Authcontrol v4 Sentry SSO and Adaptive Authentication

Contents

What is Adaptive Authentication?

Swivel Secure's AuthControl Sentry adds to the existing Authentication platform a new means by which you can manage the way users access a range of on-premises and cloud applications. Specifically if and how they need to authenticate in order to gain access to those services. We refer to this aspect of the product as **Adaptive Authentication**, as you can select your authentication requirements depending on the application you are protecting.

Sentry applies a number of rules to determine which authentication method a user needs to complete before accessing a specific service. It does this by comparing the Trust Score a user achieves according to the rules and the Require Trust Score required for the service that the user is attempting to access and then offering the user a choice of authentication options that will increase their trust score to the appropriate level.

Where we need to refer to the authentication platform web administration console (on port 8080), we will refer to this as the Core.

- Application

Generic Name for remote access/cloud/web application. Could be for example Saleforce.com, OWA or SSL VPN

- Trust Score

An overall assessment of how much confidence we are that this is a valid access request

- Required Trust Score

The required trust score a user is required to demonstrate to be allowed access to an application

- Rule

An element of logic that is used to help create an overall assessment (Trust Score) of the level of confidence associated with a specific authentication request

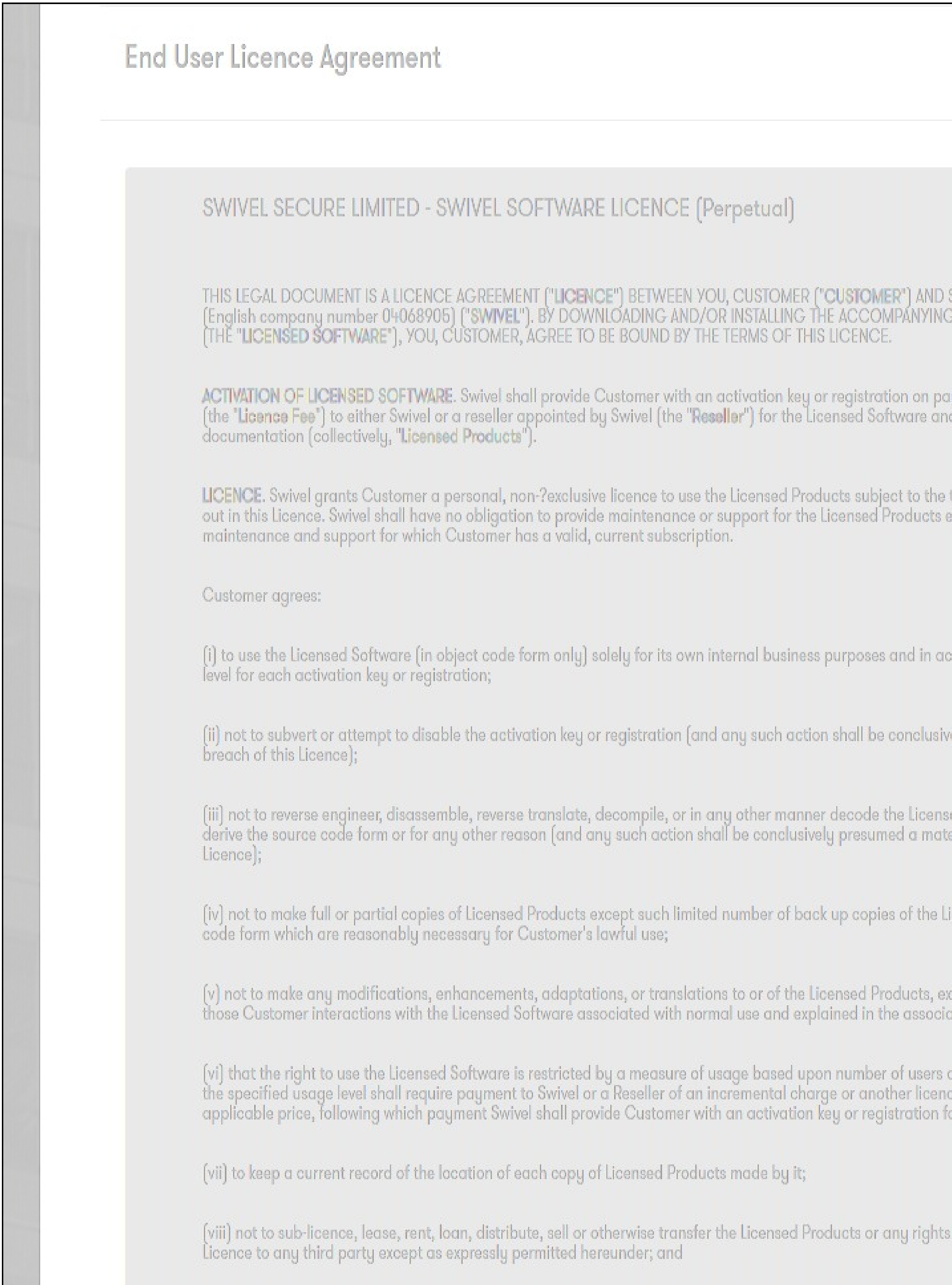
- Authentication Method

One of a number of ways that a user can be asked to authenticate.

Getting Started

Login to Sentry for the First Time

Login to Sentry using URL https://<INTERNAL_DNS_OF_SWIVEL_APPLIANCE>:8443/sentry and accept the EULA. If you can't gain access to the Sentry Admin Console, try another restart of Tomcat and wait 10-20 seconds or so before trying again.



End User Licence Agreement

SWIVEL SECURE LIMITED - SWIVEL SOFTWARE LICENCE (Perpetual)

THIS LEGAL DOCUMENT IS A LICENCE AGREEMENT ("**LICENCE**") BETWEEN YOU, CUSTOMER ("**CUSTOMER**") AND S
(English company number 04068905) ("**SWIVEL**"). BY DOWNLOADING AND/OR INSTALLING THE ACCOMPANYING
(THE "**LICENSED SOFTWARE**"), YOU, CUSTOMER, AGREE TO BE BOUND BY THE TERMS OF THIS LICENCE.

ACTIVATION OF LICENSED SOFTWARE. Swivel shall provide Customer with an activation key or registration on pa
(the "**Licence Fee**") to either Swivel or a reseller appointed by Swivel (the "**Reseller**") for the Licensed Software and
documentation (collectively, "**Licensed Products**").

LICENCE. Swivel grants Customer a personal, non-?exclusive licence to use the Licensed Products subject to the t
out in this Licence. Swivel shall have no obligation to provide maintenance or support for the Licensed Products e
maintenance and support for which Customer has a valid, current subscription.

Customer agrees:

(i) to use the Licensed Software (in object code form only) solely for its own internal business purposes and in ac
level for each activation key or registration;

(ii) not to subvert or attempt to disable the activation key or registration (and any such action shall be conclusiv
breach of this Licence);

(iii) not to reverse engineer, disassemble, reverse translate, decompile, or in any other manner decode the Licens
derive the source code form or for any other reason (and any such action shall be conclusively presumed a mate
Licence);

(iv) not to make full or partial copies of Licensed Products except such limited number of back up copies of the Li
code form which are reasonably necessary for Customer's lawful use;

(v) not to make any modifications, enhancements, adaptations, or translations to or of the Licensed Products, ex
those Customer interactions with the Licensed Software associated with normal use and explained in the associa

(vi) that the right to use the Licensed Software is restricted by a measure of usage based upon number of users o
the specified usage level shall require payment to Swivel or a Reseller of an incremental charge or another licenc
applicable price, following which payment Swivel shall provide Customer with an activation key or registration fo

(vii) to keep a current record of the location of each copy of Licensed Products made by it;

(viii) not to sub-licence, lease, rent, loan, distribute, sell or otherwise transfer the Licensed Products or any rights
Licence to any third party except as expressly permitted hereunder; and

Settings

You can generally access the Adaptive Authentication Admin console using the same username and PIN from a Admin Account on the Core server that it is working with. However you may need to change some settings first if you are running a non-standard installation.

