Quest Recovery Manager for Active Directory
10.3.2

Security Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

20 Enterprise, Suite 100

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Updated – March 2025

Contents

Introduction

This security guide provides information about the Quest® Recovery Manager for Active Directory 10.3.2 release.

Managing information system security is a priority for every organization. In fact, the level of security provided by software vendors has become a differentiating factor for IT purchase decisions. Quest strives to meet standards designed to provide its customers with their desired level of security as it relates to privacy, confidentiality, integrity, and availability. This document describes the security features of Quest® Recovery Manager for Active Directory . It reviews access control, protection of customer data, secure network communication, cryptographic standards and more.

About Quest® Recovery Manager for Active Directory 10.3.2

Recovery Manager for Active Directory enables fast, online recovery. Comparison reports highlight what objects and attributes have been changed and deleted in Active Directory enabling efficient, focused recovery at the object or attribute level. Accurate backups and a quicker recovery enable you to reduce the time and costs associated with AD outages and reduce the impact on users throughout your organization.

Recovery Manager for Active Directory is based on patented technology.

It is crucial for any modern business to maintain the availability of its network-computer environment at all times. Unplanned downtime caused by a disastrous event, such as a directory service malfunction, can severely disrupt the operation of a business. Therefore, business-critical infrastructures demand the ability to recover failed systems and services in the shortest possible time.

Recovery Manager for Active Directory (RMAD) employs advanced technologies to minimize the downtime caused by the corruption or improper modification of Active Directory®, Active Directory Lightweight Directory Services (AD LDS) (ADAM), and Group Policy data. This product allows for automatic backup, and fast remotely managed recovery of data stored in Active Directory.

Recovery Manager for Active Directory (RMAD) dramatically reduces the time required to restore Active Directory®, AD LDS (ADAM), and Group Policy data. This improves the availability of corporate networks and reduces network downtime. Given that the time required to recover Active Directory® using a conventional full-backup tool is typically a few hours, Recovery Manager for Active Directory offers huge savings on time, productivity, and administrative overhead.

Later in this document, we will use Recovery Manager for Active Directory (or RMAD for short) to refer to Recovery Manager for Active Directory Disaster Recovery Edition, except in cases where we need to explicitly distinguish between the editions.

Architecture Overview

Recovery Manager for Active Directory uses a client-server model with backup and restore agents installed on domain controllers and the Recovery Manager consoles installed on a Windows server. This model is used to orchestrate both backup and recovery operations.

The product components include:

- Backup agent
- Forest Recovery agent
- Recovery Manager Console (MMC)
- Forest Recovery Console
- PowerShell API

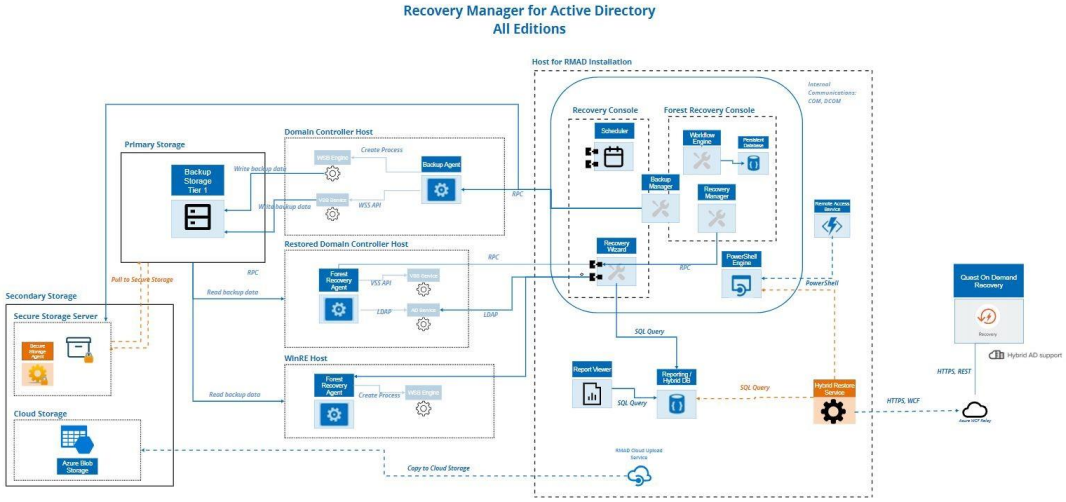

Figure 1: High-Level Architecture

NOTE Some components in figure, may not apply to your edition of Recovery Manager for Active Directory. Refer to User Guide for your edition.

