Forcepoint ONE and RSA SecurID Configuration Guide

Forcepoint

Forcepoint ONE and RSA SecurID

This guide walks through the steps to set up RSA SecurID as an external identity provider to be used with Forcepoint ONE.

RSA SecurID Introduction

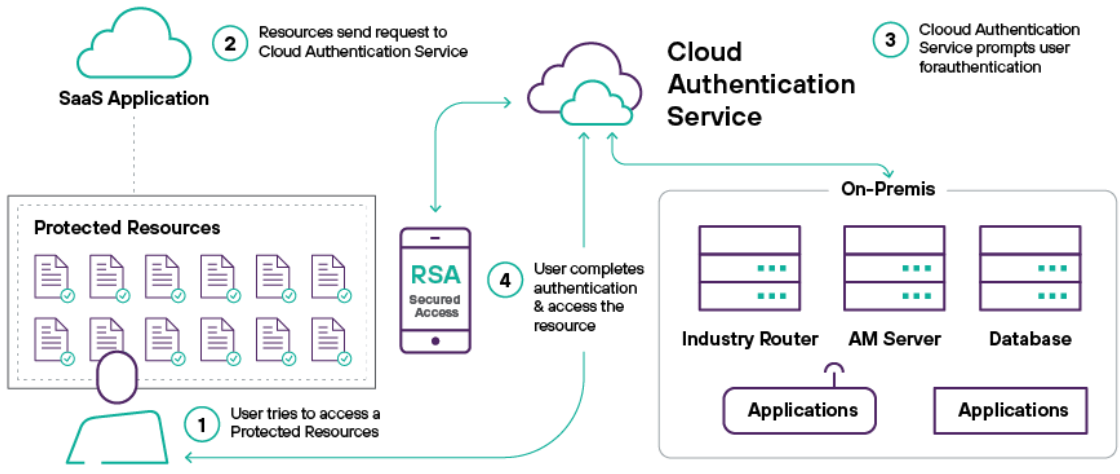
The RSA Cloud Authentication Service is an access and authentication platform with a hybrid cloud architecture. It enables your company to control how users access resources with centralized access and authentication policies and can accelerate user productivity with Single Sign-On (SSO).

With the RSA SecurID solution, we can have three ways to authenticate users.

Applications	Relying Parties	RADIUS Clients
Configure authentication and single sign-on for applications using the SSO service.	Configure authentication for applications and third-party SSP solutions using the Cloud Authentication Service.	Configure authentication for RADIUS clients such as VPNs.

The Cloud Authentication Service helps protect SaaS and on-premises web applications, third-party SSO solutions and on-premises resources accessed via RADIUS. In our case, we will be focused on relying parties.

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 set up through risk analytics, based on user characteristics such as past behavior, authenticators previously used for authentication and other factors.

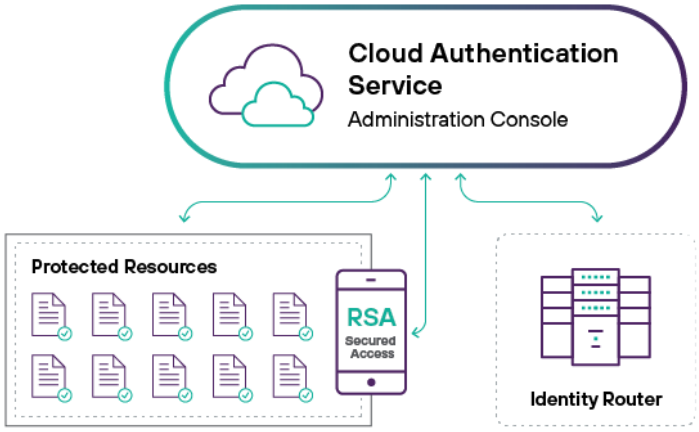


This graphic illustrates how the Cloud Authentication Service works

Cloud Authentication Service Components

A Cloud Authentication Service deployment consists of four main components:

1. The Cloud Authentication Service (which is both the name of the managed server and the name of the set of components)
2. The Identity Router
3. The Cloud Adminstration Console
4. The SecurID app installed on user devices



Cloud Authentication Service

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

Identity Router

The Identity Router enforces authentication and access for users of protected resources:

