CIS Forescout Network Device Management STIG Benchmark

v1.0.0 - 08-27-2025

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

Forescout Network Device Management Secure Technical Implementation Guide (STIG)

Version: 2 Release: 3 Benchmark

Date: 02 Jul 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 Forescout Network Device Management and are looking to comply with the STIG guidance

Recommendation Definitions

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 Forescout Network Device Management

Recommendations

1 STIG RULES

Forescout Network Device Manager

Forescout Network Device Management Secure Technical Implementation Guide (STIG)

Version: 2 Release: 3 Benchmark

Date: 02 Jul 2025

CLASSIFICATION unclassified

1.1 FORE-NM-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must limit the number of concurrent sessions to one for each administrator account.

```
GROUP ID: V-230930
RULE ID: SV-230930r960735
```

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:

Determine if Forescout requires a limit of one session per user. This requirement may be verified by demonstration or configuration review.

1. Log on to the Forescout Administrator UI.
2. From the menu, select Tools >> Options >> CounterAct user profiles >> Password and Sessions >> Session.
3. Verify the "allow only one login session per user", "Terminate existing session upon new login", and "Console and web portal sessions cannot exist concurrently".

If Forescout does not enforce one session per user, this is a finding.

Remediation:

Configure Forescout to require a limit of one session per user.

1. Log on to the Forescout Administrator UI.
2. From the menu, select Tools >> Options >> CounterAct user profiles >> Password and Sessions >> Session.
3. Check "allow only one login session per user".
4. Select the "Terminate existing session upon new login" radio button.
5. Select "Console and web portal sessions cannot exist concurrently".

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 FORE-NM-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must terminate the account of last resort password when members with access to the password leave the group.

```
GROUP ID: V-230931
RULE ID: SV-230931r1018751
```

Rationale:

A shared/group account credential is a shared form of authentication that allows multiple individuals to access the network device using a single account. If shared/group account credentials are not terminated when individuals leave the group, the user that left the group can still gain access even though they are no longer authorized. There may also be instances when specific user actions need to be performed on the network device without unique administrator identification or authentication. Examples of credentials include passwords and group membership certificates.

Audit:

Review the documentation to verify a procedure exists to change the account of last resort and root account password when users with knowledge of the password leave the group.

If a procedure does not exist to change the account of last resort and root account password when users with knowledge of the password leave the group, this is a finding.

Remediation:

Establish and document a procedure that requires the changing of the account of last resort and root account password when users with knowledge of the password leave the group.

To change the password:

1. Log on to the Forescout Administrator UI.
2. From the menu, select Tools >> Options >> Console Preferences >> Password and Sessions.
3. Click the Password tab.
4. Click "User must change password at next logon if changed by admin user".
5. Note: the next time the account of last resort is accessed, the user will be prompted to change their password.

Note: Use of a cryptographically generated password is recommended. Password must be stored in a locked safe and used only when necessary since individual accounts are required to be used to ensure non-repudiation.

Additional Information:

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

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

CCI-002142 The information system terminates shared/group account credentials when members leave the group.

- NIST SP 800-53 Revision 4::AC-2 (10)

1.3 FORE-NM-000030 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must be configured with only one web account and one CLI account of last resort with limited access and used only when the authentication server is unavailable.

```
GROUP ID: V-230932
RULE ID: SV-230932r1111863
```

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 must be added to the envelope as a record. Administrators must secure the credentials and disable the root account (if possible) when not needed for system administration functions.

Audit:

Verify only one local account exists and that it has full administrator privileges.

1. Log on to the Forescout Administrator UI.
2. From the menu, select Tools >> Options >> CounterACT User Profiles.

If local accounts in the CounterACT User profile or CLI exist other than the accounts of last resort, this is a finding.

Remediation:

There are two default accounts of last resort. The CLIAdmin root account can only be used to access Forescout with the CLI. Accounts created in CounterACT user profile in the management console do not have access to login to the CLI. The default console account "Admin" allows access only to the management console. These accounts can be used as the accounts of last resort or two other accounts may be created for this purpose as long as a strong password that meets DoD requirements is used for both.

1. Log on to the Forescout Administrator UI.
2. From the menu, select Tools >> Options >> CounterACT user profiles.

Remove unauthorized local accounts not identified as the account of last resort.

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

1.4 FORE-NM-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must be configured to enforce the limit of three consecutive invalid logon attempts, after which time it must lock out the user account from accessing the device for 15 minutes.

```
GROUP ID: V-230933
RULE ID: SV-230933r960840
```

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:

Determine if Forescout is configured either to enforce the limit of three consecutive invalid logon attempts by a user during a 15-minute time period, or to use an authentication server to perform this function.

1. Log on to the Forescout Administrator UI.
2. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
3. Verify the "Lock account after" radio button is selected.
4. Verify that "3" password failures for "15 minutes" is configured.

If the limit of three consecutive invalid logon attempts by a user during a 15-minute time period is not enforced, this is a finding.

Remediation:

Configure Forescout or its associated authentication server to enforce the limit of three consecutive invalid logon attempts by a user during a 15-minute time period.

1. Log on to the Forescout Administrator UI.
2. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
3. Ensure the "Lock account after" radio button is selected.
4. Ensure that "3" password failures for "15" minutes is configured.

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

1.5 FORE-NM-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the device.

```
GROUP ID: V-230934
RULE ID: SV-230934r960843
```

Rationale:

Display of the DoD-approved use notification before granting access to the application 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.

The banner must be formatted in accordance with DTM-08-060.

Audit:

1. Log on to the Forescout Administrator UI.
2. Select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
3. Select the Login tab and check the "Display this Notice and Consent Message after login" option.
4. Select the "Before login, prompt user to accept these Terms and Conditions" and view the text.

If the banner is not present or not in exact compliance with the current verbiage and spacing in DTM-08-060, this is a finding.

Remediation:

Log on to the Forescout Administrator UI.

1. Select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Select the "Login" tab and check the "Display this Notice and Consent Message after login" option.
3. Select the "Before login, prompt user to accept these Terms and Conditions".
4. Copy the exact text and formatting for the Standard Mandatory DoD and Consent Banner into the white box. Be sure to adhere to the exact line spacing required by DTM-08-060.

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

1.6 FORE-NM-000080 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must generate log records when successful attempts to access privileges occur.

```
GROUP ID: V-230936
RULE ID: SV-230936r960885
```

Rationale:

Without generating log records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Log records can be generated from various components within the information system (e.g., module or policy filter).