Overview of Data Handled by RMAD

Recovery Manager for Active Directory manages and protects critical data in an Active Directory (AD) environment, focusing on ensuring the availability and integrity of AD components in case of disasters or failures. The types of data handled by Recovery Manager include:

- Active Directory backups, which contain the DIT database, SYSVOL, and registry hives
- AD LDS (ADAM) backups

Location of Customer Data

All data, application logs and computations are performed on server(s) provided by the customer.

Backups created with Recovery Manager for Active Directory can be stored in multiple locations. Primary storage of backups allows backup files to be saved on a distributed network or on selected computers with physically restricted access. Recovery Manager considers these locations as primary storage, referred to as Tier 1 storage.

Primary Storage (Tier 1)

Recovery Manager for Active Directory provides options for primary storage in both local and remote locations. Local storage refers to storage on the Recovery Manager console computer, while remote storage refers to storage on the backed-up domain controller or other remote servers on network shares. These locations are considered remote because they are not on the Recovery Manager console computer.

For both local and remote storage locations, a primary backup path can be provided, along with an alternate backup path.

Primary storage is used for saving the original backup files to a safe location. For primary storage, the backup agent creates the backup file, compresses the data, and then saves the file to the configured storage locations. In the diagram below, refer to lines numbered 1 to view the process that is followed to save the backup file to primary storage locations. The RPC protocol is used to save backup files to the console computer. For saving to remote storage locations, the SMB protocol is used.

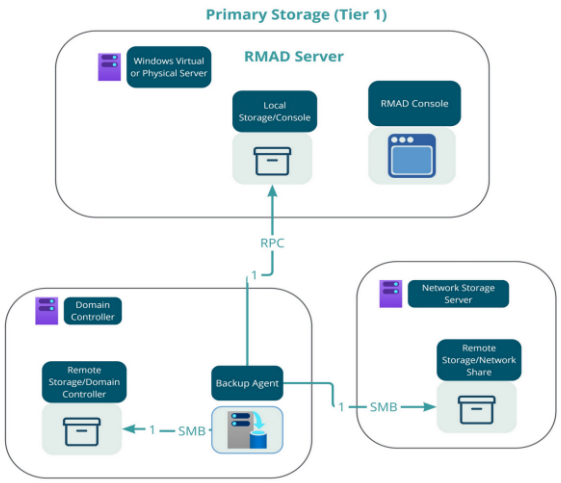

Figure 2: Primary Storage for Backups

The figure above illustrates how Recovery Manager for Active Directory creates and saves backup files to primary storage locations.

NOTE Some components in figure, may not apply to your edition of Recovery Manager for Active Directory. Refer to User Guide for your edition.

Privacy and Protection of Customer Data

Recovery Manager for Active Directory provides protection for customer sensitive data both in transit and at rest.

Recovery Manager for Active Directory uses encryption algorithms to do the following:

- Encryption of backup files
- Encryption of data (passwords, scripts) in the Recovery Manager configuration database (rmad.db3)
- Encryption of credentials for AD and AD LDS (ADAM) instances
- Encryption of reporting database credentials
- Encryption of password in email settings
- Encryption of password for persistence database
- Encryption of passwords for configuration backups

Also, Recovery Manager uses signing algorithms for communication with the following components:

- Hybrid Connect Service – data signing is done in communications via WCF transport security.
- Agents – data signing is done in communications via RPC transport security, including RPC over Schannel mode.

Network Communications

The architectural diagram of the product with all the components is shown in Figure 1. Figures 5 and 6 provide information about the communication ports required to work with Recovery Manager for Active Directory.
This section provides information about the communication ports required to work with Recovery Manager for Active Directory.

