NETWORK DEVICE MANAGEMENT (NDM) SRG REVISION HISTORY

Version 4, Release 1

23 April 2021

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V4R1	- Network Device Management SRG, V3R4	- DISA migrated the Network Device Management SRG to a new content management system. The new content management system renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version number from V3R4 to V4R1. - SRG-APP-000149-NDM-000247- Added PKI Multifactor requirement. - SRG-APP-000175-NDM-000262 - Added PKI certificate requirement. - SRG-APP-000177-NDM-000263 - Added PKI account mapping requirement. - SRG-APP-000033-NDM-000212 - Updated requirement to support AAA broker.	23 April 2021
V3R4	- Network Device Management SRG, V3R3	- V-55073 - Removed SRG-APP-000353-NDM-000292. - V-55089 - Removed SRG-APP-000090-NDM-000222. - V-55157 - Removed SRG-APP-000109-NDM-000233. - V-55209 - Removed SRG-APP-000125-NDM-000241.	24 July 2020
V3R3	- Network Device Management SRG, V3R2	- V-55033, V-55073, V-55255 - Corrected rule title. - V-55055, V-55197 - Corrected rule title and check content. - V-100099 - Add generic requirement SRG-APP-000516-NDM-000317 for CCI 266.	24 April 2020
V3R2	- Network Device Management SRG, V3R1	- V-99017 - Added requirement to send log data to a syslog server. - V-99019 - Added requirement that OS must be supported by the vendor. - V-55299 - Revised check and fix and changed to CAT I. - V-55037, V-55039, V-55041, V-55061, V-55063, V-55065, V-55069, V-55071, V-55077, V-55103, V-55105, V-55107, V-55113, V-55117, V-55135, V-55139, V-55141, V-55145, V-55151, V-55175, V-55181, V-55185, V-55187, V-55189,	24 January 2020

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		V-55193, V-55207, V-55211, V-55213, V-55237, V-55247, V-55251, V-55253, V-55257, V-55259, V-55291, V-55293, V-55301, V-55303, V-55305, V-55311, V-80967 - Removed requirements.	
V3R1	- Network Device Management SRG, V2R14	- V-55055 - Added to the requirement to lock out account for 15 minutes. - V-55081 - Revised NTP synchronization intervals to within seconds (64 to 10024), not hours. - V-55083 - Removed as there is no such thing in the RFC 1305 or 5905 to specify offset values as to when to synchronize. - V-55087 - Removed requirement as there is no DoD list of auditable events. - V-55109 - Corrected rule title phrasing. - V-55153 - Corrected typo in check content. - V-55169 - Removed requirement as all admins need to see log data. - V-55177 - Operator class must be able to see error messages. - V-55195 - Removed requirement, which is redundant with SRG-APP-000190-NDM-000267. - V-55231 - Removed “different geographical regions” from rule title. - V-55255 - Removed bidirectional and added FIPS-140-2 to rule title and check/fix content. - V-55267 - Added FIPS-140-2 to rule title and check/fix content. - V-55269 - Corrected rule title phrasing. - V-55285 - Redundant with SRG-APP-000026-NDM-000208, SRG-APP-000027-NDM-000209, SRG-APP-000028-NDM-000210, and SRG-APP-000029-NDM-000211. - V-55289 - Removed as this is policy and not configurable. - V-55295 - Changed rule title from “generate audit log events” to “generate log records”. - V-55299 - Changed rule title to “The device must be configured to use an AAA server for	25 October 2019

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		authenticating users prior to granting administrative access." - V-55307 - Changed requirement to back up configuration after a change is made. - V-64001 - Corrected rule title phrasing and removed statement about setting the privilege level in the check content.	
V2R14	- Network Device Management SRG, V2R13	- Update SRG-APP-000175-NDM-000262 (V-55141) to clarify acceptance of DoD-approved CA certificates. - Add SRG-APP-000175-NDM-000350 (V-80967) to not accept revoked CA certificates. - Update SRG-APP-000175-NDM-000262 (V-55141) to CAT I severity level. - Update SRG-APP-000171-NDM-000258 (V-55131) to CAT I severity level. - Update SRG-APP-000172-NDM-000259 (V-55133) to CAT I severity level. - Update SRG-APP-000178-NDM-000264 (V-55149) to CAT I severity level. - Update SRG-APP-000033-NDM-000212 (V-55051) to CAT I severity level. - Update SRG-APP-000142-NDM-000245 (V-55101) to CAT I severity level. - Update SRG-APP-000148-NDM-000246 (V-55103) to CAT I severity level. - Update SRG-APP-000179-NDM-000265 (V-55153) to CAT I severity level. - Update SRG-APP-000190-NDM-000267 (V-55159) to CAT I severity level. - Update SRG-APP-000231-NDM-000271 (V-55171) to CAT I severity level. - Update SRG-APP-000340-NDM-000288 (V-55221) to CAT I severity level. - Update SRG-APP-000411-NDM-000330 (V-55265) to CAT I severity level. - Update SRG-APP-000412-NDM-000331 (V-55267) to CAT I severity level.	27 July 2018
V2R13	- Network Device Management	- Modify SRG-APP-000023-NDM-000205 (V-55037) to remove references to SV-69283r3.	26 January 2018

