SecurID

Cloud Authentication Service Planning Guide

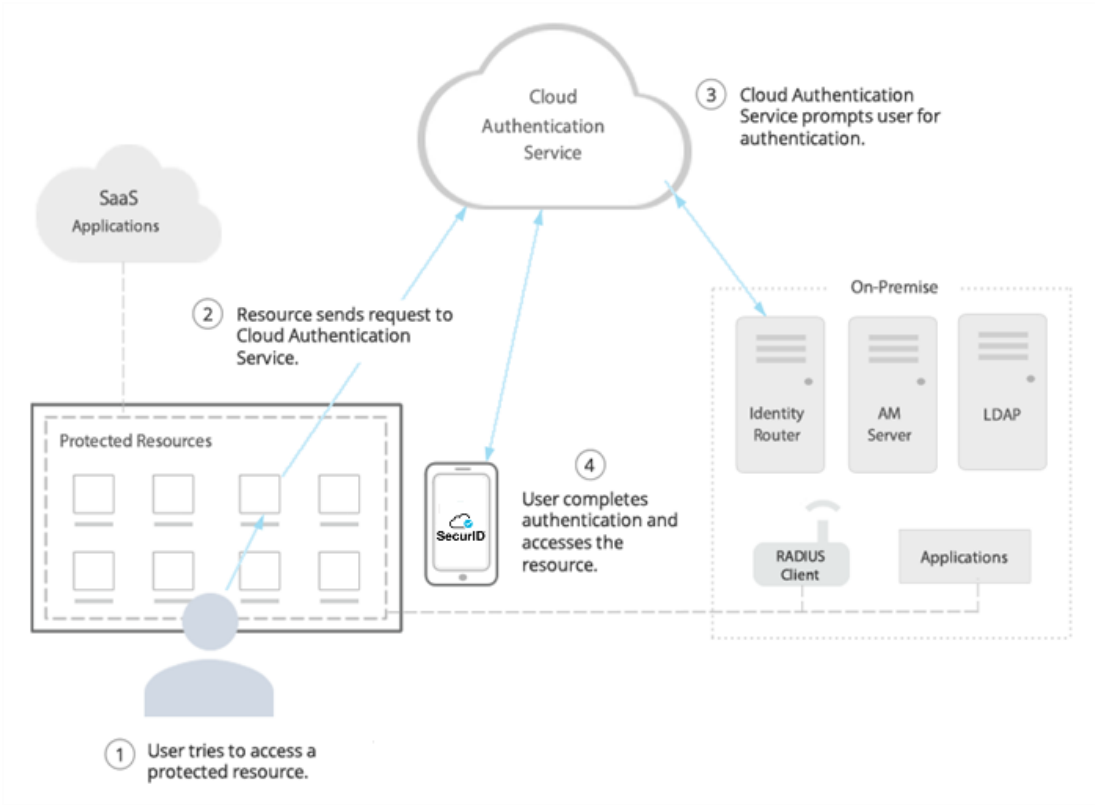
This guide provides an overview of the Cloud Authentication Service and the supported deployment types. Use this guide along with your *Quick Setup Guide* to quickly set up your production deployment.

Cloud Authentication Service Overview

The Cloud Authentication Service is an access and authentication platform with a hybrid cloud architecture. The Cloud Authentication Service enables your company to control how users access resources with centralized access and authentication policies and can accelerate user productivity with single sign-on (SSO).

The Cloud Authentication Service helps protect SaaS and on-premises web applications, third-party SSO solutions, and on-premises resources that support RADIUS. The Cloud Authentication Service includes transparent and interactive authentication methods for multifactor identity assurance. These methods include biometric methods such as fingerprint verification, hardware devices such as SecurID Token and FIDO authenticators, and context-based authentication using factors such as the user's location and network. Confidence in a user's identity can also be established through risk analytics, based on user characteristics such as past behavior, authenticators previously used for authentication, and other factors.

The following graphic illustrates how the Cloud Authentication Service works.



Note: The identity router can be deployed on-premises, in the Amazon Web Services cloud, or on your SecurID Authentication Manager server.

Benefits

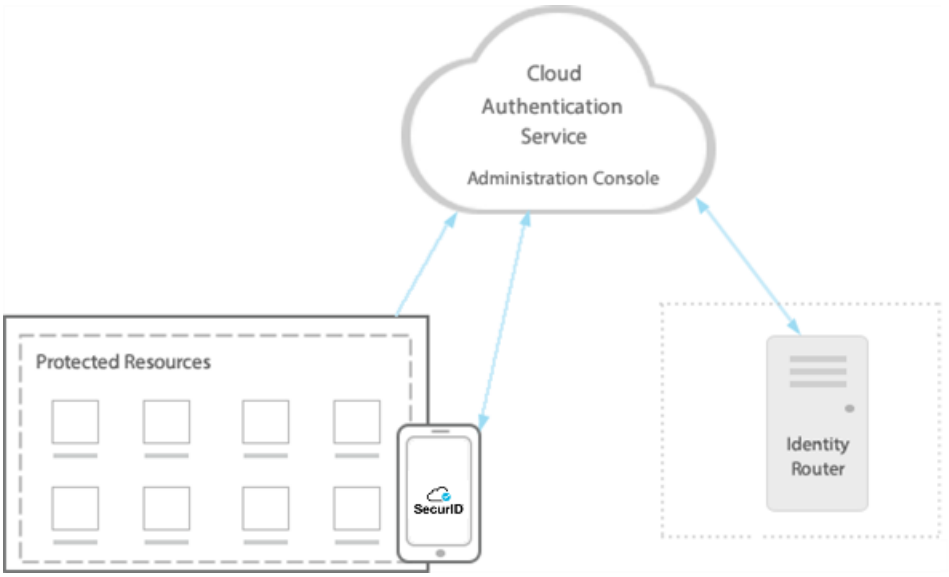
The Cloud Authentication Service provides the following key benefits:

- Integration with SecurID Authentication Manager 8.x to extend your SecurID deployment by making additional authentication methods available to protect Authentication Manager resources.
- Convenient multifactor authentication (MFA) that leverages capabilities built into devices through the SecurID Authenticate app.
- Centralized access control policies that consistently enforce different security requirements for applications based on assurance levels.
- Support of relying parties, RADIUS-capable devices, SAML and non-SAML applications, and SaaS and on-premises web applications for MFA.
- SSO with out-of-the-box connectivity to popular applications.
- Single point of access to protected applications with the application portal.
- LDAP directory server user passwords stay on-premises and are not synchronized to the Cloud Authentication Service.
- SecurID Authentication API, a REST-based programming interface that allows you to develop clients that process multifactor, multistep authentications through SecurID Authentication Manager and the Cloud Authentication Service. The interface definition can be integrated with any programming language. For instructions, see the SecurID Authentication API Developer's Guide.

