White Paper

EMC Physical Security Enabled by RSA SecurID Two-Factor Authentication with Verint Nextiva Review and Control Center Clients

A Detailed Review

EMC Information Infrastructure Solutions

Abstract

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

November 2010

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Part number: H8095.1

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 it 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.

The objectives of this solution are to:

- Demonstrate how to incorporate Verint Nextiva 6.1 into an existing RSA-secured Windows domain.
- Describe the recommended configuration to provide secure single-login capability for RSA® SecurID® users running Nextiva Review and Nextiva Control Center thick clients.
- Demonstrate how to integrate Nextiva with Microsoft Active Directory as part of the RSA user authentication environment.

Note RSA SecurID can be easily integrated with a pre-existing Active Directory or can be installed just prior to or after switching to Windows Authentication. This document discusses the configuration required to integrate Nextiva after RSA SecurID is successfully integrated with Active Directory. For detailed information on how to configure Active Directory for RSA SecurID, refer to the *RSA SecurID Implementation Guide*.

Verint Nextiva 6.1 includes various servers controlled by the Nextiva Control Center, and a Review Client that is used to access live and archived video. EMC conducted tests against these Nextiva components.

As part of this solution, RSA SecurID Windows Authentication Agent was validated with:

- Nextiva Review
- Nextiva Control Center
- Nextiva Active Directory Bridge service
- Nextiva Master Server

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.

Access to the Windows domain and to the Verint Nextiva application becomes more granular using RSA-enabled Verint Nextiva video surveillance systems. 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 security and the Windows domain administrator.

Verint Nextiva servers installed on an RSA-secured domain provide high security through RSA authentication of each user using RSA passcodes—only RSA-authenticated users can access the Nextiva application.

EMC's testing verifies the successful operation of Nextiva Master Server, Nextiva Recorder Servers, Nextiva Review and Nextiva Control Center clients when integrated with RSA SecurID and Microsoft Active Directory.

In all cases, once the user logs in to the Windows domain, and authenticates through RSA SecurID, they can then easily log in to either the Control Center or the Review clients. When logging in to any Nextiva application, the Nextiva login screen inherits the username and password from the initial Windows domain login; the user only needs to press **Enter** or select **OK** to continue with the login.

This demonstrates how Nextiva can be deployed as part of an RSA-secured environment, while at the same time providing the simplicity of single secure login.

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 Verint Nextiva within a Windows domain that is secured using RSA SecurID, and that uses Microsoft Active Directory.

Scope

The scope of this paper is to:

- Describe how to integrate Verint Nextiva within a Windows domain that is secured using RSA SecurID
- Describe how to implement secure single login.
- Describe how to configure Verint Nextiva to use Microsoft Active Directory.
- Summarize EMC’s testing of this solution.

Audience

This paper is for anyone wishing to learn more about how to integrate RSA into a Verint Nextiva 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 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, a user simply combines their secret PIN (something they alone know) with a token code generated by their RSA SecurID authenticators (something they have). The result is a unique, one-time-use passcode that is used to positively identify, or authenticate, the user. If the code is validated by the RSA SecurID system, 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.

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.

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
- 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 on boarding of users to their credentials.

Verint Nextiva

Verint Nextiva 6.1

Verint Nextiva software aggregates physical security content from multiple sources, integrating IP networking and a full range of physical security systems, including:

- Video surveillance cameras
- Access control devices and intrusion detection systems
- Information security applications
- Visitor management and identity recognition
- Asset management
- Sensors and alarms
- RFID, biometrics, plus future enhancements and analytics

Nextiva Control Center

Nextiva Control Center is a client application used for administrating all aspects of the Nextiva application suite. The key functions of the Nextiva Control Center are:

- User setup and permissions
- Camera installation and configuration
- Alarm configuration, for example, motion detection
- Media control, for example, specifying which disks to use for video

Nextiva Recorder Server

The Nextiva Recorder Server captures live video streams to storage volumes for archiving. The Recorder application keeps a separate index for all the video captured and acts as the source for video playback and review requests.

