Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

Dell, RSA, the RSA Logo, EMC and other trademarks, are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell Inc. or its subsidiaries are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by Dell Inc.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any Dell software described in this publication requires an applicable software license.

Dell Inc. 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.” DELL INC. 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.

Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

December 2018

Revised: July 2019
# Contents

**Revision History** ......................................................................................................................... 9  
**Preface** ......................................................................................................................................... 11  
  About This Guide ............................................................................................................................. 11  
  RSA SecurID Access Support and Service ....................................................................................... 11  
  Support for RSA Authentication Manager ...................................................................................... 11  
  Support for the Cloud Authentication Service and Identity Routers ............................................. 11  
  RSA Ready Partner Program ............................................................................................................ 11  
**Chapter 1: Preparing for Deployment** ........................................................................................... 13  
  Planning Decisions .......................................................................................................................... 14  
  Appliance Support ............................................................................................................................ 14  
  Amazon Web Services Virtual Appliance Requirements ................................................................. 16  
  DNS Server Configuration on the Amazon Web Services Virtual Private Cloud ....................... 16  
  Create a DHCP Options Set ............................................................................................................. 17  
  Associate DHCP Options with a VPC .............................................................................................. 17  
  Change the VPC Properties ............................................................................................................. 17  
  Security Groups for Amazon Web Services ................................................................................... 18  
  Example of a Security Group for Outbound Rules ....................................................................... 18  
  Example of a Security Group for Inbound Rules ........................................................................... 19  
  Azure Virtual Appliance Requirements .......................................................................................... 20  
  DNS Server Configuration on the Azure Virtual Network ............................................................. 20  
  Create an Azure Network Security Group ...................................................................................... 20  
  Azure Feature Support .................................................................................................................... 22  
  VMware Virtual Appliance Requirements ..................................................................................... 22  
  VMware Software Requirements .................................................................................................... 23  
  VMware Software Support ............................................................................................................. 23  
  VMware Primary or Replica Instance Hardware Requirements ................................................... 23  
  VMware Feature Support ............................................................................................................... 24  
  Hyper-V Virtual Appliance Requirements ..................................................................................... 24  
  Hyper-V Software Requirements ................................................................................................... 25  
  Hyper-V Primary or Replica Instance Hardware Requirements ................................................ 25  
  Hyper-V Feature Support .............................................................................................................. 26
Supported Data Stores ................................................................. 26
  Internal Database ....................................................................... 26
  Supported Directory Servers ...................................................... 27
Supported Web Browsers ............................................................... 27
Supported RSA Authentication Agents .......................................... 28
RSA Authentication Manager License Support ............................. 28
Accurate System Date and Time Settings .................................... 29
Secure Appliance Deployment ....................................................... 30
Deployment Checklist for the Primary and Replica Instance .......... 31
  Amazon Machine Image Deployment ........................................... 31
  Azure Image File Deployment ..................................................... 31
  VMware Virtual Appliance Deployment ...................................... 31
  Hyper-V Virtual Appliance Deployment ...................................... 32
Hardware Appliance Deployment ................................................. 32
Quick Setup Checklist for the Primary Instance......................... 32
Quick Setup Checklist for the Replica Instance ............................ 33
Setup and Configuration Information List ..................................... 33
  Appliance Deployment .............................................................. 34
    Amazon Web Services Virtual Appliance ................................... 34
    Azure Virtual Appliance ......................................................... 34
    VMware or Hyper-V Virtual Appliance ..................................... 34
    Hardware Appliance .............................................................. 35
  Primary Appliance Setup .......................................................... 35
  Replica Appliance Setup ........................................................... 35
  Load Balancer Configuration ..................................................... 35
  Web Tier Installation .............................................................. 35

Chapter 2: Deploying a Primary Appliance ................................. 37
Perform Deployment Tasks for the Primary Instance ..................... 38
Deploy the RSA Authentication Manager Amazon Machine Image .... 38
Deploy the RSA Authentication Manager Azure Image File .......... 40
Deploy the Virtual Appliance Through VMware vCenter Server 6.0 43
Deploy the Virtual Appliance Through VMware vCenter Server 6.5 or 6.7 44
Deploy the Virtual Appliance Directly to the VMware ESXi 6.0 Server 46
Deploy the Virtual Appliance Directly to the VMware ESXi Server 6.5 or 6.7 ............................................. 47
Deploy the Virtual Appliance Through the Hyper-V Virtual Machine Manager Console .................................. 49
Deploy the Virtual Appliance Through the Hyper-V Manager ................................................................. 51
Deploy the Hardware Appliance ........................................................................................................... 53
Run Quick Setup on the Primary Instance .................................................................................................. 55
Certificate Management for Secure Sockets Layer ..................................................................................... 57
Log On to the Consoles .......................................................................................................................... 58

Chapter 3: Deploying a Replica Appliance ........................................................................................................... 61
Perform Deployment Tasks for a Replica Instance ...................................................................................... 62
Generate and Download a Replica Package File .......................................................................................... 62
Run Quick Setup on the Replica Instance .................................................................................................. 63
Attach the Replica Instance to the Primary Instance ..................................................................................... 66
Replica Attachment Issues and Solutions .................................................................................................. 67

Chapter 4: Configuring a Virtual Host and Load Balancer ................................................................................. 71
Virtual Host and Load Balancer Overview .................................................................................................. 72
Load Balancer Requirements .................................................................................................................. 72
Configure a Load Balancer and Virtual Host ............................................................................................. 72
Load Balance Using the Web Tier with Round Robin DNS ........................................................................ 74

Chapter 5: Installing Web Tiers .......................................................................................................................... 75
Web Tier Overview ....................................................................................................................................... 76
Self-Service, Dynamic Seed Provisioning, and RBA Traffic in a Web Tier ....................................................... 76
Web-Tier Hardware and Operating System Requirements ......................................................................... 77
Performing Web Tier Pre-Installation Tasks ............................................................................................. 78
Installing the Web Tier .................................................................................................................................. 79
Add a Web-Tier Deployment Record ......................................................................................................... 80
Web-Tier Installation Checklist .................................................................................................................. 81
Install a Web Tier on Windows Using the Graphical User Interface ............................................................. 82
Install a Web Tier on Windows Using the Command Line ........................................................................... 83
Install a Web Tier on Linux Using the Graphical User Interface ................................................................... 84
Install a Web Tier on Linux Using the Command Line ................................................................................ 86

Chapter 6: Next Steps for Your Deployment ..................................................................................................... 89
Next Steps for Your Deployment .................................................................................................................. 90

Appendix A: Upgrading to RSA Authentication Manager 8.4 ................................................................. 93
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports for the RSA Authentication Manager Instance</td>
<td>114</td>
</tr>
<tr>
<td>Restricting Access to the RSA Consoles</td>
<td>118</td>
</tr>
<tr>
<td>Required RSA RADIUS Server Listening Ports</td>
<td>118</td>
</tr>
<tr>
<td>Ports on the Web Tier with a Load Balancer Deployed</td>
<td>119</td>
</tr>
<tr>
<td>Ports on the Web Tier Without a Load Balancer</td>
<td>119</td>
</tr>
<tr>
<td>Access Through Firewalls</td>
<td>120</td>
</tr>
<tr>
<td>Securing Connections Between the Primary and Replica Instances</td>
<td>120</td>
</tr>
<tr>
<td><strong>Appendix D: Administrative Accounts</strong></td>
<td>121</td>
</tr>
<tr>
<td>System Administrator Accounts</td>
<td>122</td>
</tr>
<tr>
<td>Authentication Manager Administrator Accounts</td>
<td>122</td>
</tr>
<tr>
<td>Appliance Operating System Account</td>
<td>123</td>
</tr>
<tr>
<td>Manage a Super Admin Account</td>
<td>123</td>
</tr>
<tr>
<td><strong>Appendix E: Installing the RSA Authentication Manager Token Management Snap-In</strong></td>
<td>125</td>
</tr>
<tr>
<td>Overview</td>
<td>126</td>
</tr>
<tr>
<td>System Requirements</td>
<td>126</td>
</tr>
<tr>
<td>Install the Token Management Snap-In for Local Access</td>
<td>126</td>
</tr>
<tr>
<td>Install the Token Management Snap-In for Remote Access</td>
<td>127</td>
</tr>
<tr>
<td>Performing Post-Installation Tasks</td>
<td>129</td>
</tr>
<tr>
<td>Start the Active Directory User and Computer Management Console</td>
<td>129</td>
</tr>
<tr>
<td>Configure the Connection with Authentication Manager</td>
<td>129</td>
</tr>
</tbody>
</table>
### Revision History

<table>
<thead>
<tr>
<th>Revision Number</th>
<th>Date</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>May 2019</td>
<td>Added best practices for administrative accounts, including a recommendation to use separate administrative accounts with their own credentials for external identity sources and RSA Authentication Manager.</td>
</tr>
<tr>
<td>3</td>
<td>July 2019</td>
<td>Added a reference to the Model 350 hardware appliance.</td>
</tr>
</tbody>
</table>
Preface

About This Guide

This guide is intended for network and system administrators who are responsible for installing and securing the various components of an RSA® Authentication Manager deployment.

For a complete list of documentation, see "RSA SecurID Access Product Documentation" on RSA Link at https://community.rsa.com/docs/DOC-60094.

For a description of common RSA Authentication Manager terms, see the "RSA Authentication Manager Glossary" on RSA Link at https://community.rsa.com/docs/DOC-76682.

RSA SecurID Access Support and Service

You can access community and support information on RSA Link at https://community.rsa.com. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Support for RSA Authentication Manager

Before you call Customer Support for help with the RSA Authentication Manager appliance, have the following information available:

- Access to the RSA Authentication Manager appliance.
- Your license serial number. To find this number, do one of the following:
  - Look at the order confirmation e-mail that you received when you ordered the product. This e-mail contains the license serial number.
  - Log on to the Security Console, and click License Status. Click View Installed License.
- The appliance software version. This information is located in the top, right corner of the Quick Setup, or you can log on to the Security Console and click Software Version Information.

Support for the Cloud Authentication Service and Identity Routers

If your company has deployed identity routers and uses the Cloud Authentication Service, RSA provides you with a unique identifier called the Customer Support ID. This is required when you register with RSA Customer Support. To see your Customer Support ID, sign in to the Cloud Administration Console and click My Account > Company Settings.

RSA Ready Partner Program

The RSA Ready Partner Program website at www.rsaready.com provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.
Chapter 1: Preparing for Deployment

Planning Decisions ........................................................................................................... 14
Appliance Support ............................................................................................................. 14
Amazon Web Services Virtual Appliance Requirements .................................................. 16
 Azure Virtual Appliance Requirements ........................................................................... 20
 VMware Virtual Appliance Requirements ...................................................................... 22
 Hyper-V Virtual Appliance Requirements .................................................................... 24
 Supported Data Stores .................................................................................................... 26
 Supported Web Browsers ............................................................................................... 27
 Supported RSA Authentication Agents ............................................................................ 28
 RSA Authentication Manager License Support ............................................................... 28
 Accurate System Date and Time Settings ....................................................................... 29
 Secure Appliance Deployment ........................................................................................ 30
 Deployment Checklist for the Primary and Replica Instance ........................................... 31
 Setup and Configuration Information List ....................................................................... 33
Planning Decisions

Before you set up your RSA Authentication Manager deployment, you must decide which Authentication Manager components you want to install. A deployment can include the following components:

- **Primary Instance.** The instance on which all administration takes place. It can also service authentication requests.
- **Replica Instance.** Provides redundancy of the primary instance and authenticates users.
- **Web Tiers.** Allows the secure deployment of the RSA Self-Service Console, dynamic seed provisioning, and the risk-based authentication (RBA) service within the demilitarized zone (DMZ).
- **Load Balancer.** Used to distribute authentication requests and to facilitate failover between the primary and replica web tiers.
- **Authentication Agents.** Installed on any resource that you want to protect.

For more information on deployment planning topics, see the RSA Authentication Manager Planning Guide.

Appliance Support

RSA Authentication Manager supports an Amazon Web Services (AWS) virtual appliance, an Azure virtual appliance, a VMware virtual appliance, a Hyper-V virtual appliance, and a hardware appliance. Each type of appliance provides the same Authentication Manager features. You can use one type of appliance or both virtual and hardware appliances in your deployment.

Both a virtual appliance and a hardware appliance include a Linux operating system that is installed with Authentication Manager and RSA RADIUS server software. To configure an appliance as an Authentication Manager instance, you must complete Quick Setup.

The following differences apply:

- **AWS virtual appliance:**
  - Deployed on AWS or AWS GovCloud (US) with an Amazon Machine Image (AMI) file that RSA provides.
  - Requires a Virtual Private Cloud (VPC) with a private subnet on AWS.
  - Supports a mixed deployment with cloud and on-premises appliances. For example, you can deploy your Authentication Manager primary instance on your local network and your replica instances in AWS.

- **Azure virtual appliance**
  - Deployed on the Azure Marketplace with an Azure Image file and an RSA Authentication Manager deployment JSON template that RSA provides.
  - Requires a Virtual Network with a private subnet on Azure.
  - Supports a mixed deployment with cloud and on-premises appliances. For example, you can deploy your Authentication Manager primary instance on your local network and your replica instances in Azure.
• VMware virtual appliance:
  • The VMware virtual appliance is deployed with VMware vCenter Server or the VMware ESXi Server (VMware Hypervisor) on a host machine that you provide. You must use a host machine that meets the hardware requirements.
  • The VMware virtual appliance supports VMware features, such as VMware snapshots.

• Hyper-V virtual appliance:
  • The Hyper-V virtual appliance is deployed with the Hyper-V System Center Virtual Machine Manager (VMM) Console or the Hyper-V Manager on a host machine that you provide. You must use a host machine that meets the hardware requirements.
  • The Hyper-V virtual appliance supports Hyper-V features, such as Hyper-V checkpoints.

• Hardware appliance:
  • Before performing Quick Setup, the RSA-supplied hardware appliance is deployed by directly accessing the hardware, and connecting a keyboard and monitor to the machine to configure the network and keyboard language settings.
  • You can use Clonezilla to create a backup image of the hardware appliance in case you need to restore the original settings for the hardware appliance. For instructions, "Using Clonezilla to Back Up and Restore the RSA Authentication Manager 8.4 Hardware Appliance" on RSA Link at https://community.rsa.com/docs/DOC-97375.
  • If a backup image is not available, you can download and install the original hardware appliance system image from https://my.rsa.com.

All of the appliance platforms provide the following:
  • Pre-installed Authentication Manager software with all of the Authentication Manager features
  • Pre-installed RSA RADIUS server software
  • Appliance configuration through Quick Setup, a software wizard that creates access permission and specifies whether the appliance is a primary instance or a replica instance
  • SUSE Linux Enterprise Server (SLES) 12 Service Pack 3

The following Authentication Manager packages are available at https://my.rsa.com.

<table>
<thead>
<tr>
<th>New Deployments</th>
<th>Required Package on myRSA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The Amazon Web Services virtual appliance and the Azure virtual appliance are not on myRSA. For the AWS virtual appliance, use the AMI file that RSA provides for your Amazon account ID. For the Azure virtual appliance, use the Azure Image file that RSA provides in the Azure Marketplace.</td>
</tr>
<tr>
<td></td>
<td>• For the VMware virtual appliance, download rsa-am-vmware-virtual-appliance-8.4.0.0.0.ova.</td>
</tr>
<tr>
<td></td>
<td>• For the Hyper-V virtual appliance, download rsa-am-hyper-v-virtual-appliance-8.4.0.0.0.zip.</td>
</tr>
<tr>
<td></td>
<td>• For the hardware appliance, the required software is included on the appliance.</td>
</tr>
</tbody>
</table>

| Upgrades         | To upgrade from version 8.3 to version 8.4, download rsa-am-update-8.4.0.0.0.zip. |

| Web Tier installation (for new deployments and upgrades) | Installation files are in the Extras download kit, rsa-am-extras-8.4.0.0.0.zip. |
### Required Package on myRSA

| Additional Software | The Extras download kit, **rsa-am-extras-8.4.0.0.0.zip**, includes additional software, such the RSA Authentication Manager Software Development Kit (SDK). If you need to restore your hardware appliance to a pre-configured state, you can download and apply **rsa-am-hardware-appliance-8.4.0.0.0.iso**. For instructions, see the Help topic “Hardware Appliance System Image Installation” on RSA Link: [https://community.rsa.com/docs/DOC-76910](https://community.rsa.com/docs/DOC-76910). |

## Amazon Web Services Virtual Appliance Requirements

You can deploy an RSA Authentication Manager 8.4 primary or replica instance on Amazon Web Services (AWS). To do so, you must meet the following prerequisites:

- You must have already deployed a Virtual Private Cloud (VPC) on AWS. The VPC is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud.
- You must set up a private subnet. A private subnet has no direct route to the Internet gateway, uses private IP addresses, and is protected by an AWS security group. For more information on VPCs and subnets, see the [Amazon Virtual Private Cloud User Guide](https://docs.aws.amazon.com/vpc/).
- You must have permission to deploy m4.large or better instance types.
- Configure your DNS server. For instructions, see DNS Server Configuration on the Amazon Web Services Virtual Private Cloud below.
- Create security groups for the AWS virtual appliance. For instructions, see Security Groups for Amazon Web Services on page 18.

### DNS Server Configuration on the Amazon Web Services Virtual Private Cloud

For hostname resolution, the Amazon Web Services (AWS) appliance requires you to configure a DNS server in the Virtual Private Cloud (VPC).

You must create a DHCP options set, associate it with the VPC, and then change the VPC properties. In a mixed on-premises and AWS deployment, any on-premises RSA Authentication Manager primary and replica instances need to use the DNS server that is configured in the VPC.

The default DNS server for AWS uses the IP address 169.254.169.253. If you use the default DNS server, any subnet within the VPC can use 169.254.169.253 as the primary DNS server for Authentication Manager.

For more information on DNS servers, see the [Amazon Virtual Private Cloud User Guide](https://docs.aws.amazon.com/vpc/).

**Note:** AWS also includes a default Network Time Protocol (NTP) server with the IP address 169.254.169.123 that you can specify during Quick Setup.
Create a DHCP Options Set

Each VPC requires at least one DHCP options set. You can create multiple sets of DHCP options, but you can only associate one set of DHCP options with your VPC at a time.

Procedure

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, select DHCP Options Sets, and then select Create DHCP options set.
3. In the dialog box, enter values for the options that you want to use. For the Domain name servers value, specify your own DNS server or Amazon’s DNS server (AmazonProvidedDNS). The default DNS server for AWS uses the IP address 169.254.169.253.

   **Note:** This must be the same DNS server that is used to configure RSA Authentication Manager during Quick Setup.

4. Select Yes, Create.

   The new set of DHCP options appears in your list of DHCP options.

5. Record the ID for the new set of DHCP options (dopt-xxxxxxxx). The ID is required to associate the new set of options with your VPC.

Associate DHCP Options with a VPC

You can change the DHCP options associated with the VPC.

Procedure

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, select Your VPCs.
3. Select the VPC, and select Edit DHCP Options Set from the Actions list.
4. In the DHCP Options Set list, select a set of options.
5. Click Save.

   Any existing AWS instances and all new AWS instances that you launch in that VPC will use the options.

   You do not need to restart or relaunch the AWS instances. The instances automatically pick up the changes within a few hours, depending on how frequently the instance renews its DHCP lease. You can explicitly renew the lease in AWS. For instructions, see the AWS documentation.

Change the VPC Properties

You can change the VPC properties. Any on-premise RSA Authentication Manager primary and replica instances need to use the DNS server that is configured in the VPC.

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, select Your VPCs.
3. Select the VPC, and select **Edit DNS Resolution**. Select **Yes**.

4. Select the VPC, and select **Edit DNS Hostnames**. Select **No**.

**After you finish**

You must update the on-premise primary instance and replica instance hostname and IP address to the DNS server that was used in the above configuration. For instructions, see the Help topics "Change the Primary Instance IPv4 Network Settings" and "Change the Replica Instance IPv4 Network Settings.

**Security Groups for Amazon Web Services**

Security group rules control inbound traffic to the RSA Authentication Manager instance and the outbound traffic that leaves the instance. By default, security groups allow all outbound traffic. Each port the user needs to access in the Authentication Manager instance must be configured in the security group rules for inbound traffic.

Refer to the following examples to configure the security groups for the Authentication Manager instance. For instructions on creating security groups for your Virtual Private Cloud (VPC), see the Amazon Virtual Private Cloud User Guide at [https://docs.aws.amazon.com/vpc/](https://docs.aws.amazon.com/vpc/).

**Example of a Security Group for Outbound Rules**

The following example of a security group for outbound rules allows all outbound traffic from the Virtual Private Cloud (VPC).
Example of a Security Group for Inbound Rules

The following example of a security group for inbound rules allows inbound traffic to access the specified ports. All of the ports listed in Ports for the RSA Authentication Manager Instance on page 114 are enabled, including port 22 (TCP) for SSH, port 49 (TCP) that should remain closed unless TACACS is configured, and the legacy RADIUS Client ports 1645 (UDP) and 1646 (UDP).

You should add any feature-specific ports to your security groups. For example, if you need to support an LDAP connection to an Oracle Directory Server instance, you must add the port 1389 (which is required for an ODS instance) in the security group for Authentication Manager. If you need to enable the connection to the Authentication API, then port number 5555 must be added to the security groups.

If you are using the ping command, you must enable the ICMP port in your security groups. For security.
reasons, RSA does not recommend opening the ICMP port on the cloud, but if you require ping to work, the ICMP port must be added to your security groups.

**Azure Virtual Appliance Requirements**

You can deploy an RSA Authentication Manager 8.4 primary or replica instance on Azure. To do so, you must meet the following prerequisites:

- An Azure Virtual Network (VNet) is required. Do the following:
  - (Existing virtual network) Note the Resource Group of the virtual network.
  - (New virtual network) Do the following:
    1. Deploy an Azure virtual network. The virtual network dedicated to your Azure account is logically isolated from other virtual networks in the Azure cloud.
    2. Set up a private subnet that you can use to deploy the virtual appliance. A private subnet uses private IP addresses and is protected by an Azure Security Group.
    3. Note the Resource Group of the virtual network.


- Have permission to deploy Standard_D8s_v3 or Standard_D4s_v3 instance types.
- Collect the required network information:
  - The hostname or IP address of at least one Network Time Protocol (NTP) server. Authentication Manager requires accurate time for authentication and replication. Authentication Manager uses a static IPv4 address. DHCP is not supported. The IPv6 protocol is not supported for the Authentication Manager virtual appliance on Azure, because Azure requires DHCP to support the IPv6 protocol.
  - The network information for each appliance: the fully qualified domain name (FQDN), static IP address, subnet mask, default gateway, and DNS server IP addresses.

  **Note:** Azure virtual machines support only one NIC and one IP address for each NIC. Features that require more than one NIC are not available on the Azure virtual machine.

- Configure your DNS server. For instructions, see DNS Server Configuration on the Azure Virtual Network below.
- Create an Azure security group. For instructions, see Create an Azure Network Security Group below.

**DNS Server Configuration on the Azure Virtual Network**

For hostname resolution, the Azure appliance requires you to configure a DNS server in the virtual network or use the DNS server provided by Azure. Any on-premises Authentication Manager primary instance or replica instances must use the DNS server that is configured in the virtual network. For information on Azure DNS, see [https://docs.microsoft.com/en-us/azure/dns/](https://docs.microsoft.com/en-us/azure/dns/).

**Create an Azure Network Security Group**

Azure network security group rules control the inbound traffic to the Authentication Manager instance and the outbound traffic from the instance. By default, security groups allow all outbound traffic. Each port the user needs to access in the Authentication Manager instance must be configured in the security group rules for inbound traffic.
Procedure

1. Log on to the Azure portal.
2. On the Services tab, select **Network security groups**.
3. Select Add.
4. Select the resource group of your Azure virtual network.
5. Create a security group that allows inbound traffic to the following ports, except where noted:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>Secure Shell (SSH)</td>
</tr>
<tr>
<td>49</td>
<td>TCP</td>
<td>TACACS authentication. Required for the TACACS client.</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>Quick Setup, Operations Console, Security Console</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>SNMP</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Quick Setup, Operations Console, Security Console, Self-Service Console</td>
</tr>
</tbody>
</table>

If RADIUS clients only communicate to the RADIUS servers on ports 1812 and 1813, you can block the legacy RADIUS UDP ports 1645 and 1646.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1645</td>
<td>UDP</td>
<td>RADIUS authentication (legacy port)</td>
</tr>
<tr>
<td>1646</td>
<td>UDP</td>
<td>RADIUS accounting (legacy port)</td>
</tr>
</tbody>
</table>

If you do not use RSA RADIUS, but you have replica instances, you must allow connections between Authentication Manager instances on the TCP ports 1812 and 1813. These ports are required for tasks such as replica attachment, replica promotion, and IP address and hostname changes. You should restrict connections from other systems that are not Authentication Manager instances.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1812</td>
<td>TCP</td>
<td>RADIUS replication port</td>
</tr>
<tr>
<td>1813</td>
<td>TCP</td>
<td>RADIUS administration</td>
</tr>
</tbody>
</table>

If you do not plan to use RSA RADIUS, you can close the UDP ports 1812 and 1813.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1812</td>
<td>UDP</td>
<td>RADIUS authentication</td>
</tr>
<tr>
<td>1813</td>
<td>UDP</td>
<td>RADIUS accounting</td>
</tr>
<tr>
<td>5500</td>
<td>TCP</td>
<td>Agent authentication</td>
</tr>
<tr>
<td>5500</td>
<td>UDP</td>
<td>Agent authentication</td>
</tr>
<tr>
<td>5550</td>
<td>TCP</td>
<td>Agent auto-registration</td>
</tr>
<tr>
<td>5580</td>
<td>TCP</td>
<td>Offline authentication service</td>
</tr>
<tr>
<td>7002</td>
<td>TCP, SSL-encrypted</td>
<td>Authentication Manager and the RSA Token Management snap-in for the Microsoft Management Console (MMC)</td>
</tr>
<tr>
<td>7004</td>
<td>TCP, SSL-encrypted</td>
<td>Security Console, Self-Service Console and risk-based authentication (RBA), and Cryptographic Token-Key Initialization Protocol (CT-KIP)</td>
</tr>
<tr>
<td>7022</td>
<td>TCP, SSL-encrypted</td>
<td>Authentication Manager, trusted realm network access point, or the web tier</td>
</tr>
<tr>
<td>7072</td>
<td>TCP, SSL-encrypted</td>
<td>Operations Console</td>
</tr>
<tr>
<td>7082</td>
<td>TCP, SSL-encrypted</td>
<td>RADIUS Configuration SSL</td>
</tr>
<tr>
<td>8443</td>
<td>TCP, SSL-encrypted</td>
<td>Authentication Manager patches and service packs</td>
</tr>
</tbody>
</table>

For more information about these ports, see **Port Usage on page 113**.
Add any feature-specific ports to your security group. For example, an LDAP connection to an Oracle Directory Server instance might require you to add port 1389 in the security group. If you need to enable the connection to the Authentication API, then port number 5555 must be added to the security groups.