- SecurID Cloud Administration REST APIs, web service interfaces you can use to create clients that perform administrative operations. These operations include importing audit log events into your security information and event management (SIEM) solution, retrieving event logs from the Cloud Administration Service, and performing certain Help Desk functions. For instructions, see Using the Cloud Administration APIs.

Cloud Authentication Service Components

A Cloud Authentication Service deployment consists of four main components: the Cloud Authentication Service (which is both the name of the managed server and the name for the set of components), the Identity Router®, the Cloud Administration Console, and the SecurID Authenticate app installed on user devices.



Note: The identity router can be deployed on-premises, in the Amazon Web Services cloud, or on your SecurID Authentication Manager server.

Cloud Authentication Service

The Cloud Authentication Service performs run-time authentication for the protected resources. The Cloud Authentication Service also allows SecurID to modify and improve authentication capabilities.

The Cloud Authentication Service runs on Microsoft Azure, a cloud computing platform that is hosted through a global network of Microsoft data centers. SecurID uses a multi-tenant database in an environment that shares infrastructure while segregating customer data to ensure privacy. Service levels and operational procedures are standardized for all customers due to the shared nature of the platform.

Identity Router®

The identity router is a virtual appliance that communicates with the following components.

Component	Purpose
Cloud Authentication Service	The Cloud Authentication Service enforces access policies, which determine which applications users can access, when additional authentication is needed, and which authentication methods are required. For example, a policy might allow only your sales team to access an application with sensitive customer information. Access policies are based on session information, such as IP addresses (for example, within a corporate network or not).

Component	Purpose
Identity sources	Identity routers connect to identity sources in real-time and synchronize a limited subset of user data to the Cloud Authentication Service. A minimum amount of user data is required to register authenticators. LDAP directory server user passwords are never synchronized and remain secure on your directory server.
SecurID Authentication Manager	SecurID Authentication Manager enables users to authenticate with SecurID tokens or the SecurID Authenticate app from all access points controlled by Authentication Manager. For integration instructions, see Select an Integration Path for SecurID Authentication Manager with the Cloud Authentication Service.

The identity router can be installed on the following platforms:

- On VMware or Hyper-V virtual appliances on-premises within your network.
- Amazon Web Services cloud (in a subnet)
- SecurID Authentication Manager 8.5 or later

All platforms support RADIUS and single sign-on (SSO) in the Cloud Authentication Service, except for SecurID Authentication Manager 8.5 and later. For details about supported platforms and services, see Identity Router.

Cloud Administration Console

The Cloud Authentication Service component contains a hosted, multi-tenant Cloud Administration Console that Super Admins use to perform setup and daily management tasks. Super Admins and Help Desk administrators both use the console to troubleshoot user issues. This is a partial list of tasks that can be performed using the console:

- Configure your company domain and certificates, if necessary.
- Add and manage identity routers.
- Add identity sources so the identity router can verify user attributes to allow or deny access to resources.
- Add resources, such as relying parties, RADIUS clients, and applications.
- Configure assurance levels that can be used by protected resources.
- Configure access policies to determine user access to protected resources.
- Configure the SecurID Application Portal.
- Troubleshoot user issues with the Event Monitor.
- Unlock tokencodes for users.
- Manage user authenticators and known browsers.

The SecurID Authenticate App

SecurID My Page helps provide a secure way for users to complete registration with the SecurID Authenticate app, using MFA and QR or numeric registration codes. My Page guides users through registration, including downloading the SecurID Authenticate app from the Apple App Store, Google Play, or Microsoft Store. The administrator provides users with the My Page URL. After successful registration, users can complete authentication for applications that require it.

Cloud Authentication Service Deployment Options

The Cloud Authentication Service supports several deployment options:

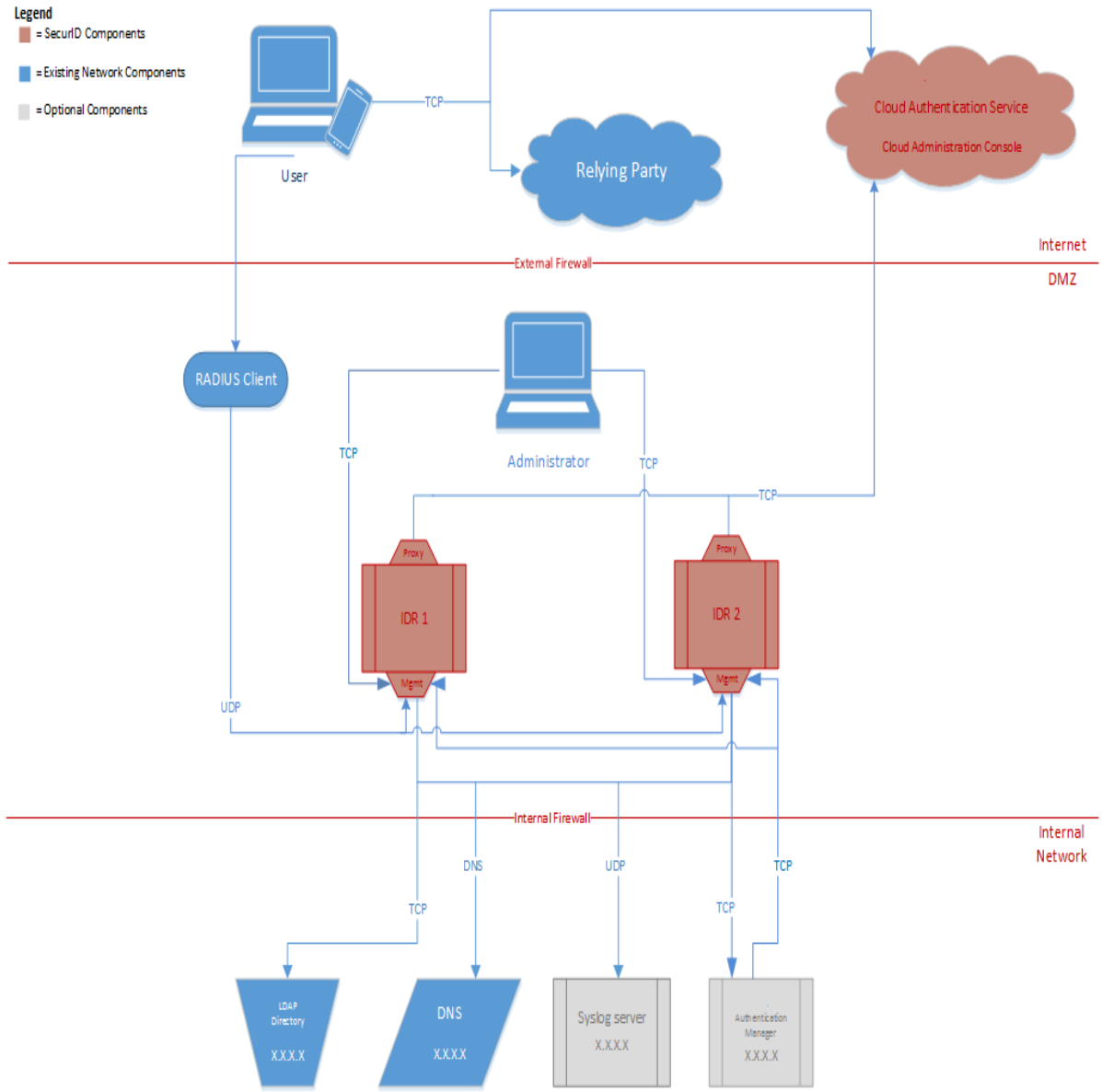
- If you do not need the Cloud Authentication Service to provide single sign-on services, use the RADIUS or Relying Party option. This deployment is used for SAML applications, third-party SSO solutions, Microsoft Azure Active Directory, and RADIUS clients.
- If you need the Cloud Authentication Service to provide single sign-on services, use the SSO Agent option.

