CIS VMware NSX 4.x Manager NDM STIG Benchmark

v1.0.0 – 01-30-2025

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

VMware NSX 4.x Manager NDM Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 30 Jan 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 VMware NSX 4.x Manager NDM and are looking to comply with the STIG guidance

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

The Rule Title from the STIG.

Rationale Statement

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

Audit Procedure

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

Remediation Procedure

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

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

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 VMware NSX 4.x Manager NDM

Recommendations

1 STIG RULES

VMware NSX

VMware NSX 4.x Manager NDM Secure Technical Implementation Guide (STIG)

Version: 1 Release: 2 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 NMGR-4X-000007 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must configure logging levels for services to ensure audit records are generated.

```
GROUP ID: V-265289
RULE ID: SV-265289r994090
```

Rationale:

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

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

Satisfies: SRG-APP-000027-NDM-000209, SRG-APP-000495-NDM-000318, SRG-APP-000499-NDM-000319, SRG-APP-000503-NDM-000320, SRG-APP-000504-NDM-000321, SRG-APP-000505-NDM-000322, SRG-APP-000506-NDM-000323, SRG-APP-000516-NDM-000334

Audit:

From an NSX Manager shell, run the following commands:

get service async_replicator | find Logging

get service auth | find Logging

get service http | find Logging

get service manager | find Logging

get service telemetry | find Logging

Expected result:

Logging level: info

If any service listed does not have logging level configured to "info", this is a finding.

Remediation:

From an NSX Manager shell, run the following commands:

```
set service async_replicator logging-level info
set service auth logging-level info
set service http logging-level info
set service manager logging-level info
set service telemetry logging-level info
```

1.2 NMGR-4X-000010 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Manager must assign users/accounts to organization-defined roles configured with approved authorizations.

```
GROUP ID: V-265292
RULE ID: SV-265292r994099
```

Rationale:

The lack of authorization-based access control could result in the immediate compromise and unauthorized access to sensitive information. Users must be assigned to roles which are configured with approved authorizations and access permissions. The NSX Manager must be configured granularly based on organization requirements to only allow authorized administrators to execute privileged functions. Role assignments should control which administrators can view or change the device configuration, system files, and locally stored audit information.

Satisfies: SRG-APP-000033-NDM-000212, SRG-APP-000038-NDM-000213, SRG-APP-000119-NDM-000236, SRG-APP-000120-NDM-000237, SRG-APP-000133-NDM-000244, SRG-APP-000231-NDM-000271, SRG-APP-000329-NDM-000287, SRG-APP-000340-NDM-000288, SRG-APP-000378-NDM-000302, SRG-APP-000380-NDM-000304, SRG-APP-000408-NDM-000314, SRG-APP-000516-NDM-000335

Audit:

From the NSX Manager web interface, go to System >> Settings >> User Management >> User Role Assignment.

View each user and group and verify the role assigned has authorization limits as appropriate to the role and in accordance with the site's documentation.

If any user/group or service account are assigned to roles with privileges that are beyond those required and authorized by the organization, this is a finding.

Remediation:

To create a new role with reduced permissions, do the following:

From the NSX Manager web interface, go to System >> Settings >> User Management >> Roles.

Click "Add Role", provide a name and the required permissions, and then click "Save".

To update user or group permissions to an existing role with reduced permissions, do the following:

From the NSX Manager web interface, go to System >> User Management >> User Role Assignment.

Click the menu dropdown next to the target user or group and select "Edit".

Remove the existing role, select the new one, and then click "Save".

1.3 NMGR-4X-000012 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-265293
RULE ID: SV-265293r994102
```

Rationale:

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

Audit:

From an NSX Manager shell, run the following commands:

get auth-policy api lockout-reset-period

Expected result:

900 seconds

If the output does not match the expected result, this is a finding.

get auth-policy api lockout-period

Expected result:

900 seconds

If the output does not match the expected result, this is a finding.

get auth-policy api max-auth-failures

Expected result:

3

If the output does not match the expected result, this is a finding.

get auth-policy cli lockout-period

Expected result:

900 seconds

If the output does not match the expected result, this is a finding.

get auth-policy cli max-auth-failures

Expected result:

3

If the output does not match the expected result, this is a finding.

Remediation:

From an NSX Manager shell, run the following commands:

set auth-policy api lockout-reset-period 900

set auth-policy api lockout-period 900

set auth-policy api max-auth-failures 3

set auth-policy cli lockout-period 900

set auth-policy cli max-auth-failures 3

1.4 NMGR-4X-000013 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must display the Standard Mandatory DOD Notice and Consent Banner before granting access.

