Duo MFA for AWS Directory Service on the AWS Cloud

Quick Start Reference Deployment

April 2019

Vishal Gupta, Duo Security
Rob Barnes, AWS Professional Services
Shivansh Singh, AWS Quick Start team

Visit our GitHub repository for source files and to post feedback, report bugs, or submit feature ideas for this Quick Start.

Contents
Overview ................................................................................................................................. 2
  Duo Authentication Proxy for AWS Directory Service on AWS .................................. 3
  Cost and licenses ............................................................................................................... 3
Architecture ........................................................................................................................... 4
Planning the deployment ....................................................................................................... 6
  Specialized knowledge ...................................................................................................... 6
  AWS account .................................................................................................................... 7
  Technical requirements ..................................................................................................... 7
Deployment steps .................................................................................................................. 8
  Step 1. Sign in to your AWS account ............................................................................. 8
  Step 2. Obtain a license .................................................................................................. 8
  Step 3. Launch the Quick Start ...................................................................................... 9
    Parameters for deploying Duo MFA for AWS Directory Service ..................................... 10
  Step 3. Validate the deployment .................................................................................... 12
Overview


This Quick Start is for those who currently use or intend to use AWS Directory Service directory types such as AWS Directory Service for Microsoft Active Directory (also known as AWS Managed Microsoft AD) or Active Directory Connector (AD Connector), and who want to apply MFA.

Duo MFA helps mitigate the threat of compromised credentials caused by phishing, malware, and other vectors, reducing risk while meeting compliance requirements for access security.
Duo Authentication Proxy for AWS Directory Service on AWS

Traditional login on the AWS Management Console involves providing a user name and password. To help mitigate the threat of leaked credentials, AWS offers the ability to enable MFA for your AWS Identity and Access Management (IAM) users or your root credentials.

If you’re using a federation mechanism like AWS Single Sign-On (AWS SSO) or Active Directory Federation Services (AD FS) with an AWS Directory Service option, however, you must configure your own MFA implementation. One common approach is to use an MFA provider like Duo. In this scenario, you log in to the AWS Management Console using your AD credentials. You then use the Duo Mobile app, along with Duo’s wide variety of authentication methods, and your AD credentials to authenticate you to AWS.

For a quick primer on configuring MFA manually using your on-premises Remote Authentication Dial-In User Service (RADIUS) implementation, see the blog post How to Enable Multi-Factor Authentication for AWS Services by Using AWS Microsoft AD and On-Premises Credentials.

If you don’t have a current RADIUS implementation, you can use this solution to automate the process of provisioning a RADIUS infrastructure in AWS using the Duo Authentication Proxy as the MFA provider. This provides an additional layer of security for accessing your critical resources integrated with AWS Directory Service.

Cost and licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

**Tip** After you deploy the Quick Start, we recommend that you enable the AWS Cost and Usage Report to track costs associated with the Quick Start. This report delivers billing metrics to an S3 bucket in your account. It provides cost estimates based on usage throughout each month, and finalizes the data at the end of the month. For more information about the report, see the AWS documentation.
This Quick Start requires a license for Duo MFA. Learn more about the Duo license and sign up for a license at https://duo.com/pricing. You must set up at least one Duo user whose email address is associated with at least one user in Active Directory.

**Architecture**

Enabling MFA on a directory service requires at least one RADIUS server that has been configured to integrate with an MFA provider. For fault tolerance, at least two RADIUS servers should be used, ideally in different Availability Zones in the region where your directory service resides.

This solution creates a set of RADIUS EC2 instances across the Availability Zones that your directory service uses. If one instance fails for any reason, the Auto Scaling group automatically starts a new instance, installs and configures the Duo Authentication Proxy, and then registers the new instance with your directory service. This failover process takes about five minutes.

The solution uses an AWS Systems Manager document to automatically install and configure the Duo Authentication Proxy on the instances when they start up; the instances themselves don’t include any start-up scripts. This is known as *dynamic bootstrapping*. Your Duo secret key and RADIUS shared secret are encrypted in the Systems Manager Parameter Store using an AWS Key Management Service (AWS KMS) encryption key. The instances use a role that has permission to retrieve and decrypt these values when they are being configured by Systems Manager.

