Cloud Authentication Service Quick Setup Guide for RADIUS Clients

This guide helps you quickly set up your production deployment for the Cloud Authentication Service and add authentication for a RADIUS client.

Use this guide in conjunction with the Planning Guide. If you have completed a deployment with another Quick Setup Guide and want to set up the deployment described in this guide, skip the steps that you have already completed.

**Step 1: Plan**

There are a few things you need to plan to deploy your system.

**What You Need to Have**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign-in credentials to the Cloud Administration Console</td>
<td>Sign-in credentials are emailed to you after you request an environment from RSA Sales or your partner. Be sure that the email address that you provide to RSA is for a real user in your LDAP directory and not, for example, a group alias or general account. For browser requirements for the Cloud Administration Console, see <a href="https://community.rsa.com/docs/DOC-81615">https://community.rsa.com/docs/DOC-81615</a>.</td>
</tr>
</tbody>
</table>
| Virtual appliance infrastructure | Hardware requirements for image file:  
- Disk space: 54 GB  
- Memory: 8 GB  
- Virtual CPUs: 4  
- Network interface:  
  - VMware: Two E1000  
Required only for identity router deployment on-premises in a VMware or Hyper-V environment |
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| virtual network adapters or Microsoft Hyper-V: Two synthetic network adapters | Software requirements:  
  - VMware or  
    - VMware Platform: VMware ESXi 5.5 or later (currently 6.x series)  
    - VMware vSphere Client: Any version that works with the supported ESXi deployments  
  - Hyper-V 2012 R2 |
| Amazon Web Services (AWS) account                                    | Amazon Virtual Server Instance hardware requirements:  
  - Family: General purpose  
  - Type: t2.large  
  - vCPUs: 2  
  - Memory: 8 GB |
| Required only for identity router deployment in an Amazon Web Services cloud environment | AWS cloud environment requirements:  
  - Access to t2.large or better instance types  
  - Virtual Private Cloud with private and public subnets  
  - Route Tables, Security Groups, and Network ACLs that allow traffic between the identity router and all other components in your deployment  
  - DHCP Option Sets that specify all DNS servers required for your deployment  
  - Elastic IP addresses (if your organization manages its own DNS service) |
| Note: To deploy an identity router in the Amazon cloud, you must be familiar with the following concepts as they relate to AWS:  
  Elastic Compute Cloud (EC2)  
  Amazon Machine Image (AMI)  
  Elastic IP Address  
  Security Groups  
  Virtual Private Cloud (VPC)  
  Subnets  
  Route Tables  
  Network Access Control Lists (ACL)  
  DHCP Option Sets  
  Internet Gateway  
  NAT Gateway  
  Virtual Private Gateway  
  VPN Connection  
  VPC Peering | |
| Microsoft Active Directory 2008 or 2012 or LDAPv3 directory server | Create a group of a limited number of users (for example, RSA SecurID Access Test Group) to synch and test with. |
| SSL certificate from your LDAP directory server                      | Used for an encrypted connection (LDAPS) to your directory server.  
  Download the SSL certificate from your directory server. If your directory |
What You Need to Know

RSA SecurID Access uses a hybrid architecture that consists of two components:

- The **Cloud Authentication Service** is a cloud service that provides an easy-to-use Cloud Administration Console and powerful identity assurance engine.
- The **identity router** is a virtual appliance that securely connects your on-premises resources, such as Active Directory, and the Cloud Authentication Service. You can deploy the identity router in your on-premises VMware or Hyper-V environment, or in the Amazon Web Services (AWS) cloud.

In AWS deployments, the identity router has one network interface to which you assign public and private IP addresses and connect other network resources from the internet or your private network.

In VMware and Hyper-V deployments, the identity router has two network interfaces. Place one interface in a public-facing network and the other in a private network where it can reach your LDAP directory. For more information about configuring your system to use these interfaces, see https://community.rsa.com/docs/DOC-54091.

Add your values to the following worksheet. You will use this information in the next section and during setup.