→ Identity Sources

→ Authentication Manager

→ Cloud Auth Service

→ Cloud Administration Console

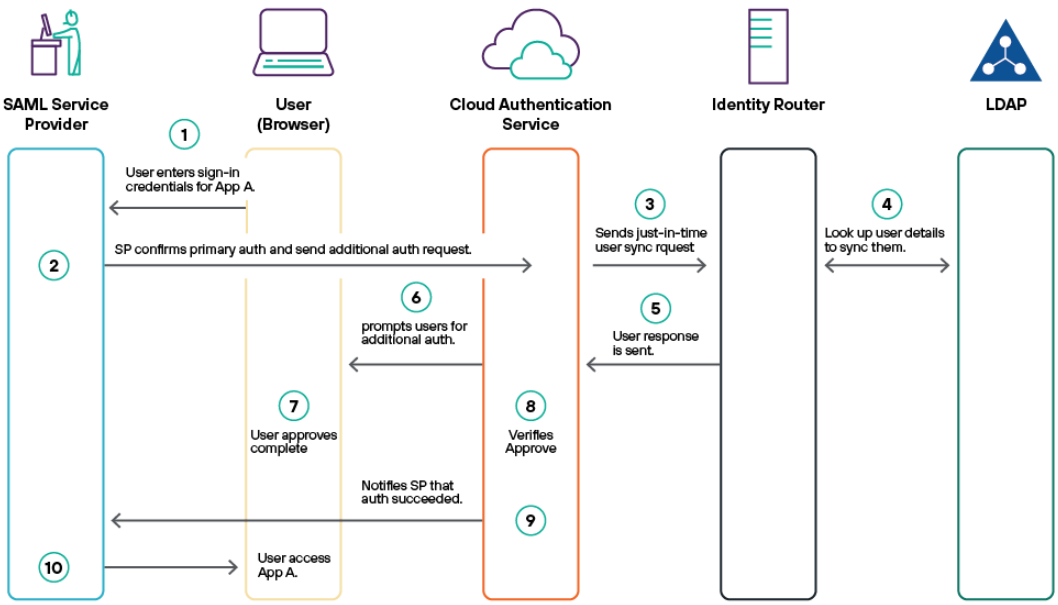
Cloud Administration Console

The Cloud Authentication Service component contains a hosted, multi-tenant Cloud Administration Console that admins use to perform setup and daily management tasks.

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 dentity 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



This is a high-level description of how RSA SecurID works normally in customer environments.

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 sends a just-in-time (JIT) synchronization request to the identity router.
4. The just-in-time (JIT) update/create request is processed to synchronize the users from LDAP to the cloud database.
5. The identity router sends the user response to the Cloud Authentication Service.
6. The Cloud Authentication Service determines the additional authentication policy to use and prompts the user for additional authentication (Approve or Authenticate OTP).
7. The user completes the Approve authentication method.
8. The Cloud Authentication Service verifies the Approve.
9. The Cloud Authentication Service notifies the SP that authentication for the user ID succeeded.
10. The user accesses App A.

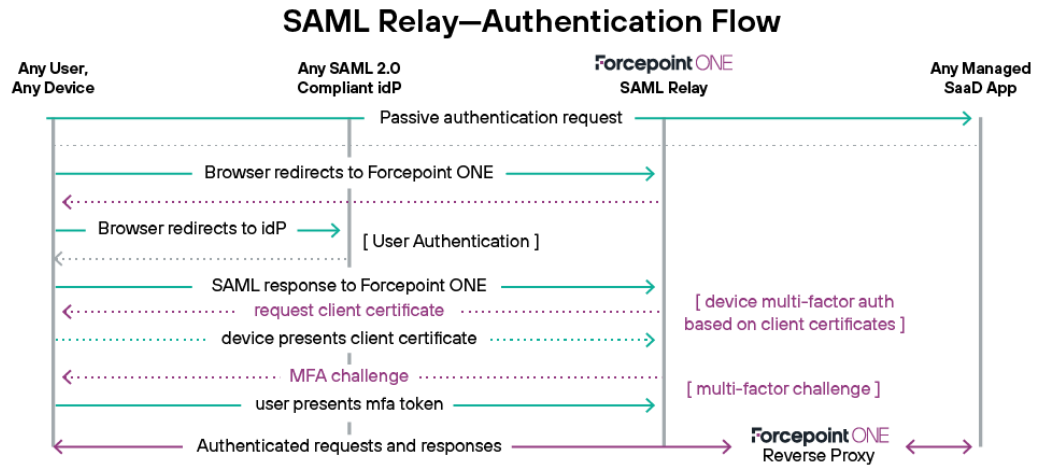
Forcepoint ONE

When we integrate Forcepoint ONE, the flow will be slightly different. A new hop must be introduced between the service provider and the identity provider. This new hop is Forcepoint ONE, which will be introduced between the SaaS app and RSA SecurID identity provider.

As authentication is a key function of security, Forcepoint ONE offers three modes of authentication:

1. SAML relay with a third-party IdP
2. SAML relay with Forcepoint ONE built-in IdP
3. SAML ACS proxy with a third-party IdP

In this guide we will use the first option**: SAML relay** is the most common method to integrate Forcepoint ONE with a third-party IdP. With SAML relay, Forcepoint ONE is configured as the IdP for your tenant in the SaaS application, but in addition, the third-party IdP is configured as the IdP for Forcepoint ONE as a service provider.



1. The SaaS application recognizes that Forcepoint ONE is the IdP for the customer domain.
2. Forcepoint ONE knows that the IdP for this application tenant is RSA SecurID and sends a new redirect message to the user browser that redirects the user to RSA SecurID.
3. The user is redirected to the RSA SecurID login page, where the user enters their credentials for authentication. At this point we can fully take advantage of all the security features to control user access.
4. Once RSA SecurID authenticates the user, it sends a POST request message to the user browser which redirects the user back to Forcepoint ONE.
5. Forcepoint ONE first validates the authenticity of the SAML response.
6. Forcepoint ONE sends a POST request to the user browser, with the SAML authentication response from Forcepoint ONE to the SaaS.