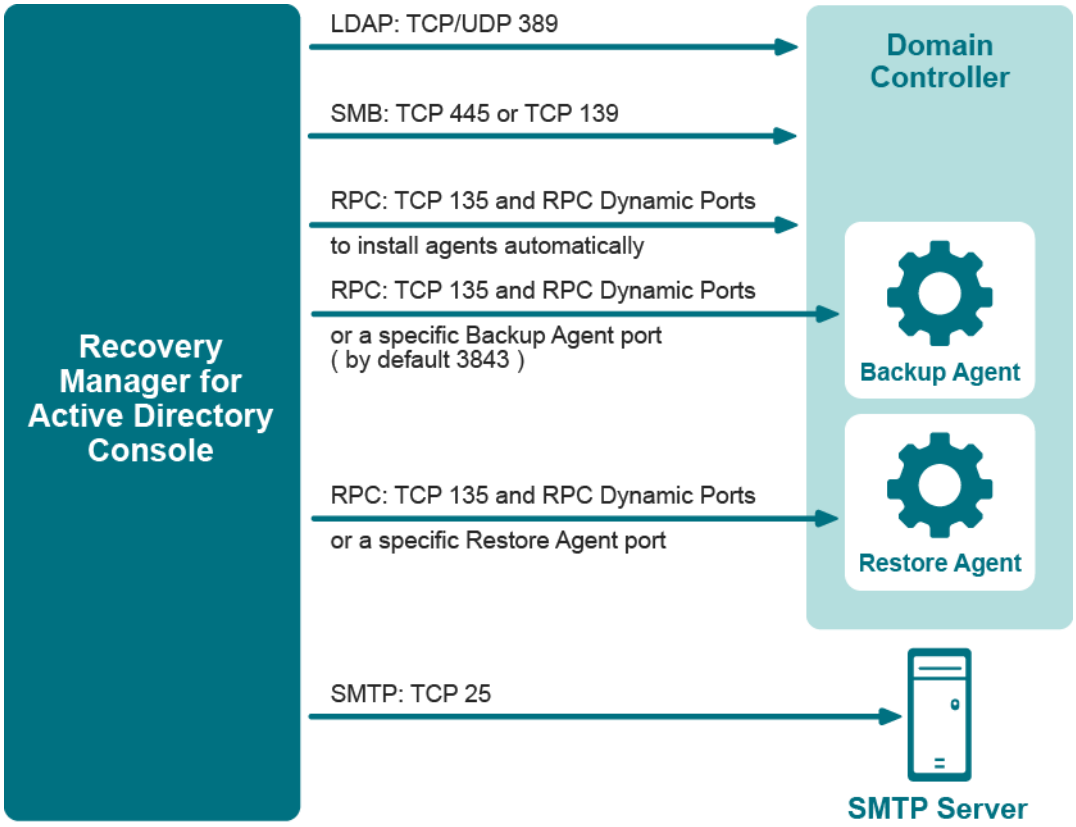

Figure 5: Ports used by Recovery Manager for Active Directory Console to work with Active Directory

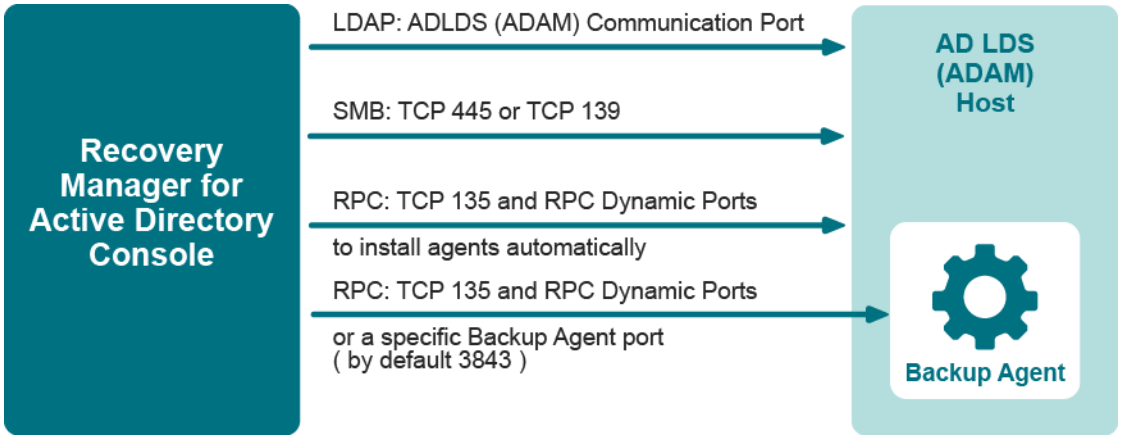

Figure 6: Ports used by Recovery Manager for Active Directory Console to work with AD LDS (ADAM)

Authentication of Users and Services

Recovery Manager for Active Directory relies upon Windows Authentication and Active Directory group membership to authenticate users.

In scenarios where Windows Authentication may be unavailable due to Active Directory failures, Recovery Manager uses certificate-based SCHANNEL authentication to establish secure connection between Forest Recovery Console and the Forest Recovery Agent.

Role Based Access Control

Currently, Recovery Manager for Active Directory does not allow granular permission delegation for product settings and operations. Any locally logged-on accounts with local administrative rights will be able to gain control over the entire Recovery Manager functionality.

This requires ensuring that the security level for access to the machine with the Recovery Manager console is no lower than the security level for access to other parts of the Active Directory infrastructure.

FIPS 140-2 compliance

Backup encryption

RMAD allows backups to be encrypted and protected with a password, to prevent unauthorized access.