Audit:

Verify the syslog trigger is configured.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under "User Operations", verify "Include user operations" is checked.

If Forescout does not generate log records when successful attempts to access privileges occur, this is a finding.

Remediation:

Configure the syslog trigger.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under "User Operations", check "Include user operations".

Additional Information:

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

1.7 FORE-NM-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must retain the Standard Mandatory DOD Notice and Consent Banner on the screen until the administrator acknowledges the usage conditions and takes explicit actions to log on for further access.

```
GROUP ID: V-230935
RULE ID: SV-230935r1113787
```

Rationale:

The banner must be acknowledged by the administrator prior to the device allowing the administrator access to the network device. This provides assurance that the administrator has seen the message and accepted the conditions for access. If the consent banner is not acknowledged by the administrator, DOD will not be in compliance with system use notifications required by law.

To establish acceptance of the network administration policy, a click-through banner at management session logon is required. The device must prevent further activity until the administrator executes a positive action to manifest agreement.

In the case of CLI access using a terminal client, entering the username and password when the banner is presented is considered an explicit action of acknowledgement. Entering the username, viewing the banner, then entering the password is also acceptable. The web management tool configuration setting works for both the CLI and the web management tool.

Audit:

Verify Forescout retains the Standard Mandatory DOD-approved Notice and Consent Banner on the screen until users acknowledge the usage conditions and takes explicit actions to log on for further access.

Attempt to log on to the Forescout device as a system administrator using the web management tool.

If Forescout does not retain the Standard Mandatory DOD-approved Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access, this is a finding.

Remediation:

Configure banner retention.

1. From the UI, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Select the "Login" tab and check the "Before login, prompt user to accept these Terms and Conditions".
3. Select "Apply" to save the settings.

Additional Information:

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

1.8 FORE-NM-000090 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must generate log records when attempts to modify administrator privileges occur.

```
GROUP ID: V-230937
RULE ID: SV-230937r961800
```

Rationale:

Without generating log records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Log records can be generated from various components within the network device (e.g., module or policy filter).

Audit:

Verify the syslog trigger is configured.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, verify "Include user operations" is checked.

If Forescout does not generate log records when attempts to modify administrator privileges occur, this is a finding.

Remediation:

Configure the syslog trigger.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, check "Include user operations".

Additional Information:

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

1.9 FORE-NM-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must generate log records when attempts to delete administrator privileges occur.

```
GROUP ID: V-230938
RULE ID: SV-230938r961812
```

Rationale:

Without generating log records specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Log records can be generated from various components within the network device (e.g., module or policy filter).

Audit:

Verify the syslog trigger is configured.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, verify "Include user operations" is checked.

If Forescout does not generate log records when attempts to delete administrator privileges occur, this is a finding.

Remediation:

Configure the syslog trigger.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, check "Include user operations".

Additional Information:

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

1.10 FORE-NM-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must generate log records showing when successful logon attempts occur.

```
GROUP ID: V-230939
RULE ID: SV-230939r961824
```

Rationale:

Without generating log records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Log records can be generated from various components within the network device (e.g., module or policy filter).

Audit:

Verify the syslog trigger is configured.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, verify "Include user operations" is checked.

If Forescout does not generate log records when successful logon attempts occur, this is a finding.

Remediation:

Configure the syslog trigger.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, check "Include user operations".

Additional Information:

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

1.11 FORE-NM-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must generate log records for privileged activities or other system-level access.

```
GROUP ID: V-230940
RULE ID: SV-230940r961827
```

Rationale:

Without generating log records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Log records can be generated from various components within the network device (e.g., module or policy filter).

Audit:

Verify the syslog trigger is configured.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, verify "Include user operations" is checked.

If Forescout does not generate log records when for privileged activities or other system-level access, this is a finding.

Remediation:

Configure the syslog trigger.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, check "Include user operations".

Additional Information:

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

1.12 FORE-NM-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must generate log records showing starting and ending time for administrator access to the system.

```
GROUP ID: V-230941
RULE ID: SV-230941r961830
```

Rationale:

Without generating log records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Log records can be generated from various components within the network device (e.g., module or policy filter).

Audit:

Verify the syslog trigger is configured.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, verify "Include user operations" is checked.

If Forescout does not generate log records showing starting and ending time for administrator access to the system, this is a finding.

Remediation:

Configure the syslog trigger.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, check "Include user operations".

Additional Information:

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

1.13 FORE-NM-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must generate log records when concurrent logons from different workstations occur.

```
GROUP ID: V-230942
RULE ID: SV-230942r961833
```

Rationale:

Without generating log records that are specific to the security and mission needs of the organization, it would be difficult to establish, correlate, and investigate the events relating to an incident or identify those responsible for one.

Log records can be generated from various components within the network device (e.g., module or policy filter).

Audit:

Verify the syslog trigger is configured.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, verify "Include user operations" is checked.

If Forescout does not generate log records when concurrent logons from different workstations occur, this is a finding.

Remediation:

Configure the syslog trigger.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Under User Operations, check "Include user operations".

Additional Information:

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

1.14 FORE-NM-000150 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The Forescout must configure a remote syslog where audit records are stored on a centralized logging target that is different from the system being audited.

```
GROUP ID: V-230943
RULE ID: SV-230943r1111869
```

Rationale:

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

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

Audit:

Verify the syslog.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Send Events To.
3. Click the IP address of the site's centralized syslog server.
4. Verify Identity, Facility, and Severity, as required by the SSP, are configured.

If the site's syslog server is not configured, this is a finding.

Remediation:

Configure the syslog.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Send Events To.
3. Click "Add".
4. Enter the IP address of the site's centralized syslog.
5. Configure Identity, Facility, and Severity as required by the SSP.

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)

1.15 FORE-NM-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must be configured to synchronize internal information system clocks using redundant authoritative time sources.

```
GROUP ID: V-230944
RULE ID: SV-230944r1112438
```

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 the source synchronizes 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.

Audit:

Determine if Forescout is configured to synchronize internal clocks with the organization's primary and secondary NTP servers.

Determine if Forescout is configured to synchronize internal clocks with the organization's primary and secondary NTP servers.

1. Open an SSH session and authenticate to the Forescout command line.
2. Verify a primary and secondary NTP server has been configured with the command "fstool ntp test".

Or

1. Open the Forescout console.
2. Navigate to General >> Time and verify "Enable sync with NTP server" is checked.

If Forescout is not configured to synchronize internal information system clocks with the organization's primary and secondary NTP servers, this is a finding.

