White Paper

EMC Physical Security Enabled by RSA SecurID Two-Factor Authentication with Genetec Omnicast Client Applications

A Detailed Review

EMC Information Infrastructure Solutions

Abstract

This white paper provides the reader with an overall understanding of how to integrate Genetec Omnicast within a Microsoft Windows domain that has been secured using RSA® SecurID® and that uses Microsoft Active Directory.

November 2010

Part number: H8090.1

Table of Contents

Executive summary

Business case

Private businesses and public entities alike have responded to rising concerns about theft, fraud, and terrorism by sharpening their focus on physical security and surveillance systems. These organizations are looking to integrate disparate technologies to create a comprehensive solution that can collect endless streams of data and transform them into business intelligence, while at the same time provide protection for their ever-growing volume of physical security information.

The ability to access the right data at the right time from anywhere is crucial to supporting physical security and surveillance needs. However, comprehensive solutions may be hindered by:

- Administrative overhead around system-access policies and procedures
- Security risks associated with the need to maintain multiple sets of credentials
- Proprietary software
- Closed hardware platforms
- Lack of manageable archival capabilities
- Lost data
- Content authenticity

These limitations are amplified by the high expansion costs of legacy video surveillance systems based on CCTV, digital video recorders (DVRs), or networked video recorder (NVR) technologies, and non-integrated IT and physical security systems.

Once the information is captured—and throughout the initial response, detection, legal, judicial submission, and the data disposal processes—information management, availability, security, and protection are the core capabilities needed for tamper-proof evidence collection, increased conviction rates, and asset protection.

Organizations that can benefit from a comprehensive physical-security solution include:

- Casinos
- Financial institutions
- Government agencies
- Higher-education institutions
- Law enforcement
- Prison systems
- Retailers
- School systems
- Transportation companies

Solution overview

Video surveillance systems running on networks secured by technology from RSA, The Security Division of EMC, provide the best-in-class solutions currently available on the market. These very scalable and highly flexible solutions benefit customers by meeting the increasing demands placed on physical security.

RSA integration strengthens user authentication and system security, augmenting the security of the at-rest video, as well as the health of the physical security installation.

This solution provides a recommended configuration that provides a secure, single-login capability for RSA® SecurID® users running Genetec Omnicast services and clients. The purpose of integrating Omnicast with Microsoft Windows Active Directory is to have a unified user management system within the organization, and to simplify the initial Omnicast setup. The system administrator can import any groups of users defined in Active Directory as Omnicast users and user groups.

The objectives of this solution are to:

- Demonstrate how to incorporate Genetec Omnicast into an existing RSA-secured Windows domain.
- Describe the recommended configuration to provide secure single-login capability for RSA SecurID users running Genetec Omnicast services and clients (Archive Player, Live Viewer, and Config Tool).
- Provide a secure single-login feature for Genetec Omnicast applications in an RSA-secured Windows domain.

RSA SecurID can be easily integrated with a pre-existing Active Directory; alternatively, Active Directory can be installed just prior to installing RSA SecurID. This document discusses the configuration required to integrate Omnicast after RSA SecurID has been successfully integrated with Active Directory.

Note For detailed information on how to configure Active Directory for RSA SecurID, refer to the *RSA Authentication Manager 7.1 Microsoft Active Directory Integration Guide*.

A Genetec Omnicast installation can consist of a single server or multiple servers. EMC conducted tests against each of the following Omnicast components to ensure compatibility with RSA SecurID:

- Omnicast Server Admin
- Omnicast Config Tool client
- Omnicast Live Viewer client
- Omnicast Archive Player client

All tests were carried out on both Genetec Omnicast 4.4 and Genetec Omnicast 4.6.

Key results

RSA offers industry-leading solutions for identity assurance and access control, encryption and key management, compliance and security information management, and fraud protection. These solutions bring trust to millions of user identities, the transactions they perform, and the data that is generated. With RSA, customers are confident that their information assets are protected, and are free to realize new business possibilities.

RSA-enabled Genetec Omnicast video surveillance systems enable access to the Windows domain and to the Omnicast application to become more granular. When RSA SecurID is coupled with Active Directory, user access moves from the control of the physical security administrator into the control of IT system securities and the Windows domain administrator.

Genetec Omnicast servers installed on an RSA-secured domain provide high security through RSA authentication of each user, using RSA passcodes.