RSA Cloud Authentication Setup

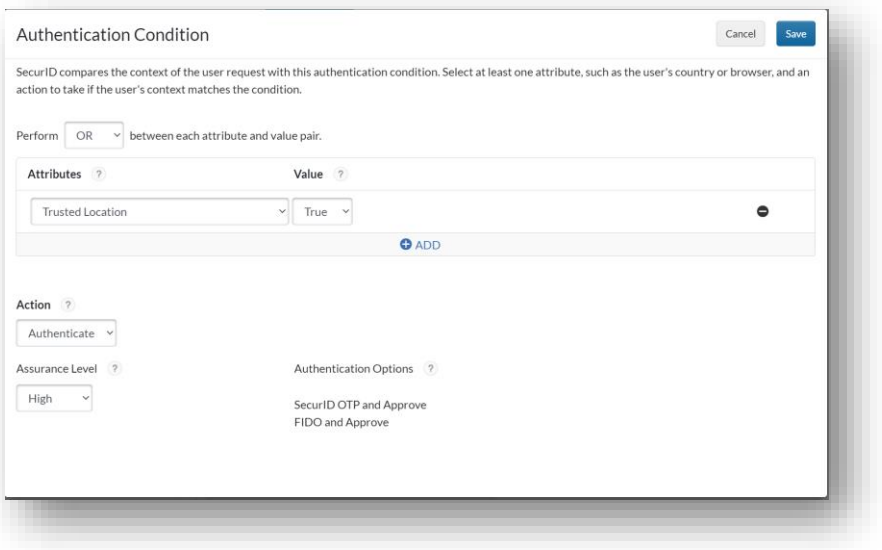
In the next section we are going to show how to set up RSA SecurID as an IdP in Forcepoint ONE. Make sure to keep open “the two configurations” portals as we will need to fill fields in on each side during the configuration.

Prerequisites on SecureID
Before configuring integration between Forcepoint and RSA, we need to be sure that some work has been done on the RSA side.

Identity Router
The Identity Router is an on-prem component needed to speak with on-prem databases and then with the cloud service. It plays a key role in the RSA hybrid depolyment. Log in to the SecurID portal and check if an Identity Router is configured and working properly.

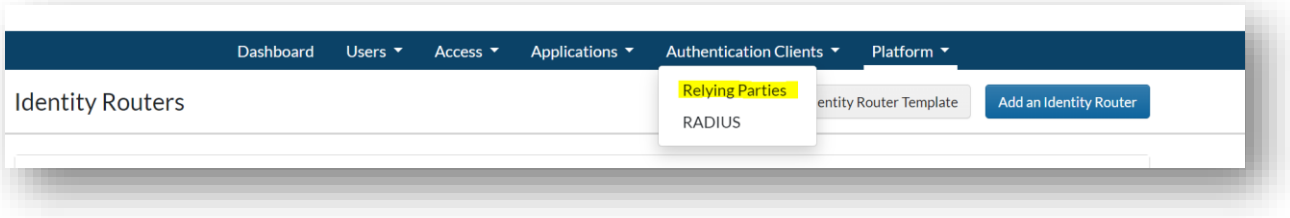
Identity Source
Make sure that an Identity Source exists and is well configured. An Identity Source contains an organization’s users. Each source may be an LDAP/on-premises AD instance, a Local directory in CAS or an external source managed by the SCIM API. The identity source is important as users are not immediately available in the cloud service.

Policy
Make sure that a policy is also defined. The policy will be used to choose the identity source and to enforce rules upon user authentication (conditional access, target users, MFA). For example, you can set up MFA for unstrusted locations, based on risky users, for specific countries or for other attributes.

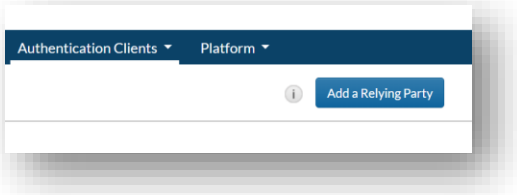


After these steps are complete, we can address the main configuration. The next step is defining Forcepoint ONE as a service provider in the SecurID cloud portal.

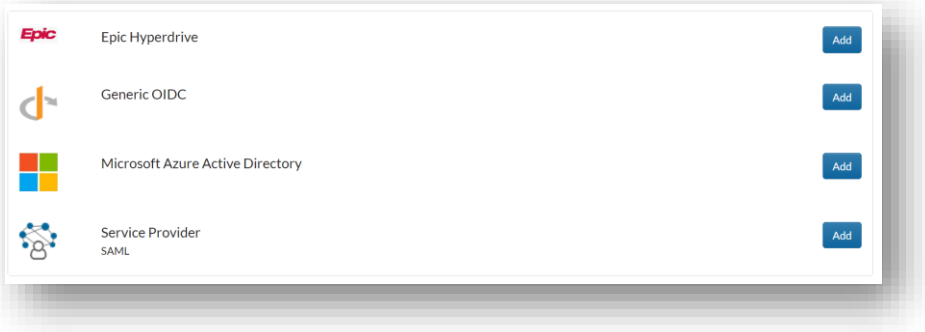
Select the **Authentication Clients** > **Relying Parties** menu item at the top of the page.