The key functions of the Nextiva Recorder Server are to:

- Ingest video and place that video on disk
- Perform motion detection functions if required
- Maintain a database of the video to which the recorder writes
- Remove video when the retention period expires

There can be many Recorder Servers within the same Nextiva system.

Nextiva Master Server

The key functions of the Nextiva Master Server are to:

- Maintain the SQL database for the Nextiva system
- Track system events and alarms
- Authenticate users into the Nextiva system
- Authenticate servers into the Nextiva system

- Watch all the servers in the system and react to failures (Nextiva watchdog function)
- Provide access to the video capture by the Nextiva recorders

The Nextiva Master Server and Nextiva Recorder Server applications can be installed on a single server if required. This configuration is referred to as the Master Recorder.

There can be only one Nextiva Master Server within a Nextiva system.

Nextiva Review

Nextiva Review is a client application that is accessed by ordinary users of the Nextiva system. Nextiva Review can be used to:

- View live data. Nextiva Review drives one or more monitors that are used by security personnel to view feed from live cameras.
- Review recorded video. This is done by security personnel evaluating an event or alarm.

Nextiva Review is compatible with the RSA SecurID Windows Authentication agent, and provides multiple secure-access layers to the physical security infrastructure, and authenticated tamper-proof video data for increased conviction rates.

Login process for Verint Nextiva in an RSA SecurID environment

Login process overview

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

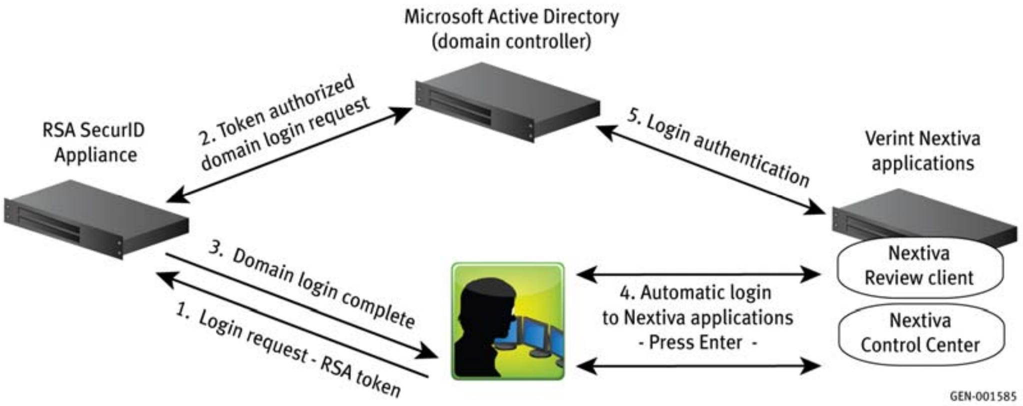


Figure 1 Login process overview

Login process description

The login process for Verint Nextiva in an RSA SecurID environment consists of five phases. Table 1 describes the process.

Table 1 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 Nextiva	The user does not need to enter credentials again. The user may be required to press **Enter** before continuing into the application (this is application-specific).
5	Login authentication	To ensure that the user has access rights for the requested application, the Nextiva application proxies the login request to Active Directory for authentication. The user is then able to use the chosen Nextiva application.

Environment

Prerequisites

This solution environment has the following prerequisites:

- RSA SecurID has been installed into an existing Active Directory domain.
- RSA two-factor authentication is successfully implemented and tested within a Windows domain environment.
- Clients 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 Nextiva 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.

Nextiva

- RSA SecurID was tested against:
  - A pre-existing Active Directory Windows domain
  - An Active Directory Windows domain specific to the Verint Nextiva install
- Nextiva clients on client systems:
  - Nextiva Review client
  - Nextiva Control Center client

Note Nextiva Control Center was configured in Windows authentication mode; therefore, Nextiva Authentication was not available. This was done to ensure that the login authentication is carried out by RSA SecurID, and not by the Nextiva application.

