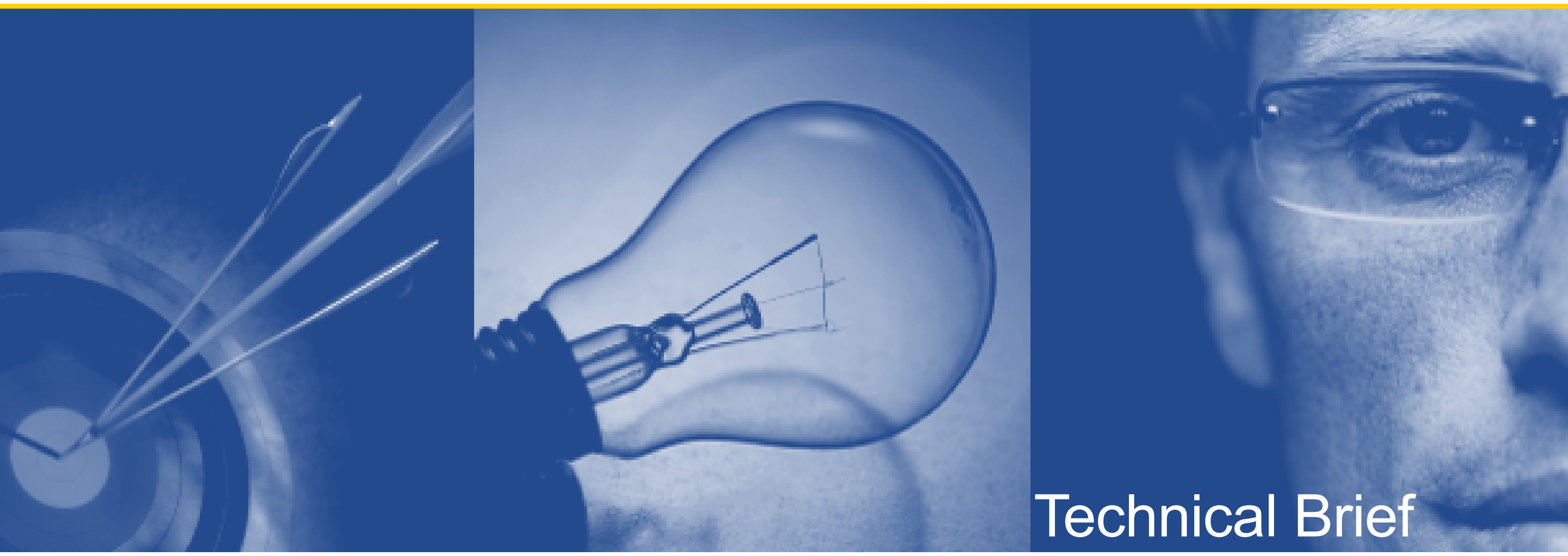
Security Guide for ActiveRoles Server 6.1

Written by
Einar Mykletun, Ph.D
Security and Compliance Architect
Quest Software, Inc.



Technical Brief

WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
e-mail: info@quest.com

Please refer to our Web site (www.quest.com) for regional and international office information.

Updated—September 2009

CONTENTS

INTRODUCTION

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 Software strives to meet standards designed to provide its customers with their desired level of security, whether it relates to privacy, authenticity and integrity of data, availability, or protection against malicious users and attacks.

This document describes the security features of Quest ActiveRoles Server 6.1. It reviews access control, protection of customer data, secure network communication, and more. There is also an appendix that describes how ActiveRoles Server's security features meet the NIST's recommended federal information security standards as detailed in the Federal Information Security Management Act (FISMA).

ABOUT ACTIVEROLES SERVER

The following image provides a high-level view of ActiveRoles Server.

