protocols: None
Hardware entropy generation is enabled
Haveged entropy generation is disabled
Jitter entropy generation is disabled
!
```

If both hardware entropy and haveged entropy are disabled, this is a finding.

Step 2: Review the Arista network device configuration to verify that FIPS restrictions are enabled for management security to use EOS Crypto Module for the RSA key pair used for SSH and the device can only use FIPS-approved algorithms.

```
switch(config)show run | section management ssh
management ssh
   fips restrictions
!
```

If the FIPS restrictions line is not present, this is a finding.

Remediation:

Configure the Arista network device to use FIPS 140-2 approved algorithms for authentication to a cryptographic module.

Step 1: Configure the Arista network device to ensure hardware or software entropy is enabled and FIPS restrictions are used in accordance with NIST-specified validated cryptographic requirements.

```
switch(config)#management security
   switch(config-mgmt-security)#entropy source hardware
OR (only set one or the other, not both)
   switch(config-mgmt-security)#entropy source haveged
!
```

Step 2: Configure the Arista network device to ensure the old RSA key pairs are zeroized and a new FIPS-approved hostkey is generated. It is extremely important to complete this step after hardware or software entropy is configured.

```
switch#reset ssh hostkey rsa
!
```

IMPORTANT part of Step 2 Review the Arista network device configuration new key has been generated.

```
switch#show management ssh hostkey rsa public
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCz8vDiTWYcGuVrv04fwPj8YYBaHU+UFFl5zrFjeYiVl/dvs
wsiRSophF98aLjnRdJJ0NcjovjEEUnP0Q39UCoSYQRjrUzK2nzRMMD2IKxZyNhx9+/OT60lgh4M//
kwxq0vMI1nk1pUO/wRaN1B4IzDizcyP9jY28bSdz8Y5TyLgrca6Ja4v99Io+lkHG0bj6X8s+VnBsF
WMrlabw1s4bUPr9PzMfUHx9gLHCVR+DFZvPHMR4sSK14F949IJgOKsXj
chassisAddr=84:73:cf:6f:6c:55
```

Step 3: Enable FIPS restrictions for SSH and so the device can only use FIPS-approved algorithms.

switch(config)management ssh

switch(config-mgmt-ssh)#fips restrictions

Additional Information:

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

1.10 ARST-ND-000490 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Arista network device must terminate all network connections associated with a device management session at the end of the session, or the session must be terminated after 10 minutes of inactivity except to fulfill documented and validated mission requirements.

```
GROUP ID: V-255956
RULE ID: SV-255956r991784
```

Rationale:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free up resources committed by the managed network element.

Terminating network connections associated with communications sessions includes, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. This does not mean that the device terminates all sessions or network access; it only ends the inactive session and releases the resources associated with that session.

Satisfies: SRG-APP-000190-NDM-000267, SRG-APP-000186-NDM-000266

Audit:

Verify the Arista device is configured for 10-minute inactivity timeout for management sessions.

```
switch#sh run | section management
!
interface Management1
   ip address 172.28.134.55/20
!
management console
idle-timeout 10
!
management ssh
   idle-timeout 10
!
```

If the Arista network device is not configured to terminate the connection associated with a device management session at the end of the session or after 10 minutes of inactivity, this is a finding.

Remediation:

Configure the Arista network device to terminate the connections after 10 minutes of inactivity.

Step 1: Configure the settings for the console.

```
switch(config)#management console
switch(config-mgmt-console)#idle-timeout 10
switch(config-mgmt-console)#exit
switch(config)#
!
```

Step 2: Configure the settings for SSH.

```
switch(config)#management ssh
switch(config-mgmt-ssh)#idle-timeout 10
switch(config-mgmt-console)#exit
switch(config)#
!
```

Additional Information:

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

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

1.11 ARST-ND-000550 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

If the Arista network device uses role-based access control, the network device must enforce organization-defined role-based access control policies over defined subjects and objects.

```
GROUP ID: V-255957
RULE ID: SV-255957r987662
```

Rationale:

Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles. When administrators are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. Role-based access control (RBAC) simplifies privilege administration for organizations because privileges are not assigned directly to every administrator (which can be a significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of access control.

The RBAC policies and the subjects and objects are defined uniquely for each network device, so they cannot be specified in the requirement.

Satisfies: SRG-APP-000329-NDM-000287, SRG-APP-000380-NDM-000304

Audit:

Determine if the network device enforces role-based access control policy over defined subjects and objects. This requirement may be met through use of a properly configured authentication server.

Note: If not using role-based access for the network device, this check is Not Applicable.

Step 2: Verify the Arista network device configured AAA servers are synchronized for all role-based authentication access control structure defined by role types and user-defined control policies over defined subjects and objects.