Hardware resources

Table 2 lists the hardware resources that were used to validate the solution.

Table 2 Hardware resources

Equipment	Quantity	Configuration
RSA SecurID Appliance	1	Specified in the RSA documentation
Nextiva Review workstation	1	Specified in the Verint Nextiva documentation
Nextiva Control Center workstation with Active Directory	1	Specified in the Verint Nextiva documentation

Software resources

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

Table 3 Software resources

Software	Version	Configuration
Microsoft Windows Server 2003	SP2/R2	Domain controller, Active Directory, and DNS Operating system for the Nextiva servers and workstations Operating system for RSA Authentication Agent
RSA Authentication Agent	6.1.3	
Nextiva Master Server	2	One server with the Active Directory option and another without Active Directory using the existing Active Directory.
Nextiva Recorder Server	Multiple	
Nextiva Control Center	2	
Nextiva Review	1	

Configuring Verint Nextiva for use with RSA SecurID

Process overview

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

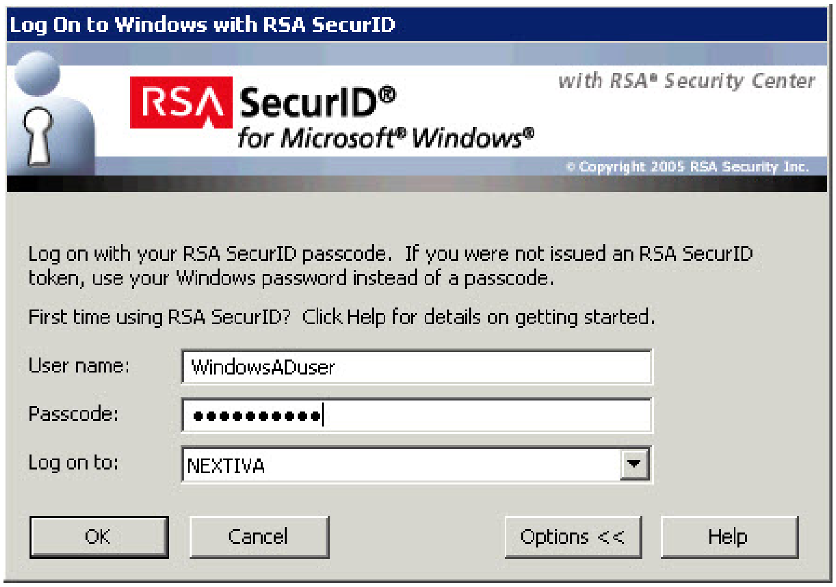
1. Install Nextiva 6.1.
2. Configure Nextiva for Windows authentication.
3. Switch from Nextiva authentication mode to Windows authentication mode.
4. Map Active Directory user groups to Nextiva user groups.

Each of these steps is described in detail below.

Installing Nextiva

To install Nextiva 6.1 follow the steps described in Table 4.

Table 4 Installing Nextiva

Step	Action
1	Log in to a server or workstation using a valid username and an RSA passcode, consisting of a secret PIN and a token code generated by an RSA authenticator.  Log On to Windows with RSA SecurID RSA SecurID® for Microsoft® Windows® with RSA® Security Center © Copyright 2005 RSA Security Inc. Log on with your RSA SecurID passcode. If you were not issued an RSA SecurID token, use your Windows password instead of a passcode. First time using RSA SecurID? Click Help for details on getting started. User name: WindowsADuser Passcode: ●●●●●●●●●● Log on to: NEXTIVA OK Cancel Options << Help **Figure 2 Log On to Windows with RSA SecurID**
2	Install the Nextiva 6.1 application. **Note** The server or workstation should already be part of a Windows domain.
3	Clear the checkboxes for the Active Directory/DNS install options.
4	Repeat these steps for each server and workstation that will run the Nextiva 6.1 application.

Windows authentication and Nextiva

RSA authentication requires that Nextiva be configured for Windows authentication. This means that user accounts and Windows group memberships are authenticated in Active Directory.