```
GROUP ID: V-265294
RULE ID: SV-265294r994105
```

Rationale:

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

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

Audit:

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

From the NSX Manager web interface, go to System >> Settings >> General Settings >> User Interface.

Review the Login Consent Settings.

If the "Consent Message Description" does not contain the Standard Mandatory DOD Notice and Consent Banner verbiage, this is a finding.

The Standard Mandatory DOD Notice and Consent Banner verbiage is as follows:

"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."

Remediation:

From the NSX Manager web interface, go to System >> Settings >> General Settings >> User Interface.

Under Login Consent Settings click "Edit".

Enter the banner language in the "Consent Message Description" text box, formatted in accordance with DTM-08-060, and click "Save".

"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."

1.5 NMGR-4X-000014 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-265295
RULE ID: SV-265295r994108
```

Rationale:

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

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

In the case of CLI access using a terminal client, entering the username and password when the banner is presented is considered an explicit action of acknowledgement. Entering the username, viewing the banner, then entering the password is also acceptable.

Audit:

From the NSX Manager web interface, go to System >> Settings >> General Settings >> User Interface.

Review the Login Consent Settings.

Verify "Login Consent" is not On.

Verify "Require Explicit User Consent" is set to Yes.

If the Standard Mandatory DOD Notice and Consent Banner is not retained on the screen until the administrator acknowledges the usage conditions and takes explicit actions to log on for further access, this is a finding.

Remediation:

From the NSX Manager web interface, go to System >> Settings >> General Settings >> User Interface.

Under Login Consent Settings, click "Edit".

Toggle "Login Consent" to On.

Toggle "Require Explicit User Consent" to Yes.

Note: The banner text is also entered; however, that is covered by NMGR-4X-000013.

1.6 NMGR-4X-000035 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-265313
RULE ID: SV-265313r1051115
```

Rationale:

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

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

Audit:

From the NSX Manager web interface, go to the System >> Settings >> User Management >> Local Users and view the status column.

If any local account other than the account of last resort are active, this is a finding.

Remediation:

From the NSX Manager web interface, go to the System >> Settings >> User Management >> Local Users.

Select the menu drop down next to any local user on the list except for the "admin" account. Click modify and click "Deactivate User".

1.7 NMGR-4X-000038 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Manager must only enable TLS 1.2 or greater.

```
GROUP ID: V-265315
RULE ID: SV-265315r994168
```

Rationale:

A replay attack may enable an unauthorized user to gain access to the application. Authentication sessions between the authenticator and the application validating the user credentials must not be vulnerable to a replay attack. Configuration of TLS on the NSX also ensures that passwords are not transmitted in the clear.

TLS 1.0 and 1.1 are deprecated protocols with well-published shortcomings and vulnerabilities. TLS 1.2 or greater must be enabled on all interfaces and TLS 1.1 and 1.0 disabled where supported.

Satisfies: SRG-APP-000156-NDM-000250, SRG-APP-000172-NDM-000259

Audit:

Viewing TLS protocol enablement must be done via the API.

Execute the following API call using curl or another REST API client:

GET https:///api/v1/cluster/api-service

Example result:

"protocol_versions": [

{

"name": "TLSv1.1",

"enabled": false

},

{

"name": "TLSv1.2",

"enabled": true

},

{

"name": "TLSv1.3",

"enabled": true

}

]

If TLS 1.1 is enabled, this is a finding.

Remediation:

Capture the output from the check GET command and update the TLS 1.1 protocol to false.

Run the following API call using curl or another REST API client:

PUT https:///api/v1/cluster/api-service

Example request body:

{

"session_timeout": 1800,

"connection_timeout": 30,

"protocol_versions": [

{

"name": "TLSv1.1",

"enabled": false

},

{

"name": "TLSv1.2",

"enabled": true

},

{

"name": "TLSv1.3",

"enabled": true

}

],

"cipher_suites": [

{

"name": "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA",
"enabled": true
},
{
"name": "TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256",
"enabled": true
},
{
"name": "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"enabled": true
},
{
"name": "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA",
"enabled": true
},
{
"name": "TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384",
"enabled": true
},
{
"name": "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"enabled": true
},
{
"name": "TLS_RSA_WITH_AES_128_CBC_SHA",
"enabled": true
},
{
"name": "TLS_RSA_WITH_AES_128_CBC_SHA256",
"enabled": true

},
{
"name": "TLS_RSA_WITH_AES_128_GCM_SHA256",
"enabled": true
},
{
"name": "TLS_RSA_WITH_AES_256_CBC_SHA",
"enabled": true
},
{
"name": "TLS_RSA_WITH_AES_256_CBC_SHA256",
"enabled": true
},
{
"name": "TLS_RSA_WITH_AES_256_GCM_SHA384",
"enabled": true
},
{
"name": "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
"enabled": true
},
{
"name": "TLS_AES_128_GCM_SHA256",
"enabled": true
},
{
"name": "TLS_AES_256_GCM_SHA384",
"enabled": true
},
{

"name": "TLS_CHACHA20_POLY1305_SHA256",
"enabled": true
}
],
"redirect_host": "",
"client_api_rate_limit": 100,
"global_api_concurrency_limit": 199,
"client_api_concurrency_limit": 40,
"basic_authentication_enabled": true,
"cookie_based_authentication_enabled": true,
"resource_type": "ApiServiceConfig",
"id": "reverse_proxy_config",
"display_name": "reverse_proxy_config",
"_create_time": 1703175890703,
"_create_user": "system",
"_last_modified_time": 1703175890703,
"_last_modified_user": "system",
"_system_owned": false,
"_protection": "NOT_PROTECTED",
"_revision": 0
}

Note: Changes are applied to all nodes in the cluster. The API service on each node will restart after it is updated using this API. There may be a delay of up to a minute or so between the time this API call completes and when the new configuration goes into effect.

1.8 NMGR-4X-000015 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Manager must be configured to integrate with an identity provider that supports multifactor authentication (MFA).