Instructions below refer to a location *<swivelhome>*. This is the base directory containing the settings files for all Swivel applications. On an appliance, it is **/home/swivel/.swivel**.

The following settings are under <swivelhome>/sentry in a file called settings.properties.

The first section dictates how Sentry should communicate with the Core Server. It is recommended you change the default secret before putting into production.

```
pinsafessl=false
pinsafeserver=localhost
pinsafecontext=sentry
pinsafesecret=secret
pinsafeport=8181
```

The next section dictates how Adaptive Authentication should retrieve images from the core

```
imagessl=false
imageserver=localhost
imagecontext=proxy
imageport=8443
selfsigned=true
```

This entry determines which Core server group a user must be a member of in order to access the Adaptive Authentication Admin console. If you want the same users to administer both Adaptive Authentication and the Core, you can generally leave this setting at its default as shown below.

```
administrationGroup=SwivelAdmin
```

The administration group attribute can be specified through the CMI menu, Appliance Menu > Sentry Menu > Set Administration Group

Accessing the Web Administration Console

If the settings are correct then you can access the admin console login by going in a browser to http(s)://<swivelserver>:8443/sentry and then following the link to the admin login. Here, <swivelserver> is the IP address or host name by which the Swivel appliance is accessed.

You can then login to AuthControl Sentry Adaptive Authentication using the same credentials as for the core Sentry administration.

Troubleshooting Login

1. If no TURing image appears, check that the settings.properties are correct for your installation.
2. If you see a session start in the Core logs but no authentication request then check the settings for pinsafeserver etc in settings.properties.
3. If there is an authentication request but the Core logs indicate that the agent is not authorised, check that there is an Agent defined on the core administration for localhost (127.0.0.1), and that the secret for that Agent matches the one in settings.properties.
4. If the Core indicates that the authentication was successful but you still cannot access Adaptive Authentication, check on the Core that the user is in the group defined in settings.properties, e.g. SwivelAdmins.
5. If you cannot reach the Adaptive Authentication Admin Console it may be because access to the admin console is not possible from your IP Address. Check the settings in <swivelhome>/sentry/security.properties. This file shows the IP Addresses from which the admin console is accessible. The default is admin.iprange=0.0.0.0/0 which allows access from anywhere. A setting of 192.168.0.0/16, for example, would restrict access to the 192.168.x.x address range.

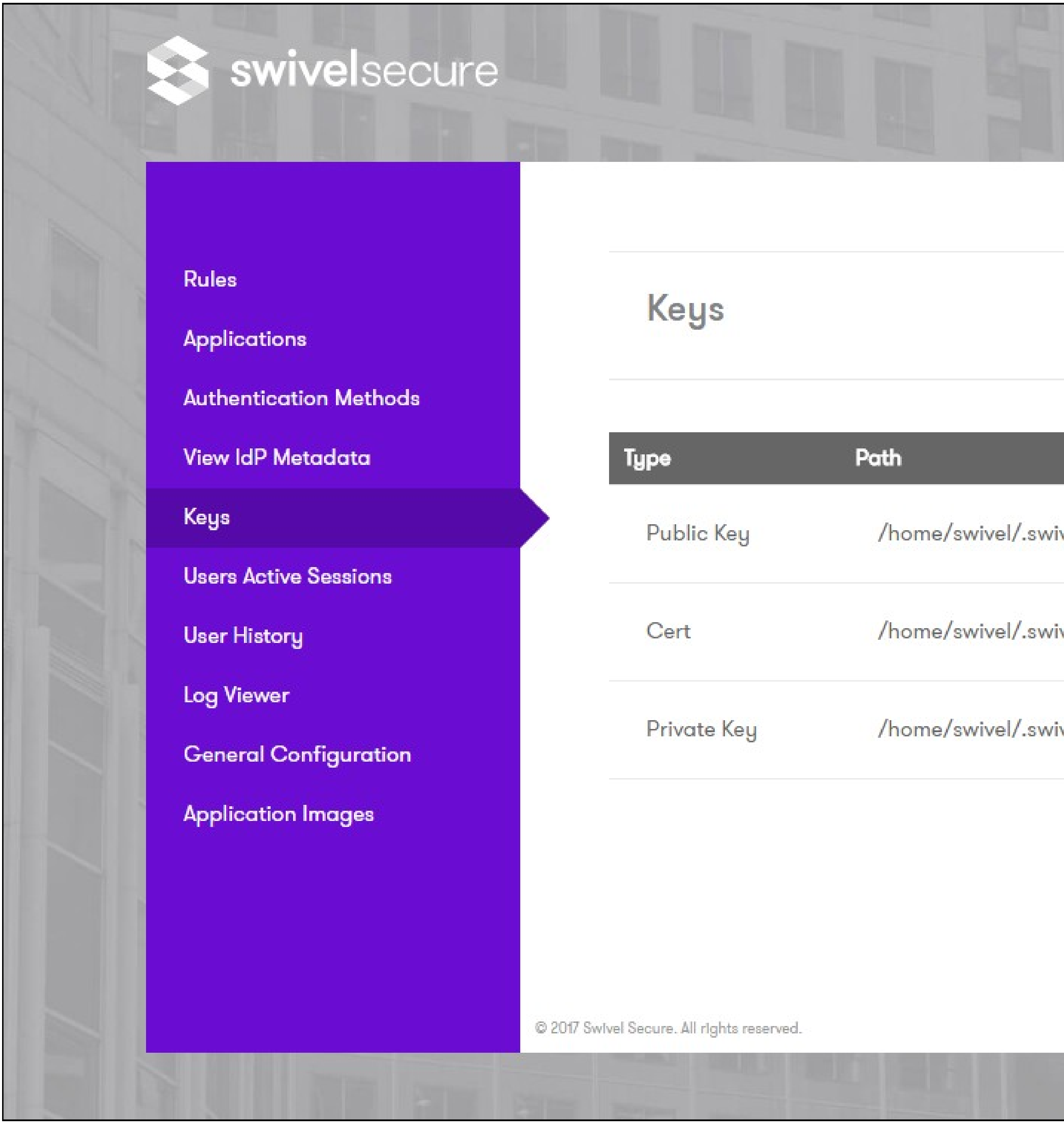
Setup Sentry Keys

Before you are able to create a Single Sign On configuration, you will need to setup the application URL and some Keys.

To specify the application URL you need to use the appliance CMI Menu. Select the Appliance menu, then select Sentry Menu and then select the option Set Application Root URL.

Keys are used to secure the communication between Sentry and Cloud Services. Please see a separate article: How To Create Keys On Cmi.

