SafeNet Authentication Service

SAML Authentication Quick Start Guide

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Number: 007-012471-001, Rev. J

Release Date: January 2018

Contents

Preface

This guide describes the application, configuration, and use of SAS as a SAML Identity Provider (IdP) to Service Providers (SPs); including:

- How to configure a Virtual Server to be an IdP.
- How to use SAML Provisioning Rules in SAS and LDAP to automatically enable SAML authentication for users to one or more designated SPs, such as Google Apps.
- How to customize login and other pages presented to the user during SAML authentication.
- Examples of SAML configurations for Google Apps and Salesforce.

Audience

This guide is intended for SAS administrators responsible for how authentication services are delivered and responsible for configuring SAS to reflect the internal business processes, service level agreements, and management hierarchy.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

Region	**Telephone number** (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1-410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421
Japan	0066 3382 1699
Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608

1
SafeNet Authentication Service and SAML

SafeNet Authentication Service adds SAML to the authentication options available to cloud subscribers.

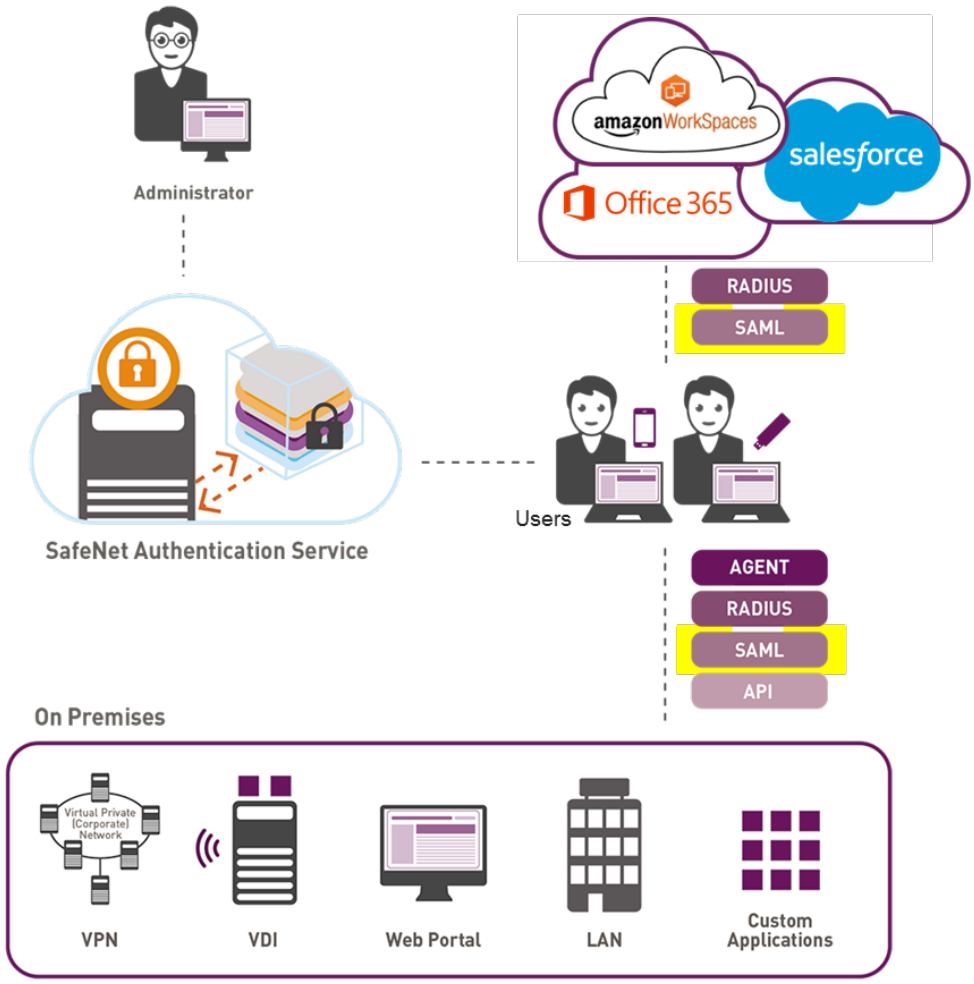


Figure 1: SafeNet Authentication Service

This means that enterprises can:

- Extend strong authentication beyond the enterprise perimeter to include cloud apps such as Salesforce and Google Apps.
- Use SAS to protect internal applications such as SAP and others that support SAML authentication.

- Use SAS with perimeter devices, such as SSL VPNs, that support SAML authentication.
- Enable authorized users to authenticate into cloud apps in a simple, familiar, and consistent manner using the same token/authentication method they use for VPN and other traditional access.
- Automate cloud app authorization.
- Use SAS reporting to audit all user authentication activity, including authentication into cloud apps.

NOTE: This document describes Service Provider (SP) initiated workflows only.

A Brief Introduction to SAML

SAML (Security Assertion Markup Language) is an Extensible Markup Language (XML) standard for exchanging authentication and authorization data between security domains; that is, between an identity provider (IdP) such as SafeNet Authentication Service (SAS) and a service provider (SP), typically a web application such as Google Apps. It allows a user to login once for affiliated, but separate, web sites or web applications.

SAML specifies three components—assertions, protocol, and binding. There are three assertions—authentication, attribute, and authorization.

- Authentication assertion validates the user's identity.
- Attribute assertion contains specific information about the user.
- Authorization assertion identifies what the user is authorized to do.

Protocol defines how SAML asks for and receives assertions. Binding defines how SAML message exchanges are mapped to Simple Object Access Protocol (SOAP) exchanges. SAML works with multiple protocols, including Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP), and also supports SOAP, BizTalk, and Electronic Business XML (ebXML).

While generally considered an authentication protocol for web apps, and in particular cloud computing, SAML is in fact supported by a range of applications and devices, including SAP, and perimeter devices such as SSL VPNs.

RADIUS on Steroids?

Those familiar with RADIUS might want to think of SAML as “RADIUS on steroids”, though the protocol is vastly different and substantially more flexible.

In a traditional RADIUS scenario, a user is prompted to provide authentication credentials (user ID and password) by an access point such as a VPN. The VPN uses the RADIUS protocol to pass the credentials to the authentication service for validation which in turn sends an “accept” or “reject” message via RADIUS back to the VPN (Figure 2: RADIUS Authentication User Experience on page 9).

By standardizing on RADIUS, an organization gains the freedom to choose any vendor’s RADIUS client (for example, a VPN) and be assured that it could use any other vendor’s RADIUS Server (for example, SAS).

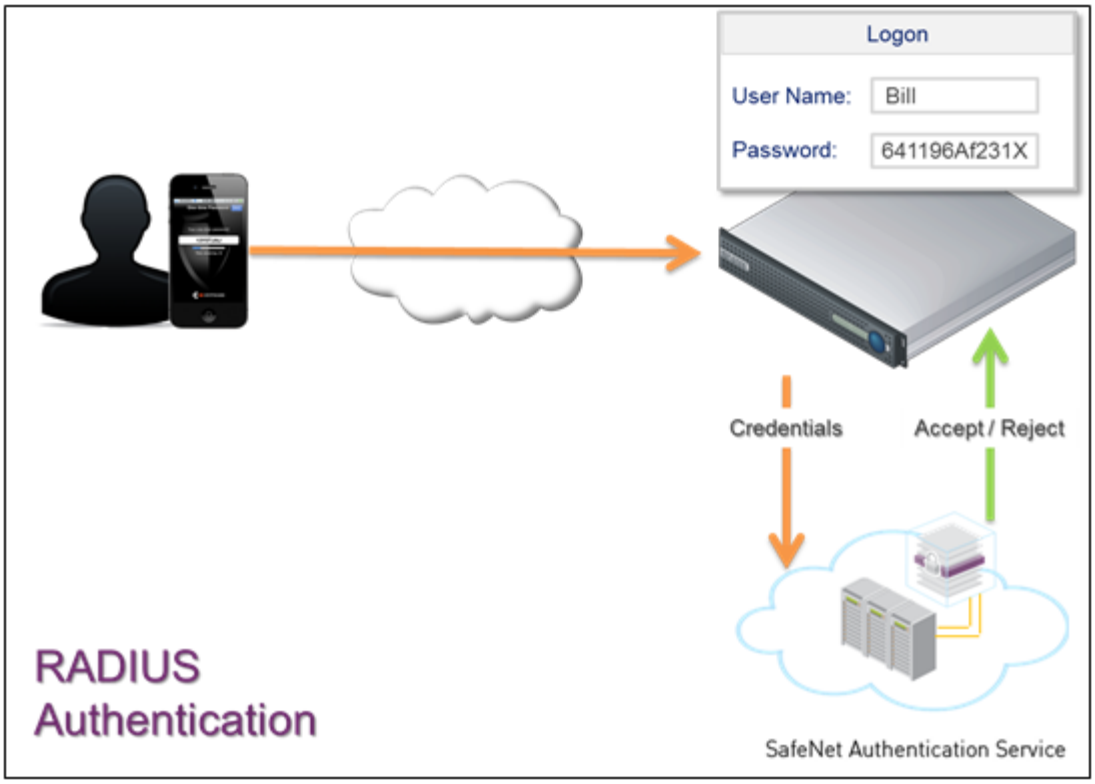


Figure 2: RADIUS Authentication User Experience

However, RADIUS has rarely been adopted outside of network perimeter devices. Much like the days before the adoption of RADIUS, applications have each tended to have their own authentication mechanism. As a result, users tend to have many passwords and had to log into individual applications.