```
GROUP ID: V-265296
RULE ID: SV-265296r994111
```

Rationale:

Common attacks against single-factor authentication are attacks on user passwords. These attacks include brute force password guessing, password spraying, and password credential stuffing. This requirement also supports nonrepudiation of actions taken by an administrator.

This requirement ensures the NSX Manager is configured to use a centralized authentication services to authenticate users prior to granting administrative access.

As of NSX 4.1 and vCenter 8.0 Update 2, NSX Manager administrator access can also be configured by connecting VMware NSX to the Workspace ONE Access Broker in VMware vCenter for federated identity. Refer to the NSX product documentation to configure this access option.

Satisfies: SRG-APP-000080-NDM-000220, SRG-APP-000149-NDM-000247, SRG-APP-000516-NDM-000336

Audit:

From the NSX Manager web interface, go to System >> Settings >> Users Management >> Authentication Providers.

Verify that the "VMware Identity Manager" and "OpenID Connect" tabs are configured.

If NSX is not configured to integrate with an identity provider that supports MFA, this is a finding.

Remediation:

To configure NSX to integrate with VMware Identity Manager or Workspace ONE Access, as the authentication source, do the following:

From the NSX Manager web interface, go to System >> Users and Roles >> VMware Identity Manager and click "Edit".

If using an external load balancer for the NSX Management cluster, enable "External Load Balancer Integration". If using a cluster VIP, leave this disabled.

Click the toggle button to enable "VMware Identity Manager Integration".

Enter the VMware Identity Manager or Workspace ONE Access appliance name, OAuth Client ID, OAuth Client Secret, and certificate thumbprint as provided by the administrators.

Enter the NSX Appliance FQDN. For a cluster, enter the load balancer FQDN or cluster VIP FQDN.

Click "Save", import users and groups, and then assign them roles. (The users are not actually local and remain in the authentication/AAA server.)

Note: As of NSX 4.1 and vCenter 8.0 Update 2, NSX Manager administrator access can also be configured by connecting VMware NSX to the Workspace ONE Access Broker in VMware vCenter for federated identity. Refer to the NSX product documentation to configure this access option.

Ensure the identity provider administrators have configured the provider to support multi-factor authentication.

1.9 NMGR-4X-000039 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must enforce a minimum 15-character password length for local accounts.

```
GROUP ID: V-265316
RULE ID: SV-265316r994171
```

Rationale:

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

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

Audit:

From an NSX Manager shell, run the following command:

```
get password-complexity
```

If the minimum password length is not 15 or greater, this is a finding.

Remediation:

From an NSX Manager shell, run the following command:

```
set password-complexity minimum-password-length 15
```

1.10 NMGR-4X-000040 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must enforce password complexity by requiring that at least one uppercase character be used for local accounts.