You will need to use the certificate you generate when creating SAML integrations. This can be retrieved from the View Keys menu option of Swivel Sentry



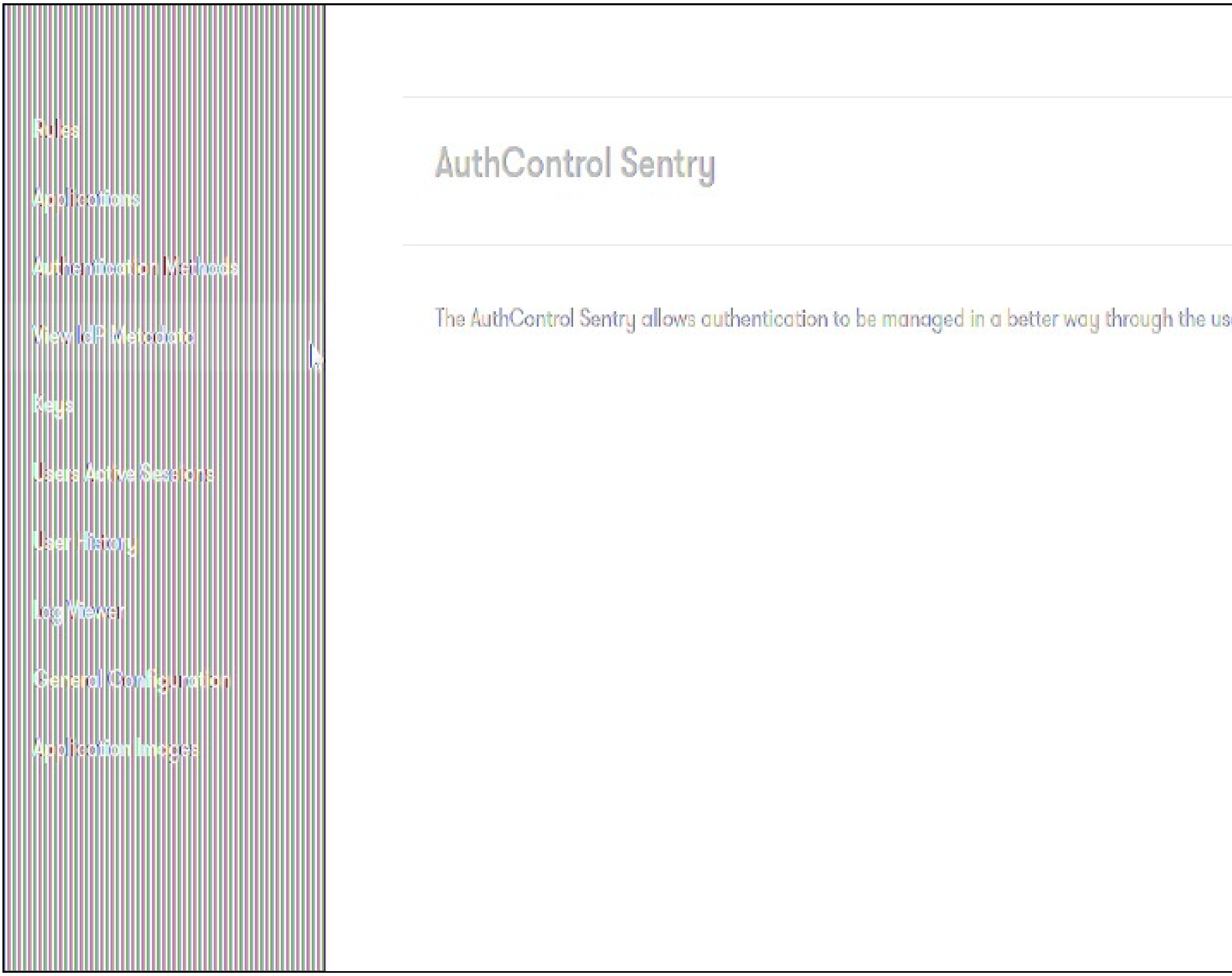
Keys

Type	Path
Public Key	/home/swivel/.swiv
Cert	/home/swivel/.swiv
Private Key	/home/swivel/.swiv

Viewing Certificate and Metadata

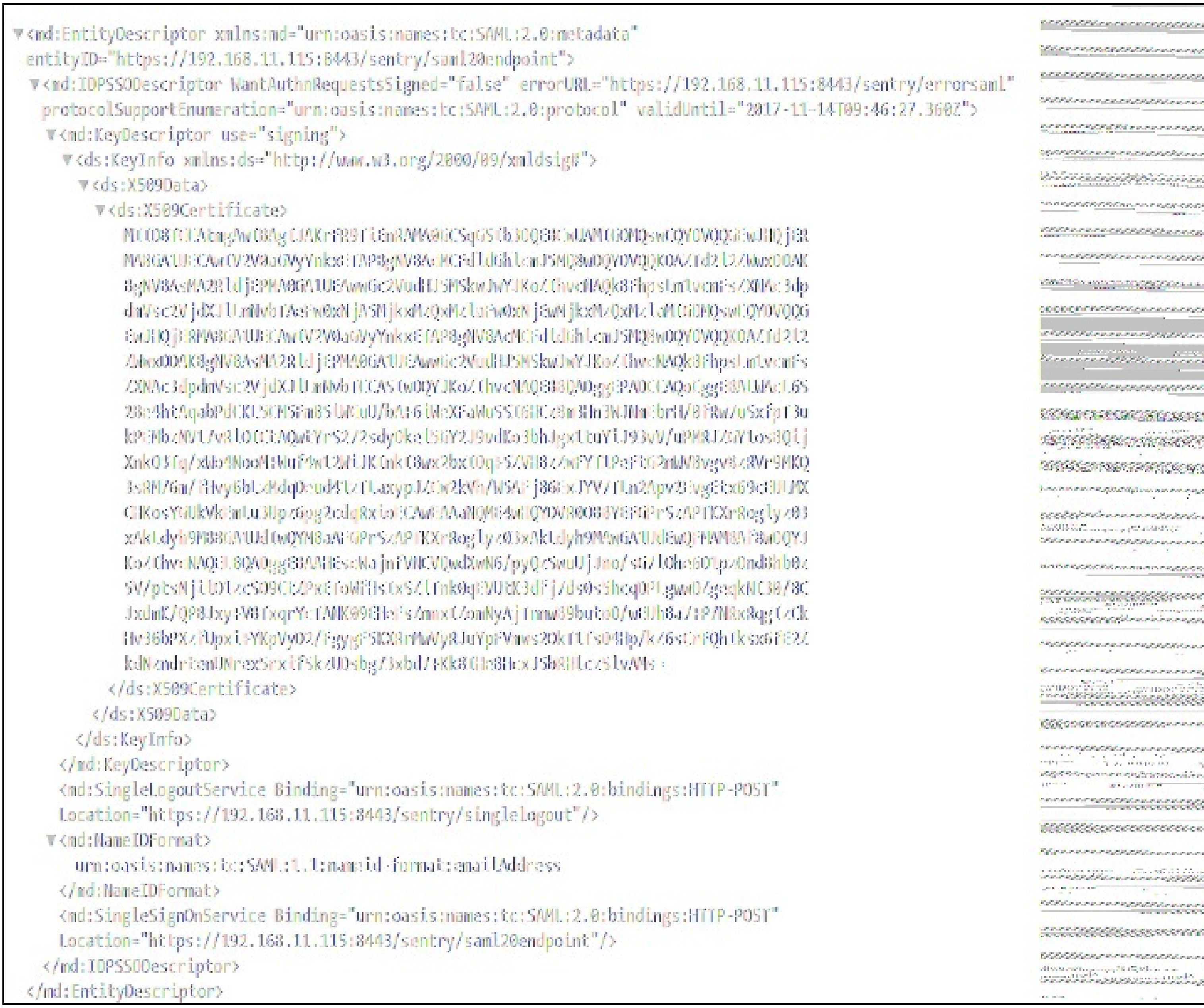
The certificates you have created will be required by cloud services in order to secure the communications between the cloud service provider and the Sentry installation. The certificate information is contained within the Sentry IdP Metadata and can be access by the cloud service provider via the View IdP Metadata link.