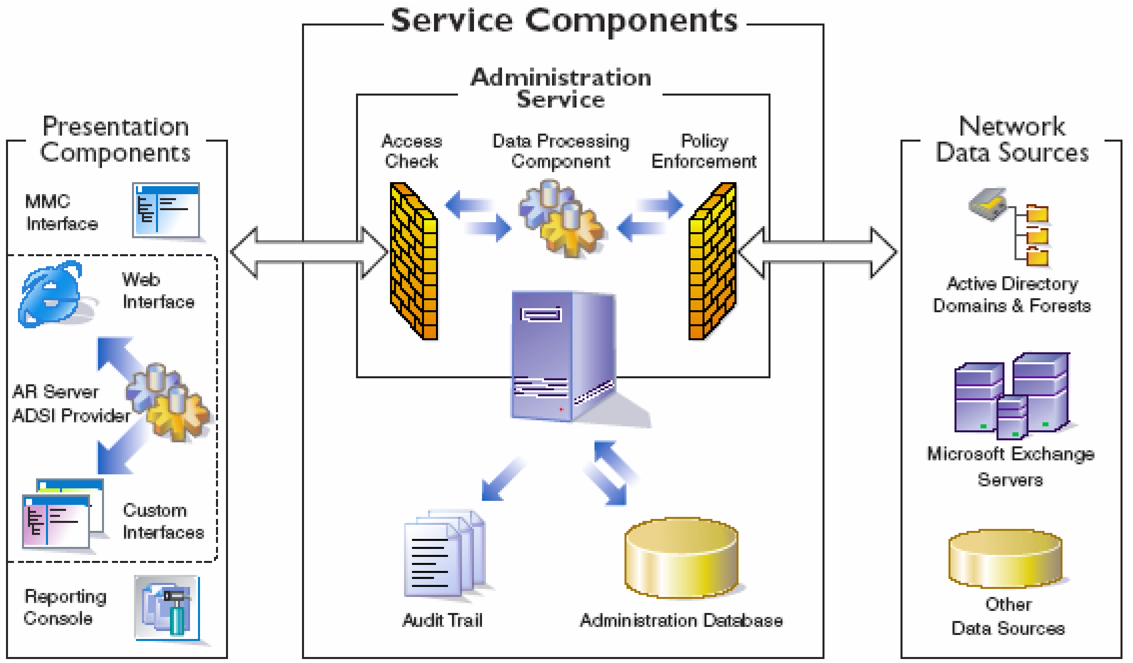


Figure 1 Overview of ActiveRoles Server and its three functional layers: presentation components, service components, and network data sources.

The service components provide client interfaces with controlled access to the network data sources such as Active Directory, Microsoft Exchange 2000/2003/2007 servers, and other business databases. When an operation request from a client is received, the service:

- Checks whether the client has sufficient permissions to perform the requested operation (access check).
- Ensures that the requested operation does not violate the corporate policies (policy enforcement).
- Performs all actions required by corporate policies, before committing the request (policy enforcement).
- Issues operating system function calls to perform the requested operation on network data sources.
- Performs all actions required by corporate policies, after the request is processed by the operating system (policy enforcement).

The service then generates an audit trail of all operations performed or attempted with ActiveRoles Server. Directory change tracking reports are based on this trail.

The administration database is used to store information about all permission and policy settings, as well as additional data that relates to the ActiveRoles Server configuration.

SECURITY FEATURES IN ACTIVEROLES SERVER

The following sections describe the security features provided by ActiveRoles Server.

Encryption of Passwords

ActiveRoles Server stores the passwords for the following accounts that are created during installation:

- *Administration service account* Allows the administrator to log on to the managed domain (requires sufficient privileges)
- *SQL Server account* Establishes a connection to the SQL Server (account must be a member of the *sysadmin* role on the SQL Server); the user name and password are only stored if user authentication is enforced when ActiveRoles Server connects to the SQL Server
- *User account on a managed domain* Enables administrators to use a different account to manage the domain
- *ActiveRoles Server MMC account – "Connect As"* Specifies an optional account that can be used to connect to the administration service
- *ActiveRoles Server Collector account (by schedule)* Connects to the collector processes

All passwords are encrypted automatically by Microsoft Windows or ActiveRoles Server. The *Administration Service* account's password is encrypted by Windows when ActiveRoles Server calls the `CreateService` Windows function. Encryption of the *Collector* account's password is also handled automatically by Windows, and ActiveRoles Server configures the account information by calling `IScheduledWorkItem::SetAccountInformation` function.

ActiveRoles Server uses the Windows Data Protection API (DPAPI) to encrypt the passwords of the *SQL Server* and *MMC – "Connect As"* accounts by calling the `CryptoProtectData` function. DPAPI uses the 3DES encryption algorithm in CBC mode. The SQL Server account's password is encrypted under the machine specific key (`CRYPTPROTECT_LOCAL_MACHINE = True`), while the MMC – "Connect As" account's password is encrypted under the user specific key (`CRYPTPROTECT_LOCAL_MACHINE = False`).