```
GROUP ID: V-265317
RULE ID: SV-265317r994174
```

Rationale:

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

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

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

Audit:

From an NSX Manager shell, run the following command:

```
get password-complexity
```

If the minimum uppercase characters is not 1 or more, this is a finding.

Note: If a maximum number of uppercase characters has been configured a minimum will not be shown.

Remediation:

From an NSX Manager shell, run the following command:

```
set password-complexity upper-chars -1
```

Note: Negative numbers indicate a minimum number of characters.

1.11 NMGR-4X-000041 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must enforce password complexity by requiring that at least one lowercase character be used for local accounts.

```
GROUP ID: V-265318
RULE ID: SV-265318r994177
```

Rationale:

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

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

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

Audit:

From an NSX Manager shell, run the following command:

```
get password-complexity
```

If the minimum lowercase characters is not 1 or more, this is a finding.

Note: If a maximum number of lowercase characters has been configured, a minimum will not be shown.

Remediation:

From an NSX Manager shell, run the following command:

```
set password-complexity lower-chars -1
```

Note: Negative numbers indicate a minimum number of characters.

1.12 NMGR-4X-000042 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must enforce password complexity by requiring that at least one numeric character be used for local accounts.

```
GROUP ID: V-265319
RULE ID: SV-265319r994180
```

Rationale:

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

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

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

Audit:

From an NSX Manager shell, run the following command:

```
get password-complexity
```

If the minimum numeric characters is not 1 or more, this is a finding.

Note: If a maximum number of numeric characters has been configured, a minimum will not be shown.

Remediation:

From an NSX Manager shell, run the following command:

```
set password-complexity digits -1
```

Note: Negative numbers indicate a minimum number of characters.

1.13 NMGR-4X-000043 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must enforce password complexity by requiring that at least one special character be used for local accounts.

```
GROUP ID: V-265320
RULE ID: SV-265320r994183
```

Rationale:

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

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

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

Audit:

From an NSX Manager shell, run the following command:

```
get password-complexity
```

If the minimum special characters is not 1 or more, this is a finding.

Note: If a maximum number of special characters has been configured, a minimum will not be shown.

Remediation:

From an NSX Manager shell, run the following command:

```
set password-complexity special-chars -1
```

Note: Negative numbers indicate a minimum number of characters.

1.14 NMGR-4X-000044 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-265321
RULE ID: SV-265321r1043189
```

Rationale:

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

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

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

Audit:

From an NSX Manager shell, run the following command:

```
get password-complexity
```

If the number of consecutive characters allowed for reuse is not eight or more, this is a finding.

Note: If this has not previously been configured it will not be shown in the output.

Remediation:

From an NSX Manager shell, run the following command:

```
set password-complexity max-repeats 8
```

1.15 NMGR-4X-000052 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Manager must terminate all network connections associated with a session after five minutes of inactivity.

```
GROUP ID: V-265327
RULE ID: SV-265327r994204
```

Rationale:

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

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

Satisfies: SRG-APP-000190-NDM-000267, SRG-APP-000186-NDM-000266, SRG-APP-000400-NDM-000313

Audit:

From an NSX Manager shell, run the following command:

```
get service http | find Session
```

Expected result:

Session timeout: 300

If the session timeout is not configured to 300 or less, this is a finding.

From an NSX Manager shell, run the following command:

```
get cli-timeout
```

Expected result:

300 seconds

If the CLI timeout is not configured to 300 or less, this is a finding.

Remediation:

From an NSX Manager shell, run the following commands:

```
        set service http session-timeout 300
    set cli-timeout 300
```

1.16 NMGR-4X-000067 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must be configured to synchronize internal information system clocks using redundant authoritative time sources.

```
GROUP ID: V-265338
RULE ID: SV-265338r994237
```

Rationale:

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

Multiple time sources provide redundancy by including a secondary source. Time synchronization is usually a hierarchy; clients synchronize time to a local source while that source synchronizes its time to a more accurate source. The network device must use an authoritative time server and/or be configured to use redundant authoritative time sources.

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

Audit:

From the NSX Manager web interface, go to System >> Configuration >> Fabric >> Profiles >> Node Profiles.

Click "All NSX Nodes" and verify the NTP servers listed.

or

From an NSX Manager shell, run the following command:

```
get ntp-server
```

If the output does not contain at least two authoritative time sources, this is a finding.

If the output contains unknown or nonauthoritative time sources, this is a finding.

Remediation:

To configure a profile to apply NTP servers to all NSX Manager nodes, do the following:

From the NSX Manager web interface, go to System >> Configuration >> Fabric >> Profiles >> Node Profiles.

Click "All NSX Nodes" and then click "Edit".