If the cloud service provider is not able to consume this metadata, the actual public key and certificate are also available for download from the Sentry Admin Console.



AuthControl Sentry

The AuthControl Sentry allows authentication to be managed in a better way through the us



```
▼<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://192.168.11.115:8443/sentry/saml20endpoint">
  ▼<md:IDPSSODescriptor WantAuthnRequestsSigned="false" errorURL="https://192.168.11.115:8443/sentry/errorsaml"
   protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" validUntil="2017-11-14T09:46:27.360Z">
    ▼<md:KeyDescriptor use="signing">
      ▼<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        ▼<ds:X509Data>
          ▼<ds:X509Certificate>
              MIIDBTCCAtmgAwIBAgIJAKrFR9TiEnRAMA0GCSqGSIb3DQEBCwUAMIGOMQswCQYDVQQGEwJHQjER
              MA8GA1UECAwIV2V0aGVyYnkxETAPBgNVBAcMCFdldGhlcmJ5MQ8wDQYDVQQKDAZTd2l2ZWwxDDAK
              BgNVBAsMA2RldjEPMA0GA1UEAwwGc2VudHJ5MSkwJwYJKoZIhvcNAQkBFhpsLm1vcmFsZXNAc3dp
              dmVsc2VjdXJlLmNvbTAeFw0xNjA5MjkxMzQxMzlaFw0xNjEwMjkxMzQxMzlaMIGOMQswCQYDVQQG
              EwJHQjERMA8GA1UECAwIV2V0aGVyYnkxETAPBgNVBAcMCFdldGhlcmJ5MQ8wDQYDVQQKDAZTd2l2
              ZWwxDDAKBgNVBAsMA2RldjEPMA0GA1UEAwwGc2VudHJ5MSkwJwYJKoZIhvcNAQkBFhpsLm1vcmFs
              ZXNAc3dpdmVsc2VjdXJlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALWAcL6S
              28e4htAqabPdCKL5CM5Fm85UKCuU/bA+6iWeXFaWuSS6HCz8m3Hn3NJNmebrH/8fRw/uSxfpI3u
              kPeMbzNV1/v8lOCCtAQwtYrS2/2sdyOkeI5GY2J9vdKo3bhJgxUbuYiJ93vV/uPMRJ/GYlos8Qij
              XnkO3fq/xWo4NooMtNuf4wt2MiUKGnkC8wx2bxtOq+SZVH8z/wFYTlPaFtG2mWV8vgv8z8Vr9MKQ