ActiveRoles Server protects the *user account's* password by encrypting it under one of the following symmetric key encryption algorithms: RC2 and AES (Advanced Encryption Standard). RC2 can be configured to use 128-bit keys while AES can use both 128- and 256-bit keys, and both algorithms operate in CBC mode (cipher block chaining). An ActiveRoles Server administrator can choose which encryption algorithm to use via a configuration file. The cryptographic provider used by ActiveRoles Server is either "Microsoft Enhanced Cryptographic Provider" or "Microsoft RSA and AES Cryptographic Provider", which are both part of the Microsoft *Crypto API* (CAPI). The choice depends upon the version of Microsoft Windows on which ActiveRoles Server is installed, and upon the choice of RC2 or AES. RC2 is currently the default algorithm used.

Support for the symmetric key encryption algorithm RC4 (with 40-bit keys) was introduced in ActiveRoles Server version 5.X but is not supported in version 6.0 and will not be supported in future releases. There is one exception: when customers upgrade from ActiveRoles Server 5.X, RC4 will remain the default encryption algorithm. We recommend that these customers switch to using the FIPS 140-2 approved AES encryption algorithm.

All password entries are masked with asterisks to prevent bystanders from observing the typed passwords on the screen.

Cryptographic Key Management

ActiveRoles Server uses the Windows *Data Protection API* (DPAPI) to protect the symmetric encryption key used to encrypt the *User Account's* passwords. The DPAPI encryption keys are generated and protected by the Windows operating system. ActiveRoles Server uses two encryption keys. The first is the *replication group session key* (RGSK) which is the symmetric 3DES-192 (by default), AES-128 or AES-256 key used to encrypt the password. The second key is a *machine specific 2048-bit RSA* key. The public RSA key encrypts RGSK and the resulting ciphertext is stored in the ActiveRoles Server administration database. The RSA key is then protected by Windows DPAPI and stored in the operating system's registry. It can only be accessed by administrators of the machine where ActiveRoles Server is installed.

All encryption keys are generated during product installation with the `CryptGenKey()` function in Microsoft's Cryptographic API. It is also possible for customers to import their own RGSK keys. ActiveRoles Server auditing and logging functions are configured not to include encryption keys in their output.

The RGSK key can be exported to a file during the installation of the first administration service in the replication group. The exported session key can optionally be protected with a password. In environments where multiple ActiveRoles Server services use the same administration database, the RGSK is distributed to other servers by encrypting it under their (public) RSA keys.

Authentication of ActiveRoles Server Users

Users authenticate to the administration service through Windows integrated authentication. Both Kerberos and NTLM authentication protocols are supported, with Kerberos as the default. There is also an option to specify alternate credentials ('Connect As'). When alternate credentials are specified, only NTLM authentication can be used.

The administrator will connect to the domain controller using the *administration service account* configured during installation. If the “Connect As” option has not been configured, then any user with privileges to access the server on with an installation of the administration service can administer ActiveRoles Server through the MMC Console. For this reason, it is important to control which users are granted access to this server.

The ActiveRoles Server Web interface can be configured to use either Windows integrated authentication or basic authentication (username and password). If Windows integrated authentication is desired and the Web interface is installed on a computer other than the one that hosts administration service, it will be necessary to register the Web interface computer account for delegation (trust relationship).

Permissions

Permissions in ActiveRoles Server are controlled by access templates. Access templates are collections of permissions representing administrative roles. Permissions are used to allow or deny specific administrative operations to a user or group. ActiveRoles Server enables delegated administration by linking access templates to collections of objects (managed units), directory folders (containers), or individual (leaf) objects.

Open Communication Ports and Firewall Configurations

ActiveRoles Server consists of multiple components that can be run in different network segments. In addition, ActiveRoles Server needs access to multiple network services, which could also be placed in different network segments. Depending on which components and services you want to place behind your firewall, you will need to open different sets of ports.