<table>
<thead>
<tr>
<th>Item</th>
<th>Your Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Item</strong></td>
<td><strong>Your Values</strong></td>
</tr>
</tbody>
</table>
| A mobile device or Windows PC | - iOS 11.0 or later
  - Android 6.0 or later
  - Windows 10 Version 1511 or later |

### Cloud Administration Console and Cloud Authentication Service

Current values:

- US region: `<authentication_service_domain>`, access.securid.com, na2.access.securid.com, or na3.access.securid.com (191.237.22.167, 104.42.197.125)
- EMEA region: `<authentication_service_domain>`, access-eu.securid.com (104.40.223.169, 40.127.204.94)
- ANZ region: `<authentication_service_domain>`, access-anz.securid.com (20.36.34.174, 20.36.64.73)

Your authentication service domain appears in the Cloud Administration Console on the **Platform > Identity Router > Registration** page when you add an identity router.

New IP addresses in September 2019:

- US region: 168.61.48.213, 13.93.181.131
<table>
<thead>
<tr>
<th>Item</th>
<th>Your Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA recommends that you ensure access to these IP addresses to prevent service disruption in September.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LDAP directory server</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• IP address</td>
<td></td>
</tr>
<tr>
<td>• FQDN</td>
<td></td>
</tr>
<tr>
<td>• Base DN of users (the root where users will be synchronized from, for example, DC=company, DC=com)</td>
<td></td>
</tr>
<tr>
<td>• Administrator account credentials that RSA SecurID Access can use to connect to the directory server</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNS servers IP addresses</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>For DNS configuration requirements, see <a href="https://community.rsa.com/docs/DOC-54152">https://community.rsa.com/docs/DOC-54152</a>.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NTP server IP address</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) RADIUS client IP address</td>
<td></td>
</tr>
</tbody>
</table>

**Required only for VMware and Hyper-V identity router deployments:**

<table>
<thead>
<tr>
<th>Identity router management interface (private)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• IP address</td>
<td></td>
</tr>
<tr>
<td>• Netmask</td>
<td></td>
</tr>
<tr>
<td>• Gateway</td>
<td></td>
</tr>
<tr>
<td>• Short hostname</td>
<td></td>
</tr>
<tr>
<td>• FQDN</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity router proxy interface (public)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• IP address</td>
<td></td>
</tr>
<tr>
<td>• Netmask</td>
<td></td>
</tr>
<tr>
<td>• Gateway</td>
<td></td>
</tr>
<tr>
<td>• Short hostname</td>
<td></td>
</tr>
<tr>
<td>• FQDN</td>
<td></td>
</tr>
</tbody>
</table>

**Required only for Amazon Web Services identity router deployments:**

<table>
<thead>
<tr>
<th>Identity router</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Private IP Address</td>
<td>Used for communication with internal resources in the same VPC, another VPC, or your on-premises network.</td>
</tr>
<tr>
<td>• Public Elastic IP Address</td>
<td>Used for communication with public resources over the internet if the identity router is in a public subnet. Not required if a NAT/load balancer with a public IP address manages traffic to the identity router.</td>
</tr>
</tbody>
</table>
### Connectivity Requirements