              3s8M/6m/fHvy6bLzMdqDcud4tzTLaxypJZCw2kVh/WSAfj86ExJYV/TLn2Apv2EvgEtx69cEULMX
              CHKosYGUkVkEmLu3Up46pg2cdqRxioECAwEAAaNQME4wHQYDVR0OBBYEFGPrSzAPTKXrRoglyz03
              xAkLdyh9MB8GA1UdIwQYMBaAFGPrSzAPTKXrRoglyz03xAkLdyh9MAwGA1UdEwQFMAMBAf8wDQYJ
              KoZIhvcNAQELBQADggEBAAHEscWajnfVNCVQwdXwN6/pyQzSwuUjJmo/sti/lOhe6D1pzOnd8hb0z
              SV/ptsNjiLDIzcS09CtZPxEfoWiHsCxSZlTnk0qEVUtK3dfj/ds0sShcqDPLgwwD/geqkNC38/8C
              JxdmK/QP8JxyPV8IxqrYcIANK09Ehe1s/mmxC/onNyAjInnw89butoO/wEUh8a/tP/NRx8qgCzCk
              Hv36bPXzfUpxiFYKpVyO2/FggFSKX8rMWVy8JuYpFVmws2DkTLTsO4Rp/k/6sCrFQhIksx6fE2Z
              kdNzndrEanUNrex5rxifSkzUDsbg/3xbd/FKk8Gle8HexJSb8HLczSlvAMs=
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://192.168.11.115:8443/sentry/singleLogout"/>
  ▼<md:NameIDFormat>
      urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    </md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://192.168.11.115:8443/sentry/saml20endpoint"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

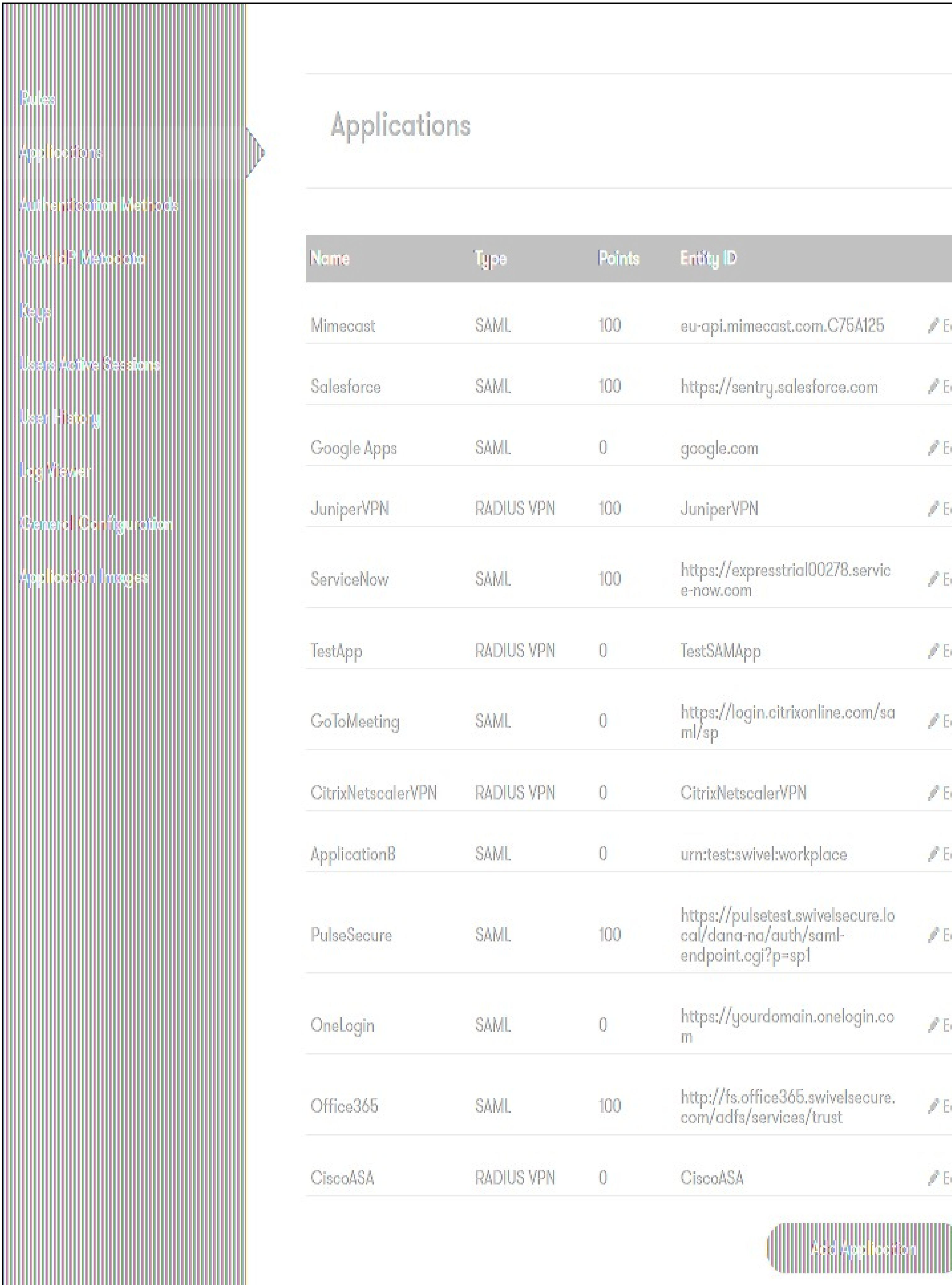
Defining Applications

Applications that support federation standards such as SAML and ADFS will use those standards to integrate with Sentry. Legacy applications and services will need to integrate in a different way and they will use Swivel Secure?s Proprietary Claims approach which works in a similarly way to SAML but works with the constraints of non-cloud systems such as VPNs.

The flow is as follows:

1. The user goes to the Sentry Universal Login Page and selects the VPN application.
2. The user is asked to present credentials as per the policies and the Sentry uses these credentials to request a Claim for that endpoint.