```
switch(config)#show running-config | section role

role network-admin
   10 permit command .*
!
role operator
   10 permit command show running-config [all|detail] sanitized
   20 deny command
>|>>|extension|\||session|do|delete|copy|rmdir|mkdir|python-
shell|bash|platform|scp|append|redirect|tee|more|less|who|show run.*
   30 deny mode config command (no |default
)?(username|role|aaa|tcpdump|schedule|event.*)
   40 permit command .*
!
role tester
   10 permit command show running-config [all|detail] sanitized
   20 deny command
>|>>|extension|\||session|do|delete|copy|rmdir|mkdir|python-
shell|bash|platform|scp|append|redirect|tee|more|less|who|show run.*
   30 deny mode config command (no |default
)(username|role|aaa|tcpdump|schedule|event.*)
   40 permit command .*
```

If role-based access control policy is not enforced over defined subjects and objects, this is a finding.

Remediation:

Configure the network device and its associated authentication server to enforce role-based access control policy over defined subjects and objects.

```
switch(config)#
role network-admin
   10 permit command .*
!
role operator
   10 permit command show running-config [all|detail] sanitized
   20 deny command
>|>>|extension|\||session|do|delete|copy|rmdir|mkdir|python-
shell|bash|platform|scp|append|redirect|tee|more|less|who|show run.*
   30 deny mode config command (no |default
)?(username|role|aaa|tcpdump|schedule|event.*)
   40 permit command .*
!
role tester
   10 permit command show running-config [all|detail] sanitized
   20 deny command
>|>>|extension|\||session|do|delete|copy|rmdir|mkdir|python-
shell|bash|platform|scp|append|redirect|tee|more|less|who|show run.*
   30 deny mode config command (no |default
)(username|role|aaa|tcpdump|schedule|event.*)
   40 permit command .*
```

Additional Information:

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)

CCI-002169 Enforce a role-based access control policy over defined subjects and objects based upon organization-defined roles and users authorized to assume such roles.

- NIST SP 800-53 Revision 4::AC-3 (7)
- NIST SP 800-53 Revision 5::AC-3 (7)

1.12 ARST-ND-000600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must be configured to synchronize internal system clocks using redundant authenticated time sources.

```
GROUP ID: V-255958
RULE ID: SV-255958r1015711
```

Rationale:

The loss of connectivity to a particular authoritative time source will result in the loss of time synchronization (free-run mode) and increasingly inaccurate time stamps on audit events and other functions.

Multiple time sources provide redundancy by including a secondary source. Time synchronization is usually a hierarchy; clients synchronize time to a local source while that source synchronizes its time to a more accurate source. The network device must utilize an authoritative time server and/or be configured to use redundant authoritative time sources. This requirement is related to the comparison done in CCI-001891.

DOD-approved solutions consist of a combination of a primary and secondary time source using a combination or multiple instances of the following: a time server designated for the appropriate DOD network (NIPRNet/SIPRNet); United States Naval Observatory (USNO) time servers; and/or the Global Positioning System (GPS). The secondary time source must be located in a different geographic region than the primary time source.

Satisfies: SRG-APP-000373-NDM-000298, SRG-APP-000374-NDM-000299, SRG-APP-000375-NDM-000300, SRG-APP-000395-NDM-000347

Audit:

Determine if the network device is configured to synchronize internal information system clocks with authenticated primary and secondary time sources.

Verify the Arista network device configuration with the following example:

```
switch# show running-config | section ntp

ntp authentication-key 12 sha1 7 06131C2058470A58
ntp trusted-key 12
ntp authenticate servers
ntp local-interface Management1
ntp server 192.168.16.36 prefer key 12
ntp server 192.168.16.37 key 12
```

If the Arista network device is not configured to synchronize internal system clocks with the primary and secondary time sources, this is a finding.

If the Arista network device does not authenticate Network Time Protocol sources using authentication that is cryptographically based, this is a finding.

Remediation:

Configure the Arista network device for at least two trusted time sources and to use cryptographic authentication with the following command example:

```
switch#config
switch(config)#ntp authentication-key 12 sha1 0 <key>
switch(config)#ntp trusted-key 12
switch(config)#ntp authenticate servers
switch(config)#ntp local-interface Management1
switch(config)#ntp server 192.168.16.36 prefer key 12
switch(config)#ntp server 192.168.16.37 key 12
switch(config)#exit
```

Configure the local time zone for the device.