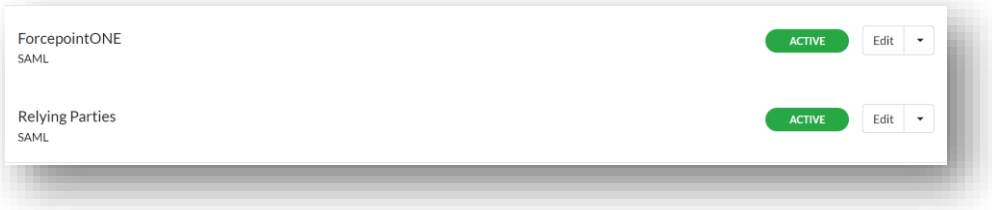
Click the **Add a Relying Party** button.



Then select **Relying Party** and choose **Service Provider SAML.**



We will need to define the relying party that we will call Forcepoint ONE.



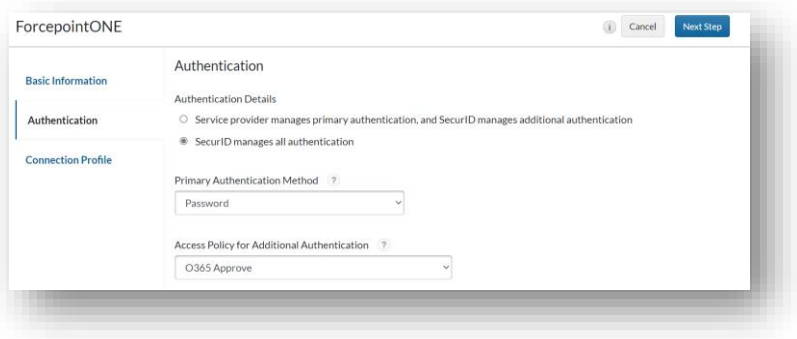
Before continuing the configuration, make sure to open Forcepoint ONE on a second page.

When we add the new party, we will have to define three main topics:

- Basic information
- Authentication
- Connection profile

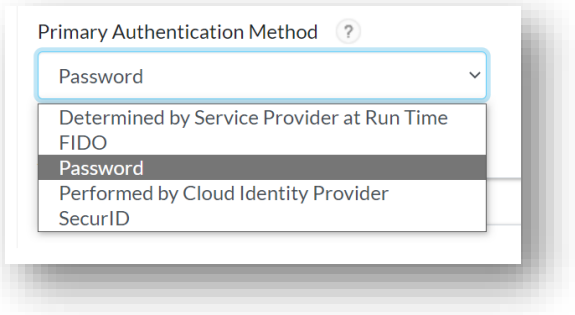
Basic information: Here we must add the name and description.

Authentication: Here we need to define how the authentication is going to take place. In this case we want to set up the first authentication factor and the policy that we have set up earlier.



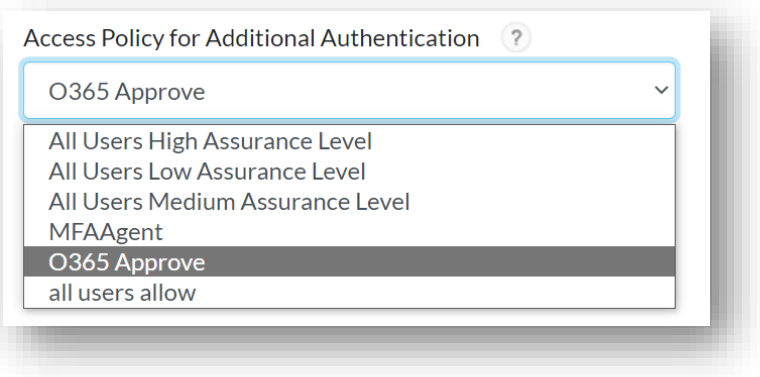
Authentication details: Use **SecurID Managed All Authentication** if you want the Cloud Authentication Service to manage both primary and additional authentication. In our case, Forcepoint ONE will rely on SecurID to authenticate users for both authentication factors.

In the next step we have **Primary Authentication Method.** Remember this is the first factor of authentication, and it can be either password or SecurID. Primary authentication (for example, password) is the initial identifying information of the user that is requesting access to the application.



In the **Access Policy for Additional Authentication** drop-down list, select the access policy to apply to SAML requests from this SP if primary authentication succeeds. The policy has been defined previously, so you only need to select it from the menu.

Choose the option appropriate for your company security policy as outlined in the previous section. A default policy may also be used.

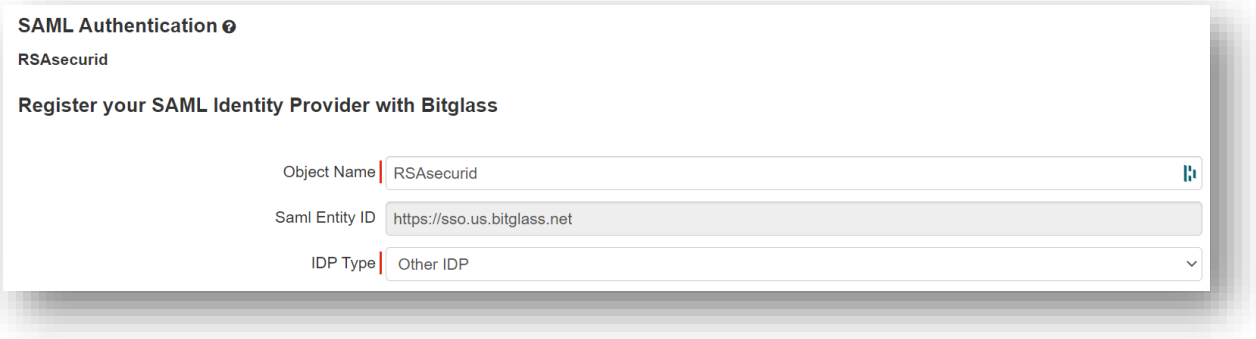


Connections profile: This is in the Forcepoint ONE console. In here we need to set up parameters that are important to make RSA and Forcepoint work together.