All user account management for the Nextiva system is performed by the Nextiva administrator in Active Directory. This includes creating, deleting, renaming, activating, and deactivating user accounts, as well as creating user groups and assigning users to these groups. Typically, the same user accounts and groups are used for all Windows-based applications in the organization.

- The Nextiva administrator maps the Active Directory groups to Nextiva user groups.
- Users who log in to Nextiva applications and are authenticated with their Windows user name and password.

Switching from Nextiva authentication to Windows authentication

By default, Nextiva is configured to perform authentication at the application level. After Nextiva is installed, it is necessary to switch from Nextiva authentication mode to Windows authentication mode. This enables Nextiva to use Active Directory for user authentication.

To switch from Nextiva authentication mode to Windows domain authentication mode, follow the steps described in Table 5.

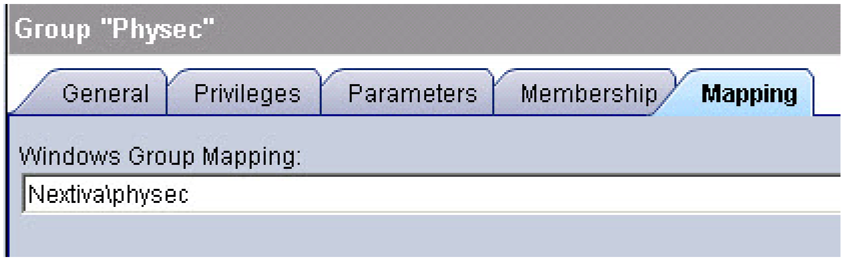
Table 5 Switching from local authentication to Windows authentication

Step	Action
1	Configure the Active Directory Bridge service.
2	Switch the system to Windows authentication.
3	Map the Active Directory user groups to the Nextiva user groups.
4	Log in to the Windows domain.

Mapping Active Directory user groups to Nextiva user groups

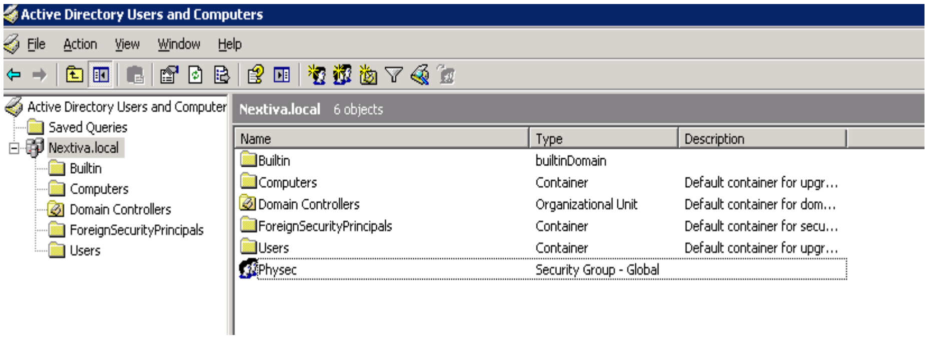
To map Active Directory user groups to Nextiva user groups follow the steps described in Table 6.

Table 6 Mapping Active Directory user groups to Nextiva user groups

Step	Action
1	Log in to Nextiva Control Center as an Administrator.
2	Select **Global settings** > **Groups and privileges**.
3	Select a Nextiva group from the tree view on the left side of the screen.
4	Select the **Mapping** tab.  Group "Physec" Windows Group Mapping: Nextiva\physec General Privileges Parameters Membership Mapping **Figure 3 Global Settings > Groups and privileges > Mapping**
5	Type the Windows group game, using the format <domain>\<group name>. For example, Nextiva\Administrators.
6	Click **Validate**. If the Windows group does not exist an error message is displayed, directing you to type another group name or to ask your system administrator to add the group to Active Directory.
7	Click **Apply**.

Different groups can be created for administrators, health monitors, and so on, depending on the privileges assigned to users.