If you are using the ping command, you must enable the ICMP port in your security groups. RSA does not recommend opening the ICMP port on the cloud, but this port is required for ping to work.

For instructions on how to create security groups, see https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group.

**Azure Feature Support**

RSA Authentication Manager supports Azure features, such as Azure snapshots, Azure Backup, and the Azure Redeploy feature.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure snapshots</td>
<td>You can create an Azure snapshot for an Authentication Manager primary or replica instance, but snapshots do not replace the Operations Console backup feature. In a complex Authentication Manager deployment, restoring a virtual machine to a snapshot requires you to perform additional tasks. For more information, see the <a href="https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group">RSA Authentication Manager Administrator’s Guide</a>.</td>
</tr>
<tr>
<td>Azure Backups</td>
<td>You can use Azure Backup to back up and restore the RSA Authentication Manager primary or replica instance data in the Microsoft cloud. Azure Backup does not replace the Operations Console backup in Authentication Manager. In a complex Authentication Manager deployment, restoring a virtual machine to an Azure Backup requires you to perform additional tasks. For more information, see the <a href="https://docs.microsoft.com/en-us/azure/virtual-network/manage-network-security-group">RSA Authentication Manager Administrator’s Guide</a>.</td>
</tr>
<tr>
<td>Redeploy</td>
<td>A virtual machine can encounter issues caused by user configuration or the host infrastructure. The Azure Redeploy feature migrates your Azure virtual machine to a new host. The original virtual machine, including the local disk, is deleted, and the configurations and associated resources are transferred to a new virtual machine of the same size on a new host. On doing so, the virtual machine is restarted and the data on the temporary drive is lost. While the redeployment is in progress, the virtual machine is unavailable. To redeploy, click Redeploy from the virtual machine that you intend to redeploy. For more information, see the Azure documentation.</td>
</tr>
</tbody>
</table>

**VMware Virtual Appliance Requirements**

If you deploy RSA Authentication Manager 8.4 on a VMware virtual appliance, you can deploy a virtual appliance through VMware vCenter Server or directly on the VMware ESXi platform (also known as VMware vSphere Hypervisor 6.0 or later). VMware vCenter Server is not required to deploy the virtual appliance.

You must deploy a VMware virtual appliance with the RSA Authentication Manager Open Virtualization Appliance (OVA) file that is located in the RSA Authentication Manager 8.4 download kit.
VMware Software Requirements

<table>
<thead>
<tr>
<th>Required Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Platforms</td>
<td>Deploy the virtual appliance on one of the following platforms: Adam Refrigerator ESXi 6.0 (VMware vSphere Hypervisor 6.0) Adam Refrigerator ESXi 6.5 (VMware vSphere Hypervisor 6.5) Adam Refrigerator ESXi 6.7 (VMware vSphere Hypervisor 6.7)</td>
</tr>
<tr>
<td>VMware vSphere Client</td>
<td>If you are using ESXi or vCenter Server 6.0, you must have any version of the VMware vSphere Client able to connect to and manage supported ESXi (Hypervisor) and vCenter Server deployments. ESXi or vCenter Server 6.5 or 6.7 does not require a separate installed vSphere Client. For VMware ESXi 6.5, Patch Release ESXi65O-201801001 (52236) or later is required to deploy the virtual appliance directly on the VMware ESXi Server 6.5. You can check your ESXi Embedded Host Client version by logging on to the ESXi host with SSH, and running the following command: &quot;esxcli software vib get -n esx-ui&quot; To download the required software, go to <a href="https://my.vmware.com">https://my.vmware.com</a>.</td>
</tr>
</tbody>
</table>

For the VMware host hardware requirements, see your VMware documentation.

VMware Software Support

<table>
<thead>
<tr>
<th>Supported Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) VMware vCenter Server</td>
<td>VMware vCenter Server provides centralized management for multiple virtual machines and includes administrative features, such as vMotion. The virtual appliance supports the versions of VMware vCenter Server that are compatible with the supported ESXi versions: VMware vCenter Server 6.0 VMware vCenter Server 6.5 VMware vCenter Server 6.7</td>
</tr>
</tbody>
</table>

VMware Primary or Replica Instance Hardware Requirements

The virtual appliance for each RSA Authentication Manager instance requires hardware that meets or exceeds the minimum requirements. Each instance is deployed with the default values.

<table>
<thead>
<tr>
<th>Description</th>
<th>Minimum Requirement</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Space</td>
<td>100 GB</td>
<td>100 GB</td>
</tr>
<tr>
<td></td>
<td>4 GB swap file</td>
<td>4 GB swap file</td>
</tr>
<tr>
<td>Memory Requirements</td>
<td>4 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>CPU Requirements</td>
<td>One virtual CPU</td>
<td>Two virtual CPUs</td>
</tr>
</tbody>
</table>

The virtual appliance may require additional disk space for virtual machine operations, such as snapshots and memory management. Use the following formula to calculate the total amount of storage required:

Total disk space = 104 GB + (GB of memory allocated to the virtual appliance x 2) + (Number of snapshots x GB of memory allocated to the virtual appliance)
For example, a virtual appliance with 8 GB of memory and three snapshots requires about 150 GB of storage. The calculation 104 GB + (2 x 8 GB of memory) + (3 snapshots x 8 GB of memory) indicates that 144 GB is required, or 150 GB if you include a 6 GB buffer.

Automatic tuning on the virtual appliance supports 4 GB, 8 GB, 16 GB, or 32 GB of memory. For example, the appliance uses 32 GB of memory if more than 32 GB is available.

The virtual appliance only supports the E1000 virtual network adapter. Do not change the default network adapter.

For the VMware host hardware requirements, consult your VMware documentation.

For information on ports used by Authentication Manager, see Port Usage on page 113.

**VMware Feature Support**

RSA Authentication Manager supports VMware features, such as vMotion, Storage vMotion, High Availability, Fault Tolerance, Distributed Resource Scheduler (DRS), and Snapshots. Restrictions are described in the following table.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Fault Tolerance</td>
<td>VMware Fault Tolerance has the following requirements:</td>
</tr>
<tr>
<td></td>
<td>* By default, vSphere Fault Tolerance can accommodate Symmetric</td>
</tr>
<tr>
<td></td>
<td>Multiprocessing (SMP) virtual machines with up to four virtual CPUs.</td>
</tr>
<tr>
<td></td>
<td>* By default, each Authentication Manager instance is deployed with</td>
</tr>
<tr>
<td></td>
<td>two virtual CPUs.</td>
</tr>
<tr>
<td></td>
<td>* You can change the number of virtual CPUs. For instructions, see the</td>
</tr>
<tr>
<td></td>
<td>VMware documentation.</td>
</tr>
<tr>
<td></td>
<td>* VMware Legacy Fault Tolerance does not support IPv6. If you use</td>
</tr>
<tr>
<td></td>
<td>Legacy Fault Tolerance, do not create an IPv6 network address on an</td>
</tr>
<tr>
<td></td>
<td>Authentication Manager primary or replica instance.</td>
</tr>
<tr>
<td>VMware snapshots</td>
<td>You can take a VMware snapshot of an Authentication Manager primary or</td>
</tr>
<tr>
<td></td>
<td>replica instance, but snapshots do not replace the Operations</td>
</tr>
<tr>
<td></td>
<td>Console backup feature.</td>
</tr>
<tr>
<td></td>
<td>When you take a snapshot of an Authentication Manager instance, specific settings are required. In a complex Authentication Manager deployment, restoring snapshots requires you to perform additional tasks.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the RSA Authentication Manager Administrator's Guide.</td>
</tr>
<tr>
<td>VMware Distributed Resource Scheduler (DRS)</td>
<td>For security and redundancy, you can install primary and replica instances on separate hosts.</td>
</tr>
<tr>
<td></td>
<td>VMware DRS can move both instances onto the same host. Configure DRS to</td>
</tr>
<tr>
<td></td>
<td>keep instances on separate physical hosts.</td>
</tr>
</tbody>
</table>

**Hyper-V Virtual Appliance Requirements**

If you deploy RSA Authentication Manager on a Hyper-V virtual appliance, use the Microsoft Hyper-V System
Center Virtual Machine Manager (VMM) Console or the Hyper-V Manager.

Deploy a Hyper-V virtual appliance with the RSA Authentication Manager Hyper-V virtual appliance zip file that is available at https://my.rsa.com.

**Hyper-V Software Requirements**

<table>
<thead>
<tr>
<th>Required Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Servers</td>
<td>- Microsoft Windows 2016 host machine</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 2012 R2 host machine</td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 2012 host machine</td>
</tr>
<tr>
<td>Hyper-V Management Tools</td>
<td>Deploy the Hyper-V virtual appliance with one of the following tools:</td>
</tr>
<tr>
<td></td>
<td>- Hyper-V System Center 2016, 2012 R2, or 2012 Virtual Machine Manager</td>
</tr>
<tr>
<td></td>
<td>(VMM).</td>
</tr>
<tr>
<td></td>
<td>- Hyper-V Manager 2016, 2012 R2, or 2012.</td>
</tr>
<tr>
<td>PowerShell</td>
<td>If you are using Hyper-V System Center 2016, 2012 R2, or 2012 VMM, you can use the Windows PowerShell version that is included with the VMM Console installation.</td>
</tr>
<tr>
<td></td>
<td>If you are using Hyper-V Manager 2016, 2012 R2, or 2012, you can use the Windows PowerShell version that is included with your version of Windows.</td>
</tr>
<tr>
<td>Hyper-V Virtual Machine Manager (VMM) Modules</td>
<td>If you are using VMM, then install the VMM Console to obtain the required Virtual Machine Manager Windows PowerShell module.</td>
</tr>
<tr>
<td></td>
<td>To verify that the required Hyper-V and VirtualMachineManager PowerShell modules are available, run these two PowerShell commands:</td>
</tr>
<tr>
<td></td>
<td>Get-Command -Module Hyper-V</td>
</tr>
<tr>
<td></td>
<td>Get-Command -Module VirtualMachineManager</td>
</tr>
<tr>
<td></td>
<td>The output displays a list of commands related to each module.</td>
</tr>
<tr>
<td></td>
<td>For more information, see your Hyper-V documentation.</td>
</tr>
<tr>
<td>Hyper-V Manager Software</td>
<td>If you are using Hyper-V Manager, then install both the Hyper-V role and the management tools. For example, if you use Server Manager to install the Hyper-V role, the management tools are included by default.</td>
</tr>
<tr>
<td></td>
<td>For instructions, see your Hyper-V documentation.</td>
</tr>
</tbody>
</table>

For the Hyper-V host hardware requirements, see your Hyper-V documentation.

**Hyper-V Primary or Replica Instance Hardware Requirements**

The virtual appliance for each RSA Authentication Manager instance requires hardware that meets or exceeds the minimum requirements.

<table>
<thead>
<tr>
<th>Description</th>
<th>Minimum Requirement</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Space</td>
<td>100 GB storage</td>
<td>100 GB storage</td>
</tr>
<tr>
<td></td>
<td>4 GB swap file</td>
<td>4 GB swap file</td>
</tr>
<tr>
<td>Memory Requirements</td>
<td>4 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>CPU Requirements</td>
<td>One virtual CPU</td>
<td>Two virtual CPUs</td>
</tr>
</tbody>
</table>

The virtual appliance may require additional disk space for virtual machine operations, such as checkpoints and
memory management. For example, you may need 150 GB in total storage, or you may need 200 GB in total storage if you are using 16 GB of memory.

Automatic tuning on the virtual appliance supports 4 GB, 8 GB, 16 GB, or 32 GB of memory. For example, the appliance uses 32 GB of memory if more than 32 GB is available.

The Hyper-V virtual appliance provides a virtual network adapter that uses the hv_netvsc driver. Do not use the legacy network adapter. The legacy network adapter is not supported.

For the Hyper-V host hardware requirements, consult your Hyper-V documentation.

For information on ports used by Authentication Manager, see Port Usage on page 113.

**Hyper-V Feature Support**

RSA Authentication Manager supports Hyper-V features, such as live migration, high availability through failover clustering, NIC teaming for virtual machines, and checkpoints. Restrictions are described in the following table.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic memory</td>
<td>Dynamic memory is not supported for the Hyper-V virtual appliance. Static memory is supported. For more information on memory requirements, see Hyper-V Primary or Replica Instance Hardware Requirements on the previous page.</td>
</tr>
<tr>
<td>Hyper-V checkpoints</td>
<td>You can create a Hyper-V checkpoint for an Authentication Manager primary or replica instance, but checkpoints do not replace the Operations Console backup feature.</td>
</tr>
<tr>
<td></td>
<td>In a complex Authentication Manager deployment, restoring a virtual machine to a checkpoint requires you to perform additional tasks. For information, see the RSA Authentication Manager Administrator's Guide.</td>
</tr>
<tr>
<td>Hyper-V high availability</td>
<td>For security and redundancy, you can install primary and replica instances on separate hosts. Hyper-V live migration can move both instances onto the same host. Configure high availability to use availability sets to keep instances on separate physical hosts.</td>
</tr>
</tbody>
</table>

**Supported Data Stores**

You can store data in:

- The RSA Authentication Manager internal database
- One or more external directory servers that use LDAP (called an identity source within Authentication Manager).

**Internal Database**

RSA Authentication Manager is installed with an internal database. The following information is stored only in the internal database:

- Data that is specific to Authentication Manager, such as token data or policies for administrative roles and passwords.
- Data that links Authentication Manager with LDAP directory user and user group records.
Users, user groups, and identity attribute data can be stored in an external LDAP directory or in the internal database.

**Supported Directory Servers**

RSA Authentication Manager supports the following external LDAP directory servers for user, user group, and identity attribute data:

- Microsoft Active Directory 2008 R2
- Microsoft Active Directory 2012
- Microsoft Active Directory 2012 R2
- Microsoft Active Directory Lightweight Directory Services 2012 R2
- Microsoft Active Directory 2016
- Microsoft Active Directory 2019
- Sun Java System Directory Server 7.0
- Oracle Directory Server Enterprise Edition 11g
- OpenLDAP 2.4.40

**Note:** The certificate used by the LDAPS protocol must be at least 2048 bits. For example, you must replace the default Oracle Directory Server certificate, which is 1024 bits.

In Active Directory, you can add a Global Catalog as an identity source, which is used to look up users and resolve group membership during authentications. You cannot use a Global Catalog identity source to perform administrative tasks.

**Note:** Authentication Manager supports Active Directory Lightweight Directory Services (LDS) servers if the same server does not also have an Active Directory Domain Controller role. If a server has an Active Directory Domain Controller role, select that identity source type when connecting the identity source to Authentication Manager.

Authentication Manager has read-only access to all external directory servers. However, you can configure the system to allow users to change their passwords in LDAP during authentication.

Authentication Manager LDAP integration does not modify your existing LDAP schema, but rather creates a map to your data that Authentication Manager uses.

Authentication Manager supports Secure Socket Layer (SSL) for LDAP connections. SSL is required if you are allowing users to change their passwords from Authentication Manager. Non-SSL connections can expose sensitive data as it passes over the connection. For example, if bind LDAP operations to authenticate are performed over a non-SSL connection, the password is sent in the clear. The use of LDAP over SSL requires that the appropriate certificate is accessible by Authentication Manager.

For more information, see the chapter “Integrating LDAP Directories” in the *RSA Authentication Manager Administrator’s Guide*.

**Supported Web Browsers**

RSA Authentication Manager 8.4 uses a web-based interface for administration. RSA tested the following web browsers for RSA Authentication Manager 8.4:
- Microsoft Internet Explorer 11
- Google Chrome 68
- Mozilla Firefox 61
- Safari 11

The web browser must allow Javascript and cookies. See your web browser documentation for instructions.

**Note:** To correctly display the web-based interface, you must have a screen resolution of 1024 X 768 or higher.

### Supported RSA Authentication Agents

Authentication agents are software applications that securely pass user authentication requests to and receives responses from RSA Authentication Manager. Authentication agents are installed on each machine, such as a domain server, web server, or a personal computer, that you protect with Authentication Manager. Any resource that is used with SecurID authentication, on-demand authentication (ODA) or risk-based authentication (RBA) requires an authentication agent.

The agent that you need depends on the type of resource you want to protect. For example, to protect an Apache web server, you need to download the RSA Authentication Agent for Apache. You may purchase products that contain embedded RSA Authentication Agent software. For example, these products include all the major brands of remote access servers and firewalls.


For a list of third-party products that have embedded RSA agents, go to the The RSA Ready Partner Program website at [www.rsaready.com](http://www.rsaready.com).

For more information, see the Help topic "RSA Authentication Agents."

### RSA Authentication Manager License Support


Authentication Manager has the following requirements:

- For RSA Authentication Manager 8.0 or later, you cannot use a version 6.1 or version 7.1 license.
- If version 8.2 Patch 3 is applied or if you have version 8.2 Service Pack 1 (SP1) or later, any version 8.0 or later license can be used.
- If you have version 8.2 Patch 2 or earlier, you cannot use a later license. Instead, you must apply a version 8.2 license, a version 8.1 license, a version 8.0 license, or any combination of these licenses.

Authentication Manager supports stackable licenses that allow you to add users and authenticators to your existing license. In Authentication Manager, authenticators include hardware tokens, software tokens, and the RSA SecurID Authenticate app. When Authentication Manager users successfully authenticate with the Authenticate Tokencode or Approve authentication, their user records are assigned the Authenticate app as a token. The Authenticate app does not affect the license count for users who already have an assigned
authenticator in Authentication Manager. The Authenticate app increases the license count by one for users who do not have an assigned authenticator in Authentication Manager.


Each edition includes the following Authentication Manager features:

- A specific number of tokens (authenticators).
- Self-Service
- Authenticator workflow provisioning
- RADIUS
- Offline authentication

An edition can include the following optional Authentication Manager features:

- On-demand authentication (ODA)
- Risk-based authentication (RBA)
- Business continuity

The Premium Edition includes risk-based identity confidence. This feature allows the Cloud Authentication Service to establish high or low confidence in a user's identity based on data it collects when users attempt to authenticate over a period of time.

It is important to know:

- You can install multiple licenses.
- The Account ID must be the same for all licenses.
- The License ID (or Stack ID), must be unique for each license. You cannot install the same license twice.
- Users only count against the license limit if they have one or more assigned authenticators. Users without authenticators do not count against the limit.
- The Security Console displays warning messages when you exceed 85, 95, and 100 percent of the user limit.
- The system updates the user counts every hour and each time that a administrator views the license status in the Security Console.

RSA provides the license files separately from your RSA Authentication Manager download kit. Make sure that you know the location of the license file before running the primary appliance Quick Setup. The license file must be accessible to the browser that is used to run the primary appliance Quick Setup. Do not unzip the license file.

### Accurate System Date and Time Settings

RSA Authentication Manager requires accurate date and time settings for replication and authentication. If the token clock and the Authentication Manager system clock do not match, the generated tokencode will not match, and authentication attempts can fail. Specifying a Network Time Protocol (NTP) server for the instance prevents replication and authentication issues that are caused by clock drift.

**Note:** An NTP server is required in a replicated deployment. RSA requires that all Authentication Manager instances have their time synchronized to an NTP server.
If you do not specify an NTP server in Authentication Manager, the virtual appliance uses the date and time provided by the physical machine hosting the virtual appliance. In this situation, the physical machine hosting the virtual appliance should be configured to obtain accurate date and time information from an NTP server.

Make sure that you have the hostname or IP address of an NTP server before running Quick Setup.

**Secure Appliance Deployment**

After you deploy RSA Authentication Manager on a hardware appliance or a virtual appliance, the operating system console screen displays a Quick Setup Access Code along with a Quick Setup URL. The Quick Setup Access Code is only available until Quick Setup is complete.

The Quick Setup Access Code is required to begin Quick Setup, which configures the appliance as an RSA Authentication Manager instance. This code makes it harder for a malicious user to access Quick Setup and take control of the appliance.

| Note: | You must have the Quick Setup Access Code to begin Quick Setup. |

RSA recommends the following guidelines when deploying an appliance:

- Deploy a hardware appliance in a test environment or in an isolated network. Only connect the appliance to your organization’s network after Quick Setup is complete. Restrict physical and network access to the appliance to authorized individuals.
  
  For example, you can deploy a hardware appliance and run Quick Setup in a protected test environment that duplicates your production environment. After Quick Setup is complete, you can move the appliance into the production environment without changing the network settings, such as the hostname and the IP Address.
  
  Alternately, you can deploy the hardware appliance and run Quick Setup in a protected test environment and later change the network settings, such as the hostname and IP address, to attach the appliance to your production environment. For more information, see the Help topic “Primary or Replica Instance Network Settings Updates.”

- Deploy a VMware or Hyper-V virtual appliance on an isolated network until Quick Setup is complete. Use VMware or Hyper-V to maintain full control over the appliance. Restrict network access to the appliance, and only allow authorized individuals to access the virtual appliance.

- Deploy the Amazon Machine Image (AMI) in a private subnet in your virtual private cloud (VPC). A private subnet has no route to the Internet gateway. The VPC is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud.

- Deploy the Azure appliance in a private subnet in the your Azure Virtual Network (VNet). A private subnet uses private IP addresses and is protected by an Azure Security Group. The virtual network dedicated to your Azure account is logically isolated from other virtual networks in the Azure cloud.

- If you access an appliance to run Quick Setup, and you discover that the appliance has already been configured or you receive error messages because Quick Setup is in progress, then do the following:
  
  a. Contact other administrators in your organization to ensure that a malicious user is not trying to take control of the appliance.

  b. If you believe that the appliance has been compromised, remove the primary or replica instance from your deployment. For instructions, see the RSA Authentication Manager Administrator’s Guide.
c. Do one of the following:
   - For a hardware appliance, shut down the appliance and remove the machine from service.
   - For a virtual appliance, suspend the appliance, and quarantine the machine for further investigation.

d. Contact your IT department or RSA immediately.

Deployment Checklist for the Primary and Replica Instance

Before you set up the RSA Authentication Manager primary instance or the replica instance, you must collect the following information. You enter this information during the appliance deployment and Quick Setup.

Amazon Machine Image Deployment

If you are deploying RSA Authentication Manager Amazon Machine Image (AMI), you must collect the following items and information:

- **Client computer.** You will use this computer to deploy the appliance through Amazon Web Services (AWS). Use this computer to run Quick Setup through a supported web browser. For a list of supported web browsers, see Supported Web Browsers on page 27.

- **RSA Authentication Manager AMI file.** You must deploy an AWS virtual appliance with the Authentication Manager AMI file that RSA provides for your AWS account ID. To request access to the AMI, contact RSA Customer Support.

- **IPv4 Network settings.** You must provide the appliance network settings in this order: default gateway, hostname (Fully Qualified Domain Name), IP address, Netmask, primary DNS server (optional), and secondary DNS server (optional). You can record the appliance network settings in a text file, and paste it into AWS when you are create the virtual appliance.

Azure Image File Deployment

If you are deploying the RSA Authentication Manager Azure Image file, you must collect the following items and information:

- **Client computer.** You will use this computer to deploy the appliance through Azure. Use this computer to run Quick Setup through a supported web browser. For a list of supported web browsers, see Supported Web Browsers on page 27.

- **RSA Authentication Manager Azure Image file.** You must deploy an Azure virtual appliance with the Authentication Manager Azure Image file that RSA provides in the Azure Marketplace. The Azure image file contains the required VHD files and the Azure deployment JSON template.

- **IPv4 Network settings.** You must provide the network information for each appliance: the fully qualified domain name (FQDN), static IP address, subnet mask, default gateway, and DNS server IP addresses.

VMware Virtual Appliance Deployment

If you are deploying RSA Authentication Manager on a virtual appliance, you must collect the following items and information:

- **VMware vSphere Client computer.** You will use this computer to deploy the appliance through the VMware vSphere Client. Use this computer to run Quick Setup through a supported web browser. For a list
of supported web browsers, see Supported Web Browsers on page 27.

- **RSA Authentication Manager Open Virtualization Appliance (OVA) file.** The RSA Authentication Manager OVA file is used to create your virtual appliance. Copy the OVA file to a location accessible to VMware.

- **IPv4 Network settings.** Identify the fully qualified domain name and static IP address for the appliance, the subnet mask and default gateway, and the IP address or hostname of the DNS servers in the network. You must provide this network information when deploying the appliance. The IP address that you specify for the appliance is used to access Quick Setup.

**Hyper-V Virtual Appliance Deployment**

If you are deploying RSA Authentication Manager on a virtual appliance, you must collect the following items and information:

- **Microsoft Windows client computer with access to a Microsoft Windows 2012, 2012 R2, or 2016 Hyper-V host machine.** Use Remote Desktop Protocol or direct access to log on to the Microsoft Windows 2012, 2012 R2, or 2016 Hyper-V host machine. You can deploy the appliance through either the Hyper-V Virtual Machine Manager (VMM) Console or the Hyper-V Manager. You will also use the Microsoft Windows client computer to run Quick Setup through a supported web browser. For a list of supported web browsers, see Supported Web Browsers on page 27.

- **RSA Authentication Manager virtual appliance zip file.** The RSA Authentication Manager Hyper-V virtual appliance zip file is used to deploy your virtual appliance. Copy the file to a location accessible to Hyper-V. For VMM deployment, copy the file to an existing Hyper-V VMM library server or a shared folder on a Microsoft Windows 2012, 2012 R2, or 2016 machine that can be added as a library server. For Hyper-V Manager deployment, copy the file to a location on the Microsoft Windows 2012, 2012 R2, or 2016 Hyper-V host machine.