3. The user is redirected to the VPN login page with the claim as the password parameter.
4. The user logs into VPN using their username and claim.
5. The core then validates the claim, checking that the claim was issued for this endpoint. So in this case the Application name on the Sentry must match the NAS name on the core.

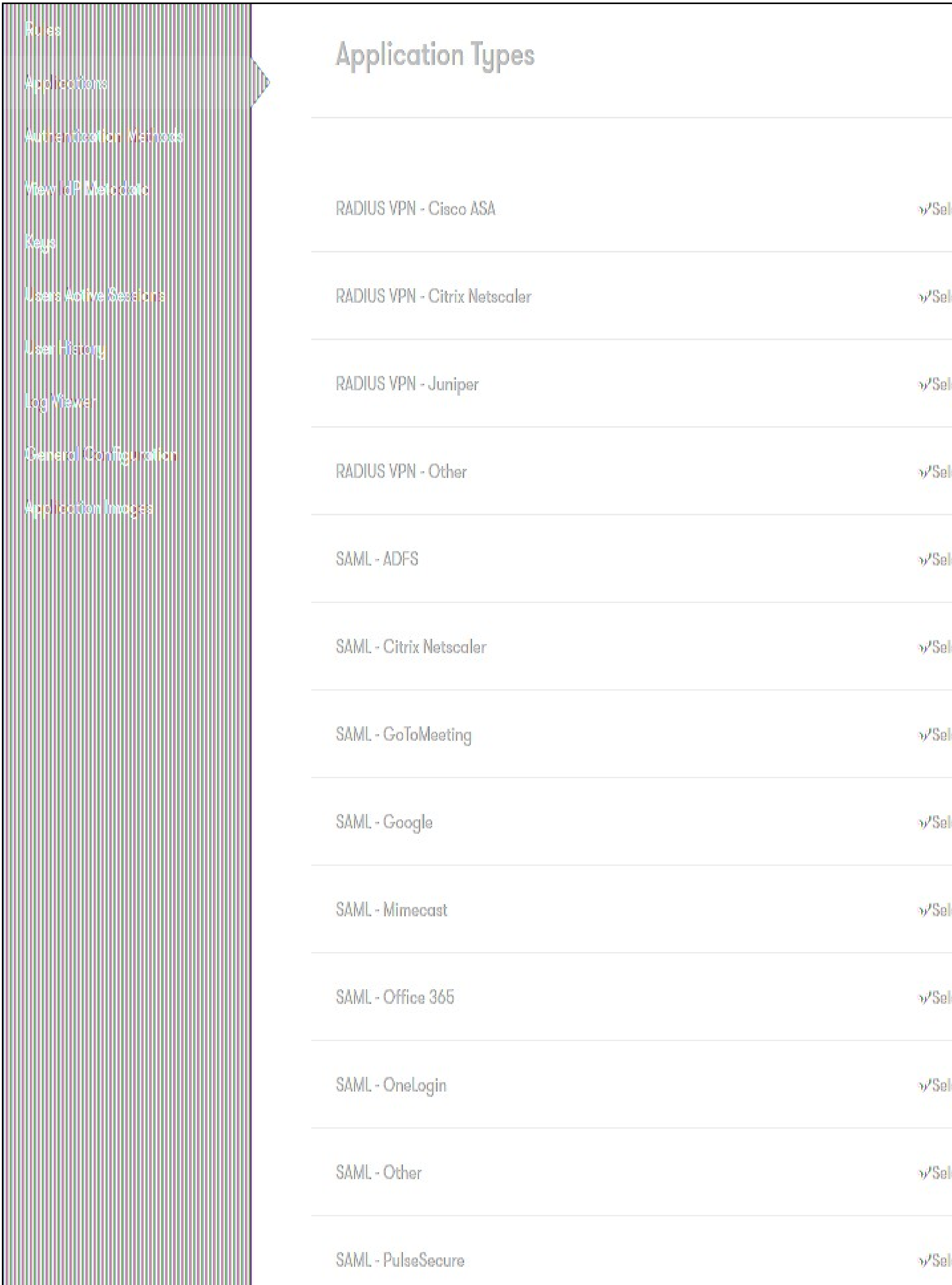
To create a new application, go to the Applications section and click on Add Application:



Applications

Name	Type	Points	Entity ID	
Mimecast	SAML	100	eu-api.mimecast.com.C75A125	✎ E
Salesforce	SAML	100	https://sentry.salesforce.com	✎ E
Google Apps	SAML	0	google.com	✎ E
JuniperVPN	RADIUS VPN	100	JuniperVPN	✎ E
ServiceNow	SAML	100	https://expresstrial00278.service-now.com	✎ E
TestApp	RADIUS VPN	0	TestSAMApp	✎ E
GoToMeeting	SAML	0	https://login.citrixonline.com/saml/sp	✎ E
CitrixNetscalerVPN	RADIUS VPN	0	CitrixNetscalerVPN	✎ E
ApplicationB	SAML	0	urn:test:swivel:workplace	✎ E
PulseSecure	SAML	100	https://pulsetest.swivelsecure.local/dana-na/auth/saml-endpoint.cgi?p=sp1	✎ E
OneLogin	SAML	0	https://yourdomain.onelogin.com	✎ E
Office365	SAML	100	http://fs.office365.swivelsecure.com/adfs/services/trust	✎ E
CiscoASA	RADIUS VPN	0	CiscoASA	✎ E

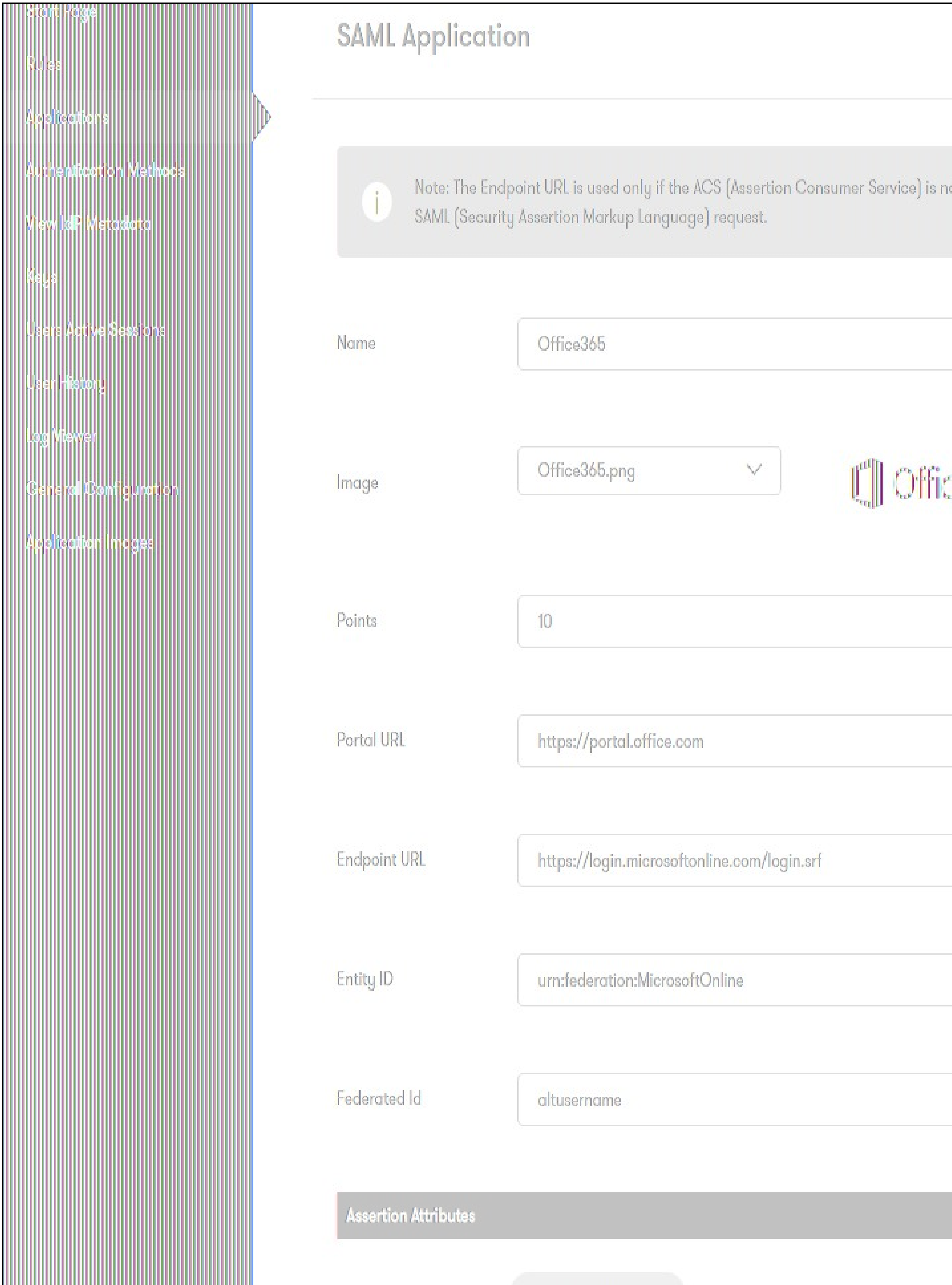
A list of default applications will be displayed. If the application that you need to integrate with does not appear on the list click SAML-Other or RADIUS VPN-Other depending of the integration type required.



Application Types

RADIUS VPN - Cisco ASA	✓Sel
RADIUS VPN - Citrix Netscaler	✓Sel
RADIUS VPN - Juniper	✓Sel
RADIUS VPN - Other	✓Sel
SAML - ADFS	✓Sel
SAML - Citrix Netscaler	✓Sel
