NetScaler with Unified Gateway

Configuring Sumologic

Contents

Disclaimer (Documentation)

This document is furnished "AS IS." Citrix Systems, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix System, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix Systems, Inc. and its licensors, and are furnished under a license from Citrix Systems, Inc.

Citrix Systems, Inc., the Citrix logo, and Citrix Provisioning Services are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Preface

This section provides an overview about the information included in this guide.

Intended Audience

The information in this guide is intended for the System Administrators.

Document Conventions

The following table lists various conventions used in this guide.

Table 1: Document conventions used in this guide

Convention	Description
Bold	Used for names of interface elements (such as names of fields, panes, windows, menus, buttons, dialog boxes) and what the user specifically selects, clicks, presses, or types.
Note	Used to highlight information that is important.

Overview

The Citrix NetScaler application delivery controller (ADC) helps to load balance, accelerate, optimize, and secure enterprise applications.

Sumologic can be integrated with Identity Provider (IdP) for user authentication. This enable the users to sign in to Sumologic using the same Single Sign On (SSO

Terminology

An Identity Provider (IdP) provides authentication module to verify users with their corporate network. A Service Provider (SP) supports receiving SSO SAML assertions.

The following table lists various terms that are used alternatively for completing configurations for service providers and identity providers.

Table 2: Terminology used for SP and IdP configurations

Service Provider (SP)	Identity Provider (IdP)
Identity Provider Issuer	Issuer Name
SP Entity ID	Service Provider ID
SP Assertion Consumer Service URL	Assertion Consumer Service URL

Configuring Sumologic for Single Sign-On

Sumologic supports SP/IdP initiated flow, which is supported in Netscaler (12.1).

Before you start, you need the following:

- Admin account for Sumologic.
- Admin account for NetScaler.
- Server Domain.
  For example if your IdP deployment URL is https://ug1.<server_domain>.com/logon/LogonPoint/index.html , your Server domain will be <server_domain>.

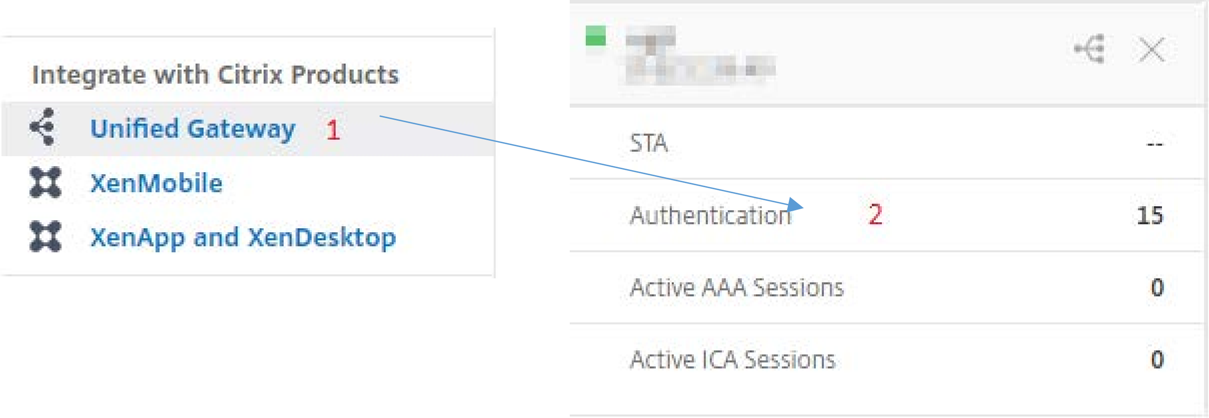
Sumologic Configuration

The Sumologic configuration steps are as follows:

1. Configure Sumologic with the App Catalog.
2. Configure SAML Setting into Sumologic.

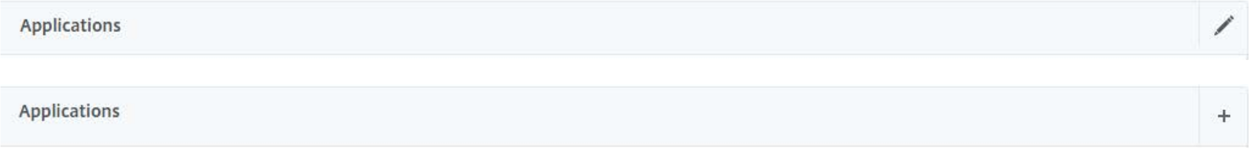
Step 1: Configure Sumologic with App catalog

