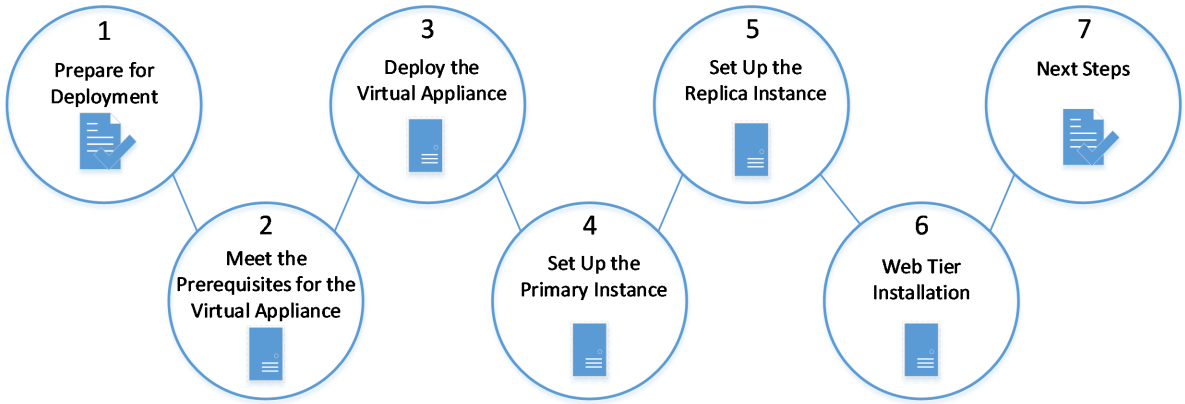
RSA SECURID® ACCESS

RSA® Authentication Manager 8.4

Hyper-V Virtual Appliance Getting Started

Thank you for purchasing RSA® Authentication Manager 8.4. This document provides an overview of how to deploy Authentication Manager on the Hyper-V 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 and Meet the Prerequisites

See the documentation on RSA Link at https://community.rsa.com/community/products/securid/authentication-manager-84:

- Read the *Release Notes*, available at https://community.rsa.com/docs/DOC-99418.
- Read the *Planning Guide*, available at https://community.rsa.com/docs/DOC-99427, for deployment considerations. For example, if users outside of your network require access to resources, you might want to deploy a web tier.
- Meet the prerequisites described in the *Setup and Configuration Guide*, available at https://community.rsa.com/docs/DOC-99426.

Step 2: Meet the Prerequisites for the Virtual Appliance

You must meet the following requirements for deploying RSA Authentication Manager 8.4 on a Hyper-V virtual appliance.

Software Requirements

On a Microsoft Windows 2012, 2012 R2, or 2016 host machine, deploy the Hyper-V virtual appliance with one of

the following tools:

- Hyper-V System Center 2012, 2012 R2, or 2016 Virtual Machine Manager (VMM).
- Hyper-V Manager 2012, 2012 R2, or 2016.

If you are using Hyper-V System Center 2012, 2012 R2, or 2016 VMM, use the Windows PowerShell version that is included with the VMM Console installation.

If you are using Hyper-V Manager 2012, 2012 R2, or 2016, use the Windows PowerShell version that is included with your version of Windows.

If you are using VMM, verify that the required Hyper-V and VirtualMachineManager PowerShell modules are available. Run these two PowerShell commands to display a list of commands related to each module:

- Get-Command -Module Hyper-V
- Get-Command -Module VirtualMachineManager

For more information, see your Hyper-V documentation.

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. For instructions, see your Hyper-V documentation.

Primary or Replica Instance Requirements

The Hyper-V virtual appliance for each RSA Authentication Manager instance requires hardware that meets or exceeds the following minimum requirements:

- 100 GB of disk space for storage and a 4 GB swap file
- 4 GB of memory
- At least one virtual CPU

By default, each Authentication Manager instance is deployed with 8 GB of memory and two virtual CPUs.

Note: 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 additional hardware requirements for the physical server hosting the virtual appliances, see your Hyper-V documentation.

Step 3: Deploy the Virtual Appliance

Deploy RSA Authentication Manager 8.4 on a Hyper-V virtual appliance. When you run Quick Setup, you configure the virtual appliance as an RSA Authentication Manager primary instance or replica instance.

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

Follow this procedure to deploy a Hyper-V virtual appliance through the Hyper-V System Center Virtual Machine Manager (VMM) Console. Deployment through the Hyper-V Manager is also supported. When you run Quick Setup, you configure the virtual appliance as an RSA Authentication Manager primary instance or replica instance.

Before you begin

- 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.

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 files, select the server, and click **Next**.
   e. Select the share that contains the VHD files, and click **Next**.
   f. Click **Add Library Servers**.
3. Run the Virtual Machine Manager Windows PowerShell module as an administrator, and change directories to the location of the Windows batch file.
4. 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.
   - -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 '\\windowshyperv.yourorganization.com\libraryshare'** to create a Hyper-V virtual machine template that uses the default port and template name.
5. 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.
6. 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.