This integration supports external SAML 2.0 user authentication using an already deployed IAM product which provides Single Sign-On (SSO). Authentication requests for users in the configured domain will be sent to the Identity Provider (IdP). The IdP will need to be configured to receive and respond to these requests from Forcepoint ONE.

The Forcepoint domain will need to be configured to send the requests to the correct login, logout and password change URLs. The first is the **Assertion Consumer Service** where the assertion is sent by the IDP once the user is authenticated.

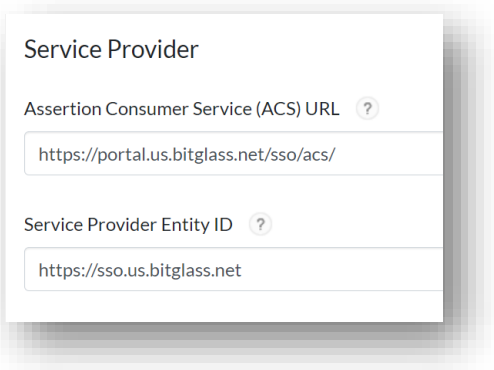
The second is the **Entity ID** that identifies the SP. Typically this is a URL, but a URL is not required. This must be taken from the Forcepoint ONE portal. This is why it's best to keep both portals open. In this case, switch to the Forcepoint portal, go to **Protect** > **Common Objects** > **Extern IDP** and click the green plus icon once the IdP is added.



Please note that in the case that other IdPs already exist, the URL will be slighty different, with an identifier appended at the end of the URLs like: https://saml.us.bitglass.net/uf1GW8xk0ttcsA==

Copy the Entity ID in the recently added configuration.

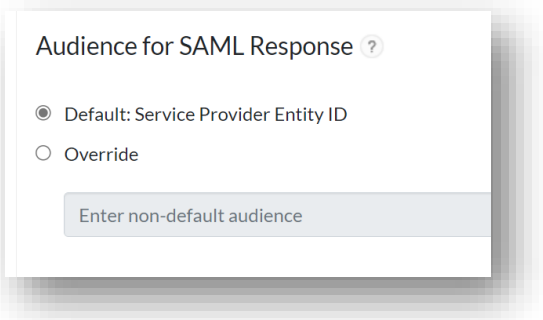
Fill in the URL for the Assertion Consumer Service (ACS) on the SP where the SAML response is posted. The SP ACS endpoint accepts SAML responses with assertions, validates assertions and grants users access to the application.



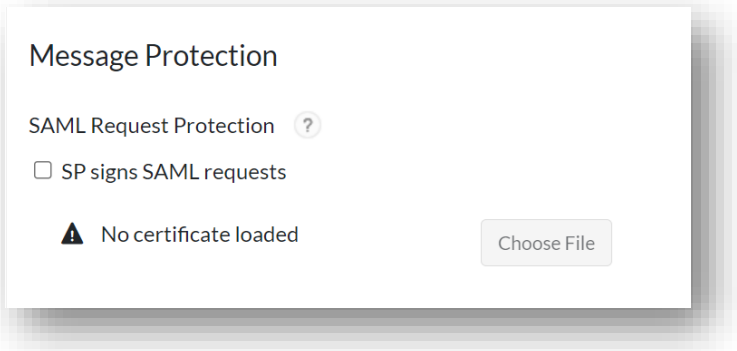
Take into consideration that previous URLs are different for trial and production environments and use the appropriate ones.

Let's continue to the SecurID portal.

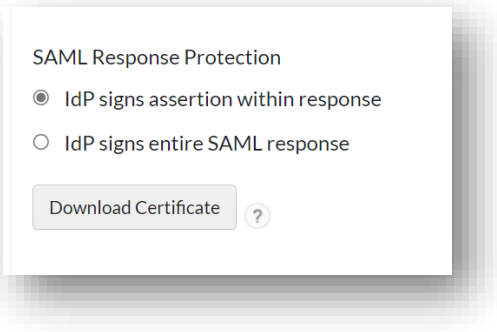
Audience for SAML Response: Specify the Audience string to include in the SAML response. You can select the Default Service Provider Entity ID or specify a different Audience in the Override field.



