Abstract

This guide describes required components and configuration steps for deploying RSA SecurID® two-factor authentication in the VSPEX VMware View end-user computing proven infrastructures. This guide and its associated Design Guide are designed to be used as additions, or “overlays,” to one of the specific VSPEX View proven infrastructure documents.

January, 2013
Copyright © 2013 EMC Corporation. All rights reserved. Published in the USA.

Published January 2013

EMC believes the information in this publication is accurate 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. Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC², EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to the technical documentation and advisories section on the EMC online support website.

**Securing VSPEX VMware View 5.1 End-User Computing Solutions with RSA, VMware vSphere 5.1 for up to 2000 Virtual Desktops**

**Implementation Guide**

Part Number H11373
Securing VSPEX VMware View 5.1 End-User Computing Solutions with RSA, VMware vSphere 5.1 for up to 2000 Virtual Desktops

Chapter 1   Introduction.................................................................9
Purpose .........................................................................................10
Business value ...........................................................................10
Scope ..........................................................................................10
Audience .....................................................................................10

Chapter 2   Solution Overview.......................................................11
Key components ...........................................................................12
   Existing infrastructure .............................................................12
   RSA SecurID with Authentication Manager ............................12
   EMC VSPEX ...........................................................................12
   Virtual machine requirements and profile ...............................12
High-level solution architecture ..................................................14
   Architecture overview .............................................................14

Chapter 3   Before You Start........................................................17
Prerequisites ................................................................................18
   Ensure availability of compute, memory, and storage resources ...18
   Acquire software and licenses .................................................18
   Allocate required IP Addresses, create DNS entries ...............18
   Acquire SSL certificates – Authentication Manager ................18
   Acquire SSL certificates – VMware View ..............................19
   Create two Windows Server 2008 R2 guests .........................19
Support resources ........................................................................19

Chapter 4   Solution Implementation.............................................21
Server, virtualization, and network implementation ....................22
   Design considerations ............................................................22
Application implementation .........................................................22
   Install and configure RSA Authentication Manager ...............22
   Configure VMware View for SecurID functionality ...............25
Figure 1. Logical architecture: generalized VSPEX VMware View 5.1 proven infrastructure with RSA Authentication Manager overlaid in a redundant configuration........................................................................................................ 14
Figure 2. VMware View Client.......................................................................................... 28
Figure 3. View Client SecurID authentication dialog ..................................................... 28
Figure 4. View Client Active Directory authentication dialog ........................................ 29
Table 1. Baseline compute, memory, and storage requirements for SecurID overlay .......................................................... 13
Table 2. Required configuration information for Authentication Manager....... 34
Table 3. Required configuration information for VMware View..................... 34
This chapter presents the following topics:

Purpose........................................................................................................10
Business value ..........................................................................................10
Scope..........................................................................................................10
Audience.................................................................................................10
Purpose

This document provides an end-to-end configuration pathway for the deployment of RSA SecurID two-factor authentication in a VSPEX VMware View end-user computing infrastructure.

EMC VSPEX End-User Computing Solutions for VMware View 5.1 and VMware vSphere 5.1 provide proven, best-of-breed solutions for end-user computing. Customers requiring additional access protection for remotely available or sensitive View environments can enable RSA SecurID two-factor authentication as a highly-effective additional layer of virtual desktop access protection. In addition to Active Directory credentials, accessing a SecurID-protected resource requires a personal identification number and a constantly changing code from a hardware or software-based “token”. Credentials based on something the user knows (the PIN) and something the user has (the token code) is the basis of two-factor authentication and is a standard in access security.

Implementation of SecurID in VSPEX View infrastructures requires deployment of RSA Authentication Manager as part of the supporting infrastructure. SecurID is tightly integrated into View 5.1; once Authentication Manager is online, activation of SecurID through the View Administrator Console and Authentication Manager Security Console takes minutes.