Managed Domain over a Firewall

If you want ActiveRoles Server to manage domains where the domain controllers are located behind a firewall, you need to open the following ports:

	PORT	TYPE	DIRECTION	NOTES
DNS				
	53	TCP/UDP	In/Out	Domain Name Server
Domain Controllers				
	88	TCP/UDP	In/Out	Kerberos
	135	TCP	In/Out	Remote Procedure Call (RPC) endpoint mapper. Port 135 is a dynamically allocated TCP port for RPC communication with the domain controller. See [1] for instructions on how to configure the Active Directory to use a predefined port number for RPC communication.
	139	TCP	In/Out	SMB/CIFS
	445	TCP	In/Out	SMB/CIFS
	389	TCP	Out	LDAP
	3268	TCP	Out	LDAP
	636	TCP	Out	LDAPS – if SSL is used to manage the domain
	3269	TCP	Out	LDAPS – if SSL is used to manage the domain
Exchange Servers				
	135	TCP	In/Out	Remote Procedure Call (RPC) end-point mapper. Port 135 is a dynamically allocated TCP port for RPC communication with the Exchange server (MSExchangeIS). See [2] for instructions on how to configure Exchange to use predefined port numbers for RPC communication.
Computer Resource Management				
	139	TCP	In/Out	SMB/CIFS on the managed computers
	445	TCP	In/Out	SMB/CIFS on the managed computers

	PORT	TYPE	DIRECTION	NOTES
Computer Restart				
	137	UDP	Out	NetBIOS name service
	138	UDP	Out	NetBIOS datagram
	139	TCP	In/Out	SMB/CIFS on the managed computers
Home Folder Provisioning & De-provisioning				
	139	TCP	In/Out	SMB/CIFS on the servers used to host home folders and shares
	445	TCP	In/Out	SMB/CIFS on the servers used to host home folders and shares
SMTP Servers (email notification feature)				
	N/A	TCP	Out	The SMTP server hostname and the TCP port number can be configured in the *Properties* dialog of the *Mail Configurations* objects
Active Directory LDS	N/A	TCP	Out	The TCP port used for LDAP communication with the Active Directory Lightweight Directory Service server is configurable in the *Add Managed AD Lightweight Directory Service Instance Wizard*

ActiveRoles Server MMC Over a Firewall

If you want to place a firewall between ActiveRoles Server clients (MMC snap-in and Web interface) and the ActiveRoles Server administration service, you need to open the following ports:

	PORT	TYPE	DIRECTION	NOTES
Domain Controllers				
	135	TCP	In/Out	Remote Procedure Call (RPC) endpoint mapper
ActiveRoles Server Admin Services				
	Auto	TCP	In/Out	Administration Service client requests ActiveRoles Server Administration Service uses Distributed COM (DCOM) over two separate TCP ports to accept client connections and requests. Port 135 is used by Administration Service clients to locate the Administration Service. The second TCP connection has its port number automatically assigned by the RPC end-point mapper. By default, any available port

	PORT	TYPE	DIRECTION	NOTES
				in the 1024-65535 range will be used. All requests from Administration Service clients, such as the MMC Console or ADSI Provider, are sent over this port. Note that the port range can be restricted or set to a static port through the Component Services snap-in (part of the Windows administration tools). Port 1433 is used for SQL replication in ActiveRoles Server.

SQL Server Over a Firewall

If you want to host the configuration database on a SQL Server that is behind a firewall and located on a different network segment than the ActiveRoles Server services, you need to open the following ports:

	PORT	TYPE	DIRECTION	NOTES
SQL Server				
	1433	TCP	In/Out	By default, port 1433 is used for connections to the Administration Database. This port can be changed using Microsoft Management Tools.

Web user interface over a firewall

If you want to access ActiveRoles Server's Web user interface behind a firewall, you need to open the following ports:

	PORT	TYPE	DIRECTION	NOTES
Web Server				
	80	TCP	In/Out	HTTP connection
Web Server				
	443	TCP	In/Out	HTTP over SSL (HTTPS). Note that SSL is turned off by default.

The following ports are made accessible on the machine with an ActiveRoles Server installation:

DNS servers

53/tcp, 53/udp

Web interface

80/tcp (HTTP), 443/tcp (SSL)

The Web interface runs over port 80, or over port 443 if SSL is enabled (off by default).

SQL Server

By default, the port 1433/tcp is used for connection to the Administration Database.

This port can be changed using Microsoft management tools.