EMC's testing of this solution demonstrates that in all cases:

- Omnicast access is granted only to RSA-authenticated users.
- The Omnicast login screen inherits the username and password from the initial Windows domain login. A user only needs to press **Enter** or click **OK** to continue with login.
- Users not authenticated with RSA cannot access the Omnicast systems.

Introduction

Introduction to this white paper

This white paper includes the following sections:

Purpose

This white paper provides the reader with an overall understanding of how to integrate Genetec Omnicast within a Windows domain that is secured using RSA SecurID, and that uses Microsoft Active Directory.

Scope

The scope of this white paper is to:

- Describe how to integrate Genetec Omnicast within a Windows domain that is secured using RSA SecurID
- Describe how to implement secure single login
- Describe how to configure Genetec Omnicast to use Microsoft Active Directory
- Summarize the testing performed by EMC for this solution

Audience

This paper is for anyone wishing to learn more about how to integrate RSA into a Genetec Omnicast physical security solution.

Terminology

This section defines terms used in this document.

Term	Definition
RSA SecurID authenticator	A hardware or software device that generates a simple, one-time authentication code (token code) that changes every 60 seconds. The token code generated by the authenticator is used in combination with a user’s secret personal identification number (PIN) to create a one-time-use RSA passcode.
RSA SecurID two-factor authentication	An authentication method based on something you know (a password or PIN) and something you have (an authenticator); it provides a much more reliable level of user authentication than reusable passwords.
RSA passcode	An access code made up of a user’s secret PIN (something they alone know) and a token code generated by their RSA SecurID authenticator (something they have).
Token code	A unique multi-digit number that is generated by an RSA SecurID authenticator. It is used in combination with a user’s secret PIN to create a one-time-use RSA passcode.

RSA SecurID

RSA SecurID two-factor authentication

RSA SecurID two-factor authentication is based on something you know (a password or personal identification number (PIN)) and something you have (an authenticator)—providing a much more reliable level of user authentication than reusable passwords.

To access resources protected by the RSA SecurID system, users simply combine their secret PIN with the token codes generated by their RSA SecurID authenticators. The result is a unique, one-time-use passcode that is used to positively identify, or authenticate, the user. If the RSA SecurID system validates the code, the user is granted access to the protected resource. If it is not recognized, the user is denied access.

RSA SecurID Appliance

The RSA SecurID Appliance delivers RSA Authentication Manager, the engine behind the industry-leading two-factor user authentication technology, in an integrated, rack-mountable hardware appliance. Used in combination with RSA SecurID authenticators, the RSA SecurID Appliance validates the identities of users before granting access to critical company resources. Additionally, the system logs all transactions and user activity, allowing administrators to use it as an auditing, accounting, and compliance tool.

With quick setup times, a web-management interface, streamlined credential deployment, and user self-service, greater cost savings and improved security can be gained.

Note RSA, Active Directory, and DNS must be integrated prior to integrating with Omnicast.

Flexibility and scalability

The RSA SecurID Appliance is available in two models that can be configured to meet the varying needs and preferences of small and large organizations. The solution is capable of handling from as few as 10 users up to 50,000 users.

The RSA SecurID Appliance can be installed and running in as few as 30 minutes and is interoperable with more than 350 products from over 200 vendors. RSA SecurID has a very straightforward setup and management console that can be accessed from any web browser.

Credentialing methods

The RSA SecurID Appliance supports authenticators in a variety of form factors from the traditional hardware authenticators to software-based authenticators that install on PCs and smart phones, to the SecurID On-demand Authenticator that delivers one-time codes using Short Message Service (SMS) or e-mail. All of these credentials are centrally managed from a common interface.

Deployment and maintenance

The RSA SecurID Appliance is designed so that a customer can be up and running in as few as 30 minutes. The built-in web server and web-based graphical user interface provide access to the straightforward setup and management console from any web browser.

In addition to the primary setup, common tasks that can be managed through the web interface include:

- Adding users and assigning authenticators
- Installing and configuring agents
- Viewing the activity monitor
- Specifying the location of backup files

Native LDAP integration enables the RSA SecurID Appliance to point to a single authoritative data store in real time for user and group information. Both the Base and Enterprise editions of the RSA Authentication Manager software include RSA Credential Manager, a completely integrated software module that enables user self-service (Base and Enterprise) and workflow provisioning (Enterprise only) to dramatically speed the onboarding of users to their credentials.