Business value

As described in their individual infrastructure documentation, VSPEX VMware View end-user computing solutions provide defined infrastructures with proven, tested performance, scalability, and functionality for up to 2000 desktops. This overlay enhances the value proposition by strengthening access security, especially for remote connections.

Scope

The access and security enhancements presented in this guide are assembled as an “overlay” to the VMware View VSPEX solutions. This document briefly describes SecurID and Authentication Manager, illustrates their integration into the VSPEX solution, and presents an end-to-end configuration path based on RSA and VMware installation documentation. The overlay is not intended as a stand-alone solution; infrastructure services built into the VSPEX solutions (notably Active Directory and DNS) are used to support the extended functionality described here.

This guide is intended to be used in conjunction with the VSPEX Proven Infrastructure documents for VMware View. Familiarity with the relevant solution documents is a minimum prerequisite for using this guide.

Audience

This guide is targeted to EMC internal staff and channel partners. It is not intended for external distribution or the VSPEX end users.
Chapter 2  Solution Overview

This chapter presents the following topics:

Key components ........................................................................................................12
High-level solution architecture .............................................................................14
Key components

**Existing infrastructure**
The View environment and supporting infrastructure services such as Active Directory and DNS should be configured according to the appropriate VSPEX end-user computing proven infrastructure document. Compute and storage resource for the components described below may be added for the purpose or consumed from the solution pool as described later in this overlay document.

**RSA SecurID with Authentication Manager**
RSA SecurID provides enhanced access security through two-factor authentication, which requires the user to answer an authentication challenge with two pieces of information:

- A personal identification number (PIN) – something the user knows, analogous to a password.
- A one-time token code or password from a hardware- or software based token – something the user has in possession. This token code changes every 60 seconds.

SecurID functionality is managed by RSA Authentication Manager, which for this overlay is installed on redundant Windows® Server 2008 R2 virtual machines. Built-in Authentication Manager features provide backup and synchronization services.

Authentication Manager is used to create an Authentication Record corresponding to the Authentication Agent that is built into the View Connection Server. With creation of the record, the View Connection server is registered as an authentication agent with Authentication Manager. A configuration file containing this information is then generated. When SecurID is enabled on the View connection server, this file is uploaded to complete the link between View and Authentication Manager.

**Note** Authentication Manager (version 7.1) can be installed on Windows or Linux and is also available as a physical appliance. This overlay utilizes the virtualized Windows Server environment on which the VSPEX VMware View solutions are built.

**EMC VSPEX**
VSPEX validated and modular architectures are built with proven best-of-breed technologies to create complete virtualization solutions that enable you to make an informed decision about the hypervisor, compute, and networking layers. VSPEX eliminates desktop virtualization planning and configuration burdens. VSPEX accelerates your IT Transformation by enabling faster deployments, greater choice, efficiency, and lower risk.

**Virtual machine requirements and profile**
Refer to the VSPEX Proven Infrastructure for VMware View document for the hardware requirement information, which defines a standard “Reference Virtual Machine.”

**Table 1** shows the compute, memory, and storage requirements for a high-availability SecurID implementation. This resource can be drawn from the VSPEX pool with a corresponding reduction in desktop capacity, or additional server hardware can be added.
Ensure that the redundant Authentication Manager nodes are placed on the different physical servers so that a hardware failure does not interrupt service.

The Active Directory and DNS services that are already in place for the VSPEX VMware View environment are used to support the SecurID components; additional imposed overhead is minimal and not expected to require additional hardware.

**Table 1. Baseline compute, memory, and storage requirements for SecurID overlay**

<table>
<thead>
<tr>
<th></th>
<th>CPU (cores)</th>
<th>Memory (GB)</th>
<th>Disk (GB)</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA Authentication Manager</td>
<td>2</td>
<td>8*</td>
<td>60</td>
<td>RSA Authentication Manager 7.1 Performance and Scalability Guide</td>
</tr>
</tbody>
</table>

* RSA recommends an 8 GB minimum for VMware-based deployments. A 4 GB or even 2 GB configuration is acceptable on stand-alone servers.