In the following examples, the identity router is hosted on-premises within your network, but you can choose to host it in the Amazon Web Services cloud instead. To learn more about this feature, see Amazon Web Services Identity Router Deployment Models on the next page.

RADIUS or Relying Party Deployment

The RADIUS for Cloud Authentication Service or relying party deployment architecture consists of two identity routers in a cluster with relying parties or RADIUS clients. If one identity router stops responding, users can still access protected applications through the remaining identity router at reduced capacity.

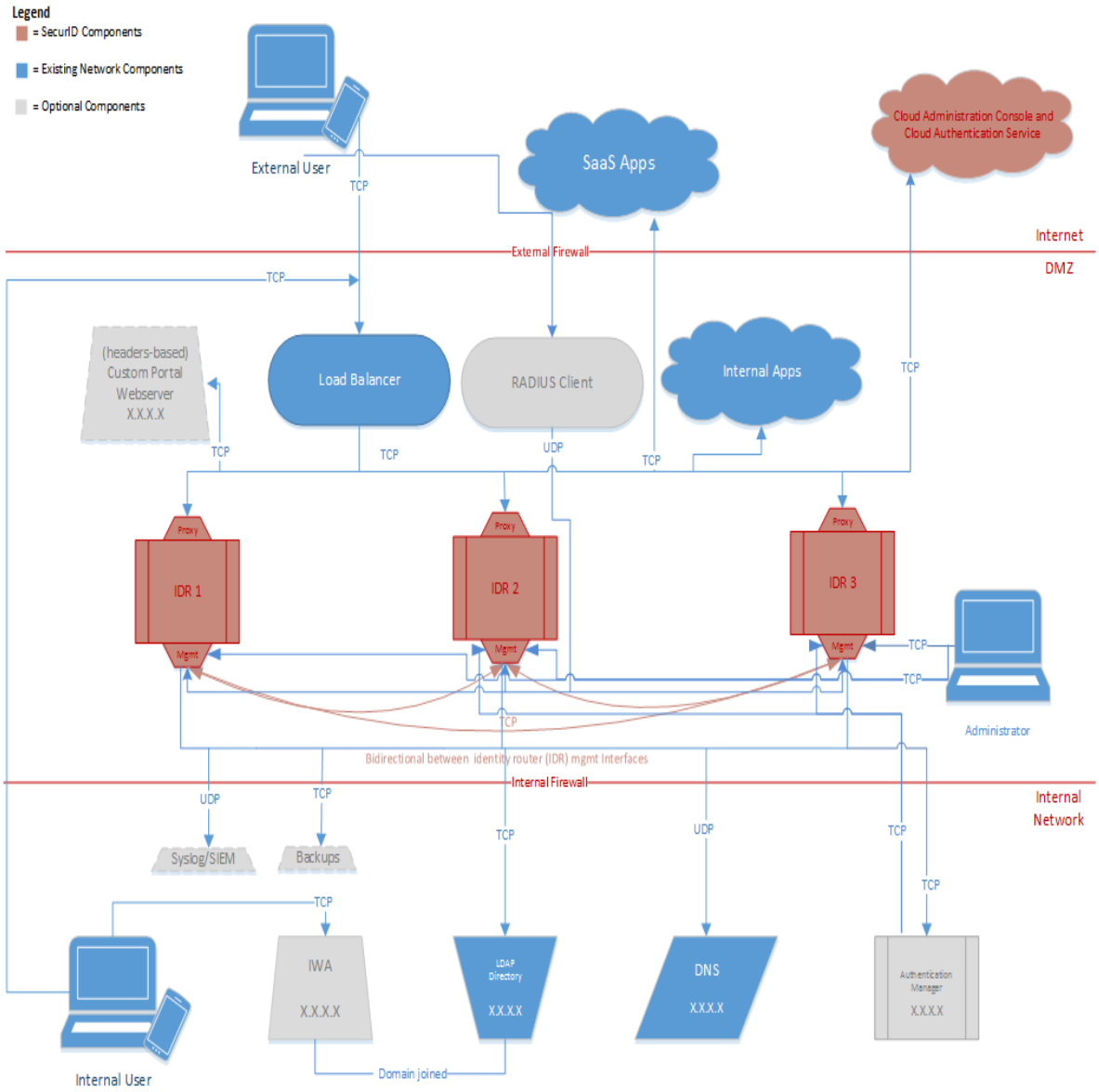
The following diagram illustrates how this deployment can be set up in your network.



SSO Agent Deployment

The SSO Agent deployment consists of three identity routers in an active cluster. If up to two identity routers stop responding, users can still access protected applications through the remaining identity routers at reduced capacity. Also, you can add additional clusters based on your requirements.

The following diagram illustrates how this deployment can be set up in your network.