With the growth in web apps, and in particular cloud computing, this quickly becomes unmanageable for users and administrators alike. Obviously, a new authentication standard is required that can be adopted by application developers with ease, without requiring specific knowledge of how or what the authentication method will be. And equally important, the standard must provide a way to federate identity so that users do not require many passwords or a separate logon to individual applications.

SAML, and in particular SAML 2.0, is the standard that makes this possible.

How Does SAML Work?

A SAML Service Provider (such as Google Apps, Salesforce, and SSL VPNs) “relies” on a SAML IdP (such as SAS) to present the logon page and authenticate users.

When a user logs in to an application that supports SAML, they are redirected to SAS where they must authenticate. If the authentication is successful, the user is redirected to their cloud app where access is granted. The SAML “assertion” generated by the IdP in response to a successful authentication is used by the Service Provider to grant the user access to the application.

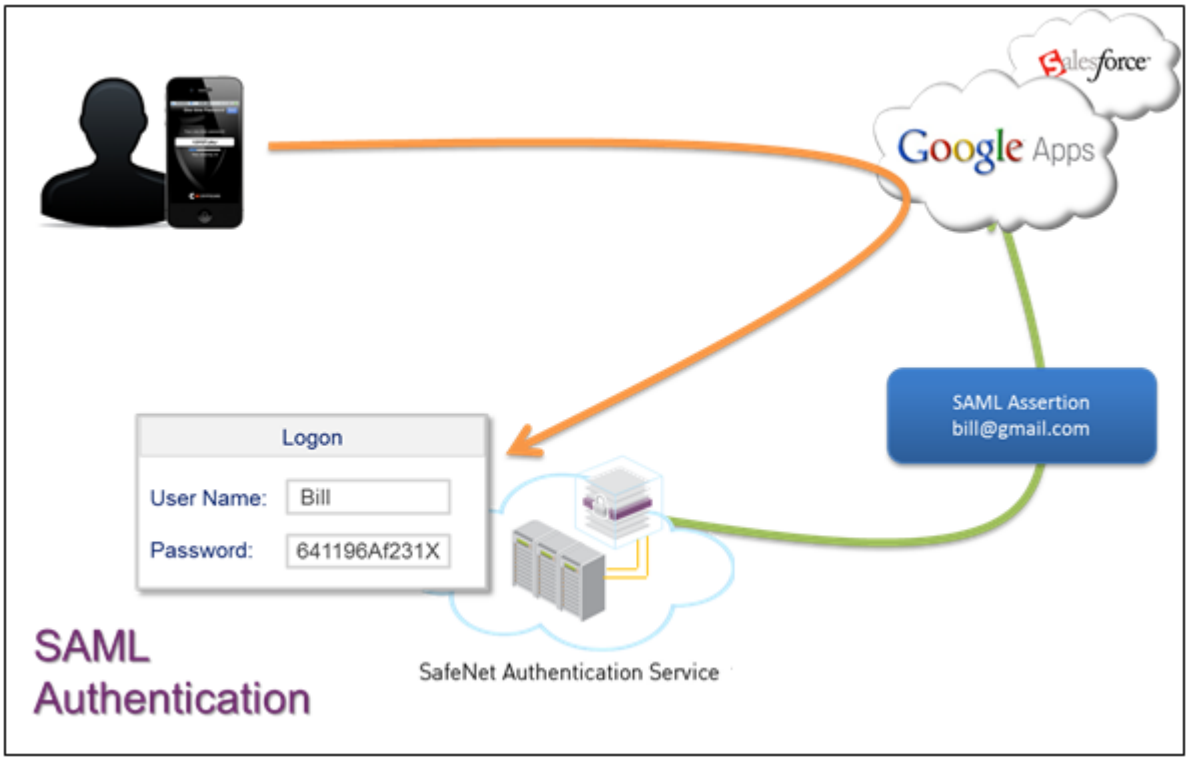


Figure 3: SAML Authentication User Experience

Web Application SSO

Where an affiliation exists between separate web sites or applications, the successful SAML authentication will result in user access to the affiliate without imposing additional user logon – essentially web SSO. Figure 3: SAML Authentication User Experience illustrates a possible affiliation between Google Apps and Salesforce that would permit a user authenticated into one of these services to be able to use the other service without additional authentication.

Managing Cloud Identities

It's not uncommon for individual cloud applications to impose specific requirements with respect to user IDs. For example, a user may require a Gmail account (for example, bill@gmail.com) to log in to Google Apps, whereas Salesforce may require a domain-specific email address (for example, bill@company.com). If there's no affiliation between the web apps, the user may be required to log on separately to each application using different credentials. These, of course, may be in addition to the user ID required for logon through the corporate VPN (for example, bill).

This can quickly become confusing and unmanageable for users and administrators. Fortunately, there are several remedies:

- Use SAS to normalize the user's logon credentials across corporate and cloud applications and services.
- Use SAS in conjunction with a cloud single sign-on (SSO) service.

Normalizing User Credentials Using SafeNet Authentication Service

One of the capabilities of SAS is to authenticate a user with a single credential—their user ID and one-time password (OTP)—but provide a different, specific credential required by the cloud app service. Effectively, SAS, on successful authentication, replaces the user ID provided during authentication with the user ID required by the cloud application in the SAML assertion. For the user, this delivers a consistent logon methodology (for example, UserID: Bill, Password: OTP) and insulates the user from any other credential management requirements.

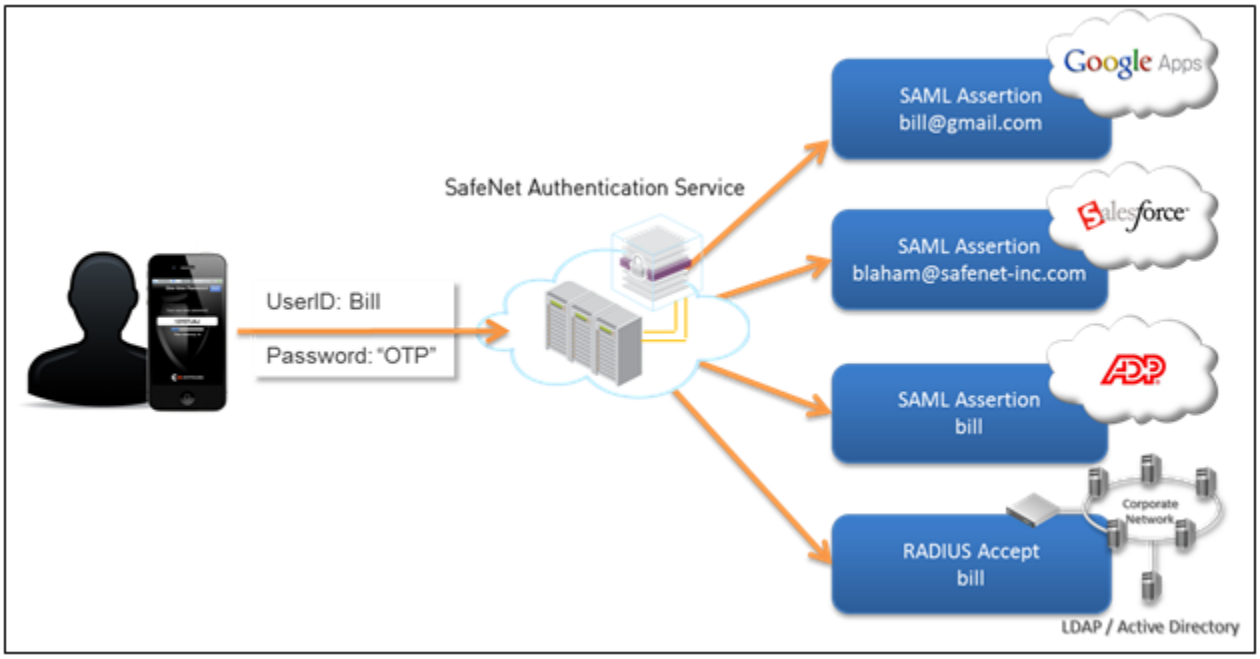


Figure 4: User Credentials Using SAS

SafeNet Authentication Service with Cloud SSO Service Providers

Cloud SSO service providers provide a front-end for managing multiple cloud service providers and applications. Typically, these front-ends support SAML authentication and can therefore use SAS as the IdP.