According to the *RSA Authentication Manager 7.1 Performance and Scalability Guide*, a small current-generation server with a single dual-core processor and 2 GB RAM can process 40 SecurID authentications per second. Thus, an entire user database for a 2,000 desktop VSPEX environment can be authenticated in under a minute (RSA tests performed on dedicated hardware with no antivirus, security, or other software installed).

**Note** Deployment of Authentication Manager on VMware guests involves specific requirements and restrictions.

- Allocated memory should be set to 8 GB for 64-bit operating systems.
- Cloning, physical-to-virtual conversion, and virtual-to-physical conversion are supported.
- Snapshots, vMotion™, High Availability, and several other VMware virtualization features are not supported. RSA recommends using the Authentication Manager built-in features for these types of services.

See *Authentication Manager 7.1 Service Pack 4 Release Notes* (available on RSA SecurCare® Online) for more information.
High-level solution architecture

Figure 1 shows the generalized logical architecture of the VSPEX VMware View infrastructures with the Authentication Manager hosts added. The VNX with Fibre Channel variant is shown. NFS and VNXe variants are described in the VMware View VSPEX proven infrastructure documents.

Figure 1. Logical architecture: generalized VSPEX VMware View 5.1 proven infrastructure with RSA Authentication Manager overlaid in a redundant configuration

Architecture overview

The SecurID overlay architecture consists of the following components.

**EMC VSPEX End-User Computing: VMware View 5.1 and VMware vSphere 5.1 for up to 250 or 2000 Virtual Desktops** – The foundation infrastructure supports View and provides Active Directory, DNS, DHCP, and SQL Server services. Active Directory and DNS are also utilized by the overlay.

**RSA Authentication Manager 7.1 SP4** – Authentication Manager controls all operational aspects of SecurID functionality. Authentication agent functionality is built into VMware View, eliminating the necessity of manually installing agent software. Once Authentication Manager is online, enabling SecurID in the View environment consists of the following steps:

1. Create an Agent Record in Authentication Manager Security console to register the View server as an authentication agent.
2. Generate and download a configuration file from the Authentication Manager to provide shared secret and other information to the View server(s).
3. Enable SecurID in the View Administrator console and upload the configuration file.
The *RSA Authentication Manager 7.1 Administrator’s Guide* contains steps for importing and assigning SecurID tokens to users.

Redundant nodes provide high availability. Authentication Manager’s installation wizard provides easy setup of primary and secondary nodes. After setup, changes are made to the primary, and are then ported to the secondary via a synchronization process. If one node becomes unavailable, the remaining node services traffic.

**Note**  For VMware installation, ensure that nodes are installed on different physical hosts to preclude a service interruption caused by hardware failure.
This chapter presents the following topics:

Prerequisites ........................................................................................................... 18
Support resources .................................................................................................... 19
Before You Start

Prerequisites

Steps contained in this guide are targeted to an existing VSPEX VMware View end-user computing infrastructure, as described in the following documents:

- **EMC VSPEX End-User Computing: VMware View 5.1 and VMware vSphere 5.1 for up to 250 Virtual Desktops, Enabled by EMC VNXe and EMC Next Generation Backup – VSPEX Proven Infrastructure**
- **EMC VSPEX End-User Computing: VMware View 5.1 and VMware vSphere 5.1 for up to 2000 Virtual Desktops, Enabled by EMC VNX and EMC Next Generation Backup – VSPEX Proven Infrastructure**

Complete the following steps before installation.

Ensure availability of compute, memory, and storage resources

Refer to Table 1 for guidance on resource provisioning.

Acquire software and licenses

The following software and licenses are required:

- RSA Authentication Manager 7.1 SP4 or later (plus sufficient hardware or software tokens): Installation media received or downloaded, and licenses, tokens, token records, and import passwords that have been received from RSA
- Licenses for two Windows Server 2008 R2 instances

**Note** Authentication Manager is available as a physical appliance, which can be implemented in place of the virtual appliance installation steps below. Post-installation configuration is the same.