Deploying this Quick Start for a new virtual private cloud (VPC) with default parameters builds the following Duo MFA for AWS Directory Service environment in the AWS Cloud.
Figure 1: Quick Start architecture for Duo MFA for AWS Directory Service on AWS
The Quick Start includes an AWS CloudFormation template that creates the following Duo MFA for AWS Directory Service environment in the AWS Cloud, based on parameter settings that you specify:

- A set of Amazon Elastic Compute Cloud (Amazon EC2) instances that are configured with the Duo Authentication Proxy.
- An AWS Systems Manager document that is used by AWS Systems Manager State Manager to configure the EC2 instances with the Duo Authentication Proxy.
- A Remote Authentication Dial-In User Service (RADIUS) shared secret created by AWS Secrets Manager.
- An AWS Lambda function used by Secrets Manager to automatically rotate the RADIUS shared secret on a weekly basis.
- An Amazon Simple Notification Service (SNS) topic invoked when a new RADIUS EC2 instance is created.
- A Lambda function that subscribes to the SNS topic that configures AWS Directory Service to use RADIUS servers.
- An Amazon Simple Storage Service (Amazon S3) bucket that stores the Systems Manager State Manager executions.
- An Amazon CloudWatch log group that stores Duo Authentication Proxy logs from the RADIUS servers.

**Note** You can gain access to the RADIUS EC2 instances using Systems Manager Session Manager. For more information about using Session Manager for shell access, see the [AWS Systems Manager Session Manager for Shell Access to EC2 Instances](https://aws.amazon.com/blogs/monitoring/aws-systems-manager-session-manager-shell-access-to-ec2-instances/) blog post.

**Planning the deployment**

**Specialized knowledge**

This Quick Start assumes familiarity with AWS Directory Service. For more information, see the [AWS Directory Service](https://aws.amazon.com/directoryservice/) documentation.

This deployment guide also requires a moderate level of familiarity with AWS services. If you’re new to AWS, visit the [Getting Started Resource Center](https://aws.amazon.com/getting-started/) and the [AWS Training and Certification website](https://aws.amazon.com/training/) for materials and programs that can help you develop the skills to design, deploy, and operate your infrastructure and applications on the AWS Cloud.
AWS account

If you don’t already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.

Your AWS account is automatically signed up for all AWS services. You are charged only for the services you use.

Technical requirements

Before you launch the Quick Start, ensure that you have the following in place:

- An existing AWS Directory Service directory, either Managed AD or AD Connector, with at least one AD user. To deploy a directory, see the Active Directory Domain Services on AWS Quick Start.

- A Duo license. Learn more about the Duo license at https://duo.com/pricing. You must set up at least one Duo user whose email address is associated with at least one user in Active Directory.

- Duo Mobile used for authentication.

- The existing security group associated with your domain controllers must allow User Datagram Protocol (UDP) port 1812 egress to their own subnet CIDR range (or the entire VPC).

Your account must also be configured as specified in the following table. Otherwise, deployment might fail.

<table>
<thead>
<tr>
<th>Resources</th>
<th>If necessary, request service limit increases for the following resources. You might need to do this if you already have an existing deployment that uses these resources, and you think you might exceed the default limits with this deployment. For default limits, see the AWS documentation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Trusted Advisor</td>
<td>offers a service limits check that displays your usage and limits for some aspects of some services.</td>
</tr>
<tr>
<td></td>
<td><strong>Resource</strong></td>
</tr>
<tr>
<td></td>
<td><strong>t2.micro instances</strong></td>
</tr>
<tr>
<td>Regions</td>
<td>This deployment includes AWS Directory Service, which isn’t currently supported in all AWS Regions. For a current list of supported regions, see AWS Regions and Endpoints in the AWS documentation.</td>
</tr>
</tbody>
</table>
IAM permissions

To deploy the Quick Start, you must log in to the AWS Management Console with IAM permissions for the resources and actions the templates will deploy. The AdministratorAccess managed policy within IAM provides sufficient permissions, although your organization may choose to use a custom policy with more restrictions.

S3 buckets

Unique S3 bucket names are automatically generated based on the account number and region. If you delete a stack, the logging buckets are not deleted (to support security review). If you plan to re-deploy this Quick Start, additional S3 buckets will created; you must manually delete S3 buckets that were created during the previous deployments.