Remediation:

Configure Forescout to synchronize internal information system clocks with the primary and secondary time sources located in different geographic regions using redundant authoritative time sources.

1. Open an SSH session and authenticate to the Forescout command line.
2. Configure the primary and secondary NTP servers with the command "fstool ntp setup ".

or

1. Open the Forescout console.
2. Navigate to General >> Time.
3. Check the box for "Enable sync with NTP server".

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

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-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)

1.16 FORE-NM-000170 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must be configured to use Coordinated Universal Time (UTC).

```
GROUP ID: V-230945
RULE ID: SV-230945r1111875
```

Rationale:

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

Time stamps generated by the application include date and time. Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC.

Audit:

Determine if Forescout records time stamps for log records that can be mapped to UTC. This requirement may be verified by demonstration or configuration review.

Note: Updating time preferences will force Forescout into maintenance mode and the service must be restarted. Use a scheduled outage for planned maintenance and stop Forescout service prior to adjusting time settings.

1. From the CLI run "fstool tz".
2. Type "yes" to change the timezone.
3. Type "2" for GMT offset.
4. Type "0" to enter the offiset (GMT 0 is equal to UTC time).
5. Ensure the Local time and Universal time match and type "yes" to continue.
6. Type "yes" to reboot.

If Forescout does not record time stamps for log records that can be mapped to UTC, this is a finding.

Remediation:

Remove accounts that are not authorized. Do not remove the account of last resort.

1. Log on to the Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> CounterAct User Profiles.
3. Select (highlight) the user profile to be reviewed (group or user) and then select "Remove".
4. Remove any applicable external group membership or individual users on the external directory service.

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

1.17 FORE-NM-000190 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must prohibit installation of software without explicit privileged permission by only authorized individuals.

```
GROUP ID: V-230946
RULE ID: SV-230946r1018753
```

Rationale:

Allowing anyone to install software, without explicit privileges, creates the risk that untested or potentially malicious software will be installed on the system. This requirement applies to code changes and upgrades for all network devices.

Audit:

Determine if the network device prohibits installation of software without explicit privileged status. This requirement may be verified by demonstration or configuration review.

1. From the menu, select Tools >> Options >> User Console and Options.
2. Select (highlight) the user profile to be reviewed (group or user) and then select Edit >> Permissions.
3. Check a sampling of users against the current SSP to verify only the users that should have privilege to update software have the Software Upgrade privilege selected.

If installation of software is not prohibited without explicit privileged status, this is a finding.

Remediation:

Remove accounts that are not authorized. Do not remove the account of last resort.

Compare users with the current SSP and ensure only the users that should have the privilege to update software have the Software Upgrade privilege selected.

1. From the menu, select Tools >> Options >> User Console and Options.
2. Select (highlight) the user profile to be reviewed (group or user) and then select Edit >> Permissions.
3. Disable or delete unauthorized users.

Additional Information:

CCI-003980 Allow user installation of software only with explicit privileged status.

- NIST SP 800-53 Revision 5::CM-11 (2)

CCI-001812 The information system prohibits user installation of software without explicit privileged status.

- NIST SP 800-53 Revision 4::CM-11 (2)

1.18 FORE-NM-000200 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must enforce access restrictions associated with changes to device configuration.

```
GROUP ID: V-230947
RULE ID: SV-230947r961461
```

Rationale:

Failure to provide logical access restrictions associated with changes to device configuration may have significant effects on the overall security of the system.

For Forescout, ensure only authorized users have access to user profile permissions. All other admins are blocked from access via the console tools and/or web portal based on permissions set on the Edit user profile.

Audit:

Determine if the network device enforces access restrictions associated with changes to device configuration.

1. Log on to the Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> User Console and Options.
3. Select (highlight) the user profile to be reviewed (group or user) and then select Edit >> Permissions.
4. Check user against the current SSP and ensure only the users that should have the privilege to make changes have the CounterACT Appliance Configuration; CounterACT Appliance Control; Module Control; Multiple CounterACT Appliance Management; Policy Control; Policy Management; and User Management privileges selected.

If the network device does not enforce such access restrictions, this is a finding.

Remediation:

Remove accounts that are not authorized. Do not remove the account of last resort.

1. Log on to the Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> User Console and Options.
3. Select (highlight) the user profile to be reviewed (group or user) and then select Edit >> Permissions.
4. Check user against current SSP and ensure only the users that should have privilege to make changes have the CounterACT Appliance Configuration; CounterACT Appliance Control; Module Control; Multiple CounterACT Appliance Management; Policy Control; Policy Management; and User Management privileges selected.
5. Delete or disable unauthorized users.

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)

1.19 FORE-NM-000210 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must audit the enforcement actions used to restrict access associated with changes to the device.

```
GROUP ID: V-230948
RULE ID: SV-230948r1018754
```

Rationale:

Without auditing the enforcement of access restrictions against changes to the device configuration, it will be difficult to identify attempted attacks, and an audit trail will not be available for forensic investigation for after-the-fact actions.

Forescout must only be configures such that only authorized users have access to user profile permissions. All other admins are blocked from access via the console tools and/or web portal based on permissions set on the Edit user profile.

Audit:

Determine if the network device audits the enforcement actions used to restrict access associated with changes to the device. This requirement may be verified by demonstration, configuration review, or validated test results.

1. Log on to the Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> User Console and Options.
3. Select (highlight) the user profile to be reviewed (group or user) and then select Edit >> Permissions.
4. Check user against current SSP and ensure only the users with privileges to make changes have the Least Privilege required permissions.

If the network device does not audit the enforcement actions used to restrict access associated with changes to the device, this is a finding.

Remediation:

Remove accounts that are not authorized. Do not remove the account of last resort. Ensure a Least Privilege Permission approach is taken with all accounts created.

1. Log on to the Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> User Console and Options.
3. Select (highlight) the user profile to be reviewed (group or user) and then select Edit >> Permissions.
4. Check user against current SSP and ensure only the users that are allowed privileges to make changes have the Least Privilege required permissions.
5. Delete or disable unauthorized users.

Additional Information:

CCI-003938 Automatically generate audit records of the enforcement actions.

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

CCI-001814 The Information system supports auditing of the enforcement actions.

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

1.20 FORE-NM-000220 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must prevent the installation of patches, service packs, plug-ins, or modules without verification the update has been digitally signed using a certificate that is recognized and approved by the organization.

```
GROUP ID: V-230949
RULE ID: SV-230949r1018755
```

Rationale:

Changes to any software components can have significant effects on the overall security of the network device. Verifying software components have been digitally signed using a certificate that is recognized and approved by the organization ensures the software has not been tampered with and has been provided by a trusted vendor.

