CIS Tanium 7.x Application on TanOS STIG Benchmark

v1.0.0 - 08-26-2025

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

Tanium 7.x Application on TanOS Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 02 Apr 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Tanium 7.x Application on TanOS 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.

References

Additional documentation relative 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 Tanium 7.x Application on TanOS

Recommendations

1 STIG RULES

Tanium 7.x Application on TanOS

Tanium 7.x Application on TanOS Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 02 Apr 2025

CLASSIFICATION unclassified

1.1 TANS-AP-000005 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium max_soap_sessions_total setting must be explicitly enabled to limit the number of simultaneous sessions.

```
GROUP ID: V-254874
RULE ID: SV-254874r1067675
```

Rationale:

Application management includes the ability to control the number of users and user sessions that utilize an application. Limiting the number of allowed users and sessions per user is helpful in limiting risks related to DoS attacks.

This requirement may be met via the application or by utilizing information system, session control provided by a web server with specialized session management capabilities. If it has been specified that this requirement will be handled by the application, the capability to limit the maximum number of concurrent single user sessions must be designed and built in to the application.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based upon mission needs and the operational environment for each system.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. In the "Filter items " search box, type "max_soap_sessions_total".
6. Click "Enter".

If no results are returned, this is a finding.
If results are returned for "max_soap_sessions_total", but the value does not follow {(Number of Users) * 1024} formula, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. Click "Create Setting".
6. Select "Server" for "Setting Type".
7. In the "Create Platform Setting" dialog box, enter "max_soap_sessions_total" for "Name".
8. Select the "Numeric" radio button from "Value Type".
9. Use this formula for determining "Setting Value" {(Number of Users) * 1024 = max_soap_sessions_total}
10. Click "Save".
11. Add this setting to the system documentation for validation.

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 TANS-AP-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium max_soap_sessions_per_user setting must be explicitly enabled to limit the number of simultaneous sessions.

```
GROUP ID: V-254875
RULE ID: SV-254875r1067678
```

Rationale:

Application management includes the ability to control the number of users and user sessions that utilize an application. Limiting the number of allowed users and sessions per user is helpful in limiting risks related to DoS attacks.

This requirement may be met via the application or by utilizing information system session control provided by a web server with specialized session management capabilities. If it has been specified that this requirement will be handled by the application, the capability to limit the maximum number of concurrent single user sessions must be designed and built in to the application.

This requirement addresses concurrent sessions for information system accounts and does not address concurrent sessions by single users via multiple system accounts. The maximum number of concurrent sessions should be defined based upon mission needs and the operational environment for each system.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and logon with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. In the "Filter items" search box, type "max_soap_sessions_per_user".
6. Click "Enter".

If no results are returned, this is a finding.
If results are returned for "max_soap_sessions_per_user", but the value is not "1024", this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. Click "Create Setting".
6. Select "Server" for "Setting Type".
7. In the "Create Platform Setting" dialog box, enter "max_soap_sessions_per_user" for "Name".
8. Select the "Numeric" radio button from "Value Type".
9. Enter "1024" for the "Value:".
10. Click "Save".
11. Add this setting to the system documentation for validation.

Additional Information:

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

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

1.3 TANS-AP-000020 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Application Server console must be configured to initiate a session lock after a 15-minute period of inactivity.

```
GROUP ID: V-254876
RULE ID: SV-254876r1067681
```

Rationale:

The Tanium Console, when multifactor authentication is enabled, will initiate a session lock based upon the ActivClient or other Smart Card software.

By initiating the session lock, the console will be locked and not allow unauthorized access by anyone other than the original user.

Although this setting does not apply when multifactor authentication is enabled, it should be explicitly disabled in the event multifactor authentication is ever broken or removed.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. In the "Filter items" search box type "max_console_idle_seconds".
6. Click "Enter".

If no results are returned, this is a finding.
If results are returned for "max_console_idle_seconds", but the value is not between the range of "1 - 900", this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. Click "Create Setting".
6. Select "Server" box for "Setting Type".
7. In the "Create Platform Setting" dialog box enter "max_console_idle_seconds" for "Name".
8. Select the "Numeric" radio button from "Value Type".
9. Select "Value" and enter a value between the range of "1 - 900".
10. Click "Save".
11. Add this setting to the system documentation for validation.

Additional Information:

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

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

1.4 TANS-AP-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server must be set to only allow connections from endpoints when TLS is used.

```
GROUP ID: V-254877
RULE ID: SV-254877r1067684
```

Rationale:

Without cryptographic integrity protections in the Tanium Client, information could be altered by unauthorized users without detection.

Cryptographic mechanisms used for protecting the integrity of Tanium communications information include signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. In the "Filter Items" search box type "require_client_tls_315_flag".
6. Click "Enter".

If no results are returned, this is a finding.
If results are returned for "require_client_tls_315_flag" but the value is not "1", this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. Click "Create Setting".
6. Select "Server" box for "Setting Type."
7. In "Create Platform Setting" dialog box, enter "require_client_tls_315_flag" for "Name".
8. Select "Numeric" radio button for "Value Type".
9. Enter "1" for "Value".
10. Click "Save".

Additional Information:

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

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

1.5 TANS-AP-000045 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Trusted Content providers must be documented.

```
GROUP ID: V-254878
RULE ID: SV-254878r960762
```

Rationale:

A Tanium Sensor, also called content, enables an organization to gather real-time inventory, configuration, and compliance data elements from managed computers. Sensors gather specific information from the local device and then write the results to the computer's standard output channel. The Tanium Client captures that output and forwards the results through the platform's unique "ring" architecture for display in the Tanium Console.

The language used for Sensor development is based on the scripting engine available on the largest number of devices under management as well as the scripting experience and background of the people who will be responsible for creating new Sensors. VBScript and PowerShell are examples of common scripting languages used for developing sensors.

Because errors in scripting can and will provide errant feedback at best and will impact functionality of the endpoint to which the content is directed, it is imperative to ensure content is only accepted from trusted sources.

Audit:

Note: If only using Tanium-provided content and not accepting content from any other content providers, this is Not Applicable.

Consult with the Tanium System Administrator to review the documented list of trusted content providers along with the Hash for their respective public keys.

If the site does not have the Tanium trusted content providers documented along with the SHA-256 Hash for their respective public keys, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium trusted content providers along with the SHA-256 Hash from their respective public keys.

Additional Information:

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

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

1.6 TANS-AP-000050 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Content providers must provide their public key to the Tanium administrator to import for validating signed content.

```
GROUP ID: V-254879
RULE ID: SV-254879r960762
```

Rationale:

A Tanium Sensor, also called content, enables an organization to gather real-time inventory, configuration, and compliance data elements from managed computers. Sensors gather specific information from the local device and then write the results to the computer's standard output channel. The Tanium Client captures that output and forwards the results through the platform's unique "ring" architecture for display in the Tanium Console.

The language used for Sensor development is based on the scripting engine available on the largest number of devices under management as well as the scripting experience and background of the people who will be responsible for creating new Sensors. VBScript and PowerShell are examples of common scripting languages used for developing sensors.

Because errors in scripting can and will provide errant feedback at best and will impact functionality of the endpoint to which the content is directed, it is imperative to ensure content is only accepted from trusted sources.

Audit:

Note: If only using Tanium-provided content and not accepting content from any other content providers, this is Not Applicable.

Obtain documentation from the Tanium System Administrator that contains the public key validation data.

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "2" for "Tanium Operations Menu," and then press "Enter".
4. Press "5" for "Manage Custom Signing Keys," and then press "Enter".
5. Press "L" for "List Content Signing Keys," and then press "Enter".

If signing keys not listed in the provided documentation are present, this is a finding.

Remediation:

Note: If only using Tanium-provided content and not accepting content from any other content providers, this is Not Applicable.

Obtain documentation from the Tanium System Administrator that contains the public key validation data.

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "2" for "Tanium Operations Menu," and then press "Enter".
4. Press "5" for "Manage Custom Signing Keys," and then press "Enter".
5. Press "A" for "List Content Signing Keys," and then press "Enter".
6. Check the provided documentation and either update the document with the name and SHA-256 hash of the key or remove the key.

Additional Information:

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

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

1.7 TANS-AP-000055 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium public keys of content providers must be validated against documented trusted content providers.

```
GROUP ID: V-254880
RULE ID: SV-254880r960762
```

Rationale:

A Tanium Sensor, also called content, enables an organization to gather real-time inventory, configuration, and compliance data elements from managed computers. Sensors gather specific information from the local device and then write the results to the computer's standard output channel. The Tanium Client captures that output and forwards the results through the platform's unique "ring" architecture for display in the Tanium Console.

The language used for Sensor development is based on the scripting engine available on the largest number of devices under management as well as the scripting experience and background of the people who will be responsible for creating new Sensors. VBScript and PowerShell are examples of common scripting languages used for developing sensors.

Because errors in scripting can and will provide errant feedback at best and will impact functionality of the endpoint to which the content is directed, it is imperative to ensure content is only accepted from trusted sources.

Audit:

Note: If only using Tanium-provided content and not accepting content from any other content providers, this is Not Applicable.

Obtain documentation from the Tanium System Administrator that contains the public key validation data.

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "2" for "Tanium Operations Menu," and then press "Enter".
4. Press "5" for "Manage Custom Signing Keys," and then press "Enter".
5. Press "L" for "List Content Signing Keys," and then press "Enter".

If signing keys not listed in the provided documentation are present, this is a finding.

Remediation:

Note: If only using Tanium-provided content and not accepting content from any other content providers, this is Not Applicable.

Obtain documentation from the Tanium System Administrator that contains the public key validation data.

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "2" for "Tanium Operations Menu," and then press "Enter".
4. Press "5" for "Manage Custom Signing Keys," and then press "Enter".
5. Press "A" for "List Content Signing Keys," and then press "Enter".
6. Check the provided documentation and either update the document with the name and SHA-256 hash of the key or remove the key.

Additional Information:

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

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

1.8 TANS-AP-000065 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Application Server must be configured to only use LDAP for account management functions.

```
GROUP ID: V-254881
RULE ID: SV-254881r1043176
```

Rationale:

Enterprise environments make application account management challenging and complex. A manual process for account management functions adds the risk of a potential oversight or other error.

To reduce risk, the Tanium Application Server must be configured to allow for LDAP to provide account management functions that immediately enforce the organization's current account policy.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "LDAP/AD Sync Configurations".
4. Ensure LDAP sync is enabled.

If LDAP is not enabled, this is a finding.

Remediation:

Vendor documentation can be downloaded from the following URL: https://docs.tanium.com/platform_user/platform_user/console_using_ldap.html?Highlight=LDAP

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "LDAP/AD Sync Configurations".
4. Follow the vendor documentation titled "Integrating with LDAP Servers" to implement correct configuration settings for this requirement.

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

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

1.9 TANS-AP-000100 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Computer Groups must be used to restrict console users from affecting changes to unauthorized computers.

```
GROUP ID: V-254882
RULE ID: SV-254882r960792
```

Rationale:

Computer Groups allow a site running Tanium to assign responsibility of specific Computer Groups to specific Tanium console users. By doing so, a desktop administrator, for example, will not have the ability to enforce an action against a high visibility server.

For large sites, it is crucial to have the Computer Groups. While a smaller site might not seem to require Computer Groups, creating them provides for a cleaner implementation. All sites will be required to have some kind of Computer Groups configured other than the default "All Computers".

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Select the "Computer Groups" tab.
4. Under the "Name" column, verify organization-specific computer groups match the organization-defined list in the system security plan (SSP).

If site- or organization-specific computer groups do not match or exist, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Server, access the Tanium Server web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Select the "Computer Groups" tab.
4. Configure specific Computer Groups to facilitate the management of computers by authorized individuals for those computers.

Note: Tanium offers two ways to define computer groups. Refer to documentation for explanation found here: https://docs.tanium.com/platform_user/platform_user/console_computer_groups.html#Computer_Group_types.

Additional Information:

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

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

1.10 TANS-AP-000105 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Documentation identifying Tanium console users, their respective User Groups, Computer Groups, and Roles must be maintained.

```
GROUP ID: V-254883
RULE ID: SV-254883r960792
```

Rationale:

System access must be reviewed periodically to verify all Tanium users are assigned the appropriate functional role, with the least privileged access possible to perform assigned tasks being the recommended best practice to avoid unauthorized access.

Audit:

Consult with the Tanium System Administrator to review the documented list of Tanium users. User Groups, Roles, Computer Groups, and correlated LDAP security groups must be documented for users.

If the documentation does not exist, or is missing any Tanium users and their respective User Groups, Roles, Computer Groups, and correlated LDAP security groups documentation, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups.

Additional Information:

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

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

1.11 TANS-AP-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must be configured to use Tanium User Groups in a manner consistent with the model outlined within the environment's system documentation.

```
GROUP ID: V-254884
RULE ID: SV-254884r960792
```

Rationale:

It is important for information system owners to document authorized user groups for the Tanium application to avoid unauthorized access to systems. Misaligned implementation of user groups grants excessive access and results in potential compromise of "need-to-know" when it comes to information access.

Audit:

Consult with the Tanium System Administrator to review the documented list of Tanium User Groups.

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Permissions, select "User Groups".
4. Click each User Group and compare both the User Group name and the assigned Role(s) to the system documentation.

If any users have access to Tanium and their User Group is not on the list of documented User Groups with the appropriate Role(s), this is a finding.

Remediation:

Consult the documentation identifying the Tanium User Groups and their respective Role(s).

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Permissions, select "User Groups".
4. Click each User Group and add any missing Role(s).
5. For any missing User Groups, make the appropriate adjustments in LDAP.