Deployment steps

Step 1. Sign in to your AWS account

1. Sign in to your AWS account at https://aws.amazon.com with an IAM user role that has the necessary permissions. For details, see Planning the deployment earlier in this guide.

2. Make sure that your AWS account is configured correctly, as discussed in the Technical requirements section.

Step 2. Obtain a license

This Quick Start requires a license for Duo MFA. To use the Quick Start in your production environment, sign up for a license at https://duo.com/pricing. For more information, see Cost and licenses, earlier in this guide.
Step 3. Launch the Quick Start

**Notes**  Depending on whether you’re using the older version of the AWS CloudFormation console or the redesigned console, some of the user interface elements reflected in this section might differ.

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Sign in to your AWS account, and use the following link to launch the AWS CloudFormation template.

   ![Deploy Duo MFA for Directory Service on AWS](deploy.png)

   **Important**  Make sure that your VPC has private subnets in different Availability Zones for the RADIUS EC2 instances. These subnets require NAT gateways in their route tables to allow the instances to download packages and software without exposing them directly to the internet.

   The deployment takes about ten minutes to complete.

2. Check the region that’s displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for Duo MFA for AWS Directory Service will be built.

3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.

4. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary.
PARAMETERS FOR DEPLOYING DUO MFA FOR AWS DIRECTORY SERVICE

View template

Parameter account settings:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duo integration key</td>
<td>Requires input</td>
<td>The integration key retrieved from the Duo RADIUS application configuration.</td>
</tr>
<tr>
<td>Duo secret key</td>
<td>Requires input</td>
<td>The secret key retrieved from the Duo RADIUS application configuration.</td>
</tr>
<tr>
<td>Duo hostname</td>
<td>Requires input</td>
<td>The API hostname retrieved from the Duo RADIUS application configuration.</td>
</tr>
</tbody>
</table>

To get these Duo account settings:

1. Log in to Duo with your Duo account, or sign up for an account, if you don’t already have one. For more account information, see Technical requirements and Cost and licenses, earlier in this guide.

2. Log in to the Duo Admin Panel, and then navigate to Applications.

3. Choose Protect an Application, and then locate RADIUS in the applications list. Choose Protect this Application to get your integration key, secret key, and API hostname.

RADIUS proxy configuration settings:

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory service ID</td>
<td>Requires input</td>
<td>The ID of the existing directory service (d-xxxxxxxxxx). The directory service ID must match the pattern d-0123456789.</td>
</tr>
<tr>
<td>Amazon Linux image ID</td>
<td>/aws/service/ami-amazon-linux-amzn-ami-hvm-x86_64-gp2</td>
<td>The parameter store location used to retrieve the latest Amazon Linux ID. IMPORTANT: Use the default value provided here; otherwise, the Systems Manager configuration could fail.</td>
</tr>
<tr>
<td>RADIUS servers</td>
<td>2</td>
<td>The number of RADIUS proxy servers to create. Two servers provide a sufficient balance between fault tolerance and cost.</td>
</tr>
<tr>
<td>RADIUS port number</td>
<td>1812</td>
<td>The port on which to listen for incoming RADIUS access requests.</td>
</tr>
</tbody>
</table>
### AWS Quick Start configuration:

**Note** We recommend that you keep the default settings for the following two parameters, unless you are customizing the Quick Start templates for your own deployment projects. Changing the settings of these parameters will automatically update code references to point to a new Quick Start location. For additional details, see the [AWS Quick Start Contributor’s Guide](#).

<table>
<thead>
<tr>
<th>Parameter label (name)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duo fail mode (DuoFailMode)</td>
<td>safe</td>
<td>Once primary authentication succeeds, Safe mode allows authentication attempts, if the Duo service cannot be contacted. Secure mode rejects authentication attempts, if the Duo service cannot be contacted.</td>
</tr>
<tr>
<td>Quick Start S3 bucket name (QSS3BucketName)</td>
<td>aws-quickstart</td>
<td>The S3 bucket you created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.</td>
</tr>
<tr>
<td>Quick Start S3 key prefix (QSS3KeyPrefix)</td>
<td>quickstart-duo-mfa/</td>
<td>The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.</td>
</tr>
</tbody>
</table>

5. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. When you’re done, choose **Next**.

6. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the two check boxes to acknowledge that the template will create IAM resources and that it might require the capability to auto-expand macros.