Amazon Web Services Identity Router Deployment Models

To reduce the footprint of the SecurID deployment in your on-premises network environment, you can deploy the identity router in the Amazon Web Services (AWS) cloud.

You can host all of your resources in the AWS Virtual Private Cloud (VPC), or connect your on-premises resources to one or more identity router instances hosted in the VPC. Each resource, including the identity router, can be part of a private or public subnet, or both, depending on connection requirements. If you deploy

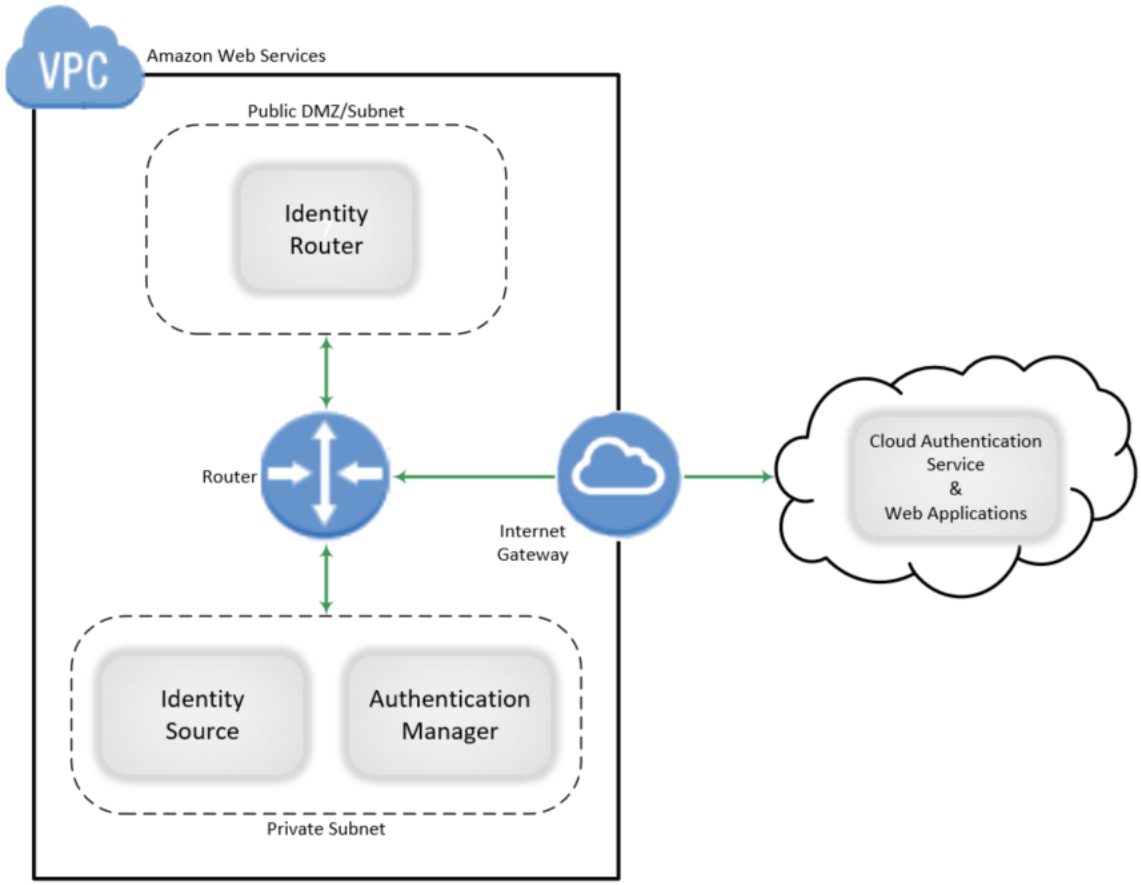
the identity router in a private subnet, you can deploy a NAT load balancer in the public subnet to direct traffic to and from the identity router.

If your deployment requires high availability, you can set up multiple identity routers in the VPC, and configure your Amazon environment so that each identity router is hosted in a different availability zone.

The following sections describe typical AWS deployments. Before setting up the identity router, refer to your AWS documentation and work with your network administrator to determine the appropriate deployment model to connect your organization's cloud-based and on-premises network resources.