Accordingly, patches, service packs, or application components must be signed with a certificate recognized and approved by the organization.

Verifying the authenticity of the software prior to installation validates the integrity of the patch or upgrade received from a vendor. This ensures the software has not been tampered with and has been provided by a trusted vendor. Self-signed certificates are disallowed by this requirement. The device should not have to verify the software again. This requirement does not mandate DOD certificates for this purpose; however, the certificate used to verify the software must be from an approved Certificate Authority (CA).

Customer portal updates file download section on the vendor website has the MD5 hashes for the updates files.

Currently, this is the method used by DOD to pull down files rather than using the internal connection to the Forescout server.

Audit:

Verify by inspecting the SSP or documentation to determine if there is a procedure for validating the MD5 hash against the Forescout updates.forescout.com portal to ensure that the software has come from the Forescout server.

If the site does not have a documented process to prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate recognized and approved by the organization, this is a finding.

Remediation:

When Forescout updates are downloaded, whether from the DOD update server or the updates.forescout.com portal, each update consists of an MD5 hash. Manually inspect, compare, and verify the MD5 hash against the Forescout website to ensure that the software has come from the Forescout server.

Additional Information:

CCI-003992 Prevent the installation of organization-defined software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

- NIST SP 800-53 Revision 5::CM-14

CCI-001749 The information system prevents the installation of organization-defined software components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.

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

1.21 FORE-NM-000230 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must limit privileges to change the modules and OSs resident within software libraries.

```
GROUP ID: V-230950
RULE ID: SV-230950r960960
```

Rationale:

Changes to any software components of the network device can have significant effects on the overall security of the network. Therefore, only qualified and authorized individuals must be allowed administrative access to the network device for implementing any changes or upgrades. If the network device were to enable non-authorized users to make changes to software libraries, those changes could be implemented without undergoing testing, validation, and approval.

Audit:

Determine if there are users defined in Forescout that are not authorized to change the software libraries.

Verify that Administrator privileges have been restricted for these users.

This is verified by reviewing the administrator account profiles and auditing the assigned privilege for updated Forescout software.

1. Log on to the Forescout Console and select Tools >> Options >> Console User Profiles.
2. Select the user group that is not authorized access according to the SSP.
3. Select "Edit" and the "Permissions" tab
4. Verify the users do not have the "Plugin Management" and "Software Upgrade" options selected.

If Forescout is not configured to limit privileges to change the software resident within software libraries for unauthorized users, this is a finding.

Remediation:

Configure Forescout to prevent access to change the software resident within software libraries for unauthorized personnel.

View each of the Forescout user group accounts that are associated with the external user directory groups (e.g., RADIUS, Active directory, LDAP). Perform the following actions for each group.

1. Log on to the Forescout Console and select Tools >> Options >> Console User Profiles.
2. Select the user group that is not authorized access according to the SSP.
3. Select "Edit" and the "Permissions" tab.
4. Unselect the options for "Module Management" and "Software Upgrade".

Additional Information:

CCI-001499 Limit privileges to change software resident within software libraries.

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

1.22 FORE-NM-000240 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must enforce access restrictions associated with changes to the firmware, OS, USB port, and console port.

```
GROUP ID: V-230951
RULE ID: SV-230951r961863
```

Rationale:

Changes to the hardware or software components of the network device can have significant effects on the overall security of the network. Therefore, only qualified and authorized individuals must be allowed administrative access to the network device for implementing any changes or upgrades. This requirement applies to updates of the application files, configuration, ACLs, and policy filters.

There is a USB port and a console RJ45 port.

The Console port is secured by the CLI security configuration.

The USB port is only accessible via the CLI, not the web manager tool. The user will be prompted to see if it should be turned on. It is off by default and requires authorized login from the CLI.

Audit:

Check Forescout to determine if only authorized administrators have permissions for changes, deletions, and updates on the network device. Inspect the maintenance log to verify changes are being made only by the system administrators.

1. Log on to the Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> CounterACT User Profiles.
3. Select (highlight) the user profile to be reviewed (group or user) and then select "Edit".
4. Verify the non-administrator account selected does not have "update" on the "Permissions" tab for "Forescout Appliance Configuration".

If unauthorized users are allowed to change the hardware or software, this is a finding.

Remediation:

Configure Forescout to prevent access to change the software resident within software libraries for unauthorized personnel.

View each of the Forescout user group accounts associated with the external user directory groups (e.g., RADIUS, Active directory, LDAP).

Perform the following actions for each group:

1. Log on to the Forescout Console and select Tools >> Options >> Console User Profiles.
2. Select the user group that is not authorized access according to the SSP.
3. Select "Edit" and the "Permissions" tab.
4. Verify the options for "Module Management" or "Software Upgrade" are not selected.

Additional Information:

CCI-000345 Enforce logical access restrictions associated with changes to the system.

- NIST SP 800-53::CM-5
- NIST SP 800-53A::CM-5.1
- NIST SP 800-53 Revision 4::CM-5
- NIST SP 800-53 Revision 5::CM-5

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

1.23 FORE-NM-000250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must be configured to use an authentication server for the purpose of authenticating users prior to granting administrative access.

```
GROUP ID: V-230952
RULE ID: SV-230952r1111877
```

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, log 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:

Review the Forescout configuration to determine if administrative accounts for device management exist on the device other than the account of last resort and root account.

1. Log on to the Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Console Preferences.
3. Select (highlight) the user profile to be reviewed (group or user) and then select "Edit".
4. Verify each user profile is for an approved administrator.
5. Verify each external LDAP group account profile by verifying on the trusted external directory group membership.

If any administrative accounts other than the account of last resort and root account exist on the device, this is a finding.

Remediation:

Remove accounts that are not authorized. Do not remove the account of last resort.

1. Log on to the Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> CounterAct User Profiles.
3. Select (highlight) the user profile to be reviewed (group or user) and then select "Remove".
4. Remove any applicable external group membership or individual users on the external directory service.

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

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)

CCI-003627 Disable accounts when the accounts have expired.

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

CCI-003628 Disable accounts when the accounts are no longer associated to a user.

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

CCI-003831 Alert organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

- NIST SP 800-53 Revision 5::AU-9 b

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

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

CCI-004047 Implement multi-factor authentication for local; network; and/or remote access to privileged accounts; and/or non-privileged accounts such that the device meets organization-defined strength of mechanism requirements.

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

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

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

CCI-004059 For password-based authentication, update the list of passwords on an organization-defined frequency.

