Abstract

This white paper explains how to integrate Milestone® XProtect® within a Microsoft Windows domain that has been secured using RSA® SecurID® and uses Microsoft® Active Directory.

December 2012
# Table of contents

**Executive summary**............................................................................................................. 5  
  Business case......................................................................................................................... 5  
  Solution overview.................................................................................................................. 6  
  Key results............................................................................................................................... 6  

**Introduction**.......................................................................................................................... 8  
  Purpose................................................................................................................................... 8  
  Scope...................................................................................................................................... 8  
  Audience................................................................................................................................. 8  
  Terminology............................................................................................................................. 8  

**Technology overview**.............................................................................................................. 9  
  Overview.................................................................................................................................. 9  
  RSA SecurID two-factor authentication....................................................................................... 9  
  RSA SecurID Appliance.............................................................................................................. 9  
  Flexibility and scalability........................................................................................................... 9  
  Credentialing methods.............................................................................................................. 9  
  Deployment and maintenance................................................................................................. 10  
  Milestone XProtect.................................................................................................................. 10  
  Milestone XProtect Management Server................................................................................ 11  

**RSA SecurID Two-Factor Authentication with Milestone XProtect**........................................ 12  
  Prerequisites.......................................................................................................................... 12  
  Environment overview............................................................................................................ 12  
  Hardware resources................................................................................................................ 12  
  Software resources................................................................................................................ 13  
  Design considerations ........................................................................................................... 13  
  Validation................................................................................................................................ 14  
  Test scenarios........................................................................................................................ 14  
  Test procedures...................................................................................................................... 14  
    Scenario 1: User is a member of the XProtect group in Active Directory.............................. 14  
    Scenario 2: User is not a member of the XProtect Group in Active Directory....................... 14  
  Login process description....................................................................................................... 15  

**Configuring Milestone XProtect for use with RSA SecurID**.................................................. 16  
  Process overview.................................................................................................................... 16  
  Installing Milestone XProtect................................................................................................... 16  
    Changing the service login user to a domain user............................................................... 16  
    Integrating XProtect with Active Directory......................................................................... 16  
  Setting XProtect permissions and privileges.......................................................................... 17
Logging in to Milestone XProtect with RSA SecurID enabled.................................................. 17
Test results ..................................................................................................................................... 17
  Scenario 1: User is a member of the XProtect Group in Active Directory ............................... 17
  Scenario 2: User is not a member of the XProtect Group in Active Directory....................... 17

Conclusion ........................................................................................................................................ 18
 Summary ........................................................................................................................................ 18
 Findings .......................................................................................................................................... 18

References ....................................................................................................................................... 19
  Physical security solutions .................................................................................................................. 19
  RSA ............................................................................................................................................ 19
  Milestone XProtect ............................................................................................................................. 19
Executive summary

Business case

Private businesses and public entities have responded to rising concerns about theft, fraud, and terrorism by sharpening their focus on physical security and surveillance systems. These organizations want to integrate disparate technologies to create a comprehensive solution that can collect endless streams of data and transform them into business intelligence, and 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 support 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 (closed circuit television), digital video recorders (DVRs), 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 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 with a secure, single-login capability for RSA SecurID® users running Milestone® XProtect® IP Video Management Software (VMS) and XProtect clients. The purpose of integrating XProtect with Microsoft® Windows® Active Directory is to have a unified user management system within the organization, and to simplify the initial XProtect setup. The system administrator can import any groups of users defined in Active Directory as XProtect users and user groups.

The objectives of this solution are to:

- Incorporate Milestone XProtect VMS into an existing RSA-secured Windows domain.
- Provide secure single-login capability for RSA SecurID users running Milestone XProtect services such as XProtect Recording Server and XProtect Smart Client.
- Provide a secure single-login feature for Milestone XProtect VMS 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 Milestone XProtect IP VMS offerings, after RSA SecurID has been successfully integrated with Active Directory.