Under NTP servers, remove any unknown or nonauthoritative NTP servers, enter at least two authoritative servers, and then click "Save".

or

From an NSX Manager shell, run the following commands:

del ntp-server

set ntp-server

1.17 NMGR-4X-000068 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC).

```
GROUP ID: V-265339
RULE ID: SV-265339r994240
```

Rationale:

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

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

Audit:

From the NSX Manager web interface, go to System >> Configuration >> Fabric >> Profiles >> Node Profiles.

Note: This check must be run from each NSX Manager as they are configured individually if done from the command line.

Click "All NSX Nodes" and verify the time zone.

or

From an NSX Manager shell, run the following command:

```
get clock
```

If system clock is not configured with the UTC time zone, this is a finding.

Remediation:

To configure a profile to apply a time zone to all NSX Manager nodes, do the following:

From the NSX Manager web interface, go to System >> Configuration >> Fabric >> Profiles >> Node Profiles.

Click "All NSX Nodes", and then click "Edit".

In the time zone drop-down list, select "UTC", and then click "Save".

or

From an NSX Manager shell, run the following command:

```
set timezone UTC
```

Note: This fix must be run from each NSX Manager as they are configured individually if done from the command line.

1.18 NMGR-4X-000079 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must be configured to protect against denial-of-service (DoS) attacks by limit the number of concurrent sessions to an organization-defined number.

```
GROUP ID: V-265346
RULE ID: SV-265346r994261
```

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.

Limiting the number of concurrent open sessions helps limit the risk of DoS attacks.

Organizations may define the maximum number of concurrent sessions for system accounts globally or by connection type. By default, the NSX Manager has a protection mechanism in place to prevent the API from being overloaded. This setting also addresses concurrent sessions for integrations into NSX API to monitor or configure NSX.

Satisfies: SRG-APP-000435-NDM-000315, SRG-APP-000001-NDM-000200

Audit:

From an NSX Manager shell, run the following command:

```
get service http | find limit
```

Expected result:

Client API concurrency limit: 40 connections

Global API concurrency limit: 199 connections

If the NSX does not limit the number of concurrent sessions to an organization-defined number, this is a finding.

Remediation:

From an NSX Manager shell, run the following commands:

```
        set service http client-api-concurrency-limit 40
    set service http global-api-concurrency-limit 199
```

Note: The limit numbers in this example, while not mandatory, are the vendor recommend options. Setting the limits to lower numbers in a large environment that is very busy may cause operational issues. Setting the limits higher may cause resource contention so should be tested and monitored.

1.19 NMGR-4X-000087 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Manager must be configured to send logs to a central log server.

```
GROUP ID: V-265348
RULE ID: SV-265348r994267
```

Rationale:

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

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

Satisfies: SRG-APP-000515-NDM-000325, SRG-APP-000357-NDM-000293, SRG-APP-000516-NDM-000350

Audit:

From the NSX Manager web interface, go to System >> Fabric >> Profiles >> Node Profiles.

Click "All NSX Nodes" and verify the Syslog servers listed.

or

From an NSX Manager shell, run the following command:

```
get logging-servers
```

Note: This command must be run from each NSX Manager as they are configured individually.

If no logging severs are configured or unauthorized logging servers are configured, this is a finding.

If the log level is not set to INFO, this is a finding.

Remediation:

To configure a profile to apply syslog servers to all NSX Manager nodes, do the following:

From the NSX Manager web interface, go to System >> Fabric >> Profiles >> Node Profiles.

Click "All NSX Nodes" and then under "Syslog Servers" click "Add".

Enter the syslog server details and choose "Information" for the log level and click "Add".

or

(Optional) From an NSX Manager shell, run the following command to clear any existing incorrect logging-servers:

```
clear logging-servers
```

From an NSX Manager shell, run the following command to configure a udp/tcp syslog server:

```
set logging-server proto level info
```

From an NSX Manager shell, run the following command to configure a TLS syslog server:

```
set logging-server proto tls level info serverca ca.pem clientca ca.pem
certificate cert.pem key key.pem
```

From an NSX Manager shell, run the following command to configure an LI-TLS syslog server:

```
set logging-server proto li-tls level info serverca root-ca.crt
```

Note: If using the protocols TLS or LI-TLS to configure a secure connection to a log server, the server and client certificates must be stored in /image/vmware/nsx/file-store on each NSX-T Manager appliance.