Replace the values in the table below with your values from the table above. This table identifies the connectivity requirements that you might need to provide to your IT group to update firewall rules for your network. If you deploy the identity router in the Amazon cloud, the route tables, security groups, and network ACLs in your AWS environment must also allow these connections. Update your connectivity settings before continuing with the next step.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol and Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>Both Cloud Authentication Service environments</td>
<td>TCP 443</td>
<td>External user access to Cloud Authentication Service</td>
</tr>
<tr>
<td>&lt; Your administrators &gt;</td>
<td>For on-premises identity routers: <code>&lt;Your identity router management interface IP address&gt;</code>&lt;br&gt;For identity routers in the Amazon cloud: <code>&lt;Your identity router private IP address&gt;</code></td>
<td>On-premises: TCP 443 Amazon: TCP 9786</td>
<td>Identity Router Setup Console</td>
</tr>
<tr>
<td>For on-premises identity routers: <code>&lt;Your identity router proxy interface IP address&gt;</code>&lt;br&gt;For identity routers in the Amazon cloud: <code>&lt;Your identity router private IP address&gt;</code></td>
<td>Cloud Administration Console and both Cloud Authentication Service environments&lt;br&gt;Note: If your company uses URL filtering, be sure that *.access.securid.com, *.auth.securid.com, and the Cloud Authentication Service IP addresses for your region are whitelisted. Also, confirm that you can access both environments. For instructions, see <a href="https://community.rsa.com/docs/DOC-79579">https://community.rsa.com/docs/DOC-79579</a>.</td>
<td>TCP 443</td>
<td>Identity router registration</td>
</tr>
<tr>
<td>For on-premises</td>
<td><code>&lt;Your LDAP directory server IP address&gt;</code></td>
<td>TCP 636</td>
<td>LDAP directory user authentication and</td>
</tr>
<tr>
<td>Source</td>
<td>Destination</td>
<td>Protocol and Port</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| identity routers:  
<Your identity router management interface IP address>  
For identity routers in the Amazon cloud:  
<Your identity router private IP address> |  |  |  |
| For on-premises identity routers:  
<Your identity router proxy interface IP address or identity router management interface IP address>  
<Your DNS server IP address>  
For identity routers in the Amazon cloud:  
<Your identity router private IP address> |  | UDP 53 | DNS |
| <Your RADIUS client IP address> | For on-premises identity routers:  
<Your identity router management interface IP address>  
For identity routers in the Amazon cloud:  
<Your identity router private IP address> |  | UDP 1812 | RADIUS |
| For on-premises identity routers:  
<Your identity router proxy interface IP address or identity router management interface IP address>  
<Your NTP server IP address> |  | UDP 123 | Network time server synchronization |
<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol and Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon cloud: &lt;Your identity router private IP address&gt;</td>
<td>For on-premises identity routers: &lt;Your identity router management interface IP address&gt; For identity routers in the Amazon cloud: &lt;Your identity router private IP address&gt;</td>
<td>TCP 22</td>
<td>(Optional) SSH for troubleshooting For more information, see <a href="https://community.rsa.com/docs/DOC-75833">https://community.rsa.com/docs/DOC-75833</a>.</td>
</tr>
</tbody>
</table>

**Step 2: Deploy the Identity Router**

**Add an Identity Router**

**Procedure**

1. Sign into the Cloud Administration Console using the URL and credentials that RSA emailed to you.
2. Click **Platform > Identity Routers**.
3. On the Identity Routers page, click **Add an Identity Router**, and follow the instructions.

   Under **Registration Details**, copy the **Registration Code** and **Authentication Service Domain** to a location where you can access them later on.

   ![Registration Details](image)

4. Click **Close**.

**Install or Create the Identity Router Virtual Appliance or Machine**

You can install the virtual appliance image using a VMware administration client such as vSphere, by either connecting to the VMware vCenter Server, or connecting directly to the VMware ESXi host.

Or you can use Hyper-V Manager or Amazon Web Services EC2 to create a virtual machine for the identity router.

**Procedure**

1. In the Cloud Administration Console, click **Platform > Identity Routers**.
2. Click **Download Identity Router Image** and do one of the following:
   - For VMware, click **Download OVA Image for VMware**, and save the image to a location accessible by VMware.
For Hyper-V, click **Download VHD Image for Hyper-V**, and save the image to a location accessible by Hyper-V.

For Amazon Web Services:
1. Click **Access AMI Image for Amazon**.
2. Enter your AWS Account ID.
3. Click **Update AMI Access**.
4. Note the values in the **Identity Router AMI Name** and **AWS Regions with AMI Access** fields. You can search the AWS private images catalog using these value to quickly locate the AMI.

3. Do one of the following:

   - To use VMware, sign into the VMware client, do the following:
     1. Follow the VMware client documentation to install the virtual appliance from the image. When prompted, enter the following data:
        1. Name to use for the virtual appliance
        2. VMware host or cluster for the virtual appliance
        3. Resource pool for the virtual appliance
        4. Storage location or data store to use for the virtual appliance
        5. Format for storing virtual disks
        6. Networks to be used for the virtual appliance
     2. Power on the virtual machine.

   - To use Hyper-V Manager, sign into Hyper-V Manager, and do the following:
     1. Click **Hyper-V Host > New > Virtual Machine**.
     2. Follow the wizard. In each dialog box, provide the following information.