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

- XProtect Management Server
- XProtect Smart Client

**Note:** All tests were based on Milestone XProtect 5.

**Key results**

RSA offers industry-leading solutions for identity assurance, access control, encryption and key management, compliance and security information management, and fraud protection. These solutions provide security for millions of user identities, the transactions they perform, and the data that is generated. RSA protects customer information and opens new business possibilities.

RSA-enabled Milestone XProtect IP VMS enable access to the Windows domain and to the XProtect IP VMS to become more granular. When RSA SecurID is used 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.

A Milestone XProtect Management server installed on an RSA-secured domain provides high security through RSA authentication of each user, by using RSA passcodes.

EMC testing of this solution demonstrates that in all cases:

- XPProot Smart Client and Management Server access is granted only to RSA-authenticated users.
- The XProtect 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 XProtect Smart Client or Manager Server systems.
Introduction

Purpose
This white paper explains how to integrate Milestone XProtect IP Video Management Software (VMS) within a Windows domain that is secured using RSA SecurID with Microsoft Active Directory.

Scope
The scope of this white paper is to:

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

Audience
This paper is for customers who wish to integrate RSA into a Milestone XProtect physical security solution.

Terminology
Table 1 defines terms used in this document.

Table 1. Terminology

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

Overview

The platform’s technology components include:

- **RSA SecurID**: Provides secure host access based on an ever-changing two-factor authentication method. Various facets of RSA SecurID are described in this paper.

- **Milestone XProtect IP Video Management Software (VMS)**: A video security management platform consisting of servers used to collect data from the cameras, perform analytics, and write the video to EMC Storage. Other services include video viewing and review as well as services to manage XProtect IP VMS offerings.

RSA SecurID two-factor authentication

RSA SecurID two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator). Two-factor authentication provides 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, thereby allowing administrators to use the log as an auditing, accounting, and compliance tool.

Save money and improve security with quick set-up times, a web-management interface, streamlined credential deployment, and user self-service.

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

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. It is capable of handling from as few as 10 users and up to 50,000 users.

You can install the RSA SecurID Appliance in as few as 30 minutes. It is interoperable with more than 350 products from over 200 vendors. RSA SecurID has a very simple setup and management console that can be accessed from any web browser.

Credentialing methods

The RSA SecurID Appliance supports authenticators in a variety of forms. Possible forms include traditional hardware authenticators, software-based authenticators that install on PCs and smart phones, and SecurID On-demand Authenticators that...
deliver 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.

**Milestone XProtect**

Milestone XProtect VMS is an open video management platform that can control and record using common camera. VMS is based on a true open platform: it has a published application programming interface (API) allowing developers to alter the functionality of XProtect. The Milestone open platform enables you to add custom, best-in-class security solutions to your surveillance, such as access control, mobile devices and video analytics. Through its scalable and flexible design, XProtect meets the expectations of the most demanding customers by providing many advanced features, including:

- **Centralized management:** A single-management user interface controls all connected cameras, devices, storage and users, helping reduce operating costs by ensuring fast, efficient management of large, multi-site installations.
- **Multi-stage storage:** Set multiple archive steps with individual retention times and frame rates, which significantly reduces the cost of long-term video storage.
- **64-bit Recording Servers:** Add more cameras while using fewer servers, helping to reduce overall hardware costs.
- **System Monitor:** Displays actual and historic information about system performance and storage use, allowing for proactive system management.
- **Edge Storage with flexible retrieval:** A redundancy option that ensures continuous recording of audio and video and allows you to control when recordings are retrieved from camera storage based on time schedules and events.
- **Milestone Federated Architecture**: Interconnect multiple, individual XProtect Corporate systems into a master/slave hierarchy of federated sites, ensuring unlimited scalability and ultimate operational flexibility.

- **Milestone Integration Platform (MIP) support**: Enables easy and flexible integration of various types of security and business systems and video analytics applications, providing ultimate usability for the security operator.

- **Alarm Manager**: Single-point alarm function that provides a clear and consolidated overview of security and system-related alarms and gives instant access to cameras for immediate visual verification, decreasing the number of false alarms.