Figure 4 and Figure 5 show the details of a group called “Physec” created in Active Directory. This group is mapped in the Nextiva application. Only users that belong to this group are authorized to access the Nextiva application.

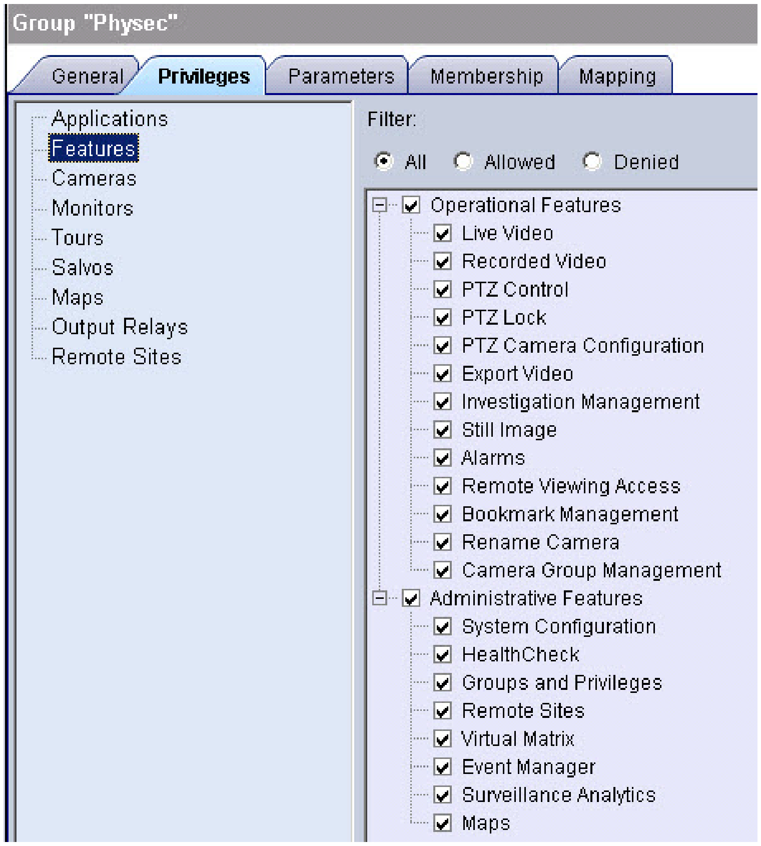

Active Directory Users and Computers
File Action View Window Help

- Active Directory Users and Computer
  - Saved Queries
  - Nextiva.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Users

Nextiva.local 6 objects

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgr...
Domain Controllers	Organizational Unit	Default container for dom...
ForeignSecurityPrincipals	Container	Default container for secu...
Users	Container	Default container for upgr...
Physec	Security Group - Global	

Figure 4 Active Directory > Nextiva groups



- Applications
- Features
- Cameras
- Monitors
- Tours
- Salvos
- Maps
- Output Relays
- Remote Sites

Filter: ● All ○ Allowed ○ Denied

- ☑ Operational Features
  - ☑ Live Video
  - ☑ Recorded Video
  - ☑ PTZ Control
  - ☑ PTZ Lock
  - ☑ PTZ Camera Configuration
  - ☑ Export Video
  - ☑ Investigation Management
  - ☑ Still Image
  - ☑ Alarms
  - ☑ Remote Viewing Access
  - ☑ Bookmark Management
  - ☑ Rename Camera
  - ☑ Camera Group Management
- ☑ Administrative Features
  - ☑ System Configuration
  - ☑ HealthCheck
  - ☑ Groups and Privileges
  - ☑ Remote Sites
  - ☑ Virtual Matrix
  - ☑ Event Manager
  - ☑ Surveillance Analytics
  - ☑ Maps