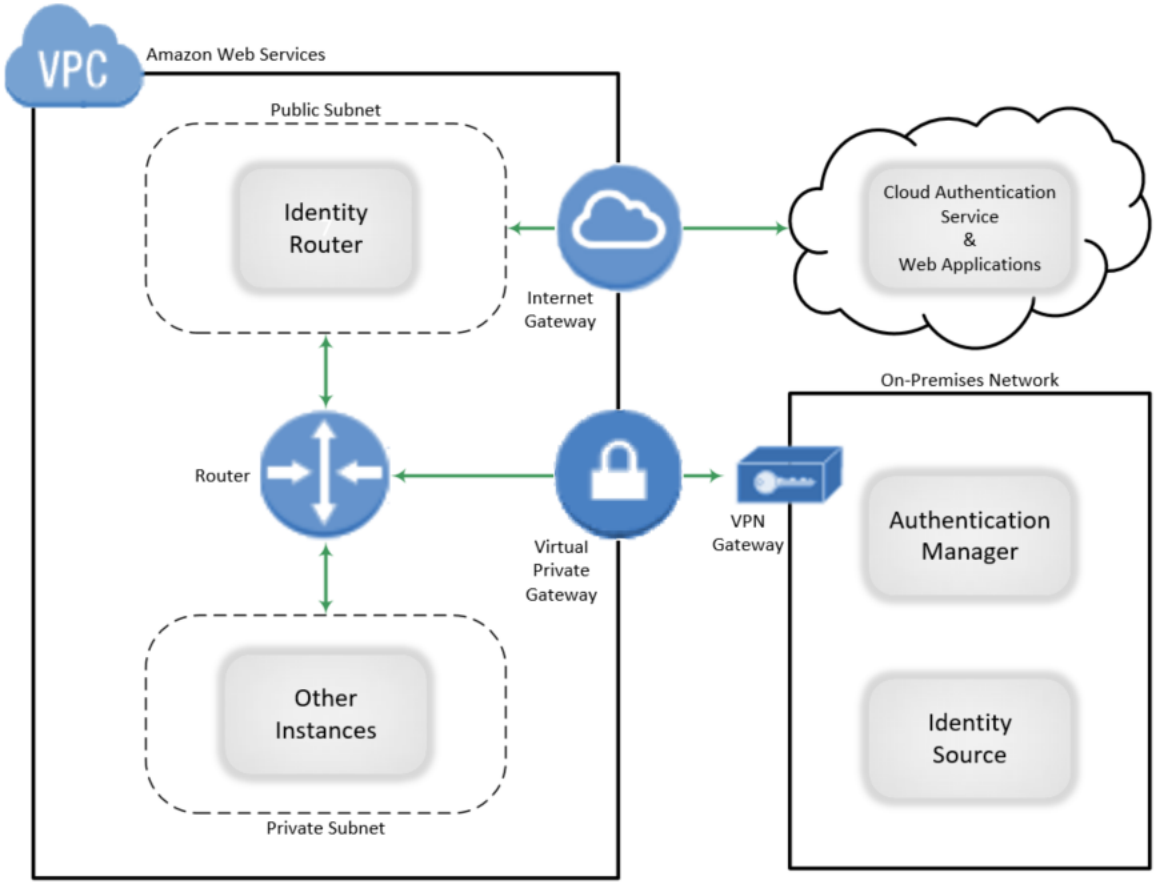
Full Cloud Deployment

In a full cloud deployment, all of your network resources are deployed in the VPC. A router in the VPC manages traffic between public and private subnets containing the identity router, identity sources, and optional resources such as SecurID Authentication Manager. The resources within the VPC communicate with the Cloud Authentication Service and protected web applications through an internet gateway.



Hybrid Cloud Deployment

In a hybrid cloud deployment, the identity router is deployed in the VPC either alone or in addition to other cloud-based instances, but resources such as identity sources and SecurID Authentication Manager are hosted on your on-premises network and connected to the VPC through a VPN gateway or AWS Direct Connect. As in the full cloud deployment, a router in the VPC manages traffic between subnets, and the identity router contacts the Cloud Authentication Service and web applications through an internet gateway.



High-Level Authentication Flows for the Cloud Authentication Service

This topic describes:

- High-Level Authentication Flows for Relying Parties below
- High-Level Authentication Flow for RADIUS for the Cloud Authentication Service on page 11
- High-Level Authentication Flows for the SSO Agent on page 12

High-Level Authentication Flows for Relying Parties

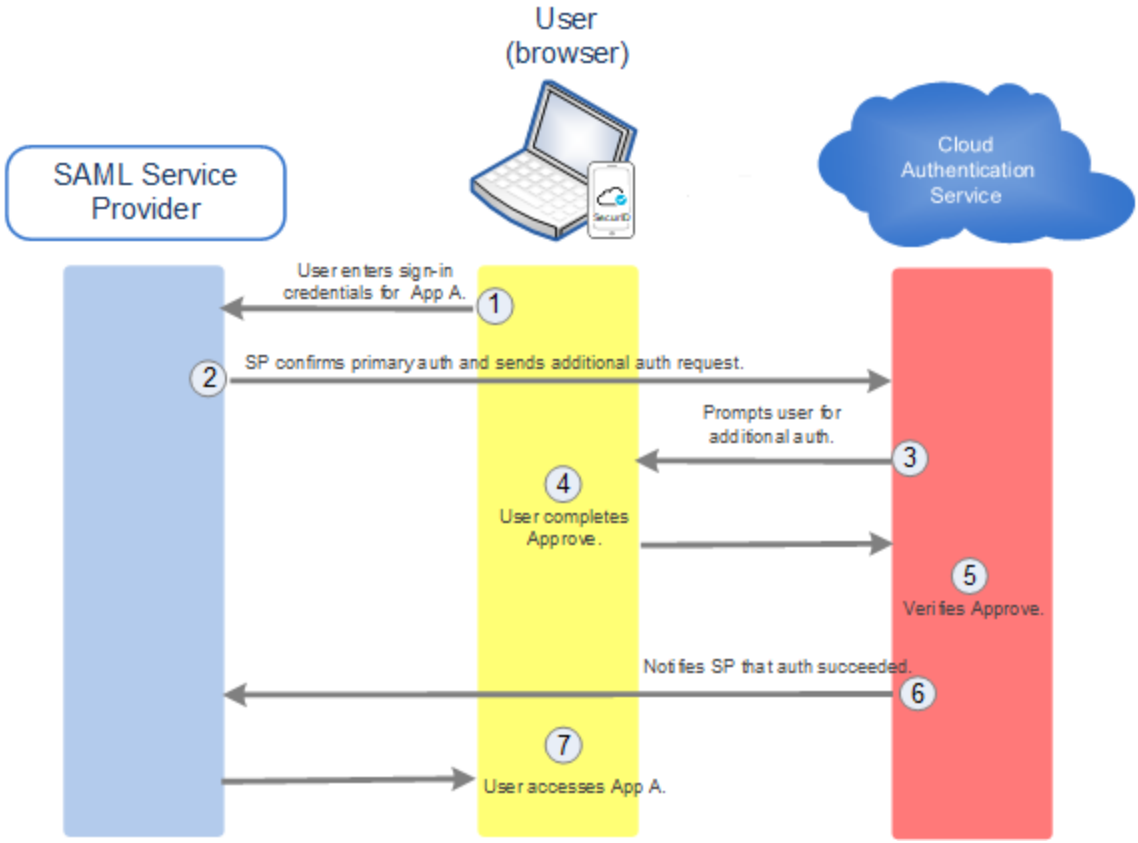
The following sections illustrate how the Cloud Authentication Service authenticates a user for a relying party. A relying party is one of the following third-party SSO solutions or web applications:

- A service provider, using SAML 2.0
- Microsoft Azure Active Directory, using OpenID Connect (OIDC)

Relying parties use the Cloud Authentication Service as the Authorization Server or the identity provider (IdP) for managing authentication.

For service providers, the Cloud Authentication Service can manage only additional (step-up) authentication or both primary authentication (for example, user ID and password) and additional authentication. For Azure Active Directory, the Cloud Authentication Service can manage only additional authentication.

