ACTIVE DIRECTORY DOMAIN STIG
REVISION HISTORY

Version 3, Release 1

01 November 2021

Developed by DISA for the DoD

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V3R1	- Active Directory Domain STIG V2R13	- DISA migrated the STIG to a new content management system, which renumbered all Groups (V-numbers) and Rules (SV-numbers). With the new Group and Rule numbers, DISA incremented the version number from V2R13 to V3R1. - AD.0008 - Updated Fix to highly recommend use of Microsoft's Local Administrator Password Solution (LAPS), and AO can approve other solutions.	01 November 2021
V2R13	- Active Directory Domain STIG	- V-92285 - Added requirement to prevent unconstrained delegation of computer accounts.	26 April 2019
V2R12	- Active Directory Domain STIG	- V-36436 -Removed requirement, addressed by PAW STIG. - V-78131 -Updated to clarify this applies to personnel user accounts, not service accounts.	25 January 2019
V2R11	- Active Directory Domain STIG	- V-36438 - Clarified to note query results require review to validate.	26 October 2018
V2R10	- Active Directory Domain STIG	- V-25841 - Removed requirement that defines frequency of reviews, out of scope of STIG. - V-36436 - Updated to reference the Windows Privileged Access Workstation (PAW) STIG for additional configuration. - V-43712, V-43713, V-43714 - Updated the link to the referenced NSA document. - V-78131 - Updated to clarify requirement applies to accounts from local domain. - The following requirements were removed, now addressed by the PAW STIG: V-36437, V-43710, V-43711, V-44058.	27 July 2018
V2R9	- Active Directory Domain STIG	- V-36438 - Corrected PowerShell query. Clarified use of LAPS and all local administrator accounts must be addressed. - V-78131 - Added requirement for domain level admin accounts to be members of the Protected Users group.	26 January 2018
V2R8	- Active Directory	- V-8548 - Removed Enterprise and Domain Admins - accounted for in other requirements.	27 January 2017

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
	Domain STIG	Moved Schema Admins to new requirement in Forest STIG. - V-8551 - Removed reference to Windows 2003 end of support. - V-25840 - Clarified requirement is for Directory Restore Mode Password (DSRM) annual password change. - Replaced the following with new requirement (V-72821) to roll hash for all smart card-enabled accounts: V-43649, V-43650, V-43651. - V-72821 - Added new requirement for smart card required for interactive logon (SCRIL) hash rolling.	
V2R7	- Active Directory Domain STIG	- Added Sections 1.6 Other Considerations and 1.7 Product Approval Disclaimer to the STIG Overview document. - V-8524 - Changed MAC references to RMF. - V-8525 - Changed MAC references to RMF. - V-8530 - Changed MAC references to RMF. - V-8540 - Added Fix details. - V-8547 - Added Fix details. - V-8553 - Added Fix details. - V-25385 - Changed MAC references to RMF. - V-36438 - Added LAPS as a solution for managing local administrator passwords. - V-43712 - Removed Windows 2003 references. - V-43713 - Removed Windows 2003 references. - V-43714 - Removed Windows 2003 references.	22 April 2016
V2R6	- Active Directory Domain STIG	- STIGs previously bundled in the Windows Server packages have been separated into individual packages (e.g., Member Server, Domain Controller, AD Domain, and AD Forest). - V-8538 - Trust - SID Filter Quarantining - Updated for clarification. - V-8551 - Domain Functional Level - Updated for clarification. - V-36436 - Dedicated Systems for Managing Active Directory - Updated for clarification.	23 January 2015

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
V2R5	- Active Directory Domain STIG	- Control Correlation Identifiers (CCIs) added to requirements. - V-53727 Domain Controllers Internet Access – added.	28 October 2014
V2R4	- Active Directory Domain STIG	- V-36436 Systems dedicated to managing Active Directory - Additional information added. - The following new requirements have been added to support Pass-the-Hash mitigations. - V-43648 Separate smart cards must be used for Enterprise Admin (EA) and Domain Admin (DA) accounts from smart cards used for other accounts. - V-43649 Enterprise Admin (EA) and Domain Admin (DA) accounts that require smart cards must have the setting Smart card is required for interactive logon disabled and re-enabled at least every 60 days. - V-43650 Administrative accounts for critical servers, that require smart cards, must have the setting Smart card is required for interactive logon disabled and re-enabled at least every 60 days. - V-43651 Other important accounts (VIPS and other administrators) that require smart cards must have the setting Smart card is required for interactive logon disabled and re-enabled at least every 60 days. - V-43652 Separate domain accounts must be used to manage public facing servers from any domain accounts used to manage internal servers. - V-43710 Systems used to manage Active Directory (AD admin platforms) must be Windows 7, Windows Server 2008 R2, or later versions of Windows. - V-43711 Separate domain administrative accounts must be used to manage AD admin platforms from any domain accounts used on, or used to manage, non-AD admin platforms.	25 April 2014

REVISION HISTORY			
Revision Number	**Document Revised**	**Description of Change**	**Release Date**
		- V-43712 Usage of administrative accounts must be monitored for suspicious and anomalous activity. - V-43713 Systems must be monitored for attempts to use local accounts to log on remotely from other systems. - V-43714 Systems must be monitored for remote desktop logons. - V-44058 Communications from AD admin platforms must be blocked, except with the domain controllers being managed. - V-44059 Windows service \ application accounts with administrative privileges and manually managed passwords, must have passwords changed at least every 60 days.	
V2R3	- Active Directory Domain STIG	- V-8521 Object Ownership Delegation - Changed Check Type to "Manual" in VMS. - V-8523 IDS Visibility of Directory VPN Data Transport - Changed Check Type to "Manual" in VMS. - V-8525 Directory Service Architecture DR Documentation - Changed Check Type to "Manual" in VMS.	24 January 2014
V2R2	- Active Directory Domain STIG	- V-36431 Enterprise Admins Group Members - new CAT I. - V-36432 Domain Admins Group Members - new CAT I. - V-36433 Domain Member Server Administrators Group Members - new CAT II. - V-36434 Domain Workstation Administrators Group Members - new CAT II. - V-36435 Delegation of Privileged Accounts - new CAT I. - V-36436 Dedicated Systems for Managing Active Directory - new CAT II. - V-36437 Block Internet Access for Dedicated Systems Used for Managing Active Directory- new CAT II. - V-36438 Unique Passwords for all Local Administrator Accounts - new CAT II.	29 March 2013