The cloud SSO can be configured as a SAML service provider, relying on SAS to authenticate the user. Once authenticated, the user has access to cloud applications and services configured for their personal cloud SSO account.

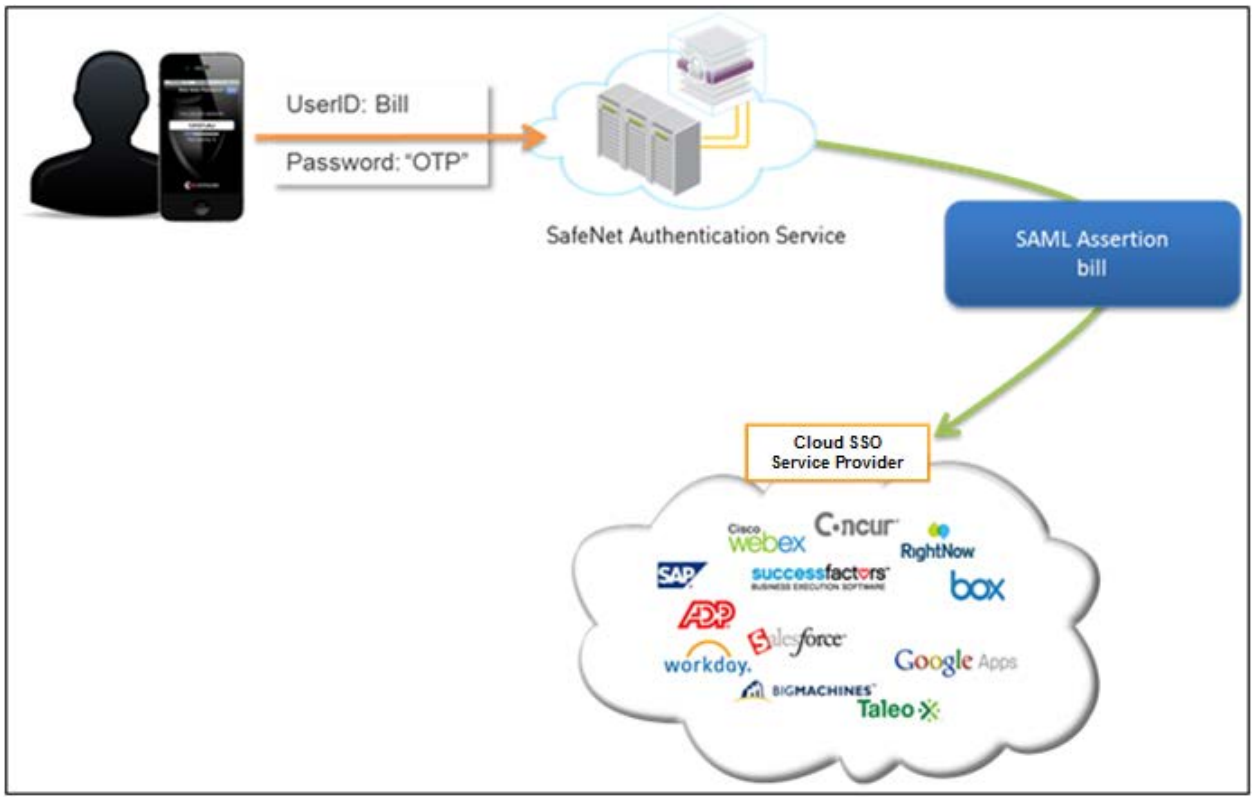


Figure 5: SAS with Cloud SSO Service Providers

Automating Cloud App Authorization

One of the challenges facing administrators of large user populations is efficient and timely activation of SAML authentication. As the number of users and cloud apps grow, so too does the challenge of timely activation/deactivation.

SAS offers an elegant solution to the problem in the form of SAML Provisioning Rules. Generally, these rules are triggered on the addition or removal of a user from an LDAP security group and/or SAS internal group, and allow/deny authentication for users authenticating at the specified SAML service providers respectively.

2
Enhanced User Login

SAS Cloud supports the Enhanced User Login feature, which provides the following improvements in user experience relative to the Classic User Login for SAML authentications using SAS:

- The user provides their User Name only; after which SAS prompts them for additional credentials.
- SAS initiates the appropriate challenge (Push, SMS or GrIDsure) for a user whom is remembered from previous successful authentication(s) on the same device + browser combination.
- SAS pre-populates the User Name field for users whom choose to be remembered from previous successful authentication(s) on the same device + browser combination.
- SAS displays the name of the requested application during login.
- SAS displays the User Name during login.

Note: Enhanced User Login is not available with SAS-PCE/SPE editions.

A comparison of the initial Classic User Login and Enhanced User Login pages is shown in Figure 6.

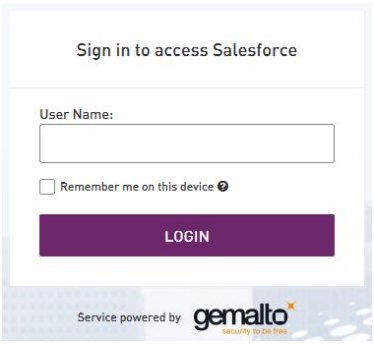
Classic User Login	Enhanced User Login
	
Fields/Features: • User Name • Use my mobile to autosend a passcode • Passcode	Fields/Features: • Name of requested application • User Name • Remember me on this device • Background image

Figure 6: Comparison of Classic User Login and Enhanced User Login

Operation

With Enhanced User Login enabled:

1. The user requests access to a SAML-protected resource (business application).
2. The Service Provider (SP) redirects the user to a SAS SAML Agent Identity Provider (IdP) login page.
3. SAS prompts for a User Name only (no passcode input field displays).
4. The user types their User Name and clicks Login.
5. SAS displays a generic (passcode or OTP) password credential prompt.

   Note: SAS does not indicate whether the User Name was valid.

If the User Chooses to be Remembered

If the user selected **Remember me on this device** and successfully authenticated on the device + browser combination that they are currently using; then, in response to a login request from the user, SAS sends a Push, SMS or GrIDsure challenge appropriate to the user's token type whenever all of the following conditions apply:

1. **Enable Enhanced User Login** is selected.
2. The user has not selected **Forget me on this device** since last selecting **Remember me on this device**.
3. The user is provisioned with one type of token only (for example, MobilePASS+ with Push enabled, SMS or GrIDsure).

Switching Between Login Types

You can enable/disable Enhanced User Login individually for each SAML SP so as to roll out the feature only after users are trained and your feature customizations are completed.

For SAML Service Providers configured prior to the introduction of the Enhanced User Login feature, the feature is OFF by default and the Classic User Login experience displays.

For SAML Service Providers configured after the introduction of the Enhanced User Login feature, the feature is ON by default and the Enhanced User Login experience displays. If the feature is thereafter set to OFF, the Classic User Login experience displays.

Activate the Enhanced User Login

To activate the Enhanced User Login feature for a SAML Service Provider:

1. Login to the SAS console.
2. Select the account that you are managing from "List Accounts" in the Shortcuts column.
3. Navigate to **VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings**.
4. Click **Add** to create a SAML Service Provider
   or
   Select a SAML Service Provider from the Service Provider Name table (if present).
5. Select the **Enable Enhanced User Login** checkbox.

Figure 7: VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings

Remember me on this Device

The **Remember me on this device** function enables users to login to a specific device (for example, desktop PC, tablet, or mobile phone) + browser (for example, Chrome, Internet Explorer, or Safari) combination multiple times without typing their user ID (that is, SAS pre-populates the User Name field) if they have previously logged in to the specific device + browser combination. This function also enables SAS to recognize users so that in later authentications it can, under certain conditions, automatically initiate a Push, GrIDsure or SMS challenge.