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

CCI-004060 For password-based authentication, update the list of passwords when organizational passwords are suspected to have been compromised directly or indirectly.

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

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

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

CCI-004063 For password-based authentication, require immediate selection of a new password upon account recovery.

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

CCI-004064 For password-based authentication, allow user selection of long passwords and passphrases, including spaces and all printable characters.

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

CCI-004065 For password-based authentication, employ automated tools to assist the user in selecting strong password authenticators.

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

CCI-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

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

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

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

1.24 FORE-NM-000260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must be running an operating system release that is currently supported by the vendor.

```
GROUP ID: V-230953
RULE ID: SV-230953r1113791
```

Rationale:

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

In October 2021, there is plan to make Version 7 end-of-life. This will be stated on the product lifecycle page of the Forescout website. All versions of V8 and above are authorized for use in DOD.

Version 8 or later is mandatory after October 2021.

Audit:

Check that Forescout is still running supported operating system versions and that all vulnerability patches and updates have been applied.

Verify the installed version is supported by Forescout by checking the Forescout support website lifecycle page. Currently, Version 8 or later is mandatory after October 2021.

If Forescout is running an operating system release that is not supported by the vendor, this is a finding.

Check from the Console:

1. Log into the Forescout management console.
2. Select Help > About Forescout to show the current version.

Check from the CLI:

1. Log into the Forescout CLI.
2. Type "fstool version" to show the current running version.

Remediation:

Check that Forescout is still running supported operating system versions and that all vulnerability patches and updates have been applied.

Establish and document a procedure that requires the auditing of OS versions and any patches and updates have been applied in accordance with Forescout support website lifecycle page.

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

1.25 FORE-NM-000270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-230954
RULE ID: SV-230954r987662
```

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.

Forescout has three predefined user roles: Admin, Web Access, and Console User. The Admin role has access to all data and management functions.

By default, the Console role has access to the management console and the Web role has access to the view-only portal. However, both roles may be assigned one or more permissions, each with its own set of privileges to the data and functions.

Audit:

Check the administrative accounts assigned to each role are documented within the SSP and have been configured correctly with least privilege.

1. Log on to Forescout UI.
2. Select Tools >> Options >> CounterACT User Profiles.
3. Select username >> Edit >> Permissions.

Check the SSP against created users and ensure least privilege has been configured properly. Options include Custom accounts for Console Access and Web Access. Each access account is then further established with permissions based on the user's authorizations.
If Forescout does not enforce organization-defined, role-based access control policies over defined subjects and objects, this is a finding.

Remediation:

Login to Forescout UI.

1. Select Tools >> Options >> CounterACT User Profiles.
2. Select username >> Edit >> Permissions.

Check the SSP against created users and ensure least privilege has been configured properly. Options include Custom accounts for Console Access and Web Access. Each access account is then further established with permissions based on the user's authorizations.

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

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)

1.26 FORE-NM-000280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must generate log records for a locally developed list of auditable events.

```
GROUP ID: V-230955
RULE ID: SV-230955r961863
```

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.

Audit:

Verify the syslog triggers are configured in accordance with SSP requirements.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Ensure the proper NAC events and System Logs and Events are selected in compliance with the SSP.

If Forescout does not generate log records for a locally developed list of auditable events, this is a finding.

Remediation:

Configure Forescout auditing messages to ensure auditing is comprehensible for monitoring and analysis.

1. Log on to Forescout Administrator UI with admin or operator credentials.
2. From the menu, select Tools >> Options >> Modules >> Syslog >> Syslog Triggers.
3. Ensure the proper NAC events and System Logs and Events are selected.

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-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

1.27 FORE-NM-000290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must be configured to conduct backups of system-level information contained in the information system when changes occur.

```
GROUP ID: V-230956
RULE ID: SV-230956r961863
```

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.

Perform scheduled backups of the Forescout system to FTP, SFTP, and SCP sites. Using scheduled backups provides extra safety and protection against hard drive failures and data loss.

The system backup feature saves all CounterACT device and Console settings.

This data includes the following:

- Configuration
- License
- Operating System configuration
- Plugins/Modules

These categories include, for example:

- Forescout platform IP address
- License information
- Channel
- Email
- Internal network parameters
- Basic and advanced NAC Policy definitions
- Legitimate traffic definitions
- Report schedules

Audit:

Check Forescout to determine if the network device is configured to conduct backups of system-level information contained in the information system when changes occur or weekly, whichever is sooner.

1. Open the Forescout Console and select Tools >> Advanced >> Backup.
2. On the “System Backup” tab, verify the "Enable System Backup" radio button is selected.
3. Verify the Backup schedule is selected to at least "weekly".

If Forescout does not support the organizational requirement to conduct backups of system-level data according to the defined frequency, this is a finding.

Remediation:

Configure Forescout to conduct backups of information system documentation, including security-related documentation, when changes occur or weekly, whichever is sooner.

Setup a backup server.

1. Open the Forescout Console and select Tools >> Advanced >> Backup >> Backup Server.
2. Click "SCP" or "SFTP" for the transfer protocol.
3. Add the IP address of the backup destination server.
4. Add the directory to receive the file.
5. Add PKI key (preferred) or add username and DoD compliant password for the backup account to be used.
6. Enable "Authenticate Destination Sever".
7. Test the file transfer.
8. Click "Apply".

Generate a backup job.

1. Click the "System Backup" tab.
2. Select "Enable System Backup".
3. Under Backup Schedule, add a "Generate backup at" and enter a time to run the backup in accordance with site procedures.
4. Select "Weekly" for Recurrence Pattern.

When changes to the configuration occur, the admin must immediately create a new backup by clicking "Backup Now" on the Backup screen.

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

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)

1.28 FORE-NM-000300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must support organizational requirements to conduct backups of information system documentation, including security-related documentation, when changes occur or weekly, whichever is sooner.