Additional Information:

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

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

1.12 TANS-AP-000115 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Documentation identifying Tanium console users and their respective Computer Group rights must be maintained.

```
GROUP ID: V-254885
RULE ID: SV-254885r960792
```

Rationale:

System access must be reviewed periodically to verify all Tanium users are assigned the appropriate computer groups, with the least privileged access possible to perform assigned tasks. Users who have been removed from the documentation should no longer be configured as a Tanium Console User.

Audit:

Consult with the Tanium System Administrator to review the documented list of Tanium users and their respective, approved Computer Group rights.

If the documented list does not have the Tanium users and their respective approved Computer Group rights documented, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium console users and their respective Computer Group rights.

Additional Information:

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

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

1.13 TANS-AP-000120 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Action Approval feature must be enabled for two-person integrity when deploying actions to endpoints.

```
GROUP ID: V-254886
RULE ID: SV-254886r1067687
```

Rationale:

The Tanium Action Approval feature provides a two-person integrity control mechanism designed to achieve a high-level of security and reduce the possibility of error for critical operations.

When this feature is enabled, an action configured by one Tanium console user will require a second Tanium console user with a role of Action Approver (or higher) to approve the action before it is deployed to targeted computers.

While this system slows workflow, the reliability of actions deployed will be greater on the Packaging and Targeting.

Satisfies: SRG-APP-000033, SRG-APP-000488

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. In the "Filter items" search box type "require_action_approval".
6. Click "Enter".

If no results are returned, this is a finding.
If results are returned for "require_action_approval", but the value is not "1", this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. If "require_action_approval" does not exist, click "Create Setting".
6. Select "Server" for "Setting Type".
7. In the "Create Platform Setting" dialog box, enter "require_action_approval" for "Name".
8. Select "Numeric" radio button from "Value Type".
9. Select "Value" and enter "1".
10. Click "Save".

Additional Information:

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

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

CCI-002460 Enforce organization-defined actions prior to executing mobile code.

- NIST SP 800-53 Revision 4::SC-18 (4)
- NIST SP 800-53 Revision 5::SC-18 (4)

1.14 TANS-AP-000130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium documentation identifying recognized and trusted IOC streams must be maintained.

```
GROUP ID: V-254887
RULE ID: SV-254887r960804
```

Rationale:

Using trusted and recognized IOC sources may detect and prevent systems from becoming compromised. An IOC stream is a series or stream of IOCs that are imported from a vendor based on a subscription service. An IOC stream can be downloaded manually or on a scheduled basis. The items in an IOC stream can be separately manipulated after they are imported.

Audit:

Consult with the Tanium System Administrator to determine if the Threat Response module is being used. If not, this is Not Applicable.

Review the documented list of IOC trusted stream sources.

If the site does use an external source for IOCs and the IOC trusted stream source is not documented, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Threat Response trusted stream sources.

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

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

1.15 TANS-AP-000135 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Threat Response must be configured to receive IOC streams only from trusted sources.

```
GROUP ID: V-254888
RULE ID: SV-254888r960804
```

Rationale:

Using trusted and recognized IOC sources may detect and prevent systems from becoming compromised. An IOC stream is a series or stream of intel that is imported from a vendor based on a subscription service or manually downloaded and placed in a folder. Threat Response can be configured to retrieve the IOC content on a regularly scheduled basis. The items in an IOC stream can be separately manipulated after they are imported.

Audit:

Consult with the Tanium System Administrator to determine if the Threat Response module is being used, if not this is Not Applicable.

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Threat Response".
4. Expand the left menu.
5. Click "Intel".
6. Select "Sources".
7. Verify all configured Threat Response Streams are configured to a documented trusted source.

If Threat Response is configured to a stream that has not been documented as trusted, this is a finding.

Remediation:

Consult the documentation on trusted intel subscription feeds.

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Threat Response".
4. Expand the left menu.
5. Click "Intel".
6. Select "Sources".
7. Click "New Source".
8. Select the specified Source from the list.
9. Fill out the specified information based on the documented trusted intel feeds.
10. Select "Create".

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

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

1.16 TANS-AP-000140 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium documentation identifying recognized and trusted folders for Threat Response Local Directory Source must be maintained.

```
GROUP ID: V-254889
RULE ID: SV-254889r960804
```

Rationale:

Using trusted and recognized IOC sources may detect and prevent systems from becoming compromised. An IOC stream is a series or stream of IOCs that are imported from a vendor based on a subscription service or manually downloaded and placed in a folder. Threat Response can be configured to retrieve the IOC content on a regularly scheduled basis. The items in an IOC stream can be separately manipulated after they are imported.

Audit:

Consult with the Tanium System Administrator to review the documented list of folder maintainers for Threat Response Local Directory Source.

If the site does not leverage Local Directory Source to import IOCs, this finding is Not Applicable.

If the site does use Local Directory Source to import IOCs and the folder maintainers are not documented, this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium Threat Response Local Directory Source maintainers.

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

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

1.17 TANS-AP-000150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium documentation identifying recognized and trusted SCAP sources must be maintained.

```
GROUP ID: V-254891
RULE ID: SV-254891r960804
```

Rationale:

NIST validated SCAP XML documents are provided from several possible sources such as DISA, NIST, and the other nongovernment entities. These documents are used as the basis of compliance definitions leveraged to automate compliance auditing of systems. These documents are updated on different frequencies and must be manually downloaded on regular intervals and imported to be current. Nonapproved SCAP definitions lead to a false sense of security when evaluating an enterprise environment.

Audit:

Consult with the Tanium System Administrator to review the documented list of trusted SCAP sources.

If the site does not have the "Tanium Comply" module, or does not use Tanium Comply for compliance validation, this finding is Not Applicable.

If the site does use Tanium Comply and the source for SCAP content is not documented, this is a finding.

Remediation:

If the site does not have the Tanium Comply module, or does not use Tanium Comply for compliance validation, this finding is Not Applicable.

Prepare and maintain documentation identifying the source of SCAP sources that will be used by the Tanium Comply module.

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

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

1.18 TANS-AP-000155 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium documentation identifying recognized and trusted OVAL feeds must be maintained.

```
GROUP ID: V-254892
RULE ID: SV-254892r960804
```

Rationale:

OVAL XML documents are provided from several possible sources such as the CIS open source repository, or any number of vendor/third-party paid repositories. These documents are used to automate the passive validation of vulnerabilities on systems and therefore require a reasonable level of confidence in their origin. Nonapproved OVAL definitions lead to a false sense of security when evaluating an enterprise environment.

Audit:

Consult with the Tanium System Administrator to review the documented list of trusted OVAL feeds.

If the site does not have Tanium Comply module, or does not use Tanium Comply for passive vulnerability scanning, this finding is Not Applicable.

Otherwise, if the site does use Tanium Comply and the source for OVAL content is not documented, this is a finding.

Remediation:

If the site does not have Tanium Comply module, or does not use Tanium Comply for passive vulnerability scanning, this finding is Not Applicable.

Prepare and maintain documentation identifying the source of OVAL feeds that will be used by Tanium Comply module.

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

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

1.19 TANS-AP-000160 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Comply must be configured to receive SCAP content only from trusted sources.

```
GROUP ID: V-254893
RULE ID: SV-254893r960804
```

Rationale:

NIST-validated SCAP XML documents are provided from several possible sources such as DISA, NIST, and the other nongovernment entities. These documents are used as the basis of compliance definitions leveraged to automate compliance auditing of systems. These documents are updated on different frequencies and must be manually downloaded on regular intervals and imported to be current. Nonapproved SCAP definitions lead to a false sense of security when evaluating an enterprise environment.

Audit:

1. Using a web browser on a system, that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top banner of the console.
3. Click "Comply".
4. Click the menu on the left side of the interface and then click "Compliance" under "Standards".

Verify all imported compliance benchmarks are from a documented trusted source.
If any compliance benchmark is found that does not come from a documented trusted source, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top banner of the console.
3. Click "Comply".
4. Click the menu on the left side of the interface and then click "Compliance" under "Standards".
5. Delete any compliance benchmarks that come from nontrusted sources.

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

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

1.20 TANS-AP-000165 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Comply must be configured to receive OVAL feeds only from trusted sources.

```
GROUP ID: V-254894
RULE ID: SV-254894r960804
```

Rationale:

OVAL XML documents are provided from several possible sources such as the CIS open source repository, or any number of vendor/third party paid repositories. These documents are used to automate the passive validation of vulnerabilities on systems and therefore require a reasonable level of confidence in their origin. Nonapproved OVAL definitions lead to a false sense of security when evaluating an enterprise environment.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Comply".
4. Expand the left menu.
5. Under "Standards," click "Vulnerability".
6. Verify all imported vulnerability sources are from a documented trusted source.

If any vulnerability sources are found that do not come from a documented trusted source, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Comply".
4. Expand the left menu.
5. Under "Standards," click "Vulnerability".
6. Delete any vulnerability sources configured to nontrusted sources, or reconfigure to point to trusted sources.

Additional Information:

CCI-001414 Enforce approved authorizations for controlling the flow of information between connected systems based on organization-defined information flow control policies.

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

1.21 TANS-AP-000175 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The publicly accessible Tanium application must display the Standard Mandatory DOD Notice and Consent Banner before granting access to the application.

```
GROUP ID: V-254895
RULE ID: SV-254895r1067691
```

Rationale:

Display of a standardized and approved use notification before granting access to the publicly accessible 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 and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060. Use the following verbiage for desktops, laptops, and other devices accommodating banners of 1300 characters:

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

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

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

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

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

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

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

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

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Verify DOD use notification is displayed prior to login.

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions: The USG
routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations. At any time, the USG may
inspect and seize data stored on this IS. Communications using, or data
stored on, this IS are not private, are subject to routine monitoring,
interception, and search, and may be disclosed or used for any USG-authorized
purpose. This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

If a DOD-approved use notification banner does not display prior to logon, this is a finding.

Remediation:

For Tanium Server versions greater than or equal to 7.5.6.1108:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Configuration, select "Settings".
4. Click "Advanced Settings".
5. In the Filter Items box on the top right, search for "console_PreLoginBannerHTMLText" and select it.
6. In the "Value" field, enter the statement below:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions: The USG
routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations. At any time, the USG may
inspect and seize data stored on this IS. Communications using, or data
stored on, this IS are not private, are subject to routine monitoring,
interception, and search, and may be disclosed or used for any USG-authorized
purpose. This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

9. Click "Save".

Note: An html file can be uploaded in place of the above similar to previous versions of Tanium as shown below.
Tanium Server versions below 7.5.6.110:

1. Create an .html file composed of the DOD-authorized warning banner verbiage.

```
"<html>You are accessing a U.S. Government (USG) Information System (IS) that
is provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions: The USG
routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations. At any time, the USG may
inspect and seize data stored on this IS. Communications using, or data
stored on, this IS are not private, are subject to routine monitoring,
interception, and search, and may be disclosed or used for any USG-authorized
purpose. This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details.</html>"
```

2. Name the file "banner.html".
3. Use SFTP to upload the HTML banner file to the /incoming folder.
4. Log on to the TanOS server with the tanadmin user role.

5. Enter 2: Tanium Operations >> X: Advanced Operations >> 4: Manage HTML Banner and follow the prompts to copy the HTML banner file to the appropriate location.
6. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
7. Click "Administration" on the top navigation banner.
8. Under Configuration, select "Settings".
9. Select "Advanced Settings".
10. Search for "console_PreLoginBannerHTML".
11. Confirm "console_PreLoginBannerHTML" a value of "banner.html".

Note: If the above setting is not present, create it using the following steps.

1. Click "Add Setting".
2. Select "Server" for "Setting Type".
3. In "Create Platform Setting" dialog box, enter "console_PreLoginBannerHTML" for "Platform Setting Name".
4. Select "Text" radio button from "Value Type".
5. Enter "banner.html" for "Value:".
6. Click "Save".

Additional Information:

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

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

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

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

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

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

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

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

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

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

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

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

1.22 TANS-AP-000180 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The publicly accessible Tanium application must retain the Standard Mandatory DOD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.

```
GROUP ID: V-254896
RULE ID: SV-254896r1067694
```

Rationale:

Display of a standardized and approved use notification before granting access to the publicly accessible 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 and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060. Use the following verbiage for desktops, laptops, and other devices accommodating banners of 1300 characters:

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

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

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

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

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

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

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

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Verify DOD use notification is displayed prior to login.
3. "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

If a DOD-approved use notification banner does not display prior to logon, this is a finding.

Remediation:

For Tanium Server versions greater than or equal to 7.5.6.1108:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Configuration, select "Settings".
4. Click "Advanced Settings".
5. In the Filter Items box on the top right, search for "console_PreLoginBannerHTMLText" and select it.
6. In the "Value" field enter the statement below:

```
"You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions: The USG
routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations. At any time, the USG may
inspect and seize data stored on this IS. Communications using, or data
stored on, this IS are not private, are subject to routine monitoring,
interception, and search, and may be disclosed or used for any USG-authorized
purpose. This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details."
```

9. Click "Save".

Note: An html file can be uploaded in place of the above, similar to previous versions of Tanium as seen below.
Tanium Server versions below 7.5.6.1108:

1. Create an .html file composed of the DOD-authorized warning banner verbiage.

```
"<html>You are accessing a U.S. Government (USG) Information System (IS) that
is provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions: The USG
routinely intercepts and monitors communications on this IS for purposes
including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations. At any time, the USG may
inspect and seize data stored on this IS. Communications using, or data
stored on, this IS are not private, are subject to routine monitoring,
interception, and search, and may be disclosed or used for any USG-authorized
purpose. This IS includes security measures (e.g., authentication and access
controls) to protect USG interests--not for your personal benefit or privacy.
Notwithstanding the above, using this IS does not constitute consent to PM,
LE or CI investigative searching or monitoring of the content of privileged
communications, or work product, related to personal representation or
services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential. See User
Agreement for details.</html>"
```

2. Name the file "banner.html".
3. Use SFTP to upload the HTML banner file to the /incoming folder.
4. Log on to the TanOS server with the tanadmin user role.