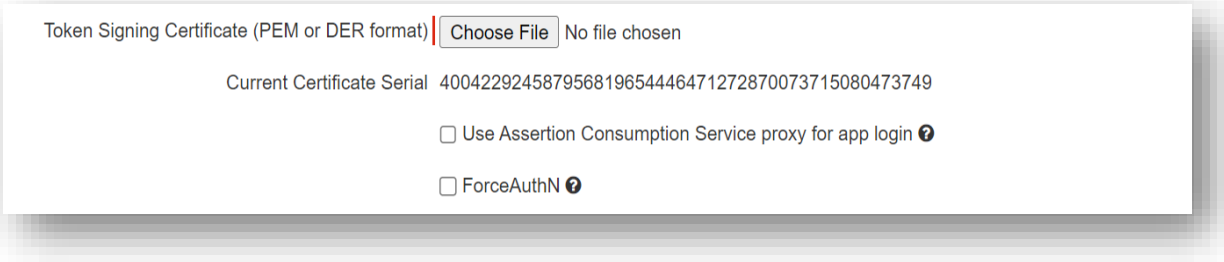
Message Protection: (Optional) If the SP is configured to sign the SAML request, select "SP signs SAML request" and click **Choose File** to load the SP certificate. Eventually for security concerns, we can enable SP request signing: In this case. SecurID will sign the message with the public key from Forcepoint ONE (in such a case we need to upload a certificate).



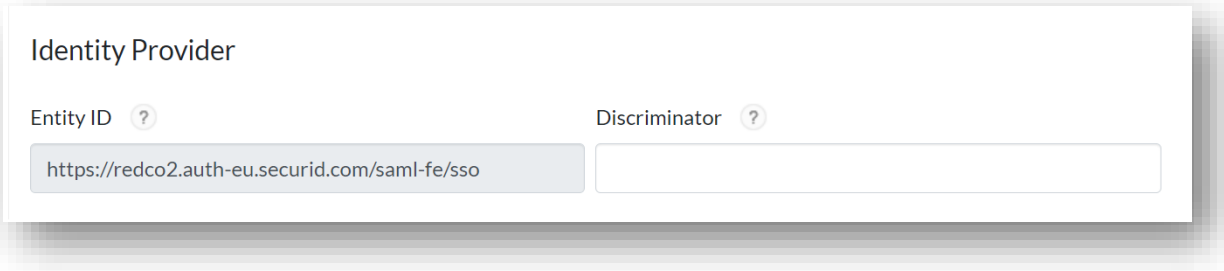
The SAML answer is signed. In this case, make sure to download the certicate from SecurID and upload it to Forcepoint ONE.



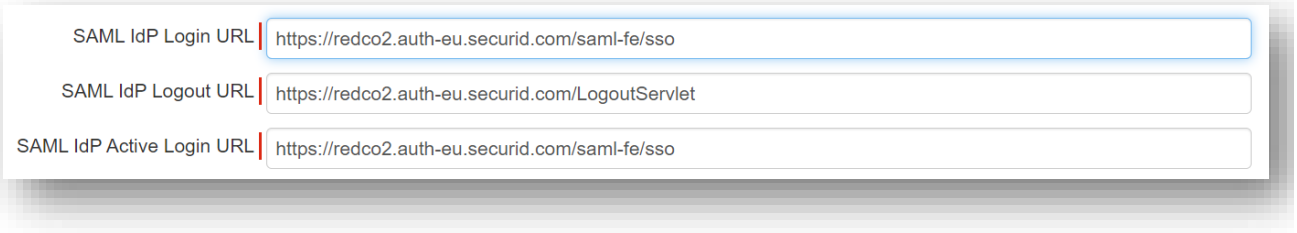
Once you have downloaded the certicate switch to Forcepoint Portal, from within the IDP configuration browse to the certificate and upload it.



Go back to the SecurID portal and click on **Advanced Feature,** then copy the identity provider URL



and copy it in the **SAML IdP Login URL** in the Login/Logout/Active Login as in the image below.

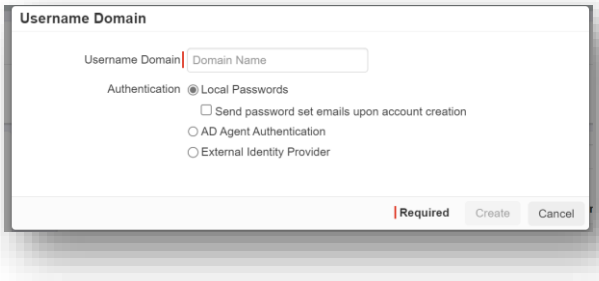


In this case, we have used our own RSA SecurID tenant, but this must be replaced with your own. Once done, save and finish on both SecurID and the Forcepoint ONE portal. The integration with the IdP should now be ready.

How to Use the New IdP

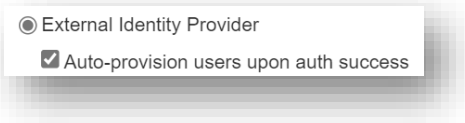
Now we must associate a domain to the new IdP that SecurID just created. We can provision as many email domains as you wish to add into the Forcepoint ONE system. Every email domain that you wish to use within Forcepoint ONE must be configured, along with a corresponding authentication type for users logging in with email addresses in that domain.

In our case, we need to associate the domain with the RSA SecurID. In the Forcepoint ONE portal, move to IAM, then “users and groups” and add a new domain. The domain is the same domain used for the identity source, which needs to be associated with the new IdP just configured.