```
GROUP ID: V-230957
RULE ID: SV-230957r961863
```

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.

Perform scheduled backups of the Forescout system to FTP, SFTP, and SCP sites. Using scheduled backups provides extra safety and protection against hard drive failures and data loss.

The system backup feature saves all CounterACT device and Console settings.

This data includes the following:

- Configuration
- License
- Operating System configuration
- Plugins/Modules

These categories include, for example:

- Forescout platform IP address
- License information
- Channel
- Email
- Internal network parameters
- Basic and advanced NAC Policy definitions
- Legitimate traffic definitions
- Report schedules

Audit:

Check Forescout to determine if the network device is configured to conduct backups.

1. Open the Forescout Console and select Tools >> Advanced >> Backup.
2. On the “System Backup” tab, verify the "Enable System Backup" radio button is selected.
3. Verify the Backup schedule is selected to at least "weekly".

If Forescout does not support organizational requirements to conduct backups of information system documentation, including security-related documentation when changes occur or weekly, whichever is sooner, this is a finding.

Remediation:

Configure Forescout to conduct backups.

Setup a backup server.

1. Open the Forescout Console and select Tools >> Advanced >> Backup >> Backup Server.
2. Click "SCP" or "SFTP" for the transfer protocol.
3. Add the IP address of the backup destination server.
4. Add the directory to receive the file.
5. Add PKI key (preferred) or add username and DoD compliant password for the backup account to be used.
6. Enable "Authenticate Destination Sever".
7. Test the file transfer.
8. Click "Apply".

Generate a backup job.

1. Click the System Backup tab.
2. Select "Enable System Backup".
3. Under Backup Schedule, add a "Generate backup at" and enter a time to run the backup in accordance with site procedures.
4. Select "Weekly" for Recurrence Pattern.

When changes to the configuration occur, the admin must immediately create a new backup by clicking "Backup Now" on the Backup screen.

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

CCI-000539 Conduct backups of system documentation, including security-related documentation, per an organization-defined frequency that is consistent with recovery time and recovery point objectives.

- NIST SP 800-53::CP-9 (c)
- NIST SP 800-53A::CP-9.1 (vi)
- NIST SP 800-53 Revision 4::CP-9 (c)
- NIST SP 800-53 Revision 5::CP-9 (c)

1.29 FORE-NM-000320 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must obtain its public key certificates from an appropriate certificate policy through an approved service provider.

```
GROUP ID: V-230958
RULE ID: SV-230958r1113789
```

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 Forescout obtains public key certificates from an appropriate certificate policy through an approved service provider.

To review the Web server certificate presented for captive portal/authentication:

1. Log into the Forescout management console.
2. Go to Options >> Certificates >> System Certificates.
3. Locate the certificates where the "Used For" column shows "Web Portal".
4. Ensure all enabled certificates are issued by a trusted CA and are not self-signed.

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

Remediation:

Generate a certificate signing request by completing the following procedures:

1. Navigate to Tools >> Options >> Certificates >> System Certificates.
2. On the right of the screen click "Generate CSR".
3. Complete the following fields (bolded fields are necessary for the Common Criteria evaluation and underlined fields have the required selection made):

- Common Name –
- Organization –
- Organizational Unit –
- Locality –
- State –
- Country Code –
- Email Address -
- Key Length –
- Signature Algorithm –
- Key Usages – < Checking all items that apply Client Authentication, Server Authentication and Email Signing>
- Validity –

4. Click "Next".
5. When the CSR is generated, scroll down to ensure the public key and common name are present.
6. Click "Scope option – ALL", and then click "Next".
7. Enter a name for system certificate.
8. Check "Enable presenting this certificate".
9. Click "Finish".
10. Click "Apply", and then click "Yes" to save the changes.

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

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

1.30 FORE-NM-000330 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Forescout must use DOD-approved PKI rather than proprietary or self-signed device certificates.

```
GROUP ID: V-230959
RULE ID: SV-230959r1043177
```

Rationale:

To mitigate the risk of unauthorized access to sensitive information by entities that have been issued certificates by DOD-approved PKIs.

Forescout generates a key-pair and a Certificate Signing Request (CSR). The CSR is sent to the approved certificate authority (CA), who signs it and returns it as a certificate. That certificate is then installed.

The process to obtain a device PKI certificate requires the generation of a CSR, submission of the CSR to a CA, approval of the request by an RA, and retrieval of the issued certificate from the CA.

Audit:

Navigate to Tools >> Options >> Certificates >> Trusted Certificates.

1. The System Certificates page appears and provides information for the local certificates.
2. Select a certificate to display the certificate details.

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

Remediation:

Replace the self-signed certificate with a CA-signed certificates for greater security. To obtain a CA-signed certificate:

Generate a certificate signing request (CSR) to obtain a CA-signed certificate for the nodes in your deployment.

1. Navigate to Tools >> Options >> Certificates >> System Certificates.
2. On the right of the screen click "Generate CSR".
3. Enter the values for generating a CSR.

- Key Length –
- Signature Algorithm –
- Examples:
- RSA: rsa size <512 | 1024 | 2048 | 4096>>
- ECDSA: size <256 | 384>>
- Key Usages – < Checking all items that apply Client Authentication, Server Authentication and Email Signing>
- Validity –

4. Click "Next".

To import the required trusted CA certificates by completing the following procedures:

1. Login to the console.
2. Navigate to Tools >> Options >> Certificates >> Trusted Certificates.
3. Click "Add".
4. Specify the Certificate file.
5. Ensure "Enable trusting this certificate" is checked.
6. Click "Next".
7. Click "Next" after reviewing the certificate data.
8. Ensure "All subsystems" is selected, and then click "Next".
9. Ensure "All Forescout devices" is selected, and then click "Finish".
10. Click "Apply".

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

1.31 FORE-NM-000340 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must disable the Request Customer Verification setting.

```
GROUP ID: V-230960
RULE ID: SV-230960r1043177
```

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.

This option connects to a user verification server at Forescout infrastructure used for verification of customer profiles and must not be used in DoD. If accidentally checked, this must error out.

Audit:

In the Password and Sessions login options, ensure "request customer verification" is not enabled.

1. Log on to the Forescout Administrator UI.
2. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
3. Ensure the option for "request customer verification" is unchecked.

If the Request Customer Verification setting is enabled, this is a finding.

Remediation:

In the Password and Sessions login options, disable the "request customer verification" option.

1. Log on to the Forescout Administrator UI.
2. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
3. Ensure the option for "request customer verification" is unchecked.

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

1.32 FORE-NM-000350 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

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

```
GROUP ID: V-230961
RULE ID: SV-230961r961506
```

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 Forescout configuration to determine if the network device authenticates SNMP endpoint devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

1. Select Tools >> Options >> Switch.
2. Select a network device and review the "SNMP" tab.
3. Verify that the "SNMPv3" option is selected and the "HMAC-SHA" authentication protocol is selected.
4. Verify that the "use privacy" radio button is selected and "AES-128" is also selected from the drop-down box.

If Forescout does not authenticate SNMP messages using a FIPS-validated Keyed-Hash Message Authentication Code (HMAC), this is a finding.

Remediation:

Configure Forescout to authenticate SNMP endpoint devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

1. Select Tools >> Options >> Switch.
2. Select a network device and review the "SNMP" tab.
3. Ensure the "SNMPv3" option is selected and the "HMAC-SHA" authentication protocol is selected.
4. Ensure the "use privacy" radio button is selected and "AES-128" or higher is selected from the drop-down box.

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)

1.33 FORE-NM-000370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-230963
RULE ID: SV-230963r1018756
```

Rationale:

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

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

Multifactor authentication (MFA) is required for all administrative and user accounts on network devices, except for an account of last resort and, where applicable, a root account. Passwords must only be used when MFA using PKI is not available, and for the account of last resort and root account.