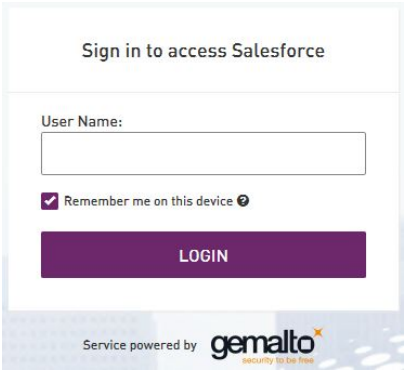


Figure 8: "Remember me on this device" Checkbox

SAS will not pre-populate the User Name field or recognize the user if the user attempts to login:

- To a device other than that which they used when **Remember me on this device** was last selected.
- Using a browser other than that which they used when **Remember me on this device** was last selected.

See “If the User Chooses to be Remembered” for further details.

Customize the Remember Me Text

You can customize the “Remember me on this device” text that displays on the login page next to the check-box that enables a user to select whether they want to be remembered on the device + browser combination that they are currently using.

1. Navigate to **VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings**.
2. Type a customized message in the Remember Me Text field.

Figure 9: Remember Me Text Field

Customize the Remember me Help Text

You can customize the text that displays on the login page when a user clicks on the question mark icon next to the “Remember me on this device” option.

1. Navigate to **VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings**.
2. Type a customized message in the Remember Me Help Text field.

Figure 10: Remember Me Help Text Field

Forget me on this Device

The **Forget me on this device** function enables users to be forgotten on the device + browser combination that they are currently using - in the context of SAML authentication; not just for the current login attempt but for all login attempts until they select “Remember me on this device”.

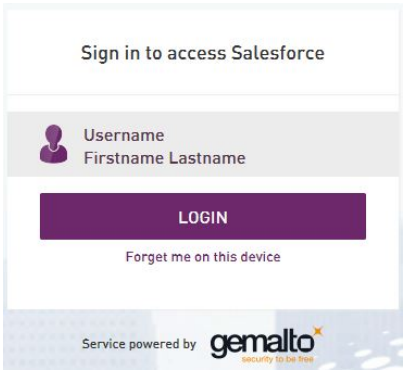


Figure 11: "Forget me on this device" Option

After selecting **Remember me on this device** (whereby the User Name field is pre-populated), a user can choose to be prompted for their User Name (i.e., type their User Name) on subsequent logins, by selecting **Forget me on this device**.

Customize the Forget Me Text

You can customize the “Forget me on this device” text that displays on the login page as a link that enables the user to be forgotten for the device + browser combination that they are currently using.

1. Navigate to **VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings**.
2. Type a customized message in the Forget Me Text field.

Figure 12: Forget Me Text Field

Display Enhancements

To add context to the authentication process, the following information displays on the login page:

- The name of the requested application (at the top of the authentication dialog box).
- The User Name of the authenticating user.

The name that SAS displays for the requested application is configured using **VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings > Resource Name** for each SAML Service Provider.

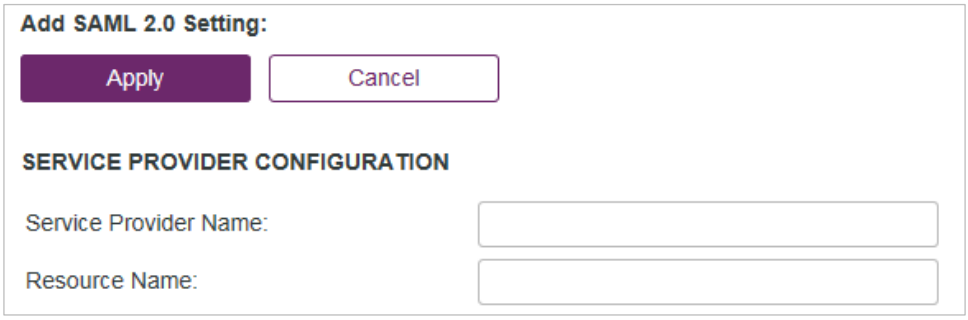


Figure 13: VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings

Login Page Customization

The Enhanced User Login for SAML feature introduces the following User Interface (UI) elements:

- Background Image
- Remember Me Text
- Remember Me Help Text
- Forget Me Text
- SIGN-IN Text
- SIGN-OUT Text
- OR Text

In the case of a SAML Service Provider application that was previously configured in SAS with some or all of the text or image fields customized, when ***Enable Enhanced User Login*** is selected, the customized values are retained and are applied to the ***Enhanced User Login*** experience where applicable and as identified in the chapters that follow.

CSS Customization

You can customize both the Enhanced User Login and the Classic User Login user interface by uploading a custom CSS file. To obtain a copy of the default CSS file:

1. Go to http://www2.gemalto.com/sas/implementation-guides.html
2. Click “SafeNet Authentication Service Cloud” to display a list of SAS Cloud documents.
3. Click “CSS for SAML Enhanced User Login” under the heading with the same name.

   The bsid.css file displays. The Classic User Login classes are defined within the “Non ID First” section and the Enhanced User Login classes are defined within the “ID First” section.

NOTE: Custom CSS files are always applied on top of the default CSS file, as such, classes specified in the custom CSS files will override classes of the same name in the default CSS file.

As you switch from Classic User Login to Enhanced User Login, or vice-versa, by changing the **Enable Enhanced User Login** setting, a previously uploaded custom CSS file is retained. However, since CSS classes for Enhanced User Login are distinct from CSS classes for Classic User Login, a previously applied custom CSS file created strictly to customize the UI for Classic User Login will have no effect on the User Interface for Enhanced User Login.

Restrictions and Limitations

The Enhanced User Login feature is not compatible with SAS Pre-Authentication rules.

In cases where the Enhanced User Login feature is enabled, if a Virtual Server is configured for Pre-Authentication rules, those rules are ignored in the context of a SAML authentication; but continue to be applied in all other contexts.

3
Configuring SAML Authentication in SafeNet Authentication Service

There are three steps to configure SAML authentication:

1. **Configure SAML Service Providers**—Configure the virtual server to process authentication requests from a specific SAML service provider.
2. **Configure SAML Services**—Manually enable SAML authentication for users to one or more of the SAML service providers created in step 1.
3. **Configure SAML Provisioning Rules**—Automatically enable SAML authentication for users to one or more of the SAML service providers created in step 1. SAML Provisioning Rules can be used instead of, or in addition to, manual configuration (step 2).

Step 1: Configure SAML Service Providers

To configure a SAML service provider, go to **VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings**.