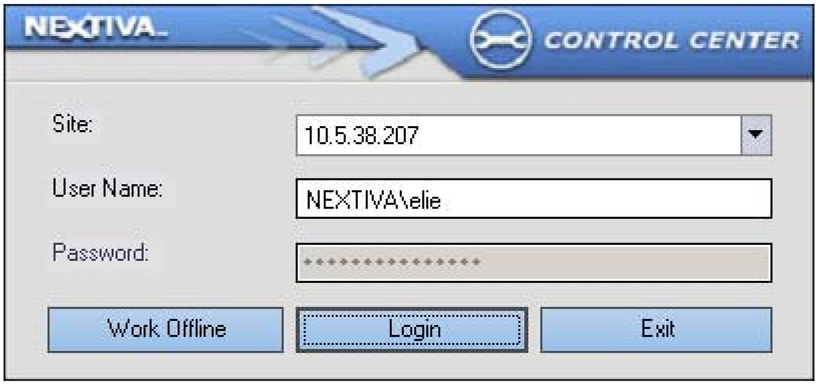
Figure 5 Details of Active Directory group “Physec”

Once the group is set and has been assigned the required privileges, the user can log in to the Nextiva application by double-clicking the Nextiva Control Center icon. The Nextiva application inherits the credentials from the Windows domain login, and the password field is grayed out.

Logging in to Nextiva with RSA SecurID enabled

Once Nextiva is configured for Windows authentication, and the appropriate Active Directory groups are mapped to the Nextiva groups, the user login experience is as described in Table 7:

Table 7 Logging in to Nextiva 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 Nextiva Control Center or Nextiva Review client icon.
3	The Nextiva login screen is displayed. The login screen inherits the credentials from the network login, and the password is grayed out.  Site: 10.5.38.207 User Name: NEXTIVA\elie Password: ****************
4	To access the Nextiva application, the user presses **Enter**.

Validation

Test objective

The objective of this test is to verify the integration of Verint Nextiva 6.1 within an RSA-secured Windows domain, and to demonstrate that secure single login operates correctly for users of the Nextiva Review and Nextiva Control Center clients.

Test scenarios

Scenario description		Expected results
1	A test user, who is a member of the Nextiva group in Active Directory, logs in to the Windows domain using an RSA passcode. The user then attempts to access the Nextiva Review client or the Nextiva Control Center client.	The user successfully accesses the client application, and does not need to enter credentials during Nextiva client login.
2	The test user is removed from the Nextiva group in Active Directory. The test user logs in to the Windows domain using an RSA passcode. The test user then attempts to access the Nextiva Review client or the Nextiva Control Center client.	The user successfully accesses the Windows domain, and is denied access to the Nextiva client application.

Test procedures

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

The following test procedure was followed for both Nextiva Review and Nextiva Control Center.

1. Ensure that Nextiva authentication is turned off.
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 Nextiva client icon.
4. The Nextiva client login screen is displayed, press **Enter.**

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

Scenario 2: User is not a member of the Nextiva group in Active Directory

The following test procedure was followed for both Nextiva Review and Nextiva Control Center.

1. Remove the user from the Nextiva group in Active Directory.
2. Ensure that Nextiva authentication is turned off.
3. Log in to the Windows domain using an RSA passcode, created by combining a PIN with a token generated by an RSA authenticator.
4. Double-click the Nextiva client icon.

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

Test results

Scenario 1: User is a member of the Nextiva 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 Nextiva client application.

Scenario 2: User is not a member of the Nextiva group in Active Directory

The user was able to log in to the RSA-secured Windows domain, but was denied access to the Nextiva 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 Nextiva application logon.

In all cases, the Verint Nextiva system was installed in an RSA-secured domain and performed very well in the EMC lab environment.

RSA integration with Nextiva provides several operational and system security benefits. These benefits include:

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

Findings

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

A user can be easily authorized to access Nextiva client applications by adding them to the appropriate Nextiva group in Active Directory. In turn, Nextiva access rights can be easily revoked by removing a user from the Nextiva 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:
EMC Tiered Storage for Physical Security - Enabled by EMC CLARiiON, EMC Centera, and Verint Nextiva

RSA SecurID

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

- *RSA SecurID Implementation 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*

Verint Nextiva

For additional information about Verint Nextiva, see:
Nextiva Installation Guide