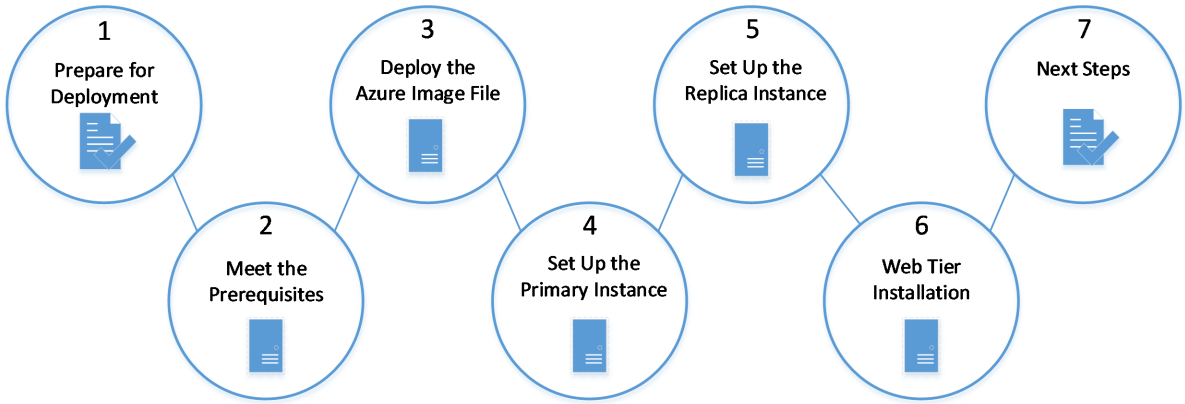
RSA® Authentication Manager 8.5

Microsoft Azure Virtual Appliance Getting Started

Thank you for purchasing RSA® Authentication Manager 8.5. This document provides an overview of how to deploy Authentication Manager on the Microsoft Azure virtual appliance.



Step 1: Prepare for Deployment

A: Download the License File

Download the license file (.zip) from https://my.rsa.com. Do not unzip the file.

Note: RSA recommends that you store the license file in a protected location that is available only to authorized administrative personnel.

B: Plan Your Deployment

See the documentation on RSA Link at https://community.rsa.com/community/products/securid/authentication-manager.

Read the *Release Notes*.

Read the *Planning Guide* for deployment considerations. For example, if users outside of your network require access to resources, you might want to deploy a web tier.

Step 2: Meet the Prerequisites for Deploying the RSA Authentication Manager Azure Image File

You must meet the following requirements for deploying the RSA Authentication Manager Azure Image file.

Configuration

Before configuring Azure, do the following:

- 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.

  For more information on Azure virtual networks, https://docs.microsoft.com/en-us/azure/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. The IPv6 protocol is not supported for the Authentication Manager virtual appliance on Azure.

    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.

DNS Server Configuration

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/.

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:

Port	Protocol	Purpose
22	TCP	Secure Shell (SSH)
49	TCP	TACACS authentication. Required for the TACACS client.
80	TCP	Quick Setup, Operations Console, Security Console
161	UDP	SNMP

443	TCP	Quick Setup, Operations Console, Security Console, Self-Service Console
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. If RADIUS clients only communicate to the RADIUS servers on port 1812, you can block the legacy RADIUS UDP port 1645.		
1645	UDP	RADIUS authentication (legacy port)
1646	UDP	RADIUS accounting (legacy port)
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.		
1812	TCP	RADIUS replication port
1813	TCP	RADIUS administration
If you do not plan to use RSA RADIUS, you can close the UDP ports 1812 and 1813. If you do not plan to use RSA RADIUS, you can close the UDP port 1812.		
1812	UDP	RADIUS authentication
1813	UDP	RADIUS accounting
5500	TCP	Agent authentication
5500	UDP	Agent authentication
5550	TCP	Agent auto-registration
5555	TCP	RSA SecurID Authentication API agents
5580	TCP	Offline authentication service
7002	TCP, SSL-encrypted	Authentication Manager and the RSA Token Management snap-in for the Microsoft Management Console (MMC)
7004	TCP, SSL-encrypted	Security Console, Self-Service Console and risk-based authentication (RBA), and Cryptographic Token-Key Initialization Protocol (CT-KIP)
7022	TCP, SSL-encrypted	Authentication Manager, trusted realm network access point, or the web tier
7072	TCP, SSL-encrypted	Operations Console
7082	TCP, SSL-encrypted	RADIUS Configuration SSL
8443	TCP, SSL-encrypted	Authentication Manager patches and service packs
9786	TCP, SSL-encrypted	Embedded identity router

For more information about these ports, see the *Setup and Configuration Guide*.