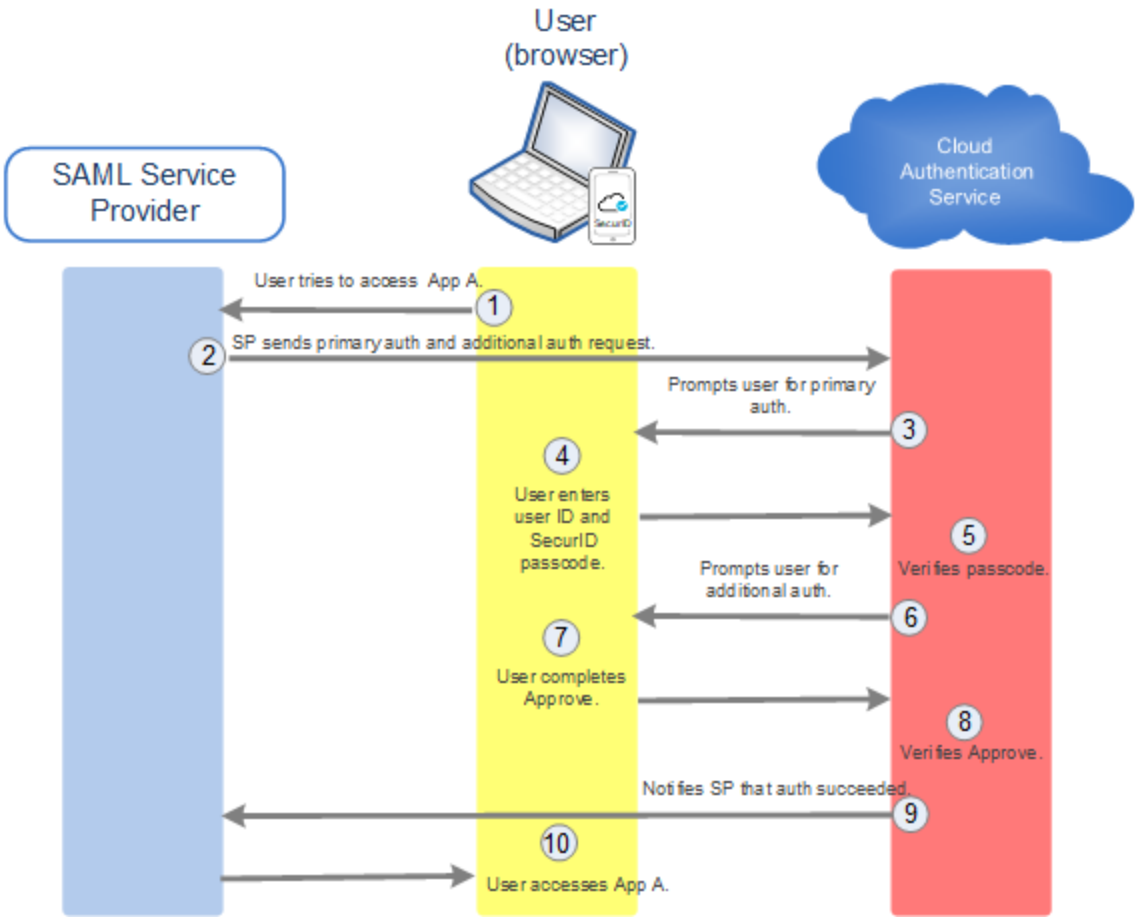
Example: Relying Party Primary Authentication and Cloud Authentication Service Additional Authentication



In this example, a SAML service provider manages primary authentication and the Cloud Authentication Service manages additional authentication. The administrator has configured an additional access policy that requires Approve or Authenticate Tokencode.

1. The user enters sign-in credentials (for example, user ID and password) to access App A (the SP).
2. The SP confirms the user's credentials and sends an additional authentication request to the Cloud Authentication Service.
3. The Cloud Authentication Service determines the additional authentication policy to use and prompts the user for additional authentication (Approve or Authenticate Tokencode).
4. The user completes the Approve authentication method.
5. The Cloud Authentication Service verifies the Approve.
6. The Cloud Authentication Service notifies the SP that authentication for the user ID succeeded.
7. The user accesses App A.

Example: Cloud Authentication Service Primary and Additional Authentication



In this example, the Cloud Authentication Service manages both primary and additional authentication for Apps A and B. For both applications, the administrator has configured SecurID Token as the primary authentication method and has selected an access policy for additional authentication with a Medium assurance level of SecurID Token and Approve.

1. The user tries to access App A (the SP).
2. The SP sends the user's authentication request to the Cloud Authentication Service.
3. The Cloud Authentication Service determines that both primary and additional authentication are required, determines the configured primary authentication method and the access policy for additional authentication, and prompts the user for primary authentication.
4. The user enters user ID and SecurID passcode.
5. The Cloud Authentication Service verifies the primary authentication.
6. The Cloud Authentication Service prompts the user to complete the Approve authentication method.

   The assurance level requires SecurID Token and Approve but because the user completed SecurID Token authentication as part of primary authentication, the Cloud Authentication Service only prompts the user for Approve for additional authentication.
7. The user completes the Approve authentication method.
8. The Cloud Authentication Service verifies the additional authentication.
9. The Cloud Authentication Service notifies the SP that authentication for the user ID succeeded.
10. The user accesses App A.

11. The user tries to access App B (another SP).
12. Steps 2- 9 are repeated.
13. The user accesses App B.

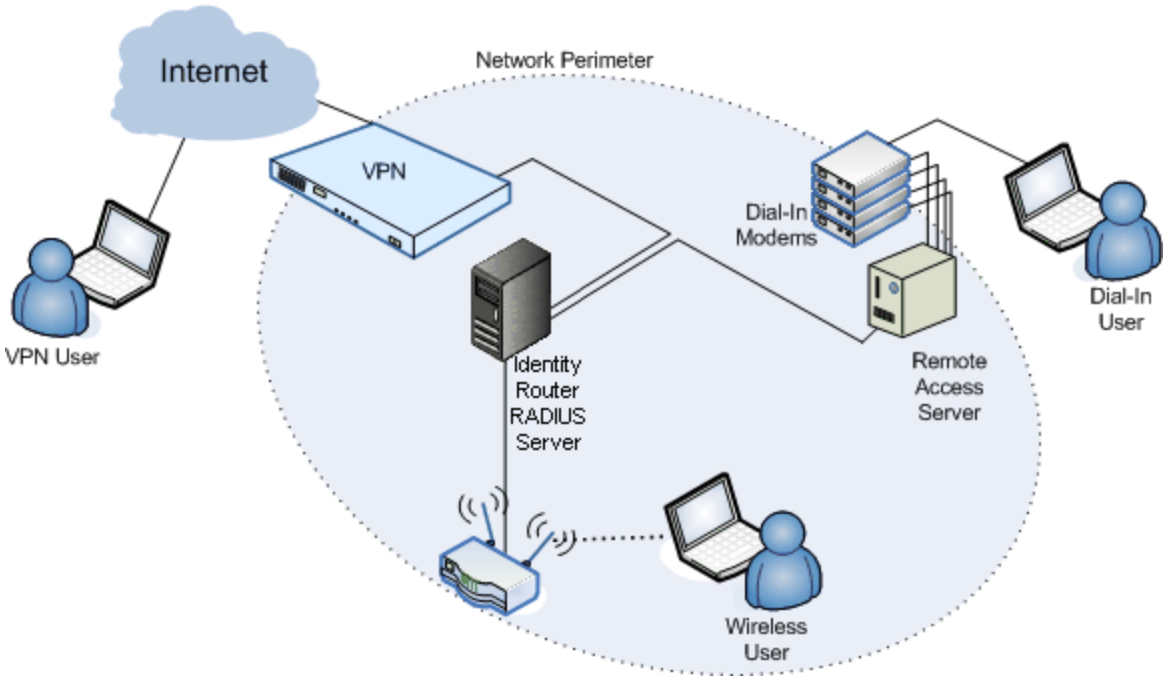
High-Level Authentication Flow for RADIUS for the Cloud Authentication Service

