Devolutions

HIPAA SECURITY RULE ASSESSMENT

April 2022

INTRODUCTION

Devolutions Server

Devolutions Server (DVLS) is a full-featured shared account and password management solution with built-in privileged access components. It deploys rapidly, implements easily, and delivers the core features of a comprehensive PAM solution. Devolutions Server is designed to meet the ever-expanding security requirements of SMBs. It securely stores business credentials, allowing teams to share access with authorized users.

Remote Desktop Manager

Remote Desktop Manager (RDM) centralizes all remote connections on a single platform that is securely shared between users and across the entire team. With support for hundreds of integrated technologies — including multiple protocols and VPNs — along with built-in enterprise-grade password management tools, global and granular-level access controls, and robust mobile apps to complement desktop clients for Windows and Mac, RDM is a Swiss Army knife for remote access. RDM empowers IT departments to drive security, speed and productivity throughout the organization, while reducing inefficiency, cost and risk. RDM can be configured to act as a client for DVLS.

HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a United States federal statute that regulates the privacy and the security of electronic Personal Health Information (ePHI). Covered Entities must implement security controls to protect ePHI that are consistent with the requirements of HIPAA's Security Rule.

HIPAA's Security Rule describes controls that apply to Covered Entities and to Business Associates who process ePHI on their behalf. DVLS and RDM do not process ePHI but may be used to grant access to systems containing ePHI. Following an analysis of the applicability of the Security Rule's requirements, some controls have been carved out of this assessment as the do not apply to DVLS and RDM's service offering.

HIPAA's Security Rule is not prescriptive: security control requirements refer to current industry standards without providing specifications. Security controls described herein reference the United States Department of Health and Human Services' Security Rule guidelines.

Object

This report assesses whether DVLS and RDM's security controls are consistent with applicable industry standards, as defined by the National Institute of Standards and Technology Special Publication 800-53 r.5 Security and Privacy Controls for Information Systems and Organizations (NIST-SP-800-53r5).

Remote Desktop Manager

	Control requirement - Reference	Validation
Administrative Safeguards		
	Information System Activity Review (R) - 164.308(a)(1)(ii)(D)	Correlation of user activity logs with information from targeted systems facilitates improves review capabilities and may be used as evidence. Content of records is consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability.
	Authorization and/or Supervision (A) Ð 164.308(a)(3)(ii)(A)	Authorization is managed via RDMÕ user and user group permissions, which requires authorization be granted to access information assets. Authorization and supervision controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control and 3.3 Audit and Accountability.
	Access Authorization (A) - 164.308(a)(4)(ii)(B)	Access authorization controls are robust and facilitate segregation of duties and compliance with the least privilege principle. Vault-based access and user group permissions enable the implementation of role-based access policies. Dual authorization and single use credentials are robust measures of access enforcement. Access authorization controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Access Establishment and Modification (A) - 164.308(a)(4)(ii)(C)	Access establishment is protected by three layers of security controls: access requires users to be authenticated; access requires users to have permission to use credentials; access requires users to be granted rights to the vault hosting the credentials. Access establishment and modification controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Log-In Monitoring (A) - 164.308(a)(5)(ii)(C)	RDM captures event logs that include log-in monitoring. Log-in monitoring controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability.
	Password Management - 164.308(a)(5)(ii)(D)	RDM facilitates password management enforcement. Shared password is managed by system administrators and permissions are controlled at the user or user group level. Password management controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.
Technical Safeguards		
	Unique User Identification (R) - 164.312(a)(2)(i)	RDM ensures that users can be uniquely identified by correlating account identifiers and user activity events. User identification controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.
	Automatic Logoff (A) - 164.312(a)(2)(iii)	Automatic log-off controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.

	Encryption and Decryption (A) - 164.312 (a)(2)(iv)	RDM uses cryptographic measures to protect data by utilizing industry standard protocols that encrypt data at rest and hash highly confidential values. Encryption and decryption controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.18 System and Communications Protection and 3.19 System and Information Integrity.
	Audit Controls - 164.312(b)	Audit controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability.
	Integrity - 164.312(c)(1)	RDM provides basic integrity control functions. Restricted write functions prevent modification and change logs document change events, but RDM does not provide versioning or data restoration functionality. Integrity controls are partially consistent with industry standards, as defined by NIST-SP-800-53r5 3.19 System and Information Integrity.
	Person or Entity Authentication - 164.312(d)	RDM enforces entity authentication in a layered manner: Users must be authentica ted to access the RDM client. RDM clients are identified with license numbers and hardware IDs. To access integrated systems, users must be granted permissions to access the credentials. Authentication controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.
	Transmission Security - 164.312(e)(1) R	DM uses cryptographic measures to protect data by utilizing industry standard ciphers that encrypt data in transit. Transmission security controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.18 System and Communications Protection and 3.19 System and Information Integrity .