5. Enter 2: Tanium Operations >> X: Advanced Operations >> 4: Manage HTML Banner and follow the prompts to copy the HTML banner file to the appropriate location.
6. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
7. Click "Administration" on the top navigation banner.
8. Under Configuration, select "Settings".
9. Select "Advanced Settings".
10. Search for "console_PreLoginBannerHTML".
11. Confirm "console_PreLoginBannerHTML" a value of "banner.html".

Note: If the above setting is not present, create it using the following steps.

1. Click "Add Setting".
2. Select "Server" for "Setting Type".
3. In "Create Platform Setting" dialog box, enter "console_PreLoginBannerHTML" for "Platform Setting Name".
4. Select "Text" radio button from "Value Type".
5. Enter "banner.html" for "Value:".
6. Click "Save".

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

1.23 TANS-AP-000195 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Multifactor authentication must be enabled and enforced on the Tanium Server for all access and all accounts.

```
GROUP ID: V-254897
RULE ID: SV-254897r1015861
```

Rationale:

To ensure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and any processes acting on behalf of users) must be uniquely identified and authenticated for all accesses, except the following.

(i) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and (ii) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Satisfies: SRG-APP-000080, SRG-APP-000148, SRG-APP-000149, SRG-APP-000150, SRG-APP-000151, SRG-APP-000152, SRG-APP-000156, SRG-APP-000391, SRG-APP-000392, SRG-APP-000402, SRG-APP-000403, SRG-APP-000005, SRG-APP-000004, SRG-APP-000002

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS console with the "tanadmin" user role.
3. Enter "2" to access the "Tanium Operations" menu.
4. Enter "2" to access the "Tanium Configuration" Settings menu.
5. Enter "1" to access the "Edit Tanium Server Settings" menu.
6. Validate the value for "ForceSOAPSSLClientCert" is set to "1".
7. Validate the following keys exist and are configured:

7A. "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name.

7B. "ClientCertificateAuthRegex"
For example:
.:\s(\d+)@.
Note: This regex may vary.
7C. "ClientCertificateAuth"
For example:
/opt/Tanium/TaniumServer/cac.pem
7D. "TrustedHostList"
For example:
Append 127.0.0.1 (for IPv4) and [::1] (for IPv6)
If the value for "ForceSOAPSSLClientCert" is not set to "1" and the remaining registry values are not configured, this is a finding.

Remediation:

Use the vendor documentation titled "Multi-Factor Authentication" to implement correct configuration settings for this requirement.

Vendor documentation can be downloaded from the following URL:
https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/smart_card_authentication.html#cac_Tanium_Appliance

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin user role.
3. Enter "2" to access the "Tanium Operations" menu.
4. Enter "2" to access the "Tanium Configuration" Settings menu.
5. Enter "1" to access the "Edit Tanium Server Settings" menu.
6. Validate the value for "ForceSOAPSSLClientCert" is set to "1".
7. Validate the following keys exist and are configured:

7A. "ClientCertificateAuthField"
For example:
X509v3 Subject Alternative Name.
7B. "ClientCertificateAuthRegex"
For example:
.:\s(\d+)@.
Note: This regex may vary.
7C. "ClientCertificateAuth"
For example:
/opt/Tanium/TaniumServer/cac.pem
Note: The path name is case sensitive.
7D. "TrustedHostList"
For example:
Append 127.0.0.1 (for IPv4) and [::1] (for IPv6).

Additional Information:

CCI-000056 Retain the device lock until the user reestablishes access using established identification and authentication procedures.

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

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

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

CCI-000060 Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

- NIST SP 800-53::AC-11 (1)
- NIST SP 800-53A::AC-11 (1).1
- NIST SP 800-53 Revision 4::AC-11 (1)
- NIST SP 800-53 Revision 5::AC-11 (1)

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

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

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

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

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

- NIST SP 800-53::IA-2 (1)

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

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

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

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

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

CCI-001953 Accept Personal Identity Verification-compliant credentials.

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

CCI-001954 Electronically verify Personal Identity Verification-compliant credentials.

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

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

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

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

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

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-000058 The information system provides the capability for users to directly initiate session lock mechanisms.

- NIST SP 800-53::AC-11 a
- NIST SP 800-53A::AC-11
- NIST SP 800-53 Revision 4::AC-11 a

CCI-000767 The information system implements multifactor authentication for local access to privileged accounts.

- NIST SP 800-53::IA-2 (3)
- NIST SP 800-53A::IA-2 (3).1
- NIST SP 800-53 Revision 4::IA-2 (3)

CCI-000768 The information system implements multifactor authentication for local access to non-privileged accounts.

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

1.24 TANS-AP-000260 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-254898
RULE ID: SV-254898r960912
```

Rationale:

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

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

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

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured Connections under "Connections" section.

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

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Expand the left menu.
5. Click "Connections".
6. Configure a Connection for the "Tanium Audit Source" source from the Tanium Application to a SIEM tool.

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

Additional Information:

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

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

1.25 TANS-AP-000270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must be configured to send audit records from multiple components within the system to a central location for review and analysis of audit records.

```
GROUP ID: V-254899
RULE ID: SV-254899r960918
```

Rationale:

Successful incident response and auditing relies on timely, accurate system information and analysis to allow the organization to identify and respond to potential incidents in a proficient manner. If the application does not provide the ability to centrally review the application logs, forensic analysis is negatively impacted.

Segregation of logging data to multiple disparate computer systems is counterproductive and makes log analysis and log event alarming difficult to implement and manage, particularly when the system or application has multiple logging components written to different locations or systems.

Automated mechanisms for centralized reviews and analyses include, for example, Security Information Management products.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured Connections under the "Connections" section.

If no Connection exists to send the "Tanium Audit Source" to a SIEM tool, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Click "Create Connection".
5. In the "Configuration" section under "Source," select "Tanium Audit Source" as the source from the drop-down menu.
6. In the "Configuration" section under "Destination," select the desired Destination and fill in the respective fields.
7. In the "Configure Output" section under "Format," select the desired file format type.
8. In the "Schedule" section, select the desired schedule.
9. Click "Create Connection".

Additional Information:

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

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

1.26 TANS-AP-000280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium applications must provide the capability to filter audit records for events of interest based upon organization-defined criteria.

```
GROUP ID: V-254900
RULE ID: SV-254900r960924
```

Rationale:

The ability to specify the event criteria of interest provides the persons reviewing the logs with the ability to quickly isolate and identify these events without having to review entries that are of little or no consequence to the investigation. Without this capability, forensic investigations are impeded.

Events of interest can be identified by the content of specific audit record fields including, for example, identities of individuals, event types, event locations, event times, event dates, system resources involved, IP addresses involved, or information objects accessed. Organizations may define audit event criteria to any degree of granularity required, for example, locations selectable by general networking location (e.g., by network or subnetwork) or selectable by specific information system component. This requires applications to provide the capability to customize audit record reports based on organization-defined criteria.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Expand the left menu.
5. Click "Connections".
6. Review the configured Connections.

If there are no configured connections, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Expand the left menu.
5. Click "Connections".
6. Click "Create Connection" or if importing, click "Import".
7. Give the "Connection" a name and description.
8. In the "Configuration" section, select "Event" as the source.
9. Select appropriate source under "Event Group". Any source to generate interest-based events (Discover, Asset, IM, THR, etc.).
10. Select the appropriate events to send.

Note: Consult with the Tanium System Administrator for the Destination.

11. Select "Listen for this Event".
12. Click "Save".

Additional Information:

CCI-000158 Provide the capability to process, sort, and search audit records for events of interest based on organization-defined audit fields within audit records.

- NIST SP 800-53::AU-7 (1)
- NIST SP 800-53A::AU-7 (1).1
- NIST SP 800-53 Revision 4::AU-7 (1)
- NIST SP 800-53 Revision 5::AU-7 (1)

1.27 TANS-AP-000295 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Access to Tanium logs on each endpoint must be restricted by permissions.

```
GROUP ID: V-254901
RULE ID: SV-254901r960933
```

Rationale:

For the Tanium Client software to run without impact from external negligent or malicious changes, the permissions on the Tanium log files and their directory must be restricted.

Tanium is deployed with a Client Hardening Solution. This solution, when applied, will ensure directory permissions are in place.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Actions, select "Scheduled Actions".
4. Look for a scheduled action titled "Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory".

If a scheduled action titled "Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory" does not exist, or there is a Scheduled Action contradicting the "Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory" scheduled action, this is a finding.
If the scheduled action exists, select it and if it is not approved (the "Approve" button at the top of the section will be displayed if not approved), this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Ask the question "Get Tanium Client Directory Permissions from all machines".

Tanium will parse the script and return a row for "Restricted" and a row for "Not Restricted", with their respective client counts.

3. Click the "Not Restricted" row.
4. Select "Deploy Action".

In the "Deploy Action" dialog box, the package "Client Service Hardening - Set SYSTEM only permissions on Tanium Client directory" will be selected.
The clients, which have their Tanium Client directory "Not Restricted" will be displayed in the bottom window.

5. Choose a schedule to deploy the hardening.
6. Under "Targeting Criteria," in the Action Group, select "All Computers" from the drop-down.
7. Click "Deploy Action".
8. Verify settings.
9. Click "Show Client Status Details".

Additional Information:

CCI-000163 Protect audit information from unauthorized modification.

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

1.28 TANS-AP-000305 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must prohibit user installation, modification, or deletion of software without explicit privileged status.

```
GROUP ID: V-254902
RULE ID: SV-254902r960939
```

Rationale:

Allowing regular users to install, modify, or delete software, without explicit privileges, creates the risk that the application performs in an inconsistent manner from its design. Explicit privileges (escalated or administrative privileges) provide the regular user with explicit capabilities and control that exceeds the rights of a regular user.

Application functionality will vary, and while users are not permitted to install unapproved applications, there may be instances where the organization allows the user to install approved software packages such as from an approved software repository.

The application must enforce software installation by users based upon what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect) by the organization.

Satisfies: SRG-APP-000121, SRG-APP-000122, SRG-APP-000123

Audit:

1. Consult with the Tanium System Administrator to review the documented list of Tanium users.
2. Review the users' respective approved roles, as well as the correlated LDAP security group for the User Roles.
3. Validate LDAP security groups/Tanium roles are documented to assign least privileged access to the functions of the Tanium Server through the Tanium interface.

If the documentation does not reflect a granular, least privileged access approach to the LDAP Groups/Tanium Roles assignment, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Permissions, select "Users".
4. Analyze the users configured in the Tanium interface.
5. Determine least privileged access required for each user to perform their respective duties.
6. Move users to the appropriate LDAP security group to ensure the user is synced to the appropriate Tanium User Role.
7. If the appropriate LDAP security groups are not already configured, create the groups and add the appropriate users.
8. Ensure LDAP sync repopulates the Tanium Users' associated Roles accordingly.

Additional Information:

CCI-001493 Protect audit tools from unauthorized access.

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

CCI-001494 Protect audit tools from unauthorized modification.

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

CCI-001495 Protect audit tools from unauthorized deletion.

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

1.29 TANS-AP-000330 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium cryptographic signing capabilities must be enabled on the Tanium Clients to safeguard the authenticity of communications sessions when answering requests from the Tanium Server.

```
GROUP ID: V-254903
RULE ID: SV-254903r1067697
```

Rationale:

All of Tanium's signing capabilities must be enabled upon install. Tanium supports the cryptographic signing and verification before execution of all Sensors, Questions, Actions, Sensor Libraries, File Shards, etc. Enabling signing does away with the ability of an attacker to conduct Man in the Middle (MitM) attacks for the purposes of remote code execution and precludes the modification of the aforementioned data elements in transit. Additionally, Tanium supports object level signing for content ingested into the Tanium platform. This allows for the detection and rejection of changes to objects (sensors, actions, etc.) by even a privileged user within Tanium.

Tanium has built-in signing capabilities enabled by default when installed. Cryptographic signing and verification of all Sensors, Questions, Actions, Sensor Libraries, File Shards, etc., before execution will be enforced by Tanium.

Signing will prevent MitM remote code execution attacks and will protect data element in transit. Tanium also supports object level signing for content within the Tanium platform.

Satisfies: SRG-APP-000131, SRG-APP-000219

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. In the "Filter Items" search box type "AllQuestionsRequireSignatureFlag".
6. Click "Enter".

If no results are returned, this is a finding.
If results are returned for "AllQuestionsRequireSignatureFlag" but the value is not "1", this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. Click "Create Setting".
6. Select "Client" for "Setting Type."
7. In the "Create Platform Setting" dialog box, enter "AllQuestionsRequireSignatureFlag" for "Name".
8. Select "Numeric" radio button for "Value Type".
9. Enter "1" for "Value".
10. Click "Save".

Additional Information:

CCI-001184 Protect the authenticity of communications sessions.

- NIST SP 800-53::SC-23
- NIST SP 800-53A::SC-23.1
- NIST SP 800-53 Revision 4::SC-23
- NIST SP 800-53 Revision 5::SC-23

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)

1.30 TANS-AP-000335 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium cryptographic signing capabilities must be enabled on the Tanium Server.