Domain controllers

88/tcp, 88/udp (Kerberos)

135/tcp (RPC endpoint mapper)

139/tcp, 445/tcp (SMB/CIFS)

389/tcp, 3268/tcp (LDAP)

636/tcp, 3269/tcp (if SSL is used to manage the domain)

Port 135 is a dynamically allocated TCP port for RPC communication with the domain controller. See http://support.microsoft.com/kb/224196/ for instructions on how to configure the Active Directory to use a predefined port number for RPC communication.

Exchange servers

135/tcp (RPC endpoint mapper)

Port 135 is a dynamically allocated TCP port for RPC communication with the Exchange server (MSExchangeIS). See http://support.microsoft.com/kb/270836/ for instructions on how to configure Exchange to use predefined port numbers for RPC communication.

Computer resource management

139/tcp, 445/tcp (SMB/CIFS) on the managed computers

Home folder provisioning and deprovisioning

139/tcp, 445/tcp (SMB/CIFS) on the servers used to host home folders and shares.

SMTP servers (e-mail notification feature)

The SMTP server hostname and the TCP port number can be configured in the Properties dialog of the Mail Configuration objects.

Managed Active Directory Lightweight Directory Service instances

The TCP port used for LDAP communication with the Active Directory Lightweight Directory Service server is configurable in the Add Managed AD Lightweight Directory Service Instance Wizard.

Secure Communication

Customers have the option of turning on SSL to protect network traffic between the Web interface and users. This is recommended because sensitive data, including passwords, may be transmitted.

Traffic between ActiveRoles Server clients (ActiveRoles Server MMC Console or ActiveRoles Server ADSI Provider) and the administration service is secured based on Windows security settings. The Windows configuration and choice of authentication protocol (Kerberos or NTLM) dictates which security algorithms are used.

LDAP communication between the administration service and the domain controller can be authenticated and encrypted by enabling SSL on the managed domain controller. Authentication only (no encryption) can be activated by configuring both the domain controller and administration service to require digitally-signed LDAP communication.

Configuring the SQL Server to use SSL will ensure authenticated and encrypted communication between this server and the administration service.

Password Policies

ActiveRoles Server enforces the password policies on the system where the user account resides. Most user accounts will be regulated by Active Directory on the domain controller. Exceptions include the account on the SQL Server, if configured during installation, and local computer accounts that do not belong to a domain. In these cases, the password policies on the SQL Server and the local computer will be enforced.

Auditing and Logging

ActiveRoles Server records auditing information about any changes made to the ActiveRoles Server and Active Directory configurations. The audit trail shows what actions were performed by who and when, including actions that were not permitted. The audit information is stored into a Microsoft EDM server event log file (.evt) that is accessible through the Microsoft Event Viewer MMC snap-in.

It is possible to switch on logging for debugging by setting the registry variable *Debug Key* = 1. Only information pertaining to debugging is logged – no passwords or other sensitive data related to cryptographic objects is recorded when the ActiveRoles Server SDK is used.

Administration Privileges

The following privileges are required during **installation** of ActiveRoles Server:

- Privileges on the designated server to install ActiveRoles Server
- Privileges on the SQL Server to create the *ActiveRoles database*, either through Windows or SQL Server authentication. If Windows authentication is chosen, then the *administration service* account's credentials are used, and this account is required to be part of the *sysadmin* role on the SQL server. If SQL Server authentication is chosen, then the specified SQL account needs to be part of the *sysadmin* role.
- Privileges to write to the ActiveRoles Server database during installation of *ActiveRoles Web interface*

The following privileges are required during **operation** of ActiveRoles Server:

- Administrative privileges on the server running the ActiveRoles Server Administration Service (provided by the *administration service* account)
- Privileges to access and manage the domain, and publish the administration service in Active Directory (the *administration service* account is used unless an *override* account is provided)
- Privileges to write to the ActiveRoles Server database and setup SQL replication between ActiveRoles Server databases; if Windows authentication to the SQL Server is chosen, it is possible to grant the *administration service* account minimum permissions on the SQL Server to operate properly; see the ActiveRoles Server Quick Start Guide for further detail.

Replication and Synchronization

ActiveRoles Server replication generates configuration data changes to all replication partners whenever the data is modified on any one of these partners. To achieve this goal, ActiveRoles Server relies on the *merge* replication provided by Microsoft SQL Server. Both Windows integrated authentication and SQL authentication can be used when setting up the SQL replication.

Verification of Input from Users

ActiveRoles Server authenticates any user input by checking for errors and validating data types. For example, no letter characters can be entered in a numeric-only field, and input fields are restricted in length.