	Control requirement - Reference	Validation
Administrative Safeguards		
	Risk Analysis (R) - 164.308(a)(1)(ii)(A)	Risk analysis, reporting, and notification features are consistent with industry standards, as defined by NIST SP 800-53r5 Ð3.16 Risk Assessment.
	Information System Activity Review (R) - 164.308(a)(1)(ii)(D)	Correlation of user activity logs with information from targeted systems facilitates improves review capabilities and may be used as evidence. Content of records is consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability.
	Assigned Security Responsibility - 164.308(a)(2)	Assignment of security responsibilities within the platform facilitates information security program management by notifying and informing relevant personnel of potential security incidents. Security responsibility assignment features are consistent with industry standards, as defined by NIST-SP-800-53r5 3.13 Program Management.
	Authorization and/or Supervision (A) Ð 164.308(a)(3)(ii)(A)	Authorization is managed via DVLSÕuser and user group permissions, which requires authorization be granted to access information assets. Supervision is managed via DVLSÕuser activity event logs. Authorization and supervision controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control and 3.3 Audit and Accountability.
	Workforce Clearance Procedure (A) - 164.308(a)(3)(ii)(B)	Access to information is managed via user and user group permissions. User accounts can be synchronised with Active Directory or Azure AD to streamline account provisioning in accordance with clearance procedures. Account provisioning logs can be audited. Workforce clearance controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Termination Procedures (A) - 164.308(a)(3)(ii)(C)	User accounts can be synchronised with Active Directory or Azure AD to streamline account termination in accordance with termination procedures. Termination controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Access Authorization (A) - 164.308(a)(4)(ii)(B)	Access authorization controls are robust and facilitate segregation of duties and compliance with the least privilege principle. Vault-based access and user group permissions enable the implementation of role-based access policies. Dual authorization and single use credentials are robust measures of access enforcement. Access authorization controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.

	Access Establishment and Modification (A) - 164.308(a)(4)(ii)(C)	Access establishment is protected by three layers of security controls: access requires users to be authenticated; access requires users to have permission to use credentials; access requires users to be granted rights to the vault hosting the credentials. Use of shared credentials are logged as user activity events. Access modification requires administrative permissions and are logged as system events. Access establishment and modification controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Log-In Monitoring (A) - 164.308(a)(5)(ii)(C)	DVLS captures event logs that include lo g-in monitoring. Events logs are access ible by administrative personnel and can be audited or presented as a report. Log -in monitoring controls are consistent with indu stry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability.
	Password Management - 164.308(a)(5)(ii)(D)	DVLS facilitates password management enforcement. Shared password is managed by system administrators and permissions are controlled at the user or user group level. Password management controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.

	Response and Reporting (R) - 164.308(a)(6)(ii)	DVLS facilitates the correlation of security incident information with other systems. Audit logs are sufficiently detailed to allow for correlation with event logs from other systems and reporting functions draw attention to potential incidents. Response and reporting controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.8 Incident Response.
	Data Backup Plan (R) - 164.308(a)(7)(ii)(A)	DVLS provides industry standard backup functions that can be configured to meet the needs of a Covered Entity's contingency plan. Data backup controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability, 3.6 Contingency Planning, and 3.18 System and Communications Protection.
Physical Safeguards		
	Data Backup and Storage (A) - 164.310(d)(2)(iv)	DVLS provides industry standard backup functions that can be configured to meet the needs of a Covered Entity's contingency plan. Data backup controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability, 3.6 Contingency Planning, and 3.18 System and Communications Protection.
Technical Safeguards		
	Unique User Identification (R) - 164.312(a)(2)(i)	DVLS ensures that accounts are unique, and that users can be properly identified and authenticated. User identification controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.
	Automatic Logoff (A) - 164.312(a)(2)(iii)	Automatic log-off controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.

	Encryption and Decryption (A) - 164.312(a)(2)(iv)	DVLS uses cryptographic measures to protect data by utilizing industry standard protocols that encrypt data at rest and hash highly confidential values. Encryption and decryption controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.18 System and Communications Protection and 3.19 System and Information Integrity.
	Audit Controls - 164.312(b)	Audit controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability.
	Integrity - 164.312(c)(1) D	VLS provides basic integrity control functions. Restricted write functions prevent modification and change logs document change events, but DVLS does not provide versioning or data restoration functionality. Integrity controls are partially consistent with industry standards, as defined by NIST-SP-800-53r5 3.19 System and Information Integrity.
	Person or Entity Authentication - 164.312(d)	DVLS enforces entity authentication in a layered manner: To access DVLS, users must first be authenticated. To access integrated systems, users must be granted permissions to access the credentials. Authentication controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.
	Transmission Security - 164.312(e)(1) D	VLS uses cryptographic measures to protect data by utilizing industry standard ciphers that encrypt data in transit. Transmission security controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.18 System and Communications Protection and 3.19 System and Information Integrity.