- **IPv4 Network settings.** Identify the fully qualified domain name and static IP address for the appliance, the subnet mask and default gateway, and the IP address or hostname of the DNS servers in the network. You must provide this network information when deploying the appliance. The IP address that you specify for the appliance is used to access Quick Setup.

**Hardware Appliance Deployment**

If you are deploying RSA Authentication Manager on a hardware appliance, you must collect the following items and information:

- **Keyboard and Monitor.** To deploy the hardware appliance and complete the initial configuration tasks that are required for the deployment process, you must attach a keyboard and monitor to the appliance.

- **IPv4 Network settings.** Identify the fully qualified domain name and static IP address for the appliance, the subnet mask and default gateway, and the IP address or hostname of the DNS servers in the network. You must provide this network information when deploying the appliance. The IP address that you specify for the appliance is used to access Quick Setup.

**Quick Setup Checklist for the Primary Instance**

You must enter the following information during the Quick Setup process for a primary instance.

- **Appliance license file.** During Quick Setup, you must have access to the .zip license file. You download the license file (.zip) at https://my.rsa.com.

  Use the credentials that were e-mailed to you to log on to the site and download the license file. If you require assistance, you can contact the License Seed Response Team on one of the following websites:
https://community.rsa.com
https://rsa.secure.force.com/gbocase/

Make sure that you know the location of the license file before running the primary appliance Quick Setup. The license file must be in a location that is accessible to the browser that is used to run the primary appliance Quick Setup. Do not unzip the file. RSA recommends that you store the license file in a protected location available only to authorized administrative personnel.

**Hostname or IP address of an NTP server.** RSA recommends that you specify a local or Internet Network Time Protocol (NTP) server, for example, nist.time.gov. During Quick Setup, you can enter the hostname or IP address of at least one NTP servers.

**Note:** An NTP server is required in a replicated deployment. RSA requires that all Authentication Manager instances have their time synchronized to an NTP server.

**Operating system password.** Choose a password to access the appliance operating system for troubleshooting and advanced administration. The password must be between 8 and 32 characters long, and contain at least 1 alphabetic character and at least 1 special character excluding ^, @, and ~. For example, gyz!8kMh is a valid password. For more information, see System Administrator Accounts on page 122.

**User ID and password for initial administrator accounts.** Choose a User ID and password to create the following:
- Initial Security Console administrator User ID and password for the Super Admin role
- Operations Console administrator User ID and password

For more information on managing administrator accounts and passwords, see System Administrator Accounts on page 122.

**Quick Setup Checklist for the Replica Instance**

You must enter the following information during the Quick Setup process for a replica instance.

**Replica package file location.** To set up a replica appliance, you must have access to the replica package file. If necessary, copy the replica package file onto the computer that you will use to run Quick Setup.

For more information on creating a replica package, see Generate and Download a Replica Package File on page 62.

**Hostname or IP address of an NTP server.** You must synchronize the time on the primary and replica appliances using a local or Internet Network Time Protocol (NTP) server. During Quick Setup, you can enter hostname or IP address of at least one NTP server.

**Operating system password.** Choose a password to access the appliance operating system for troubleshooting and advanced administration. The password must be between 8 and 32 characters long, and contain at least 1 alphabetic character and at least 1 special character excluding ^, @, and ~. For example, gyz!8kMh is a valid password. Choose a unique password for each appliance. For more information, see System Administrator Accounts on page 122.

**Setup and Configuration Information List**

Use the following list to specify setup and configuration information for RSA Authentication Manager. RSA
RSA recommends that you complete this list and distribute it to the appropriate personnel for your deployment. Save a copy of the completed list in a secure location for future reference.

**Note:** Some of the information that you enter in this list may be sensitive. Review your company’s policies before entering sensitive information, such as a password, in this list.

### Appliance Deployment

**Note:** If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete.

#### Amazon Web Services Virtual Appliance

<table>
<thead>
<tr>
<th>Element</th>
<th>Your Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact RSA Customer Support to request access to the RSA Authentication Manager Amazon Machine Image (AMI) file for your Amazon account ID.</td>
<td></td>
</tr>
<tr>
<td>Default Gateway</td>
<td></td>
</tr>
<tr>
<td>Hostname (Fully Qualified Domain Name)</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Netmask</td>
<td></td>
</tr>
<tr>
<td>Primary DNS Server (Optional)</td>
<td></td>
</tr>
<tr>
<td>Secondary DNS Server (Optional)</td>
<td></td>
</tr>
</tbody>
</table>

#### Azure Virtual Appliance

<table>
<thead>
<tr>
<th>Element</th>
<th>Your Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully Qualified Domain Name (FQDN)</td>
<td></td>
</tr>
<tr>
<td>Static IP Address</td>
<td></td>
</tr>
<tr>
<td>Subnet mask</td>
<td></td>
</tr>
<tr>
<td>Default gateway</td>
<td></td>
</tr>
<tr>
<td>Primary DNS Server</td>
<td></td>
</tr>
<tr>
<td>Secondary DNS Server (Optional)</td>
<td></td>
</tr>
</tbody>
</table>

#### VMware or Hyper-V Virtual Appliance

<table>
<thead>
<tr>
<th>Element</th>
<th>Your Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware OVA package location or Hyper-V virtual appliance zip file location</td>
<td></td>
</tr>
<tr>
<td>Fully qualified domain name</td>
<td></td>
</tr>
<tr>
<td>IPv4 Static IP address</td>
<td></td>
</tr>
<tr>
<td>IPv4 Subnet mask</td>
<td></td>
</tr>
<tr>
<td>IPv4 Default Gateway</td>
<td></td>
</tr>
<tr>
<td>IP address of the DNS servers</td>
<td></td>
</tr>
</tbody>
</table>
### Hardware Appliance

<table>
<thead>
<tr>
<th>Element</th>
<th>Your Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully qualified domain name</td>
<td></td>
</tr>
<tr>
<td>IPv4 Static IP address</td>
<td></td>
</tr>
<tr>
<td>IPv4 Subnet mask</td>
<td></td>
</tr>
<tr>
<td>IPv4 Default Gateway</td>
<td></td>
</tr>
<tr>
<td>IP address of the DNS servers</td>
<td></td>
</tr>
</tbody>
</table>

### Primary Appliance Setup

<table>
<thead>
<tr>
<th>Description</th>
<th>Your Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA Authentication Manager license file (.zip) location</td>
<td></td>
</tr>
<tr>
<td>Hostname or IP address of an NTP server</td>
<td></td>
</tr>
<tr>
<td>Operating System password</td>
<td></td>
</tr>
<tr>
<td>Super Admin user name</td>
<td></td>
</tr>
<tr>
<td>Super Admin password</td>
<td></td>
</tr>
<tr>
<td>Operations Console Administrator user name</td>
<td></td>
</tr>
<tr>
<td>Operations Console Administrator password</td>
<td></td>
</tr>
</tbody>
</table>

### Replica Appliance Setup

<table>
<thead>
<tr>
<th>Description</th>
<th>Your Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replica package file location</td>
<td></td>
</tr>
<tr>
<td>Hostname or IP address of an NTP server</td>
<td></td>
</tr>
<tr>
<td>Operating system password</td>
<td></td>
</tr>
</tbody>
</table>

### Load Balancer Configuration

<table>
<thead>
<tr>
<th>Description</th>
<th>Your Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load balancer IP address</td>
<td></td>
</tr>
<tr>
<td>Load balancer hostname/virtual hostname</td>
<td></td>
</tr>
<tr>
<td>Port number</td>
<td></td>
</tr>
<tr>
<td>IP address of virtual host or load balancer on the DNS server</td>
<td></td>
</tr>
</tbody>
</table>

### Web Tier Installation

<table>
<thead>
<tr>
<th>Description</th>
<th>Your Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of the RSA Authentication Manager 8.4 Extras download kit, which contains the web-tier installers.</td>
<td></td>
</tr>
<tr>
<td>Web-tier server IP addresses</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Your Plan</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Web-tier server hostnames</td>
<td></td>
</tr>
<tr>
<td>IP address of the DNS server</td>
<td></td>
</tr>
</tbody>
</table>
# Chapter 2: Deploying a Primary Appliance

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform Deployment Tasks for the Primary Instance</td>
<td>38</td>
</tr>
<tr>
<td>Deploy the RSA Authentication Manager Amazon Machine Image</td>
<td>38</td>
</tr>
<tr>
<td>Deploy the RSA Authentication Manager Azure Image File</td>
<td>40</td>
</tr>
<tr>
<td>Deploy the Virtual Appliance Through VMware vCenter Server 6.0</td>
<td>43</td>
</tr>
<tr>
<td>Deploy the Virtual Appliance Through VMware vCenter Server 6.5 or 6.7</td>
<td>44</td>
</tr>
<tr>
<td>Deploy the Virtual Appliance Directly to the VMware ESXi 6.0 Server</td>
<td>46</td>
</tr>
<tr>
<td>Deploy the Virtual Appliance Directly to the VMware ESXi 6.5 or 6.7</td>
<td>47</td>
</tr>
<tr>
<td>Deploy the Virtual Appliance Through the Hyper-V Virtual Machine Manager Console</td>
<td>49</td>
</tr>
<tr>
<td>Deploy the Virtual Appliance Through the Hyper-V Manager</td>
<td>51</td>
</tr>
<tr>
<td>Deploy the Hardware Appliance</td>
<td>53</td>
</tr>
<tr>
<td>Run Quick Setup on the Primary Instance</td>
<td>55</td>
</tr>
<tr>
<td>Certificate Management for Secure Sockets Layer</td>
<td>57</td>
</tr>
<tr>
<td>Log On to the Consoles</td>
<td>58</td>
</tr>
</tbody>
</table>
Perform Deployment Tasks for the Primary Instance

Perform these steps to deploy an appliance and configure an RSA Authentication Manager primary instance.

Procedure

1. Deploy the appliance. Do one of the following:
   - For an Amazon Web Services virtual appliance, Deploy the RSA Authentication Manager Amazon Machine Image below.
   - For an Azure virtual appliance, Deploy the RSA Authentication Manager Azure Image File on page 40.
   - For a VMware virtual appliance, you can do one of the following:
     - Deploy the Virtual Appliance Through VMware vCenter Server 6.0 on page 43
     - Deploy the Virtual Appliance Through VMware vCenter Server 6.5 or 6.7 on page 44
     - Deploy the Virtual Appliance Directly to the VMware ESXi 6.0 Server on page 46
     - Deploy the Virtual Appliance Directly to the VMware ESXi Server 6.5 or 6.7 on page 47
   - For a Hyper-V virtual appliance, you can either Deploy the Virtual Appliance Through the Hyper-V Virtual Machine Manager Console on page 49 or Deploy the Virtual Appliance Through the Hyper-V Manager on page 51.
   - For a hardware appliance, see Deploy the Hardware Appliance on page 53.

2. Configure the appliance with Quick Setup, a software wizard that creates access permission and specifies whether the appliance is a primary instance or a replica instance. See Run Quick Setup on the Primary Instance on page 55.

3. Accept the internal RSA certificate authority (CA) certificate. See Certificate Management for Secure Sockets Layer on page 57.

4. Log On to the Consoles on page 58.

Deploy the RSA Authentication Manager Amazon Machine Image

Deploying the RSA Authentication Manager Amazon Machine Image (AMI) requires several minutes to complete.

Before you begin

- Meet the prerequisites in Amazon Web Services Virtual Appliance Requirements on page 16.
- Request access to the RSA Authentication Manager AMI file for your Amazon account ID. To request access to the AMI, contact RSA Customer Support.

Note: RSA does not support the Amazon Web Services (AWS) feature for creating an AMI from an existing Authentication Manager primary or replica instance. Each Authentication Manager instance must be deployed from the AMI file that RSA provides.
Manually configure network settings. DHCP is not supported.

Provide the appliance network settings for the virtual appliance:

<table>
<thead>
<tr>
<th>Description</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td>This can be any IP address in the same subnet as the interface private IP address.</td>
</tr>
<tr>
<td>Hostname (Fully Qualified Domain Name)</td>
<td>This is provided in the network interface configuration details.</td>
</tr>
<tr>
<td>IP Address</td>
<td>This is provided in the network interface configuration details.</td>
</tr>
<tr>
<td>Netmask</td>
<td>This must match the netmask of the subnet.</td>
</tr>
<tr>
<td>Primary DNS Server (Optional)</td>
<td>The default DNS server in AWS, 169.254.169.253, can be reached by any private subnet in the VPC.</td>
</tr>
<tr>
<td>Secondary DNS Server (Optional)</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** If your region does not allow you to view the AWS console Instance Screenshot, you must provide your own Quick Setup Access Code along with the network settings. The Quick Setup Access is required to begin Quick Setup.

The Quick Setup Access Code must contain eight of the following characters, including at least one number: `abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789`. For example, `EgR7t4LR`. If you do not meet these requirements, you cannot deploy the virtual appliance. Redeploy the appliance with a valid access code.

You can record the appliance network settings in a text file, and paste it into AWS when you are creating the virtual appliance.

**Procedure**

1. Log on to your AWS account.
2. On the Services tab, select **EC2**.
3. In Images, select **AMIs**.
4. Select the **Private Image** filter.
5. Search for the RSA Authentication Manager 8.4 AMI ID.
6. Right-click the AMI, and select **Launch**.
7. On the Choose an Instance Type page, select **m4.large**, **m4.xlarge**, or **m4.2xlarge**, and click **Next: Configure Instance Details**.
8. On the Configure Instance Details page, select a **Network** and a **Subnet** from the drop-down lists.
9. Expand the Network Interfaces section, and add the Primary IP address.
10. Expand the Advanced Details section. In the User data section, enter the appliance network settings as text. For example, you can enter or paste:
    ```
hostname : aws-am-001.example.com  
etmask : 255.255.255.128  
primarydns : 169.254.169.253
```
secondaryDNS:0.0.0.0
accesskey:EgR7tbL7

11. Click **Next: Add Storage**.
12. Review the Add Storage page, but not modify the disk size parameter.
13. If this is a production instance, RSA recommends clearing the **Delete on Termination** checkbox. This ensures that the instance volume is retained when the instance is terminated.
14. Click **Next: Add Tags**.
15. On the Add Tags page, add any required tags. For example, you might enter "Instance Name" as the **Key** and "AM 8.4 primary instance" as the **Value**. Click **Next: Configure Security Group**.
16. On the Configure Security Group page, choose the appropriate configured security group, and click **Review and Launch**.
17. Review the settings on the Review Instance Launch page, and click **Launch**.
18. A key pair is not required for Authentication Manager. To log on to the appliance operating system, you need the password for rsaadmin account. You specify the operating system account password during Quick Setup.
   Select **Proceed without a key pair** from the drop-down list, and acknowledge that you will be able to connect to the appliance operating system with the operating system password.
19. Go to the Instances page, and right-click the new instance. Select **Instance Settings > Get Instance Screenshot** to view the console.
   If your region does not allow you to view the AWS console Instance Screenshot, proceed to step 21.
20. Click **Refresh** to view the updated screenshot.
   After 10 to 15 minutes the Authentication Manager appliance boots and starts configuring network settings. When the Authentication Manager instance is deployed, the screenshot displays the Quick Setup URL and the Quick Setup Access Code.
21. Record the following required information:
   - The Quick Setup URL, which includes the IP address that you entered in step 10.
     https://<IP Address>/
     Quick Setup uses an IP address. The administrative consoles that are available after Quick Setup completes use a fully qualified domain name (FQDN).
   - The Quick Setup Access Code, which is required to initiate Quick Setup. The code is automatically generated, unless you entered it in step 7.
22. Enter the Quick Setup URL in the browser, including https, and press ENTER:
    https://<IP Address>/
23. To confirm the authenticity of the virtual appliance, you must verify that the SHA-1 fingerprint of the certificate presented during Quick Setup matches the SHA-1 fingerprint displayed in the OS Console.

**Deploy the RSA Authentication Manager Azure Image File**

Deploying the RSA Authentication Manager Azure image file requires several minutes to complete.
Before you begin

- Meet the prerequisites in Azure Virtual Appliance Requirements on page 20.
- Manually configure network settings.

Authentication Manager uses a static IPv4 address. DHCP is not supported. The IPv6 protocol is not supported for the Authentication Manager virtual appliance on Azure, because Azure requires DHCP to support the IPv6 protocol.

Provide the appliance network settings for the virtual appliance:

<table>
<thead>
<tr>
<th>Description</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td></td>
</tr>
<tr>
<td>Hostname (Fully Qualified Domain Name)</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Netmask</td>
<td></td>
</tr>
<tr>
<td>Primary DNS Server</td>
<td></td>
</tr>
<tr>
<td>Secondary DNS Server (Optional)</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** You have an option to provide your own Quick Setup Access Code along with the network settings, or you can allow the system to generate a unique code for your virtual appliance. The Quick Setup Access Code is required to begin Quick Setup.

The Quick Setup Access Code must contain eight of the following characters, including at least one number: abcdefghijklmnopqrstuvwxyzACDEFGHIJKLMNPQRSTUVWXYZ0123456789. For example, EgR7t4LR. If you do not meet these requirements, you cannot deploy the virtual appliance. Redeploy the appliance with a valid access code.

- Resource groups are logical containers that allow you to organize your resources. Two Azure resource groups are required:
  1. The existing resource group of your Azure virtual network. You must have already created the following components:
     a. Virtual Network
     b. Subnet
     c. Azure Network Security Group for Authentication Manager
     d. Diagnostic storage account of the Standard_LRS type.
     e. An Available Private IP address in the virtual network.

Procedure

1. Log on to the Azure portal.
2. On the Services tab, select Create a resource.
3. Search for the RSA Authentication Manager 8.4 image. Click Create.
4. On the Basics blade, do the following:
   1. An Administrator Username and Password details are not required for Authentication Manager. To log on to the appliance operating system, you need the rsaadmin account and the password that you specify during Quick Setup.
2. For the **Resource Group** name, enter the name of the new, empty resource group that you created earlier. Do not choose **Create new**. You must create the resource group first, and provide the name here.
3. Select your **Subscription**, which is your Azure account, and your **Location**.
4. Click **OK**.
5. On the Virtual Machine Settings blade, do the following:
   1. Enter a **Virtual Machine name**.
   2. Select a virtual machine **Size**. RSA recommends **Standard_D8s_v3** and **Standard_D4s_v3** virtual machines.
   3. Select a **Storage Account type** for the virtual machine. For information on the performance and pricing difference between **Standard_LRS**, **Premium_LRS**, and **StandardSSD_LRS**, see the Azure documentation.
   4. Provide the Network Interface Name and the Network Interface Private IP Address for the virtual machine. During deployment, a new NIC is created with this information and attached to the new virtual machine.
6. On the Network Settings blade, select the components that you created for the existing resource group:
   - Virtual Network
   - Subnet
   - Azure Network Security Group for Authentication Manager
   - Diagnostic storage account of the **Standard_LRS** type
7. On the User Data blade, do the following:
   1. Enter the Gateway, DNS server, Subnet Mask, and Primary DNS server.
   2. A Secondary DNS server is optional. Azure requires at least one DNS server.
   3. You can provide a Quick Setup Access Code, or you can allow the system to generate a unique code for your virtual appliance.
8. On the Summary blade, review the information that you entered. You can return to any blade if changes are required.
9. On the Buy blade, review the terms and conditions for deploying Authentication Manager in the Azure Marketplace.
10. Click **Create** to deploy a new virtual machine.
    After a successful deployment, you can see the new NIC, Virtual Machine disk and Virtual Machine under the new resource group that you created earlier.
12. Click your virtual machine, select **Serial Console (Preview)**, and press **ENTER** to see the deployment status.
    After 10 to 15 minutes, the Authentication Manager appliance boots and starts configuring network settings. When the Authentication Manager instance is deployed, the screenshot displays the Quick Setup URL and the Quick Setup Access Code.
13. Record the following required information:
    - The **Quick Setup URL**, which includes the IP address that you entered in step 5.
    ```
    https://<IP Address>/
    ```
Quick Setup uses an IP address. The administrative consoles that are available after Quick Setup completes use a fully qualified domain name (FQDN).

- The Quick Setup Access Code, which is required to initiate Quick Setup. The code is automatically generated, unless you entered it in step 7.

14. Enter the Quick Setup URL in the browser, including https, and press ENTER:

https://<IP Address>/

15. To confirm the authenticity of the virtual appliance, you must verify that the SHA-1 fingerprint of the certificate presented during Quick Setup matches the SHA-1 fingerprint displayed in the OS Console.

**Deploy the Virtual Appliance Through VMware vCenter Server 6.0**

You can deploy a virtual appliance through VMware vCenter Server 6.0, if you are using this administrative tool to manage the virtual appliances. This process requires several minutes to complete.

**Note:** Depending on your VMware vCenter configuration and the version of the VMware vSphere Client, some of the windows that are described in the following procedure may not display. The window names may also vary.

**Before you begin**

- Collect the required information about each appliance instance being deployed. See Secure Appliance Deployment on page 30.
- Copy the RSA Authentication Manager Open Virtual Appliance (OVA) file to a location that the VMware vSphere Client can access.

**Procedure**

1. In the VMware vSphere Client, log on to VMware vCenter Server.
2. Select **File > Deploy OVF Template** to start the deployment wizard.
3. On the Source window, under **Deploy from a file or URL**, click **Browse**, and locate the RSA Authentication Manager OVA file to deploy. Click **Next**.
4. On the OVF Template Details window, verify that “RSA Authentication Manager” and the expected version number displays. Click **Next**.
5. On the Name and Location window, enter a **Name** for the virtual appliance, and click **Next**.
6. On the Host/Cluster window, select a host or cluster for the virtual appliance. Click **Next**.
7. On the Resource Pool window, select a resource pool. Resource pools let you manage your resources within a host or cluster. Click **Next**.
8. On the Storage window, select an existing VMware datastore for the virtual machine files. A VMware datastore can be a location such as a Virtual Machine File System (VMFS) volume, a directory on Network Attached Storage, or a local file system path. Click **Next**.
10. On the Network Mapping window, select the networks for the virtual appliance. Click **Next**.
11. On the Properties window, enter the following IPv4 network settings for the virtual appliance, and click **Next**.
• Fully Qualified Domain Name  
• IP Address.  
• Subnet Mask  
• Default Gateway  
• (Optional) Primary DNS Server  
• (Optional) Secondary DNS Server

**Note:** If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete.

12. On the Ready to Complete window, review your settings, and click **Finish**. VMware requires approximately five minutes to deploy the virtual appliance.

13. Power on the virtual machine.

14. Click the **Launch Virtual Machine Console** button.

The virtual machine console displays the progress of the virtual appliance deployment.

15. Wait 30 seconds to select the default keyboard layout, English (United States). To select a different keyboard layout, press any key and follow the instructions on the screen.

16. Verify that the settings are correct. To accept the settings, type **y**, or wait 30 seconds.

17. When the virtual appliance is deployed, the OS Console displays the Quick Setup URL and the Quick Setup Access Code. Record the following required information:

   - The Quick Setup URL includes the IP address that you entered in step 12.
     
     ```text
     https://<IP Address>/
     ```
     
     Quick Setup uses an IP address. The administrative consoles that are available after Quick Setup completes use a fully qualified domain name (FQDN).
   
   - The Quick Setup Access Code is required to initiate Quick Setup.

18. Enter the Quick Setup URL in the browser, including https, and press **ENTER**:

   ```text
   https://<IP Address>/
   ```

19. If you want to confirm the authenticity of the virtual appliance, you must verify that the SHA-1 fingerprint of the certificate presented during Quick Setup matches the SHA-1 fingerprint displayed in the OS Console.

---

**Deploy the Virtual Appliance Through VMware vCenter Server 6.5 or 6.7**

You can deploy a virtual appliance through VMware vCenter Server 6.5 or 6.7, if you are using this administrative tool to manage the virtual appliances. You can use the vSphere Client (HTML5) or the vSphere Web Client (Flash). This process requires several minutes to complete.

**Note:** Depending on your VMware vCenter configuration and the version of the VMware vSphere Client, some of the windows that are described in the following procedure may not display. The window names may also vary.
Before you begin

- Collect the required information about each appliance instance being deployed. See Secure Appliance Deployment on page 30.
- Copy the RSA Authentication Manager Open Virtual Appliance (OVA) file to a location that the VMware vSphere Client can access.

Procedure

1. Use a browser to access the vCenter Server URL.
2. On the Getting Started page, click either the **vSphere Client (HTML5)** or the **vSphere Web Client (Flash)**.
3. On the VMware vCenter Single Sign-On page, log on to the VMware vCenter Server.
4. Do one of the following:
   - (vSphere Client with HTML5) On the Navigator pane (left hand side), right-click the **VMware Datacentre/Cluster/Host** and select **Deploy OVF Template**... to start the deployment wizard.
   - (vSphere Web Client with Flash) On the Navigator pane, right-click on the vCenter server and select **Deploy OVF Template**... to start the deployment wizard.
5. On the Select Template window, select **Local File**, click **Browse**, and locate the RSA Authentication Manager OVA file to deploy. Click **Next**.
6. On the Select Name and Location window, enter a Name for the virtual appliance, select a datacenter or folder where the appliance will be deployed. Click **Next**.
7. On the Select a Resource window, select a host or cluster for the virtual appliance. Click **Next**.
8. On the Review Details window, verify that “RSA Authentication Manager” and the expected version number displays. Click **Next**.
9. On the Select Storage window, select an existing VMware datastore for the virtual machine files. A VMware datastore can be a location such as a Virtual Machine File System (VMFS) volume, a directory on Network Attached Storage, or a local file system path. Click **Next**.
10. On the Select Networks window, select the networks for the virtual appliance. Click **Next**.
11. On the Customize template window, enter the following IPv4 network settings for the virtual appliance, and click **Next**:
   - Fully Qualified Domain Name
   - IP Address.
   - Subnet Mask
   - Default Gateway
   - (Optional) Primary DNS Server
   - (Optional) Secondary DNS Server

**Note:** If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete.

12. On the Ready to Complete window, review your settings, and click **Finish**. VMware requires approximately five minutes to deploy the virtual appliance.
13. Power on the virtual machine.
14. Click the **Launch Virtual Machine Console** button.
   The virtual machine console displays the progress of the virtual appliance deployment.

15. Wait 30 seconds to select the default keyboard layout, English (United States). To select a different keyboard layout, press any key and follow the instructions on the screen.

16. Verify that the settings are correct. To accept the settings, type `y`, or wait 30 seconds.

17. When the virtual appliance is deployed, the OS Console displays the Quick Setup URL and the Quick Setup Access Code. Record the following required information:
   - The Quick Setup URL includes the IP address that you entered in step 12.
     ```
     https://<IP Address>/
     ```
   - Quick Setup uses an IP address. The administrative consoles that are available after Quick Setup completes use a fully qualified domain name (FQDN).
   - The Quick Setup Access Code is required to initiate Quick Setup.

18. Enter the Quick Setup URL in the browser, including `https`, and press ENTER:
   ```
   https://<IP Address>/
   ```

19. If you want to confirm the authenticity of the virtual appliance, you must verify that the SHA-1 fingerprint of the certificate presented during Quick Setup matches the SHA-1 fingerprint displayed in the OS Console.

### Deploy the Virtual Appliance Directly to the VMware ESXi 6.0 Server

You can deploy a virtual appliance directly to the VMware ESXi 6.0 server (VMware Hypervisor). VMware vCenter is not required to deploy the virtual machine. This process requires several minutes to complete.

**Note:** Depending on your configuration of the VMware ESXi server and the server version, some windows that are described in the following procedure may not display. The window names may also vary.

#### Before you begin

- Collect the required information about each appliance instance being deployed. See **Secure Appliance Deployment on page 30**.
- Copy the RSA Authentication Manager Open Virtual Appliance (OVA) file to a location that the VMware vSphere Client can access.

#### Procedure

1. In the VMware vSphere Client, log on to the VMware ESXi server.
2. Select **File > Deploy OVF Template** to start the deployment wizard.
3. On the Source window, under **Deploy from a File or URL**, click **Browse**, and locate the RSA Authentication Manager OVA file to deploy. Click **Next**.
4. On the OVF Template Details window, verify that “RSA Authentication Manager” and the expected version number displays. Click **Next**.
5. On the Name and Location window, enter a **Name** for the virtual appliance, and click **Next**.
6. On the Datastore window, select a directory for the virtual machine files. A VMware datastore can be a location such as a Virtual Machine File System (VMFS) volume, a directory on Network Attached Storage, or a local file system path. Click Next.

7. On the Disk Format window, select a format for storing virtual disks.

8. On the Network Mapping window, select the networks for the virtual appliance. Click Next.

9. On the Ready to Complete window, review your settings, and click Finish. VMware requires approximately five minutes to deploy the virtual appliance.


11. For the virtual appliance, click the Console tab. The OS Console displays the progress of the boot sequence.

12. Wait 30 seconds to select the default keyboard layout, English (United States). To select a different keyboard layout, press any key and follow the instructions on the screen.

13. When prompted, enter the following IPv4 network settings for the virtual appliance:
   - Fully Qualified Hostname
   - IP Address
   - Subnet Mask
   - Default Gateway
   - (Optional) DNS Server Configuration

   **Note:** If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete.

14. Verify that the settings are correct. To accept the settings, type y, or wait 30 seconds.

15. When the virtual appliance is deployed, the OS Console displays the Quick Setup URL and the Quick Setup Access Code. Record the following required information:
   - The Quick Setup URL includes the IP address that you entered in step 14.
     https://<IP Address>/
   - Quick Setup uses an IP address. The administrative consoles that are available after Quick Setup completes use a fully qualified domain name (FQDN).
   - The Quick Setup Access Code is required to initiate Quick Setup.

16. Enter the Quick Setup URL in the browser, including https, and press ENTER:

   https://<IP Address>/

   **Note:** If you want to confirm the authenticity of the virtual appliance, you must verify that the SHA-1 fingerprint of the certificate presented during Quick Setup matches the SHA-1 fingerprint displayed in the OS Console.

### Deploy the Virtual Appliance Directly to the VMware ESXi Server 6.5 or 6.7

You can deploy a virtual appliance directly to the VMware ESXi server 6.5 or 6.7 (VMware Hypervisor). VMware vCenter is not required to deploy the virtual machine. This process requires several minutes to complete.

**Note:** Depending on your configuration of the VMware ESXi server and the server version, some windows that are described in the following procedure may not display. The window names may also vary.
Before you begin

- For VMware ESXi 6.5, Patch Release ESXi650-2018010201 (52236) or later is required. You can check your ESXi Embedded Host Client version by logging on to the ESXi host with SSH, and running the following command:

  \texttt{"esxcli software vib get -n esx-ui"}

  To download the required software, go to \url{https://my.vmware.com}.

- Collect the required information about each appliance instance being deployed. See Secure Appliance Deployment on page 30.

- Copy the RSA Authentication Manager Open Virtual Appliance (OVA) file to a location that the VMware vSphere Client can access.

Procedure

1. In a browser, log on to the VMware ESXi server.
2. On the Navigator pane, right-click Host and select Create/Register VM to start the deployment wizard.
3. On the Select creation type window, select Deploy a virtual machine from an OVF or OVA file. Click Next.
4. On the Select OVF and VMDK files window, enter a Name for the virtual appliance, and locate the RSA Authentication Manager OVA file to deploy. Click Next.
5. On the Select Storage window, select an existing VMware datastore for the virtual machine files. A VMware datastore can be a location such as a Virtual Machine File System (VMFS) volume, a directory on Network Attached Storage, or a local file system path. Click Next.
6. On the Deployment options window, select the networks for the virtual appliance and other options as required. Click Next.
7. On the Additional settings window, leave all of the fields blank. Click Next.
8. On the Ready to Complete window, review your settings, and click Finish. VMware requires approximately five minutes to deploy the virtual appliance.
10. Click the Launch Console button.
    The virtual machine console displays the progress of the virtual appliance deployment.
11. Wait 30 seconds to select the default keyboard layout, English (United States). To select a different keyboard layout, press any key and follow the instructions on the screen.
12. When prompted, enter the following IPv4 network settings for the virtual appliance:
    - Fully Qualified Hostname
    - IP Address
    - Subnet Mask
    - Default Gateway
    - (Optional) DNS Server Configuration

\textbf{Note:} If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete.
13. Verify that the settings are correct. To accept the settings, type y, or wait 30 seconds.

14. When the virtual appliance is deployed, the OS Console displays the Quick Setup URL and the Quick Setup Access Code. Record the following required information:
   - The Quick Setup URL includes the IP address that you entered in step 14.
     https://<IP Address>/
   - Quick Setup uses an IP address. The administrative consoles that are available after Quick Setup completes use a fully qualified domain name (FQDN).
   - The Quick Setup Access Code is required to initiate Quick Setup.

15. Enter the Quick Setup URL in the browser, including https, and press ENTER:
   https://<IP Address>/

**Note:** If you want to confirm the authenticity of the virtual appliance, you must verify that the SHA-1 fingerprint of the certificate presented during Quick Setup matches the SHA-1 fingerprint displayed in the OS Console.

---

### Deploy the Virtual Appliance Through the Hyper-V Virtual Machine Manager Console

You can deploy a virtual appliance through the Hyper-V System Center Virtual Machine Manager (VMM) Console. RSA provides a PowerShell script that creates a virtual machine template that automatically configures the virtual machine. You complete configuration through the Hyper-V VMM Console. This process requires several minutes to complete.

**Before you begin**

- Collect the required information about each appliance instance to deploy. See Secure Appliance Deployment on page 30.
- Copy the RSA Authentication Manager Hyper-V virtual appliance file, rsa-am-hyper-v-virtual-appliance-8.4.0.0.0.zip, to an existing Hyper-V VMM library server or a shared folder on a Microsoft Windows 2012, 2012 R2, or 2016 machine that can be added as a library server.
- Unzip the file to the current location.
- The contents include a Windows batch file, a PowerShell script, and two virtual hard drive (VHD) files. The disk1 VHD file is the primary virtual hard drive that the virtual appliance uses for storage. The disk2 VHD file is a swap drive that improves virtual appliance startup times.

**Note:** Do not rename the VHD files.

**Procedure**

1. Log on to the Microsoft Windows 2012, 2012 R2, or 2016 machine that has the Hyper-V VMM Console installed.

2. (Optional) If the disk1 and disk2 VHD files are not located on an existing library server, add the location of the VHD files as follows:
   a. Open the Hyper-V VMM Console, and log on to the VMM server.
   b. On the Home tab, click Add Library Server.
   c. Select or enter the library server logon credentials, and click Next.
   d. Search for the server that contains the VHD file, select the server, and click Next.
e. Select the share that contains the downloaded VHD file, and click Next.
f. Select the share that contains the downloaded VHD file, and click Next.
g. Click Add Library Servers.

3. On the Windows taskbar, right-click Windows PowerShell, and select Run as Administrator.

4. Change directories to the location of the Windows batch file. Type the following, and press ENTER:

```
cd 'Windows_Directory_Path'
Where
'Windows_Directory_Path' is the location of the Windows batch file.
```

5. To create a Hyper-V virtual machine template, type the following, and press ENTER:

```
\create_vm.bat -vmm -server FQDN_or_IP address -port port_number -libraryserver 'Windows_Directory_Path' -templatename Template_Name
Where
```

- -vmm makes the batch file run in VMM mode.
- -server FQDN_or_IP address is the fully qualified domain name or IP address of the VMM server.
- -port port_number is the optional argument for the VMM server port. If you do not specify this option, the system uses the default value 8100.
- -libraryserver 'Windows_Directory_Path' is the location of the library server managed by the VMM where the VHD files are uploaded.

**Note:** Do not specify a local folder. The -libraryserver argument must specify a library server that is a shared location configured in the VMM server.
- -templatename Template_Name is the optional argument for the name of the template. Specify a template name if you might run the batch file more than one time. If you do not specify a name, the system uses the default value RSA Authentication Manager Appliance VM Template.

The template name must contain 69 or fewer characters and follow Windows naming conventions. For example, the filename cannot contain the characters \ / : * ? " < > and |.

For example, run `\create_vm.bat -vmm -server 192.168.0.0 -libraryserver '\\windows\hyperv.yourorganization.com\libraryshare'` to create a Hyper-V virtual machine template that uses the default port and template name.

6. If you are prompted by a security warning, type y to run the script. By default, PowerShell has a restrictive security policy that does not trust scripts that you download from the Internet.

7. When you are prompted, enter administrative credentials for the VMM server.

After the script successfully creates the virtual machine template, you can use the Create Virtual Machine wizard in the Hyper-V VMM Console.

8. If you have not already done so, open the Hyper-V VMM Console, and log on to the VMM server.

9. Click Library > Templates > VM Templates.

10. Right-click the name of the virtual machine template, and select Create Virtual Machine. The default name is RSA Authentication Manager Appliance VM Template.

The Create Virtual Machine wizard launches.

11. On the Identity window, enter a name for the virtual appliance, and click Next.
12. On the Configure Hardware window, keep the default hardware profile, and click Next. The PowerShell script automatically configured the virtual machine template.

13. On the Select Destination window, select Place the virtual machine on a host, and choose a destination. Click Next.

14. On the Select Host window, choose a Hyper-V host as the destination for deploying the virtual appliance. Click Next.

15. On the Configure Settings window, choose a location to store the virtual appliance files. Click Next.

16. On the Select Networks window, choose a network connection from the drop-down list, and click Next. You must connect the virtual appliance to your network before it is powered on.

17. On the Add Properties window, configure the action to take when the host machine starts or stops. You can choose whether to prevent the virtual appliance from being migrated by Performance and Resource Optimization. Click Next.

18. On the Summary window, click Create.

19. After the virtual appliance is successfully created, power on the virtual appliance, and connect to the virtual appliance through the VMM Console.

20. Wait 30 seconds to select the default keyboard layout, English (United States). To select a different keyboard layout, press any key and follow the instructions on the screen.

21. When the OS Console prompts you, enter the following IPv4 network settings for the virtual appliance:
   - Fully Qualified Hostname
   - IP Address
   - Subnet Mask
   - Default Gateway
   - (Optional) DNS Server Configuration

   **Note:** If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete.

22. Verify that the settings are correct. To accept the settings, type y, or wait 30 seconds.

23. When the virtual appliance is deployed, the OS Console displays the Quick Setup URL and the Quick Setup Access Code. Record the following required information:
   - The Quick Setup URL includes the IP address that you entered in step 22.
   - https://<IP Address>/
   - Quick Setup uses an IP address. The administrative consoles that are available after Quick Setup completes use a fully qualified domain name (FQDN).
   - The Quick Setup Access Code is required to initiate Quick Setup.

24. Enter the Quick Setup URL in the browser, including https, and press ENTER:
   - https://<IP Address>/

   **Note:** To confirm the authenticity of the virtual appliance, you must verify that the SHA-1 fingerprint of the certificate presented during Quick Setup matches the SHA-1 fingerprint displayed in the OS Console.

## Deploy the Virtual Appliance Through the Hyper-V Manager

You can deploy a virtual appliance through the Hyper-V Manager. RSA provides a PowerShell script that creates a virtual appliance. You complete configuration through the Hyper-V Manager. This process requires several
Before you begin

- Collect the required information about each appliance instance to deploy. See Secure Appliance Deployment on page 30.
- Verify that you have the RSA Authentication Manager virtual appliance file, rsa-am-hyper-v-virtual-appliance-8.4.0.0.0.zip.

The file contents include a Windows batch file, a PowerShell script, and two virtual hard drive (VHD) files. The disk1 VHD file is the primary virtual hard drive that the virtual appliance uses for storage. The disk2 VHD file is a swap drive that improves virtual appliance startup times.

After you create the virtual appliance, running the new appliance modifies the VHD files. For each virtual appliance that you deploy with the following procedure, you must extract a new set of VHD files from the .zip file.

Procedure

1. Log on to the Microsoft Windows 2012, 2012 R2, or 2016 Hyper-V host machine.
2. Copy the RSA Authentication Manager Hyper-V virtual appliance file, rsa-am-hyper-v-virtual-appliance-8.4.0.0.0.zip, to a location on the Microsoft Windows 2012, 2012 R2, or 2016 Hyper-V host machine.
3. Unzip the file to the location where you want to create the virtual appliance, but keep the original .zip file.
   For each virtual appliance that you deploy, you must extract a new set of VHD files from the .zip file.
   **Note:** Do not rename the VHD files.
5. Change directories to the location of the Windows batch file. The virtual appliance is created in the directory where you run the script.
   Type the following, and press ENTER:
   ```
   cd 'Windows_Directory_Path'
   Where
   'Windows_Directory_Path' is the location of the Windows batch file.
   ```
6. To create a Hyper-V virtual machine, type the following, and press ENTER:
   ```
   .\create_vm.bat -name virtual_machine
   Where
   -name virtual_machine is the name of the virtual machine. Specify a name if you might run the batch file more than one time. If you do not specify this option, the virtual appliance uses the default name RSA Authentication Manager Appliance.
   For example, type .\create_vm.bat -name AuthenticationMgrPrimary to create a virtual appliance with the name AuthenticationMgrPrimary or type .\create_vm.bat to create a virtual appliance with the default name RSA Authentication Manager Appliance.
   ```
7. If you are prompted by a security warning, type r to run the script. By default, PowerShell has a restrictive security policy that does not trust scripts that you download from the Internet.
8. When prompted, type y to confirm that you want to create a new virtual machine.

   After the script successfully completes, connect the virtual appliance to your network.

9. In the Windows Start menu, click Server Manager > Tools > Hyper-V Manager.

10. In the Hyper-V Manager, select the node and host from the left pane.

11. In the Virtual Machines pane, select the new virtual machine.

12. In the Action pane, under the virtual machine name, click Settings.

13. In the navigation pane, click Add Hardware and configure the Network Adapter, or click Network Adapter and select a virtual switch. Do not use the legacy network adapter. The legacy network adapter is not supported.

14. In the Actions pane, under the virtual machine name, click Start.

15. In the Actions pane, under the virtual machine name, click Connect.

16. Wait 30 seconds to select the default keyboard layout, English (United States). To select a different keyboard layout, press any key and follow the instructions on the screen.

17. When the OS Console prompts you, enter the following IPv4 network settings for the virtual appliance:

   - Fully Qualified Hostname
   - IP Address
   - Subnet Mask
   - Default Gateway
   - (Optional) DNS Server Configuration

   **Note:** If your deployment uses IPv6-compliant agents, you can add IPv6 network settings in the Operations Console after Quick Setup is complete.

18. Verify that the settings are correct. To accept the settings, type y, or wait 30 seconds.

19. When the virtual appliance is deployed, the OS Console displays the Quick Setup URL and the Quick Setup Access Code. Record the following required information:

   - The Quick Setup URL includes the IP address that you entered in step 18.
     https://<IP Address>/
      Quick Setup uses an IP address. The administrative consoles that are available after Quick Setup completes use a fully qualified domain name (FQDN).
   - The Quick Setup Access Code is required to initiate Quick Setup.

20. Enter the Quick Setup URL in the browser, including **https**, and press ENTER:

    https://<IP Address>/

   **Note:** To confirm the authenticity of the virtual appliance, you must verify that the SHA-1 fingerprint of the certificate presented during Quick Setup matches the SHA-1 fingerprint displayed in the OS Console.

---

### Deploy the Hardware Appliance

Use the following procedure to deploy the hardware appliance.

**Before you begin**

Collect the information and items that are required for a hardware deployment. For more information, see Secure Appliance Deployment on page 30.
Procedure

1. Connect a keyboard and monitor to the hardware appliance.
2. Connect the power cord to the appliance and power on the appliance.
3. When the appliance boot screen displays, select **Start RSA Authentication Manager** and press ENTER, or wait 10 seconds for Authentication Manager to load automatically.

   **Note:** Do not use the F2 or F4 function key options that display for language and keyboard settings in the boot screen. After you start Authentication Manager, you can change the keyboard language when you are prompted for these settings.

4. By default, the keyboard is configured for **English (United States)**. To retain this setting, wait 30 seconds. To configure a new language, do the following:
   a. Press any key.
   b. Type the number that is associated with the language you want to configure, and press ENTER.
5. When prompted, configure the following network settings for the appliance:
   - Fully Qualified Hostname
   - IP Address
   - Subnet Mask
   - Default Gateway
   - (Optional) Primary DNS Server
   - (Optional) Secondary DNS Server
6. When prompted to confirm the network settings, verify the settings are correct. To accept the settings, type **y**.
7. The Quick Setup URL and the Quick Setup Access Code display. Record the following required information:
   - The Quick Setup URL includes the IP address that you entered in step 6.
     https://<IP Address>/
     Quick Setup uses an IP address. The administrative consoles that are available after Quick Setup completes use a fully qualified domain name (FQDN).
   - The Quick Setup Access Code is required to initiate Quick Setup.
8. If you have not done so already, connect the appliance to the network.

After you finish

RSA strongly recommends doing one of the following:

- Use standard system disk imaging software to create a backup image of the hardware appliance in case you need to restore the original settings. RSA has qualified Clonezilla software. For more information, see “Using Clonezilla to Back Up and Restore the RSA Authentication Manager 8.4 Hardware Appliance” on RSA Link at [https://community.rsa.com/docs/DOC-97375](https://community.rsa.com/docs/DOC-97375).
- Prepare to remotely restore the hardware appliance in a disaster recovery situation. Do the following:
  a. Enable remote access to the hardware appliance:
     On a new Dell-based hardware appliance (RSA SecurID Appliance 130, RSA SecurID Appliance 250, or RSA SecurID Appliance 350) or an upgraded Dell-based version of the RSA SecurID Appliance 250, deploy an integrated Dell Remote Access Controller (iDRAC).
On a new or upgraded Intel-based version of the RSA SecurID Appliance 250, deploy an Intel Remote Management Module (RMM).

RSA has not qualified upgraded versions of the RSA SecurID Appliance 130 for remote access. For instructions, see "Configuring Remote Access to the RSA Authentication Manager Hardware Appliance" on RSA Link at https://community.rsa.com/docs/DOC-67160.

b. Download rsa-am-hardware-appliance-8.4.0.0.0.iso from https://my.rsa.com, and save the ISO file to a location that is accessible to the IDRAC or RMM.

   - In a disaster recovery situation, see the Help topic "Hardware Appliance System Image Installation."

### Run Quick Setup on the Primary Instance

Quick Setup configures the appliance as an RSA Authentication Manager instance. Keep the appliance on a trusted network until Quick Setup is complete. The client computer and browser used to run Quick Setup should also be on a trusted network.

If you do not complete Quick Setup, you will be prompted to verify the network settings every time you power on the virtual or hardware appliance. On Amazon Web Services, do not cancel Quick Setup, or you will be unable to access the Quick Setup URL. In that situation, you must terminate the Amazon Web Services instance, and deploy the primary instance again

**Before you begin**

- You must have deployed a virtual appliance or hardware appliance.
- Verify that the browser on the local computer can access the license file (.zip) used during Quick Setup. For more information, see Secure Appliance Deployment on page 30.

**Note:** Before performing Quick Setup, verify the date and time of the appliance BIOS. If you perform Quick Setup with an incorrect date or time, this setting can result in a failure to start Authentication Manager or other issues. For more information, see the Knowledgebase article 000016944 at https://rsaportal.force.com/customer/kA070000000PL8w.

**Procedure**

1. Launch Quick Setup. Open a web browser and go to the following URL:
   https://<IP ADDRESS>
   where <IP ADDRESS> is the IP address of the appliance.
2. If your web browser is configured for an enhanced security level, a warning states that this URL is not on the list of allowed or trusted sites. To continue, click the option that allows your browser to connect to an untrusted site. For example, your browser might ask you to click a link that reads “I Understand the Risks.”
3. When prompted, enter the Quick Setup Access Code, and click Next.
4. Read the End User License Agreement (EULA). Click Accept.
5. On the Primary and Replica Quick Setup window, click Start Primary Quick Setup.
6. On the Primary Quick Setup page, click Start Step 1.
7. Specify the location of the license file (.zip), and click **Upload**.

   If you select an evaluation license, 25 evaluation software tokens are created. The evaluation software tokens are provided for use with the evaluation license.

8. Review the license summary, and click **Next**.

9. On the Date & Time page, do the following:
   a. In the **Time Zone** section, do the following in this order:
      - Select a region, for example, America.
      - Select a location. If the time zone uses Daylight Savings Time, two offsets from Coordinated Universal Time (UTC) are shown, for example, (UTC-05/UTC-04) New York.
   b. In the **Time Source** section, choose how you want the time to be set on the appliance, manually (hardware appliance only) or automatically (hardware or virtual appliance).

   To automatically synchronize the time on a hardware appliance or virtual appliance to an NTP server:
      a. Select **Sync to NTP Server**.
      b. Enter the hostname or IP address for a local or Internet Network Time Protocol (NTP) server.

   You may enter a second NTP server.

   If Quick Setup cannot connect to an NTP server, you can add an NTP Server in the Operations Console after Quick Setup is complete.

   (Amazon Web Services appliance only) Amazon Web Services (AWS) includes a default Network Time Protocol (NTP) server with the IP address 169.254.169.123.

   c. To test the connection to the NTP server and verify that the correct time is selected, click **Preview Current Date & Time**.

   To automatically synchronize the time on a virtual appliance to the VMware or Hyper-V host machine:
      a. Select **Sync to the physical machine hosting this virtual appliance**.
      b. To test the connection to the virtual host and verify that the correct time is selected, click **Preview Current Date & Time**.

   To manually set the time on a hardware appliance:
      a. Select **Set System Time**.
      b. From the date box, select the date.
      c. From the time drop-down boxes, select the hour and minute.
   c. Click **Next**.

10. On the OS Password page, create and confirm the operating system password, and click **Next**.

    **Note:** The operating system password is required to log on to the primary instance.

    Record the operating system password, so that you can access it when you need it. For security reasons, RSA does not provide a utility for recovering the operating system password.
11. On the Initial Administration Accounts page, create the initial administration credentials for the Security Console Super Admin and the Operations Console (OC) administrator. Click **Next**.

**Note:** The User ID must be unique. It can contain 1 to 255 ASCII characters. The characters @ ~ are not allowed, and spaces are not allowed. If a User ID contains unsupported characters, the user cannot authenticate.

Record these User IDs and passwords.

**Note:** After you complete Quick Setup, you can create additional Super Admin and Operations Console administrator accounts in the Security Console.

12. Review the information that you have entered. If you want to change anything, click **Back**, and make the change on the appropriate page. If necessary, use the navigation links at the top of the page.

13. Click **Start Configuration**.

After the instance is configured, direct links are provided to the Security Console and the Operations Console.

**After you finish**

- Web browsers used to administer Authentication Manager must have JavaScript enabled. See your web browser documentation for instructions on enabling JavaScript.
- RSA recommends enabling SSH on the Amazon Web Services (AWS) virtual appliance and the Azure virtual appliance, because SSH is the only way to log on to the operating system for these cloud-based appliances. Enabling SSH is optional on the VMware virtual appliance, the Hyper-V virtual appliance, and the hardware appliance. For instructions, see the Help topic "Enable Secure Shell on the Appliance."
- (VMware only) After Quick Setup completes, you can change the appliance network settings in the Operations Console. Network Setting changes made in the VMware vSphere Client will no longer take effect.
- (Optional) You can download a text file that contains the network settings for the primary instance. You can refer to this information if you need to restore the original system image on the hardware appliance. For instructions, see the Help topic “Download Network Settings for a Primary or Replica Instance.”
- Apache components included in the Authentication Manager appliance prevent the use of nonstandard email domains, such as .bank, .law, and .sms. Authentication Manager allows the nonstandard .local domain. To use other nonstandard domains, you must edit the Authentication Manager **ims.properties** file. For instructions, see the Help topic “Allow the Use of Nonstandard Email Domains.”

## Certificate Management for Secure Sockets Layer

Secure Sockets Layer (SSL) is enabled by default for communication ports that are used for RSA Authentication Manager administration and replication. When you deploy an instance of Authentication Manager, communication is secured by a long-lived SSL certificate. This certificate is unique to your deployment, and it is signed by an internal RSA certificate authority (CA).

Because this SSL certificate is signed by an internal RSA CA, your browser may present a warning message that the default certificate cannot be verified. If an Online Certificate Status Protocol (OCSP) client is deployed, you may receive a message that revocation list information is not available. This is expected behavior.
To continue, click the option that allows your browser to proceed or to connect to an untrusted site. For example, your browser might ask you to click a link that reads “I Understand the Risks.”

To prevent this warning message from appearing, you must add the internal RSA CA to your browser’s trusted root certificate list, or replace the RSA certificate with one that is signed by a certificate authority that is trusted by your browser.

**Note:** If you use dynamic seed provisioning (CT-KIP) to distribute software tokens to RSA SecurID Software Token 2.2 or later for iOS, RSA recommends that you use a certificate that is signed by a trusted certificate authority.

See your browser documentation for instructions about adding the internal RSA CA to your browser’s list of trusted root certification authorities.

**Log On to the Consoles**

This procedure describes how to access the Security Console, Operations Console, and the Self-Service Console.

**Procedure**

1. Open a supported web browser, and enter one of the URLs listed in the following table. Each console supports more than one URL.

<table>
<thead>
<tr>
<th>Console</th>
<th>URLs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Console</td>
<td>https://&lt;fully qualified domain name&gt;</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified domain name&gt;/sc</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified domain name&gt;:7004/console-ims</td>
</tr>
<tr>
<td>Operations Console</td>
<td>https://&lt;fully qualified domain name&gt;/oc</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified domain name&gt;:7072/operations-console</td>
</tr>
<tr>
<td>Self-Service Console</td>
<td>If there is no web tier, enter:</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified domain name&gt;/ssc</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified domain name&gt;:7004/console-selfservice</td>
</tr>
<tr>
<td></td>
<td>After installing a web tier in a deployment with both primary and</td>
</tr>
<tr>
<td></td>
<td>replica instances, enter:</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified virtual host name&gt;</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified virtual host name&gt;/ssc</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified virtual host name&gt;/console-selfservice</td>
</tr>
<tr>
<td></td>
<td>After installing a web tier in a deployment with a primary instance</td>
</tr>
<tr>
<td></td>
<td>only, enter:</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified virtual host name&gt;/ssc</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified virtual host name&gt;/console-selfservice</td>
</tr>
<tr>
<td></td>
<td>If you change the default load balancer port, enter:</td>
</tr>
<tr>
<td></td>
<td>https://&lt;fully qualified virtual host name&gt;:&lt;virtual host port&gt;/ssc</td>
</tr>
</tbody>
</table>
Console | URLs
---|---
| https://<fully qualified virtual host name>:<virtual host port>/console-selfservice

For example, if the fully qualified domain name of your appliance installation is "host.mycompany.com," to access the Security Console, enter one of the following URLs in your web browser:

https://host.mycompany.com
https://host.mycompany.com/sc
https://host.mycompany.com:7004/console-ims

2. If your web browser is configured for an enhanced security level, you must add an entry to the list of allowed or trusted sites. See your browser documentation for instructions about adding allowed or trusted sites.

3. To access the Security Console, enter the Super Admin User ID and password that you specified during Quick Setup. To access the Operations Console, enter the Operations Console User ID and password that were entered during Quick Setup.

For more information on the Console accounts and passwords, see Administrative Accounts on page 121.

**Note:** The Security Console may take up to 10 minutes to complete initial startup.
Chapter 3: Deploying a Replica Appliance

- Perform Deployment Tasks for a Replica Instance .............................................. 62
- Generate and Download a Replica Package File ............................................... 62
- Run Quick Setup on the Replica Instance ......................................................... 63
- Attach the Replica Instance to the Primary Instance ........................................ 66
Perform Deployment Tasks for a Replica Instance

Perform these steps to deploy an appliance and deploy an RSA Authentication Manager replica instance.

Procedure

1. Deploy the appliance. Do one of the following:
   - For an Amazon Web Services virtual appliance, Deploy the RSA Authentication Manager Amazon Machine Image on page 38.
   - For an Azure virtual appliance, Deploy the RSA Authentication Manager Azure Image File on page 40.
   - For a VMware virtual appliance, you can do one of the following:
     - Deploy the Virtual Appliance Through VMware vCenter Server 6.0 on page 43
     - Deploy the Virtual Appliance Through VMware vCenter Server 6.5 or 6.7 on page 44
     - Deploy the Virtual Appliance Directly to the VMware ESXi 6.0 Server on page 46
     - Deploy the Virtual Appliance Directly to the VMware ESXi Server 6.5 or 6.7 on page 47
   - For a Hyper-V virtual appliance, you can either Deploy the Virtual Appliance Through the Hyper-V Virtual Machine Manager Console on page 49 or Deploy the Virtual Appliance Through the Hyper-V Manager on page 51.
   - For a hardware appliance, see Deploy the Hardware Appliance on page 53.

2. Generate and Download a Replica Package File below.

3. Configure the appliance with Quick Setup, a software wizard that creates access permission and specifies whether the appliance is a primary instance or a replica instance. See Run Quick Setup on the Replica Instance on the facing page.

4. Attach the Replica Instance to the Primary Instance on page 66.

Generate and Download a Replica Package File

Before you can add a replica instance to the deployment, you must create a replica package file on the primary instance. This file has configuration data that enables the replica instance to connect to the primary instance. The replica instance must have access to this file.

Before you begin

You must be an Operations Console administrator.

Procedure

1. On the primary instance, log on to the Operations Console.

2. Click Deployment Configuration > Instances > Generate Replica Package.
3. Click Download to download the replica package file, and click Save to save the replica package to your local machine. The name of the replica package file is replica_package.zip.

4. Click Done to return to the Operations Console Home page.

**Run Quick Setup on the Replica Instance**

Quick Setup performs the following tasks to add a replica appliance to the deployment:

- Quick Setup configures the appliance as an RSA Authentication Manager replica instance.
- Quick Setup attaches the replica instance to the primary instance.

After Quick Setup configures the replica instance, you can choose one of the following options:

- Attach the replica instance immediately to the primary instance.
- Defer attaching the replica instance until a later time.

If you choose to defer attaching the replica instance, Quick Setup powers off the replica instance. The next time you power on the replica instance, you can access Quick Startup to complete the attach process.

As a best practice, RSA recommends that you keep the appliance on a trusted network until Quick Setup is complete. The client computer and browser used to run Quick Setup should also be on a trusted network.

If you do not complete Quick Setup, you will be prompted to verify the network settings every time you power on the virtual or hardware appliance. On Amazon Web Services, do not cancel Quick Setup or defer replica attachment, or you will be unable to access the Quick Setup URL. In that situation, you must terminate the Amazon Web Services instance, and deploy the replica instance again.

**Before you begin**

- Collect the required information about each replica instance that you want to set up. See Deployment Checklist for the Primary and Replica Instance on page 31.

- You must have deployed the appliance:
  - For an Amazon Web Services AMI appliance, see Deploy the RSA Authentication Manager Amazon Machine Image on page 38.
  - For an Azure appliance, see Deploy the RSA Authentication Manager Azure Image File on page 40.
  - For a VMware virtual appliance, see Deploy the Virtual Appliance Through VMware vCenter Server 6.0 on page 43 or Deploy the Virtual Appliance Directly to the VMware ESXi 6.0 Server on page 46.
  - For a Hyper-V virtual appliance, you can Deploy the Virtual Appliance Through the Hyper-V Virtual Machine Manager Console on page 49 or Deploy the Virtual Appliance Through the Hyper-V Manager on page 51.
  - For a hardware appliance, see Deploy the Hardware Appliance on page 53.