For Active Directory backup encryption, the product uses FIPS 140-2 validated AES-256 algorithms.

Table 1: Encryption of Backup Files

Cryptographic usage	Cryptographic algorithm	Cryptographic parameters	Third-Party libraries	FIPS 140-2 Certificates Windows Server 2016
Symmetric encryption of bulk data	AES256	Key Encryption Key: CryptDeriveKey - CALG_AES_256 AES256 Mode: CRYPT_MODE_CBC Salt: CryptGenRandom - 16	CryptoAPI (crypt32.lib) WMI: Win32_EncryptableVolume class	**AES:** #4064, #5295 and #C2046
Asymmetric encryption of bulk data	RSA	RSA Key Pair: CryptAcquireContext - PROV_RSA_AES CryptGenKey - CALG_RSA_KEYX	CryptoAPI (crypt32.lib)	**RSA:** #2192, #2193, #2195, #2833, #2834, #2847, #C2046 and #C2065
Key Derivation	PDKDF2	Key Size = SHA512 ::BCryptOpenAlgorithm Provider - BCRYPT_SHA512_ALGORITHM, BCRYPT_ALG_HANDLE_HMAC_FLAG BCryptDeriveKeyPBKDF2 – iterations used meet 600,000 minimum requirement	Cryptography Next Generation API (bcrypt.lib)	**PBKDF:** Vendor affirmed

Table 2: Encryption of Forest Recovery Project Files

Cryptographic usage	Cryptographic algorithm	Cryptographic parameters	Third-Party libraries	FIPS 140-2 Certificates Windows Server 2016
Symmetric encryption of bulk data	AES256	Key Encryption Key: CryptDeriveKey - CALG_AES_256 AES256 Mode: CRYPT_MODE_CBC Salt: CryptGenRandom - 32	System.Security.Cryptography.Algorithms.dll System.Security.Cryptography.Csp.dll System.Security.Cryptography.Primitives.dll mscorlib.dll netstandard.dll	**AES:** #4064, #5295 and #C2046
Key Derivation	PDKDF2	Key Size = SHA512 PaddingMode.PKCS7 Rfc2898DeriveBytes - iterations used meet 600,000 minimum requirement	System.Security.Cryptography.Algorithms.dll System.Security.Cryptography.Csp.dll System.Security.Cryptography.Primitives.dll mscorlib.dll netstandard.dll	**PBKDF:** Vendor affirmed

Table 3: Encryption of Credentials

Cryptographic usage	Cryptographic algorithm	Cryptographic parameters	Third-Party libraries	FIPS 140-2 Certificates Windows Server 2016
Symmetric encryption of secrets	AES256	DPAPI using CRYPTPROTECT_LOCAL_MACHINE flag, AES256-CBC algorithm Hash – SHA512 Random password - 16 bytes	CryptoAPI (crypt32.lib) DPAPI (crypt32.lib)	**AES:** #4064, #5295 and #C2046

Table 4: Communication

Cryptographic usage	Cryptographic algorithm	Cryptographic parameters	Third-Party libraries	FIPS 140-2 Certificates Windows Server 2016
Communication	WCF TCP Transport Security,RPC over Schannel	System.Net.Security. ProtectionLevel. EncryptAndSign; RPC_C_AUTHN_LEVEL_PKT_PRIVACY	bcrypt.dll or bcryptprimitives.dll	#2937
Communication	SSL TLS 1.2	Negotiated by GSS (RPC over Schannel)	Microsoft.Bcryptprimitives.dll or Bcrypt.dll	#2937

Recovery Manager for Active Directory has undergone a Quest internal Self-Affirmation process to confirm that all cryptographic usage relies exclusively on Third-Party FIPS 140-2 validated modules.

More information:

- Microsoft and FIPS: https://www.microsoft.com/en-us/trustcenter/compliance/fips
- Microsoft FIPS backgrounder: https://aka.ms/fips-backgrounder

SDLC and SDL

The Recovery Manager for Active Directory team follows a strict Quality Assurance cycle.

- Access to source control and build systems is protected by domain security, meaning that only employees on Quest's corporate network have access to these systems. Therefore, should a developer leave the company, this individual will no longer be able to access source control and build systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before check in.

In addition, the Recovery Manager for Active Directory team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices.
- Threat modeling.
- OWASP guidelines.
- Regularly scheduled static code analysis is performed on regular basis.

- Regularly scheduled vulnerability scanning is performed on regular basis.
- Recovery Manager for Active Directory has been validated in a Secure Technical Implementation Guidelines (STIG) environment. See Security Technical Implementation Guides (STIGs) for more information.