```
switch#config
switch(config)#clock timezone <timezone>
switch(config)#exit
```

Additional Information:

CCI-001889 Record time stamps for audit records that meet organization-defined granularity of time measurement.

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

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

CCI-004928 Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (2) (a)

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

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

CCI-004922 Synchronize system clocks within and between systems or system components.

- NIST SP 800-53 Revision 5::SC-45

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-001893 The information system identifies a secondary authoritative time source that is located in a different geographic region than the primary authoritative time source.

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

1.13 ARST-ND-000660 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must be configured to authenticate SNMP messages using a FIPS-validated Keyed-Hash Message Authentication Code (HMAC).

```
GROUP ID: V-255959
RULE ID: SV-255959r961506
```

Rationale:

Without authenticating devices, unidentified or unknown devices may be introduced, thereby facilitating malicious activity. Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk.

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

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

Audit:

Review the network device configuration to verify SNMP messages are authenticated using a FIPS-validated HMAC.

Verify the Arista network device is configured for the following SNMP example parameters:

```
switch(config)#show run | section snmp
snmp-server engineID local f5717f444ca880dbb200
snmp-server chassis-id ID CC-7050X3
snmp-server contact FedSE
snmp-server location JITC
snmp-server view snmpview system included
snmp-server group testers v3 priv read snmpview
snmp-server user jitc-sw testers v3 localized f8527f444ca990dcc200 auth sha
7b65225a6abf5111cd951e6cb7e105aef5bcd734 priv aes
a1aedb1986642e766d4c8032d58e73b72bc3528b
snmp-server host 192.168.10.31 version 3 priv jitc-sw
snmp-server enable traps snmp authentication
snmp-server enable traps snmp link-down
snmp-server enable traps snmp link-up
!
```

If the Arista network device is not configured to authenticate SNMP messages using a FIPS-validated HMAC, this is a finding.

Remediation:

Configure the network device to authenticate SNMP messages using a FIPS-validated HMAC.

Configure the Arista network device following the example SNMP parameters to ensure messages are authenticated using FIPS-validated HMAC:

```
switch(config)#snmp-server engineID local f5717f444ca880dbb200
switch(config)#snmp-server chassis-id ID CC-7050X3
switch(config)#snmp-server contact FedSE
switch(config)#snmp-server location JITC
switch(config)#snmp-server view snmpview system included
switch(config)#snmp-server group testers v3 priv read snmpview
switch(config)#snmp-server user jitc-sw testers v3 localized
f8527f444ca990dcc200 auth sha 7b65225a6abf5111cd951e6cb7e105aef5bcd734 priv
aes a1aedb1986642e766d4c8032d58e73b72bc3528b
switch(config)#snmp-server host 192.168.10.31 version 3 priv jitc-sw
switch(config)#snmp-server enable traps snmp authentication
switch(config)#snmp-server enable traps snmp link-down
switch(config)#snmp-server enable traps snmp link-up
```

Additional Information:

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

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

1.14 ARST-ND-000690 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Arista network devices must use FIPS-validated Keyed-Hash Message Authentication Code (HMAC) to protect the integrity of remote maintenance sessions.

```
GROUP ID: V-255960
RULE ID: SV-255960r961554
```

Rationale:

Unapproved mechanisms used for authentication to the cryptographic module are not verified and therefore cannot be relied upon to provide confidentiality or integrity, and DOD data may be compromised.

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through a network, either an external network (e.g., the internet) or an internal network.

Currently, HMAC is the only FIPS-approved algorithm for generating and verifying message/data authentication codes in accordance with FIPS 198-1. Products that are FIPS 140-2 validated will have an HMAC that meets specification; however, the option must be configured for use as the only message authentication code used for authentication to cryptographic modules.

Separate requirements for configuring applications and protocols used by each application (e.g., SNMPv3, SSHv2, NTP, HTTPS, and other protocols and applications that require server/client authentication) are required to implement this requirement. Where SSH is used, the SSHv2 protocol suite is required because it includes Layer 7 protocols such as SCP and SFTP, which can be used for secure file transfers.

Satisfies: SRG-APP-000411-NDM-000330, SRG-APP-000156-NDM-000250

Audit:

Determine if the Arista network device is configured to use FIPS-validated HMAC to protect the integrity of remote maintenance sessions.

NOTE: Although allowed by SP800-131Ar2 for some applications, SHA-1 is considered a compromised hashing standard and is being phased out of use by industry and government standards. Unless required for legacy use, DOD systems should not be configured to use SHA-1 for integrity of remote access sessions.

Verify the HMAC settings for SSH using the following command:

```
switch#sh run | section management ssh

mac hmac-sha2-256 hmac-sha2-512
```

If the Arista network device does not implement replay-resistant authentication mechanisms for network access to privileged accounts, this is a finding.

Remediation:

Configure the Arista network device to use FIPS-validated HMAC to protect the integrity of remote maintenance sessions.