Genetec Omnicast

Genetec Omnicast

Genetec Omnicast is an open video management platform; it can control and record using cameras produced by most manufacturers on the market. Through its scalable and flexible design, Omnicast meets the expectations of the most demanding customers by providing many advanced features, including:

- High availability with built-in failover
- Alarm management incorporating an escalation process
- Support for cameras and software-based video analytics
- Video wall integrations
- Advanced floor plans and geographic information system (GIS) maps
- Multi-site deployments through the use of Genetec's Federation technology
- Offsite recording and monitoring
- Video indexing with metadata, for example, point of sale, access control
- Integration of CCTV equipment, for example, CCTV matrix, CCTV keyboards

Omnicast primary server

An Omnicast installation can consist of a single server or multiple servers in a hierarchical structure. The Omnicast Windows services can be distributed to additional Windows servers depending on camera count, motion detection needs, watermarking, and other complex functions.

The primary Omnicast services are:

- Gateway
- Directory
- Virtual Matrix (optional)
- Archiver

Each of these services is described in detail in Table 1.

Table 1 Omnicast services

Service	Description
Directory	• Defines an Omnicast system, therefore only a single Directory can run within an Omnicast system at any given time. • Provides a centralized configuration database through the main server module for all entities in the system; this includes cameras, users, other Omnicast services, and system applications. • Responsible for authentications and access control using a built-in security model or through Active Directory. • Can log all system events and user actions in a relational database for reporting purposes. • Offers three options for redundancy: - VMware® High-Availability (HA) and Fault-Tolerance (FT) for the Directory, SQL Database, and Gateway services. - Windows Clustering available with Microsoft Windows Server 2003/2008 - 1:N redundancy using the Omnicast Directory Failover Coordinator (DFC)
Gateway	• Acts as a proxy for the command and control channel between the Directory service and all other Omnicast services and client applications. • Detects the network connectivity and transparently redirects video streams to ensure that video is always available for any type of TCP/IP network: LAN, WAN, VPN, Internet, firewalls, or NATs. • Multiple Gateways can be installed on large Omnicast systems to increase service availability and provide load balancing.
SQL	• Database service primarily used to track event occurrences.
Virtual Matrix	• Provides the functionality of a traditional CCTV hardware matrix switch. • Camera sequencing provides a set sequence of cameras to be viewed. • The Virtual Camera function provides the ability to connect to pre-existing matrix switches. • Provides the ability to connect to pre-existing CCTV keyboards. • Enables users to automate and extend the functionality of Omnicast through the use of macros and plug-ins.
Archiver	• Manages the communication with IP cameras and the encoder; it is the only Omnicast component that communicates directly with IP cameras. • Provides support for new camera manufacturers without requiring a complete software upgrade, through a plug-in architecture. • Can record up to 300 cameras. • Maintains the database that links a specific camera, at a specific time, to a video file stored on disk. • Executes motion detection algorithms on captured video streams.

Live Viewer client

The Live Viewer client application monitors and controls the entire Omnicast system.

Live Viewer’s features include:

- An interface that enables the user to view live video feed from up to 16 cameras on each monitor
- Support for multiple monitors
- Alarm management controls
- Control of camera movement from the user interface
- Instant video replay

Archive Player client

The Archive Player client application is used to retrieve and review video and audio data stored using the Omnicast system. Users can perform a range of complex queries on the stored data to accurately identify specific events.

Archive Player’s features include:

- An interface that enables the user to simultaneously review up to 16 archived feeds.
- Support for intelligent archive queries based on time and date, event, camera, alarm type, or metadata.
- Verification of the integrity of archived data.

Config Tool client

The Config Tool client application enables users to easily perform real-time configuration of a range of components within the Omnicast system.

Components that users can configure include:

- Cameras
- Users
- Sites
- Archiving schedules

Login process for Genetec Omnicast in an RSA SecurID environment

Login process overview

Figure 1 provides an overview of the process used to log in to Genetec Omnicast applications in an RSA SecurID environment that includes Microsoft Active Directory.