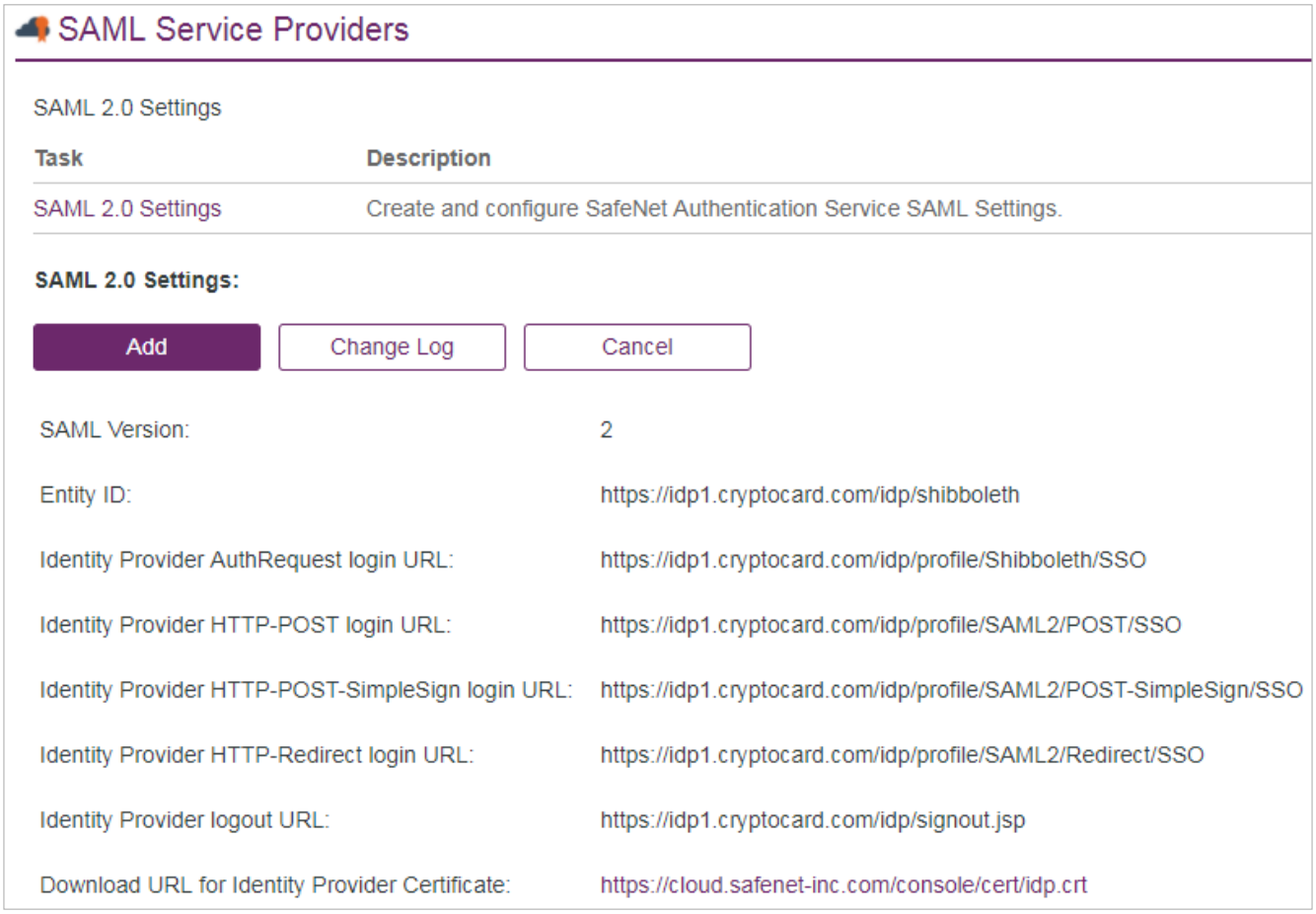


Figure 14: VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings

Complete the following sections:

- Service Provider Configuration
- Return Attributes
- User Login Settings
- Login UI Customizations
- Enhanced Login UI Customizations

Service Provider Configuration

To insert a service provider into the list, click **Add**.

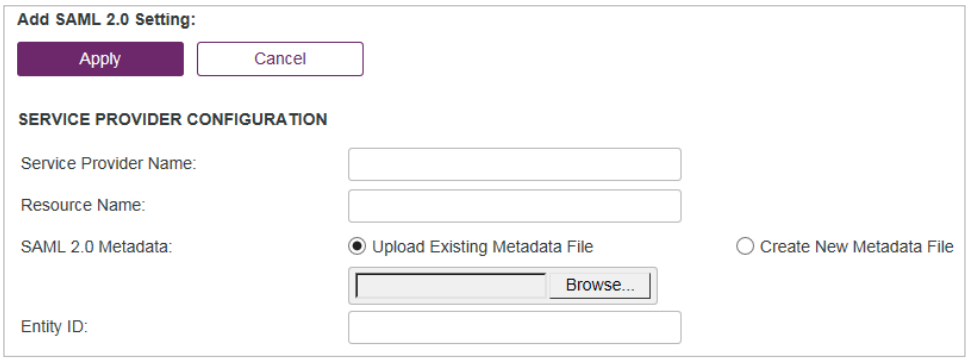


Figure 15: Service Provider Configuration Fields

Complete the following fields:

- **Service Provider Name**—The name you assign to the Relying Party for easy identification. This is used for administration purposes and must be unique within a virtual server. This name displays in SAML Services lists under **ASSIGNMENT > SAML Services** and under **POLICY > Automation Policies > SAML Provisioning Rules**.
- **Resource Name**—(Push OTP is not available with SAS PCE/SPE) Push notifications include the SAML service where a push was initiated. To ensure users easily recognize the source of the push notification, this field enables Operators to customize the SAML service name that displays. This field defaults to the SAML **Service Provider Name** after the SAS upgrade, and when a new SAML service is added.

  This name is included in the Push notification instead of the Auth Node Resource Name.
- **SAML 2.0 Metadata**
  - **Upload Existing Metadata File**—An XML file that is generated by your SAML Service Provider.
  - **Create New Metadata File**—Some SAML Service Providers do not provide a metadata file, but instead provide only their Entity ID and Location (essentially the resource being accessed). Use this option to have the virtual server create and add a metadata file based on this information.

> **NOTE**: When a SAML metadata file is provided, SAS will validate the Location URL in the metadata file. If the server cannot reach the URL, a warning message will be displayed, which provides the user with the option to either continue with the current file, or cancel the action.
>
> If the user clicks **Continue**, the upload will continue with the current file, and the SAML configuration will be added.
>
> If the user clicks **Cancel**, the SAML panel will close, and the SAML configuration will not be added.

- **Entity ID**—The Relying Party ID of the SAML Service Provider; typically in the form of a URL. This value will be provided by the SAML Service Provider or can be extracted from the metadata (XML file) provided by the SAML Service Provider.

For example:

<?xml version="1.0" encoding="UTF-8"?>

<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID=https://mycompany.salesforce.com

Return Attributes

Return attributes (not available with SAS PCE/SPE) are used to enable SAML applications to integrate with SAS and to authorize the user based on the attribute values. Operators must define all SAML return attributes for their SAML services in SAS. Note that during a SAS upgrade (to v3.5.1 or later), any existing SAML service providers are automatically configured to their existing behavior. Attributes that are not needed can be deleted.

NOTE: For newly created SAML services, the SAS Operator must add all required attributes. There are no default attributes. The agent will not send attributes that are not added.

To add a return attribute:

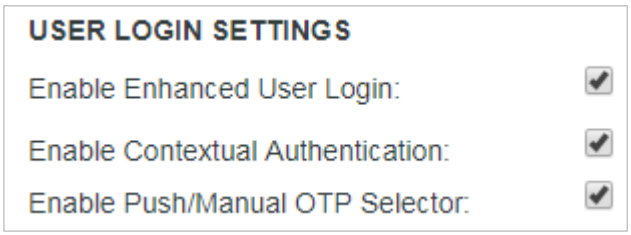
1. Click **Add attribute**.
2. Define the **Name** for the attribute, and then select the attribute type from the **Value** menu. If a custom value is needed, select **Custom** from the **Value** menu, and then enter the text to define the value.
3. To delete a return attribute, click **X** adjacent to the attribute.

The following is a list of the most commonly used return attributes:

- http://schemas.microsoft.com/ws/2008/06/identity/claims/uid
- http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
- http://schemas.xmlsoap.org/claims/EmailAddress
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
- http://schemas.xmlsoap.org/claims/CommonName
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
- principal

User Login Settings

Use the information in this section to configure the User Login Settings.



Define the login flow that will be applied to users:

- **Enable Enhanced User Login**— Controls whether Enhanced User Login or Classic User Login displays.
- **Enable Contextual Authentication**— Controls whether SAS will flexibly adapt (apply/skip) credential requirements for SAML-protected web-based applications.
- **Enable Push/Manual OTP Selector**—(Available for: SAS Cloud only.) Controls whether the Push OTP or Manual OTP option displays on the SAML login page.

NOTE: If this check box is disabled, the user can still trigger push or another challenge/response method with an empty passcode.

Login UI Customizations

Use the information in this section to customize the appearance of the user login page.

Figure 16: Comparison of Login Pages

- **Logo**—The image that displays as the logo on the login form.
- **CSS**—Modify the CSS and then upload it to customize the appearance of the page. For more information, see CSS Customization on page 18.

NOTE: Some of the following fields include recommended line lengths. Do not exceed the recommended length to ensure that the text is displayed correctly.