- **Bookmarking**: Flag video sequences of particular interest and add descriptive notes, enabling users to easily share information and increase efficiency in investigating incidents.

- **XProtect Smart Wall**: An add-on video wall product that supports any number or combination of monitors regardless of manufacturer and seamlessly integrates with the XProtect Smart Client and map function.

**Milestone XProtect Management Server**

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

The primary XProtect services are described in Table 2:

**Table 2. XProtect services**

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Server</td>
<td>Used to manage and configure recording servers, users, and devices.</td>
</tr>
<tr>
<td>XProtect Management Client</td>
<td>A single point of entry for administrators to configure and maintain the entire system. It provides remote handling of recording servers, devices and users.</td>
</tr>
<tr>
<td>XProtect Smart Client</td>
<td>An easy-to-use operator client that provides instant access to live cameras and recorded video. Enhance efficiency with task-oriented tabs and an adaptable user interface that can be tailored to your working environment including a selection of a black or white theme. The XProtect Smart Client is available in 26 languages.</td>
</tr>
<tr>
<td>Recording Servers</td>
<td>Record the video streams to the designated storage.</td>
</tr>
</tbody>
</table>
RSA SecurID Two-Factor Authentication with Milestone XProtect

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: The lab test environment is described here as an illustration of how a typical RSA-secured XProtect 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.
- Milestone XProtect
  - XProtect 4
  - Servers: Recorder
  - Clients:
    - Management Client
    - Smart Client

Hardware resources

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

<table>
<thead>
<tr>
<th>Equipment</th>
<th>Quantity</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA SecurID Appliance</td>
<td>1</td>
<td>Specified in the RSA documentation</td>
</tr>
<tr>
<td>Active Directory server</td>
<td>1</td>
<td>Microsoft Active Directory</td>
</tr>
<tr>
<td>XProtect server</td>
<td>1</td>
<td>With both the XProtect services and XProtect clients installed</td>
</tr>
</tbody>
</table>
Table 4 lists the software resources that were used to validate the solution.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows Server 2008</td>
<td></td>
<td>Enterprise, Domain controller, Active Directory, and DNS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operating system for the XProtect servers and workstations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operating system for RSA Authentication Agent</td>
</tr>
<tr>
<td>RSA Authentication Agent</td>
<td>6.1.3</td>
<td></td>
</tr>
<tr>
<td>XProtect Server</td>
<td>5.0a</td>
<td></td>
</tr>
<tr>
<td>XProtect Management Client</td>
<td>5.0a</td>
<td></td>
</tr>
<tr>
<td>XProtect Smart Client</td>
<td>7.0a</td>
<td></td>
</tr>
<tr>
<td>XProtect Smart Client</td>
<td>6.0d</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1 provides the design and overview of the process used to log in to Milestone XProtect applications in an RSA SecurID environment that includes Microsoft Active Directory.

Interaction with EMC RSA SecurID, Active Directory and the Milestone XProtect application must be taken into account as well as the interaction between the user’s host, EMC RSA SecurID and Milestone XProtect.

Various levels of user access were considered within the design.
Validation

This test verifies the integration of Milestone XProtect within an RSA-secured Windows domain, and demonstrates that secure single login operates correctly for users of the Management server and Smart Client. Test scenarios included verifying that users and administrators could successfully access the systems they required, or were blocked.

Test scenarios

Table 5 describes two test procedure scenarios:

<table>
<thead>
<tr>
<th>Scenario description</th>
<th>Expected results</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. A test user, who is a member of the XProtect group in Active Directory, logs in to the Windows domain using an RSA passcode. The test user then attempts to access the XProtect management server and Smart client.</td>
<td>The user successfully accesses the client application and does not need to enter credentials during XProtect Smart Client login.</td>
</tr>
<tr>
<td>2. The test user is removed from the XProtect Group in Active Directory. The test user logs in to the Windows domain using an RSA passcode. The test user then attempts to access XProtect management server and Smart client.</td>
<td>The user successfully accesses the Windows domain but is denied access to the XProtect client application.</td>
</tr>
</tbody>
</table>

Test procedures

Here are several examples of test procedure scenarios:

Scenario 1: User is a member of the XProtect group in Active Directory

The following test procedure was followed for the XProtect management client and smart client.