7. Choose **Create** to deploy the stack.

8. Monitor the status of the stack. When the status is **CREATE_COMPLETE**, the Duo MFA for AWS Directory Service cluster is ready.

9. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.
Step 3. Validate the deployment

After you successfully launch the stack, follow these steps as your instances are starting up:

1. Validate that the Auto Scaling group starts up the number of instances that you specified in the parameters (default of two).

2. Navigate to the Amazon EC2 console, and look for instances labeled **Duo RADIUS Proxy Server**. These should have a status of **Pending**.

3. Navigate to the Systems Manager console, and select **State Manager** from the left menu.

4. Choose the association named **BootstrapRadiusProxies-d-xxxxxxxxxxx**, where “d-xxxxxxxxxxx” is the ID of your directory service.

5. Choose the **Instances** tab. It will take a few moments for the instances to start up and register with Systems Manager. Systems Manager associates the instances based on their **DirectoryServiceId** tags.

6. After a few moments, check that the **Association status** changes to **Success**. When this happens, it means that the instances have successfully configured with the Duo Authentication Proxy. If the status is **Failed**, see **Troubleshooting**, later in this guide.

7. Navigate to the Directory Service console, and select your directory.

8. Choose the **Networking & security** tab.

9. In the **Multi-factor authentication** pane at the bottom of the page, the RADIUS status should be **Completed**. (It can take a few minutes for Systems Manager to register and configure the instances.) If the status is **Failed**, see **Troubleshooting MFA implementation**, later in this guide. To view the MFA configuration, choose the **Actions** dropdown option in the **Multi-factor authentication** pane, and then choose **Edit**. You will see the IP addresses of the RADIUS instances created by the Auto Scaling group. The shared secret code values are empty for security reasons.
Step 4. Create a service delegation role

Before you can federate using your directory, you must create a role that your directory service can use that you can federate into—for example, AD-Admin. Navigate to the IAM console, and create a service delegation role that trusts the Directory Service service:

1. Navigate to your directory service in the Directory Service console.

2. To create an application access URL, choose Create. The URL is similar to "<YOUR_APP_NAME_HERE>.awsapps.com." You will need this link later to validate the login.

3. Enable the directory service to use the IAM console. You should see your role in the dropdown box. Choose the role, and then assign your AD users to it.

4. Test the login by going to https://<YOUR_APP_NAME_HERE>.awsapps.com/console/ (using the app name that you created earlier). You should see something similar to the following screen.

![Figure 3: Login screen](image)

5. To log in to the IAM console, use your AD user name and password, and then enter the code that you get from Duo Mobile.
Modifying the implementation

If you want to increase or decrease the number of RADIUS servers after implementing the solution, update the CloudFormation stack and specify the desired number of servers.

If you increase the number of servers, the Auto Scaling group starts up the number of new instances, and installs and configures the Duo Authentication Proxy for each new instance.

After each instance is configured, the instance publishes a message to the `RadiusProxyBootstrapComplete-d-xxxxxxxxxx` Amazon Simple Notification Service (Amazon SNS) topic. This triggers the `UpdateDirectoryServiceMfaSettings-d-xxxxxxxxxx` AWS Lambda function to add the IP address of the new instance to your directory service’s RADIUS configuration.

Likewise, when you decrease the number of servers, the Auto Scaling group terminates the appropriate number of servers, and then triggers the preceding Lambda function to remove the IP addresses of the terminated instances from your directory service’s RADIUS configuration.

Troubleshooting MFA implementation

If your directory service’s MFA status is in a `Failed` status, please check the following:

1. Ensure that the RADIUS EC2 instances have access to the internet. This Quick Start solution launches the RADIUS EC2 instances in the same subnet as the DNS servers in your directory service. The subnet must have a route to the internet (typically through a NAT gateway) in order to install the Duo Authentication Proxy and other required tools used to configure the directory service.