  - Generate and Download a Replica Package File on the previous page.
**Note:** Before performing Quick Setup, verify the date and time of the appliance BIOS. If you perform Quick Setup with an incorrect date or time, this setting can result in a failure to start Authentication Manager or other issues. For more information, see the Knowledgebase article 000016944 at https://rsaportal.force.com/customer/kA070000000PL8w.

### Procedure

1. Launch Quick Setup. Open a browser and go to the following URL:
   
   https://<IP ADDRESS>
   
   where <IP ADDRESS> is the IP address of the replica appliance.

2. If your web browser is configured for an enhanced security level, a warning states that this URL is not on the list of allowed or trusted sites. To continue, click the option that your browser presents that allows you to connect to an untrusted site. For example, your browser might ask you to click a link that reads "I Understand the Risks."

3. When prompted, enter the Quick Setup Access Code, and click Next.

4. Read the End User License Agreement (EULA). Click Accept.

5. On the Primary and Replica Quick Setup window, click Start Replica Quick Setup.


7. On the Date & Time Settings page, do the following in this order:

   a. In the Time Zone section, do the following in this order:
      
      - Select a region, for example, America.
      
      - Select a location. If the time zone uses Daylight Savings Time, two offsets from Coordinated Universal Time (UTC) are shown, for example, (UTC-05/UTC-04) New York.

   b. In the Time Source section, choose how you want the time to be set on the appliance, manually (hardware appliance only) or automatically (hardware or virtual appliance).

      To automatically synchronize the time on a hardware appliance or virtual appliance to an NTP server:

      a. Select Sync to NTP Server.

      b. Enter the hostname or IP address for a local or Internet Network Time Protocol (NTP) server.

      You may enter a second NTP server.

      If Quick Setup cannot connect to an NTP server, you can add an NTP Server in the Operations Console after Quick Setup is complete.

      (Amazon Web Services appliance only) Amazon Web Services (AWS) includes a default Network Time Protocol (NTP) server with the IP address 169.254.169.123.
c. To test the connection to the NTP server and verify that the correct time is selected, click Preview Current Date & Time.

To automatically synchronize the time on a virtual appliance to the VMware or Hyper-V host machine:

a. Select Sync to the physical machine hosting this virtual appliance.

b. To test the connection to the virtual host and verify that the correct time is selected, click Preview Current Date & Time.

To manually set the time on a hardware appliance:

a. Select Set System Time.

b. From the date box, select the date.

c. From the time drop-down boxes, select the hour and minute.

c. Click Next.

8. Create and confirm the operating system password, and click Next.

**Note:** The operating system password is required to log on to the replica instance.

Record the operating system password for future use. For security reasons, RSA does not provide a utility for recovering the operating system password.

9. Review the information that you have entered. If you want to change anything, click Back, and make the change on the appropriate page. If necessary, use the navigation links at the top of the page.

10. Click Start Configuration.

After the instance is configured, do one of the following:

- Click Begin Attach to attach the replica instance to the primary instance. For instructions, see Attach the Replica Instance to the Primary Instance on the next page.

- Click Defer Attach to attach the replica instance at another time. When prompted, confirm your choice. The replica instance powers off. You can attach the replica instance the next time you power on the replica instance.

**Note:** On Amazon Web Services, do not defer replica attachment, or you will be unable to access the Quick Setup URL. In that situation, you must terminate the Amazon Web Services instance, and deploy the replica instance again.

### After you finish

- Replica Attachment Issues and Solutions on page 67.

- RSA recommends enabling SSH on the Amazon Web Services (AWS) virtual appliance and the Azure virtual appliance, because SSH is the only way to log on to the operating system for these cloud-based appliances. Enabling SSH is optional on the VMware virtual appliance, the Hyper-V virtual appliance, and the hardware appliance. For instructions, see the Help topic "Enable Secure Shell on the Appliance."

- (Optional) You can download a text file that contains the network settings for the replica instance. You
can refer to this information if you need to restore the original system image on the hardware appliance. For instructions, see the Help topic “Download Network Settings for a Primary or Replica Instance.”

**Attach the Replica Instance to the Primary Instance**

Attaching the replica instance to the primary instance enables the replica instance to synchronize data with the primary instance. The replica instance records all authentications locally and sends the authentication and log data to the primary instance at regular intervals. When the primary instance is unavailable, the replica instance holds this data locally until the primary instance becomes available.

**Note:** The replica instance cannot authenticate users during the attachment process.

The instances use the TCP/IP protocol over an encrypted link for secure database synchronization. Instances can communicate over a local area network (LAN) or a wide area network (WAN).

For information on firewalls, see Port Traffic on page 114.

**Before you begin**

Confirm the following:

- You generated a replica package file on the primary instance and downloaded the replica package to your local machine. For instructions, see the Help topic “Generate a Replica Package.”

- The primary and replica instances can resolve and connect to each other on the following ports:
  - 7002/TCP
  - 7022/TCP
  - 1812/TCP
  - 1813/TCP

  **Note:** Ports 1812 and 1813 are used by RSA RADIUS. If you do not plan to use RSA RADIUS, you must still open these ports on your network, for example, on any firewalls sitting between the primary instance and the replica instance, for attachment to succeed.

- The RSA RADIUS service is running on the primary instance.
  Even if you do not plan to use RADIUS, the service must be running for the replica attachment to succeed.

- The clocks on the primary and replica instances are synchronized. If the clocks are off by more than 10 minutes, the attachment fails.

- If you deferred attaching the replica instance after it was configured using Quick Setup, power on the replica instance and access Quick Setup. Quick Setup resumes at the Attach to Primary Instance page.

**Procedure**

1. On the Attach to Primary Instance page under **Upload Replica Package**, click **Browse**, and select the replica package file to upload from your local machine. Click **Next**.
2. Under **Provide Credentials**, enter your Operations Console administrator User ID and password, and click **Next**.

**After you finish**

- Check the replication status by viewing the Replication Status Report for the replica instance. In the Operations Console for the replica instance, click **Deployment Configuration > Instances > Status Report**.
- If you are using RSA RADIUS, verify the replication status of the RADIUS server. In the Security Console for the replica instance, click **RADIUS > RADIUS Servers**.
- Make sure that the web browsers used to access the Security Console or the Operations Console have JavaScript enabled. See your web browser documentation for instructions on enabling JavaScript.
- After the replica instance is attached to the primary instance, network setting changes made in the VMware vSphere Client will no longer take effect. Use the Operations Console in the primary instance to change the network settings.

**Replica Attachment Issues and Solutions**

If replica attachment requires additional information, perform the tasks listed in the following table.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The replica instance cannot resolve the primary instance hostname.</td>
<td>In the <strong>Associated Primary IP Address</strong> field, enter the primary instance IP address, and click <strong>Next</strong>.</td>
</tr>
<tr>
<td>The replica instance cannot reach the primary instance.</td>
<td>In the <strong>Retry Options</strong> field, correct the primary instance IP address. Choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Address network connectivity issues, and then try to reach the primary instance again.</td>
</tr>
<tr>
<td></td>
<td>• Select the <strong>Override IP Address</strong> field, and enter the correct IP address for the primary instance. This information is saved in the hosts file of this appliance, and it overrides the DNS configuration, if a DNS server is available.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>Next</strong>, and enter your Operations Console administrator credentials.</td>
</tr>
<tr>
<td>The primary instance cannot resolve the replica instance hostname</td>
<td>1. Update the DNS server, if applicable, or use the primary instance Operations Console to edit the hosts file with the correct information for the replica instance. For instructions, see the Help topic “Edit the Appliance Hosts File.”</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>The replica instance cannot communicate with the primary instance on the RADIUS ports.</td>
<td>Verify that the RSA RADIUS service is running on the primary instance. To do so:</td>
</tr>
<tr>
<td></td>
<td>1. Log on to the Operations Console on the primary instance.</td>
</tr>
<tr>
<td>Issue</td>
<td>Solution</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2. Select Deployment Configuration &gt; RADIUS Servers.</td>
<td>1. Verify that the network configuration permits remote connections over ports 1812/TCP and 1813/TCP.</td>
</tr>
<tr>
<td>3. If prompted, enter your Super Admin user ID and password.</td>
<td>2. Click Next.</td>
</tr>
<tr>
<td>4. Click the server that you want to restart.</td>
<td></td>
</tr>
<tr>
<td>5. From the context menu, select Restart Server.</td>
<td></td>
</tr>
<tr>
<td>6. Select Yes, restart RADIUS server, and click Restart Server.</td>
<td></td>
</tr>
<tr>
<td>After less than one minute, the RSA RADIUS Service starts.</td>
<td></td>
</tr>
<tr>
<td>7. Verify that the network configuration permits remote connections over ports 1812/TCP and 1813/TCP.</td>
<td></td>
</tr>
<tr>
<td>8. Click Next.</td>
<td></td>
</tr>
<tr>
<td>The primary instance cannot communicate with the replica instance on the communication port 7002/TCP, and the RADIUS ports 1812/TCP and 1813/TCP.</td>
<td></td>
</tr>
<tr>
<td>1. Verify that the network configuration permits remote connections over the communication port 7002/TCP, and the RADIUS ports 1812/TCP and 1813/TCP.</td>
<td></td>
</tr>
<tr>
<td>2. Click Next.</td>
<td></td>
</tr>
<tr>
<td>If the time difference between the primary instance and replica instance is greater than 10 minutes, replica attachment fails.</td>
<td>You can change the time.</td>
</tr>
<tr>
<td>On the primary instance, log on to the primary instance Operations Console and select Administration &gt; Date &amp; Time.</td>
<td>On the replica instance, redeploy the replica instance with the correct time. To do so:</td>
</tr>
<tr>
<td>On the replica instance, redeploy the replica instance with the correct time. To do so:</td>
<td>1. Delete the failed replica instance from the Operations Console on the primary instance. For instructions, see the Help topic “Delete a Replica Instance.”</td>
</tr>
<tr>
<td></td>
<td>2. Do the following:</td>
</tr>
<tr>
<td></td>
<td>• For a hardware appliance, restore the original backup image that you created when you first deployed the appliance.</td>
</tr>
<tr>
<td></td>
<td>If a backup image is not available, you can apply the original hardware appliance system image. For instructions, see the RSA Authentication Manager Administrator’s Guide.</td>
</tr>
<tr>
<td></td>
<td>• For a VMware virtual appliance, in VMware vCenter or on the ESXi server, shut down and delete the virtual appliance for the failed replica instance.</td>
</tr>
<tr>
<td>Issue</td>
<td>Solution</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>- For a Hyper-V virtual appliance, in the Hyper-V System Center Virtual Machine Manager Console or the Hyper-V Manager, shut down and delete the virtual appliance for the failed replica instance.</td>
</tr>
<tr>
<td></td>
<td>3. Deploy a new replica instance.</td>
</tr>
</tbody>
</table>
Chapter 4: Configuring a Virtual Host and Load Balancer

Virtual Host and Load Balancer Overview ................................................................. 72
Load Balancer Requirements ................................................................................. 72
Configure a Load Balancer and Virtual Host ....................................................... 72
Load Balance Using the Web Tier with Round Robin DNS .................................... 74
Virtual Host and Load Balancer Overview

The virtual host is the gateway to the DMZ for users outside of the network who use risk-based authentication (RBA), the Self-Service Console, and dynamic seed provisioning. You must configure a virtual host and assign each web tier to the virtual host.

Load balancing distributes web tier traffic to the web tier servers. The web-tier deployment can include a load balancer or you can use round robin DNS. The virtual host can be associated with up to 2 load balancers.

For more information on network configurations that require a load balancer, see the RSA Authentication Manager Planning Guide.

Load Balancer Requirements

A load balancer must meet the following requirements:

- **User persistence.** The load balancer must send a client to the same server repeatedly during a session. The load balancer must send the client to the same Authentication Manager instance or web-tier server, depending on your deployment scenario, during an authentication session.

- **X-Forwarded-For headers.** Load balancers in the application layer cause all requests to appear to come from the load balancer. You must configure load balancers to send the original client IP address in the “X-Forwarded-For” header. This is the default for most application layer load balancers.

In addition to the required features, consider the following:

**HTTPS Redirection.** The load balancer must be able to redirect HTTPS requests to another URL. This allows users to use the load balancer hostname to access the Self-Service Console.

Configure a Load Balancer and Virtual Host

When adding a load balancer, you must configure a virtual hostname, IP address, and listening port. The load balancer acts as the virtual host providing an entry point to the demilitarized zone (DMZ). You must configure the virtual host before you can install a web tier.

If your deployment has a load balancer, the virtual hostname must resolve to the public IP address of the load balancer.

If your deployment does not have a load balancer, the virtual hostname must resolve to the public IP address of your web tier.

If you change the name of the load balancer or use another load balancer, you must change the virtual hostname accordingly.

**Before you begin**

- You must be a Super Admin.
- The virtual hostname must be configured in the Domain Name System (DNS) to point to the load balancer.
Procedure

1. In the Operations Console on the primary instance, click Deployment Configuration > Virtual Host & Load Balancing.

2. If prompted, enter your Super Admin User ID and password.

3. On the Virtual Host & Load Balancing page, do the following:
   a. Select Configure a virtual host and load balancers.
   b. Enter a fully qualified virtual hostname unique to the deployment.
   c. (Optional) Change the default port number.
   d. Provide the IP address for each of the load balancers that you intend to use. You can add up to two load balancers.
      The virtual host must be configured in the Domain Name System to point to the load balancers.
      If you are not using a load balancer, leave the IP address blank.
   e. Click Add.

4. Click Save.
   The system saves the virtual hostname and key material in the keystore file.

5. On the confirmation page, read Mandatory Next Steps.

6. Click Done.

After you finish

In the Operations Console, perform the appropriate mandatory next steps.

- If you updated load balancer details, you must reboot the primary and replica instances. In the Operations Console, click Maintenance > Reboot Appliance and reboot each instance.

- If you updated the virtual hostname, generate a new integration script for each web-based application using RBA, and then redeploy the integration scripts.

- If the deployment includes a web tier, update the web tier. In the Operations Console, click Deployment Configuration > Web-Tier Deployments > Manage Existing. Click the update link for each web tier.

- If the deployment includes a web tier, replace the certificate on the load balancer and on the firewall with the virtual host certificate.

- If the deployment uses dynamic seed provisioning, update the hostname and port for the CT-KIP URL with the hostname and port that you specified for the virtual host. In the Security Console, go to Setup > System Settings. Click Tokens.

- If the deployment uses the RSA Self-Service Console, update the Self-Service Console URL with the hostname and port you specified for the virtual host. In the Security Console, go to Setup > Self-Service Settings. Click E-Mail Notifications for User Account Changes.
Load Balance Using the Web Tier with Round Robin DNS

If you do not want to use a load balancer, you can set up the web-tier servers to distribute risk-based authentication (RBA) requests using round robin Domain Name System (DNS).

To set up load balancing using round robin DNS, associate the virtual hostname with the publicly accessible IP addresses of the web-tier servers in your DNS, and then enable round robin. The DNS server then sends RBA requests to web-tier servers.

The following figure shows a sample deployment of Authentication Manager using round robin DNS load balancing.
Chapter 5: Installing Web Tiers

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Tier Overview</td>
<td>76</td>
</tr>
<tr>
<td>Web-Tier Hardware and Operating System Requirements</td>
<td>77</td>
</tr>
<tr>
<td>Performing Web Tier Pre-Installation Tasks</td>
<td>78</td>
</tr>
<tr>
<td>Installing the Web Tier</td>
<td>79</td>
</tr>
<tr>
<td>Add a Web-Tier Deployment Record</td>
<td>80</td>
</tr>
<tr>
<td>Web-Tier Installation Checklist</td>
<td>81</td>
</tr>
</tbody>
</table>
**Web Tier Overview**

A web tier is a secure platform for installing and deploying the Self-Service Console, dynamic seed provisioning, and the risk-based authentication (RBA) service.

The web tier protects the private network by receiving and managing inbound internet traffic before it enters the private network. This prevents end users from accessing the private network through the Self-Service Console or web-based applications, such as SSL-VPNs, thin clients, or web portals. The web-tier server only sends a subset of the traffic, such as authentication traffic, securely to your private network.

In addition to providing network security, deploying Authentication Manager on a web-tier server in your network demilitarized zone (DMZ) offers the following benefits:

- You can customize the end-user interface for the RBA service and web-based applications.
- Improves system performance by removing some processing tasks from the back end server.

Web-tier installation requires a primary instance. It is preferable that there is at least one replica instance of Authentication Manager located in your private network, as well as a load balancer and two web-tier servers located in your DMZ. An instance can have up to 16 web tiers. You need Super Admin permissions to manage the Authentication Manager and the web-tier servers.

Web tiers are not required, but your deployment might need them to satisfy your network configuration and requirements. For more information on the Authentication Manager deployment types, see the Planning Guide.

The following diagram shows traffic flow and ports in a typical web-tier deployment.

![Diagram of traffic flow and ports in a typical web-tier deployment](image)

**Self-Service, Dynamic Seed Provisioning, and RBA Traffic in a Web Tier**

In Authentication Manager, self-service and dynamic seed provisioning traffic is routed to the primary instance because these services can only run on the primary instance. RBA can run on any instance, but Authentication Manager always routes RBA traffic to the preferred RBA instance to distribute the workload.

The preferred RBA instance is the first instance to which Authentication Manager directs RBA traffic. You must
choose a preferred RBA instance when you deploy a web tier. RSA recommends that you select a different preferred RBA instance for each web tier. You can select any Authentication Manager instance as a preferred RBA instance.

The following diagram shows how Self-Service, dynamic seed provisioning, and RBA traffic flows through a web tier.

![Diagram showing web tier flow](image)

If ever the preferred RBA instance is unavailable, Authentication Manager directs RBA traffic to the next instance on the server list.

Note that if you delete a replica that is a preferred RBA instance, the associated web tier is also deleted. RBA traffic flow through the deleted web tier is stopped. If the deployment has a load balancer and virtual host, make sure that they no longer point to the deleted replica and associated web tier.

**Web-Tier Hardware and Operating System Requirements**

The following table lists the minimum requirements for the web-tier server. RSA recommends that you adjust these requirements upwards based on expected usage.

<table>
<thead>
<tr>
<th>Description</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>Hard Drive: 2 GB for web tier installation</td>
</tr>
<tr>
<td></td>
<td>Hard Drive: 4 GB-20 GB free space for logs and updated component downloads</td>
</tr>
<tr>
<td></td>
<td>RAM: 4 GB</td>
</tr>
<tr>
<td></td>
<td>CPU: At least 2 virtual CPUs.</td>
</tr>
<tr>
<td>Ports</td>
<td>External Firewall: 443 HTTPS (TCP)</td>
</tr>
</tbody>
</table>

Chapter 5: Installing Web Tiers
Performing Web Tier Pre-Installation Tasks

Before installing a web tier, perform the following tasks to set up the web-tier environment.

Procedure

1. Verify that you have Super Admin permissions, and permissions to install software.
2. Verify that you have access to the Operations Console.
3. On Linux systems, verify that the open files hard limit for the local user is at least 16384.
4. On Linux systems, if you do not plan to use the default installation directory, then you must use the following command to set the proper permissions on your custom directory:
   
   ```
   chmod -R 755 <Custom_directory_with_a_relative_path>
   ```

5. Make sure that your web-tier servers meet the recommended hardware and operating system requirements. For more information, see Web-Tier Hardware and Operating System Requirements on the previous page.

6. Set up the web-tier servers in the network DMZ.

7. Confirm that the date and time on the web-tier server match the date and time on the instance with which the web tier will be associated (primary or replica) within one minute. The time zones do not have to be the same. For example, the web-tier server time can be 7:00 am (GMT), and the associated instance time can be 9:00 am (GMT + 2).

8. Configure the virtual host. The virtual hostname can be a load balancer hostname or a round-robin Domain Name System (DNS). For instructions, see Configuring a Virtual Host and Load Balancer on
page 71.

9. (Optional) On the virtual host, replace the default certificate.

10. On the load balancer and on the firewall, replace the certificate with the virtual host certificate. For instructions, see your load balancer and firewall documentation.

11. Configure a Domain Name System (DNS) server with the Fully Qualified Hostname (FQHN) of the web tier. The web-tier FQHN must resolve from the RSA Authentication Manager primary instance, and the FQHN of the primary instance must resolve from the web tier.

   If you cannot configure a DNS server, update the appliance hosts file with the web-tier FQHN. Click Administration > Network > Hosts File, and follow the instructions in the Help topic "Edit the Appliance Hosts File."

**Installing the Web Tier**

The following procedure lists the tasks for installing the web tier that is associated with the primary instance. You must perform these tasks before you associate a replica instance with a web tier.

**Before you begin**

- Confirm that the virtual host and load balancer are configured.
- Decide which instance to select as the preferred RBA instance for each web tier.

**Procedure**

1. On the public and private DNS servers, enter the web-tier hostname and IP address.

2. On the primary instance, add a web-tier deployment record and generate a web-tier deployment package. For instructions, see Add a Web-Tier Deployment Record on the next page.

3. On the web-tier server, run the RSA Authentication Web-Tier Installer for your platform. For instructions, see the following:
   - Install a Web Tier on Windows Using the Graphical User Interface on page 82.
   - Install a Web Tier on Windows Using the Command Line on page 83.
   - Install a Web Tier on Linux Using the Graphical User Interface on page 84.
   - Install a Web Tier on Linux Using the Command Line on page 86.

4. Modify the Self-Service Console URL to point to the virtual host and virtual host port. For instructions, see the Help topic "Configure E-mail Notifications for Self-Service User Account Changes."

5. If your deployment uses dynamic seed provisioning, modify the token-key generation URL to point to the virtual hostname, virtual host port, and self-service console. For instructions, see the Help topic "Configure Token Settings."
Add a Web-Tier Deployment Record

A web-tier deployment record must exist in the database on the primary instance before you can install a web tier. The web-tier deployment record establishes communication from the primary instance to web tier.

An instance can have up to 16 web tiers. Each web tier requires a web-tier deployment record.

In the last step of this procedure you can either generate the web-tier deployment package now or generate it at a later date. The web-tier deployment package contains the information that RSA Authentication Manager uses to connect a web tier to the associated instance. The web-tier deployment package is required prior to installing the web tier. If you generate the web-tier package now, you can install the web tier now.

Before you begin

- You must be a Super Admin.
- If you are installing a new web-tier deployment, configure a virtual hostname, listening port, and load balancer. For instructions, see Configure a Load Balancer and Virtual Host on page 72.

Procedure


2. If prompted, enter your Super Admin User ID and password.

3. On the Add New Web-Tier Deployment page, in the Details section, enter the following information:
   - **Deployment name.** The name you want for the web-tier deployment (0-255 characters. The & % > < ‘ and ” characters are not allowed).
   - **Hostname.** Fully qualified hostname of the web-tier server where you are installing the web-tier deployment.
   - **Preferred RBA Instance.** The instance connected to this web-tier deployment to which risk-based authentication (RBA) traffic is directed.

4. In the Web-Tier Service Options section, turn any of the following services on or off.
   - Self-Service Console
   - Risk-based authentication
   - Dynamic seed provisioning

5. In the Virtual Host section, confirm the following information.
   - **Virtual Hostname.** Must be the fully qualified name of the virtual host.
   - **Port Number.** The default is 443.

6. Do one of the following:
- Click **Save**. The system saves the record in the database on the associated primary instance. The trust certificate is updated when you generate a web-tier deployment package.

- Click **Save & Generate Web-Tier Package**. The Generate Web-Tier Deployment Package screen is displayed.

  **Note:** If the web-tier hostname is not resolved, a confirmation screen displays. Follow the instructions on the screen.

**After you finish**

- Confirm the details of this web-tier deployment record. For instructions, see the Help topic “View Web Tier Deployments.”

- If you chose to save the web-tier deployment record without generating the web-tier deployment package, generate the web-tier deployment package before installing the web tier.

- Install the web tier. For instructions, see Installing the Web Tier on page 79.

**Web-Tier Installation Checklist**

RSA Authentication Manager includes web-tier installers for Windows and Linux, which are located in the RSA Authentication Manager 8.4 Extras download kit. After a web tier is installed, the Authentication Manager Operations Console can be used to apply version updates.

Before you launch a web-tier installer, confirm the following:

- You have obtained the RSA Authentication Manager 8.4 Extras download kit from [https://my.rsa.com](https://my.rsa.com).

- The web tier pre-installation tasks are completed.

- The web-tier server meets the system requirements.

- The public and private DNS servers are updated with the web-tier server IP address.

- A web-tier deployment package exists and has been transferred from the primary instance to the web-tier server.

- The Authentication Manager instance to which you will associate the web tier is running.