SAML - GoToMeeting	✓Sel
SAML - Google	✓Sel
SAML - Mimecast	✓Sel
SAML - Office 365	✓Sel
SAML - OneLogin	✓Sel
SAML - Other	✓Sel
SAML - PulseSecure	✓Sel

Example SAML Application:



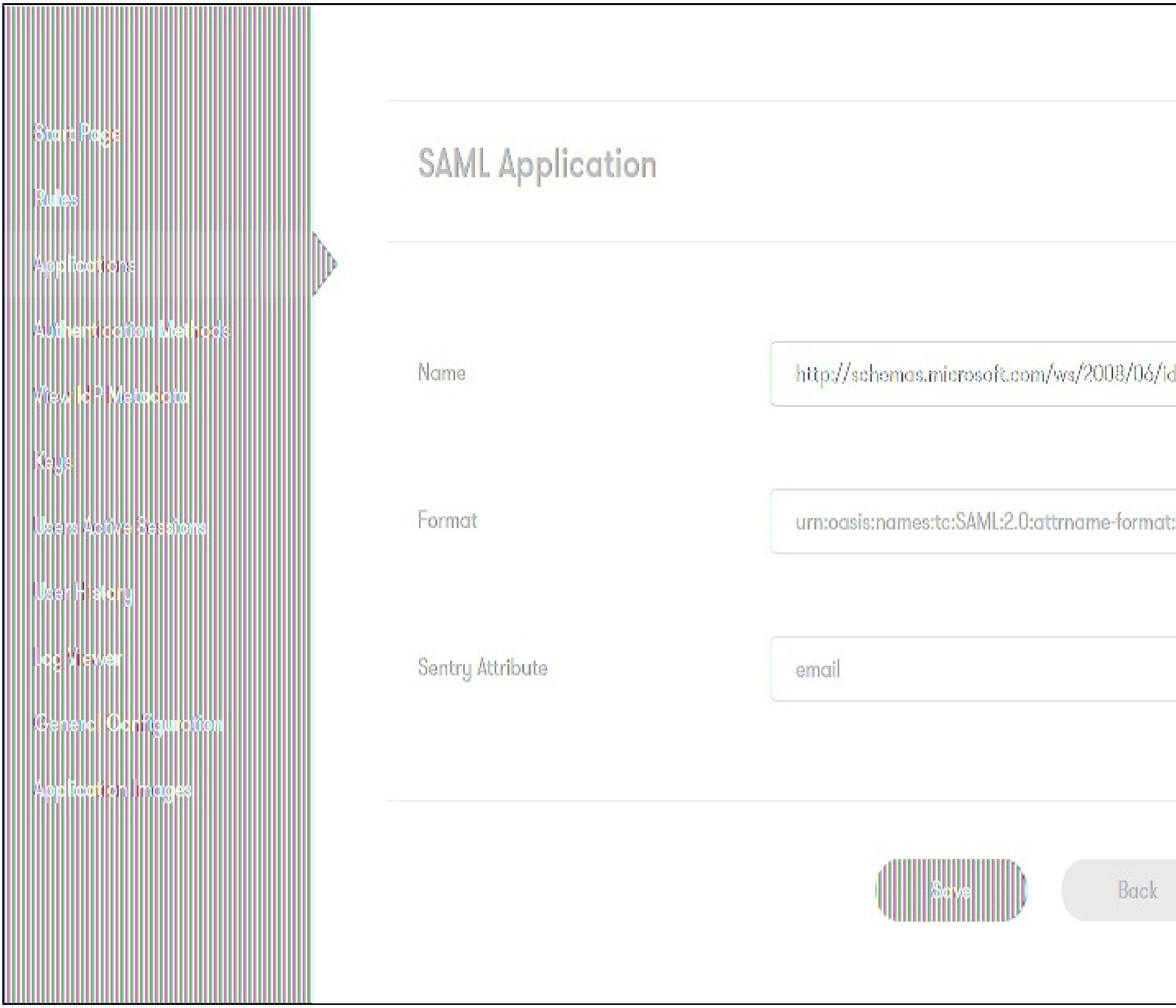
SAML Application

Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is no
SAML (Security Assertion Markup Language) request.

Name	Office365
Image	Office365.png
Points	10
Portal URL	https://portal.office.com
Endpoint URL	https://login.microsoftonline.com/login.srf
Entity ID	urn:federation:MicrosoftOnline
Federated Id	altusername

Assertion Attributes

By default, Sentry returns a single assertion, using the federated ID as defined in the application. Note that this value must correspond to a Sentry attribute defined in the Sentry Core. You can request additional SAML assertions by clicking "Add Attribute"



SAML Application

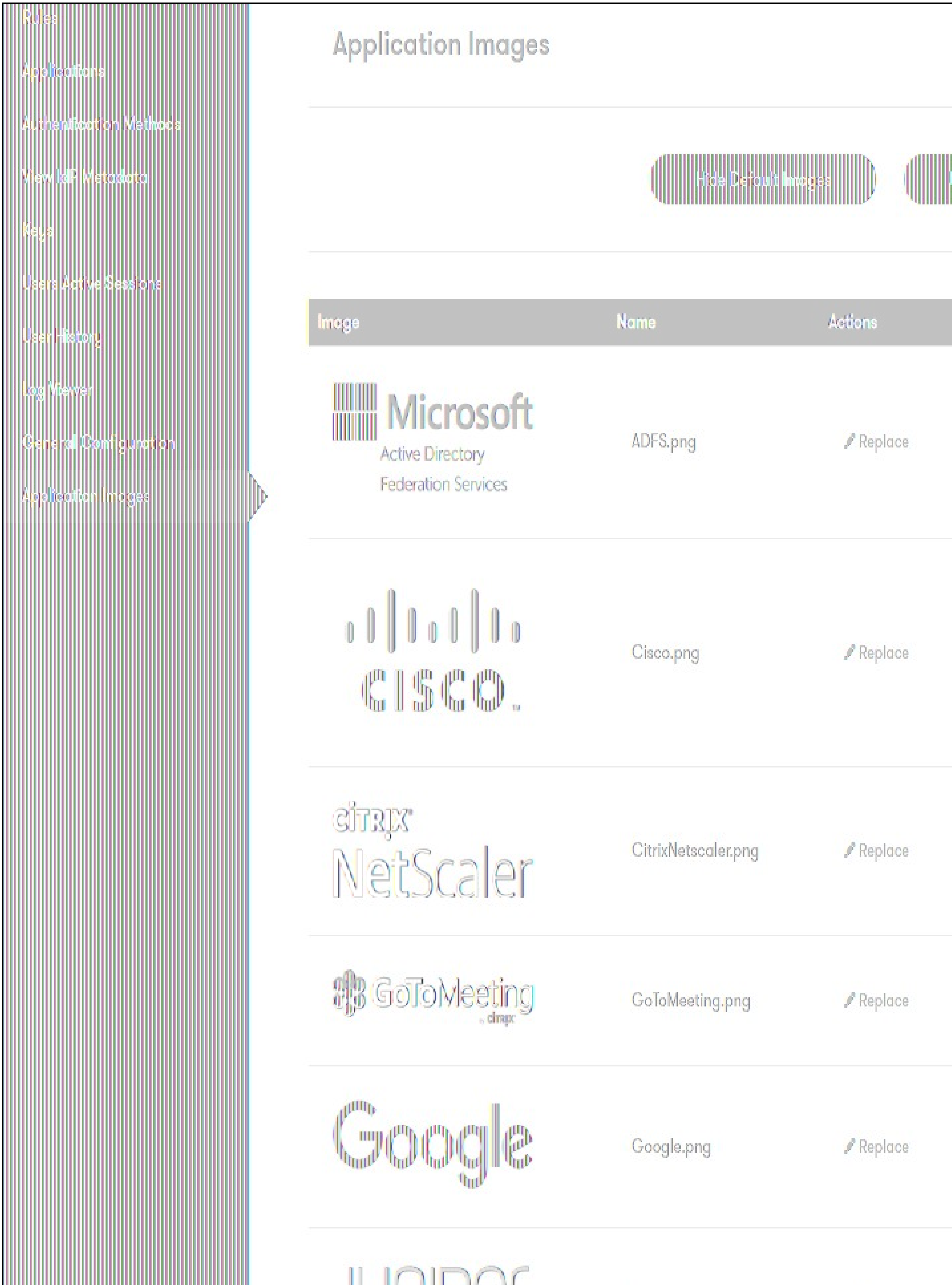
Name: http://schemas.microsoft.com/ws/2008/06/id

Format: urn:oasis:names:tc:SAML:2.0:attrname-format:

Sentry Attribute: email

The name and format are dependent on the target application. All attributes must be defined as custom attributes in Sentry.

There are some application images added by default. If you need to add a new application image or update the existing ones, please go to the section Application Images.



Application Images

Image	Name	Actions
Microsoft Active Directory Federation Services	ADFS.png	Replace
cisco	Cisco.png	Replace
citrix NetScaler	CitrixNetscaler.png	Replace
GoToMeeting by citrix	GoToMeeting.png	Replace
Google	Google.png	Replace

Defining Authentication Methods