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.

Step 3: Deploy the RSA Authentication Manager Azure Image File

Deploy the RSA Authentication Manager Azure Image file. When you run Quick Setup, you configure the Azure Image file as an Authentication Manager primary instance or replica instance.

Before you begin

- 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.

  You must provide the appliance network settings for the virtual appliance:

Description	Information
Default Gateway	
Hostname (Fully Qualified Domain Name)	
IP Address	
Netmask	
Primary DNS Server	
Secondary DNS Server (Optional)	

  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: abcdefghijkmnopqrstuvwxyzACDEFGHIJKLMNPQRSTUVWXYZ0123456789. 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.
  2. A new, empty resource group.

Procedure

1. Log on to the Azure portal.
2. On the Services tab, select **Create a resource**.
3. Search for the RSA Authentication Manager 8.5 image. Click **Create**.
4. On the Basics blade, do the following:
   a. An **Administrator Username** and **Password details** are not required for Authentication Manager. Information that you enter in these fields is not saved. To log on to the appliance operating system, you need the **rsaadmin** account and the password that you specify during Quick Setup.

b. 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.
c. Select your **Subscription**, which is your Azure account, and your **Location**.
d. Click **OK**.

5. On the Virtual Machine Settings blade, do the following:
   a. Enter a **Virtual Machine name**.
   b. Select a virtual machine **Size**. RSA recommends **Standard_D8s_v3** and **Standard_D4s_v3** virtual machines.
   c. 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.
   d. 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:
   a. Enter the Gateway, DNS server, Subnet Mask, and Primary DNS server.
   b. A Secondary DNS server is optional. Azure requires at least one DNS server.
   c. 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.

11. In the Azure menu, select **Virtual Machine**, and search for your virtual machine.
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.

Step 4: Set Up the Primary Instance

You must use Quick Setup to configure a primary instance before you deploy any replica instances.

RSA recommends a deployment containing both a primary instance and a replica instance. The RSA Authentication Manager 8.5 Base Edition, Enterprise Edition, and Premium Edition all include permission to deploy a replica instance.

Do not cancel Quick Setup, or you will be unable to access the Quick Setup URL. In that situation, you must delete the Azure virtual machine, and deploy the primary instance again.

Run Quick Setup on the Primary Instance

Keep the virtual 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.

Before you begin

Copy the license file to a location that is accessible to the browser that is used to run the primary appliance Quick Setup. Do not unzip the file.

Procedure

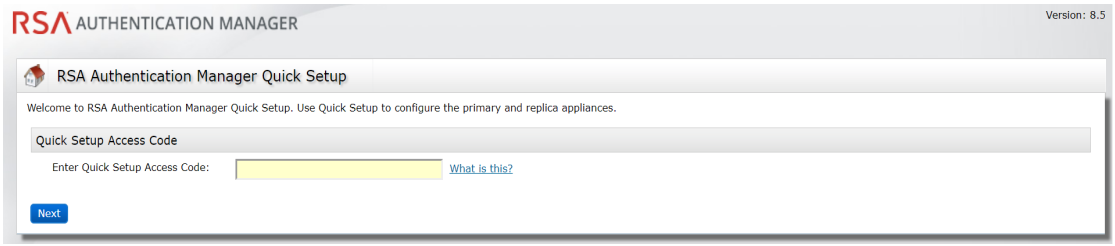
1. Launch Quick Setup with the URL provided at the end of virtual appliance deployment. Enter the Quick Setup URL in the browser, including **https**, and press **ENTER**:

   https://*<IP Address>*/

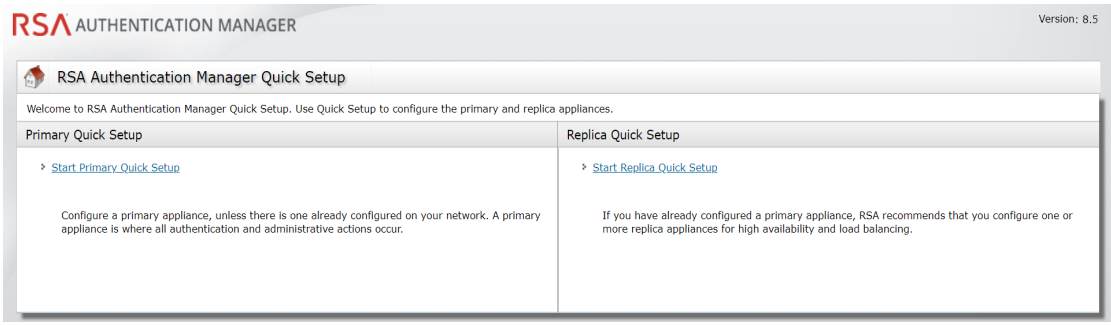
   where *<IP Address>* is the IP address of the appliance.