7. If you have not already done so, open the Hyper-V VMM Console, and log on to the VMM server.
8. Click **Library > Templates > VM Templates**.
9. Right-click the name of the virtual machine template, and select **Create Virtual Machine**. The Create Virtual Machine wizard launches.
10. On the Identity window, enter a name for the virtual appliance, and click **Next**.
11. On the Configure Hardware window, keep the default hardware profile, and click **Next**. The PowerShell script automatically configured the virtual machine template.
12. Follow the wizard to deploy the virtual appliance. On the Select Networks window, choose a network connection. You must connect the appliance to your network before it is powered on.
13. On the Summary window, click **Create**.
14. After the virtual appliance is successfully created, power on the virtual appliance, and connect to the virtual appliance through the VMM Console.
15. Wait 30 seconds to select the default keyboard layout, English (United States). To choose another keyboard layout, click any key and follow the instructions on the screen.
16. When the OS Console prompts you, enter and verify the network settings for the virtual appliance.
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 you provided for the virtual appliance:

      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.

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

Follow this procedure to deploy a Hyper-V virtual appliance through the Hyper-V Manager. Deployment through the Hyper-V Virtual Machine Manager Console is also supported. When you run Quick Setup, you configure the virtual appliance as an RSA Authentication Manager primary instance or replica instance.

Before you begin

Keep a copy of the RSA Authentication Manager Hyper-V virtual appliance file, **rsa-am-hyper-v-virtual-appliance-8.4.0.0.0.zip**. After you create the virtual appliance, running the new appliance modifies the VHD files. For each virtual appliance that you deploy, you need to 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.

   Note: Do not rename the VHD files.
4. Run Windows PowerShell as an administrator, and change directories to the location of the Windows batch file. The virtual appliance is created in the directory where you run the script.
5. 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.

6. 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.
7. 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.
8. In the Windows **Start** menu, click **Server Manager > Tools > Hyper-V Manager**.
9. In the Hyper-V Manager, select the node and host from the left pane.
10. In the **Virtual Machines** pane, select the new virtual machine.
11. In the **Action** pane, under the virtual machine name, click **Settings**.
12. 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.
13. In the **Actions** pane, under the virtual machine name, click **Start**, and **Connect**.
14. Wait for 30 seconds to select the default keyboard layout, English (United States). To choose another keyboard layout, click any key and follow the instructions on the screen.
15. When the OS Console prompts you, enter and verify the network settings for the virtual appliance.
16. 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 you specified for the virtual appliance:

    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.

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 8.4 Base Edition, Enterprise Edition, and Premium Edition all include permission to deploy a replica instance.

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

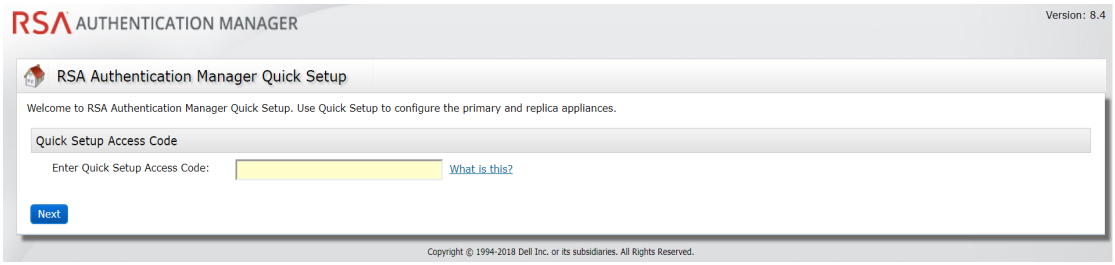
1. Launch Quick Setup with the URL provided at the end of virtual appliance deployment. Enter the Quick Setup URL in the browser, including **https**, and press **ENTER**:

   https://<*IP Address*>/

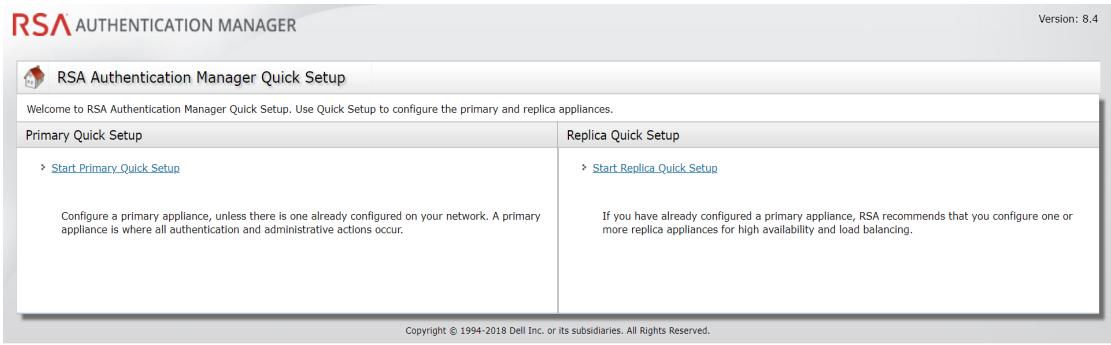
   where <*IP Address*> is the IP address of the appliance.