```
switch(config)#management ssh
switch(config-mgmt-ssh)#mac hmac-sha2-256 hmac-sha2-512
switch(config-mgmt-ssh)#exit
```

Additional Information:

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

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

CCI-002890 Implement organization-defined cryptographic mechanisms to protect the integrity of nonlocal maintenance and diagnostic communications.

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

1.15 ARST-ND-000700 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Arista network device must be configured to implement cryptographic mechanisms using a FIPS 140-2 approved algorithm to protect the confidentiality of remote maintenance sessions.

```
GROUP ID: V-255961
RULE ID: SV-255961r961557
```

Rationale:

This requires the use of secure protocols instead of their unsecured counterparts, such as SSH instead of telnet, SCP instead of FTP, and HTTPS instead of HTTP. If unsecured protocols (lacking cryptographic mechanisms) are used for sessions, the contents of those sessions will be susceptible to eavesdropping, potentially putting sensitive data (including administrator passwords) at risk of compromise and potentially allowing hijacking of maintenance sessions.

Audit:

Validate that a FIPS validated SSH encryption algorithm is selected.

NOTE: AES-CBC algorithms have been considered compromised and are no longer recommended for cryptographic algorithms. AES-CTR and AES-GCM are both superior algorithms and are recommended.

```
sh run | section management ssh
cipher aes256-ctr aes512-ctr aes128-ctr
```

If the Arista network device is not configured to implement cryptographic mechanisms to protect the confidentiality of remote maintenance sessions using a FIPS 140-2 approved algorithm, this is a finding.

Remediation:

Configure the Arista network device to use FIPS-approved algorithms to protect the confidentiality of remote maintenance sessions.

```
switch(config)#management ssh
switch(config-mgmt-ssh)#cipher aes256-ctr aes512-ctr aes128-ctr
```

Additional Information:

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

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

1.16 ARST-ND-000790 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must be configured to capture all DOD auditable events.

```
GROUP ID: V-255962
RULE ID: SV-255962r960891
```

Rationale:

Auditing and logging are key components of any security architecture. Logging the actions of specific events provides a means to investigate an attack; to recognize resource utilization or capacity thresholds; or to identify an improperly configured network device. If auditing is not comprehensive, it will not be useful for intrusion monitoring, security investigations, and forensic analysis.

Satisfies: SRG-APP-000095-NDM-000225, SRG-APP-000096-NDM-000226, SRG-APP-000097-NDM-000227, SRG-APP-000098-NDM-000228, SRG-APP-000099-NDM-000229, SRG-APP-000100-NDM-000230, SRG-APP-000516-NDM-000334, SRG-APP-000357-NDM-000293, SRG-APP-000360-NDM-000295, SRG-APP-000505-NDM-000322

Audit:

Verify the Arista network device is configured to audit all DOD auditable events.

Verify the logging settings in the configuration file with the following example:

```
switch#sh running-config | section logging

logging buffered informational
logging trap informational
```

NOTE: Acceptable settings include debugging, informational, and notifications to adjust syslog server traffic impact. Setting to higher severity levels can cause necessary lower-level events to be missed.

If the Arista network device is not configured to audit all DOD auditable events, this is a finding.

Remediation:

Configure a logging level sufficient to capture all DOD auditable events.

```
switch(config)#logging buffered informational
switch(config)#logging trap informational
```

NOTE: Acceptable settings include debugging, informational, and notifications to adjust syslog server traffic impact. Setting to higher severity levels can cause necessary lower-level events to be missed.

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-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-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

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

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

CCI-001858 Provide an alert in an organization-defined real-time-period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.

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

1.17 ARST-ND-000810 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The network device must be configured to use an authentication server to authenticate users prior to granting administrative access.