1.20 NMGR-4X-000088 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The NSX Manager must not provide environment information to third parties.

```
GROUP ID: V-265349
RULE ID: SV-265349r994270
```

Rationale:

Providing technical details about an environment's infrastructure to third parties could unknowingly expose sensitive information to bad actors if intercepted.

Audit:

From the NSX Manager web interface, go to System >> Settings >> General Settings >> Customer Program >> Customer Experience Improvement Program.

If Joined is set to "Yes", this is a finding.

Remediation:

From the NSX Manager web interface, go to System >> Settings >> General Settings >> Customer Program >> Customer Experience Improvement Program, and then click "Edit".

Uncheck "Join the VMware Customer Experience Improvement Program" and click "Save".

1.21 NMGR-4X-000093 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must be configured to conduct backups on an organizationally defined schedule.

```
GROUP ID: V-265350
RULE ID: SV-265350r994273
```

Rationale:

Information system backup is a critical step in maintaining data assurance and availability. Information system and security-related documentation contains information pertaining to system configuration and security settings. If this information were not backed up, and a system failure were to occur, the security settings would be difficult to reconfigure quickly and accurately. Maintaining a backup of information system and security-related documentation provides for a quicker recovery time when system outages occur.

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

Satisfies: SRG-APP-000516-NDM-000341, SRG-APP-000516-NDM-000340

Audit:

From the NSX Manager web interface, go to System >> Lifecycle Management >> Backup and Restore to view the backup configuration.

If backup is not configured and scheduled on a recurring frequency, this is a finding.

Remediation:

To configure a backup destination, do the following:

From the NSX Manager web interface, go to System >> Lifecycle Management >> Backup and Restore, and then click "Edit" next to SFTP Server.

Enter the target SFTP server, Directory Path, Username, Password, SSH Fingerprint, and Passphrase, and then click "Save".

To configure a backup schedule, do the following:

From the NSX Manager web interface, go to System >> Lifecycle Management >> Backup and Restore, and then click "Edit" next to Schedule.

Click the "Recurring Backup" toggle and configure an interval between backups.

Enable "Detect NSX configuration change" to trigger backups on detection of configuration changes and specify an interval for detecting changes. Click "Save".

1.22 NMGR-4X-000094 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

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

```
GROUP ID: V-265351
RULE ID: SV-265351r994276
```

Rationale:

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

Audit:

NSX Manager uses a certificate for each manager and one for the cluster VIP. In some cases these are the same, but each node and cluster VIP certificate must be checked individually.

Browse to the NSX Manager web interface for each node and cluster VIP and view the certificate and its issuer of the website.

or

From an NSX Manager shell, run the following commands:

get certificate api

get certificate cluster

Save the output to a .cer file to examine.

If the certificate the NSX Manager web interface or cluster is using is not issued by an approved certificate authority and is not currently valid, this is a finding.

Remediation:

Obtain a certificate or certificates signed by an approved certification authority.

This can be done individually by generating CSRs through the NSX Manager web interface >> System >> Settings >> Certificates >> CSRs >> Generate CSR or outside of NSX if a common manager and cluster certificate is desired.

Import the certificate(s) into NSX by doing the following:

From the NSX Manager web interface, go to System >> Settings >> Certificates >> Certificates >> Import >> Import Certificate. Provide a name for the certificate and paste the certificates contents and key.

Uncheck "Service Certificate" and click "Import".

After import, note the ID of the certificate(s).

Using curl or another REST API client, perform the following API calls and replace the certificate IDs noted in the previous steps.

To replace a managers certificate: POST https:///api/v1/node/services/http?action=apply_certificate&certificate_id=e61c7537-3090-4149-b2b6-19915c20504f

To replace the cluster certificate: POST https:///api/v1/cluster/api-certificate?action=set_cluster_certificate&certificate_id=d60c6a07-6e59-4873-8edb-339bf75711ac

Note: If an NSX Intelligence appliance is deployed with the NSX Manager cluster, update the NSX Manager node IP, certificate, and thumbprint information that is on the NSX Intelligence appliance. Refer to the VMware Knowledge Base article https://kb.vmware.com/s/article/78505 for more information.

1.23 NMGR-4X-000096 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The NSX Manager must be running a release that is currently supported by the vendor.

```
GROUP ID: V-265352
RULE ID: SV-265352r994279
```

Rationale:

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

Audit:

From the NSX Manager web interface, go to the System >> Lifecycle Management >> Upgrade.

If the NSX Manager current version is not the latest approved for use in DOD and supported by the vendor, this is a finding.