```
GROUP ID: V-254904
RULE ID: SV-254904r1067700
```

Rationale:

All of Tanium's signing capabilities must be enabled upon install. Tanium supports the cryptographic signing and verification before execution of all Sensors, Questions, Actions, Sensor Libraries, File Shards, etc. Enabling signing does away with the ability of an attacker to conduct man-in-the-middle (MITM) attacks for the purposes of remote code execution and precludes the modification of the aforementioned data elements in transit. Additionally, Tanium supports object-level signing for content ingested into the Tanium platform. This allows for the detection and rejection of changes to objects (sensors, actions, etc.) by even a privileged user within Tanium.

Tanium has built-in signing capabilities enabled by default when installed. Cryptographic signing and verification of all Sensors, Questions, Actions, Sensor Libraries, File Shards, etc., before execution will be enforced by Tanium.

Signing will prevent MITM remote code execution attacks and will protect data element in transit. Tanium also supports object-level signing for content within the Tanium platform.

Satisfies: SRG-APP-000131, SRG-APP-000233, SRG-APP-000317

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. In the "Filter Items" search box, enter "sign_all_questions_flag".
6. Click "Enter".

If no results are returned, this is a finding.
If results are returned for "sign_all_questions_flag" but the value is not "1", this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. Click "Create Setting".
6. Select "Server" for "Setting Type."
7. In "Create Platform Setting" dialog box, enter "sign_all_questions_flag" for "Name".
8. Select the "Numeric" radio button for "Value Type".
9. Enter "1" for "Value".
10. Click "Save".

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

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

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-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-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)

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

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

1.31 TANS-AP-000355 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Endpoints for Client-to-Server communications.

```
GROUP ID: V-254905
RULE ID: SV-254905r1043177
```

Rationale:

In addition to the client-to-server TCP communication that takes place over port 17472, Tanium Clients also communicate to other Tanium-managed computers over port 17472. Without proper firewall configurations, proper TCP communications may not take place as necessary for application functionality. The Tanium environment can perform hundreds or thousands of times faster than other security or systems management tools because the Tanium Clients communicate in secure, linearly-controlled peer-to-peer rings. Because clients dynamically communicate with other nearby agents based on proximity and latency, rings tend to form automatically to match a customer's topology—endpoints in California will form one ring while endpoints in Germany will form a separate ring.

Audit:

Note: This check is performed for the Tanium Endpoints and must be validated against the enterprise firewall solution (e.g., Endpoint Security Solution Firewall, Microsoft Windows Defender Firewall setting, Microsoft Advance Threat Protection Firewall, etc.) policies applied to the Endpoints.

1. Consult with the personnel who maintain the Enterprise Security Suite configuration for assistance.
2. Validate a rule exists within the firewall policies for managed clients for the following:

2A. Port Needed: Tanium Clients or Zone Clients over TCP port 17472, bi-directionally. If a host-based firewall rule does not exist to allow TCP port 17472, bi-directionally, this is a finding.

3. Consult with the boundary network firewall administrator and validate rules exist for the following:

3A. Allow TCP traffic on port 17472 from any computer to be managed on a local area network to any other computer to be managed on the same local area network.
If a network firewall rule does not exist to allow TCP port 17472 from any managed computer to any other managed computer on the same local area network, this is a finding.

Remediation:

1. Consult with the personnel who maintain the Enterprise Security Suite to configure host-based and network firewall rules to allow the following:

1A. Tanium Clients or Zone Clients over TCP port 17472, bi-directionally.

2. Consult with the boundary network firewall administrator to create a rule to allow the following:

2A. TCP traffic on port 17472 from any computer to be managed on a local area network to any other computer to be managed on the same local area network.

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 TANS-AP-000360 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Server for Client-to-Server communications.

```
GROUP ID: V-254906
RULE ID: SV-254906r1043177
```

Rationale:

In addition to the client-to-server TCP communication that takes place over port 17472, Tanium Clients also communicate to other Tanium-managed computers over port 17472. Without proper firewall configurations, proper TCP communications may not take place as necessary for application functionality. The Tanium environment can perform hundreds or thousands of times faster than other security or systems management tools because the Tanium Clients communicate in secure, linearly-controlled peer-to-peer rings. Because clients dynamically communicate with other nearby agents based on proximity and latency, rings tend to form automatically to match a customer's topology—endpoints in California will form one ring while endpoints in Germany will form a separate ring.

https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/network_ports.html

Audit:

Note: This check is performed for the Tanium Endpoints and must be validated against the enterprise firewall solution (e.g., Endpoint Security Solution Firewall, Microsoft Windows Defender Firewall setting, Microsoft Advance Threat Protection Firewall, etc.) policies applied to the Endpoints.

1. Consult with the personnel who maintain the Enterprise Security Suite configuration for assistance.
2. Validate a rule exists within the firewall policies for managed clients for the following:

2A. Port Needed: Tanium Clients or Zone Clients over TCP port 17472, bi-directionally. If a host-based firewall rule does not exist to allow TCP port 17472, bi-directionally, this is a finding.

3. Consult with the boundary network firewall administrator and validate rules exist for the following:

3A. Allow TCP traffic on port 17472 from any computer to be managed on a local area network to any other computer to be managed on the same local area network.
If a network firewall rule does not exist to allow TCP port 17472 from any managed computer to any other managed computer on the same local area network, this is a finding.

Remediation:

1. Consult with the personnel who maintain the Enterprise Security Suite to configure host-based and network firewall rules to allow the following:

1A. Tanium Clients or Zone Clients over TCP port 17472, bi-directionally.

2. Consult with the boundary network firewall administrator to create a rule to allow the following:

2A. TCP traffic on port 17472 from any computer to be managed on a local area network to any other computer to be managed on the same local area network.

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

1.33 TANS-AP-000365 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Zone Server for Client-to-Zone Server communications.

```
GROUP ID: V-254907
RULE ID: SV-254907r1043177
```

Rationale:

In customer environments using the Tanium Zone Server, a Tanium Client may be configured to point to a Zone Server instead of a Tanium Server. The communication requirements for these Clients are identical to the Server-to-Client requirements. Without proper firewall configurations, proper TCP communications may not take place as necessary for application functionality. Additionally, without proper configuration, organizations may lose complete visibility into endpoints that cannot connect directly to the Tanium Server.

https://docs.tanium.com/platform_deployment_reference/platform_deployment_reference/network_ports.html

Audit:

Note: If a Zone Server is not being used, this is Not Applicable.

1. Consult with the Tanium System Administrator to verify which firewall is being used as a host-based firewall on the Tanium Zone Server.
2. Access the host-based firewall configuration on the Tanium Zone Server.
3. Validate a rule exists for the following:

3A. Port Needed: Tanium Clients to Zone Server over TCP port 17472, bi-directionally.
If a host-based firewall rule does not exist to allow TCP port 17472, bi-directionally, from Tanium Clients to the Tanium Zone Server, this is a finding.

Remediation:

1. Consult with the personnel who maintain the Enterprise Security Suite to configure host-based and network firewall rules to allow the following:

1A. Tanium Clients or Zone Clients over TCP port 17472, bi-directionally.

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

1.34 TANS-AP-000370 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Application Server must be configured to prohibit or restrict the use of organization-defined functions, ports, protocols, and/or services, as defined in the PPSM CAL and vulnerability assessments.

```
GROUP ID: V-254908
RULE ID: SV-254908r1067702
```

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 or restrict unused or unnecessary physical and logical ports/protocols on information systems.

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

To support the requirements and principles of least functionality, the application must support the organizational requirements providing only essential capabilities and limiting the use of ports, protocols, and/or services to only those required, authorized, and approved to conduct official business or to address authorized quality of life issues.

Audit:

Review the PPSM CAL to ensure Tanium has been registered with all of the TCP ports required for functionality to include (but not limited to) TCP 17472, 17477, 17440, 17441, and 433.

If any TCP ports are being used on the Tanium Server that have been deemed as restricted by the PPSM CAL, this is a finding.

Remediation:

Submit a formal request to have the Tanium communication ports evaluated and added to the PPSM CAL.

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

1.35 TANS-AP-000415 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium endpoint must have the Tanium Servers public key in its installation.

```
GROUP ID: V-254909
RULE ID: SV-254909r960999
```

Rationale:

Without cryptographic integrity protections, information can be altered by unauthorized users without detection.

Remote access is access to DOD nonpublic information systems by an authorized user (or an information system) communicating through an external, nonorganization-controlled network. Remote access methods include, for example, dial-up, broadband, and wireless.

Cryptographic mechanisms used for protecting the integrity of information include, for example, signed hash functions using asymmetric cryptography enabling distribution of the public key to verify the hash information while maintaining the confidentiality of the secret key used to generate the hash.

Audit:

The Tanium endpoint makes a connection to the Tanium Server; the endpoint's copy of the Tanium Server's public key is used to verify the validity of the registration day coming from the Tanium Server.

If any endpoint systems do not have the correct Tanium Server public key in its configuration, they will not perform any instructions from the Tanium Server and a record of those endpoints will be listed in the Tanium Server's System Status.

To validate:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Select the "Client Status" tab.
4. Click "Administration".
5. Change "Show systems that have reported in the last:", enter "7" in the first field.
6. Select "Days" from the drop-down menu in the second field to determine if any endpoints connected with an invalid key.

If any systems are listed with "No" in the "Valid Key" column, this is a finding.

Remediation:

For systems which do not have a valid key for the Tanium Server, redeploy the client software using the Tanium Client Management (TCM) or work with the Tanium System Administrator to accomplish this.

Documentation on TCM: https://docs.tanium.com/client/client/index.html.

Additional Information:

CCI-000778 Uniquely identify organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection.

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

1.36 TANS-AP-000425 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must enforce a minimum 15-character password length.

```
GROUP ID: V-254910
RULE ID: SV-254910r1015864
```

Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

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:

Console Users:

Per guidance, Enterprise Console users are inherited via LDAP synchronization, as such passwords are not managed or enforced at the Tanium application level.

Local TanOS account:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu," and then press "Enter".
4. Press "L" for "Local Tanium User Management," and then press "Enter".
5. Press "B" for "Security Policy Local Authentication Service," and then press "Enter".

If the value of "Password Minimum Length:" is less than "15", this is a finding.

Remediation:

Console Users:

Per guidance, Enterprise Console users are inherited via LDAP synchronization, as such passwords are not managed or enforced at the Tanium application level.

Local TanOS account:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu," and then press "Enter".
4. Press "L" for "Local Tanium User Management," and then press "Enter".
5. Press "B" for "Security Policy Local Authentication Service," and then press "Enter".
6. Type "yes," and then press "Enter".
7. Input the following settings, pressing "Enter" after every value:
8. a) Minimum Password Lifetime - 1
9. b) Maximum Password Lifetime - 60
10. c) Minimum Password Length - 15
11. d) Minimum Password History - 5
12. e) Password Lockout - TRUE
13. f) Maximum Password Attempts - 3
14. Type "yes" to accept the new password policy.

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)

1.37 TANS-AP-000470 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-254912
RULE ID: SV-254912r1015865
```

Rationale:

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

Audit:

Console Users:

Per guidance, Enterprise Console users are inherited via LDAP synchronization as such passwords are not managed or enforced at the Tanium application level.

Local TanOS account:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu," and then press "Enter".
4. Press "L" for " Local Tanium User Management," and then press "Enter".
5. Press "B" for " Security Policy Local Authentication Service," and then press "Enter".

If the value of "Password Minimum Age (days):" is greater than "1", this is a finding.

Remediation:

Console Users:

Per guidance, Enterprise Console users are inherited via LDAP synchronization as such passwords are not managed or enforced at the Tanium application level.

Local TanOS account:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "C" for "User Administration Menu," and then press "Enter".
4. Press "L" for "Local Tanium User Management," and then press "Enter".
5. Press "B" for "Security Policy Local Authentication Service," and then press "Enter".
6. Type "yes" and press "Enter".
7. Input the following settings, pressing "Enter" after every value:
8. a) Minimum Password Lifetime - 1
9. b) Maximum Password Lifetime - 60
10. c) Minimum Password Length - 15
11. d) Minimum Password History - 5
12. e) Password Lockout - TRUE
13. f) Maximum Password Attempts - 3
14. Type "yes" to accept the new password policy.

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-000198 The information system enforces minimum password lifetime restrictions.

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

1.38 TANS-AP-000475 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must enforce a 60-day maximum password lifetime restriction.

```
GROUP ID: V-254913
RULE ID: SV-254913r1043190
```

Rationale:

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

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

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

Audit:

Console Users:

Per guidance, Enterprise Console users are inherited via LDAP synchronization as such passwords are not managed or enforced at the Tanium application level.

Local TanOS account:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Enter "C" for "User Administration Menu," and then press "Enter".
4. Enter "L" for " Local Tanium User Management," and then press "Enter".
5. Enter "B" for " Security Policy Local Authentication Service," and then press "Enter".

If the value of "Password Maximum Age (days):" is greater than "60", this is a finding.

Remediation:

Console Users:

Per guidance, Enterprise Console users are inherited via LDAP synchronization as such passwords are not managed or enforced at the Tanium application level.

Local TanOS account:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Enter "" for "User Administration Menu," and then press "Enter".
4. Enter "L" for "Local Tanium User Management," and then press "Enter".
5. Enter "B" for "Security Policy Local Authentication Service," and then press "Enter".
6. Type "yes," and then press "Enter".
7. Input the following settings, pressing "Enter" after every value:
8. a) Minimum Password Lifetime - 1
9. b) Maximum Password Lifetime - 60
10. c) Minimum Password Length - 15
11. d) Minimum Password History - 5
12. e) Password Lockout - TRUE
13. f) Maximum Password Attempts - 3
14. Type "yes" to accept the new password policy.

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-000199 The information system enforces maximum password lifetime restrictions.

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

1.39 TANS-AP-000480 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server certificates must have Extended Key Usage entries for the serverAuth object TLS Web Server Authentication and the clientAuth object TLS Web Client Authentication.

```
GROUP ID: V-254914
RULE ID: SV-254914r961038
```

Rationale:

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

Audit:

From Browser:

1. Navigate to the Tanium Console URI and log in using multi-factor authentication.
2. Click the lock to the left of the URI in the address bar.
3. Select the lock on the left of the URI in the address bar:
4. a) Chrome: Select "Certificate".
5. b) Edge: Select "Connection is Secure," and then select the certificate icon on the right.
6. Select the "Details" tab.
7. Scroll down through the details to find and select the "Enhanced Key Usage" field.