Patch Management

ActiveRoles Server uses the Windows installer for patch management. Microsoft Installer Patch Files (MSP format) can be sent out to customers as self-extracting .exe files.

IPv6 Compliance

ActiveRoles Server is IPv6 compliant; ActiveRoles Server’s MMC snap-in and Web interface are able to contact the administration service over IPv6. ActiveRoles Server does not store or work directly with IP addresses.

Daylight Savings Time Compliance

ActiveRoles Server is not affected by the changes introduced by the Daylight Savings Time (DST) Extension (U.S. Energy Policy Act of 2005). It relies on the operating system for time management and does not implement any special logic around DST settings. This means that if the operating system is DST compliant, then ActiveRoles Server will be as well.

CUSTOMER MEASURES

ActiveRoles Server’s security features are only one part of a secure environment. The customer’s operational and policy decisions will have a great influence on the overall level of security. Customers will need to be responsible for the physical security of the server where ActiveRoles Server resides, as well as the security configurations on the domain controller(s).

CONCLUSION

ActiveRoles Server is built with security in mind. It protects passwords by encrypting them with either the AES or RC2 symmetric encryption algorithms. ActiveRoles Server also supports SSL for its Web interface, produces an audit trail, and verifies input from users.

APPENDIX A: ACRONYMS

AD	Active Directory
AES	Advanced Encryption Standard
RC2	Rivest Cipher 2
CAPI	Microsoft Windows Crypto API
DCOM	Distributed Component Object Model
DPAPI	Microsoft Windows Data Protection API
MMC	Microsoft Management Console
SSL	Secure Socket Layer

APPENDIX B: ACTIVEROLES SERVER AND FISMA COMPLIANCE

The Federal Information Security Management Act[1] (FISMA) was passed by the U.S. Congress and signed by the president as part of the Electronic Government Act of 2002. It requires "each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information system that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."

A major component of FISMA implementation is the publication by the National Institute of Standards and Technology (NIST), entitled "*Recommended Security Controls for Federal Information Systems*", listed as NIST Special Publication 800-53[2]. This document presents 17 general security categories that can be used to evaluate an information security control program to measure its level of compliance with FISMA. For this reason, this appendix offers the 17 categories listed in 800-53 and describes how ActiveRoles Server addresses them.[3]

We would like to emphasize that the secure deployment of ActiveRoles Server is only one part of an information security program. If the appendix states that a particular security category is "applicable" to ActiveRoles Server, this means that ActiveRoles Server contains security features that may be relevant to some or all aspects of the category in question. It may not mean that ActiveRoles Server fully meets all of the requirements described in that security category, or that the use of ActiveRoles Server by itself will guarantee compliance with any information security standards or control programs. The specification, selection and implementation of a successful security program ultimately depends on how the customer deploys, operates, and maintains its entire network and physical infrastructure, including ActiveRoles Server.

NIST 800-53 Categories

Category:	Access Control (AC)
Applicable:	Yes
Description:	ActiveRoles Server enforces access control based upon a user's Active Directory privileges in. Permissions to perform specific operations are controlled by access templates.
Further Details:	Section(s) 3.3, 3.4

Category:	Awareness and Training (AT)
Applicable:	No
Description:	This category does not apply to ActiveRoles Server; the customer is responsible for developing and reviewing all security awareness and training policies.
Further Details:	N/A

Category:	Audit and Accountability (AU)
Applicable:	Yes
Description:	ActiveRoles Server records auditing information about any changes made to the configuration of ActiveRoles Server and Active Directory Logging, for debugging purposes, can be enabled by configuring a registry variable.
Further Details:	Section(s) 3.8

Category:	Certification, Accreditation and Assessments (CA)
Applicable:	No
Description:	This category does not apply to ActiveRoles Server; the customer is responsible for developing and reviewing all assessment, accreditation and certification policies.
Further Details:	N/A

Category:	Configuration Management (CM)
Applicable:	Yes
Description:	Changes to the configuration of ActiveRoles Server are recorded in an audit trail and can be reviewed at a later time. Only administrators can modify the configuration.
Further Details:	Section(s) 3.8

Category:	Contingency Planning (CP)
Applicable:	No
Description:	As defined by NIST (publication 800-34), disruptive events to IT systems include power outages, fire and equipment damage, and can be caused by natural disasters or terrorist actions. For this reason, this category does not apply to ActiveRoles Server; it is the responsibility of the customer to design and implement contingency plans.
Further Details:	N/A