- You know the following information:
  - Directory name and location where you want the web-tier software installed
  - Fully qualified hostname of the web-tier server
  - Primary NIC IP address (IPv4) of the web-tier server
  - Web-tier deployment package name, location, and web-tier package password
  - For Linux, local user name (do not use root)
The hostname in the web-tier deployment package matches the hostname on the target server.

For Linux, you have root privileges.

After you confirm the items in the checklist, launch the installer you want to use and install the web tier.

- Install a Web Tier on Windows Using the Graphical User Interface below
- Install a Web Tier on Windows Using the Command Line on the facing page
- Install a Web Tier on Linux Using the Graphical User Interface on page 84
- Install a Web Tier on Linux Using the Command Line on page 86

**Install a Web Tier on Windows Using the Graphical User Interface**

During installation, you run the RSA Authentication Web-Tier Installer on the web-tier server. This installs dynamic seed provisioning, the Self-Service Console and risk-based authentication (RBA) service.

Use only numbers and English characters when specifying paths and filenames. Single-byte and double-byte characters are not supported.

**Before you begin**

- Complete the Web-Tier Installation Checklist on the previous page.

- Copy the Webtier folder from the RSA Authentication Manager 8.4 Extras download kit to the supported Windows platform. The linux-x86_64 folder is not needed.

**Procedure**

1. In the location where you copied the RSA Authentication Manager 8.4 Extras download kit, go to Webtier/windows-x86_64 and locate install_webtier.bat.

2. Do one of the following:
   - If User Access Control (UAC) is on, right click install_webtier.bat and select Run As Administrator.
   - If User Access Control (UAC) is off, double-click install_webtier.bat.

3. On the Welcome screen, read the overview and navigation instructions. Click Next.

4. On the License Agreement screen, read the license agreement, and click Next.

5. On the Installation Folder screen, specify the installation folder and click Next.

6. On the Choose Web-Tier Package File screen, do the following:
   a. Select the Web-Tier Package for the instance to which this web-tier server is associated.
   b. Type the Password.
   c. Click Next.

7. On the Summary screen, do one of the following:
• If the summary is correct, click Next.
• If the summary is incorrect, click Previous, and correct the information.

8. On the Installation Progress screen, wait for the progress bar to indicate that the installation is finished and click Next.

9. On the Run Configuration screen, wait for the configuration to complete and click Next.

10. On the Installation Summary screen, click Done.

After you finish

After you exit the web-tier installer, the Web-Tier Update Service connects to the primary server to install the necessary services. Use the Operations Console to check the status of this process.

In the Operations Console, click Deployment Configurations > Web-Tier Deployments > Manage Existing to see the web tier installation status.

Install a Web Tier on Windows Using the Command Line

During installation, you run the RSA Authentication Web-Tier Installer on the web-tier server. This installs dynamic seed provisioning, the Self-Service Console and risk-based authentication (RBA) service.

Use only numbers and English characters when specifying paths and filenames. Single-byte and double-byte characters are not supported.

Before you begin

• Complete the Web-Tier Installation Checklist on page 81.
• Copy the Webtier folder from the RSA Authentication Manager 8.4 Extras download kit to the supported Windows platform. The linux-x86_64 folder is not needed.

Procedure

1. In the location where you copied the RSA Authentication Manager 8.4 Extras download kit, go to Webtier/windows-x86_64 and launch install_webtier.bat in console mode.

2. On the command line, type the following and press ENTER.

   install_webtier.bat -console

3. On the Welcome screen, press ENTER.

4. On the License Agreement screen, press ENTER to continue.

5. On each successive License Agreement screen, you can do the following:

   a. Press ENTER to continue to the next page of the License Agreement.

   On the last screen, type YES and press ENTER to accept the terms of the license agreement.
b. Type Q to quit the License Agreement.
   
   Type **YES** and press ENTER to accept the terms of the license agreement.

6. On the **Installation Folder** screen, enter the location of the installation folder and press ENTER.

7. On the **Choose Web Tier Package** screen, do the following:
   
   a. Enter the web-tier package location and file name, and press ENTER.
   
   b. Enter the web-tier package password, and press ENTER.
   
   c. Press ENTER.

8. On the **Summary** screen, review the summary and do one of the following:
   
   - If the summary is correct, type **1** to continue and press ENTER.
     The installation begins and the **Finish** screen displays when the installation is successful.
   
   - If the summary is incorrect, type **2** and press ENTER to quit.
     The installation terminates and you must begin again.

9. On the **Finish** screen, press ENTER to exit.

**After you finish**

After you exit the web tier installer, the Web-Tier Update Service connects to the primary server to install the necessary services. Use the Operations Console to check the status of this process.

In the Operations Console, click **Deployment Configurations > Web-Tier Deployments > Manage Existing** to see the web tier installation status.

**Install a Web Tier on Linux Using the Graphical User Interface**

During installation, you run the RSA Authentication Web-Tier Installer on the web-tier server. This installs dynamic seed provisioning, the Self-Service Console and risk-based authentication (RBA) service.

- Use only numbers and English characters when specifying paths and filenames. Single-byte and double-byte characters are not supported.

- The install user must have execute permission for the folder into which the web tier is installed.

- Do not save the web-tier installer and the web-tier package under the **/root** directory.

- Do not use spaces in the installation path.

**Before you begin**

- Verify that the open files hard limit for the local user is at least 16384.

- Complete the **Web-Tier Installation Checklist on page 81**.

- Copy the **Webtier** folder from the RSA Authentication Manager 8.4 Extras download kit to the **/tmp** directory on the supported Linux platform. You can exclude the **windows-x86_64** folder.
Procedure

1. Log on as root.

2. On the command line, change directories to the location where you copied the Webtier folder from the RSA Authentication Manager 8.4 Extras download kit. Type the following and press ENTER:
   
   ```bash
   cd /tmp/Webtier/linux-x86_64
   ```

3. Specify read, write, and execute access for the installation files. On the command line, do the following:
   
   - For the `install_webtier.sh` file, type the following, and press ENTER:
     
     ```bash
     chmod 777 ./install_webtier.sh
     ```
   - For the `/tmp/Webtier/linux-x86_64/jdk/bin` directory, type the following, and press ENTER:
     
     ```bash
     chmod 777 /*
     ```

4. On the command line, type the following, and press ENTER:
   
   ```bash
   ./install_webtier.sh
   ```

5. On the RSA Authentication Manager Web-Tier Installer screen, click Next.

6. On the Welcome screen, read the overview and navigation instructions and click Next.

7. On the License Agreement screen, read the license agreement. Accept the terms, and Click Next.

8. On the Installation Folder screen, specify the installation folder and click Next.

9. On the Choose Web-Tier Package File screen, do the following:
   
   - Select the Web-Tier Package for the instance to which this web-tier server is associated.
   - Type the Password.
   - Click Next.

10. On the Install User screen, enter the local user name and click Next.

11. On the Summary screen, do one of the following:
    
    - If the summary is correct, click Next.
    - If the summary is incorrect, click Previous, and correct the information.

12. On the Installation Progress screen, wait for the progress bar to indicate that the installation is complete and click Next.

13. On the Run Configuration screen, wait for the configuration to complete and click Next.


15. Delete the Webtier folder from the /tmp directory.
After you finish

After you exit the web-tier installer, the Web-Tier Update Service connects to the primary server to install the necessary services. Use the Operations Console to check the status of this process.

In the Operations Console, click Deployment Configurations > Web-Tier Deployments > Manage Existing to view the web tier installation status.

Install a Web Tier on Linux Using the Command Line

During installation, you run the RSA Authentication Web-Tier Installer on the web-tier server. This installs dynamic seed provisioning, the Self-Service Console and risk-based authentication (RBA) service.

- Use only numbers and English characters when specifying paths and filenames. Single-byte and double-byte characters are not supported.
- The install user must have execute permission for the folder into which the web tier is installed.
- Do not save the web-tier installer and the web-tier package under the /root directory.
- Do not use spaces in the installation path.

Before you begin

- Verify that the open files hard limit for the local user is at least 4096.
- Complete the Web-Tier Installation Checklist on page 81.
- Copy the Webtier folder from the RSA Authentication Manager 8.4 Extras download kit to the /tmp directory on the supported Linux platform. You can exclude the windows-x86_64 folder.

Procedure

1. Log on as root.

2. On the command line, change directories to the location where you copied the Webtier folder from the RSA Authentication Manager 8.4 Extras download kit. Type the following and press ENTER:
   ```
   cd /tmp/Webtier/linux-x86_64
   ```

3. Specify read, write, and execute access for the installation files. On the command line, do the following:
   - For the install_webtier.sh file, type the following, and press ENTER:
     ```
     chmod 777 ./install_webtier.sh
     ```
   - For the /tmp/Webtier/linux-x86_64/jdk/bin directory, type the following, and press ENTER:
     ```
     chmod 777 */
     ```

4. On the command line, type the following and press ENTER.
   ```
   ./install_webtier.sh -console
   ```

5. On the Welcome screen, type 1 to continue and press ENTER.
6. On the **License Agreement** screen, press ENTER to continue.

7. On each successive **License Agreement** screen, you can do the following:
   - Press ENTER to continue to the next page of the License Agreement.
     On the last screen, type **YES** and press ENTER to accept the terms of the license agreement.
   - Type **Q** to quit the License Agreement.
     Type **YES** and press ENTER to accept the terms of the license agreement.

8. On the **Installation Folder** screen, do the following:
   a. Enter the location of the installation folder.
   b. Press ENTER.

9. On the **Choose Web Tier** screen, do the following:
   a. Enter the web-tier package location and file name, and press ENTER.
   b. Enter the web-tier package password, and press ENTER.
   c. Press ENTER.

10. On the **Installation User** screen, do the following:
    a. Enter the installation user, and press ENTER.
    b. Press ENTER.

11. On the **Summary** screen, review the summary and do one of the following:
    a. If the summary is correct, type **1** to continue and press ENTER.
      The installation begins and the **Finish** screen displays when the installation is successful.
    b. If the summary is incorrect, type **2** and press ENTER to quit.
      The installation terminates and you must begin again.

12. On the **Finish** screen, press ENTER to exit.

13. Delete the **Webtier** folder from the **/tmp** directory.

**After you finish**

After you exit the web tier installer, the Web-Tier Update Service connects to the primary server to install the necessary services. Use the Operations Console to check the status of this process.

In the Operations Console, click **Deployment Configurations** > **Web-Tier Deployments** > **Manage Existing** to view the web tier installation status.
Chapter 6: Next Steps for Your Deployment

Next Steps for Your Deployment ........................................................................................................ 90
## Next Steps for Your Deployment

After deploying RSA Authentication Manager, you must perform the required configuration tasks. You can perform additional configuration tasks based upon your deployment.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
<th>For More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Required Steps for All Deployments</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Usage</td>
<td>Confirm that the ports on the primary and replica instances and the primary and replica web-tier servers are accessible to enable authentication, administration, replication, and other services on the network.</td>
<td>See Port Traffic on page 114.</td>
</tr>
<tr>
<td>RSA Authentication Manager User Accounts</td>
<td>Each user must have an account in RSA Authentication Manager. You can create and store user accounts in the internal database, or you can link Authentication Manager directly to one or more external Lightweight Directory Access Protocol (LDAP) directories.</td>
<td>For more information on using the internal database, see the Help topic &quot;RSA Authentication Manager Users.&quot; For more information on using your existing LDAP directories, see the Help topic &quot;RSA Authentication Manager Identity Sources.&quot;</td>
</tr>
<tr>
<td>Authentication Agents</td>
<td>An authentication agent is the component on the protected resource that communicates with RSA Authentication Manager to process authentication requests. Any resource that is used with SecurID authentication, on-demand authentication (ODA) or risk-based authentication (RBA) requires an authentication agent.</td>
<td>For a list of RSA authentication agents, go to <a href="http://www.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm#!offerings">http://www.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm#!offerings</a>. For a list of third-party products that have embedded RSA agents, go to the RSA Ready Partner Program web site at <a href="http://www.rsaready.com">www.rsaready.com</a>.</td>
</tr>
<tr>
<td><strong>RSA RADIUS Configuration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA RADIUS Configuration</td>
<td>In a RADIUS-protected network, RADIUS clients control user access at the network perimeter. RADIUS clients, which can be VPN servers, wireless access points, or Network Access Servers connected to dial-in modems, interact with RSA RADIUS servers for user authentication and to establish appropriate access control parameters. When authentication succeeds, RADIUS servers return a set of attributes to</td>
<td>See the Help topic &quot;RSA RADIUS Overview.&quot;</td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>For More Information</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>----------------------</td>
</tr>
<tr>
<td></td>
<td>RADIUS clients for session control.</td>
<td></td>
</tr>
<tr>
<td><strong>Authentication Method Configuration</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hardware and Software Tokens</strong></td>
<td><strong>Hardware Token</strong>&lt;br&gt;Device manufactured by RSA that generates and displays tokencodes. A tokencode is always displayed and changes automatically at intervals, such as every 60 seconds. The tokencode must be combined with the user’s PIN to create a passcode, which enables authentication.</td>
<td>See the Help topic “RSA SecurID Tokens.”</td>
</tr>
<tr>
<td></td>
<td><strong>Software Token</strong>&lt;br&gt;Software-based security token installed with an associated RSA SecurID application to a Windows desktop or laptop, a Macintosh computer, or a mobile device. In most cases, software tokens are configured to request a user’s PIN. The software token combines the PIN with the tokencode, and then displays the passcode, which enables authentication. To see if Authentication Manager supports your current software token version, go to the “Product Version Life Cycle for RSA SecurID Suite” page on RSA Link at <a href="https://community.rsa.com/docs/DOC-73369">https://community.rsa.com/docs/DOC-73369</a>.</td>
<td></td>
</tr>
<tr>
<td><strong>Cloud Authentication Service</strong></td>
<td>The Cloud Authentication Service supports a variety of secure and convenient authentication methods, including mobile-optimized push notification, device biometrics, and standards-based FIDO tokens. The Cloud Authentication Service helps secure access to software as a service (SaaS) and on-premise web applications for users. The Cloud Authentication Service can also accept authentication requests from a third-party single sign-on (SSO) solution or web application that has been</td>
<td>To deploy the Cloud Authentication Service, contact your RSA Sales representative. To use multifactor authentication, see Connect RSA Authentication Manager to the Cloud Authentication Service on RSA Link.</td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>For More Information</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>On-Demand Authentication (ODA)</td>
<td>ODA delivers a one-time token code to a user by e-mail or text message. You must configure the on-demand token code delivery method. Install the authentication agent software on the resource that you want to protect, unless the agent is already embedded in the protected resource.</td>
<td>See the Help topic &quot;On-Demand Authentication.&quot;</td>
</tr>
<tr>
<td>Additional Deployment Steps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-service configuration</td>
<td>You can configure RSA Authentication Manager to enable users to perform maintenance and troubleshooting tasks through the Self-Service Console.</td>
<td>See the Help topic &quot;RSA Self-Service Overview.&quot;</td>
</tr>
<tr>
<td>Custom logon banners</td>
<td>You can display a custom logon banner before users log on to the Operations Console, the Security Console, the Self-Service Console, or the appliance operating system with a Secure Shell (SSH) client. The logon banner is often used for legal reasons, for example, to warn users that only authorized personnel have permission to access the system.</td>
<td>See the Help topic &quot;Custom Logon Banners.&quot;</td>
</tr>
<tr>
<td>Securing Your Deployment</td>
<td>You may need to perform additional network and product configuration for secure operation, depending on your network topology and on the RSA Authentication Manager features that you intend to use. In addition, each RSA Authentication Manager instance includes Clam Antivirus (ClamAV) software. ClamAV is an open-source software toolkit that is intended to reduce the risk of intrusion or malicious system or data access.</td>
<td>See the RSA Authentication Manager Security Configuration Guide.</td>
</tr>
</tbody>
</table>
Appendix A: Upgrading to RSA Authentication Manager 8.4

Upgrading to RSA Authentication Manager 8.4 ................................................................. 94
Before Installing RSA Authentication Manager 8.4 ............................................................ 94
Installing Version 8.4 ........................................................................................................... 96
Reinstall the Web Tier ......................................................................................................... 100
Upgrading to RSA Authentication Manager 8.4

You can apply the RSA Authentication Manager 8.4 upgrade patch to any hardware appliance or virtual appliance that has RSA Authentication Manager 8.3 software.

Note: You must upgrade to RSA Authentication Manager 8.3 before applying version 8.4. For instructions, see Upgrading to RSA Authentication Manager 8.3 on page 104.

RSA Authentication Manager 8.4 includes the software fixes in the cumulative Patch 2 for version 8.3. Applying version 8.3 removes any software fixes that are not included in the cumulative Patch 2 for version 8.3, with the exception of any fixes from Patch 3 that are listed in the RSA SecurID Access Release Notes for RSA Authentication Manager. To obtain these all of the software fixes in Patch 3 and later version 8.3 patches, you must apply version 8.4 patches as they become available.

To apply version 8.4, perform these tasks in order:

1. Review the prerequisites. See Before Installing RSA Authentication Manager 8.4 below.

2. Follow the standard steps to apply an Authentication Manager update. See Installing Version 8.4 on page 96.

3. If your deployment includes a web tier, you reinstall it. See Reinstall the Web Tier on page 100.

Before Installing RSA Authentication Manager 8.4

Before installing this upgrade, review the following guidelines and requirements.

Backup Strongly Recommended

RSA Authentication Manager 8.4 is not reversible. If the upgrade patch is not applied successfully, you must restore from a backup file, an Amazon Web Services snapshot, a VMware snapshot, or a Hyper-V checkpoint. Trying to apply version 8.4 again is not recommended.

Note: RSA strongly recommends backing up your deployment, backing up a hardware appliance with PING, taking an AWS snapshot, taking a VMware snapshot, or creating a Hyper-V checkpoint before applying version 8.4.

- If you deployed a hardware appliance or a virtual appliance, you can back up the version 8.3 database. Use the Back Up Now feature in the Operations Console of the primary instance. See the Help topic “Create a Backup using Back Up Now.”

- If you deployed a hardware appliance, RSA recommends using standard system disk imaging software to create a backup image in case you need to restore the hardware appliance. RSA has qualified PING software. For more information, see "Using PING to Back Up and Restore the RSA Authentication Manager 8.2.x Hardware Appliance” on RSA Link: https://community.rsa.com/docs/DOC-41697.

- If you deployed an Amazon Web Services virtual appliance, you can take a snapshot of each virtual machine in the version 8.3 deployment. For additional instructions, see "Primary or Replica Instance Amazon Web Services Snapshots" in the RSA Authentication Manager Administrator’s Guide.

- If you deployed a VMware virtual appliance, you can take a snapshot of each virtual machine in the
version 8.3 deployment. When you take a snapshot of an Authentication Manager instance, you must specify the following settings:

- Do not save the virtual machine’s memory.
- Choose to quiesce the guest file system. This option pauses running processes on the Authentication Manager instance.

For additional instructions, see the VMware vSphere Client documentation.

- If you deployed a Hyper-V virtual appliance, you can create a checkpoint of the version 8.3 deployment. For additional instructions, see the Microsoft Hyper-V documentation.

You can restore version 8.3 if you took a VMware snapshot or a Hyper-V checkpoint before applying version 8.4. Export your data or take other steps to preserve your data before reverting to a snapshot or checkpoint. See the RSA Authentication Manager Administrator’s Guide for information about restoring snapshots and checkpoints.

You can restore version 8.3 if you backed up your deployment before applying version 8.4. See the Help topic “Restore from Backup.”

**Replicated Deployments**

If you have a replicated deployment, all replica instances must be running and replicating successfully before you apply version 8.4 or any other update or patch to the primary instance. To verify the replication status, log on to the primary instance Operations Console, and then click Deployment Configuration > Instances > Status Report.

Apply version 8.4 to the RSA Authentication Manager primary instance before upgrading the replica instances in your RSA Authentication Manager 8.3 deployment. On the primary instance, the replication status may display “Internal Replication Error” or another error until all replica instances have been upgraded or patched. The RADIUS server replication status also displays a replication status of “package failure” or another error until all replica instances have been upgraded or patched.

**Note:** You must successfully upgrade your primary instance before upgrading your replica instances.

**Additional Requirements**

Version 8.4 has the following additional requirements:

- Each virtual appliance must have at least 6 GB of free disk space to apply version 8.4.
- The minimum hardware requirements for the web-tier server have been increased:
  - 2 GB for web tier installation and 4 GB to 20 GB free space for logs and updated component downloads.
  - 4 GB of memory
  - At least two virtual CPUs
- The following credentials are required for the upgrade:
  - Operating system password for the rsaadmin user account on each virtual appliance.
  - An Operations Console administrator account, with access to the Operations Console, for the primary instance and each replica instance.
You can apply the version 8.4 update from a Windows shared folder, an NFS share, or a DVD or CD.

**Note:** From version 8.3 Patch 5, you must apply version 8.3 Patch 6 before upgrading to version 8.4. From earlier patches, you can apply Patch 4 or Patch 6 to obtain the fix that allows you to upgrade to version 8.4 through your browser.

## Installing Version 8.4

The RSA Authentication Manager 8.4 ZIP file, **am-update-8.4.0.0.0.zip**, contains the RSA Authentication Manager 8.4 ISO file, **am-update-8.4.0.0.0.iso**, that is used to apply version 8.4 to Authentication Manager.

You can apply an update through your web browser, or you can store the service pack in an NFS share, a shared folder on Windows, a DVD/CD, or an ISO image on your local machine.

The overall steps to install this service pack are as follows:

- **Specify a Product Update Location**
- **Scan for Updates**
- **Apply the Product Update**

### Specify a Product Update Location

To specify a product update location, or to edit a previously specified location, perform the following procedure to allow RSA Authentication Manager 8.3 to locate the RSA Authentication Manager 8.4 ISO file.

You can apply the version 8.4 update from a Windows shared folder, an NFS share, or a DVD or CD. Version 8.3 Patch 4 is required to upload version 8.4 with a web browser from your local machine.

If you have already specified a location, see **Scan for Updates**.

**Note:** If you are using a Windows share, RSA Authentication Manager 8.4 requires the SMBv2 or SMBv3 protocol. SMBv1 is no longer supported.

### Before you begin

- Download the version 8.4 update from **RSA Link** to a location that the primary or replica instance can access.
- If you intend to scan for updates on an RSA-supplied DVD or CD, do the following:
  - On a hardware appliance, use the DVD/CD drive or mount an ISO image.
  - On a virtual appliance, you must configure the virtual appliance to mount a DVD/CD or an ISO image. See the Help topic "VMware DVD/CD or ISO Image Mounting Guidelines" or "Hyper-V DVD/CD or ISO Image Mounting Guidelines."

### Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.
2. On the Update & Rollback page, your local browser is configured as the method for applying an update. To change that setting, click **Configure Update Source**.
3. On the Configure Update Sources page, specify a location for updates.
To upload the update from your local machine, select **Use your web browser to upload an update**.

To scan for updates on an NFS share, select **Use NFS as the update source**. Enter the full path, including the IP address or hostname where updates are stored. For example: \192.168.1.2\updates

To scan for updates on a Windows shared folder, select **Use Windows Share** as the update source.

- In the **Windows Share Path** field, enter the full path, including the IP address or hostname where updates are stored. For example: \192.168.1.2\updates
- (Optional) In the **Windows Username** field, enter a username. If your Windows share configuration requires it, enter the domain and username.
- (Optional) In the Windows Password field, enter a password only if it is required by your Windows share configuration.

To scan for updates on a DVD or CD, select **Use DVD/CD as the update source**.

4. To test the NFS or Windows share directory settings, click **Test Connection**. A message indicates whether the configured shared directory is available to the primary or replica instance.

5. Click **Save**.

**After you finish**

Do one of the following:

- If you configured your local web browser as the method to apply an update, see **Apply the Product Update**.
- If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, see **Scan for Updates**.

**Scan for Updates**

If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, you can scan to locate and review a list of available product updates.

**Note:** If you are using a Windows share, RSA Authentication Manager 8.4 requires the SMBv2 or SMBv3 protocol. SMBv1 is no longer supported.

**Procedure**

1. In the Operations Console, click **Maintenance > Update & Rollback**.

2. Click **Scan for Updates**. You can view the progress of the scan on the **Basic Status View** tab. You can view more detailed information on the **Advanced Status View** tab.

3. Click **Done** to return to the **Update & Rollback** page.

The **Available Updates** section displays a list of updates, with the following information for each update:
- **Version.** The version of the update. To see the current Authentication Manager version, see the top of the Update and Rollback page.