Audit:

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Verify the first "password must contain at least" is checked.
3. Verify there is a minimum of one in the "upper case alphabetic characters" configuration box.

If the Forescout does not enforce password complexity by requiring that at least one uppercase character be used, this is a finding.

Remediation:

Configure Forescout to require a minimum of one uppercase character.

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Check the first "password must contain at least" option.
3. Add a 1 (or higher) in the "upper case alphabetic characters" configuration box.

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-000192 The information system enforces password complexity by the minimum number of upper case characters used.

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

1.34 FORE-NM-000380 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-230964
RULE ID: SV-230964r1018757
```

Rationale:

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

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

Multifactor authentication (MFA) is required for all administrative and user accounts on network devices, except for an account of last resort and (where applicable) a root account. Passwords should only be used when MFA using PKI is not available, and for the account of last resort and root account.

Audit:

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Verify the second "password must contain at least" is checked.
3. Verify there is a minimum of one in the "lower case alphabetic characters" configuration box.

If the Forescout does not enforce password complexity by requiring that at least one lowercase character be used, this is a finding.

Remediation:

Configure Forescout to require a minimum of one lowercase character.

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Check the second "password must contain at least" option.
3. Add a 1 (or higher) in the "lower case alphabetic characters" configuration box.

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-000193 The information system enforces password complexity by the minimum number of lower case characters used.

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

1.35 FORE-NM-000390 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Forescout must enforce a minimum 15-character password length.

```
GROUP ID: V-230965
RULE ID: SV-230965r1018758
```

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:

Determine if the network device enforces a minimum 15-character password length. This requirement may be verified by demonstration or configuration review.

1. Log on to the Forescout Administrator UI.
2. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
3. Verify the "minimum length" is configured for "15".

If Forescout does not enforce a minimum 15-character password length, this is a finding.

Remediation:

Log on to the Forescout Administrator UI.

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Configure the "minimum length" for "15".

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)

1.36 FORE-NM-000400 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-230966
RULE ID: SV-230966r1018759
```

Rationale:

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

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

Multifactor authentication (MFA) is required for all administrative and user accounts on network devices, except for an account of last resort and (where applicable) a root account. Passwords should only be used when MFA using PKI is not available, and for the account of last resort and root account.

Audit:

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Verify the third "password must contain at least" is checked.
3. Verify there is 1 (or higher) in the "digits" configuration box.

If the Forescout does not enforce password complexity by requiring that at least one numeric character be used, this is a finding.

Remediation:

Configure Forescout to require a minimum of one numeric character.

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Check the third "password must contain at least" option.
3. Add a 1 (or higher) in the "digits" configuration box.

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-000194 The information system enforces password complexity by the minimum number of numeric characters used.

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

1.37 FORE-NM-000410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-230967
RULE ID: SV-230967r1018760
```

Rationale:

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

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

Multifactor authentication (MFA) is required for all administrative and user accounts on network devices, except for an account of last resort and (where applicable) a root account. Passwords should only be used when MFA using PKI is not available, and for the account of last resort and root account.

Audit:

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Verify the fourth "password must contain at least" is checked.
3. Verify there is 1 (or higher) in the "in the special character" configuration box.

If the Forescout does not enforce password complexity by requiring that at least one special character be used, this is a finding.

Remediation:

Configure Forescout to require a minimum of one special character.

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Check the fourth "password must contain at least" option.
3. Add a 1 (or higher) in the "in the special character" configuration box.

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-001619 The information system enforces password complexity by the minimum number of special characters used.

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

1.38 FORE-NM-000420 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

Forescout must require that when a password is changed, the characters are changed in at least eight of the positions within the password.

```
GROUP ID: V-230968
RULE ID: SV-230968r1043189
```

Rationale:

If the application allows the user to consecutively reuse extensive portions of passwords, this increases the chances of password compromise by increasing the window of opportunity for attempts at guessing and brute-force attacks.

The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. In other words, characters may be the same within the two passwords; however, the positions of the like characters must be different.

Multifactor authentication (MFA) is required for all administrative and user accounts on network devices, except for an account of last resort and (where applicable) a root account. Passwords should only be used when MFA using PKI is not available, and for the account of last resort and root account.

Audit:

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Verify the fifth "password must contain at least" is checked.
3. Verify there is 1 (or higher) in the "repeated characters or digits" configuration box.

If Forescout does not enforce the requirement that when the password is changed, the characters are changed in at least eight of the positions within the password, this is a finding.

Remediation:

Configure Forescout to be required that when a password is changed, the characters are changed in at least eight of the positions within the password.

1. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
2. Check the fifth "password must contain at least" option.
3. Add a 1 (or higher) in the "repeated characters or digits" configuration box.

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-000195 The information system, for password-based authentication, when new passwords are created, enforces that at least an organization-defined number of characters are changed.

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

1.39 FORE-NM-000430 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Forescout must use FIPS 140-2 approved algorithms for authentication to a cryptographic module.

```
GROUP ID: V-230969
RULE ID: SV-230969r961050
```

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:

Log on using the CLIAdmin credentials established upon initial configuration.

Verify FIPS mode by typing the command "fstool version".

If Forescout does not use FIPS 140-2 approved algorithms for authentication to a cryptographic module, this is a finding.

Remediation:

To enable FIPS mode on the Forescout appliance, start by opening a secure shell to the CLI of the management appliance using Putty or another tool.

Log on using the CLIAdmin credentials established upon initial configuration.

To enable FIPS mode, type "fstool fips". At the prompt to alert the user FIPS 140-2 will be enabled, type "Yes" to accept.

Note: Use of FIPS mode is not mandatory in DoD. However, it is the primary method for mitigation of this requirement and ensuring FIPS compliance.

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

1.40 FORE-NM-000440 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Forescout 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-230970
RULE ID: SV-230970r961068
```

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.