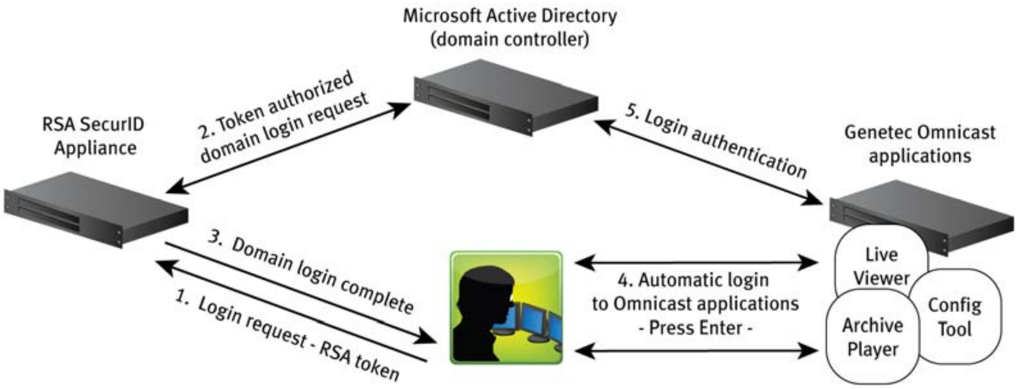
Microsoft Active Directory
(domain controller)
RSA SecurID Appliance
2. Token authorized domain login request
5. Login authentication
Genetec Omnicast applications
3. Domain login complete
1. Login request - RSA token
4. Automatic login to Omnicast applications - Press Enter -
Live Viewer
Config Tool
Archive Player

Figure 1 Login process overview

Login process description

The login process for Omnicast in an RSA SecurID environment consists of five phases. Table 2 describes the process.

Table 2 Login process

Phase		Description
1	Login request – RSA token	The user enters a login request that includes a one-time-use passcode. The passcode is created by combining the user's secret PIN with a token code generated from their RSA authenticator. The login request is sent to an RSA SecurID Appliance.
2	Token authorized	If the user's credentials are correct, the RSA SecurID Appliance proxies the login to Active Directory.
3	Domain login complete	Active Directory authenticates the login to the requested Windows domain.
4	Automatic login to Omnicast	The user does not need to enter credentials again; the client application automatically connects to the Omnicast Directory.
5	Login authentication	To ensure that the user has access rights for the requested application, the Omnicast Directory service proxies the login request to Active Directory for authentication. The user is then able to use the chosen Omnicast application.

Environment

Prerequisites

The following prerequisites apply:

- RSA SecurID is installed into an existing Active Directory domain.
- RSA two-factor authentication is successfully implemented and tested within the Windows domain.
- Domain users are able to log in using RSA passcodes that consist of a secret PIN and a token code generated by an RSA authenticator.

Environment overview

Note This is the lab test environment. It is described here as an illustration of how a typical RSA-secured Omnicast environment could be configured.

The validated environment consists of the following elements:

- Active Directory and DNS
  - One Microsoft Windows Server 2003 domain controller with Active Directory and DNS.
- RSA
  - Two Microsoft Windows clients with RSA® Authentication Agent 6.1.3 installed on each one.
  - One RSA SecurID Appliance configured on the same network as the Windows domain and the Windows clients.
  - Two new users and an Administrator user; a token was assigned to each user.
- Genetec Omnicast
  - Omnicast 4.4 and Omnicast 4.6
  - Servers:
    - Directory
    - Gateway
    - Archiver
  - Clients:
    - Config Tool
    - Archive Player
    - Live Viewer

Hardware resources

Table 3 lists the hardware resources that were used to validate the solution.

Table 3 Hardware resources

Equipment	Quantity	Configuration
RSA SecurID Appliance	1	Specified in the RSA documentation
Active Directory server	1	Microsoft Active Directory
Omnicast server	1	With both the Omnicast services and Omnicast clients installed.

Software resources

Table 4 lists the software resources that were used to validate the solution.

Table 4 Software resources

Software	Version	Configuration
Microsoft Windows Server 2003	SP2/R2	• Domain controller, Active Directory, and DNS • Operating system for the Omnicast servers and workstations • Operating system for RSA Authentication Agent
RSA Authentication Agent	6.1.3	
Omnicast Directory	4.4 and 4.6	
Omnicast Gateway	4.4 and 4.6	
Omnicast Archiver	4.4 and 4.6	
Omnicast Live Viewer	4.4 and 4.6	
Omnicast Archiver Player	4.4 and 4.6	
Omnicast Config Tool	4.4 and 4.6	

Configuring Genetec Omnicast for use with RSA SecurID

Process overview

To configure Genetec Omnicast for use with RSA SecurID, perform the following steps:

1. Install Genetec Omnicast.
2. Change the service login user from a local user to a domain user.
3. Integrate Genetec Omnicast with Active Directory.
4. Set Omnicast permissions and privileges.