Category:	Identification and Authentication (IA)
Applicable:	Yes
Description:	ActiveRoles Server enforces identification and authentication of users through Windows integrated authentication, supporting both the Kerberos and NTLM protocols. Only authorized users are able to gain access to ActiveRoles Server.
Further Details:	Section(s) 3.3, 3.4

Category:	Incident Response (IR)
Applicable:	No
Description:	This category does not apply to ActiveRoles Server; the customer is responsible for developing and reviewing incident response policies and procedures.
Further Details:	N/A

Category:	Maintenance (MA)
Applicable:	Yes
Description:	Quest Software monitors the software components and libraries used by ActiveRoles Server for security developments and flaws and provides product updates and patches to customers when necessary.
Further Details:	N/A

Category:	Media Protection (MP)
Applicable:	No
Description:	This category does not apply to ActiveRoles Server; the customer is responsible for developing and reviewing media protection policies.
Further Details:	N/A

Category:	Physical and Environmental Protection (PE)
Applicable:	No
Description:	This category does not apply to ActiveRoles Server; the customer is responsible for developing and reviewing physical and environmental policies.
Further Details:	N/A

Category:	Planning (PL)
Applicable:	No
Description:	This category does not apply to ActiveRoles Server; the customer is responsible for developing and reviewing security planning policies.
Further Details:	N/A

Category:	Personnel Security (PS)
Applicable:	No
Description:	This category does not apply to ActiveRoles Server; the customer is responsible for enforcing personnel security policies, including personnel screening and termination.
Further Details:	N/A

Category:	Risk Assessment (RA)
Applicable:	No
Description:	This category does not apply to ActiveRoles Server; the customer is responsible for developing and reviewing risk assessment policies.
Further Details:	N/A

Category:	System and Services Acquisition (SA)
Applicable:	No
Description:	This category does not apply to ActiveRoles Server; the customer is responsible for developing and reviewing system and services acquisition policies.
Further Details:	N/A

Category:	System and Communications Protection (SC)
Applicable:	Yes
Description:	Customers can enable SSL to protect network traffic between the Web interface and ActiveRoles Server users. Communication between ActiveRoles Server clients (ActiveRoles Server MMC Console and ActiveRoles Server ADSI Provider) and the underlying operating system is secured according to the Windows Server configuration. All account passwords are encrypted, either implicitly by Microsoft or explicitly by ActiveRoles Server. ActiveRoles Server supports the use of the FIPS 140-2 approved AES (Advanced Encryption Standard) algorithm.
Further Details:	Section(s) 3.1, 3.2, 3.5, 3.6

Category:	System and Information Integrity (SI)
Applicable:	Yes
Description:	ActiveRoles Server authenticates user input by checking for errors and validating data types. Third-party software components and libraries used by ActiveRoles Server are monitored through US-CERT, and Quest will take appropriate action when applicable vulnerabilities are published.
Further Details:	Section(s) 3.11

ABOUT THE AUTHOR

Einar Mykletun, Ph.D. is the security and compliance architect for research and development at Quest Software. He is responsible for risk analysis of product architectures, cryptographic solutions, code samples and internal and customer-facing product security documentation. Einar assists Quest Public Sector with government customers' security and certification concerns and is their bridge with R&D for security and compliance related issues. Einar's compliance expertise includes FDCC, FIPS 140-2, Common Criteria, IPv6 and FISMA.

ABOUT QUEST SOFTWARE, INC.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports systems management products—helping our customers solve everyday IT challenges faster and easier. Visit www.quest.com for more information.

Contacting Quest Software

Phone:	949.754.8000 (United States and Canada)
Email:	info@quest.com
Mail:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site:	www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at http://support.quest.com

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the ***Global Support Guide*** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: http://support.quest.com/pdfs/Global Support Guide.pdf

NOTES

[1] http://csrc.nist.gov/sec-cert/

[2] http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

[3] Note that under 800-53, these seventeen listed categories define general security control “families” (e.g., “AC”), and that each family in turn contains several subcategories (e.g., “AC-1”, “AC-2”, “AC-3”, etc.) that further detail related aspects of information security and assurance. Consult Appendix F of 800-53 for further information.