```
GROUP ID: V-255963
RULE ID: SV-255963r961863
```

Rationale:

Centralized management of authentication settings increases the security of remote and nonlocal access methods. This control is particularly important protection against the insider threat. With robust centralized management, audit records for administrator account access to the organization's network devices can be more readily analyzed for trends and anomalies. The alternative method of defining administrator accounts on each device exposes the device configuration to remote access authentication attacks and system administrators with multiple authenticators for each network device.

Audit:

Verify the Arista network device is configured to use an authentication server as primary source for authentication.

Verify the Arista network device configuration for RADIUS server IP, aaa group server, and defined encryption key using the following example command:

```
switch#show running-config |section radius
radius-server host 192.168.10.101 key 7 106D1A182224E12AZ
!
aaa group server radius RADIUS_1
   server 192.168.10.101
!
switch#show running-config | section aaa
aaa authentication login default group radius local
aaa authentication login console group radius local
aaa authentication dot1x default group radius
aaa authentication policy on-success log
aaa authentication policy on-failure log
aaa authorization console
aaa authorization commands all default local
aaa accounting exec default start-stop group radius logging
aaa accounting system default start-stop group radius logging
aaa accounting commands all default start-stop logging group radius
```

If the Arista network device is not configured to use an authentication server to authenticate users prior to granting administrative access, this is a finding.

Remediation:

Configure the Arista network device to use an authentication server.

Step 1: Configure the Arista network device to use RADIUS server using the following commands:

```
switch#config
switch(config)#radius-server host 192.168.10.101 key 7 106D1A182224E12AZ
aaa group server radius RADIUS_1
   server 192.168.10.101
```

Step 2: Configure all network connections associated with device management to use an authentication server for login authentication.

```
switch(config)#aaa authentication login default group radius local
aaa authentication login console group radius local
aaa authentication dot1x default group radius
aaa authentication policy on-success log
aaa authentication policy on-failure log
aaa authorization console
aaa authorization commands all default local
aaa accounting exec default start-stop group radius logging
aaa accounting system default start-stop group radius logging
aaa accounting commands all default start-stop logging group radius
switch(config)#exit
```

Additional Information:

CCI-000370 Manage configuration settings for organization-defined system components using organization-defined automated mechanisms.

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

1.18 ARST-ND-000820 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The network device must be configured to conduct backups of system level information contained in the information system when changes occur.

```
GROUP ID: V-255964
RULE ID: SV-255964r961863
```

Rationale:

System-level information includes default and customized settings and security attributes, including ACLs that relate to the network device configuration, as well as software required for the execution and operation of the device. Information system backup is a critical step in ensuring system integrity and availability. If the system fails and there is no backup of the system-level information, a denial of service condition is possible for all who utilize this critical network component.

This control requires the network device to support the organizational central backup process for system-level information associated with the network device. This function may be provided by the network device itself; however, the preferred best practice is a centralized backup rather than each network device performing discrete backups.

Audit:

Verify the Arista network device is configured with an “event-handler” to complete an incremental backup of the running configuration, which can be maintained in the switch flash memory stored in /mnt/flash/startup-config_directory (filetime):

```
switch#show run | section event-handler
event-handler CFG_BACKUP
   trigger on-startup-config
   action bash buf () { filetime=$(date +%Y%m%d); cp /mnt/flash/startup-
config /mnt/flash/startup-config_${filetime}; }; buf
!
```

If the Arista network device is not configured to conduct backups of system-level data when changes occur, this is a finding.

Remediation:

Configure the Arista network device with an “event-handler” to complete an incremental backup of the running configuration, which can be maintained in the switch flash memory stored in /mnt/flash/startup-config_directory (filetime):

```
switch#config
switch(config)#event-handler CFG_BACKUP
switch(config-handler-CFG_BACKUP)#trigger on-startup-config
switch(config-handler-CFG_BACKUP)#action bash buf () { filetime=$(date
+%Y%m%d); cp /mnt/flash/startup-config /mnt/flash/startup-config_${filetime};
}; buf
switch(config-handler-CFG_BACKUP)#exit
switch(config)#exit
!
```

Additional Information:

CCI-000537 Conduct backups of system-level information contained in the system per organization-defined frequency that is consistent with recovery time and recovery point objectives.

- NIST SP 800-53::CP-9 (b)
- NIST SP 800-53A::CP-9.1 (v)
- NIST SP 800-53 Revision 4::CP-9 (b)
- NIST SP 800-53 Revision 5::CP-9 (b)

1.19 ARST-ND-000840 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Arista network device must obtain its public key certificates from an appropriate certificate policy through an approved service provider.