If there is no "Enhanced Key Usage" field, this is a finding.
In the bottom screen, verify "Server Authentication" and "Client Authentication" are both identified.
If "Server Authentication" and "Client Authentication" are not both identified, this is a finding.
From Server:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Press "2" for "Tanium Operations Menu," and then press "Enter".
4. Press "7" for "Download SOAP Certificate," and then press "Enter".

5. In a browser with access to the Tanium Server Console, navigate to https:///pub/SOAPServer.crt.
6. Download the SOAPServer.crt file when prompted.
7. Double-click on the file to open the certificate.
8. Select the "Details" tab.
9. Scroll down through the details to find and select the "Enhanced Key Usage" field.

If there is no "Enhanced Key Usage" field, this is a finding.
In the bottom screen, verify "Server Authentication" and "Client Authentication" are both identified.
If "Server Authentication" and "Client Authentication" are not both identified, this is a finding.

Remediation:

Request or regenerate the certificate being used to include both the "Server Authentication" and "Client Authentication" objects.

Additional Information:

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

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

1.40 TANS-AP-000490 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must be configured for LDAP user/group synchronization to map the authenticated identity to the individual user or group account for PKI-based authentication.

```
GROUP ID: V-254915
RULE ID: SV-254915r961044
```

Rationale:

Without mapping the certificate used to authenticate to the user account, the ability to determine the identity of the individual user or group will not be available for forensic analysis.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "LDAP/AD Sync Configurations".
4. Verify a sync exists under "Enabled Servers".

If no sync exists, this is a finding. If sync exists under "Disabled Servers" and there are no Enabled Servers, this is a finding."

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "LDAP/AD Sync Configurations".
4. Verify a sync exists under "Enabled Servers".
5. If no sync exists, click "Add Server".
6. Fill in the correct information for connecting to the organizations LDAP server. Work with a systems administrator to get this information if necessary.
7. Click "Save".
8. If a sync exists and it is disabled, click the edit icon.
9. Change the status to "enabled".
10. Click "Save".

Additional Information:

CCI-000187 For public key-based authentication, map the authenticated identity to the account of the individual or group.

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

1.41 TANS-AP-000505 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must uniquely identify and authenticate nonorganizational users (or processes acting on behalf of nonorganizational users).

```
GROUP ID: V-254916
RULE ID: SV-254916r961053
```

Rationale:

Lack of authentication and identification enables nonorganizational users to gain access to the application or possibly other information systems and provides an opportunity for intruders to compromise resources within the application or information system.

Nonorganizational users include all information system users other than organizational users, which include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors and guest researchers).

Nonorganizational users must be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization when related to the use of anonymous access, such as accessing a web server.

Audit:

Local users can be identified by the following:

1. Using a web browser on a system, which has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Permissions," select "Users".
4. Compare users listed to the prepared documentation.

If documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups does not exist this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups.

Additional Information:

CCI-000804 Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

- NIST SP 800-53::IA-8
- NIST SP 800-53A::IA-8.1
- NIST SP 800-53 Revision 4::IA-8
- NIST SP 800-53 Revision 5::IA-8

1.42 TANS-AP-000555 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must separate user functionality (including user interface services) from information system management functionality.

```
GROUP ID: V-254917
RULE ID: SV-254917r961095
```

Rationale:

Application management functionality includes functions necessary for administration and requires privileged user access. Allowing nonprivileged users to access application management functionality capabilities increases the risk that nonprivileged users may obtain elevated privileges.

The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, different TCP/UDP ports, virtualization techniques, combinations of these methods, or other methods, as appropriate.

An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different security domain and with additional access controls.

Audit:

Consult with the Tanium System Administrator to review the documented list of Tanium users. The users' User Groups, Roles, Computer Groups, and correlated LDAP security groups or Local Users must be documented.

Local users can be identified by the following:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Permissions," select "Users".
4. Compare users that do not have a Domain listed to the prepared documentation.

If documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups does not exist this is a finding.

Remediation:

Prepare and maintain documentation identifying the Tanium console users and their respective User Groups, Roles, Computer Groups, and associated LDAP security groups.

Additional Information:

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

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

1.43 TANS-AP-000600 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server and Client applications must have logging enabled.

```
GROUP ID: V-254918
RULE ID: SV-254918r961125
```

Rationale:

Failure to a known state can address safety or security in accordance with the mission/business needs of the organization. Failure to a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Preserving application state information helps to facilitate application restart and return to the operational mode of the organization with less disruption to mission-essential processes.

Audit:

Tanium Server:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "Common".
4. Select "Log Level".
5. In "Log Verbosity Level for Troubleshooting," verify current level for "Tanium Server" is set.

If the value for current level for "Tanium Server" is not set to "1" or higher this is a finding.
Tanium Client:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Interact".
4. In the "Explore Data" box, type the following question:

4A. Get Tanium Client Explicit Setting[LogVerbosityLevel] < 1 and Is Windows from all machines with Tanium Client Explicit Setting[LogVerbosityLevel] < 1

Note: For VDI systems, follow vendor guidance:
https://docs.tanium.com/client/client/os_imaging.html#VDI
If there are any answers returned that are "0" this is a finding.

Remediation:

Tanium Server:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "Common".
4. Select "Log Level".
5. In "Log Verbosity Level for Troubleshooting," verify current level for "Tanium Server" is set.

Tanium Client:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Interact".
4. In the "Explore Data" box, type the following question:
5. 4A. Get Tanium Client Explicit Setting[LogVerbosityLevel] < 1 and Is Windows from all machines with Tanium Client Explicit Setting[LogVerbosityLevel] < 1
6. Select the row with "Is windows" set to "True" and deploy the following action and settings:
7. a) Deployment Package: Modify Tanium Client Setting
8. b) RegType: REG_DWORD
9. c) ValueName: LogVerbosityLevel
10. d) ValueData: 1 or higher
11. Schedule Deployment
12. a) Distribute over: 1 hour
13. Click "Show Preview to continue".
14. Click "Deploy Action".
15. Select the row with "Is windows" set to "False" and deploy the following action and settings:
16. a) Deployment Package: Modify Tanium Client Setting [Non-Windows]
17. b) RegType: NUMERIC
18. c) ValueName: LogVerbosityLevel
19. d) ValueData: 1 or higher
20. Schedule Deployment
21. a) Distribute over: 1 hour
22. Click "Show Preview to continue".
23. Click "Deploy Action".

Additional Information:

CCI-001665 Preserve organization-defined system state information in the event of a system failure.

- NIST SP 800-53::SC-24
- NIST SP 800-53A::SC-24.1 (v)
- NIST SP 800-53 Revision 4::SC-24
- NIST SP 800-53 Revision 5::SC-24

1.44 TANS-AP-000630 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must restrict the ability of individuals to use information systems to launch organization-defined denial-of-service (DoS) attacks against other information systems.

```
GROUP ID: V-254919
RULE ID: SV-254919r1067705
```

Rationale:

The Tanium Action Approval feature provides a two-person integrity control mechanism designed to achieve a high-level of security and reduce the possibility of error for critical operations and DoS conditions.

When this feature is enabled, an action configured by one Tanium console user will require a second Tanium console user with a role of Action Approver (or higher) to approve the action before it is deployed to targeted computers.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. In the "Filter items" search box, type "require_action_approval".
6. Click "Enter".

If no results are returned, this is a finding.
If results are returned for "require_action_approval", but the value is not "1", this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. Click "Create Setting".
6. Select "Server" for "Setting Type".
7. In "Create Platform Setting" dialog box, enter "require_action_approval" does not exist: Flag" for " Name".
8. Select the "Numeric" radio button for "Value Type".
9. Enter "1" for "Value".
10. Click "Save".

Additional Information:

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

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

1.45 TANS-AP-000635 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must manage bandwidth throttles to limit the effects of information flooding types of Denial of Service (DoS) attacks.

```
GROUP ID: V-254920
RULE ID: SV-254920r961155
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

In the case of application DoS attacks, care must be taken when designing the application to ensure the application makes the best use of system resources. SQL queries have the potential to consume large amounts of CPU cycles if they are not tuned for optimal performance. Web services containing complex calculations requiring large amounts of time to complete can bog down if too many requests for the service are encountered within a short period of time.

The methods employed to meet this requirement will vary depending upon the technology the application utilizes. However, a variety of technologies exist to limit or, in some cases, eliminate the effects of application related DoS attacks. Employing increased capacity and bandwidth combined with specialized application layer protection devices and service redundancy may reduce the susceptibility to some DoS attacks.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "Bandwidth Throttles".
4. Work with the Tanium Administrator to confirm settings.
5. If bandwidth throttles are not configured, this is a finding. For more information, see the following: https://docs.tanium.com/platform_user/platform_user/console_bandwidth_throttling.html.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "Bandwidth Throttles".
4. Click "Add" on the line for "Global Throttle for All Data".
5. Work with Tanium Administrator to configure the required bandwidth throttles.
6. Click "Save".
7. Work with the Tanium Administrator to confirm or set settings for the remaining options:

7A. Global Throttle for Package Files.
7B. Global Throttle for Sensors.
7C. Site Throttles.

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

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

1.46 TANS-AP-000655 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must reveal error messages only to the ISSO, ISSM, and SA.

```
GROUP ID: V-254921
RULE ID: SV-254921r961170
```

Rationale:

Only authorized personnel should be aware of errors and the details of the errors. Error messages are an indicator of an organization's operational state or can identify the application. Additionally, Personally Identifiable Information (PII) and operational information must not be revealed through error messages to unauthorized personnel or their designated representatives.

The structure and content of error messages must be carefully considered by the organization and development team. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role.
3. Enter "C" for "User Administration Menu," and then press "Enter".
4. Enter "U" for "TanOS User Management," and then press "Enter".

If there are any users other than the documented approved TanOS users this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role, or any additional user with administrative privileges.
3. Enter "C" for "User Administration Menu," and then press "Enter".
4. Enter "U" for "TanOS User Management," and then press "Enter".
5. Work with Tanium System Administrator to either document approved accounts or remove nonapproved accounts.

Additional Information:

CCI-001314 Reveal error messages only to organization-defined personnel or roles.

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

1.47 TANS-AP-000700 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must notify system administrator (SA) and the information system security officer (ISSO) when accounts are created.

```
GROUP ID: V-254923
RULE ID: SV-254923r1067707
```

Rationale:

Once an attacker establishes initial access to a system, the attacker often attempts to create a persistent method of re-establishing access. One way to accomplish this is for the attacker to simply create a new account. Notification of account creation is one method for mitigating this risk. A comprehensive account management process will ensure an audit trail, which documents the creation of application user accounts and notifies administrators and ISSO exists. Such a process greatly reduces the risk that accounts will be surreptitiously created and provides logging that can be used for forensic purposes.

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

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured connections.

If no sources exist to send audit logs from Tanium to a SIEM tool or email destination, this is a finding.
Work with the SIEM administrator to determine if an alert is configured when accounts are created.
If there is no alert configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Click "Create Connection" in the "Connections" section.
5. Configure sources to send audit logs from the Tanium Server to a SIEM tool or email destination.
6. Work with email administrator to configure email destination.
7. Work with the SIEM administrator to configure an alert when accounts are created.

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

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

CCI-001683 The information system notifies organization-defined personnel or roles for account creation actions.

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

1.48 TANS-AP-000705 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must notify system administrators (SAs) and the information system security officer (ISSO) when accounts are modified.

```
GROUP ID: V-254924
RULE ID: SV-254924r1067709
```

Rationale:

When application accounts are modified, user accessibility is affected. Accounts are utilized for identifying individual users or for identifying the application processes themselves. Sending notification of account modification events to the SA and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured connections.

If no sources exist to send audit logs from the Tanium Database to a SIEM tool or email destination, this is a finding.
Work with the SIEM administrator to determine if an alert is configured when accounts are modified.
If there is no alert configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Click "Create Connection" in the "Connections" section.
5. Configure sources to send audit logs from the Tanium Server to a SIEM tool or email destination.
6. Work with email administrator to configure email destination.
7. Work with the SIEM administrator to configure an alert when accounts are modified.

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

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

CCI-001684 The information system notifies organization-defined personnel or roles for account modification actions.

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

1.49 TANS-AP-000710 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must notify system administrators (SAs) and the information system security officer (ISSO) for account disabling actions.

```
GROUP ID: V-254925
RULE ID: SV-254925r1067711
```

Rationale:

When application accounts are disabled, user accessibility is affected. Accounts are utilized for identifying individual users or for identifying the application processes themselves. Sending notification of account disabling events to the SA and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured connections.

If no sources exist to send audit logs from the Tanium SQL Server to a SIEM tool or email destination, this is a finding.
Work with the SIEM administrator to determine if an alert is configured when accounts are disabled.
If there is no alert configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Click "Create Connection" in the "Connections" section.
5. Configure sources to send audit logs from the Tanium Server to a SIEM tool or email destination.
6. Work with email administrator to configure email destination.
7. Work with the SIEM administrator to configure an alert when accounts are modified.

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

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

CCI-001685 The information system notifies organization-defined personnel or roles for account disabling actions.

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

1.50 TANS-AP-000715 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must notify system administrators (SAs) and the information system security officer (ISSO) for account removal actions.