1. Click on Unified Gateway > Authentication

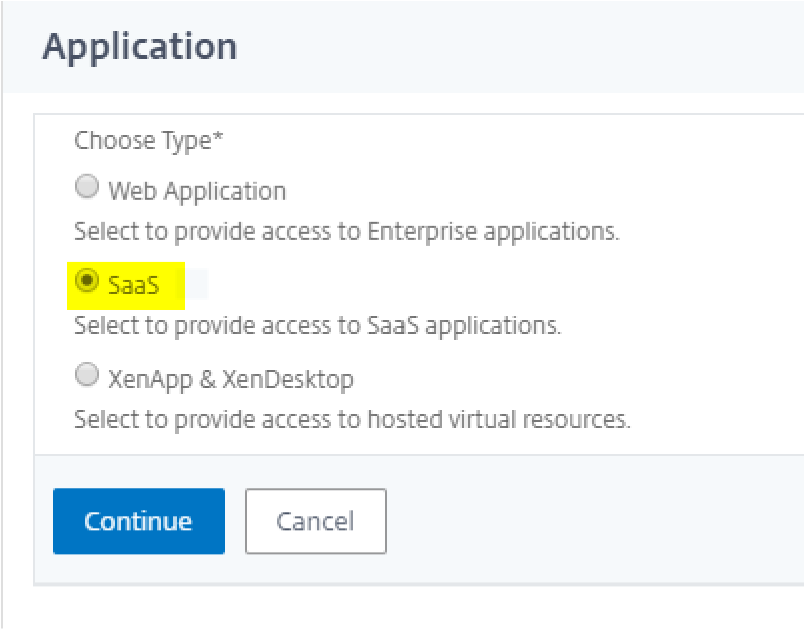


STA	--
Authentication	15
Active AAA Sessions	0
Active ICA Sessions	0

The Unified Gateway Configuration screen appears.



2. Go to **Application** section. Click on ✎ **icon**. Now you can see + **icon**. Click on it.
   The **Application** window appears.



Application

Choose Type*

○ Web Application

Select to provide access to Enterprise applications.

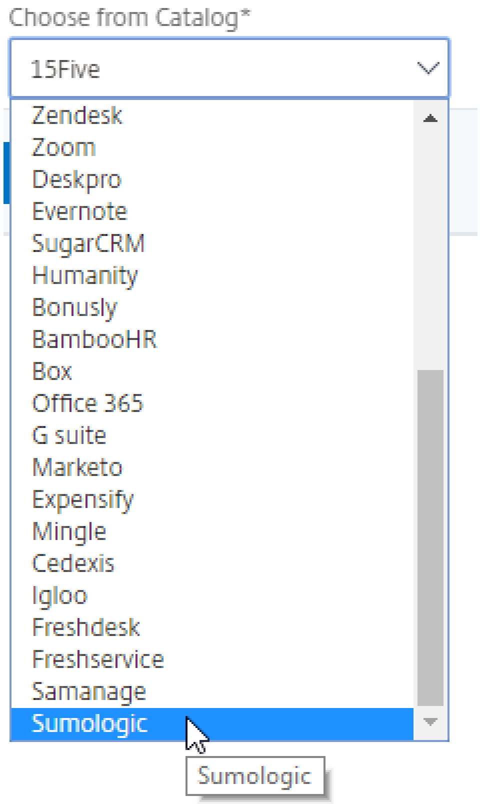
● SaaS

Select to provide access to SaaS applications.

○ XenApp & XenDesktop

Select to provide access to hosted virtual resources.