Note: All identity router platforms support RADIUS authentication, except when the identity router is embedded in SecurID Authentication Manager 8.5 or later.

When you protect your network with RADIUS for the Cloud Authentication Service, the authentication process works as follows:

1. The user provides authentication information to a RADIUS client, such as a VPN server or firewall.
2. The RADIUS client sends an Access-Request message to a RADIUS server hosted on an identity router in your deployment. The request provides information about the client and the user, such as:
    - User ID
    - User password (encrypted)
    - Client ID
    - Port ID
3. The RADIUS server validates the client using a password shared between the client and server, known as a shared secret. If the client does not provide the correct shared secret, authentication is not possible.
4. The RADIUS server checks requirements (known as checklist attributes) that must be met for the user to access the resource. Checklist attributes may include:
    - Password
    - Clients through which the user can access a resource
    - Ports on which the user can access
5. The RADIUS server forwards the request to the Cloud Authentication Service.
6. The Cloud Authentication Service accepts, challenges, or rejects the request.
7. The RADIUS server sends one of three responses to the client:
    - Access-Accept. The RADIUS server allows access and returns a set of attributes (known as return list attributes) to the client for session control.
    - Access-Challenge. The RADIUS server returns the additional (step-up) authentication methods the user must satisfy, such as Approve, Authenticate Tokencode, or SecurID Token.
    - Access-Reject. Authentication methods or policy conditions are not satisfied, so access is denied.
8. When authentication succeeds, the RADIUS server sends return list attributes to the client to manage the user session.

RADIUS clients control user access at the network perimeter. The following figure shows how a RADIUS server runs as a service on an identity router and connects to RADIUS clients and other components in a typical deployment.



High-Level Authentication Flows for the SSO Agent

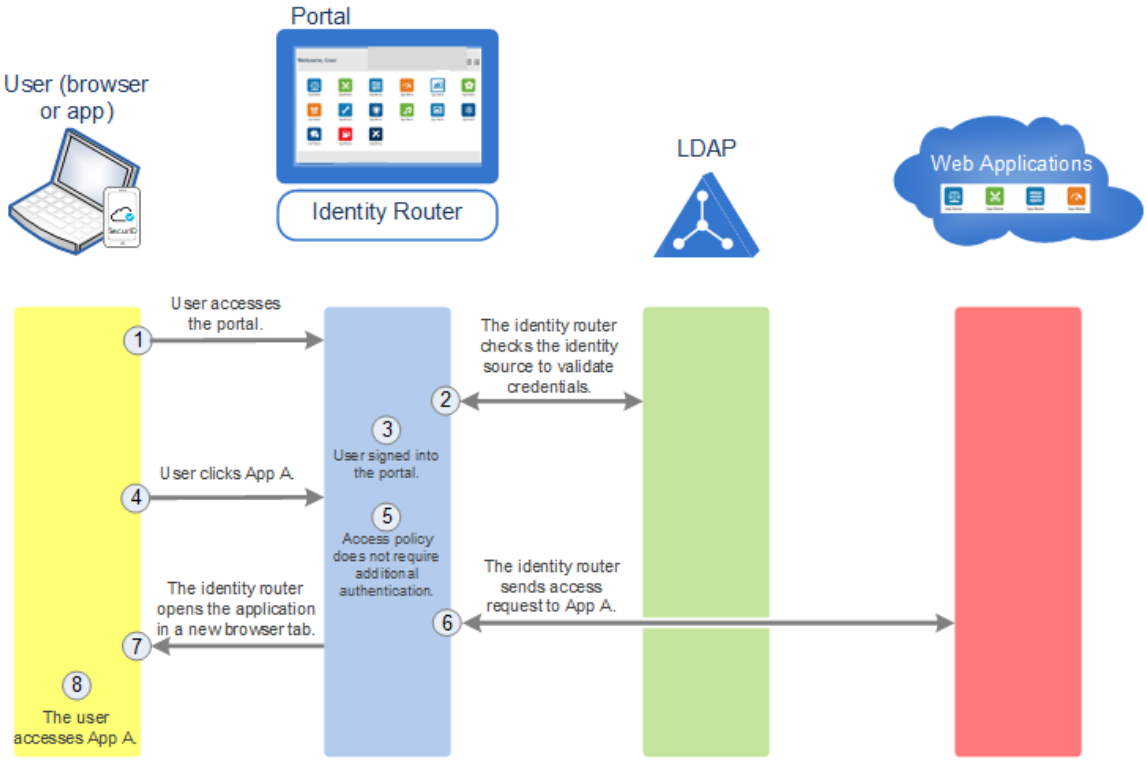
The following sections illustrate how SecurID authenticates a user for applications in a deployment with an SSO Agent. The process flow depends on the following factors:

- If the application requires additional (step-up) authentication after the user accesses the application portal.
- If the user has recently authenticated to another application with similar authentication requirements.

In these examples, the user accesses the applications through the SecurID Application Portal. Depending on your configuration, users can also access the applications through a custom portal or other methods (for example, a bookmark or using the application URL).

Note: All identity router platforms support the SSO Agent, except when the identity router is embedded in SecurID Authentication Manager 8.5 or later.