```
GROUP ID: V-254926
RULE ID: SV-254926r1067713
```

Rationale:

When application accounts are removed, user accessibility is affected. Accounts are utilized for identifying users or for identifying the application processes themselves. Sending notification of account removal events to the SA and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To address access requirements, many operating systems can be integrated with enterprise-level authentication/access/auditing mechanisms that meet or exceed access control policy requirements.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured connections.

If no sources exist to send audit logs from the Tanium SQL Server to a SIEM tool or email destination, this is a finding.
Work with the SIEM administrator to determine if an alert is configured when accounts are deleted.
If there is no alert configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Configure sources to send audit logs from the Tanium Server to a SIEM tool or email destination.
5. Work with email administrator to configure email destination.
6. Work with the SIEM administrator to configure an alert when accounts are deleted.

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

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

CCI-001686 The information system notifies organization-defined personnel or roles for account removal actions.

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

1.51 TANS-AP-000720 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must set an inactive timeout for sessions.

```
GROUP ID: V-254927
RULE ID: SV-254927r1067716
```

Rationale:

Leaving sessions open indefinitely is a major security risk. An attacker can easily use an already authenticated session to access the hosted application as the previously authenticated user. By closing sessions after a set period of inactivity, the web server can make certain that sessions not closed through the user logging out of an application are eventually closed.

Acceptable values are 5 minutes for high-value applications, 10 minutes for medium-value applications, and 20 minutes for low-value applications.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. In "Filter Items" box, enter "max_console_idle_seconds".
6. Click "Enter".

If no results are returned, this is a finding.
If results are returned for "max_console_idle_seconds", but the value is not "900" or less, this is a finding.

Remediation:

In the event the "max_console_idle_seconds" setting exists, but is not "900" or less:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. In the "Filter Items" box, enter "max_console_idle_seconds".
6. Select the "max_console_idle_seconds" setting.
7. Enter "900" or less for "Value".
8. Click "Save".

In the event the "max_console_idle_seconds" setting does not exist:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Settings".
4. Click the "Advanced Settings" tab.
5. Click "Create Setting" in the top right.
6. Select "Server" for "Setting Type".
7. In "Create Platform Setting" dialog box, enter "max_console_idle_seconds" for "Name".
8. Select "Numeric" for the "Value Type".
9. Enter "900" or less for the "Value".
10. Click "Save".

Additional Information:

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

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

1.52 TANS-AP-000765 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Application Server must be configured with a connector to sync to Microsoft Active Directory for account management functions.

```
GROUP ID: V-254928
RULE ID: SV-254928r1015871
```

Rationale:

By restricting access to the Tanium Server to only Microsoft Active Directory, user accounts and related permissions can be strictly monitored. Account management will be under the operational responsibility of the System Administrator for the Windows Operation System Active Directory.

Satisfies: SRG-APP-000233, SRG-APP-000317, SRG-APP-000233

Audit:

Console Users:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "LDAP/AD Sync Configurations".
4. Verify a sync exists under "Enabled Servers".

If no sync exists, this is a finding.
If sync exists under "Disabled Servers" and there are no Enabled Servers, this is a finding.
Local TanOS Accounts:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role, or any additional user with administrative privileges.
3. Enter "C" for "User Administration Menu," and then press "Enter".
4. Enter "L" for "Local Tanium User Management," and then press "Enter".
5. Press "2" for "Manage Local User(s)," and then press "Enter".

If there are any users other than the documented approved local users this is a finding.

Remediation:

Console Users:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web UI and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "LDAP/AD Sync Configurations".
4. Click "Add Server".
5. Complete the settings using guidance from https://docs.tanium.com/platform_user/platform_user/console_using_ldap.html.
6. Click "Show Preview to Continue".
7. Review the users and groups to be imported.
8. Click "Save".

Local TanOS Accounts:

1. Access the Tanium Server interactively.
2. Log on to the TanOS server with the tanadmin role, or any additional user with administrative privileges.
3. Enter "C" for "User Administration Menu," and then press "Enter".
4. Enter "L" for "Local Tanium User Management," and then press "Enter".
5. Press "2" for "Manage Local User(s)," and then press "Enter".
6. Work with Tanium System Administrator to either document approved accounts or remove nonapproved accounts.

Additional Information:

CCI-001084 Isolate security functions from nonsecurity functions.

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

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)

1.53 TANS-AP-000780 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium must notify the system administrator (SA) and information system security officer (ISSO) of account enabling actions.

```
GROUP ID: V-254929
RULE ID: SV-254929r1067719
```

Rationale:

Once an attacker establishes access to an application, the attacker often attempts to create a persistent method of re-establishing access. One way to accomplish this is for the attacker to simply enable a new or disabled account. Sending notification of account enabling events to the SA and ISSO is one method for mitigating this risk. Such a capability greatly reduces the risk that application accessibility will be negatively affected for extended periods of time and also provides logging that can be used for forensic purposes.

To detect and respond to events that affect user accessibility and application processing, applications must notify the appropriate individuals so they can investigate the event.

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

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured sources.

If no sources exist to send audit logs from the Tanium Server to a SIEM tool or email destination, this is a finding.

1. Work with the SIEM administrator to determine if an alert is configured when account-enabling actions are performed.

If there is no alert configured, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web UI and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Configure sources to send audit logs from the Tanium Server to a SIEM tool or email destination.
5. Work with email administrator to configure email destination.
6. Work with the SIEM administrator to configure an alert when account-enabling actions are performed.

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

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

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

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

1.54 TANS-AP-000800 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Control of the Tanium Client service must be restricted to SYSTEM access only for all managed clients.

```
GROUP ID: V-254930
RULE ID: SV-254930r961317
```

Rationale:

The reliability of the Tanium client's ability to operate depends upon controlling access to the Tanium client service. By restricting access to SYSTEM access only, the non-Tanium system administrator will not have the ability to impact operability of the service.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Actions, select "Scheduled Actions".
4. Look for a scheduled action titled "Client Service Hardening - Allow Only Local SYSTEM to Control Service".

If a scheduled action titled "Client Service Hardening - Allow Only Local SYSTEM to Control Service" does not exist, this is a finding.

5. If the scheduled action exists, select it and if it is not approved (the "Approve" button at the top of the section will be displayed if not approved), this is a finding.

If the scheduled action exists and has been approved but does not restrict control of the Tanium Client service to "Allow Only Local SYSTEM to Control Service," this is a finding.
If the action is not configured to repeat at least every hour, this is a finding.
If the scheduled action is not targeted at an "All Computers" Action Group, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Interact".
4. In "Categories" section, select "Client Service Hardening".
5. In "Dashboards" section, select "Control Service State Permissions".
6. The results will show a "Count" of clients matching the "Service Control is set to default permissions" query.
7. Select the result line for "Service Control is set to default permissions".
8. Choose "Deploy Action".
9. Deployment Package drop-down select "Client Service Hardening - Allow Only Local SYSTEM to Control Service".
10. Configure the schedule to repeat at least every hour for the requested action.
11. Under "Targeting Criteria" in the Action Group, select "All Computers" from the drop-down.
12. Click "Show preview to continue".
13. Noncompliant systems will be displayed at the bottom.
14. Click "Deploy Action".
15. Verify settings.
16. Click "Show Client Status Details".

Additional Information:

CCI-002165 Enforce organization-defined discretionary access control policies over defined subjects and objects.

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

1.55 TANS-AP-000805 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The ability to uninstall the Tanium Client service must be disabled on all managed clients.

```
GROUP ID: V-254931
RULE ID: SV-254931r961317
```

Rationale:

By default, end users have the ability to uninstall software on their clients. In the event the Tanium Client software is uninstalled, the Tanium Server is unable to manage the client and must redeploy to the client. Preventing the software from being displayed in the client's Add/Remove Programs will lessen the risk of the software being uninstalled by non-Tanium System Administrators.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Actions, select "Scheduled Actions".
4. Look for a scheduled action titled "Client Service Hardening - Hide Client from Add-Remove Programs".
5. If a scheduled action titled "Client Service Hardening - Hide Client from Add-Remove Programs" does not exist, this is a finding.

If the scheduled action exists, select it and if it is not approved (the "Approve" button at the top of the section will be displayed if not approved), this is a finding.
If the scheduled action exists and has been approved but does not disable the visibility of the client in Add-Remove Programs, this is a finding.
If the action is not configured to repeat at least every hour, this is a finding.
If the scheduled action is not targeted at an "All Computers" Action Group, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Interact".
4. In the "Categories" section, select "Client Service Hardening".
5. In "Dashboard" section, select "Hide From Add-Remove Program".
6. The results will show a "Count" of clients matching the "Tanium Client Visible in Add-Remove Programs" query.
7. Select the result line.
8. Choose "Deploy Action".
9. The "Deploy Action" dialog box will display "Client Service Hardening - Hide Client from Add-Remove Programs" as the package. The computer names comprising the "count" of noncompliant systems will be displayed in the bottom.
10. Deployment Package drop-down select "Client Service Hardening - Hide Client from Add-Remove Programs".
11. Configure the schedule to repeat at least every hour for the requested action.
12. Under "Targeting Criteria", in the "Action Group," select "All Computers" from the drop-down.
13. Click "Show preview to continue". Noncompliant systems will be displayed in the bottom.
14. Click "Deploy Action".
15. Verify settings.
16. Click "Show Client Status Details".

Additional Information:

CCI-002165 Enforce organization-defined discretionary access control policies over defined subjects and objects.

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

1.56 TANS-AP-000810 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The permissions on the Tanium Client directory must be restricted to only the SYSTEM account on all managed clients.

```
GROUP ID: V-254932
RULE ID: SV-254932r961317
```

Rationale:

By restricting access to the Tanium Client directory on managed clients, the Tanium client's ability to operate and function as designed will be protected from malicious attack and unintentional modifications by end users.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Actions, select "Scheduled Actions".
4. Look for a scheduled action titled "Client Service Hardening - Set SYSTEM only permissions on the Tanium Client directory".

If a scheduled action titled "Client Service Hardening - Set SYSTEM only permissions on the Tanium Client directory" does not exist, this is a finding.
If the scheduled action exists, select it and if it is not approved (the "Approve" button at the top of the section will be displayed if not approved), this is a finding.
If the scheduled action exists and has been approved but does not disable the visibility of the client in Add-Remove Programs, this is a finding.
If the action is not configured to repeat at least every hour, this is a finding.
If the scheduled action is not targeted at an "All Computers" Action Group, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Interact".
4. In the "Categories" section, select "Client Service Hardening".
5. In the "Dashboard" section, select "Set Client Directory Permissions".

The results will show a "Count" of clients' compliant and noncompliant hardening for the "Tanium Client Directory Permissions".
Noncompliant clients will have a count other than "0" for "Not Restricted" or "Error: No Permissions".

6. Select each of the "Not Restricted" or "Error: No Permissions." Statuses.
7. Select "Deploy Action".
8. In the "Deploy Action" dialog box, change the package to "Client Service Hardening - Set SYSTEM only permissions on the Tanium Client directory" as the package.
9. Configure the schedule to repeat at least every hour for the requested action.
10. Under "Targeting Criteria", in the Action Group, select "All Computers" from the drop-down.
11. Click "Show preview to continue". Noncompliant systems will be displayed in the bottom.
12. Click "Deploy Action".
13. Verify settings.
14. Click "Show Client Status Details".

Additional Information:

CCI-002165 Enforce organization-defined discretionary access control policies over defined subjects and objects.

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

1.57 TANS-AP-000860 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must allocate audit record storage capacity in accordance with organization-defined audit record storage requirements.

```
GROUP ID: V-254933
RULE ID: SV-254933r1067722
```

Rationale:

To ensure applications have a sufficient storage capacity in which to write the audit logs, applications need to be able to allocate audit record storage capacity.

The task of allocating audit record storage capacity is usually performed during initial installation of the application and is closely associated with the DBA and system administrator roles. The DBA or system administrator will usually coordinate the allocation of physical drive space with the application owner/installer and the application will prompt the installer to provide the capacity information, the physical location of the disk, or both.

Audit:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "1" for "Check current status," and then press "Enter".

If the syslog status page states "No existing TanOS syslog forwarding configuration found" this is a finding.
If the syslog status page states "Syslog forwarding configuration" and the SIEM administrator verifies SIEM is receiving the events correctly and generating notifications for low free disk space, this is not a finding.

Remediation:

1. Access the TanOS interactively.
2. Press "A" for "Appliance Configuration Menu," and then press "Enter".
3. Press "4" for "Syslog Configuration," and then press "Enter".
4. Press "5" for "Configure syslog forwarding," and then press "Enter".
5. Enter the destination host (IP address or hostname) provided by the SIEM administrator, and then press "Enter".
6. Enter the destination port number and press "Enter".
7. If TLS is required for this syslog destination, enter "Yes", otherwise enter "No", and press "Enter".
8. Enter the destination protocol, "udp" or "tcp", and press "Enter".
9. Work with the SIEM administrator to validate events are being received, and to configure notifications for low free disk space.

Additional Information:

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

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

1.58 TANS-AP-000865 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must offload audit records onto a different system or media than the system being audited.

```
GROUP ID: V-254934
RULE ID: SV-254934r961395
```

Rationale:

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

Offloading is a common process in information systems with limited audit storage capacity.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on using multi-factor authentication.
2. Click "Modules" on the top of the banner of the console.
3. Click "Connect".
4. Review the configured connections under "Connections" section.

If no connection exists to send the "Tanium Audit Source" to a SIEM tool, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on using multi-factor authentication.
2. Click "Modules" on the top of the console.
3. Click "Connect".
4. Click "Create Connection".
5. In the "Configuration" section under "Source", select "Tanium Audit Source" as the source from the drop-down menu.
6. In the "Configuration" section under "Destination", select the desired destination and fill in the respective fields.
7. In the "Configure Output" section under "Format", select the desired file format type.
8. In the "Schedule" section, select the desired schedule.
9. Click "Save".

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)

1.59 TANS-AP-000870 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must provide an immediate warning to the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75 percent of repository maximum audit record storage capacity.