```
GROUP ID: V-255965
RULE ID: SV-255965r961863
```

Rationale:

For user certificates, each organization obtains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice.

Audit:

Determine if the Arista network device obtains public key certificates from an appropriate certificate policy through an approved service provider.

Note: This check is Not Applicable if not using any PKI certificates.

Verify the DOD PKI certificates are copied to /certificate directory on the switch as outlined in the Arista Military Deployment Guide and configured as in the section "Configuring RSA SecureID with OTP Management".

```
  switch# #dir certificate:
Directory of certificate:/
       -rw-        2025           Apr 30 17:34  ARISTA_ROOT_CA.crt
       -rw-        2110           Apr 30 17:34  ARISTA_SIGNING_CA.crt
       -rw-        2015           Apr 30 17:35  Arista-CCS-720XP-48Y6.pem
       -rw-        2020           Apr 30 17:35
DOD_JITC_Root_CA_3__0x01__DOD_JITC_Root_CA_3.cer
       -rw-        2125           Apr 30 17:35  CA-60.cer
!
```

Verify the provider of the certificate is a DOD-approved certificate authority.

If the Arista network device does not obtain its public key certificates from an appropriate certificate policy through an approved service provider, this is a finding.

Remediation:

Configure the Arista network device to obtain its public key certificates from an appropriate certificate policy through an approved service provider.

Step 1: Configure the Arista network device by following the steps outlined in the Arista Military Unique Deployment Guide to generate the DOD PKI certificate signing request [switch.csr] for submission to DOD PKI CA. Example configuration:

```
switch#security pki certificate generate signing-request key rsa1.key
Common Name for use in subject: 192.168.25.26
Two-Letter Country Code for use in subject: US
State for use in subject: AZ
Locality Name for use in subject: Ft Huachuca
Organization Name for use in subject: CONTRACTOR,PKI,DOD
Organization Unit Name for use in subject: U.S. GOVERNMENT
Email address for use in subject:
IP addresses (space separated) for use in subject-alternative-name:
192.168.25.26
DNS names (space separated) for use in subject-alternative-name:
Email addresses (space separated) for use in subject-alternative-name:
-----BEGIN CERTIFICATE REQUEST-----
MIIC6DCCAdACAQAwgYAxCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJBWjEUMBIGA1UE
BwwLRnQgSHVhY2h1Y2ExGzAZBgNVBAoMEkNPTlRSQUNUT1IsUEtJLERvRDEYMBYG
A1UECwwPVS5TLiBHT1ZFUk5NRU5UMRcwFQYDVQQDDA4xOTIuMTY4LjI0MC4yMzCC
i7TGBvhm5PTbfAzBma8/hSlsBGJ0qnOteb1Zaw== <Abbreviated Output Due to Size>
-----END CERTIFICATE REQUEST-----
```

Step 2: Once the DOD PKI signed certificates are received, CA Root Certificate and Intermediate Certificates obtained from CA must be uploaded onto the Arista network device directory of /certificate: The certificate's transfer can be accomplished by SCP or USB. The detail configuration can be found in the Arista Military Unique Deployment Guide in the section "Configuring RSA SecureID with OTP Management".

The following commands copy the certificates using device USB1: to directory of the certificate:

```
switch#copy usb1:Arista-23.pem certificate:
Copy completed successfully.
switch#copy usb1: CA-60.crt certificate:
Copy completed successfully.
switch#copy usb1: DODDISASWCA_60.crt certificate:
Copy completed successfully.
!
```

The following commands verify all three certificates are correctly copied to the certificate directory:

```
switch#directory certificate
switch#dir certificate:
Directory of certificate:/
       -rw-        2025          Aug 11 10:52  CA-60.crt
       -rw-        2110          Aug 11 10:52  ARISTA_SIGNING_CA.crt
       -rw-        1724           Aug 9 14:35  DODDISASWCA_60.crt
       -rw-        1722          Aug 12 09:38  arista-b64.cer
       -rw-        1696          Aug 12 14:35  Arista-23.pem
       -rw-        1696          Aug 12 14:36  intCert.pem
!
```

The following commands configure the SSL-profile using the PKI certificates on the switch with the RSA SecureID server and trust chain:

```
switch(config)#management security
switch(config-mgmt-security)#ssl profile RSA01
switch(config-mgmt-sec-ssl-profile-RSA01)#tls versions 1.2
switch(config-mgmt-sec-ssl-profile-RSA01)#certificate Arista-23.pem key
rsa1.key
switch(config-mgmt-sec-ssl-profile-RSA01)#trust certificate Arista-23.pem
switch(config-mgmt-sec-ssl-profile-RSA01)#trust certificate
DODDISASWCA_60.crt
switch(config-mgmt-sec-ssl-profile-RSA01)#chain certificate CA-60.cer
switch(config-mgmt-sec-ssl-profile-RSA01)#show active
management security
   ssl profile RSA01
      tls versions 1.2
      certificate Arista-23.pem.pem key rsa1.key
      trust certificate certificate Arista-23.pem
      trust certificate CA-60.cer
      trust certificate DODDISASWCA_60.crt
      chain certificate CA-60.crt
radius-server tls ssl-profile RSA01
!
```

Step 3: Configure the switch RadSec Proxy server and RSA SecureID server IP address and RADIUS attribute configuration for ssl-profile RSA01.

```
switch(config)#radius-server tls ssl-profile RSA01
switch(config)#radius-server host 192.168.16.102 key 7 09595D080D0C1453
switch(config)#radius-server host 192.168.16.55 key 7 120C161606020F45
switch(config)#radius-server host 192.168.16.55 tls
switch(config)#aaa group server radius RADsecProxy
   server 192.168.16.55 tls
!
```

Step 4: Configure the AAA authentication and authorization parameters for SSL-profile and RadSec Proxy Server.

```
switch(config)#no aaa root
switch(config)#aaa authorization policy local default-role aristaadmin
switch(config)#logging level AAA informational
switch(config)#aaa group server radius RADsecProxy
   server 192.168.16.55 tls
switch(config)#aaa group server radius TIC1
   server 192.168.16.103
switch(config)#aaa authentication login default local group RADsecProxy
switch(config)#aaa authentication login console local
switch(config)#aaa authentication policy on-success log
switch(config)#aaa authentication policy on-failure log
switch(config)#aaa authorization exec default local group RADsecProxy
switch(config)#aaa authorization commands all default local
switch(config)#aaa accounting commands all default start-stop logging group
radius
switch(config)#write
!
```

Step 5: Verify the AAA configuration to ensure all parameters from the previous step are accurate with the following command:

```
switch(config)#show running-config | section aaa
no aaa root
aaa authorization policy local default-role aristaadmin
logging level AAA informational
aaa group server radius RADsecProxy
   server 192.168.16.55 tls
aaa group server radius TIC1
   server 192.168.16.103
aaa authentication login default local group RADsecProxy
aaa authentication login console local
aaa authentication policy on-success log
aaa authentication policy on-failure log
aaa authorization exec default local group RADsecProxy
aaa authorization commands all default local
aaa accounting commands all default start-stop logging group radius
!
switch#show aaa methods authentication
Authentication method lists for LOGIN:
  name=default methods=local, group RADsecProxy
  name=login methods=local
Authentication method list for ENABLE:
  name=default methods=local
Authentication method list for DOT1X:
  name=default methods=
!
switch##sh radius
RADIUS server             : 192.168.16.45, authentication port 1812,
accounting port 1813
             Messages sent:          10
         Messages received:      10
         Requests accepted:      9
         Requests rejected:        1
          Requests timeout:       0
    Requests retransmitted:  0
             Bad responses:           0
         Connection errors:        0
                DNS errors:              0
      CoA request received:     0
       DM request received:    0
              CoA ack sent:            0
               DM ack sent:           0
              CoA Nak sent:           0
               DM Nak sent:          0

RADIUS server-group: RSA1
     0: 192.168.16.45, authentication port 1812, accounting port 1813

RADIUS server-group: TIC1
     0: 192.168.16.103, authentication port 1812, accounting port 1813
Last time counters were cleared: never
!
trust certificate Arista-23.pem
switch#(config-mgmt-sec-ssl-profile-RSA1)#Aug 24 15:56:41 switch SuperServer:
%SECURITY-3-SSL_PROFILE_VALID: SSL profile 'RSA01' is valid.
```

Additional Information:

CCI-001159 Issue public key certificates under an organization-defined certificate policy or obtain public key certificates from an approved service provider.

- NIST SP 800-53::SC-17
- NIST SP 800-53A::SC-17.1
- NIST SP 800-53 Revision 4::SC-17
- NIST SP 800-53 Revision 5::SC-17 a

1.20 ARST-ND-000850 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Arista network Arista device must be configured to send log data to a central log server for the purpose of forwarding alerts to the administrators and the ISSO.