- **Reversible.** Indicates whether you can roll back (undo) the update. Service pack 1 is not reversible.

- **Automatic Appliance Reboot.** Indicates whether Authentication Manager automatically restarts the Appliance to apply the update. If the Appliance restarts, you must perform another scan to see a current list of updates.

- **Automatic Operations Console Reboot.** Indicates whether Authentication Manager automatically restarts the Operations Console to apply the update. If the Operations Console restarts, you must perform another scan to see a current list of updates.

- **Action.** States whether the update is available to apply. Lists the minimum system requirement for the update.

4. In the **Applied Updates** section, click **Download Detailed History Log** for a complete update history.

   The **Applied Updates** section displays the updates applied to the instance. This section includes the update version numbers, the time and date that each update was applied, and which administrator applied the update.

   After you scan for updates, the new list displays for 24 hours. Logging out of the Operations Console does not remove the list from the system cache. If you restart the Operations Console, download additional updates, or change the product update locations, you must perform another scan to see the most current list.

After you finish

Apply the version 8.4 upgrade patch to the RSA Authentication Manager deployment. See Apply the Product Update below.

**Apply the Product Update**

Apply the product update to the primary instance first, and then to each replica instance. As each replica instance is updated, all of the accumulated data on each replica instance is sent to the primary instance.

**Note:** You must successfully upgrade your primary instance before upgrading your replica instances.

Before you begin

- Ensure that port 8443/TCP is open for https traffic.

  Access to this port is required for real-time status messages when applying RSA Authentication Manager patches and service packs.

  During a product update, the appliance opens this port in its internal firewall. The appliance closes this port when the update is complete.

  If an external firewall blocks this port, the browser displays an inaccessible or blank web page, but the update can successfully complete.

- **Specify a Product Update Location**
You can apply the version 8.4 update from a Windows shared folder, an NFS share, or a DVD or CD. Version 8.3 Patch 4 is required to upload version 8.4 with a web browser from your local machine.

- If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, click **Scan for Updates**.

- In a replicated deployment, all replica instances must be running and replicating successfully before you apply version 8.4 or any other update or patch to the primary instance. To verify the replication status, log on to the primary instance Operations Console, and then click **Deployment Configuration > Instances > Status Report**.

  After upgrading the primary instance, the Authentication Manager replication status may display "Internal Replication Error" or another error until all replica instances have been upgraded or patched. The RADIUS server replication status also displays a replication status of "package failure" or another error until all replica instances have been upgraded or patched.

**Procedure**

1. In the Operations Console, click **Maintenance > Update & Rollback**.

2. RSA recommends applying the most recent update. Do one of the following, depending on your configuration:

   - To apply an update through your local web browser, do the following:
     - a. Click **Upload & Apply Update**.
     - b. Click **Browse** to navigate to the location of the update. You cannot type the update location in the **Update Path** field.
     - c. Click **Upload**.
     - d. Verify the update details, and click **Apply**.

   - If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, do the following:
     - a. Click **Scan for Updates. Available Updates** displays all of the updates that can be applied.
     - b. Next to the update to apply, click **Apply Update**.
     - c. Click **Confirm** to apply the update.

3. In the **Password** field, enter the password for the operating system user rsaadmin, and click **Log On**.

4. The basic status messages appear while the update is applied. You can view more detailed information on the **Advanced Status View** tab.

**Note:** If the browser displays an inaccessible or blank web page, then port 8443/TCP might be blocked by an external firewall. Real-time status messages are not available. Wait for the update to complete.

After the upgrade is applied, the following occurs:
The appliance automatically restarts. When the restart is complete, click Done.

Authentication Manager moves the update from the Available Updates section to the Applied Updates section.

When you return to the Update & Rollback page, the update is listed in the Applied Updates section. To save the high-level update history, click Download Detailed History Log.

The software version information is updated. To view the software version information, log on to the Security Console, and click Software Version Information.

After you finish

You can download a detailed log file containing the information that was displayed on the Advanced Status View tab. The file is named update-version-timestamp.log, where version is the update version number and timestamp is the time that the update completed. For instructions, see the Help topic “Download Troubleshooting Files.”

After you have upgraded the primary instance and all of the replica instances, do the following:

- Verify that replication and radius replication is functioning correctly on the primary instance and the replica instance.
- Version 8.4 includes the software fixes in the cumulative Patch 2 for version 8.3. As needed, obtain later software fixes by applying the latest version 8.4 cumulative patches to the upgraded Authentication Manager instances.
- If the deployment includes a web tier, you must reinstall it. For instructions, see Reinstall the Web Tier on page 110.

Reinstall the Web Tier

If your deployment includes a web tier, after upgrading the primary and replica instances, you must upgrade the web tier. Follow these procedures to retain all existing web-tier configuration and customization settings:

1. Uninstall the Web Tier below
2. Run the Web-Tier Installer for Your Platform on the facing page
3. Update the Web Tier on page 102

Uninstall the Web Tier

Uninstalling a web tier removes the web tier and all features and components of RSA Authentication Manager from the web-tier server. Uninstalling a web tier does not delete the web-tier deployment record.

For instructions, see the following:

Uninstall a Web Tier on Linux below
Uninstall a Web Tier on Windows on the facing page

Uninstall a Web Tier on Linux

Run the RSA Authentication Web-Tier Uninstaller for Linux on the web-tier server.
Before you begin

- Confirm that you have root privileges.
- Verify that the open files hard limit for the local user is at least 4096.

Procedure

1. Log on to the web-tier server.
3. On the command line, type:
   ```
   ./uninstall.sh
   ```
4. Press ENTER.
5. On the Welcome screen, type:
   ```
   yes
   ```
6. Press ENTER.
   
   The system uninstalls the web tier and displays “Uninstall Complete” when finished.

Uninstall a Web Tier on Windows

Run the RSA Authentication Web-Tier Uninstaller for Windows on the web-tier server.

Before you begin

Confirm that you have Windows credentials to uninstall a program.

Procedure

1. On the web-tier server, go to `Start > Control Panel > Programs and Features > Uninstall a Program`.
2. Right-click `RSA Authentication Web Tier`, and select `Uninstall`.
3. On the command line, type:
   ```
   y
   ```
   and press ENTER.
   
   When finished, the uninstaller screen displays Uninstall finished.
4. Press ENTER.
   
   The system removes the web-tier services and installation folders, except the top-level folder.

Run the Web-Tier Installer for Your Platform

Obtain the Extras download kit for your version of RSA Authentication Manager from [https://my.rsa.com](https://my.rsa.com). On the web-tier server, run the RSA Authentication Manager Web-Tier Installer for your platform. For instructions, see the following:
- Install a Web Tier on Windows Using the Graphical User Interface on page 82.
- Install a Web Tier on Windows Using the Command Line on page 83.
- Install a Web Tier on Linux Using the Graphical User Interface on page 84.
- Install a Web Tier on Linux Using the Command Line on page 86.

**Update the Web Tier**

You must update the web tier when you make any changes such as updating your version of Authentication Manager and customizing the web-tier pages. Authentication Manager displays an update button in the Operations Console for each web tier that is not up-to-date. If you have multiple web tiers to update, update one web tier at a time. Each update can take up to 20 minutes to complete.

**Procedure**

1. In the Operations Console, click Deployment Configuration > Web-Tier Deployments > Manage Existing.

2. On the Web Tiers page, in the Status column, click Update for the web tier that you want to update.

   When the update is complete, the Status column for the updated web tier displays Online.
Appendix B: Upgrading to RSA Authentication Manager 8.3

Upgrading to RSA Authentication Manager 8.3 .............................................................. 104
Before Installing RSA Authentication Manager 8.3 ...................................................... 105
Installing Version 8.3 .................................................................................................. 106
Reinstall the Web Tier ................................................................................................. 110
Upgrading to RSA Authentication Manager 8.3

You can apply the RSA Authentication Manager 8.3 upgrade patch to any hardware appliance or virtual appliance that has RSA Authentication Manager 8.2 SP1 software.

**Note:** You must upgrade to RSA Authentication Manager 8.2 SP1 before applying version 8.3. For instructions, see the *RSA Authentication Manager 8.3 Setup and Configuration Guide* on RSA Link.

RSA Authentication Manager 8.3 includes the software fixes in the cumulative Patch 5 for version 8.2 SP1. Applying version 8.3 removes any software fixes that are not included in the cumulative Patch 5 for version 8.2 SP1, with the exception of any fixes from Patches 6 and 7 that are listed in the *RSA SecurID Access Release Notes for RSA Authentication Manager and the Cloud Authentication Service*. You must apply version 8.3 patches to obtain all of the fixes in Patches 6 and 7.

To apply version 8.3, perform these tasks in order:

1. Review the prerequisites. See Before Installing RSA Authentication Manager 8.3 on the facing page.

2. Follow the standard steps to apply an Authentication Manager update. See Installing Version 8.3 on page 106.

3. If your deployment includes a web tier, you reinstall it. See Reinstall the Web Tier on page 110.
**Before Installing RSA Authentication Manager 8.3**

Before installing this upgrade, review the following guidelines and requirements.

**Backup Strongly Recommended**

RSA Authentication Manager 8.3 is not reversible. If the upgrade patch is not applied successfully, you must restore from a backup file, a VMware snapshot, or a Hyper-V checkpoint. Trying to apply version 8.3 again is not recommended.

**Note:** RSA strongly recommends backing up your deployment, backing up a hardware appliance with PING, taking a VMware snapshot, or creating a Hyper-V checkpoint before applying version 8.3.

- If you deployed a hardware appliance or a virtual appliance, you can back up the version 8.2 Service Pack 1 (SP1) database. Use the Back Up Now feature in the Operations Console of the primary instance. See the Help topic “Create a Backup using Back Up Now.”

- If you deployed a hardware appliance, RSA recommends using standard system disk imaging software to create a backup image in case you need to restore the hardware appliance. RSA has qualified PING software. For more information, see “Using PING to Back Up and Restore the RSA Authentication Manager 8.2.x Hardware Appliance” on RSA Link: [https://community.rsa.com/docs/DOC-41697](https://community.rsa.com/docs/DOC-41697).

- If you deployed a VMware virtual appliance, you can take a snapshot of each virtual machine in the version 8.2 SP1 deployment. When you take a snapshot of an Authentication Manager instance, you must specify the following settings:
  - Do not save the virtual machine’s memory.
  - Choose to quiesce the guest file system. This option pauses running processes on the Authentication Manager instance.

  For additional instructions, see the VMware vSphere Client documentation.

- If you deployed a Hyper-V virtual appliance, you can create a checkpoint of the version 8.2 SP1 deployment. For additional instructions, see the Microsoft Hyper-V documentation.

You can restore version 8.2 SP1 if you took a VMware snapshot or a Hyper-V checkpoint before applying version 8.3. Export your data or take other steps to preserve your data before reverting to a snapshot or checkpoint. See the **RSA Authentication Manager Administrator’s Guide** for information about restoring snapshots and checkpoints.

You can restore version 8.2 SP1 if you backed up your deployment before applying version 8.3. See the Help topic “Restore from Backup.”

**Replicated Deployments**

If you have a replicated deployment, all replica instances must be running and replicating successfully before you apply version 8.3 or any other update or patch to the primary instance. To verify the replication status, log on to the primary instance Operations Console, and then click **Deployment Configuration > Instances > Status Report**.

Apply version 8.3 to the RSA Authentication Manager primary instance before upgrading the replica instances in your RSA Authentication Manager 8.2 SP1 deployment. On the primary instance, the replication status displays...
"Internal Replication Error" or another error until all replica instances have been upgraded or patched. The RADIUS server replication status also displays a replication status of "package failure" or another error until all replica instances have been upgraded or patched.

**Note:** You must successfully upgrade your primary instance before upgrading your replica instances.

**Additional Requirements**

Version 8.3 has the following additional requirements:

- Each virtual appliance must have at least 4 GB of free disk space to apply version 8.3.

- The following credentials are required for the upgrade:
  - Operating system password for the rsaadmin user account on each virtual appliance.
  - An Operations Console administrator account, with access to the Operations Console, for the primary instance and each replica instance.

**Installing Version 8.3**

The RSA Authentication Manager 8.3 ZIP file, **am-update-8.3.0.0.0.zip**, contains the RSA Authentication Manager 8.3 ISO file, **am-update-8.3.0.0.0.iso**, that is used to apply version 8.3 to Authentication Manager.

You can apply an update through your web browser, or you can store the service pack in an NFS share, a shared folder on Windows, a DVD/CD, or an ISO image on your local machine.

The overall steps to install this service pack are as follows:

- Specify a Product Update Location
- Scan for Updates
- Apply the Product Update

**Specify a Product Update Location**

To specify a product update location, or to edit a previously specified location, perform the following procedure to allow RSA Authentication Manager 8.2 SP1 to locate the RSA Authentication Manager 8.3 ISO file.

If you have already specified a location, see **Scan for Updates**.

**Before you begin**

- Download the version 8.3 update from RSA Link to a location that the primary or replica instance can access.

- If you intend to scan for updates on an RSA-supplied DVD or CD, do the following:
  - On a hardware appliance, use the DVD/CD drive or mount an ISO image.
  - On a virtual appliance, you must configure the virtual appliance to mount a DVD/CD or an ISO image. See the Help topic "VMWare DVD/CD or ISO Image Mounting Guidelines" or "Hyper-V DVD/CD or ISO Image Mounting Guidelines."
Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.

2. On the Update & Rollback page, your local browser is configured as the method for applying an update. To change that setting, click **Configure Update Source**.

3. On the Configure Update Sources page, specify a location for updates.
   - To upload the update from your local machine, select **Use your web browser to upload an update**.
   - To scan for updates on an NFS share, select **Use NFS as the update source**. Enter the full path, including the IP address or hostname where updates are stored. For example: 192.168.1.2:/updates
   - To scan for updates on a Windows shared folder, select **Use Windows Share** as the update source.
     - In the **Windows Share Path** field, enter the full path, including the IP address or hostname where updates are stored. For example: \192.168.1.2\updates
     - (Optional) In the **Windows Username** field, enter a username. If your Windows share configuration requires it, enter the domain and username.
     - (Optional) In the **Windows Password** field, enter a password only if it is required by your Windows share configuration.
   - To scan for updates on a DVD or CD, select **Use DVD/CD as the update source**.

4. To test the NFS or Windows share directory settings, click **Test Connection**. A message indicates whether the configured shared directory is available to the primary or replica instance.

5. Click **Save**.

**After you finish**

Do one of the following:

- If you configured your local web browser as the method to apply an update, see **Apply the Product Update**.
- If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, see **Scan for Updates**.

**Scan for Updates**

If you configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, you can scan to locate and review a list of available product updates.

**Procedure**

1. In the Operations Console, click **Maintenance > Update & Rollback**.

2. Click **Scan for Updates**. You can view the progress of the scan on the **Basic Status View** tab. You can
view more detailed information on the Advanced Status View tab.

3. Click Done to return to the Update & Rollback page.

The Available Updates section displays a list of updates, with the following information for each update:

- **Version.** The version of the update. To see the current Authentication Manager version, see the top of the Update and Rollback page.

- **Reversible.** Indicates whether you can roll back (undo) the update. Service pack 1 is not reversible.

- **Automatic Appliance Reboot.** Indicates whether Authentication Manager automatically restarts the Appliance to apply the update. If the Appliance restarts, you must perform another scan to see a current list of updates.

- **Automatic Operations Console Reboot.** Indicates whether Authentication Manager automatically restarts the Operations Console to apply the update. If the Operations Console restarts, you must perform another scan to see a current list of updates.

- **Action.** States whether the update is available to apply. Lists the minimum system requirement for the update.

4. In the Applied Updates section, click Download Detailed History Log for a complete update history.

The Applied Updates section displays the updates applied to the instance. This section includes the update version numbers, the time and date that each update was applied, and which administrator applied the update.

After you scan for updates, the new list displays for 24 hours. Logging out of the Operations Console does not remove the list from the system cache. If you restart the Operations Console, download additional updates, or change the product update locations, you must perform another scan to see the most current list.

**After you finish**

Apply the version 8.3 upgrade patch to the RSA Authentication Manager deployment. See Apply the Product Update below.

**Apply the Product Update**

Apply the product update to the primary instance first, and then to each replica instance. As each replica instance is updated, all of the accumulated data on each replica instance is sent to the primary instance.

**Note:** You must successfully upgrade your primary instance before upgrading your replica instances.

**Before you begin**

- Ensure that port 8443/TCP is open for https traffic.

  Access to this port is required for real-time status messages when applying RSA Authentication Manager patches and service packs.
During a product update, the appliance opens this port in its internal firewall. The appliance closes this port when the update is complete.

If an external firewall blocks this port, the browser displays an inaccessible or blank web page, but the update can successfully complete.

- **Specify a Product Update Location**

  - If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, Scan for Updates.

- In a replicated deployment, all replica instances must be running and replicating successfully before you apply version 8.3 or any other update or patch to the primary instance. To verify the replication status, log on to the primary instance Operations Console, and then click **Deployment Configuration > Instances > Status Report**.

  After upgrading the primary instance, the Authentication Manager replication status displays "Internal Replication Error" or another error until all replica instances have been upgraded or patched. The RADIUS server replication status also displays a replication status of "package failure" or another error until all replica instances have been upgraded or patched.

### Procedure

1. In the Operations Console, click **Maintenance > Update & Rollback**.

2. RSA recommends applying the most recent update. Do one of the following, depending on your configuration:
   - To apply an update through your local web browser, do the following:
     a. Click **Upload & Apply Update**.
     b. Click **Browse** to navigate to the location of the update. You cannot type the update location in the **Update Path** field.
     c. Click **Upload**.
     d. Verify the update details, and click **Apply**.
   - If you have configured an NFS share, a Windows shared directory, or a DVD/CD as an update location, do the following:
     a. Click **Scan for Updates. Available Updates** displays all of the updates that can be applied.
     b. Next to the update to apply, click **Apply Update**.
     c. Click **Confirm** to apply the update.

3. In the **Password** field, enter the password for the operating system user **rsaadmin**, and click **Log On**.

4. The basic status messages appear while the update is applied. You can view more detailed information on the **Advanced Status View** tab.
Note: If the browser displays an inaccessible or blank web page, then port 8443/TCP might be blocked by an external firewall. Real-time status messages are not available. Wait for the update to complete.

After the upgrade is applied, the following occurs:

- The appliance automatically restarts. When the restart is complete, click Done.
- Authentication Manager moves the update from the Available Updates section to the Applied Updates section.
- When you return to the Update & Rollback page, the update is listed in the Applied Updates section. To save the high-level update history, click Download Detailed History Log.
- The software version information is updated. To view the software version information, log on to the Security Console, and click Software Version Information.

After you finish

- You can download a detailed log file containing the information that was displayed on the Advanced Status View tab. The file is named update-version-timestamp.log, where version is the update version number and timestamp is the time that the update completed. For instructions, see the Help topic “Download Troubleshooting Files.”
- After you have upgraded the primary instance and all of the replica instances, do the following:
  - Verify that replication and radius replication is functioning correctly on the primary instance and the replica instance.
  - Version 8.3 includes the software fixes in the cumulative Patch 5 for version 8.2 SP1. As needed, obtain later software fixes by applying the latest version 8.3 cumulative patches to the upgraded Authentication Manager instances.
- If the deployment includes a web tier, you must reinstall it. For instructions, see Reinstall the Web Tier below.

Reinstall the Web Tier

If your deployment includes a web tier, after upgrading the primary and replica instances, you must upgrade the web tier. Follow these procedures to retain all existing web-tier configuration and customization settings:

1. Uninstall the Web Tier below
2. Run the Web-Tier Installer for Your Platform on page 112
3. Update the Web Tier on page 112

Uninstall the Web Tier

Uninstalling a web tier removes the web tier and all features and components of RSA Authentication Manager from the web-tier server. Uninstalling a web tier does not delete the web-tier deployment record.

For instructions, see the following:

Uninstall a Web Tier on Linux on the facing page
Uninstall a Web Tier on Windows below

Uninstall a Web Tier on Linux

Run the RSA Authentication Web-Tier Uninstaller for Linux on the web-tier server.

Before you begin

- Confirm that you have root privileges.
- Verify that the open files hard limit for the local user is at least 4096.

Procedure

1. Log on to the web-tier server.
3. On the command line, type:
   
   ```
   ./uninstall.sh
   ```
4. Press ENTER.
5. On the Welcome screen, type:
   
   ```
   yes
   ```
6. Press ENTER.

   The system uninstalls the web tier and displays "Uninstall Complete" when finished.

Uninstall a Web Tier on Windows

Run the RSA Authentication Web-Tier Uninstaller for Windows on the web-tier server.

Before you begin

Confirm that you have Windows credentials to uninstall a program.

Procedure

1. On the web-tier server, go to **Start > Control Panel > Programs and Features > Uninstall a Program**.
2. Right-click **RSA Authentication Web Tier**, and select **Uninstall**.
3. On the command line, type:
   
   ```
   y
   ```
   and press ENTER.

   When finished, the uninstaller screen displays Uninstall finished.
4. Press ENTER.

   The system removes the web-tier services and installation folders, except the top-level folder.
Run the Web-Tier Installer for Your Platform

Obtain the Extras download kit for your version of RSA Authentication Manager from https://my.rsa.com. On the web-tier server, run the RSA Authentication Manager Web-Tier Installer for your platform. For instructions, see the following:

- Install a Web Tier on Windows Using the Graphical User Interface on page 82.
- Install a Web Tier on Windows Using the Command Line on page 83.
- Install a Web Tier on Linux Using the Graphical User Interface on page 84.
- Install a Web Tier on Linux Using the Command Line on page 86.

Update the Web Tier

You must update the web tier when you make any changes such as updating your version of Authentication Manager and customizing the web-tier pages. Authentication Manager displays an update button in the Operations Console for each web tier that is not up-to-date. If you have multiple web tiers to update, update one web tier at a time. Each update can take up to 20 minutes to complete.

Procedure

1. In the Operations Console, click Deployment Configuration > Web-Tier Deployments > Manage Existing.
2. On the Web Tiers page, in the Status column, click Update for the web tier that you want to update.
   When the update is complete, the Status column for the updated web tier displays Online.
Appendix C: Port Usage

Port Traffic .................................................................................................................................114
Ports for the RSA Authentication Manager Instance ...............................................................114
Ports on the Web Tier with a Load Balancer Deployed ............................................................119
Ports on the Web Tier Without a Load Balancer ....................................................................119
Access Through Firewalls ........................................................................................................120
Port Traffic

The following figure represents a common RSA Authentication Manager deployment with primary and replica instances, web tiers, and a load balancer. An external firewall protects the primary and replica instances, and another external firewall protects the DMZ. For more information on RADIUS ports, see Ports for the RSA Authentication Manager Instance below.

Ports for the RSA Authentication Manager Instance

The RSA Authentication Manager instance has an internal firewall that limits traffic to specific ports. The internal firewall restricts inbound traffic to the hosts and services that provide product functionality. Outbound traffic is not restricted. RSA recommends that you deploy the instance in a subnet that also has an external firewall to segregate it from the rest of the network.

The following table lists ports used by the Authentication Manager instance. Note the following:

- These ports are configured to be able to accept network traffic from remote systems. You should configure these ports for access on your local network.
- Authentication Manager uses other, internal network connections for communication between processes. Remote access to these ports is blocked by the internal firewall configured on the appliance.