   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 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 at https://community.rsa.com/docs/DOC-77019.

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 at https://community.rsa.com/docs/DOC-76799.

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: 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

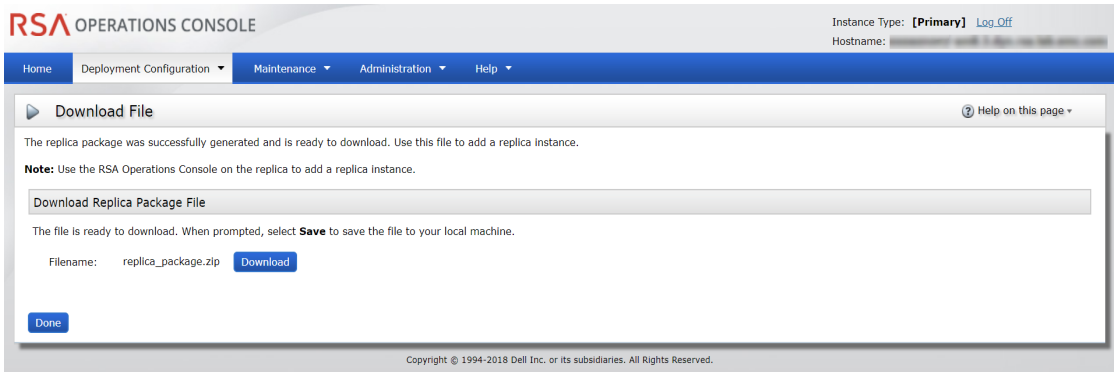
After you configure the primary instance, you can deploy another virtual appliance and set up a replica instance.

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 at https://community.rsa.com/docs/DOC-77158.



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*>/

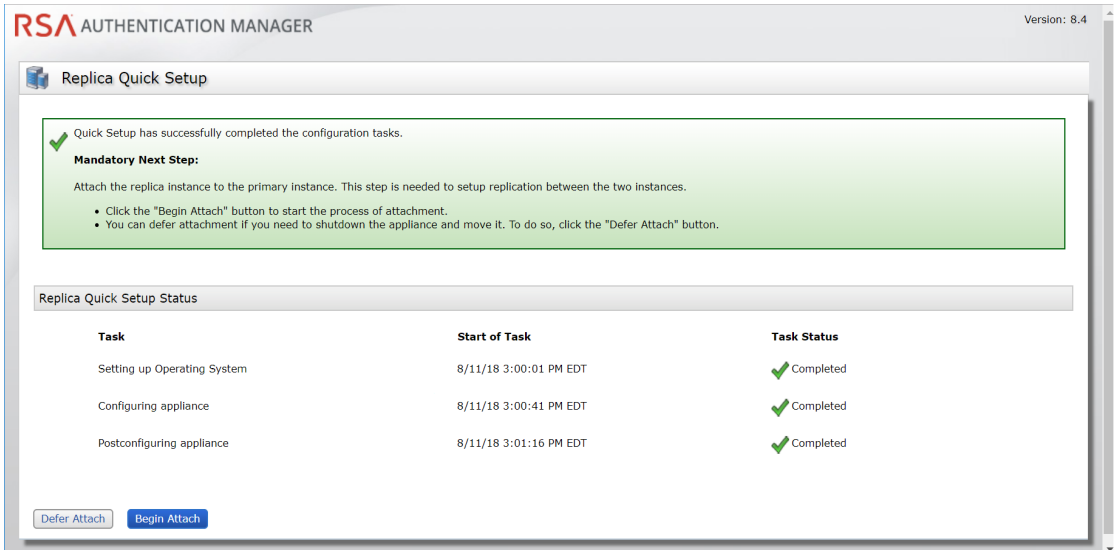
   where <*IP Address*> is the IP address of the appliance.

   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, do one of the following:

   - Click **Begin Attach** to attach the replica instance to the primary instance.
   - 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.

   For instructions, see the "Attach the Replica Instance to the Primary Instance" topic on RSA Link at https://community.rsa.com/docs/DOC-76808.



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 at https://community.rsa.com/docs/DOC-77019.

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 at https://community.rsa.com/docs/DOC-76799.

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.

December 2018

Trademarks

Intellectual Property Notice

Open Source License