Recovery Manager for Active Directory developers go through the same set of hiring processes and background checks as other Quest employees.

Customer Measures

Recovery Manager for Active Directory security features are only one part of a secure environment. Customers should follow their own security best practices when deploying Recovery Manager for Active Directory within their environment.

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

Third-Party Contributions

This product contains the third-party components listed below. For third-party license information, go to https://www.quest.com/legal/third-party-licenses.aspx. Source code for components marked with an asterisk (*) is available at http://opensource.quest.com.

List of third-party contributions

Component	License or acknowledgment
7-ZIP 19.0	Copyright 1999-2019 Igor Pavlov Copyright 2015-2016 Apple Inc. All rights reserved.
AeroWizard 2.2.3	MIT 1.0
AWSSDK.Core 3.7.9.2	Apache 2.0
AWSSDK.S3 3.7.8.12	Apache 2.0
Azure.Core 1.45.0	MIT Template 2020
Azure.Core.Amqp 1.3.1	MIT Template 2020
Azure.Messaging.ServiceBus 7.18.4	MIT 1.0
Azure.Storage.Blobs 12.23.0	Template 2020
Azure.Storage.Common 12.22.0	MIT Template 2020
Boost 1.72.0	Boost 1.0
EntityFramework 6.4.4	Apache 2.0
DiscUtils 1.15.1	DiscUtils Kenneth Bell N/A
Fody 4.2.1	MIT N/A
FontAwesome.WPF 4.7.0.9	MIT N/A
Group Controls 1.8	Apache 2.0 Copyright Notice - Group Controls 1.5.3
Microsoft .Net Framework 4.8	Microsoft .Net Framework 4.8
Microsoft.Azure.Amqp 2.6.9	MIT Template 2020
Microsoft.Bcl.AsyncInterfaces 9.0.2	MIT Template 2020
Microsoft.Dism 2.0.20	MIT N/A
Microsoft.Extensions.DependencyInjecttion.Abstractions 9.0.2	MIT Template 2020
Microsoft.Extensions.Logging.Abstractions 9.0.2	MIT Template 2020
Microsoft.PowerShell.3.ReferenceAssemblies 1.0.0	MIT N/A
Microsoft.PowerShell.5.ReferenceAssemblies 1.1.0	MIT N/A
Microsoft.SqlServer.TransactSql.ScriptDom.dll 12.0.1	Microsoft Component Copyright 2002
Microsoft.SqlServer.Types 12.0.5000.0	MIT
Microsoft.Xaml.Behaviors.Wpf 1.1.19	MIT N/A

Component	License or acknowledgment
MinHook 1.3.2.1	BSD - MinHook 1.0 Copyright 2009 Tsuda Kageyu All rights reserved.
MinHook 1.3.3	BSD - MinHook 1.0 Copyright 2009 Tsuda Kageyu All rights reserved.
Newtonsoft.Json 13.0.3	MIT Template 2020
PropertyChanged.Fody 2.6.1	MIT N/A
RazorEngine 3.10.0	Apache 2.0
SQLiteCodeFirst 1.7.0.34	Apache 2.0
SSH.Net 2024.0.0 2024.0.0	MIT N/A
System.Buffers 4.6.0	MIT N/A
System.ClientModel 1.3.0	MIT Template 2020
System.Diagnostics.DiagnosticSource 9.0.2	MIT Template 2020
System.IO.Hashing 6.0.0	MIT Template 2020
System.IO.Pipelines 9.0.2	MIT Template 2020
System.Management.Automation 6.2.3	MIT Template 2020
System.Memory 4.5.5	License: MIT 1.0
System.Memory.Data 9.0.2	License: MIT 1.0
System.Numerics.Vectors 4.6.0	LIcense: MIT 1.0
System.Runtime.CompilerServices.Unsafe 6.1.0	License: MIT Template 2020
System.Text.Encodings.Web 9.0.2	MIT Template 2020
System.Text.Json 9.0.2	MIT Template 2020
System.Threading.Channels 9.0.2	MIT Template 2020
System.Threading.Tasks.Extensions 4.6.0	MIT 1.0
System.ValueTuple 4.5.0	MIT 1.0
TaskScheduler 2.8.18	MIT
Task Scheduler Managed Wrapper 2.8.18	MIT N/A
TimeSpan Helper Library 2.2	New BSD N/A
Windows Installer XML Toolset (aka WiX) 3.14	Microsoft Reciprocal License (MS-RL) N/A
ZLib 1.1.4	zlib 1.2.3 Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product.