Installing Genetec Omnicast

Install Genetec Omnicast following the detailed instructions provided in the Genetec Omnicast product documentation.

Changing the service login user to a domain user

The default service login user, ‘OmnicastSvcUsr’, created during the Omnicast Server installation is a local user and is not eligible to access the Active Directory.

Once the integration of Omnicast with Active Directory is complete, the service login user must be changed to a domain user with the necessary rights to access the Active Directory.

Note Users in the same Windows domain as Omnicast are able to log in to the Omnicast server, but only the users in the user groups that are added to Omnicast groups in the Active Directory have the access to run the application.

Integrating Omnicast with Active Directory

The purpose of integrating Omnicast with Active Directory is to establish a unified user management system within the organization, and to simplify the initial Omnicast setup. The system administrator can import any user groups that are defined in the Active Directory as Omnicast users and Omnicast user groups. Once Active Directory is enabled, only the imported users are able to run Omnicast applications.

The Directory Service user must be a part of the same domain as Omnicast and must have access to Active Directory. Also, this user must be a part of the local Administrators group on the server running the Omnicast Directory.

Table 5 provides an overview of the integration process; full details can be found in the Genetec Omnicast product documentation.

Table 5 Integrating Omnicast with Active Directory

Step	Action
1	Launch Omnicast Directory.
2	Navigate to **Omnicast Server Admin** > **Directory** > **Active Directory** and click **Activate**.
3	Select the Active Directory user groups that require access to Omnicast.
4	Click **Activate**.
5	After integrating Omnicast with Active Directory, Omnicast users can be added or deleted using Active Directory.

Warning After integrating Omnicast into Active Directory, all pre-existing Omnicast users and user groups that have no match in the Active Directory will be deleted. Therefore, prior to integration, it is important to first create these users and user groups in Active Directory.

Setting Omnicast permissions and privileges

To configure Omnicast user management, follow the steps in Table 6.

Table 6 Setting Omnicast permissions and priviliges

Step	Action
1	Launch the Genetec Omnicast Config Tool.
2	Set the permissions and privileges for each of the new entities that were imported from Active Directory. The recommended best practice is to set privileges on the associated Active Directory group; users who are members of the group inherit the group's privileges. In this way, no intervention is required when a new user is added to Active Directory.
3	Once this is complete, users no longer need to enter their username and password when launching the following Omnicast client applications: • Config Tool • Live Viewer • Archive Player
4	Select the **Use Windows credentials** option. This ensures that the username and password are inherited from the user’s initial Windows domain login, and disables the username and password fields.

Logging in to Omnicast with RSA SecurID enabled

Once Omnicast is configured for use with RSA SecurID, the user login experience is as described in Table 7.

Table 7 Logging in to Omnicast with RSA SecurID enabled

Step	Action
1	The user logs in to the Windows Domain using their Windows domain username and an RSA passcode that consists of their secret PIN and a token code generated from an RSA authenticator.
2	The user double-clicks the appropriate Omnicast client icon.
3	The Omnicast client login screen is displayed. • During the first login, the user must select the **Use Windows credentials** option. • The login screen inherits the credentials from the network login, and the password is grayed out.
4	To access the Omnicast client application, the user presses **Enter**. **Note** To avoid step 3 and 4, the administrator can configure the client options (**Tools** > **Options** > **General**) to automatically connect using Active Directory to a specific Omnicast Directory server.

Validation

Test objective

The objective of this test is to verify the integration of Genetec Omnicast within an RSA-secured Windows domain, and to demonstrate that secure single login operates correctly for users of the Omnicast Config Tool, Live Viewer, and Archive Player clients.

Test scenario

Scenario description		Expected results
1	A test user, who is a member of the Omnicast Group in Active Directory, logs in to the Windows domain using an RSA passcode. The test user then attempts to access the Omnicast Config Tool, Live Viewer, or Archive Player client.	The user successfully accesses the client application and does not need to enter credentials during Omnicast client login.
2	The test user is removed from the Omnicast Group in Active Directory. The test user logs in to the Windows domain using an RSA passcode. The test user then attempts to access Omnicast Config Tool, Live Viewer, or Archive Player client.	The user successfully accesses the Windows domain but is denied access to the Omnicast client application.