```
GROUP ID: V-255966
RULE ID: SV-255966r961863
```

Rationale:

The aggregation of log data kept on a syslog server can be used to detect attacks and trigger an alert to the appropriate security personnel. The stored log data can used to detect weaknesses in security that enable the network IA team to find and address these weaknesses before breaches can occur. Reviewing these logs, whether before or after a security breach, are important in showing whether someone is an internal employee or an outside threat.

Satisfies: SRG-APP-000516-NDM-000350, SRG-APP-000119-NDM-000236, SRG-APP-000120-NDM-000237, SRG-APP-000515-NDM-000325

Audit:

Verify the Arista network device has been configured Syslog server for auditing data by using the following command:

switch#show running-config | section logging

```
logging host 192.168.16.30 514
!
```

If logging host is not configured to send log data to a central log server, this is a finding.

Remediation:

The Arista network device must be configured for Syslog server for auditing data by using the following commands:

```
switch(config)#logging host 192.168.16.30 514
```

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

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)

1.21 ARST-ND-000860 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The Arista network device must be running an operating system release that is currently supported by the vendor.

```
GROUP ID: V-255967
RULE ID: SV-255967r961863
```

Rationale:

Network devices running an unsupported operating system lack current security fixes required to mitigate the risks associated with recent vulnerabilities.

Audit:

Verify the Arista device is running a certified version of EOS from the Arista.com website on the Support/Software Download section.

```
switch#show version
Arista DCS-7280SRA-48C6-F
Hardware version: 21.00
Serial number: SSJ18250372
Hardware MAC address: 7483.ef6d.86f7
System MAC address: 7483.ef6d.86f7

Software image version: 4.26.4M
Architecture: i686
Internal build version: 4.26.4M-25280047.4264M
Internal build ID: 79589245-f1f3-49b7-8bee-cbfacac004e6
Image format version: 1.0

Uptime: 2 weeks, 0 days, 9 hours and 53 minutes
Total memory: 8098984 kB
Free memory: 6155528 kB
```

If the Arista network device is not running an operating system release that is currently supported by Arista Networks, this is a finding.

Remediation:

Upgrade the Arista network device to an operating system that is supported by the vendor.

Step 1: The Administrator would log on to www.arista.com/support/software-download website and choose EOS/Active Releases and choose appropriate version of EOS to download.

Step 2: Transfer the EOS-4.x.yz.swi.sha512sum to Arista network device directory "flash:".

Step 3: From the EOS CLI, type dir flash: to verify the file EOS-4.x.yz.swi.sha512sum is in the directory "flash:".

```
switch#directory flash:
EOS-4.x.yz.swi.sha512sum
```

Step 4: Use the command verify to verify the checksum sha512sum:

```
switch#verify flash: /sha512 flash:EOS-4.x.yz
checksum should match
```

Step 5: The file can also be verified from bash.

```
switch#bash
#bash
# sha512sum  /mnt/flash/EOS-4.x.yz
```

*note the Arista network device would not run an invalid version of EOS and if the checksum does not match, contact an Arista Representative for assistance.

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	ARST-ND-000010 (Manual)	☐	☐
1.2	ARST-ND-000110 (Manual)	☐	☐
1.3	ARST-ND-000120 (Manual)	☐	☐
1.4	ARST-ND-000130 (Manual)	☐	☐
1.5	ARST-ND-000150 (Manual)	☐	☐
1.6	ARST-ND-000340 (Manual)	☐	☐
1.7	ARST-ND-000350 (Manual)	☐	☐
1.8	ARST-ND-000380 (Manual)	☐	☐
1.9	ARST-ND-000470 (Manual)	☐	☐
1.10	ARST-ND-000490 (Manual)	☐	☐
1.11	ARST-ND-000550 (Manual)	☐	☐
1.12	ARST-ND-000600 (Manual)	☐	☐
1.13	ARST-ND-000660 (Manual)	☐	☐
1.14	ARST-ND-000690 (Manual)	☐	☐
1.15	ARST-ND-000700 (Manual)	☐	☐
1.16	ARST-ND-000790 (Manual)	☐	☐
1.17	ARST-ND-000810 (Manual)	☐	☐
1.18	ARST-ND-000820 (Manual)	☐	☐
1.19	ARST-ND-000840 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	ARST-ND-000850 (Manual)	☐	☐
1.21	ARST-ND-000860 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 28, 2025	1.0.0	Initial CIS Release