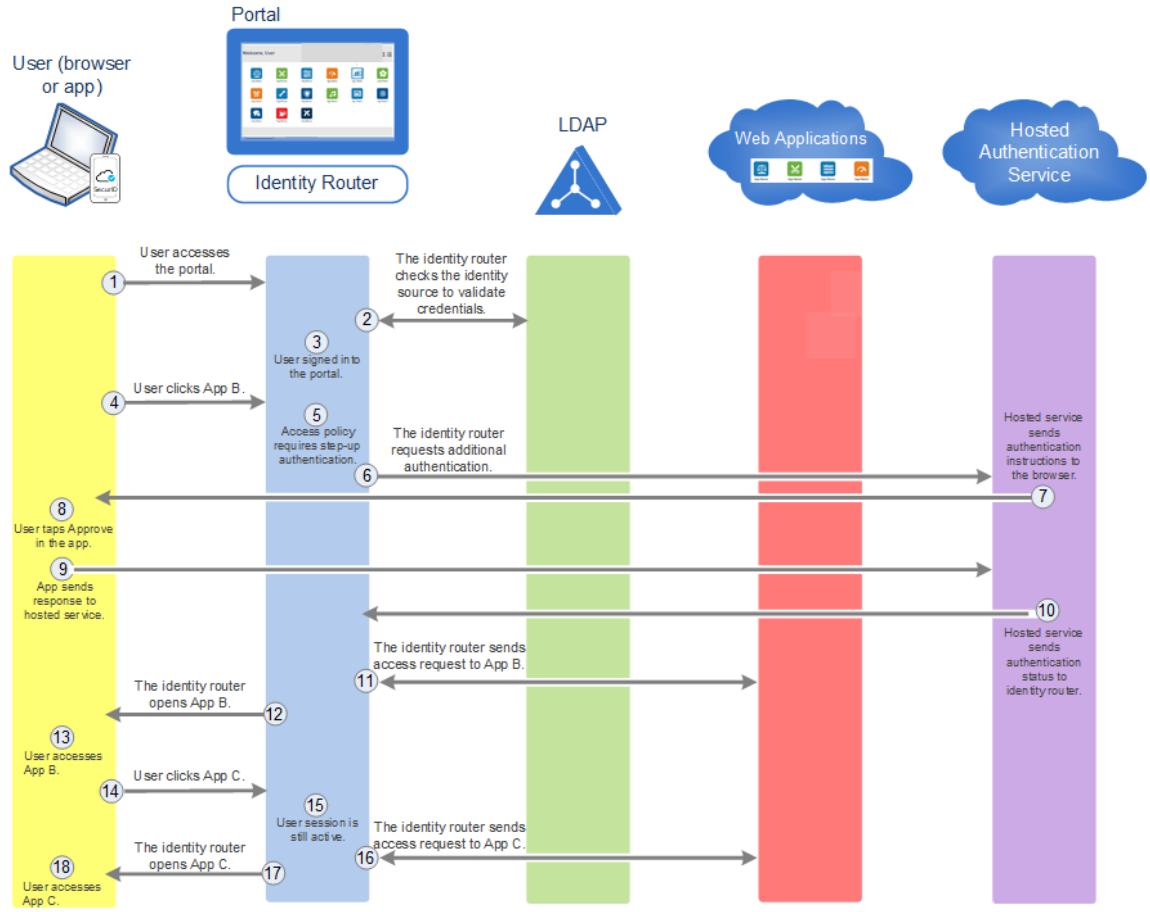
Authentication Flow without Additional Authentication Example



In this example, the company is using the SecurID Application Portal. The administrator has assigned an access policy to App A that does not require additional (step-up) authentication.

1. The user enters sign-in credentials to access the SecurID Application Portal. Or, if the administrator has configured Integrated Windows Authentication (IWA), the user navigates to the portal URL and is automatically signed into the portal.
2. The identity router checks the identity source to confirm the user's credentials and checks the access policies for all applications available to the user.
3. The user is signed into the portal.
4. The user clicks the App A icon to open an app.
5. The identity router enforces the access policy for the application, which does not require the user to complete additional authentication.
6. The identity router sends the access request to App A.
7. The identity router opens App A in a new browser tab.
8. The user accesses App A.

Authentication Flow with Additional Authentication and Single Sign-On Example



In this example, the company is using the SecurID Application Portal. The administrator has assigned an access policy that uses the Low assurance level to App B and App C. (An assurance level defines the authentication methods required to access applications during additional authentication.)

1. The user enters sign-in credentials to access the SecurID Application Portal. Or, if the administrator has configured IWA, the user navigates to the portal URL and is automatically signed in to the portal.
2. The identity router checks with the identity source to confirm the user's credentials and checks the access policies for all applications available to the user.
3. The user is signed into the portal.
4. The user clicks the App B icon to open the app.
5. The identity router enforces the access policy for App B. App B requires additional authentication using the Low assurance level (Approve authentication method).
6. Because additional authentication is required, the identity router sends the request to the Cloud Authentication Service.
7. In a new browser tab, SecurID provides instructions in the browser for the user to follow and sends a notification to the SecurID Authenticate.
8. The user taps Approve in the Authenticator to complete authentication.
9. The Authenticator sends the response to the Cloud Authentication Service.
10. The Cloud Authentication Service sends the authentication status to the identity router.
11. The identity router sends the access request to App B.
12. The identity router opens App B.
13. The user accesses App B.

14. In the application portal, the user clicks the App C icon to open the app.
15. The identity router enforces the access policy for App C. App C also uses the Low assurance level. Because the user's session is still active from authenticating to App B (which uses the same assurance level as App C), the user does not need to provide the additional authentication required by App C.
16. The identity router sends the access request to App C.
17. In a new browser tab, SecurID opens App C.
18. The user accesses App C.

Additional Information

Are you interested in learning more about the Cloud Authentication Service? RSA Link contains all the information that you need to set up your deployment and administer it. The following table provides links in key areas to help you learn more.

Concept	Link
Identity routers	https://community.rsa.com/docs/DOC-54099
Identity sources	https://community.rsa.com/docs/DOC-53989
Authentication methods	https://community.rsa.com/docs/DOC-53973
Assurance levels	https://community.rsa.com/docs/DOC-53965
Access policies	https://community.rsa.com/docs/DOC-53992
Protecting RADIUS clients	https://community.rsa.com/docs/DOC-75832
Protecting SAML applications, third-party SSO solutions, or Microsoft Azure Active Directory without the SSO Agent	https://community.rsa.com/docs/DOC-75848
Protecting SSO Agent applications	https://community.rsa.com/docs/DOC-54137
Administrative roles	https://community.rsa.com/docs/DOC-54059
End-user rollout	https://community.rsa.com/docs/DOC-75817
Integrating with SecurID Authentication Manager	https://community.rsa.com/docs/DOC-84669

Trademarks

Intellectual Property Statement

Open Source License