Remediation:

To upgrade NSX, reference the upgrade guide in the documentation for the relevant version being upgraded. Refer to the NSX documentation and release notes for information on the latest releases.

https://docs.vmware.com/en/VMware-NSX/index.html

If NSX is part of a VMware Cloud Foundation deployment, refer to that documentation for latest supported versions and upgrade guidance.

1.24 NMGR-4X-000097 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must disable SSH.

```
GROUP ID: V-265353
RULE ID: SV-265353r994282
```

Rationale:

The NSX shell provides temporary access to commands essential for server maintenance. Intended primarily for use in break-fix scenarios, the NSX shell is well suited for checking and modifying configuration details, not always generally accessible, using the web interface. The NSX shell is accessible remotely using SSH. Under normal operating conditions, SSH access to the managers must be disabled as is the default. As with the NSX shell, SSH is also intended only for temporary use during break-fix scenarios. SSH must therefore be disabled under normal operating conditions and must only be enabled for diagnostics or troubleshooting. Remote access to the managers must therefore be limited to the web interface and API at all other times.

Audit:

From an NSX Manager shell, run the following command:

get service ssh

Expected results:

Service name: ssh

Service state: stopped

Start on boot: False

If the SSH server is not stopped or starts on boot, this is a finding.

Remediation:

From an NSX Manager shell, run the following command(s):

stop service ssh

clear service ssh start-on-boot

1.25 NMGR-4X-000098 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must disable SNMP v2.

```
GROUP ID: V-265354
RULE ID: SV-265354r994285
```

Rationale:

SNMPv3 supports commercial-grade security, including authentication, authorization, access control, and privacy. Previous versions of the protocol contained well-known security weaknesses that were easily exploited. As such, SNMPv1/2 receivers must be disabled.

Audit:

From the NSX Manager web interface, go to the System >> Configuration >> Fabric >> Profiles >> Node Profiles.

Click "All NSX Nodes" and view the SNMP Polling and Traps configuration.

If SNMP v2c Polling or Traps are configured, this is a finding.

Remediation:

From the NSX Manager web interface, go to the System >> Configuration >> Fabric >> Profiles >> Node Profiles.

Click on "All NSX Nodes" and delete and v2c Polling or Trap configurations.

1.26 NMGR-4X-000099 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must enable the global FIPS compliance mode for load balancers.

```
GROUP ID: V-265355
RULE ID: SV-265355r994288
```

Rationale:

If unsecured protocols (lacking cryptographic mechanisms) are used for load balancing, the contents of those sessions will be susceptible to eavesdropping, potentially putting sensitive data at risk of compromise.

Audit:

From the NSX Manager web interface, go to the Home >> Monitoring Dashboards >> Compliance Report.

Review the compliance report for code 72024 with description load balancer FIPS global setting disabled.

Note: This may also be checked via the API call GET https:///policy/api/v1/infra/global-config

If the global FIPS setting is disabled for load balancers, this is a finding.

Remediation:

Execute the following API call using curl or another REST API client:

PUT https:///policy/api/v1/infra/global-config

Example request body:

{

"fips": {

"lb_fips_enabled": true

},

"resource_type": "GlobalConfig",

"_revision": 2

}

The global setting is used when the new load balancer instances are created. Changing the setting does not affect existing load balancer instances.

To update existing load balancers to use this setting, do the following:

From the NSX Manager web interface, go to the Networking >> Load Balancing and then click "Edit" on the target load balancer.

In the attachment field, click the "X" to detach the load balancer from its current Gateway and click "Save".

Edit the target load balancer again, reattach it to its Gateway, and then click "Save".

Caution: Detaching a load balancer from the Tier-1 gateway results in a traffic interruption for the load balancer instance.

1.27 NMGR-4X-000102 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Manager must be configured as a cluster.

```
GROUP ID: V-265358
RULE ID: SV-265358r994297
```

Rationale:

Failure in a known state can address safety or security in accordance with the mission 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 SDN controller. Preserving network element state information helps to facilitate continuous network operations minimal or no disruption to mission-essential workload processes and flows.

Audit:

From the NSX Manager web interface, go to System >> Configuration >> Appliances.

Verify three NSX Managers are deployed, a VIP or external load balancer is configured, and the cluster is in a healthy state.

If three NSX Managers are not deployed, a VIP or external load balancer is not configured, and the cluster is not in a healthy state, this is a finding.

Remediation:

To add additional NSX Manager appliances do the following:

From the NSX Manager web interface, go to System >> Configuration >> Appliances, and then click "Add NSX Appliance".

Supply the required information to add additional nodes as needed, up to three total.