```
GROUP ID: V-254935
RULE ID: SV-254935r961398
```

Rationale:

If security personnel are not notified immediately upon storage volume utilization reaching 75 percent, they are unable to plan for storage capacity expansion.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the TanOS console as the user "tanadmin".
3. Enter "3" to access the "Tanium Support" menu.
4. Enter "6" to display last scheduled health check results.

If none exists, then this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the TanOS console as the user "tanadmin".
3. Enter "3" to access the "Tanium Support" menu.
4. Enter "5" to Run a Health Check.

Additional Information:

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

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

1.60 TANS-AP-000875 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must provide an immediate real-time alert to the system administrator (SA) and information system security officer (ISSO), at a minimum, of all audit failure events requiring real-time alerts.

```
GROUP ID: V-254936
RULE ID: SV-254936r1067725
```

Rationale:

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

Alerts provide organizations with urgent messages. Real-time alerts provide these messages immediately (i.e., the time from event detection to alert occurs in seconds or less).

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Review the configured Tanium Sources listed.

If an "Audit Log" source does not exist, this is a finding.

5. Select the "Audit Log" source.
6. Select the audit connection found in the lower half of the screen.
7. Verify the "Destination Type" is a SIEM tool.

If the "Destination Type" is not a SIEM tool, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Connect".
4. Configure sources to send audit logs from the Tanium Server to a SIEM tool or email destination.
5. Work with email administrator to configure email destination.
6. Work with the SIEM administrator to configure alerts based on audit failures.

Consult documentation located at https://docs.tanium.com/connect/connect/siem.html#siem for reference on configuring other applicable SIEM connections.

Additional Information:

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

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

1.61 TANS-AP-000940 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must prohibit user installation of software without explicit privileged status.

```
GROUP ID: V-254938
RULE ID: SV-254938r1015873
```

Rationale:

Allowing regular users to install software without explicit privileges creates the risk that untested or potentially malicious software will be installed on the system. Explicit privileges (escalated or administrative privileges) provide the regular user with explicit capabilities and control that exceeds the rights of a regular user.

Application functionality will vary, and while users are not permitted to install unapproved applications, there may be instances where the organization allows the user to install approved software packages such as from an approved software repository.

The application must enforce software installation by users based upon what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect) by the organization.

This requirement applies, for example, to applications that provide the ability to extend application functionality (e.g., plug-ins, add-ons) and software management applications.

Audit:

Consult with the Tanium System Administrator to review the documented list of Tanium users.

1. Review the users' respective approved roles, as well as the correlated LDAP security group for the User Roles.
2. Validate LDAP security groups/Tanium roles are documented to assign least privileged access to the functions of the Tanium Server through the Tanium interface.

If the documentation does not reflect a granular, least privileged access approach to the LDAP Groups/Tanium Roles assignment, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multifactor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Permissions, select "Users".
4. Analyze the users configured in the Tanium interface.
5. Determine least privileged access required for each user to perform their respective duties.
6. Move users to the appropriate LDAP security group to ensure the user is synced to the appropriate Tanium User Role.
7. If the appropriate LDAP security groups are not already configured, create the groups and add the appropriate users.
8. Ensure LDAP sync repopulates the Tanium users' associated roles accordingly.

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)

1.62 TANS-AP-000950 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must enforce access restrictions associated with changes to application configuration.

```
GROUP ID: V-254939
RULE ID: SV-254939r961461
```

Rationale:

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

When dealing with access restrictions pertaining to change control, it should be noted that any changes to the hardware, software, and/or firmware components of the information system and/or application can potentially have significant effects on the overall security of the system.

Accordingly, only qualified and authorized individuals should be allowed to obtain access to application components for the purposes of initiating changes, including upgrades and modifications.

Logical access restrictions include, for example, controls that restrict access to workflow automation, media libraries, abstract layers (e.g., changes implemented into third-party interfaces rather than directly into information systems), and change windows (e.g., changes occur only during specified times, making unauthorized changes easy to discover).

Audit:

Consult with the Tanium System Administrator to review the documented list of Tanium Administrators.

1. Review the administrators' respective approved roles, as the correlated LDAP security group for the User Roles.

If the documentation does not reflect a granular, least privileged access approach to the LDAP Groups/Tanium Roles assignment, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Permissions", select "Users".
4. Analyze the users configured in the Tanium interface.
5. Determine least privileged access required for each user to perform their respective duties.
6. Move users to the appropriate LDAP security group to ensure the user is synced to the appropriate Tanium User Role.
7. If the appropriate LDAP security groups are not already configured, create the groups and add the appropriate users.
8. Ensure LDAP sync repopulates the Tanium Users' associated Roles accordingly.

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)

1.63 TANS-AP-000975 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium module server to allow Server-to-Module Server communications from the Tanium Server.

```
GROUP ID: V-254942
RULE ID: SV-254942r1067730
```

Rationale:

The Tanium Module Server is used to extend the functionality of Tanium through the use of various workbenches. The Tanium Module Server requires communication with the Tanium Server on port 17477. Without a proper connection from the Tanium Server to the Tanium Module Server, access to the system capabilities could be denied.

https://docs.tanium.com/platform_install/platform_install/reference_network_ports.html.

Audit:

Consult with the network firewall administrator and validate rules exist for the following:

- Allow TCP traffic on port 17477 from the Tanium Server to the Tanium Module Server.

If a network firewall rule does not exist to allow TCP traffic on port 17477 from the Tanium Server to the Tanium Module Server, this is a finding.

Remediation:

Configure the network firewall to allow TCP traffic on port 17477 from the Tanium Server to the Tanium Module Server.

Additional Information:

CCI-001762 Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.64 TANS-AP-000980 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Server for Server-to-Module Server communications.

```
GROUP ID: V-254943
RULE ID: SV-254943r1067733
```

Rationale:

The Tanium Module Server is used to extend the functionality of Tanium through the use of various workbenches. The Tanium Module Server requires communication with the Tanium Server on port 17477. Without a proper connection from the Tanium Server to the Tanium Module Server, access to the system capabilities could be denied.

https://docs.tanium.com/platform_install/platform_install/reference_network_ports.html.

Audit:

Consult with the network firewall administrator and validate rules exist for the following:

- Allow TCP traffic on port 17477 from the Tanium Module Server to the Tanium Server.

If a network firewall rule does not exist to allow TCP traffic on port 17477 from the Tanium Module Server to the Tanium Server, this is a finding.

Remediation:

Configure the network firewall to allow TCP traffic on port 17477 from the Tanium Module Server to the Tanium Server.

Additional Information:

CCI-001762 Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.65 TANS-AP-000985 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Firewall rules must be configured on the Tanium Server for Server-to-Zone Server communications.

```
GROUP ID: V-254944
RULE ID: SV-254944r961470
```

Rationale:

If using the Tanium Zone Server to proxy traffic from Tanium-managed computers on less trusted network segments to the Tanium Server on the core network, then the Tanium Zone Server Hub, typically installed to the Tanium Server device must be able to connect to the Zone Server(s) in the DMZ. This is the only configuration that requires outbound traffic to be allowed on port 17472 from the Tanium Server device. The ZoneServerList.txt configuration file located in the Tanium Zone Server Hub's installation folder identifies the addresses of the destination Zone Servers. See the Zone Server Configuration page for more details.

Port Needed: Tanium Server to Zone Server over TCP port 17472.

Network firewall rules:

Allow TCP traffic on port 17472 from the Zone Server Hub, usually the Tanium Server device, to the destination DMZ devices(s) hosting the Zone Server(s).

Endpoint firewall rules—for additional security, configure the following endpoint firewall rules:

Allow TCP traffic outbound on port 17472 from only the Zone Server Hub process running on the Tanium Server device.

Allow TCP traffic inbound on port 17472 to only the Zone Server process running on the designated Zone Server device(s).

https://docs.tanium.com/platform_install/platform_install/reference_network_ports.html.

Audit:

Note: If a Zone Server is not being used, this is Not Applicable.

Consult with the Tanium System Administrator to verify which firewall is being used as a host-based firewall on the Tanium Server.

1. Access the Tanium Server interactively.
2. Log on to the server with an account that has administrative privileges.

3. Access the host-based firewall configuration on the Tanium Server.
4. Validate a rule exists for the following:

4A. Port Needed: Tanium Server to Zone Server over TCP port 17472.
Note: By default, the Zone Server uses 17472 for traffic from Zone Server Hubs and Tanium Clients. However, as a best practice to improve the security of the Zone Server, different ports can be configured for the hubs and clients.
If a host-based firewall rule does not exist to allow TCP port 17472 or other defined port, bidirectionally, from Tanium Server to the Tanium Zone Server, this is a finding.

Remediation:

1. Configure host-based firewall rules on the Tanium Zone server to include the following required traffic:

1A. Allow Tanium Server to Zone Server over TCP port 17472.

2. Configure the network firewall to allow the above traffic.

Note: By default, the Zone Server uses 17472 for traffic from Zone Server Hubs and Tanium Clients. However, as a best practice to improve the security of the Zone Server, different ports can be configured for the hubs and clients.

Additional Information:

CCI-001762 Disable or remove organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure.

- NIST SP 800-53 Revision 4::CM-7 (1) (b)
- NIST SP 800-53 Revision 5::CM-7 (1) (b)

1.66 TANS-AP-001090 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SSLHonorCipherOrder must be configured to disable weak encryption algorithms on the Tanium Server.

```
GROUP ID: V-254945
RULE ID: SV-254945r962034
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The application must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the server with the tanadmin role.
3. Enter 2: Tanium Operations >> 2: Tanium Configuration Settings >> 1: Edit Tanium Server Settings.
4. Verify the existence of a "SSLHonorCipherOrder" key with a value of "1".

If the "SSLHonorCipherOrder" key does not exist with a value of "1", this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the server with the tanadmin role.
3. Enter 2: Tanium Operations >> 2: Tanium Configuration Settings >> 1: Edit Tanium Server Settings.
4. Enter number associated with key "SSLHonorCipherOrder" to edit its value.
5. Add or modify the "SSLHonorCipherOrder" key to have a value of "1".

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

1.67 TANS-AP-001095 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The SSLCipherSuite must be configured to disable weak encryption algorithms on the Tanium Server.

```
GROUP ID: V-254946
RULE ID: SV-254946r962034
```

Rationale:

Use of weak or untested encryption algorithms undermines the purposes of utilizing encryption to protect data. The application must implement cryptographic modules adhering to the higher standards approved by the federal government since this provides assurance they have been tested and validated.

Audit:

1. Access the Tanium Server interactively.
2. Log on to the server with the tanadmin role.
3. Enter 2: Tanium Operations >> 2: Tanium Configuration Settings >> 1: Edit Tanium Server Settings.
4. Verify the existence of a "SSLCipherSuite" key with a value of:

ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK
If the String "SSLCipherSuite" does not exist with the appropriate list values, this is a finding.

Remediation:

1. Access the Tanium Server interactively.
2. Log on to the server with the tanadmin role.
3. Enter 2: Tanium Operations >> 2: Tanium Configuration Settings >> 1: Edit Tanium Server Settings.
4. Enter the number associated with key "SSLCipherSuite" to edit its value.
5. Add or modify the "SSLCipherSuite" key to have a value of:

ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA256:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK

Additional Information:

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

1.68 TANS-AP-001130 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium Server certificate must be signed by a DOD Certificate Authority.

```
GROUP ID: V-254947
RULE ID: SV-254947r961596
```

Rationale:

The Tanium Server has the option to use a "self-signed" certificate or a Trusted Certificate Authority signed certificate for SSL connections. During evaluations of Tanium in Lab settings, customers often conclude that a "self-signed" certificate is an acceptable risk. However, in production environments it is critical that a SSL certificate signed by a Trusted Certificate Authority be used on the Tanium Server in lieu of an untrusted and insecure "self-signed" certificate.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. When connected, review the Certificate for the Tanium Server.
3. In the web browser, view the presented Certificate and verify that the Certificate shows as issued by a DOD Root CA. Also verify that the Certification path's top-level is a DOD Root CA.
4. If the certificate authority is not DOD Root CA, this is a finding.

Remediation:

Request or regenerate the certificate from a DOD Root Certificate Authority.

Additional Information:

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

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

1.69 TANS-AP-001150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The Tanium application must limit the bandwidth used in communicating with endpoints to prevent a denial of service (DoS) condition at the server.

```
GROUP ID: V-254948
RULE ID: SV-254948r961620
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

This requirement addresses the configuration of applications to mitigate the impact of DoS attacks that have occurred or are ongoing on application availability. For each application, known and potential DoS attacks must be identified and solutions for each type implemented. A variety of technologies exist to limit or, in some cases, eliminate the effects of DoS attacks (e.g., limiting processes or restricting the number of sessions the application opens at one time). Employing increased capacity and bandwidth, combined with service redundancy, may reduce the susceptibility to some DoS attacks.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration", select "Bandwidth Throttles".
4. Work with the Tanium Administrator to confirm settings.

If bandwidth throttles are not configured, this is a finding.
For more information, see the following:
https://docs.tanium.com/platform_user/platform_user/console_bandwidth_throttling.html
.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Configuration, select "Bandwidth Throttles".
4. Click "Add" on the line for "Global Throttle for All Data".
5. Work with Tanium Administrator to configure the required bandwidth throttles.
6. Click "Save".
7. Work with the Tanium Administrator to confirm or set settings for the remaining options:
8. a) Global Throttle for Package Files
9. b) Global Throttle for Sensors
10. c) Site Throttles

Additional Information:

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

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

1.70 TANS-AP-001215 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-254949
RULE ID: SV-254949r961683
```

Rationale:

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

Organization-defined time periods for updating security-relevant software may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw).