Audit:

To verify the device is configured to terminate management sessions after 10 minutes of inactivity, verify the timeout value is configured.

1. Go to the Enterprise Manager Console.
2. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
3. Verify the "User Inactivity Timeout" check box is selected and the associated setting is set to "10 minutes".

If applicable, verify exceptions to this requirement are documented and signed.
If Forescout does not terminate the connection associated with an Enterprise Manager Console at the end of the session or after 10 minutes of inactivity, this is a finding.

Remediation:

Forescout is inherently designed to terminate upon exit or session disconnection, thus this part of the requirement does not have a fix.

To configure Forescout to terminate the connection after 10 minutes of inactivity perform the following steps.

1. Go to the Enterprise Manager Console.
2. From the menu, select Tools >> Options >> CounterACT User Profiles >> Password and Sessions.
3. Ensure the "User In-activity Timeout" check box is selected and the associated setting is set to "10 minutes".

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

1.41 FORE-NM-000450 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Forescout must only allow authorized administrators to view or change the device configuration, system files, and other files stored either in the device or on removable media (such as a flash drive).

```
GROUP ID: V-230971
RULE ID: SV-230971r961128
```

Rationale:

This requirement addresses the confidentiality and integrity of system information at rest (e.g., network device rule sets) when it is located on a storage device within the network device or as a component of the network device. This protection is required to prevent unauthorized alteration, corruption, or disclosure of information when not stored directly on the network device.

Files on the network device or on removable media used by the device must have their permissions set to allow read or write access to those accounts specifically authorized to access or change them. Note that different administrative accounts or roles will have varying levels of access.

File permissions must be set so that only authorized administrators can read or change their contents. Whenever files are written to removable media and the media removed from the device, the media must be handled appropriately for the classification and sensitivity of the data stored on the device.

Audit:

List the contents of Forescout’s local storage, including any drives supporting removable media (such as flash drives), and check the file permissions of all files on those drives.

1. Review accounts with incorrect update privileges to Forescout appliance configuration by selecting Tools >> Options >> CounterACT User Profiles.
2. Select a user to edit.
3. Select the "Permissions" tab.
4. Verify the "CounterAct Appliance Configuration" and "CounterACT Appliance Control" radio buttons are set to "View only".

If any files allow read or write access by accounts not specifically authorized access or access using non-privileged accounts, this is a finding.

Remediation:

Review the SSP or other documentation for a list of user accounts and privileges. Set the file permissions on files on Forescout or on removable media used by the device so that only authorized administrators can read or change their contents. This is completed by limiting access to SUDO accounts and command line admin accounts.

1. Review accounts with incorrect update privileges to Forescout appliance configuration by selecting Tools >> Options >> CounterACT User Profiles.
2. Select a user to edit.
3. Select the "Permissions" tab.
4. Ensure the "CounterACT Appliance Configuration" and "CounterACT Appliance Control" radio buttons are set to "View only".

Additional Information:

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

1.42 FORE-NM-000460 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

Forescout must be configured to send log data to a central log server for the purpose of forwarding alerts to the administrators and the Information System Security Officer (ISSO).

```
GROUP ID: V-230972
RULE ID: SV-230972r961863
```

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 be 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.

Audit:

Check the Forescout logs periodically to ensure proper auditing functions are still enabled and have not been changed. A proper security policy performs periodic checks to help ensure the proper information is being gathered in the event of a security breach, or internal/external threat.

If the Forescout auditing functions are disabled or have been changed, this is a finding.

Remediation:

Establish and document a procedure that periodically checks to ensure audit logs are in keeping with the security best practices of detailed security audit logs.

1. Log on to the Forescout UI.
2. Select Tools >> Options >> Modules >> Syslog >> Add.
3. Configure the:
4. Server Address
5. Server Port
6. Select Use TLS
7. Configure Identify, Facility, and Severity and then select OK >> Apply.

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	FORE-NM-000010 (Manual)	☐	☐
1.2	FORE-NM-000020 (Manual)	☐	☐
1.3	FORE-NM-000030 (Manual)	☐	☐
1.4	FORE-NM-000040 (Manual)	☐	☐
1.5	FORE-NM-000050 (Manual)	☐	☐
1.6	FORE-NM-000080 (Manual)	☐	☐
1.7	FORE-NM-000060 (Manual)	☐	☐
1.8	FORE-NM-000090 (Manual)	☐	☐
1.9	FORE-NM-000100 (Manual)	☐	☐
1.10	FORE-NM-000110 (Manual)	☐	☐
1.11	FORE-NM-000120 (Manual)	☐	☐
1.12	FORE-NM-000130 (Manual)	☐	☐
1.13	FORE-NM-000140 (Manual)	☐	☐
1.14	FORE-NM-000150 (Manual)	☐	☐
1.15	FORE-NM-000160 (Manual)	☐	☐
1.16	FORE-NM-000170 (Manual)	☐	☐
1.17	FORE-NM-000190 (Manual)	☐	☐
1.18	FORE-NM-000200 (Manual)	☐	☐
1.19	FORE-NM-000210 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	FORE-NM-000220 (Manual)	☐	☐
1.21	FORE-NM-000230 (Manual)	☐	☐
1.22	FORE-NM-000240 (Manual)	☐	☐
1.23	FORE-NM-000250 (Manual)	☐	☐
1.24	FORE-NM-000260 (Manual)	☐	☐
1.25	FORE-NM-000270 (Manual)	☐	☐
1.26	FORE-NM-000280 (Manual)	☐	☐
1.27	FORE-NM-000290 (Manual)	☐	☐
1.28	FORE-NM-000300 (Manual)	☐	☐
1.29	FORE-NM-000320 (Manual)	☐	☐
1.30	FORE-NM-000330 (Manual)	☐	☐
1.31	FORE-NM-000340 (Manual)	☐	☐
1.32	FORE-NM-000350 (Manual)	☐	☐
1.33	FORE-NM-000370 (Manual)	☐	☐
1.34	FORE-NM-000380 (Manual)	☐	☐
1.35	FORE-NM-000390 (Manual)	☐	☐
1.36	FORE-NM-000400 (Manual)	☐	☐
1.37	FORE-NM-000410 (Manual)	☐	☐
1.38	FORE-NM-000420 (Manual)	☐	☐
1.39	FORE-NM-000430 (Manual)	☐	☐
1.40	FORE-NM-000440 (Manual)	☐	☐
1.41	FORE-NM-000450 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	FORE-NM-000460 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 27, 2025	1.0.0	Initial CIS Release