   If a browser warning states that this URL is not on the list of allowed or trusted sites, click the option that allows your browser to connect to an untrusted site.

2. You must enter the Quick Setup Access Code



3. Accept the End User License Agreement (EULA), and then follow the prompts to configure the Authentication Manager primary instance.



4. Record all of the passwords for the administrative accounts that you create during Quick Setup:

   - **Super Admin.**Super Admins can perform all Authentication Manager administrative tasks. Any Super Admin can create a new administrator in the Security Console.
   - **Operations Console administrator.** Operations Console administrators can perform administrative tasks in the Operations Console.
   - **Appliance Operating System Administrator.** Use the rsaadmin account if you require access to the appliance operating system for advanced maintenance or troubleshooting tasks. For security reasons, RSA does not provide a utility for recovering the operating system password.

   For more information, see the appendix "Administrative Accounts" in the *Setup and Configuration Guide*.

5. After the instance is configured, the first time you access the Security Console or the Operations Console, a warning appears because the default self-signed certificate created after Quick Setup is not trusted by your browser.

   Accept the certificate to access the console and prevent the warning from occurring again. For more information, see the chapter "Deploying a Primary Appliance" in the *Setup and Configuration Guide*

   If your web browser is configured for an enhanced security level, you must add the URL for each console to the list of allowed or trusted sites. See your browser documentation for additional instructions.

6. RSA recommends enabling SSH on the Azure virtual appliance, because SSH is the only way to log on to the operating system for this cloud-based appliance. Enabling SSH is optional on the VMware virtual appliance, the Hyper-V virtual appliance, and the hardware appliance. For instructions, see the Enable Secure Shell on the Appliance topic in the Operations Console or on RSA Link.

7. (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 replace a virtual appliance. For instructions, see the Download Network Settings for a Primary or Replica Instance topic in the Operations Console or on RSA Link.

Log On to the Consoles

You can access the consoles with the accounts that you specified during Quick Setup:

- The Super Admin account can access the Security Console and the Self-Service Console.
- The Operations Console administrator can access the Operations Console.

To view a complete list of URLs that are available for the consoles, see the *Setup and Configuration Guide*.

Console	URL
Security Console	https://<*fully qualified domain name*>/sc
Operations Console	https://<*fully qualified domain name*>/oc
Self-Service Console	If there is no web tier, enter: https://<*fully qualified domain name*>/ssc
	After installing a web tier, enter:

Console	URL
	https://<*fully qualified virtual host name*>/ssc
	If you change the default load balancer port, enter: https://<*fully qualified virtual host name*>:<*virtual host port*>/ssc

Step 5: Set Up a Replica Instance

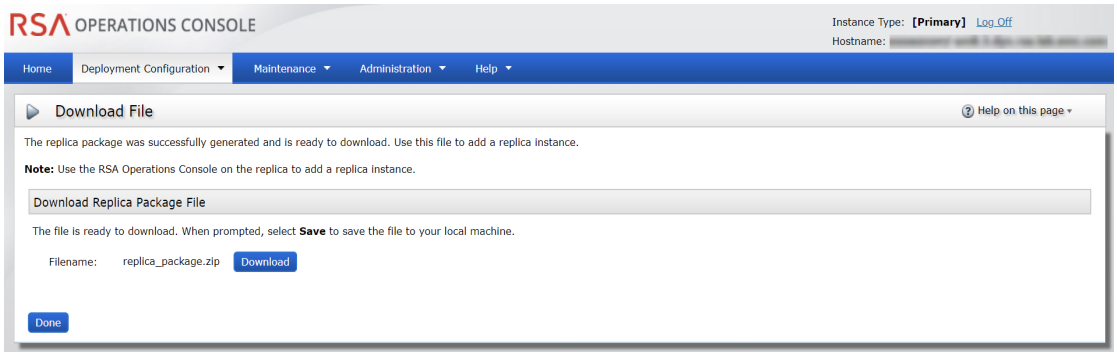
After you configure the primary instance, you can deploy another virtual appliance and set up a replica instance.

Before you begin

A primary instance must be deployed on the network.

Procedure

1. On the primary appliance, log on to the Operations Console, and click **Deployment Configuration** > **Instances** > **Generate Replica Package**. For instructions, see the Generate a Replica Package topic in the Operations Console or on RSA Link.