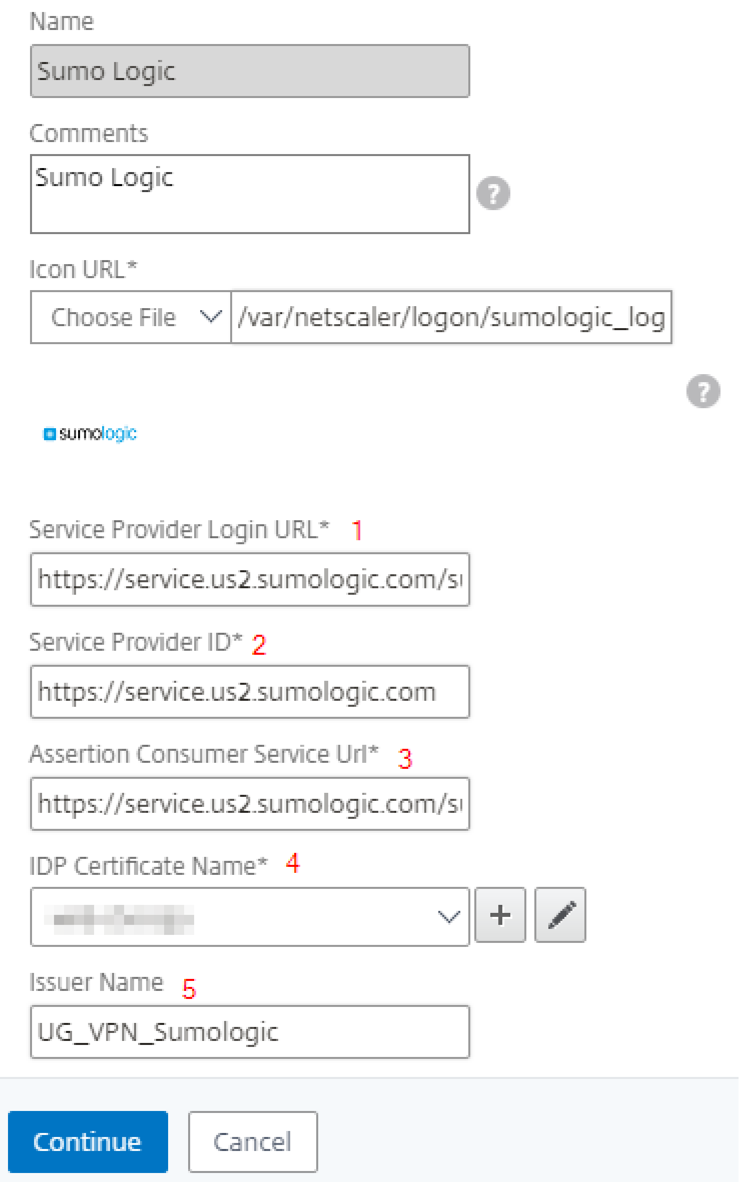
3. Select **SaaS** from the Application type.
4. Select Sumologic from the dropdown list.



Choose from Catalog*

15Five

5. Fill the Application template with appropriate values.



Name

Sumo Logic

Comments

Sumo Logic

Icon URL*

Choose File /var/netscaler/logon/sumologic_log

Service Provider Login URL* 1

https://service.us2.sumologic.com/su

Service Provider ID* 2

https://service.us2.sumologic.com

Assertion Consumer Service Url* 3

https://service.us2.sumologic.com/su

IDP Certificate Name* 4

[redacted]

Issuer Name 5

UG_VPN_Sumologic

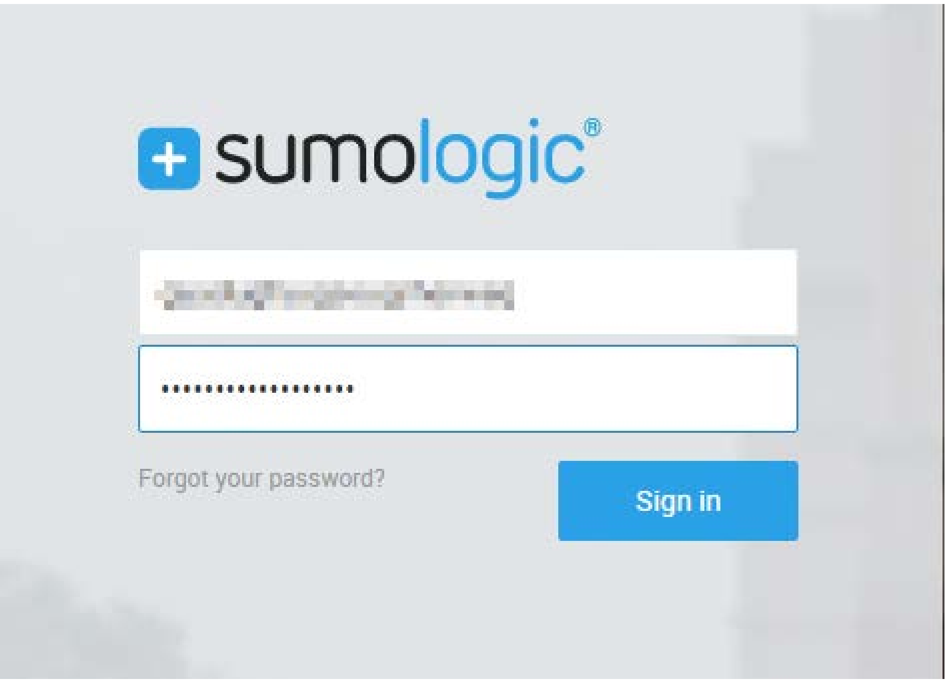
6. You must update the fields in Netscaler with the following values:

Field Name	Values
URL	https://service.us2.sumologic.com/sumo/saml/login/<customer_id>
Service Provider ID	https://service.us2.sumologic.com
ACS URL	https://service.us2.sumologic.com/sumo/saml/consume/<customer_id>
Signing Certificate Name	IDP certificate needs to be selected
Issuer Name	Issuer name can be filled as per your choice

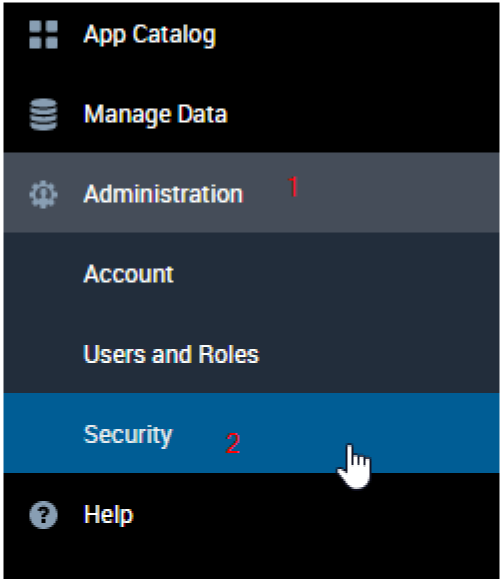
7. In place of <customer_id>, enter your company id (Follow Step 3 to get the customer id).
8. After providing the required values, click **continue.** Click **done**.

Step 2: Configure SAML Setting into Sumologic

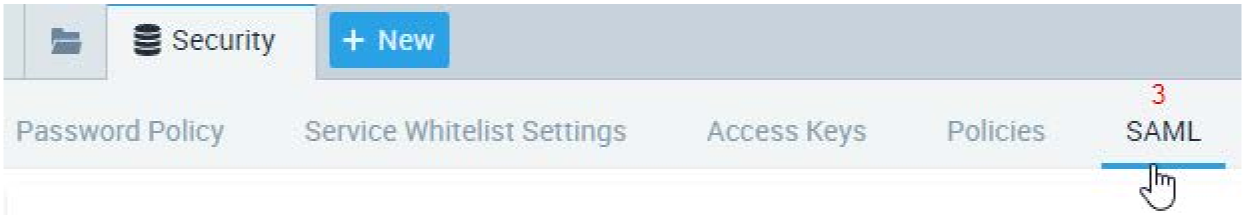
1. Login to **Sumologic** as an Admin user.



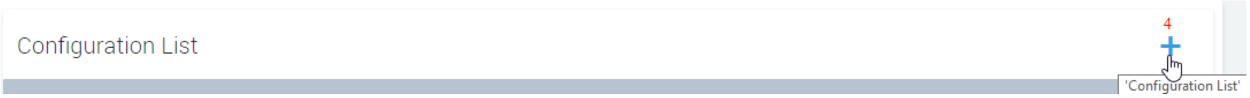
2. Click on **Administration** > **Security**.