Allocate required IP Addresses, create DNS entries

Use the tables in Appendix A to plan and record naming and network information for Authentication Manager hosts.

Acquire SSL certificates – Authentication Manager

SSL certificates are required for the RSA Authentication Manager servers (two). Refer to “Managing Certificates and Keystores for SSL” in the *RSA Authentication Manager Installation and Configuration Guide* for instructions to generate and assign SSL certificates for Authentication Manager.

Since SSL certificates are assigned to a specific Fully Qualified Domain Name (FQDN), it is important to carefully plan naming conventions for physical and virtual servers.

Upon receipt from the issuing Certificate Authority (CA), copy SSL certificates to a location that can be easily accessed by the Authentication Manager servers, such as a network share or VMware datastore.
If the View servers do not yet have SSL certificates in place, refer to the VMware View Installation document available through the “View support” section of the VMware website at [http://www.vmware.com](http://www.vmware.com) for instructions.

These virtual machines are used for the primary and secondary Authentication Manager nodes.

Each instance should be configured and patched to production standards and joined to applicable domain.

Support resources

Support of SecurID and Authentication Manager is provided through RSA ([http://www.rsa.com](http://www.rsa.com)).

Support for VMware View is provided through VMware ([http://www.vmware.com](http://www.vmware.com)).
Before You Start
This chapter presents the following topics:

- Server, virtualization, and network implementation ........................................... 22
- Application implementation .................................................................................. 22
- Backup and recovery ............................................................................................ 26
Solution Implementation

Server, virtualization, and network implementation

Design considerations

The primary new requirement for enabling SecurID in the VSPEX View infrastructures is installation of a high availability (HA) Authentication Manager environment. Active Directory, DNS, and other infrastructure services supporting the View environment also support Authentication Manager.

This overlay is intended to provide a basic HA Authentication Manager service in the VSPEX VMware View environment. Optimization and operational planning (for backup, node synchronization, etc.) are beyond the scope of the guide.

Infrastructure for the SecurID overlay conforms to the design presented in the relevant VSPEX VMware View end-user computing proven infrastructure. Storage requirements are minimal and should be available from the VSPEX pool without additional drives.

Application implementation

The following configuration activities are required to implement RSA SecurID in a VSPEX VMware View deployment:

- Install and configure RSA Authentication Manager
- Configure VMware View for SecurID functionality

Install and configure RSA Authentication Manager

This section contains steps for installing a high-availability Authentication Manager 7.1 SP4 on Windows Server 2008 R2 virtual machines. The steps are performed in the Authentication Manager installation wizard. As the wizard proceeds, use default settings except as noted. Be sure to record all information used, such as IP assignments, IDs and passwords, DNS aliases, etc.

References

- RSA Authentication Manager 7.1 Installation and Configuration Guide
- RSA Authentication Manager 7.1 Administrator’s Guide

Steps

1. Install Authentication Manager 7.1SP4 on the primary host, using IP, DNS, and other network information previously recorded in Appendix A.

   a. Map target server access to the installation media.
   b. Place the license files in the same location as media for easy access when prompted.
   c. Start the installation executable. Double-click the autorun.exe file if necessary. When prompted, provide the following information:

      - Installation type: Primary instance
      - Path to License file folder
      - RSA Security Console credentials
Solution Implementation

Note

- The RSA Security Console credentials are local credentials. Record and store them in a secure location.
- The installation triggers creation of a 2048-byte certificate issued by "RSA Authentication Manager Root CA" for the FQDN of the Authentication Manager host.

2. To import the Certificate Authority root certificate, select Deployment Configuration → Certificates → Identity Source Certificates in the Security Operations Console.

3. To set up Active Directory as identity source, select Deployment Configuration → Identity Sources → Add New in the Security Operations Console.
   a. When the wizard prompts for the AD source in the Directory URL: field, use ldaps instead of http or https as the protocol.
   b. In the Directory User ID field, use the fully qualified <domain><userid> format.