<table>
<thead>
<tr>
<th>Dialog Box</th>
<th>Required Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify Name and Location</td>
<td>Name of the identity router virtual machine.</td>
</tr>
<tr>
<td>Specify Generation</td>
<td>Select Generation 1.</td>
</tr>
<tr>
<td>Assign Memory</td>
<td>Startup memory = 8192 MB (recommended).</td>
</tr>
<tr>
<td>Configure Networking</td>
<td>Select the network for the management network adaptor.</td>
</tr>
<tr>
<td>Connect Virtual Hard Disk</td>
<td>Select <strong>Use an existing virtual hard disk</strong> and browse to the location where the identity router VHD image is available.</td>
</tr>
<tr>
<td>Completing the New Virtual Machine Wizard</td>
<td>Review and click <strong>Finish</strong>.</td>
</tr>
</tbody>
</table>

   c. To configure the second network, select the new virtual machine, right-click, and select **Settings**.
   d. On the Add Hardware page, select **Network Adapter** and click **Add**.
   e. Select the network for your proxy interface, then click **Apply** and **OK**.
   f. Select the new virtual machine from the list of virtual machines. Right-click and select
g. With the virtual machine selected, right-click again and select **Connect**.

- To use Amazon Web Services, sign into Amazon EC2 and follow the documentation provided by Amazon to do the following:
  a. Make sure your AWS environment includes a VPC which meets the following requirements:
     - Private and public subnets are configured according to your deployment requirements.
     - Route tables, security groups, and network ACLs are configured to allow necessary traffic to and from the other network resources in your deployment, such as users and identity sources.
     - All DNS servers required for your deployment are specified in the DHCP options set.
  b. Launch the virtual instance using the AMI.

When prompted, specify the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMI template</td>
<td>The AMI template image provided by RSA.</td>
</tr>
<tr>
<td>Instance type</td>
<td>Determines presets for the virtual instance. The identity router requires a t2.large instance or greater.</td>
</tr>
<tr>
<td>Virtual Private Cloud (VPC)</td>
<td>The section of your Amazon environment where you will deploy the identity router.</td>
</tr>
<tr>
<td>Subnet</td>
<td>A subnetwork within your VPC where you will deploy the identity router. The subnet can be either public or private, depending on how resources and users will connect to the identity router.</td>
</tr>
<tr>
<td>Auto-assign Public IP</td>
<td>Determines whether Amazon issues dynamic public IP addresses for the identity router, or the IP address is determined by the subnet settings. If your organization manages its own DNS service, RSA recommends allocating a persistent Elastic IP address through Amazon Web Services, and assigning it to the identity router instance after you complete the launch process.</td>
</tr>
<tr>
<td>Storage</td>
<td>Virtual storage space. The identity router requires 54 GB General Purpose SSD (GP2) storage.</td>
</tr>
<tr>
<td>Tags</td>
<td>Optional labels that describe this identity router. RSA recommends adding a tag specifying the Fully Qualified Domain Name, which acts as a unique identifier to differentiate this identity router from others in your deployment.</td>
</tr>
<tr>
<td>Security groups</td>
<td>Firewall rules that control traffic to and from the identity router. Add security groups that allow necessary traffic from other network resources according to your deployment model.</td>
</tr>
</tbody>
</table>

- Review the configuration and launch the instance.
d. If prompted to select a key pair, select **Proceed without a keypair**.
e. Use the **Get instance screenshot** feature to monitor instance deployment status. When deployment is complete, refresh the screenshot and write down the URL displayed for the Identity Router Setup Console.

**Configure Initial Network Settings Using the Identity Router VM Console**

You use the Identity Router VM Console to configure IP addresses and static routes for on-premises identity routers deployed in your VMware or Hyper-V environment.

**Note:** This procedure is not required for identity routers in the Amazon Web Services cloud.

**Procedure**

1. Connect to the identity router using your VMware or Hyper-V management client.
2. Sign into the Identity Router VM Console:
   
   **Username:** idradmin  
   **Password:** s1mp13  
   
   You are prompted to change these credentials the first time you sign in.
3. Refer to the planning worksheet for the values to complete the **Management**, **Proxy**, and **DNS** sections.
   