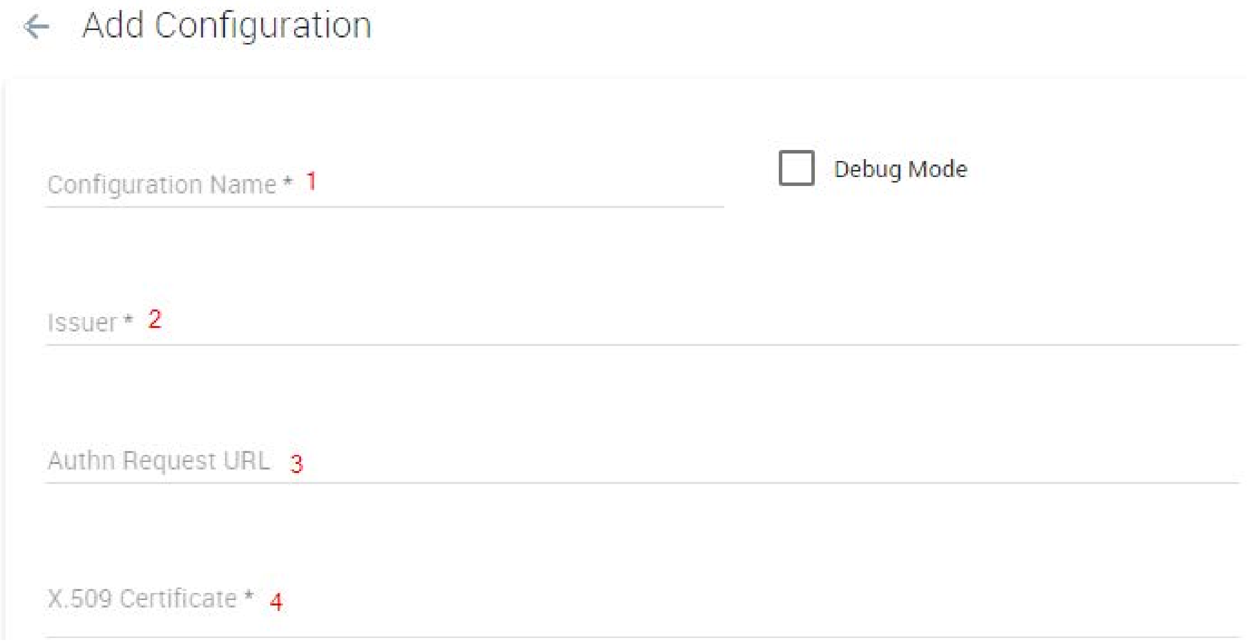
3. Security window will appear, click on **SAML**.

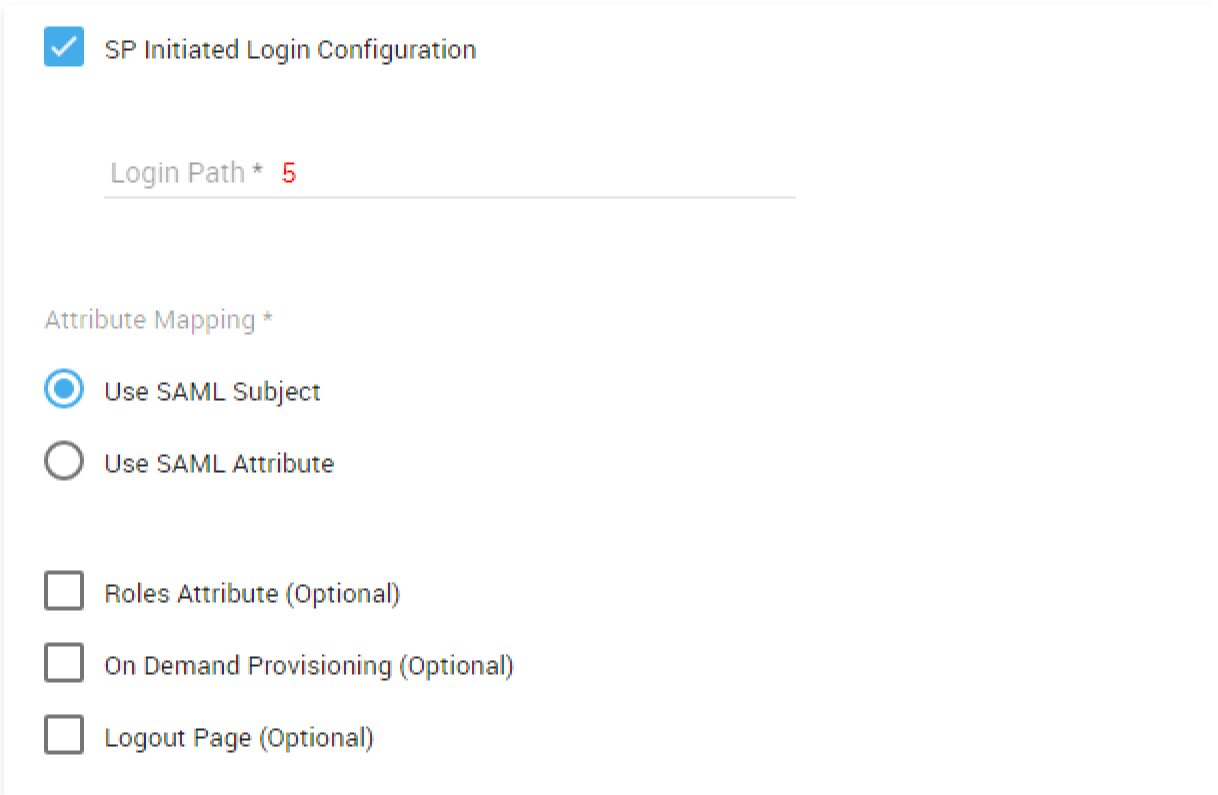


4. Click on plus icon in **Configuration list** section.



5. **Add configuration** window will appears, check **on SP initiated login configuration** and **Use SAML Subject** buttons and complete all the fields with appropriate values.