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
	SRG, V2R12	- Modify SRG-APP-000166-NDM-000254 (V-55119) to clarify conditions for password use. - Modify SRG-APP-000167-NDM-000255 (V-55121) to clarify conditions for password use. - Modify SRG-APP-000168-NDM-000256 (V-55123) to clarify conditions for password use. - Modify SRG-APP-000169-NDM-000257 (V-55125) to clarify conditions for password use. - Modify SRG-APP-000170-NDM-000329 (V-55127) to clarify conditions for password use. - Modify SRG-APP-000109-NDM-000233 (V- 55157) to clarify availability as an overriding concern. - Modify SRG-APP-000516-NDM-000334 (V-55295) to include control AU-12a and CCI-000169. - Modify SRG-APP-000149-NDM-000247 (V- 55105) to remove references to CAC and clarify MFA implementation. - Modify SRG-APP-000171-NDM-000258 (V- 55131) to include hashed representations of password as the preference, and deny the use of MD5.	
V2R12	- Network Device Management SRG, V2R11	- History for V2R7, change “V-55401”. STIG ID of SRG-APP-000025-NDM-000207) read “V-55041 in place of “V-55401”. - Added missing CCI to SRG-APP-000395-NDM-000347. Added CCI-001967.	27 October 2017
V2R11	- Network Device Management SRG, V2R10	- V-55153 - Added the requirement for both FIPS 140-2 validation and FIPS-approved algorithm to vulnerability discussion. - V-55265 - Included the requirement to use FIPS 140-2, SSHv2, and HMAC. - V-64001- Clarified requirement text to remove references to emergency account, which was missed in a previous update. Added audit of safe credentials to prevent tampering.	28 July 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		The signature of the auditor and the date of the audit should be stored. Root account should be disabled to ensure there is only one account as per the requirement.	
V2R10	- Network Device Management SRG, V2R9	- Modified V-55105 SRG-APP-000149-NDM-000247 - removed extra paragraph - This requirement also applies to the account of last resort and the root account only if non-local access via the network is enabled for these accounts (not recommended). - Removed STIG ID: SRG-APP-000023-NDM-000205 Rule ID: SV-69283r3_rule Vuln ID: V-55037.	04 May 2017
V2R9	- Network Device Management SRG, V2R8	- Updated V-55105, downgraded from CAT I to CAT II. Policy also now exempts the root and account of last resort from the network multi-factor authentication requirement. - Modified V-55107, policy now exempts the root and account of last resort from the local multi-factor authentication requirement.	28 April 2017
V2R8	- Network Device Management SRG, V2R7	- Modified V-55037 vulnerability discussion to provide an explanation of redundancy of authentication server. Previous discussion did not align well with requirement language.	28 April 2017
V2R7	- Network Device Management SRG, V2R6	- Modified V-55299 to use the term account of last resort and add root account reference. Reworded vulnerability discussion, check, and fix to clarify. - Modified V-55103 to use the term account of last resort and add root account reference. Reworded vulnerability discussion, check, and fix to clarify. - Modified V-55105 Update the severity level to CAT 1 finding when a local account of last resort does not use an approved multifactor authentication method. - Modified V-55175 to use the term account of last resort and add root account reference. Reworded vulnerability discussion, check, and fix to clarify. - Modified V-55113 to use the term account of last resort and add root account reference.	28 October 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		Reworded vulnerability discussion, check, and fix to clarify. - Modified V-55041 to use the term account of last resort and add root account reference. Reworded vulnerability discussion, check, and fix to clarify. - Modified V-55135 to use the term account of last resort and add root account reference. Reworded vulnerability discussion, check, and fix to clarify. - Modified V-55139 to use the term account of last resort and add root account reference. Reworded vulnerability discussion, check, and fix to clarify. - Modified V-55037 to use the term account of last resort and add root account reference. Reworded vulnerability discussion, check, and fix to clarify. - Modified V-55027 to add reference to account of last resort and add root account. Reworded vulnerability discussion, check, and fix to clarify. - Modified V-55187 to add reference to account of last resort and add root account. Reworded vulnerability discussion, check, and fix to clarify.	
V2R6	- Network Device Management SRG, V2R5	- Modified V-55255 to cover SNMP only. - Added V-68747 to cover NTP only.	22 July 2016
V2R5	- Network Device Management SRG, V2R4	- Modified V-55113; modified requirement to exclude the emergency administration account. - Modified V-55135; modified requirement to exclude the emergency administration account.	22 April 2016
V2R4	- Overview - Network Device Management SRG, V2R3	- Modified overview to better explain applicability. - Modified V-55127; modified requirement to provide correct value. - Modified V-55101; modified requirement to - make it specific to management protocols. - Modified V-55199; modified requirement to account for terminal sessions.	22 January 2016

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- Modified V-55059; modified requirement to account for terminal sessions. - Modified V-55211; modified requirement for clarity. - Modified V-55037; modified requirement for clarity. - Modified V-55299; modified requirement for clarity. - Modified V-55175; modified requirement to use the correct value. - Deleted V-55249; removed redundant requirement. - Added V-63997; added requirement to incorporate NET0240. - Added V-64001; added requirement to incorporate NET0440.	
V2R3	- Network Device Management SRG, V2R2	- Modified V-55175; Modified requirement for clarity; added exclusion for the emergency administration account. - Modified V-55089; Updated acronyms in requirement. - Modified V-55151; Updated acronyms in requirement. - Modified V-55177; Updated acronyms in requirement. - Modified V-55207; Updated acronyms in requirement. - Modified V-55237; Updated acronyms in requirement.	26 October 2015
V2R2	- Network Device Management SRG, V2R1	- Modified V-55033; Vulnerability Discussion, Check, and Fix changed to clarify requirement. - Modified V-55171; Vulnerability Discussion, Check, and Fix changed to clarify requirement. - Removed V-55241.	24 July 2015
V2R1	- Network Device Management SRG	- Initial Release.	20 October 2014