   Use the Up and Down arrows to navigate the main menu. Press Enter to select a menu option or configure its settings. Use Tab and Shift + Tab to navigate between settings and back to the main menu. When the cursor is in the settings panel, press F10 to save or Esc to revert. Press F10 after you complete each section to save your values.
4. Select **Commit** in the left-hand frame to save the network configuration settings.
5. Write down the URL that appears.

**Connect Identity Router to Cloud Administration Console**

**Procedure**

1. Open a web browser and go to the URL that you wrote down in the previous section.
2. Sign into the Identity Router Setup Console:
   
   **Username:** idradmin  
   **Password:** s1mp13  
   
   You are prompted to change these credentials the first time you sign in.
3. Add any DNS servers that you did not add in the Identity Router VM Console.

   **Note:** These DNS server settings do not apply for identity routers in the Amazon cloud. Edit the DHCP option set in your Amazon Web Services environment if you need to add DNS servers for an Amazon cloud-based identity router.

4. Click **Update IDR Setup Configuration**.
5. Click **Connect Administration Console**.
6. In the **Registration Code** field, enter the **Registration Code** displayed when you added the identity router in the Cloud Administration Console.
7. In the **Authentication Service Domain** field, enter the **Authentication Service Domain** displayed when you added the identity router in the Cloud Administration Console.
8. Click **Submit**.

   A confirmation message appears when the identity router is connected to the Cloud Administration Console. Also, note that the Identity Router Setup Console contains other pages that provide network diagnostics and detailed logs for the identity router.

9. Sign into the Cloud Administration Console to check the status of the identity router (**Platform > Identity Routers**).

   When the identity router is connected to the Cloud Administration Console, the status reads **Active**. This process usually takes up to five minutes.

10. In the Cloud Administration Console, click **Publish Changes** to apply the configuration settings for the new identity router.

### Step 3: Enable RADIUS on the Cluster

**Procedure**

1. In the Cloud Administration Console, click **Platform > Clusters**.
2. Select **Edit** from the drop-down menu next to the cluster.
3. Select the **Enable the RADIUS service on all identity routers in the cluster** checkbox.
4. Click **Save and Finish**.
5. Click **Publish Changes**.

### Step 4: Connect LDAP Directory

**Add a Connection to LDAP Directory**

**Procedure**

1. In the Cloud Administration Console, click **Users > Identity Sources**.
2. Click **Add an Identity Source > Select** next to the directory to add.
3. Enter the identity source name and root (the base DN for users from the planning worksheet).

4. In the SSL Certificates section:
   a. Select **Use SSL encryption to connect to the directory servers.**
   b. Click **Add** and select the SSL certificate.

5. In the Directory Servers section, add each directory server in the identity source, and test the connection.

6. Click **Next Step.**

7. On the User Attributes page, click **Refresh Attributes**, and verify that a valid list of attributes appears.

8. Select **Use selected policy attributes with the Cloud Authentication Service.**

9. In the **Policies** column, select **sAMAccountName**, **virtualGroups**, and **memberOf** or other attributes that you might use to identify users.

10. Click **Next Step.**

11. In the **User Search Filter** field, specify your test group using a filter. The following is an Active Directory example:

   ```
   (&(objectCategory=Person)(sAMAccountName=*)(objectClass=user)(mail=*)(memberOf=<yourgroup_distinguishedName>))
   ```

   Where `<yourgroup_distinguishedName>` is the name of your test administrator group.

   For example, `(objectCategory=Person)(sAMAccountName=*)(objectClass=user)(mail=*)(memberOf=CN=SecurIDAccessUsers,OU=Groups,DC=Corp,DC=local))

12. Click **Save and Finish.**

13. Click **Publish Changes.**

**Synchronize LDAP Directory for the Cloud Authentication Service**

Synchronize data between the Cloud Authentication Service and your LDAP directory to ensure that the Cloud Authentication Service reflects any updates made to the LDAP directory.

During synchronization, users are added and attribute values that you selected in the previous step are copied to the Cloud Authentication Service. User passwords are not synchronized.
Procedure

1. In the Cloud Administration Console, click **Users > Identity Sources**.
2. Next to your identity source, select **Synchronization** from the drop-down menu.
3. In the Identity Source Details section, click **Synchronize Now**.
   Depending on the number of users you are synchronizing, this process can take a number of minutes.