Test procedure

Scenario 1: User is a member of the Omnicast Group in Active Directory

The following test procedure was followed for the Omnicast Config Tool, Live Viewer, and Archive Player clients.

1. Log in to the Windows domain using an RSA passcode, created by combining a PIN with a token generated by an RSA authenticator.
2. Double-click the Omnicast client icon.
3. Select the **Use Windows credentials** option.
4. Press **Enter** when the Omnicast client login screen is displayed.

Result: User successfully accesses the client application and does not need to enter credentials during Omnicast client login.

Scenario 2: User is not a member of the Omnicast Group in Active Directory

The following test procedure was followed for the Omnicast Config Tool, Live Viewer, and Archive Player clients.

1. Remove the user from the Omnicast Group in Active Directory.
2. Log in to the Windows domain using an RSA passcode, created by combining a PIN with a token generated by an RSA authenticator.
3. Double-click the Omnicast client icon.
4. Select the **Use Windows credentials** option and press **Enter**.

   Result: The user is denied access to the Omnicast client application.

Test result

Scenario 1: User is a member of the Omnicast Group in Active Directory

In all cases, the user's credentials were inherited from the Windows domain login. Pressing **Enter** allows the user to access the Omnicast client application.

Scenario 2: User is not a member of the Omnicast Group in Active Directory

The user was able to log in to the RSA-secured Windows domain but was denied access to the Omnicast client application.

Conclusion

Summary

RSA adds a level of security beyond what a Microsoft Windows Active Directory provides. In addition, RSA integration provides a more secure method for single Omnicast application login.

By integrating Omnicast with Active Directory, a unified user management system is provided within the organization and the user management of Omnicast is simplified. The system administrator can grant, deny, or remove access to Omnicast by simply adding or removing a user from an Active Directory group linked to Omnicast.

Using RSA-enabled Genetec Omnicast video surveillance systems, not all the domain users are authorized to use the application. The administrator can specify which user groups can perform specific operations within the Omnicast system.

RSA integration with Omnicast provides several operational and system security benefits, including:

- RSA key authentication, which provides a level of security well beyond User ID and Password.
- The ability to move control of Omnicast user access to the corporation's or government agency's system-security group.
- Single secure-login to Omnicast clients provided by RSA with Active Directory.
- Omnicast user management can be done by a Windows administrator.
- More granular control over user access to specific Omnicast operations.
- Greater convenience for users as they no longer have to enter credentials each time they wish to access an Omnicast client application.

Findings

Testing performed by EMC demonstrates that RSA SecurID integration with Omnicast is beneficial in providing additional system security, while at the same time simplifying Omnicast client login.

A user can be easily authorized to access Omnicast client applications by adding the user to the appropriate Omnicast Group in Active Directory. In turn, Omnicast access rights can be easily revoked by removing a user from the Omnicast Group in Active Directory—most importantly, this can be done without impacting a user’s ability to access the Windows domain.

The RSA SecurID documentation was easy to follow, allowing the integration to be carried out quickly

Next steps

To learn more about this and other solutions contact an EMC representative or visit: www.emc.com.

References

Physical security solutions

For additional information about EMC physical security solutions, see the documents listed below:

- *EMC Storage for Physical Security - Enabled by EMC CLARiiON and Genetec Omnicast*
- *EMC Virtual Infrastructure for Physical Security - Enabled by EMC CLARiiON, VMware ESX/ESXi, and Genetec Omnicast Reference Architecture*

RSA

For additional information about RSA products, see the documents listed below.

- *RSA SecurID Installation Guide*
- The RSA SecurID content on the RSA website at http://www.rsa.com/node.aspx?id=1156
- *RSA SecurID Appliance 2.0 Owner's Guide*
- *RSA SecurID Appliance 2.0 Getting Started*
- *RSA ACE/Agent 6.0 for Windows Installation and Administration Guide*
- *RSA SecurID for Microsoft Windows Planning Guide*

Genetec Omnicast

For additional information about Genetec Omnicast, see the documents listed below.

- *Genetec Omnicast 4.4 Administrator Guide*
- *Genetec Omnicast 4.6 Administrator Guide*