☑ SP Initiated Login Configuration

Login Path * 5

Attribute Mapping *

● Use SAML Subject

○ Use SAML Attribute

□ Roles Attribute (Optional)

□ On Demand Provisioning (Optional)

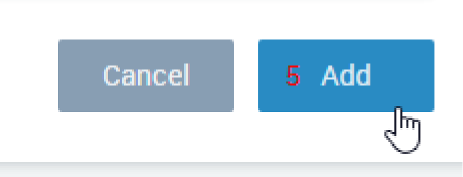
□ Logout Page (Optional)

6. Most complete all the required field.

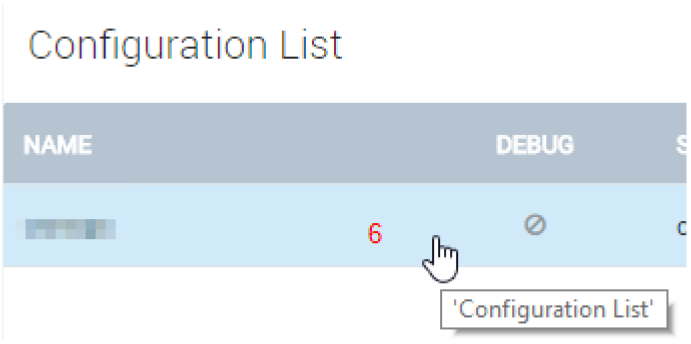
Field Name	Values
Configuration Name	Enter a name to identify the SSO policy
Issuer	Enter your Issuer name same as IdP
Authn Request URL	https://ug1.<server_domain >.com/saml/login
X.509 Certificate	Paste IdP certificate
Login Path	Enter a unique identifier, it will use to generate unique URL for user login
Logout Page	https://ug1.<server_domain>.com/cgi/logout

7. In place of <server_domain>, enter your server domain name (See **Introduction** to know more about the <server_domain> values).

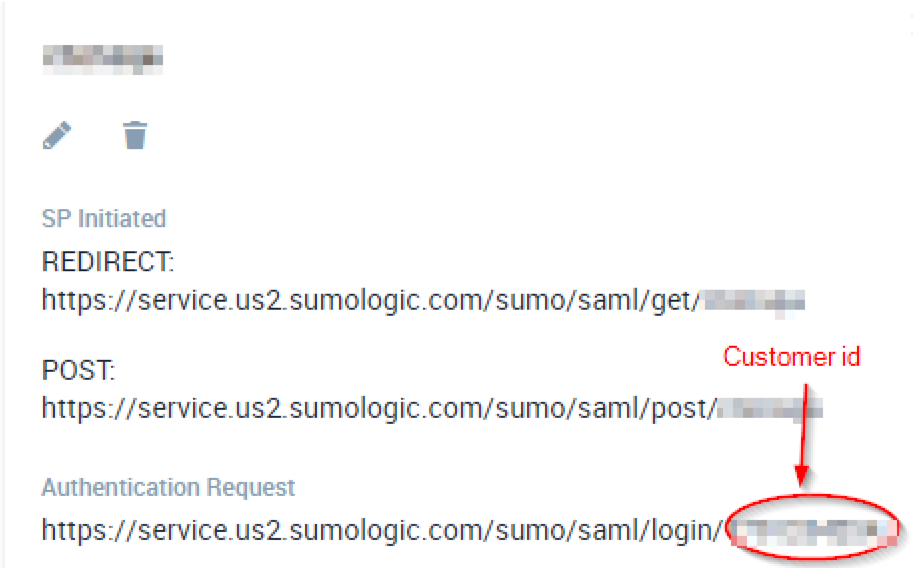
8. After providing the all values, click on **Add**.



9. Now you can see your configuration in configuration list, click on your configuration.



10. One window will pop up in right side.



[redacted]

SP Initiated

REDIRECT:
https://service.us2.sumologic.com/sumo/saml/get/[redacted]

POST:
https://service.us2.sumologic.com/sumo/saml/post/[redacted]

Customer id

Authentication Request
https://service.us2.sumologic.com/sumo/saml/login/[redacted]

11. Copy the **customer id**.