**Step 5: Add an Access Policy**

Create an access policy that you will assign to RSA SecurID Access My Page (a web portal used for device registration) when you configure it. For simplicity, this access policy will not require additional authentication of users. You can change this policy in the future.

1. Sign in to the Cloud Administration Console.
2. Click **Access > Policies**.
3. Click **Add a Policy**.
4. Enter the name (for example, No Additional Authentication), and select the identity source.
5. On the Rule Sets page, do the following:
   a. In **Apply to**, select **All Users**.
   b. In the **Access**, specify **Allowed**.
   c. In **Additional Authentication**, select **Not Required**.
6. Click **Save and Finish**.
7. Click **Publish Changes**.

**Step 6: Enable My Page**

RSA SecurID Access My Page is a web portal that helps provide a secure way for users to complete RSA SecurID Authenticate device registration, using multifactor authentication and QR or numeric registration codes.

1. In the Cloud Administration Console, click **Platform > My Page**.
2. Enable My Page.
3. Write down your My Page URL.
4. In the **Primary Authentication Method** drop-down list, select the authentication method to use.
5. In the **Access Policy for Additional Authentication** drop-down list, select the No Additional Authentication policy that you created earlier.
6. Click **Save**.

**Step 7: Protect a Resource**

Configure a RADIUS client to be protected by RSA SecurID Access. In the wizard, select the preconfigured policy **All Users Low Assurance Level** as the access policy.

For example, for instructions for configuring Cisco Adaptive Security Appliance, see this. For instructions for all supported RADIUS clients, see the RSA SecurID Access category on RSA Ready.

**Step 8: Test**

**Complete RSA SecurID Authenticate Device Registration**

**Procedure**

1. On one device (for example, your computer), do the following:
   a. Go to RSA SecurID Access My Page.
   b. Enter your email address.
   c. Enter your RSA SecurID passcode or password, depending on what you configured.
   d. Complete any additional authentication that you are prompted for.
   e. Click **Get Started**.
2. On another device (iOS, Android, or Windows 10), download the RSA SecurID Authenticate app:
   - iOS: [Apple App Store](#)
   - Android: [Google Play](#)
   - Windows 10: [Microsoft Store](#)
3. On your computer, on the Registration page, click **Next**.
4. On your mobile device, do the following:
   a. Open the RSA SecurID Authenticate app.
   b. Tap **Allow** to allow the Authenticate app to send notifications.
   c. Allow or deny Google Analytics data collection. You can select either option to use the Authenticate app.
   d. Accept the license agreement.
   e. Tap **Scan QR Code**.
   f. Allow the app to access your camera.
   g. Scan the QR code that displays in My Page.
   h. Tap **OK** after setup is complete.
   i. Swipe through the tutorial.
   j. The app home screen appears, and the app is ready for use.

5. On your computer, on the Registration page, click **Test Now**.

6. RSA SecurID Access sends a notification to your registered device.

7. On your mobile device, tap the notification and approve it.

8. The My Page home screen displays. You have successfully registered and tested your device.
Sign Into the Protected Resource

Procedure

1. Start the sign-in process to the protected resource.
   RSA SecurID Access sends a notification to your phone.
2. Tap Approve on your mobile device.
3. Select Remember this browser, and click Continue.
   You are signed into the resource.
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.

RSA provides you with a unique identifier, called the Customer Support ID, which 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.

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

Trademarks

RSA, the RSA Logo, SecurID, and EMC are either registered trademarks or trademarks of Dell Inc throughout the world. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Intellectual Property Notice

This software contains the intellectual property of Dell Inc or is licensed to Dell Inc 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 Dell Inc.

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, Dell Inc. or its subsidiaries will provide a copy of the source code that is required to be made available in accordance with the applicable open source license. Dell Inc. or its subsidiaries may charge reasonable shipping and handling charges for such distribution. Please direct requests in writing to Dell Legal, 176 South St., Hopkinton, MA 01748, ATTN: Open Source Program Office.