To configure NSX with a cluster VIP or external load balancer, do the following:

From the NSX Manager web interface, go to System >> Configuration >> Appliances, and then click "Set Virtual IP", enter a VIP that is part of the same subnet as the other management nodes, and then click "Save".

To configure NSX with an external load balancer, setup an external load balancer with the following requirements:

- Configure the external load balancer to control traffic to the NSX Manager nodes.
- Configure the external load balancer to use the round robin method and configure source persistence for the load balancer's virtual IP.

- Create or import a signed certificate and apply the same certificate to all the NSX Manager nodes. The certificate must have the FQDN of the virtual IP and each of the nodes in the SAN.

Note: An external load balancer will not work with the NSX Manager VIP. Do not configure an NSX Manager VIP if using an external load balancer.
If the cluster status is not in a healthy state, identify the degraded component on the appliance and troubleshoot the issue with the error information provided.

1.28 NMGR-4X-000103 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The NSX Managers must be deployed on separate physical hosts.

```
GROUP ID: V-265359
RULE ID: SV-265359r994300
```

Rationale:

SDN relies heavily on control messages between a controller and the forwarding devices for network convergence. The controller uses node and link state discovery information to calculate and determine optimum pathing within the SDN network infrastructure based on application, business, and security policies. Operating in the proactive flow instantiation mode, the SDN controller populates forwarding tables to the SDN-aware forwarding devices. At times, the SDN controller must function in reactive flow instantiation mode; that is, when a forwarding device receives a packet for a flow not found in its forwarding table, it must send it to the controller to receive forwarding instructions.

With total dependence on the SDN controller for determining forwarding decisions and path optimization within the SDN infrastructure for both proactive and reactive flow modes of operation, having a single point of failure is not acceptable. A controller failure with no failover backup leaves the network in an unmanaged state. Hence, it is imperative that the SDN controllers are deployed as clusters on separate physical hosts to guarantee high network availability.

Audit:

This check must be performed in vCenter.

From the vSphere Client, go to Administration >> Hosts and Clusters >> Select the cluster where the NSX Managers are deployed >> Configure >> Configuration >> VM/Host Rules.

If the NSX Manager cluster does not have rules applied to it that separate the nodes onto different physical hosts, this is a finding.

Remediation:

This fix must be performed in vCenter.

From the vSphere Client, go to Administration >> Hosts and Clusters >> Select the cluster where the NSX Managers are deployed >> Configure >> Configuration >> VM/Host Rules.

Click "Add" to create a new rule.

Provide a name and select "Separate Virtual Machines" under Type.

Add the three NSX Manager virtual machines to the list and click "OK".

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	NMGR-4X-000007 (Manual)	☐	☐
1.2	NMGR-4X-000010 (Manual)	☐	☐
1.3	NMGR-4X-000012 (Manual)	☐	☐
1.4	NMGR-4X-000013 (Manual)	☐	☐
1.5	NMGR-4X-000014 (Manual)	☐	☐
1.6	NMGR-4X-000035 (Manual)	☐	☐
1.7	NMGR-4X-000038 (Manual)	☐	☐
1.8	NMGR-4X-000015 (Manual)	☐	☐
1.9	NMGR-4X-000039 (Manual)	☐	☐
1.10	NMGR-4X-000040 (Manual)	☐	☐
1.11	NMGR-4X-000041 (Manual)	☐	☐
1.12	NMGR-4X-000042 (Manual)	☐	☐
1.13	NMGR-4X-000043 (Manual)	☐	☐
1.14	NMGR-4X-000044 (Manual)	☐	☐
1.15	NMGR-4X-000052 (Manual)	☐	☐
1.16	NMGR-4X-000067 (Manual)	☐	☐
1.17	NMGR-4X-000068 (Manual)	☐	☐
1.18	NMGR-4X-000079 (Manual)	☐	☐
1.19	NMGR-4X-000087 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	NMGR-4X-000088 (Manual)	☐	☐
1.21	NMGR-4X-000093 (Manual)	☐	☐
1.22	NMGR-4X-000094 (Manual)	☐	☐
1.23	NMGR-4X-000096 (Manual)	☐	☐
1.24	NMGR-4X-000097 (Manual)	☐	☐
1.25	NMGR-4X-000098 (Manual)	☐	☐
1.26	NMGR-4X-000099 (Manual)	☐	☐
1.27	NMGR-4X-000102 (Manual)	☐	☐
1.28	NMGR-4X-000103 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
08-26-2025	1.0.0	Initial CIS Release