Note Refer to the following examples of Active Directory entries:

- Directory URL: ldaps://myDomainController.myDomain.com
- User Base DN: cn=Users,dc=myDomain,dc=com
- User Group Base DN: cn=Users,dc=myDomain,dc=com (same as base DN)

   c. Link the new AD identity source to the default System Domain or custom realm to make AD users available for token assignment. See “Appendix A Linking an Identity Source to a Realm,” in the Administrator’s Guide for more information.
      i. Navigate to Security Console → Administration → Realms → Manage Existing.
      ii. Select the realm.
      iii. Click Edit.
      iv. Follow the instructions in the dialog for other options.

4. Generate an Authentication Manager "replica package file" according to Chapter 4 of the Installation and Configuration Guide. Even when Automatic option is selected for how to transfer data, click the link to download and save the .pkg file.

5. Configure a secondary host (replica) for High Availability.
   a. Run the AuthMgr 7.1SP4 installable file.
      i. Select Replica instance for the installation type in setup wizard.
      ii. When prompted, provide a path to the .pkg file generated in step 4.
   b. After installation, follow the steps in Chapter 4 of the Installation and Configuration Guide to connect the primary and replica.
c. Start the Security Operations Console on the replica (the only available Authentication Manager service) and trigger the connection function presented. It may run a long time.

6. Confirm the replication link between primary and secondary nodes.
   a. On Security Operations Console, navigate to Deployment Configuration → Instances → Manage Existing.
   b. Click Check Replication Status at the bottom of the page.
   c. The resulting Replication Status Report page provides help for resolving any necessary actions.

7. Set up tokens.
   Note This step can be performed either now or deferred until the remainder of the SecurID infrastructure is configured.
   a. Import Token Records, which are supplied on compact disks (CDs) from RSA along with license files, and the actual tokens into the primary AM server.
      i. On Security Console, navigate to Authentication → SecurID Tokens → Import Tokens Job → Add New.
      ii. Follow steps provided in RSA SecurID Token Records Getting Started Guide on the token records CD.
   b. To assign tokens to users, follow steps in the "Deploying Tokens to Users" section in Chapter 3 of the Administrator's Guide.
      ii. Click the Unassigned tab.
      iii. Select a token to assign.
      iv. Ensure the Assign to Users… function is selected in the token list.
      v. Click Go.

8. Register VMware View servers as authentication agents.
   a. On primary Authentication Manager node, log in to the RSA Security console using the local administrator credentials created during installation.
   c. Enter the following information. Use default values for the fields not explicitly cited here, unless the new deployment expressly requires a different entry:
      i. Hostname: FQDN of the View server
      ii. IP Address: select Resolve IP adjacent to the Hostname field to populate this field. Verify the address is the management address of the View host.
d. If this is the final View server to be added, click Save; otherwise, click Save & Add Another and repeat the preceding steps.

9. Create the configuration file that will be uploaded to VMware View in the next section.
   a. On the primary Authentication Manager node, log in to the RSA Security console using the local administrator credentials created during installation.
      i. The only configurable values on the page pertain to timeout retry settings. Default values are acceptable.
      ii. Click Generate Config File.
      iii. Click Download Now to save the file in a location accessible to the View server to which the file is uploaded.
      iv. The file is downloaded as a ZIP file. Extract the single file (sdconf.rec).

Configure VMware View for SecurID functionality

The following steps give guidance for enabling SecurID authentication on a single VMware View management server in the VSPEX infrastructure. Repeat these steps for each View server for which SecurID is to be implemented.

1. If not already in place, install SSL certificates per guidance in the VMware View Installation document that is available through the View support section of the VMware website at http://www.vmware.com.