This requirement will apply to software patch management solutions that are used to install patches across the enclave and also to applications themselves that are not part of that patch management solution. For example, many browsers today provide the capability to install their own patch software. Patch criticality, as well as system criticality will vary. Therefore, the tactical situations regarding the patch management process will also vary. This means that the time period utilized must be a configurable parameter. Time frames for application of security-relevant software updates may be dependent upon the Information Assurance Vulnerability Management (IAVM) process.

The application will be configured to check for and install security-relevant software updates within an identified time period from the availability of the update. The specific time period will be defined by an authoritative source (e.g., IAVM, CTOs, DTMs, and STIGs).

Audit:

Ensure all components of the Tanium application have been updated within 60 days of the vulnerability being announced by Tanium. Critical Vulnerabilities must be updated within 30 days.

Consult with the Tanium System Administrator to review the documented time window designated for updates.

If a window of time is not defined, or does not specify a reoccurring frequency, this is a finding.

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under "Configuration," select "Solutions".

If any module has the text, "Update to" a newer (greater) version number compared to the Installed version number in the Tanium Modules section of the page, this is a finding.
If the Tanium application is an "airgap" installation, work with the Tanium Technical System Administrator to determine if the modules are up to date.

Remediation:

Consult with the Tanium System Administrator to review the documented time window designated for updates.

If a window of time is not defined, or does not specify a reoccurring frequency, work with the Tanium Administrator to document.

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Administration" on the top navigation banner.
3. Under Configuration, select "Solutions".

If any module has the text, "Update to" a newer (greater) version number compared to the Installed version number in the Tanium Modules section of the page, work with the Tanium Administrator to update those modules or content.
If the Tanium application is an "airgap" installation, work with the Tanium Technical System Administrator to determine if the modules are up to date.

Additional Information:

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

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

1.71 TANS-AP-001250 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:
Tanium must alert the ISSO, ISSM, and other individuals designated by the local organization when the following Indicators of Compromise (IOCs) or potential compromise are detected: real time intrusion detection; threats identified by authoritative sources (e.g., CTOs); and Category I, II, IV, and VII incidents in accordance with CJCSM 6510.01B.

```
GROUP ID: V-254950
RULE ID: SV-254950r961728
```

Rationale:

When a security event occurs, the application that has detected the event must immediately notify the appropriate support personnel so they can respond appropriately.

Alerts may be generated from a variety of sources, including, audit records or inputs from malicious code protection mechanisms, intrusion detection, or prevention mechanisms. Alerts may be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Individuals designated by the local organization to receive alerts may include, for example, system administrators, mission/business owners, or system owners.

IOCs are forensic artifacts from intrusions identified on organizational information systems (at the host or network level). IOCs provide organizations with valuable information on objects or information systems that have been compromised. These indicators reflect the occurrence of a compromise or a potential compromise.

This requirement applies to applications that provide monitoring capability for unusual/unauthorized activities including, but not limited to, host-based intrusion detection, antivirus, and malware applications.

Audit:

Note: If THR is not licensed or used for detection then this is not applicable.

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Threat Response".
4. Expand the left menu.
5. Click "Alerts".
6. Filter on status "Unresolved".

If any alerts are unresolved, this is a finding.

Remediation:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Click "Threat Response".
4. Expand the left menu.
5. Click "Alerts".
6. Filter on status "Unresolved".
7. Resolve any open IOC-based alerts and change status to applicable status.

Additional Information:

CCI-002664 Alert organization-defined personnel or roles when organization-defined compromise indicators generate the occurrence of a compromise or a potential compromise.

- NIST SP 800-53 Revision 4::SI-4 (5)
- NIST SP 800-53 Revision 5::SI-4 (5)

1.72 TANS-AP-001405 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The application must, at a minimum, offload interconnected systems in real time and offload standalone systems weekly.

```
GROUP ID: V-254951
RULE ID: SV-254951r961860
```

Rationale:

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

Offloading is a common process in information systems with limited audit storage capacity.

Audit:

1. Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.
2. Click "Modules" on the top navigation banner.
3. Select "Connect".
4. Review the "Connections" sections for source "Tanium Audit Source".

If necessary, filter the connections by filtering by "Source" and the term "Audit".

5. Select "Audit" from list.
6. In the Summary section, verify the "State" is "Enabled" and the "Next Run" value is less than "7" days.

If no results are returned, this is a finding.
If results are returned but the state is not "Enabled", this is a finding.
If the schedule duration is more than one week, this is a finding.
If a schedule is not set, this is a finding.

Remediation:

1.Using a web browser on a system that has connectivity to the Tanium Application, access the Tanium Application web user interface (UI) and log on with multi-factor authentication.

2. Click "Modules" on the top navigation banner.
3. Select "Connect".
4. Click "Create Connection".
5. Enter "Name".
6. Enter "Description".
7. In the "Configuration" section, select "Source: Tanium Audit Source" and then under "Basic" options select appropriate audits.
8. In the Destination section, select a source from the drop-down menu.
9. Enter "Destination Name".
10. Enter "Host".
11. Select "Network Protocol", then "TCP" or "UDP".
12. Enter "Port".
13. In the Schedule section, select "Enable Schedule".
14. Select "Basic".
15. Select the drop-down under "Frequency" and choose, "One run per day, on selected days of the week".
16. Select a day.
17. Select a time.
18. Select "Save".

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)

1.73 TANS-AP-001410 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Client processes must be excluded from on-access scan.

```
GROUP ID: V-254952
RULE ID: SV-254952r961863
```

Rationale:

Similar to any other host-based applications, the Tanium Client is subject to the restrictions other system-level software may place on an operating environment. That is to say that Antivirus, IPS, Encryption, or other security and management stack software may disallow the Client from working as expected.

https://docs.tanium.com/client/client/requirements.html#Host_system_security_exceptions

Audit:

Review the settings of the antivirus software.

Validate exclusions exist that exclude the Tanium Client process interactions from on-access scans and are treated as low-risk.

If exclusions do not exist, this is a finding.

Remediation:

Implement exclusion policies within the antivirus software solution to exclude the on-access scanning of Tanium Client process interactions. These processes should be treated as low-risk and not scanned during read or write events.

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

1.74 TANS-AP-001415 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium Client directory and subsequent files must be excluded from on-access scan.

```
GROUP ID: V-254953
RULE ID: SV-254953r961863
```

Rationale:

Similar to any other host-based applications, the Tanium Client is subject to the restrictions other system-level software may place on an operating environment. That is to say that Antivirus, IPS, Encryption, or other security and management stack software may disallow the Client from working as expected.

https://docs.tanium.com/client/client/requirements.html#Host_system_security_exceptions

Audit:

Review the settings of the antivirus software.

Validate exclusions exist that exclude the Tanium Client directory and subsequent files interactions from on-access scans.

If exclusions do not exist, this is a finding.

Remediation:

Implement exclusion policies within the antivirus software solution to exclude the on-access scanning of Tanium Client directory and subsequent files interactions.

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

1.75 TANS-AP-001420 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

Tanium endpoint files must be excluded from host-based intrusion prevention intervention.

```
GROUP ID: V-254954
RULE ID: SV-254954r1067672
```

Rationale:

Similar to any other host-based applications, the Tanium Client is subject to the restrictions other system-level software may place on an operating environment. Antivirus, IPS, encryption, or other security and management stack software may disallow the Tanium Server from working as expected.

https://docs.tanium.com/client/client/requirements.html#Host_system_security_exceptions

Audit:

Consult with the Tanium system administrator to determine the intrusion prevention software used on the Tanium Clients.

Review the settings of the intrusion prevention software.

Validate exclusions exist that exclude the Tanium program files from being restricted by intrusion prevention.

If exclusions do not exist, this is a finding.

Remediation:

In the host-based intrusion prevention system, ensure the following folders are excluded:

Windows (64-bit OS versions) - \Program Files (x86)\Tanium\Tanium Client

Windows (32-bit OS versions) - \Program Files\Tanium\Tanium Client

macOS - /Library/Tanium/TaniumClient

Linux, Solaris, AIX - /opt/Tanium/TaniumClient

In the host-based intrusion prevention system, ensure the following processes are excluded:

Windows, macOS, Linux - <Tanium Client>/Tools/StdUtils directory or all the files that it contains, including:

Windows, macOS, Linux - 7za.exe (Windows) or 7za (macOS, Linux)

Windows, macOS, Linux - runasuser.exe (Windows only)

Windows, macOS, Linux - runasuser64.exe (Windows only)

Windows, macOS, Linux - TaniumExecWrapper.exe (Windows) or TaniumExecWrapper (macOS, Linux)

Windows, macOS, Linux - TaniumFileInfo.exe (Windows only)

Windows, macOS, Linux - TPowerShell.exe (Windows only)

macOS, Linux, Solaris, AIX - <Tanium Client>/TaniumClient

macOS, Linux, Solaris, AIX - <Tanium Client>/taniumclient

macOS, Linux - <Tanium Client>/distribute-tools.sh

macOS, Linux - <Tanium Client>/TaniumCX

Windows - <Tanium Client>\TaniumClient.exe

Windows - <Tanium Client>\TaniumCX.exe

Additional Information:

CCI-000366 Implement the security configuration settings.

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

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	TANS-AP-000005 (Manual)	☐	☐
1.2	TANS-AP-000010 (Manual)	☐	☐
1.3	TANS-AP-000020 (Manual)	☐	☐
1.4	TANS-AP-000040 (Manual)	☐	☐
1.5	TANS-AP-000045 (Manual)	☐	☐
1.6	TANS-AP-000050 (Manual)	☐	☐
1.7	TANS-AP-000055 (Manual)	☐	☐
1.8	TANS-AP-000065 (Manual)	☐	☐
1.9	TANS-AP-000100 (Manual)	☐	☐
1.10	TANS-AP-000105 (Manual)	☐	☐
1.11	TANS-AP-000110 (Manual)	☐	☐
1.12	TANS-AP-000115 (Manual)	☐	☐
1.13	TANS-AP-000120 (Manual)	☐	☐
1.14	TANS-AP-000130 (Manual)	☐	☐
1.15	TANS-AP-000135 (Manual)	☐	☐
1.16	TANS-AP-000140 (Manual)	☐	☐
1.17	TANS-AP-000150 (Manual)	☐	☐
1.18	TANS-AP-000155 (Manual)	☐	☐
1.19	TANS-AP-000160 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	TANS-AP-000165 (Manual)	☐	☐
1.21	TANS-AP-000175 (Manual)	☐	☐
1.22	TANS-AP-000180 (Manual)	☐	☐
1.23	TANS-AP-000195 (Manual)	☐	☐
1.24	TANS-AP-000260 (Manual)	☐	☐
1.25	TANS-AP-000270 (Manual)	☐	☐
1.26	TANS-AP-000280 (Manual)	☐	☐
1.27	TANS-AP-000295 (Manual)	☐	☐
1.28	TANS-AP-000305 (Manual)	☐	☐
1.29	TANS-AP-000330 (Manual)	☐	☐
1.30	TANS-AP-000335 (Manual)	☐	☐
1.31	TANS-AP-000355 (Manual)	☐	☐
1.32	TANS-AP-000360 (Manual)	☐	☐
1.33	TANS-AP-000365 (Manual)	☐	☐
1.34	TANS-AP-000370 (Manual)	☐	☐
1.35	TANS-AP-000415 (Manual)	☐	☐
1.36	TANS-AP-000425 (Manual)	☐	☐
1.37	TANS-AP-000470 (Manual)	☐	☐
1.38	TANS-AP-000475 (Manual)	☐	☐
1.39	TANS-AP-000480 (Manual)	☐	☐
1.40	TANS-AP-000490 (Manual)	☐	☐
1.41	TANS-AP-000505 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	TANS-AP-000555 (Manual)	☐	☐
1.43	TANS-AP-000600 (Manual)	☐	☐
1.44	TANS-AP-000630 (Manual)	☐	☐
1.45	TANS-AP-000635 (Manual)	☐	☐
1.46	TANS-AP-000655 (Manual)	☐	☐
1.47	TANS-AP-000700 (Manual)	☐	☐
1.48	TANS-AP-000705 (Manual)	☐	☐
1.49	TANS-AP-000710 (Manual)	☐	☐
1.50	TANS-AP-000715 (Manual)	☐	☐
1.51	TANS-AP-000720 (Manual)	☐	☐
1.52	TANS-AP-000765 (Manual)	☐	☐
1.53	TANS-AP-000780 (Manual)	☐	☐
1.54	TANS-AP-000800 (Manual)	☐	☐
1.55	TANS-AP-000805 (Manual)	☐	☐
1.56	TANS-AP-000810 (Manual)	☐	☐
1.57	TANS-AP-000860 (Manual)	☐	☐
1.58	TANS-AP-000865 (Manual)	☐	☐
1.59	TANS-AP-000870 (Manual)	☐	☐
1.60	TANS-AP-000875 (Manual)	☐	☐
1.61	TANS-AP-000940 (Manual)	☐	☐
1.62	TANS-AP-000950 (Manual)	☐	☐
1.63	TANS-AP-000975 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	TANS-AP-000980 (Manual)	☐	☐
1.65	TANS-AP-000985 (Manual)	☐	☐
1.66	TANS-AP-001090 (Manual)	☐	☐
1.67	TANS-AP-001095 (Manual)	☐	☐
1.68	TANS-AP-001130 (Manual)	☐	☐
1.69	TANS-AP-001150 (Manual)	☐	☐
1.70	TANS-AP-001215 (Manual)	☐	☐
1.71	TANS-AP-001250 (Manual)	☐	☐
1.72	TANS-AP-001405 (Manual)	☐	☐
1.73	TANS-AP-001410 (Manual)	☐	☐
1.74	TANS-AP-001415 (Manual)	☐	☐
1.75	TANS-AP-001420 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 22, 2025	1.0.0	Initial CIS Release