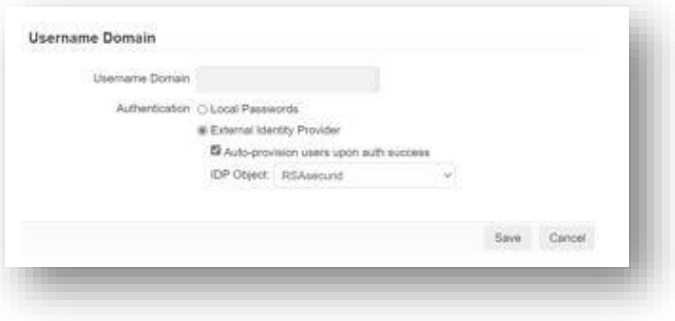
- Type your domain name
- Choose External Identity Provider
- Pick “RSA SecurID,” which we just defined

For testing, please also select auto-provisioning. We will see later how to set up users in the next session since this topic must be approached directly.



Access the Forcepoint ONE Portal and under IAM click the domain associated with the new IdP, RSAsecurid.

Click the domain and examine the options.



The next step is to create a policy for the web, sanctioned apps or ZTNA depending on your specific use case(s). All three functions will be taking advantage of the RSA SecurID solution.

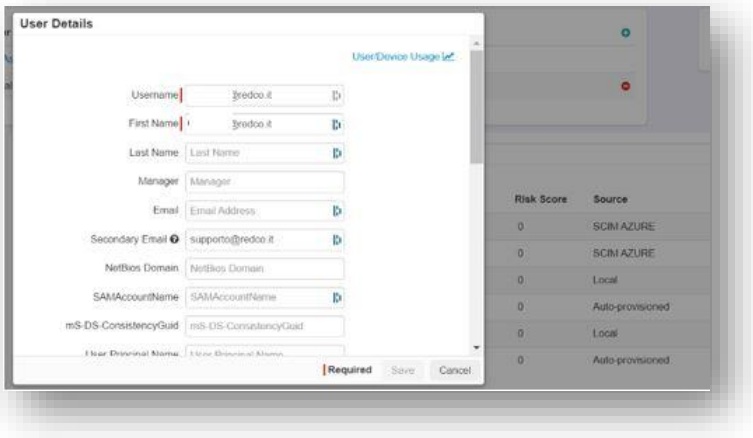
User Provisioning
Prior to an end user being able to use Forcepoint ONE, the user must exist within the portal under the People tab. There are three primary ways users can be imported/created: the Active Directory Synchronization agent (AD Sync), SAML auto-provisioning and/or config REST API.

For test purposes, we can initially set up auto-provisioning for users with the “Auto-provision upon auth success.” This is often useful during a POC/trial or pilot. Doing this will create a new user after a successful authentication.

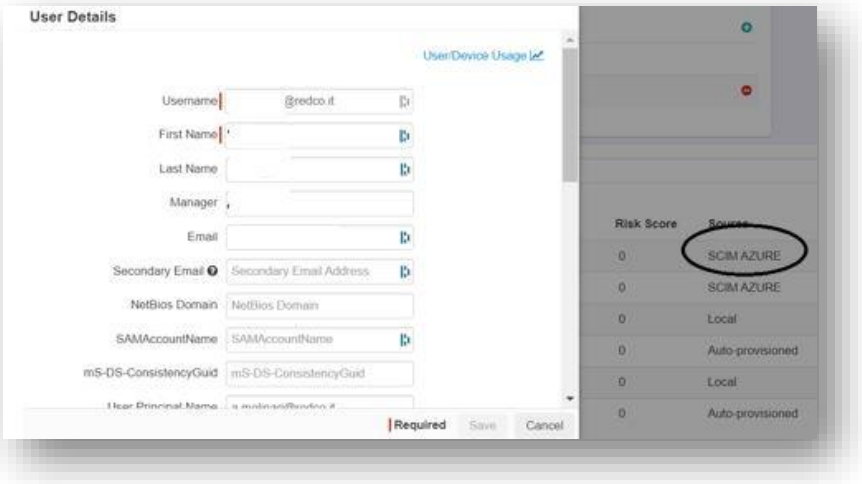
This is not usually feasible in a normal production environment, as group and OU membership details may not be available for users that are auto-provisioned. In this case we need something that will synchronize users from the identity source to Forcepoint ONE.

SecurID is not supported for users provisioning to Forcepoint ONE in the same way we do for Okta or AzureAD. Usually, customers with RSA have already configured an Identity Router to use AD as the primary identity source. For such environments, we have two main options.