2. Deploy a virtual appliance.
3. Launch Quick Setup with the URL provided at the end of the virtual appliance deployment. Enter the Quick Setup URL in the browser, including **https**, and press **ENTER**:

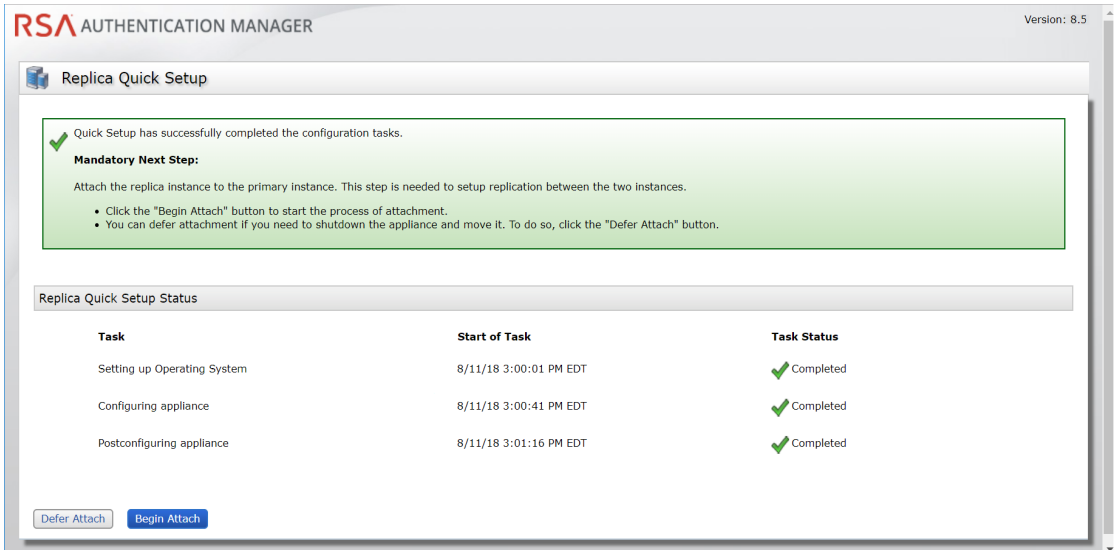
   https://<*IP Address*>/

   where <*IP Address*> is the IP address of the appliance.

   If a browser warning states that this URL is not on the list of allowed or trusted sites, click the option that allows your browser to connect to an untrusted site.
4. When prompted, enter the Quick Setup Access Code, and click **Next**.
5. Follow the prompts to complete Quick Setup.
6. Record the operating system password that is created during Quick Setup.

   The operating system password is required to access your replica instance. For security reasons, RSA does not provide a utility for recovering the operating system password.
7. After the instance is configured, click **Begin Attach** to attach the replica instance to the primary instance. For instructions, see the Attach the Replica Instance to the Primary Instance topic on RSA Link.

Note: Do not defer replica attachment, or you will be unable to access the Quick Setup URL. In that situation, you must delete the Azure virtual machine, and deploy the replica instance again.



8. 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 Enable Secure Shell on the Appliance topic in the Operations Console or on RSA Link.

9. (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 replace a virtual appliance. For instructions, see the Download Network Settings for a Primary or Replica Instance topic in the Operations Console or on RSA Link.

Step 6: Web Tier Installation

Web tiers are not required, but your deployment might need them to satisfy your network configuration and requirements. Authentication Manager includes services, such as dynamic seed provisioning and the Self-Service Console, that may be required by users outside of your corporate network. If your network includes a DMZ, you can use a web tier to deploy these services inside the DMZ. For more information, see the chapter "Planning Your Deployment" in the *Planning Guide*.

Step 7: Next Steps

After setting up the appliance, see the *Setup and Configuration Guide* for information on the next steps that you might perform for your deployment. You must perform all post-setup tasks on the primary instance.

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.

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.

July 2020

Revised: April 2021

Intellectual Property Notice

This software contains the intellectual property of RSA or is licensed to RSA from third parties. Use of this software and the intellectual property contained therein is expressly limited to the terms and conditions of the License Agreement under which it is provided by or on behalf of RSA.

Open Source License

This product may be distributed with open source code, licensed to you in accordance with the applicable open source license. If you would like a copy of any such source code, RSA or its affiliates will provide a copy of the source code that is required to be made available in accordance with the applicable open source license. RSA or its affiliates may charge reasonable shipping and handling charges for such distribution. Please direct requests in writing to RSA Legal, 174 Middlesex Turnpike, Bedford, MA 01730, ATTN: Open Source Program Office.