- When blocking external access to ports on web-tier servers, do not block connections and traffic from services on the same system. For example, you can use a firewall to block external access to ports 7030, TCP, and 7036, TCP, but you must allow connections on the external NIC if the connections are from the same web-tier server.
- All ports support IPv4 only, unless IPv6 support is specified in the description.
<table>
<thead>
<tr>
<th>Port Number and Protocol</th>
<th>Function</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22, TCP</td>
<td>Secure Shell (SSH)</td>
<td>SSH client</td>
<td>Disabled by default. SSH can be enabled in the Operations Console. SSH allows the operating system account (rsaadmin) to access the operating system.</td>
</tr>
<tr>
<td>49, TCP</td>
<td>TACACS authentication</td>
<td>TACACS client</td>
<td>This port is closed unless TACACS is configured. Used to receive authentication requests from a Network Access Device (NAD).</td>
</tr>
<tr>
<td>80, TCP</td>
<td>Quick Setup Operations Console, Security Console</td>
<td>Administrator’s browser</td>
<td>Used for Quick Setup. After Quick Setup is complete, the appliance redirects connections from this port to the appropriate console.</td>
</tr>
<tr>
<td>161, UDP</td>
<td>SNMP</td>
<td>SNMP client</td>
<td>Used by the Authentication Manager SNMP agent to listen for GET requests and send responses to a Network Management System (NMS). This port is closed, unless SNMP is enabled. It can be configured in the Security Console.</td>
</tr>
<tr>
<td>443, TCP</td>
<td>Quick Setup Operations Console, Security Console, Self-Service Console</td>
<td>Administrator’s browser</td>
<td>Used for Quick Setup. After Quick Setup is complete, the appliance redirects connections from this port to the appropriate console.</td>
</tr>
<tr>
<td>1645, UDP</td>
<td>RADIUS authentication (legacy port)</td>
<td>RADIUS client</td>
<td>This port receives authentication requests from a RADIUS client. For more information, see Required RSA RADIUS Server Listening Ports on page 118.</td>
</tr>
<tr>
<td>1646, UDP</td>
<td>RADIUS accounting (legacy port)</td>
<td>RADIUS client</td>
<td>This port receives inbound accounting requests from a RADIUS client. For more information, see Required RSA RADIUS Server Listening Ports on page 118.</td>
</tr>
<tr>
<td>1812, TCP</td>
<td>RADIUS replication port</td>
<td>Another RADIUS server</td>
<td>This port is used for communication between primary RADIUS and replica RADIUS services. If you do not use RSA RADIUS, but you have replica instances, you must allow</td>
</tr>
<tr>
<td>Port Number and Protocol</td>
<td>Function</td>
<td>Source</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------</td>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>connections between Authentication Manager instances on this port. You should restrict connections from other systems that are not Authentication Manager instances. For more information, see Required RSA RADIUS Server Listening Ports on page 118.</td>
</tr>
<tr>
<td>1812, UDP</td>
<td>RADIUS authentication</td>
<td>RADIUS client</td>
<td>This port receives authentication requests from a RADIUS client. If you do not plan to use RSA RADIUS authentication, you can close this port.</td>
</tr>
<tr>
<td>1813, TCP</td>
<td>RADIUS administration</td>
<td>RADIUS server</td>
<td>This port is used to administer RADIUS from the Security Console over the protected RADIUS remote administration channel. If you do not use RSA RADIUS, but you have replica instances, you must allow connections between Authentication Manager instances on this port. You should restrict connections from other systems that are not Authentication Manager instances. For more information, see Required RSA RADIUS Server Listening Ports on page 118.</td>
</tr>
<tr>
<td>1813, UDP</td>
<td>RADIUS accounting</td>
<td>RADIUS client</td>
<td>This port receives accounting requests from a RADIUS client. If you do not plan to use RSA RADIUS authentication, you can close this port.</td>
</tr>
<tr>
<td>5500, TCP</td>
<td>Agent authentication</td>
<td>RSA SecurID Authentication protocol agents</td>
<td>Accepts requests from TCP-based authentication agents and sends replies. Required for RSA SecurID and on-demand authentication (ODA). This port supports both IPv4- and IPv6-compliant agents.</td>
</tr>
<tr>
<td>5500, UDP</td>
<td>Agent authentication</td>
<td>RSA SecurID Authentication protocol agents</td>
<td>Accepts requests from UDP-based authentication agents and sends replies. Required for RSA SecurID, ODA and risk-based authentication (RBA). This port only supports IPv4-compliant agents.</td>
</tr>
<tr>
<td>5550, TCP</td>
<td>Agent auto-registration</td>
<td>RSA agents</td>
<td>Used for communication with authentication agents that are attempting to register with Authentication Manager.</td>
</tr>
<tr>
<td>5555, TCP</td>
<td>Agent authentication</td>
<td>RSA SecurID Authentication API agents</td>
<td>Accepts requests from REST-based authentication agents and sends replies.</td>
</tr>
<tr>
<td>Port Number and Protocol</td>
<td>Function</td>
<td>Source</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>5580, TCP</td>
<td>Offline authentication service</td>
<td>RSA agents</td>
<td>Required for RSA SecurID and on-demand authentication (ODA). This port supports both IPv4- and IPv6-compliant agents. Used to receive requests for additional offline authentication data, and send the offline data to agents. Also used to update server lists on agents. This can be closed if offline authentications are not in use and no agents in your deployment use the Login Password Integration API.</td>
</tr>
<tr>
<td>7002, TCP SSL-encrypted</td>
<td>Authentication Manager</td>
<td>Another appliance</td>
<td>Used for communication between an Authentication Manager primary and replica instances and for communication between replica instances (for replay detection). Used by the RSA application programming interface (API). Enable if you have at least one replica instance.</td>
</tr>
<tr>
<td>7002, TCP SSL-encrypted</td>
<td>RSA Token Management snap-in for the Microsoft Management Console (MMC)</td>
<td>Microsoft Management Console</td>
<td>Enable this port if you plan to use the RSA Token Management snap-In to manage users and authenticators from MMC.</td>
</tr>
<tr>
<td>7004, TCP SSL-encrypted</td>
<td>Self-Service Console and RBA</td>
<td>User’s browser</td>
<td>Required for using the Self-Service Console or RBA. Accepts requests for Self-Service Console functions and RBA authentication.</td>
</tr>
<tr>
<td>7004, TCP SSL-encrypted</td>
<td>Cryptographic Token-Key Initialization Protocol (CT-KIP)</td>
<td>User’s browser</td>
<td>Required for using dynamic seed provisioning.</td>
</tr>
<tr>
<td>7022, TCP SSL-encrypted</td>
<td>Authentication Manager, trusted realm</td>
<td>Another appliance, trusted realm, or the web tier and another appliance</td>
<td>Used for communication between Authentication Manager primary and replica instances and for communication</td>
</tr>
<tr>
<td>Port Number and Protocol</td>
<td>Function</td>
<td>Source</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>network access point, RBA, or the web tier</td>
<td></td>
<td>between replica instances (for replay detection). Used to communicate with trusted realms and for RBA. Allows communication between the appliance and its web tier.</td>
</tr>
<tr>
<td>7072, TCP SSL-encrypted</td>
<td>Operations Console</td>
<td>Super Admin’s browser</td>
<td>Required for administering your deployment from the Operations Console. Accepts requests for Operations Console functions.</td>
</tr>
<tr>
<td>7082, TCP SSL-encrypted</td>
<td>RADIUS Configuration SSL</td>
<td>Authentication Manager instance</td>
<td>Used for configuring RADIUS and restarting the RADIUS service from the Operations Console.</td>
</tr>
<tr>
<td>8443, TCP SSL-encrypted</td>
<td>Authentication Manager patches and service packs</td>
<td>Administrator’s browser</td>
<td>Access to this port is required for real-time status messages when applying Authentication Manager patches and service packs. During a product update, the appliance opens this port in its internal firewall. The appliance closes this port when the update is complete. If an external firewall blocks this port, the browser displays an inaccessible or blank web page, but the update can successfully complete.</td>
</tr>
</tbody>
</table>

**Restricting Access to the RSA Consoles**

Access to the Security Console (port 7004) and the Operations Console (port 7072) should be restricted to internal administrators only. While port 7004 is used by the Security Console, dynamic seed provisioning, and the Self-Service Console, it should not be directly accessible outside the intranet. To allow access to the Self-Service Console or dynamic seed provisioning for external users, set up a web tier to help protect port 7004 and restrict access to the Security Console.

**Required RSA RADIUS Server Listening Ports**

RSA RADIUS is installed and configured with RSA Authentication Manager. All the RADIUS-related ports (1645, 1646, 1812, 1813, and 7082) on the Authentication Manager server are open by default.

The RADIUS standard initially used UDP ports 1645 and 1646 for RADIUS authentication and accounting packets. The RADIUS standards group later changed the port assignments to 1812 and 1813. The Authentication Manager RADIUS server listens on all four ports for backward compatibility. If all the RADIUS clients are configured to talk to the RADIUS servers only on ports 1812 and 1813, you should block legacy ports 1645 and 1646 on the external firewall.

Whether or not you use RSA RADIUS, if you have replica instances in your deployment, you must allow connections between Authentication Manager instances on TCP ports 1812 and 1813. These ports are required.
for tasks such as replica attachment, replica promotion, and IP address and hostname changes. You should restrict connections from other systems that are not Authentication Manager instances. For example, use your external firewall to block access or use additional layers of network protection to block unauthorized internal users.

If you do not plan to use RADIUS, you can close the RADIUS authentication UDP ports 1645 and 1812.

### Ports on the Web Tier with a Load Balancer Deployed

The following table lists the default listening ports on the web-tier server when a load balancer is installed in a deployment.

If your environment has firewalls or proxy servers, make sure that they allow communication between the web tier and all other hosts and services that provide Authentication Manager functionality. These hosts and services, which are listed in the Source column, include Authentication Manager appliances, load balancers, and browsers.

<table>
<thead>
<tr>
<th>Port Number and Protocol</th>
<th>Function</th>
<th>Source</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443, TCP</td>
<td>Self-Service Console, risk-based authentication (RBA), and dynamic seed provisioning</td>
<td>User's browser</td>
<td>Primary web-tier hostname</td>
<td>Accepts requests for Self-Service Console functions, RBA authentication, and dynamic seed provisioning.</td>
</tr>
<tr>
<td>443, TCP</td>
<td>RBA</td>
<td>Load balancer</td>
<td>Web-tier virtual hostname</td>
<td>Accepts requests for RBA authentication that use the virtual hostname.</td>
</tr>
</tbody>
</table>

### Ports on the Web Tier Without a Load Balancer

The following table lists the default listening ports on the web-tier server when a load balancer is not used in your deployment.

If your environment has firewalls or proxy servers, make sure that they allow communication between the web tier and all other hosts and services that provide Authentication Manager functionality. These hosts and services, which are listed in the Source column, include Authentication Manager appliances, load balancers, and browsers.

<table>
<thead>
<tr>
<th>Port Number and Protocol</th>
<th>Function</th>
<th>Source</th>
<th>Destination</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>443, TCP</td>
<td>Self-Service Console, risk-based authentication (RBA), and dynamic seed provisioning</td>
<td>User’s browser</td>
<td>Primary web-tier hostname</td>
<td>Accepts requests for Self-Service Console functions, RBA authentication, and dynamic seed provisioning.</td>
</tr>
<tr>
<td>443, TCP</td>
<td>RBA</td>
<td>User’s browser</td>
<td>Web-tier virtual hostname</td>
<td>Accepts requests for RBA authentication.</td>
</tr>
</tbody>
</table>
**Note:** Keep port 443 (or another port number if you change the default) open on the replica web tier, so that a listening port is available.

## Access Through Firewalls

RSA recommends that you set up all RSA Authentication Manager instances in a subnet that has an external firewall to segregate it from the rest of the network. To enable authentication through external firewalls and to accommodate static Network Address Translation (NAT), you can configure alias IP addresses for Authentication Manager instances and alternate IP addresses for authentication agents. You can assign the following:

- Four distinct IP addresses (the original IP address and up to three aliases) to each Authentication Manager instance. For instructions, see the Help topic “Add Alternative IP Addresses for Instances.”

- An unlimited number of alternate IP addresses (one primary IP address) to your agents. For instructions, see the Help topic “Add an Authentication Agent.”

Each distinct IP address must be assigned to only one Authentication Manager instance. Authentication Manager instances must not share an IP address, even if it is hidden by NAT.

You must know the primary IP address and aliases for each Authentication Manager instance. If your deployment includes multiple locations, you must also know which ports are used for Authentication Manager communications and processes. You may need to open new ports in your firewall, or clear some existing ports for your deployment. Port translation is supported if the primary and replica instances are communicating on the standard Authentication Manager ports. For example, the primary and replica instances must communicate on port 7002, TCP. For more information on ports, see Port Traffic on page 114.

## Securing Connections Between the Primary and Replica Instances

Authentication Manager uses port 7002 to replicate data between the primary and replica instance databases. To secure this channel from unauthorized use, RSA recommends the following:

- If your deployment does not include a replica, or if your primary and replica instances are on the same LAN, close port 7002 on your external firewall (not the appliance firewall) so that it does not pass external traffic to the primary or replica instances.

- If your primary and replica instances are connected through a WAN and there is a firewall between them, open port 7002 on the firewall, but restrict traffic on this port to originate only from the IP addresses of the primary and replica instances.
Appendix D: Administrative Accounts

System Administrator Accounts ........................................................................................................ 122
Manage a Super Admin Account ..................................................................................................... 123
System Administrator Accounts

The following accounts provide permission to modify, maintain, and repair the Authentication Manager deployment. Quick Setup creates these accounts with information that you enter. If you plan to record the logon credentials for these accounts, be sure that the storage method and location are secure.

Authentication Manager Administrator Accounts

The following table lists the administrator accounts for Authentication Manager. The administrator who deploys the primary instance creates these accounts during Quick Setup.

<table>
<thead>
<tr>
<th>Name</th>
<th>Permissions</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Admin</td>
<td>Super Admins can perform all administrative tasks in the Security Console with full administrative permission in all security domains in the deployment.</td>
<td>Any Super Admin can create other Super Admin users in the Security Console. The Super Admin also creates the security domain hierarchy, and links identity sources to the deployment. An Operations Console administrator can recover a Super Admin account if no Super Admin can access the system.</td>
</tr>
<tr>
<td>Operations Console administrator</td>
<td>Operations Console administrators can perform administrative tasks in the Operations Console. Operations Console administrators also use command line utilities to perform some procedures, such as recovering the Super Admin account. Command line utilities require the appliance operating system account password. Some tasks in the Operations Console also require Super Admin credentials. Only Super Admins whose records are stored in the internal database are accepted by the Operations Console.</td>
<td>Any Super Admin can create and manage Operations Console administrators in the Security Console. For example, you cannot recover a lost Operations Console administrator password, but a Super Admin can create a new one. Operations Console administrator accounts are stored outside of the Authentication Manager internal database. This ensures that if the database becomes unreachable, an Operations Console administrator can still access the Operations Console and command line utilities.</td>
</tr>
</tbody>
</table>

User IDs for a Super Admin and a non-administrative user are validated in the same way. A valid User ID must be a unique identifier that uses 1 to 255 ASCII characters.

A valid User ID for an Operations Console administrator must be a unique identifier that uses 1 to 255 ASCII characters. The characters @ ~ are not allowed, and spaces are not allowed.

RSA recommends the following best practices for administrative accounts:

- Create a separate administrative account for each administrator, for example, create a separate Operations Console administrator account for each Operations Console user. Do not share account information, especially passwords, among multiple administrators.
- RSA does not recommend associating administrative roles with external LDAP or Active Directory user accounts. Use separate administrative accounts with their own credentials for external identity source administrators and Authentication Manager administrators.
If you have multiple administrators, restrict the scope and permissions of Authentication Manager administrative accounts, and restrict access by dividing your deployment into security domains. Separation of privileges is especially important if you are using LDAP or Active Directory users as administrators.

- If administrative roles in Authentication Manager are associated with an external LDAP account, a specific role, with appropriate limiting controls, should be used. For instructions, see the Help topic Administrative Role Scope and Permissions on RSA Link.

## Appliance Operating System Account

The appliance operating system account User ID is **rsaadmin**. This User ID cannot be changed. You specify the operating system account password during Quick Setup. You use this account to access the operating system when you perform advanced maintenance or troubleshooting tasks. The **rsaadmin** account is a privileged account to which access should be strictly limited and audited. Individuals who know the **rsaadmin** password and who are logged on as **rsaadmin** have sudo privileges and shell access.

Every appliance also has a root user account. This account is not needed for normal tasks. You cannot use this account to log on to the appliance.

You can access the operating system with Secure Shell (SSH) on a hardware appliance or a virtual appliance. Before you can access the appliance operating system through SSH, you must use the Operations Console to enable SSH on the appliance.

On a VMware virtual appliance, you can also access the appliance operating system with the VMware vSphere Client. On a Hyper-V virtual appliance, you can also access the appliance operating system with the Hyper-V System Center Virtual Machine Manager Console or the Hyper-V Manager.

An Operations Console administrator can change the operating system account password, **rsaadmin**, in the Operations Console.

RSA does not provide a utility to recover the operating system password.

## Manage a Super Admin Account

Only a Super Admin can manage a Super Admin account.

**Procedure**

1. In the Security Console, click **Identity > Users > Manage Existing**.
2. Use the search fields to find the user that you want to edit.
3. Click the user that you want to edit and select **Edit**.
4. Update the user settings.
5. Click **Save**.
## Appendix E: Installing the RSA Authentication Manager Token Management Snap-In

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>126</td>
</tr>
<tr>
<td>System Requirements</td>
<td>126</td>
</tr>
<tr>
<td>Install the Token Management Snap-In for Local Access</td>
<td>126</td>
</tr>
<tr>
<td>Install the Token Management Snap-In for Remote Access</td>
<td>127</td>
</tr>
<tr>
<td>Performing Post-Installation Tasks</td>
<td>129</td>
</tr>
</tbody>
</table>
Overview

The RSA Token Management snap-in provides a convenient way to manage RSA SecurID tokens for deployments that have an Active Directory identity source. The RSA Token Management snap-in extends the context menus, property pages, control bars, and toolbars in the Active Directory Users and Computers snap-in for the Microsoft Management Console (MMC). You can use the RSA Token Management snap-in to enable or disable a token, assign a token, or perform other token-related tasks without logging on to the Security Console. For more information on the administrative actions enabled by this extension, see the RSA Token Management Snap-In for the Microsoft Management Console Help.

System Requirements

You can install the RSA Token Management Snap-In on the following platforms:

- Windows Server 2012 R2 Domain Controller
- Windows Server 2012 R2 with the Active Directory Domain Services (AD DS) Snap-Ins and Command Line Tools
- Windows Server 2008 R2 Domain Controller
- Windows Server 2008 R2 Server with the Active Directory Domain Services (AD DS) Snap-Ins and Command Line Tools
- Windows Server 2008 Server with the Active Directory Domain Services Snap-Ins and Command Line Tools
- Windows 7 with the with the Active Directory Domain Services Snap-Ins and Command Line Tools

**Note:** The RSA Token Management snap-in does not support Microsoft Active Directory Lightweight Directory Services.

Windows Server 2012 R2 Active Directory includes the required .NET FrameWork 4.5 installation. For all other supported platforms, you must install .NET 4.5 before installing the RSA Token Management Snap-In.

Install the Token Management Snap-In for Local Access

Use this procedure if you want to administer the Authentication Manager through the Token Management Snap-In directly on the host where Active Directory is installed.

**Before you begin**

You must have the administrative permissions. These permissions (for example, domain level) depend on your Windows network configuration. At minimum, you must be a domain administrator and a local machine administrator.

Microsoft .NET 4.5 must be installed on the system where you update the Token Management Snap-In.
Procedure

1. Obtain the RSA Token Management Snap-In installation files. The files are in the RSA Authentication Manager 8.4 – Token Management Snap-In for MMC.zip file that you can download from RSA Link.

2. Unzip all of the installation files into a directory that is located on the same machine where you are installing the snap-in.

3. Do one of the following:
   - If you have a 32-bit operating system, run setup32.exe.
   - If you have a 64-bit operating system, run setup64.exe.

   **Note:** The installer also installs the Visual C++ redistributable package if it is not already present.

4. Respond to the prompts for Welcome, Select Region, and License Agreement.

5. For Authentication Manager server settings, enter values for the following:
   - Authentication Manager server hostname
   - Authentication Manager server port number
   - Command Server Port

6. When prompted for Destination Location, either accept the default location or enter an alternative location.

7. Review the Pre-installation screen, and click Next to continue.

8. Click Finish.

Install the Token Management Snap-In for Remote Access

Use this procedure if you want to administer the Authentication Manager through the Token Management Snap-In remotely from Windows 7 or a Windows Server 2008 or 2012 R2 without Active Directory.


For Windows 7, you can perform remote administration using the Remote Server Administration Tools. This tools package must be downloaded and installed separately, and can be installed only on Windows 7 (32-bit and 64-bit).

On Windows 2008 and Windows Server 2012 R2, the Remote Server Administration Tools feature is part of the operating system and can be added from the Server Manager.

You can enable the AD DS Snap-Ins and Command Line Tools after installing the Remote Server Administration Tools.
Before you begin

- For Windows 7, download and install the Remote Server Administration Tools package from the Microsoft web site.
- You must have the appropriate permissions. These permissions (for example, domain level) depend on your Windows network configuration. At minimum, you must be a domain administrator and a local machine administrator.
- The administrator using the AD DS Snap-In and Command Line Tools to remotely administer the Active Directory must have appropriate administrative permissions. These permissions (for example, domain level) depend on your Windows network configuration.

Procedure

2. Obtain the RSA Token Management Snap-In installation files. The files are in the RSA Authentication Manager 8.4 – Token Management Snap-In for MMC.zip file that you can download from RSA Link.
3. Unzip all of the installation files into a directory that is located on the same machine where you are installing the snap-in.
4. Do one of the following:
   - If you have a 32-bit operating system, run setup32.exe.
   - If you have a 64-bit operating system, run setup64.exe.
5. Respond to the prompts for Welcome, Select Region, and License Agreement.
6. For Authentication Manager server settings, enter values for the following:
   - Authentication Manager server hostname
   - Authentication Manager server port number
   - Authentication Manager Command Server Port
7. When prompted for Destination Location, either accept the default location or enter an alternative location.
8. Review the Pre-installation screen, and click Next to continue.
9. Click Finish.
Performing Post-Installation Tasks

After a successful installation, perform the following tasks to complete the MMC Extension setup.

Procedure

1. Make sure that the Authentication Manager is set up and running.

2. Make sure that Active Directory is configured and registered as an identity source. For more information see the Help topic "Identity Sources."

3. Start the Active Directory User and Computer Management Console below to open the RSA Token Management Snap-In.

4. Configure the Connection with Authentication Manager below

5. Make sure that the Windows user for the Token Management Snap-In is a valid Active Directory administrator and a valid Authentication Manager administrative user. For more information on administrator and administrative permissions, see System Administrator Accounts on page 122.

Start the Active Directory User and Computer Management Console

To use the Token Management Snap-In for Authentication Manager administration, you must start the Active Directory User and Computer Management Console.

Before you begin

Perform all of the preceding steps in Performing Post-Installation Tasks above.

Procedure

Do one of the following:

- Click Control Panel > Administrative Tools > Active Directory Users and Computers.
- From a command prompt, run dsa.msc.

Configure the Connection with Authentication Manager

You must specify connection settings such as server information and authentication information to enable the Token Management snap-in to access Authentication Manager Server.

Before you begin

Perform all of the preceding steps in Performing Post-Installation Tasks above

Procedure

1. Access the Active Directory Users and Computers Management Console.

2. Click on any user. This makes the RSA button visible in the toolbar.

3. Click RSA in the toolbar.

   The RSA Token Management Setting page is displayed.
4. In the **Server Information** section, do the following:
   
a. In the **AM Server Host** field, enter the name of the machine on which RSA Authentication Manager is running.

   b. In the **AM Server Port** field, enter the port number on which RSA Authentication Manager is running.

   c. In the **Command Server Port** field, enter the port number on which the Command Server is running on the Authentication Manager Server.

5. In the **Authentication Information** section, do the following:
   
a. Select the **UserID type** for the user.

      The format of the username displayed in the **Login User** field will be based on the chosen UserID type.

      **Note:** The UserID type must be the same as that defined for this identity source in the Authentication Manager.
      This user must be a member of the Domain Administrators group in Active Directory and must be assigned Super Admin privileges in Authentication Manager.

   b. In the **User Password** field, enter the user’s password.

   c. Click **Test Authentication** to perform a test authentication.

      If the UserID exists in more than one identity source, you can choose the identity source to test. The chosen identity source will be displayed in the **Identity Source Name** field. When prompted to use the certificate for future communication, click yes.