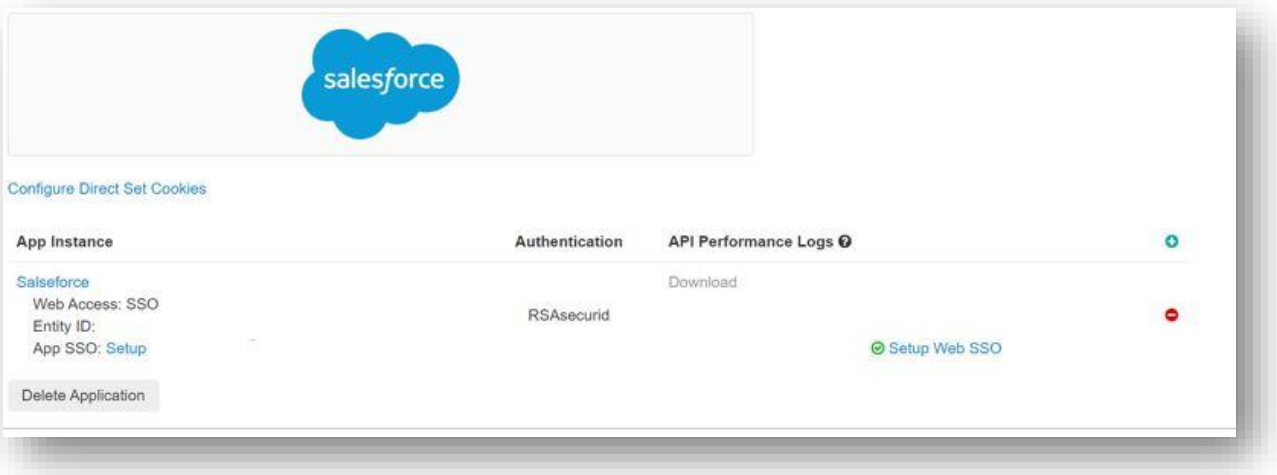
Option 1:
We know that Forcepoint supports integration with Active Directory using software called AD Connectors. This integration supports automatic provisioning and deprovisioning of users, as well as synchronization of user group membership changes made in Active Directory (AD). To set up directory sync, you need to deploy the Forcepoint ONE AD Connector. Select groups and organizational units (OUs) which will be used as the source for synchronizing user and group membership change. The synched groups/OUs can also be used in policy rules for security enforcement.



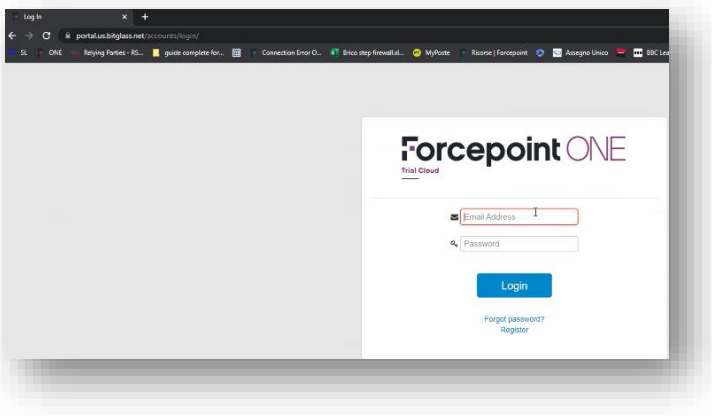
Option 2:
Forcepoint ONE supports SCIM for provisioning users from Azure into Forcepoint ONE. Customers with AD will likely already have a sync in place to send on-prem user information to AzureAD, for users accessing cloud apps. We can use SCIM in this scenario. To set up SCIM, you will need to first set up an OAuth token (see the OAuth guide page for more info) and then create an app inside of Azure using the unique key that was generated.



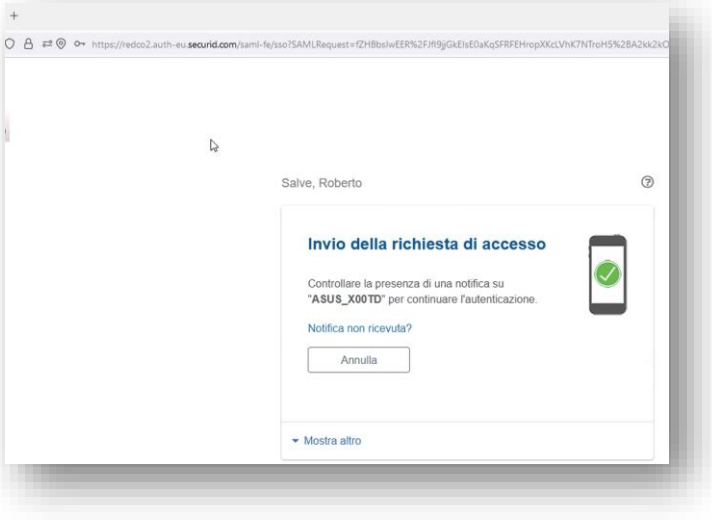
Add a Service Provider
Now that we have added Forcepoint ONE as SP in the SecurID portal, we need to add a new SP in the Forcepoint ONE configuration. To do that, go in to **Protect** > **Add Apps** > **Managed App.** Make sure to add SSO for the domain.



The configuration of the SP, clicking on “Setup Web SSO,” is done according to the best practice you can find in the documentation. Let’s try **SaaS Access** when the user accesses the portal/workspace.



Once the username is entered, the user will be redirected to RSA and a login pop-up will be displayed.



The user will add a username and password (first factor), and the second factor will be sent to the user via the RSA application.

Web Access

Regarding web access, nothing additional must be done. Once the user is authenticated through the RSA portal, they can start web browsing using the policy assigned to their group.

ZTNA

ZTNA Access follows standard documentation for configuration for both HTTP and non-HTTPS transactions. We tested both agentless access and agent-based access. For agentless access, the user experience is similar to that seen for Saleforce. For agent access, the user experience is similar to web access.

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP ONE Integrated and RSA SecurID Configuration Guide] 18Oct2023