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 XProtect Management client icon.
3. Select the Use Windows Authentication (Current User) option.
4. Press Enter when the XProtect client login screen is displayed.

Result: The user successfully accesses the client application and does not need to enter credentials during XProtect client login.

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

The following test procedure was followed for the XProtect management client and smart client.

1. Remove the user from the XProtect group in the 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 XProtect smart client icon.

4. Select the **Use Windows Authentication (Current User)** option and press **Enter**.

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

The login process for XProtect in an RSA SecurID environment consists of five phases. **Table 6** describes the process.

**Table 6. Login process**

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

Process overview
To configure Milestone XProtect for use with RSA SecurID, perform the following steps:

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

Installing Milestone XProtect
Install Milestone XProtect following the detailed instructions provided in the Milestone XProtect product documentation.

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

Once the integration of XProtect 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 XProtect are able to log in to the XProtect server; however, only the users in the user groups that are added to XProtect groups in the Active Directory have the access to run the application.

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

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

Here is an overview of the integration process; see the Milestone XProtect product documentation for complete details.

1. Launch Milestone management client.
2. Create a users group on Active Directory for Milestone application access.
3. Navigate to Security > Roles > Add Role > Add users and groups
4. Assign appropriate rights to each user or group.
5. After adding a group from Active Directory to the application, users can be added or deleted from Active Directory without any access to the application.
To configure XProtect user management, follow these steps:

1. Launch the Milestone Management client.

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. No intervention is required when you add a new user to Active Directory.

3. Once this is complete, users no longer need to enter their username and password when launching the following Milestone client applications:
   - Management Client
   - XProtect Smart Client

4. Select the **Use Windows Authentication (Current User)** 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.

Once Milestone XProtect is configured for use with RSA SecurID, the user login experience is as follows:

1. The user logs into 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 Milestone XProtect client icon.

3. The XProtect client login screen is displayed.

   During the first login, the user must select the Windows Authentication (Current User) option. The login screen inherits the credentials from the network login, and the password is unavailable.

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

In all cases, the user credentials were inherited from the Windows domain login. Pressing **Enter** allows the user to access the XProtect client applications.

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

The user was able to log in to the RSA-secured Windows domain but was denied access to the XProtect client applications.
Conclusion

**Summary**

RSA adds a level of security beyond that provided by a Microsoft Windows Active Directory. In addition, RSA integration provides a more secure method for single Milestone XProtect application login.

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

Using RSA-enabled Milestone XProtect 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 XProtect system.

RSA integration with XProtect 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 XProtect user access to the system-security group of the corporation or government agency.
- Single secure-login to XProtect clients provided by RSA with Active Directory.
- XProtect user management can be done by a Windows administrator.
- More granular control over user access to specific XProtect operations.
- Greater convenience for users as they no longer have to enter credentials each time they wish to access an XProtect client application.

**Findings**

Tests performed by EMC demonstrate that RSA SecurID integration with XProtect is beneficial in providing additional system security, and simplifying XProtect Smart Client login.

Easily authorize users to access XProtect client applications by adding the users to the appropriate XProtect Groups in Active Directory. Simply revoke XProtect access rights by removing a user from the XProtect Group in Active Directory without impacting the user’s ability to access the Windows domain.

The RSA SecurID documentation is easy to follow, and allows the integration to be carried out quickly.
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 Milestone XProtect*
- *EMC Virtual Infrastructure for Physical Security — Enabled by EMC CLARiiON, VMware ESX/ESXi, and Milestone XProtect Reference Architecture*

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

- *RSA SecurID Installation Guide*
- *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*

Milestone XProtect
For additional information about Milestone XProtect, see *Milestone XProtect Corporate Administrator Manual*