- **Background Image**—(Available for: SAS Cloud - Enhanced User Login only.) The image that displays as the background on the login form.
- **Button Image**—(Available for: SAS Cloud - Classic User Login only.) The image that displays as the login button on the login form.
- **Page Title**—The title displayed on the browser tab.
- **Icon**—The icon displayed on the browser tab.
- **Push/Manual OTP Selector Text**—(not available with SafeNet Authentication Service – PCE/SPE editions) This field is displayed if the **Enable Push/Manual OTP Selector** checkbox is selected. This is the "**I want to:**" text to display on the SAML **Login** page. Recommended length: 20 characters
- **Push OTP Button Text**—(not available with SafeNet Authentication Service – PCE/SPE editions) This field is displayed if the **Enable Push/Manual OTP Selector** checkbox is selected. This is the text to display for the option to use Push OTP. Recommended length: 29 characters
- **Manual OTP Button Text**—(not available with SafeNet Authentication Service – PCE/SPE editions) This field is displayed if the **Enable Push/Manual OTP Selector** checkbox is selected. This is the text to display for the option to use a manual OTP. Recommended length: 29 characters
- **Push OTP Processing Text**—(not available with SafeNet Authentication Service – PCE/SPE editions) This is the text to display when a Push OTP request is processing and waiting for a response from the user. Recommended length: 30 characters
- **Push OTP Cancellation Text**—(not available with SafeNet Authentication Service – PCE/SPE editions) This is the text to display on the button that is used to cancel a Push OTP request. Recommended length: 40 characters
- **Push OTP Cancellation Link**—(not available with SafeNet Authentication Service – PCE/SPE editions) This is text to display when a Push OTP request is cancelling. Recommended length:10 characters
- **Push OTP Authenticating Text**—(not available with SafeNet Authentication Service – PCE/SPE editions) This is the text to display when a Push OTP request is authenticating. Recommended length: 22 characters

NOTE: If the **Enable Push/Manual OTP Selector** option is disabled, the user can still trigger push or another challenge/response method with an empty passcode.

Note that the passcode triggers (introduced in SAS Cloud v3.5.1) to override Push OTP apply also to the push behavior for SAML login.

- **Login Header Text**—This field is no longer used.
- **Login Button Text**—This is the text displayed on the logon button. Recommended length: 10 characters
- **Login Message**—This field is no longer used.
- **Username Text**—This is the label for the user name field. Recommended length: 20 characters
- **Password Text**—This is the label for the password field. Recommended length: 20 characters

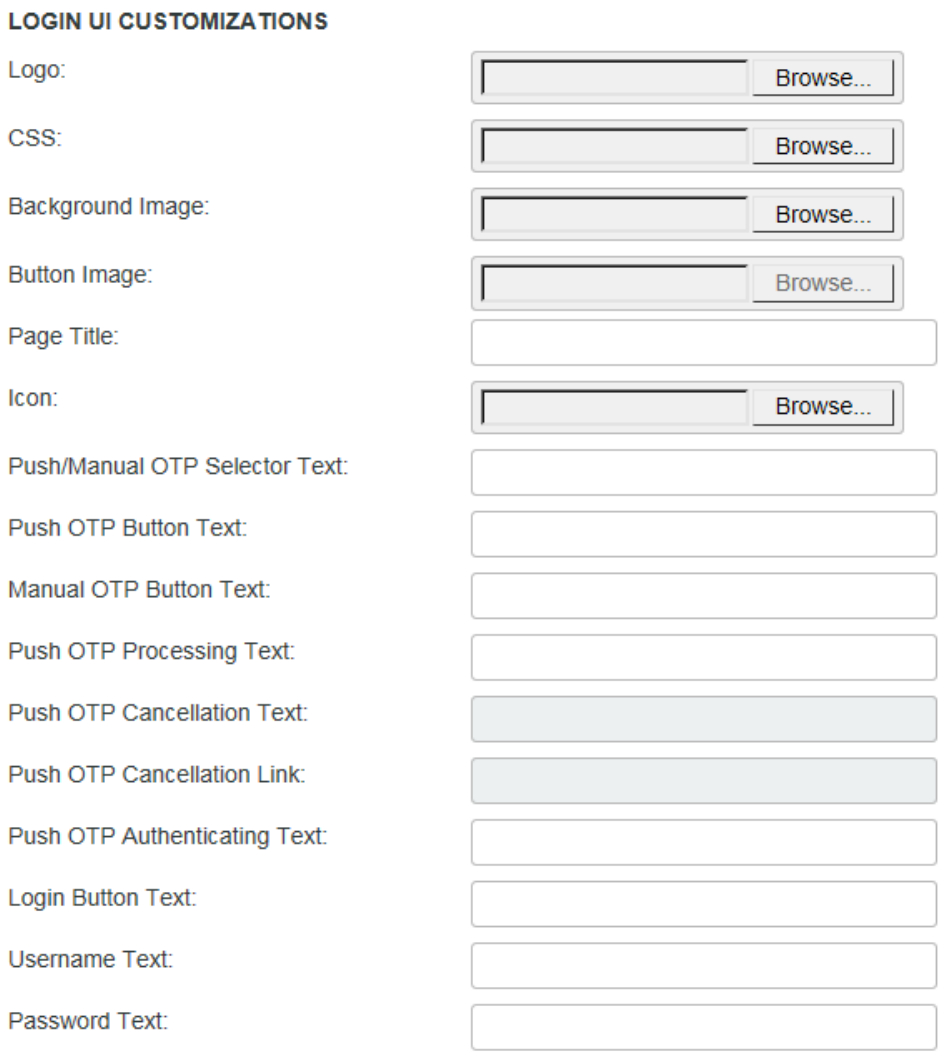


Figure 17: Login UI Customizations Fields

Enhanced Login UI Customizations

- **Remember Me Text**—(Available for: SAS Cloud - Enhanced User Login only.) The label for the Remember me on this device field. Recommended length: 35 characters or less. This parameter is used only when Enhanced User Login is set to ON.
- **Remember Me Help Text**—(Available for: SAS Cloud - Enhanced User Login only.) The text displayed after the Help icon (next to the Remember me on this device checkbox) is clicked. Recommended length: 80 characters or less. This parameter is used only when Enhanced User Login is set to ON.
- **Forget Me Text**—(Available for: SAS Cloud - Enhanced User Login only.) The label for the Forget Me on this Device field. Recommended length: 40 characters or less. This parameter is used only when Enhanced User Login is set to ON.
- **SIGN-IN Text**—(Available for: SAS Cloud - Enhanced User Login only.) The text that displays at the top of the authentication dialog box next to the application name (Resource Name). Recommended length: 24 characters or less. This parameter is used only when Enhanced User Login is set to ON.

- **SIGN-OUT Text**—(Available for: SAS Cloud - Enhanced User Login only.) The text that displays upon signing out. Recommended length: 24 characters or less. This parameter is used only when Enhanced User Login is set to ON.
- **OR Text**—(Available for: SAS Cloud - Enhanced User Login only.) The text that displays in between the Push OTP progress message and the manual Passcode field prompt – the default is the conjunction "or". Recommended length: 20 characters or less. This parameter is used only when Enhanced User Login is set to ON.

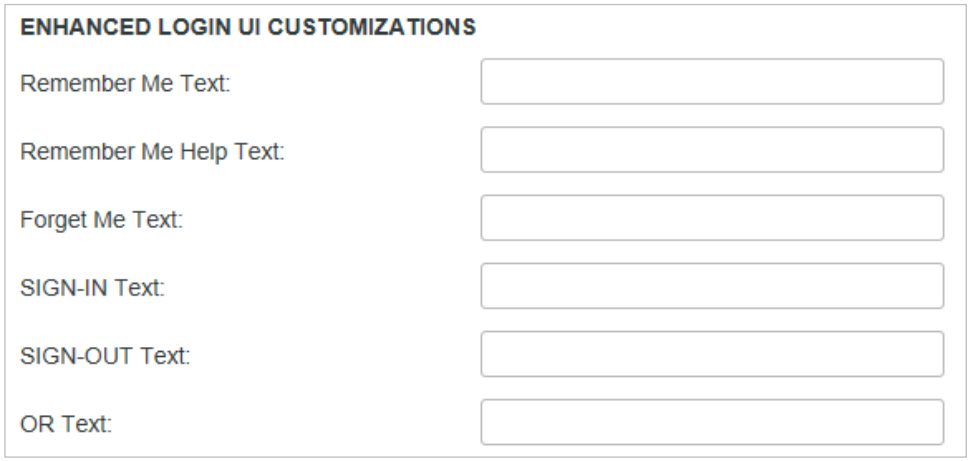


Figure 18: Enhanced Login UI Customizations

Step 2: Configure SAML Services

Use this module to manually enable a user to authenticate against one or more SAML Service Providers.