2. Log in to the View Administration Console with administrator privilege.


4. Click the Connection Servers tab.

5. Select the connection server to be SecurID-enabled and click Edit....
   a. In the Edit View Connection Server Settings dialog, click the Authentication tab.
   b. In the Advanced Authentication section, select RSA SecurID in the 2-Factor Authentication list box.
   c. Select Enforce SecurID and Windows user name matching to ensure that a SecurID and associated Active Directory ID match.
   d. Click Upload File... to select and upload the sdconf.rec downloaded earlier.
   e. After uploading the file, SecurID function is enabled without any reboot or service restart.
Backup and recovery

Backup and recovery are described in the infrastructure documentation for the VSPEX solution to which SecurID is being added. RSA recommends the use of its native toolset for backup and restoration of the Authentication Manager internal database.
Chapter 5  Solution Validation

This chapter presents the following topics:

Baseline hardware validation .......................................................... 28
RSA SecurID validation ................................................................. 28
RSA Authentication Manager validation ........................................... 30
Baseline hardware validation

Hardware validation is beyond the scope of this document. Refer to the VSPEX View proven infrastructure documents for more information.

RSA SecurID validation

To check SecurID function, follow these steps:

1. Start the VMware View Client shown in Figure 2, and click Connect.

2. The View Client SecurID authentication dialog box appears. Type the SecurID user id and passcode configured during Authentication Manager setup, as shown in Figure 3.
3. Upon successful SecurID authentication, the View Client Active Directory authentication dialog box appears as shown in Figure 4. After successful Active Directory authentication, the user desktop is presented.

![View Client Active Directory authentication dialog](image)

**Figure 4.** View Client Active Directory authentication dialog
RSA Authentication Manager validation

Presentation of the View Client dialog box prompting for SecurID name and passcode and subsequent successful authentication is the practical success criterion.

Take the following steps for more information.

1. On Authentication Manager Security Console, open **Reporting → Realtime Activity Monitors → Authentication Activity Monitor**. Type the user name to be verified in the **Search** field if necessary.
2. Click **Start Monitor**.
3. Log in to a desktop through the View Client, going through the two-step authentication process.
4. In the monitor window, verify that SecurID credentials are validated.
5. Close the monitor.

Basic High Availability function can be tested in the following procedure.

1. Using VMware vSphere, edit the settings for the primary Authentication Manager node to disconnect the guest virtual NIC, or shut down the guest.
2. Verify successful SecurID authentication.
3. Reconnect the primary node virtual NIC.
4. Repeat the preceding steps with the secondary node.
This chapter presents the following topics:

**Product documentation** ........................................................................................................32
**Other documentation** ...........................................................................................................32
Product documentation

For additional information, see the product documentation listed below.

- *Securing VSPEX VMware View 5.1 End-User Computing Solutions with RSA, VMware vSphere 5.1 for up to 2000 Virtual Desktops* - Design Guide

- *EMC VSPEX End-User Computing: VMware View 5.1 and VMware vSphere 5.1 for up to 250 Virtual Desktops,Enabled by EMC VNXe and EMC Next Generation Backup* – VSPEX Proven Infrastructure

- *EMC VSPEX End-User Computing: VMware View 5.1 and VMware vSphere 5.1 for up to 2000 Virtual Desktops, Enabled by EMC VNX and EMC Next Generation Backup* – VSPEX Proven Infrastructure

Other documentation

For additional information, see the documents listed below.

- *RSA Authentication Manager 7.1 Installation and Configuration Guide*

- *RSA Authentication Manager 7.1 Administrator’s Guide*

- *RSA Authentication Manager 7.1 Performance and Scalability Guide*

- *VMware RSA SecurID Ready Implementation Guide*
This appendix presents the following topic:

Table of required configuration information ...................................................... 34
### Table 2. Required configuration information for Authentication Manager

<table>
<thead>
<tr>
<th></th>
<th>Primary</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname (FQDN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCenter (ESXi) host</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install media location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>License and token record file location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local admin ID/password</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 3. Required configuration information for VMware View

<table>
<thead>
<tr>
<th></th>
<th>Primary</th>
<th>Secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname (FQDN)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCenter (ESXi) host</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local admin ID/password</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>