2. Ensure that the security group associated with your directory service’s DNS servers have a rule that allows output traffic on port 1812 to the security group created by this solution.
   
   a. To find the security group associated with your DNS servers, navigate to the Directory Service console, and note the IP addresses under `DNS address`.
   
   b. Navigate to the EC2 console, and choose the Network Interfaces link from the menu.
   
   c. In the search field, enter one of the DNS IP addresses found in the previous step.
   
   d. From the lower pane of the console, choose `View outbound rules` and determine whether there is a rule allowing egress on port 1812 for UDP to the
For advanced troubleshooting, do the following:

- View the Lambda function logs in CloudWatch Logs
- View the RADIUS proxy logs in CloudWatch Logs

**View the Lambda function logs in CloudWatch Logs**

1. Navigate to the CloudFormation console, and select the stack that was just launched.
2. Choose the Resources tab.
3. Look for `UpdateDirectoryServiceMfaSettingsCloudWatchLogsGroup` in the Logical ID column and choose the resource link in the Physical ID column. This opens a CloudWatch Logs log group for the Lambda function that is responsible for configuring the MFA settings for your directory service.
4. You should see one or more log streams. Select each one and look for specific error conditions. If you see an error that says, “Found addresses: [], but two are required,” this means that the RADIUS EC2 instances were not configured successfully. Proceed to the steps in the next section.

**View the RADIUS proxy logs in CloudWatch Logs**

1. Navigate to the CloudFormation console, and select the stack that was just launched.
2. Choose the Resources tab.
3. Look for `RadiusProxyCloudWatchLogsGroup` in the Logical ID column and choose the resource link in the Physical ID column. This opens a CloudWatch Logs log group for the Duo Authentication Proxy running on each of the RADIUS EC2 instances.
4. You should see one or more log streams; each stream represents logs from the Duo Authentication Proxy on each EC2 instance. Select each of the log streams, and look for possible error messages.
5. If there aren’t any log streams in the log group, the instances might not have access to the internet.
Configuring Duo MFA for AWS Directory Service on AWS

Once you've installed Duo Mobile and enrolled into it, you're ready to go. Log in as usual with your user name and password, and then use your device to verify that it's you. You can set up the system to do this via options like SMS, voice call, one-time passcode, and Duo Mobile.

You'll see a **Second Password** or **MFA Code** field when using any of the clients (Amazon WorkSpaces, Amazon WorkDocs, AWS Management Console, etc.). These fields accept a Duo passcode, which is generated with Duo Mobile or sent via SMS. You can also enter the word “push” to use Duo Push, “sms” to get a new batch of SMS passcodes, or “phone” to authenticate via a phone call.

The following login screen shows an example of logging in where you enter the word “push” in the **MFA Code** field to receive a push notification.

![Login screen example](image)

**Figure 4: Setting up push notifications**

For more information about configuring Duo, see the [Guide to Duo Deployment Best Practices](#).
FAQ

Q. I encountered a CREATE_FAILED error when I launched the Quick Start.
A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with Rollback on failure set to No. (This setting is under Advanced in the AWS CloudFormation console, Options page.) With this setting, the stack’s state will be retained and the instance will be left running, so you can troubleshoot the issue. (For Windows, look at the log files in %ProgramFiles%\Amazon\EC2ConfigService and C:\cfn\log.)

Important  When you set Rollback on failure to No, you will continue to incur AWS charges for this stack. Please make sure to delete the stack when you finish troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

Q. I encountered a size limitation error when I deployed the AWS CloudFormation templates.
A. We recommend that you launch the Quick Start templates from the links in this guide or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.

Send us feedback

To post feedback, submit feature ideas, or report bugs, use the Issues section of the GitHub repository for this Quick Start. If you’d like to submit code, please review the Quick Start Contributor’s Guide.

Additional resources

AWS resources

- Getting Started Resource Center
- AWS General Reference
- AWS Glossary
AWS services

- AWS CloudFormation
- Amazon CloudWatch
- AWS Directory Service
- Amazon EC2
- AWS KMS
- AWS Lambda
- IAM
- Amazon SNS
- AWS Systems Manager
- Amazon VPC

Duo Authentication Proxy for AWS Directory Service documentation

- Authentication Proxy reference
- Duo RADIUS

Other Quick Start reference deployments

- AWS Quick Start home page

Document revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Change</th>
<th>In sections</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 2019</td>
<td>Initial publication</td>
<td>—</td>
</tr>
</tbody>
</table>
© 2019, Amazon Web Services, Inc. or its affiliates, and Duo Security, Inc. All rights reserved.

**Notices**

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at [http://aws.amazon.com/apache2.0/](http://aws.amazon.com/apache2.0/) or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.