Figure 19: ASSIGNMENT > Search User > (User ID) > User Detail: (User ID) > SAML Services

To manage SAML services, click **ASSIGNMENT > Search User > (User ID) > User Detail: (User ID) > SAML Services**. The following functions are available:

- **Service**—Lists all of the configured SAML Service Providers configured in Step 1.
- **SAML Login ID**—The UserID that is returned to the service provider in the SAML assertion. If your service provider (e.g., Salesforce) requires a user ID of name@domain.com, and this is identical to the user's email address, choose the **E-mail** option. Doing so allows the user to consistently use their user ID to authenticate regardless of the service provider's requirements. Typically, a service provider will require either the user ID or e-mail. For all other cases, choose the **Custom** option and enter the required user ID to be returned.

You can automate the creation/removal of SAML Services for users by creating a SAML provisioning rule. Refer to Step 3: SAML Provisioning Rules.

Step 3: SAML Provisioning Rules

Use this module to automate adding or removing the right for users to authenticate to SAML service providers.

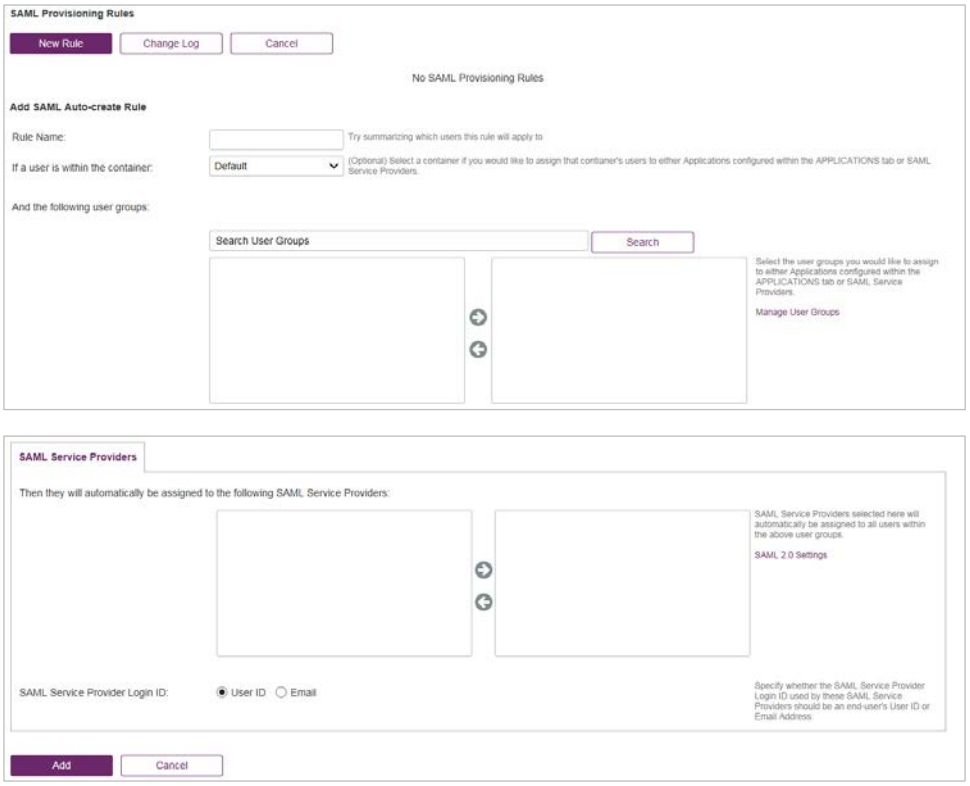


Figure 20: VIRTUAL SERVERS > POLICY > Automation Policies > SAML Provisioning Rules

- **Rule Name**—A name that describes the rule.
- **User is in container**—Users affected by this rule must be in the selected container.
- **Server Groups**—Users in these groups are not affected by this rule.
- **Rule Groups**—Users must be in one or more of these groups to be affected by this rule.
- **Relying Parties**—Service providers in this section are not affected by this rule.
- **Rule Parties**—Users that belong to one or more of the Rule Groups will be able to authenticate against Service Providers in this section.
- **SAML Login ID**—The user ID that is returned to the service provider in the SAML assertion.

4
Sample SAML Configurations

The following examples illustrate how to configure various SAML service providers to use SAS as a SAML IdP. The data used in these examples is for illustration only. Be sure to use data as displayed in your SAS and SAML service provider.

Salesforce

To use SAML with Salesforce, you must configure “My Domain” in Salesforce. Refer to Salesforce **Administration Setup > Company Profile > My Domain**.

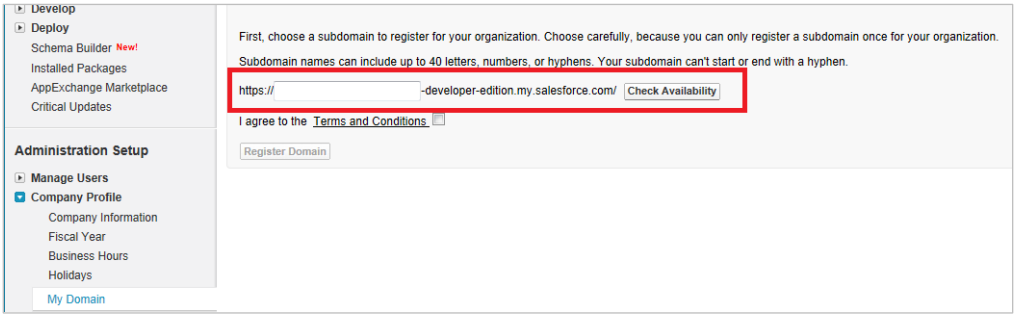


Figure 21: Administration Setup > Company Profile > My Domain

Step 1: Configure Single Sign-On

1. Log in to **Salesforce > Administration Setup > Security Controls > Single Sign-On Settings**.
2. Select the option **SAML Enabled**.

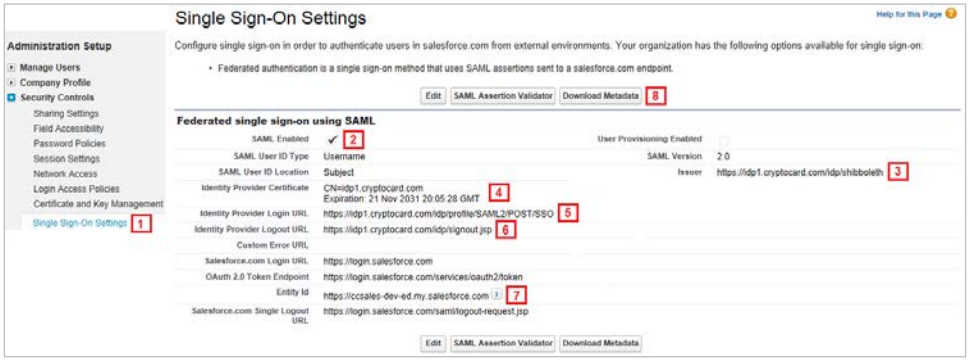


Figure 22: Salesforce > Administration Setup > Security Controls > Single Sign-On Settings

3. Add the Issuer URL.

   Use the value from **Entity ID** displayed under **COMMS > SAML Service Providers > SAML 2.0 Settings**.

4. Upload the SAS Identity Provider Certificate.

   Obtain this certificate from the **Download URL for Identity Provider Certificate** link displayed under **COMMS > SAML Service Providers > SAML 2.0 Settings**.

5. Add the Identity Provider Login URL.

   Use the value from **Identity Provider AuthenRequest URL** displayed under **COMMS > SAML Service Providers > SAML 2.0 Settings**.

6. Add the Identity Provider Logout URL.

   Use the value from **Identity Provider Logout URL** displayed under **COMMS > SAML Service Providers > SAML 2.0 Settings**.

7. Record the Entity ID.

   This is a unique ID created by Salesforce for your organization. This information, usually in the form of a URL, must be entered into the **Entity ID** field in SAS.

8. Download the metadata file from Salesforce and save it to a convenient location. You will upload this file to SAS in step 11, below.

Step 2: Add Salesforce as a SAML Service Provider

Under **SAML Service Providers > SAML 2.0 Settings**, click **Add** to configure a new SAML service provider.

Note: The step numbers in this procedure are purposely continuing from the preceding procedure.

9. Entity ID

   Copy the **Entity ID** information displayed in Salesforce (step 7, above) into the **Entity ID** field in SAS.

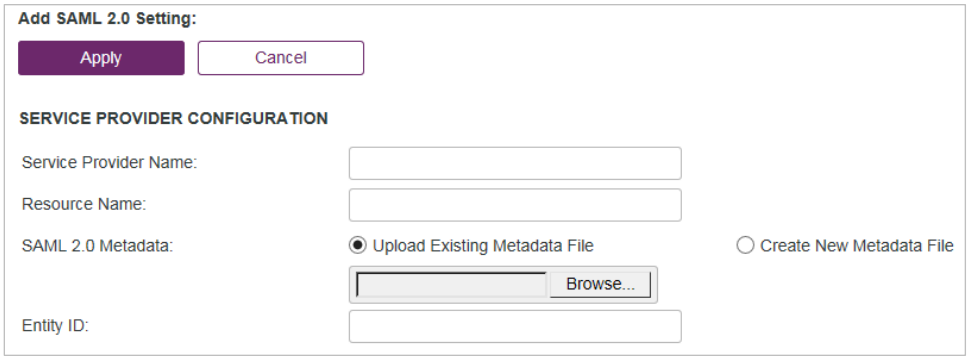


Figure 23: VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings

10. Service Provider Name (SAS Cloud)/Friendly Name (SAS PCE)

    This is a name you assign to the Relying Party for easy identification. This name will appear in **SAML Services** lists under **Assignment > SAML Services** and under **Policies > Automation Policies > SAML Provisioning Rules**.

11. SAML 2.0 Metadata

    Upload the Salesforce metadata file from step 8, above, to SAS.

12. Customize the logon page presented to users during logon to Salesforce.

Google Apps

Step 1: Set Up Single-Sign-On

Log in to **Google Apps > Advanced tools > Authentication > Set up Single Sign-on (SSO)**.

1. Select the option **Enable Single Sign-on**.

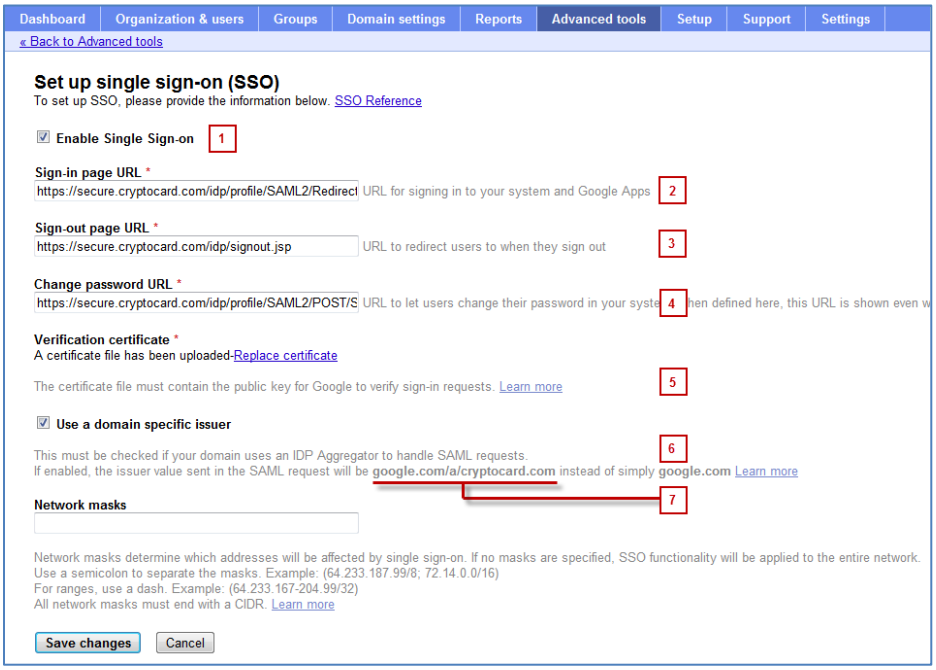


Figure 24: Google Apps > Advanced tools > Authentication > Set up Single Sign-on (SSO)

2. Sign-in page URL.

   Use the value from **Identity Provider HTTP-Redirect logon URL** displayed under **COMMS > SAML Service Providers > SAML 2.0 Settings**.

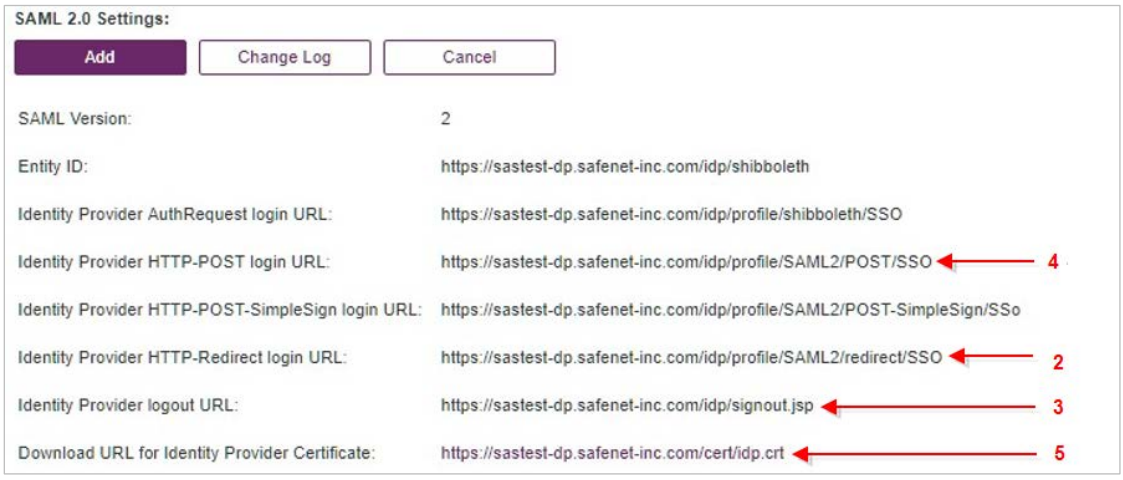


Figure 25: VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings

3. Sign-out Page URL.

   Use the value from **Identity Provider logout URL** displayed under **COMMS > SAML Service Providers > SAML 2.0 Settings**.

4. Change Password URL.

   Use the value from **Identity Provider HTTP=POST logon URL** displayed under **COMMS > SAML Service Providers > SAML 2.0 Settings**.

5. Verification Certificate.

   Use the **Download URL for Identity Provider Certificate** link displayed under **COMMS > SAML Service Providers > SAML 2.0 Settings** to obtain the SAS certificate. Upload this certificate to Google Apps.

6. Use a domain-specific issuer.

   Ensure that this option is selected. Use the value generated by Google Apps, typically **google.com/a/mycompany**, where **mycompany** is your domain registered in Google Apps. This information will be required in next steps.

Step 2: Add Google Apps as a SAML Service Provider

Under **SAML Service Providers > SAML 2.0 Settings**, click **Add** to configure a new SAML Service Provider.

Note: The step numbers in this procedure are purposely continuing from the preceding procedure.

7. Entity ID

   Copy the domain-specific identifier generated by Google Apps displayed in Salesforce (step 6 above) into the **Entity ID** field in SAS.

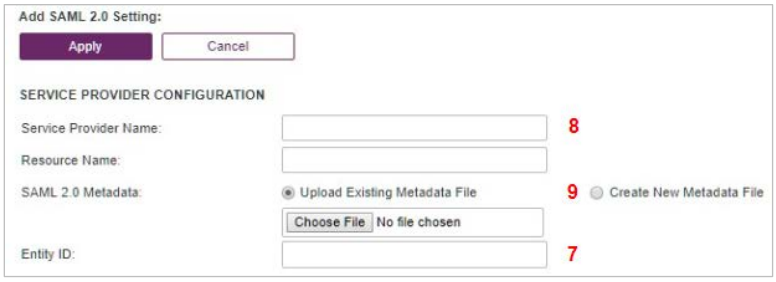


Figure 26: VIRTUAL SERVERS > COMMS > SAML Service Providers > SAML 2.0 Settings

8. Service Provider Name (SAS Cloud)/Friendly Name (SAS PCE)

   This is a name you assign to the Relying Party for easy identification. This name will appear in SAML Services lists under **Assignment > SAML Services** and under **Policies > Automation Policies > SAML Provisioning Rules**.

9. SAML 2.0 Metadata

   Google Apps does not generate metadata. To compensate, select the **Create New Metadata File** option, and then enter the following:

   - **Entity ID**—This is the Google Apps Entity ID from step 7 above (for example, google.com/a/mycompany)
   - **Location**—This is the SAML assertion consumer URL, typically the Entity ID preceded by **https://www**. Note: **/acs** must be added at the end (for example, https://www.google.com/a/mycompany/acs).

10. Customize the logon page presented to users during logon to Google Apps.