Sentry supports a range of user authentication types. These can be assigned different numbers of points. Generally, the stronger the authentication the more points are allocated to the authentication type.

For example, if you were using Sentry to protect two services, one more security-critical than the other, you could enforce two-factor authentication for the more secure service by

- Making the required trust points for the more secure equal to 200 and 100 for the less secure.
- Allocating 200 points to two-factor authentication types (e.g. token) and 100 points for Image-based authentication (e.g. PINpad).

Then when the user attempts to access the more secure service they will be prompted to use a two-factor authentication method and only be allowed access if they complete authentication in that way.

You can assign any scores you like to any authentication types, being mindful of the points required to access services and the points that a user can gain from the rules.

All authentication types are enforced by the Swivel Core Server. Current Supported Types Are

Password Check of Users Repository (eg AD) Password

TURing Image-based authentication via TURing Image

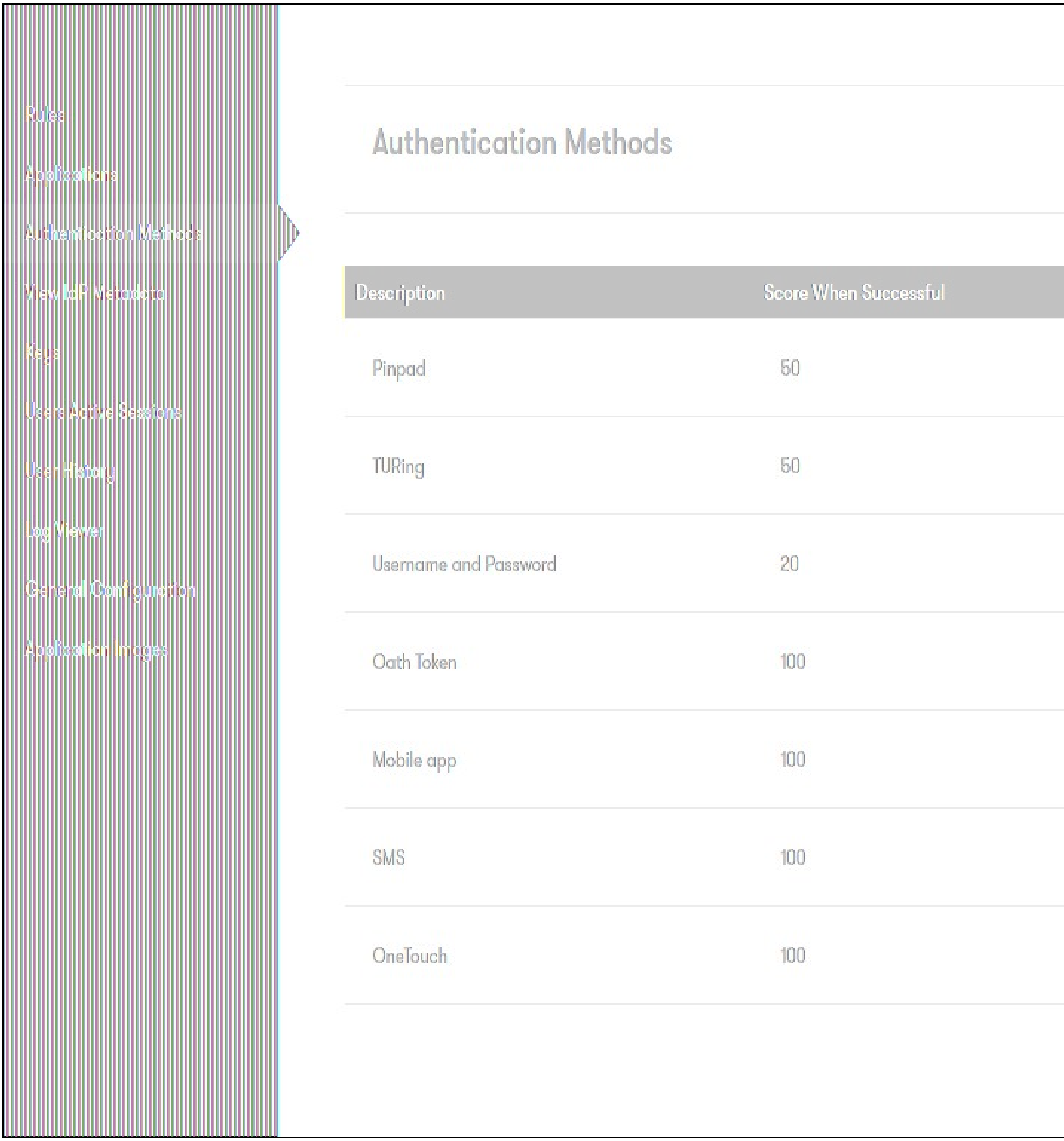
PINpad Image-based authentication via PINpad Image

SMS SMS-based authentication

Soft Token AuthControl Mobile Client Authentication

OneTouch AuthControl Sentry Push Authentication

OATH Token OATH Hardware Token

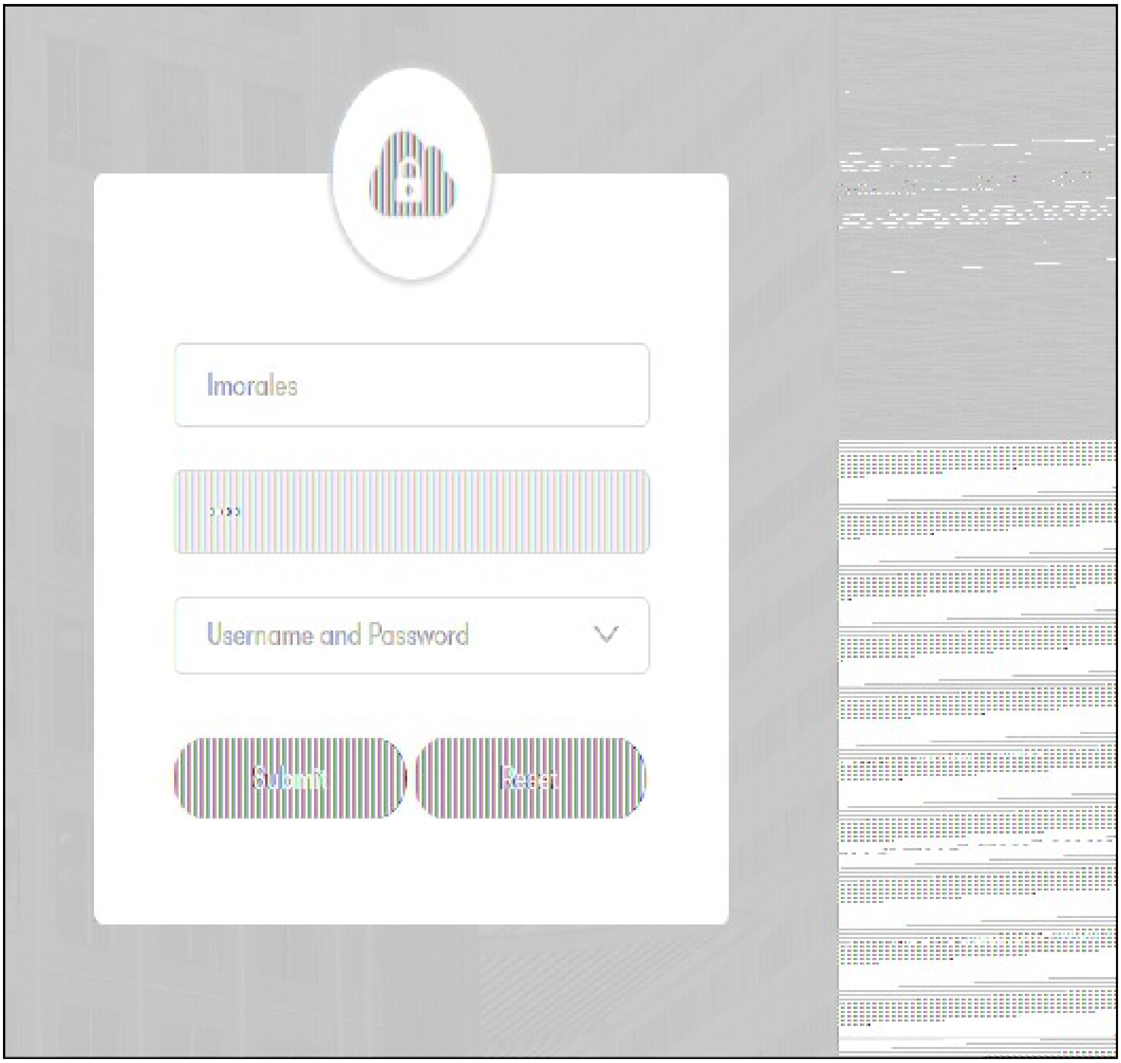


Authentication Methods

Description	Score When Successful
Pinpad	50
TURing	50
Username and Password	20
Oath Token	100
Mobile app	100
SMS	100
OneTouch	100

If a type of authentication is allocated zero points, it means it is not supported by this installation of Sentry

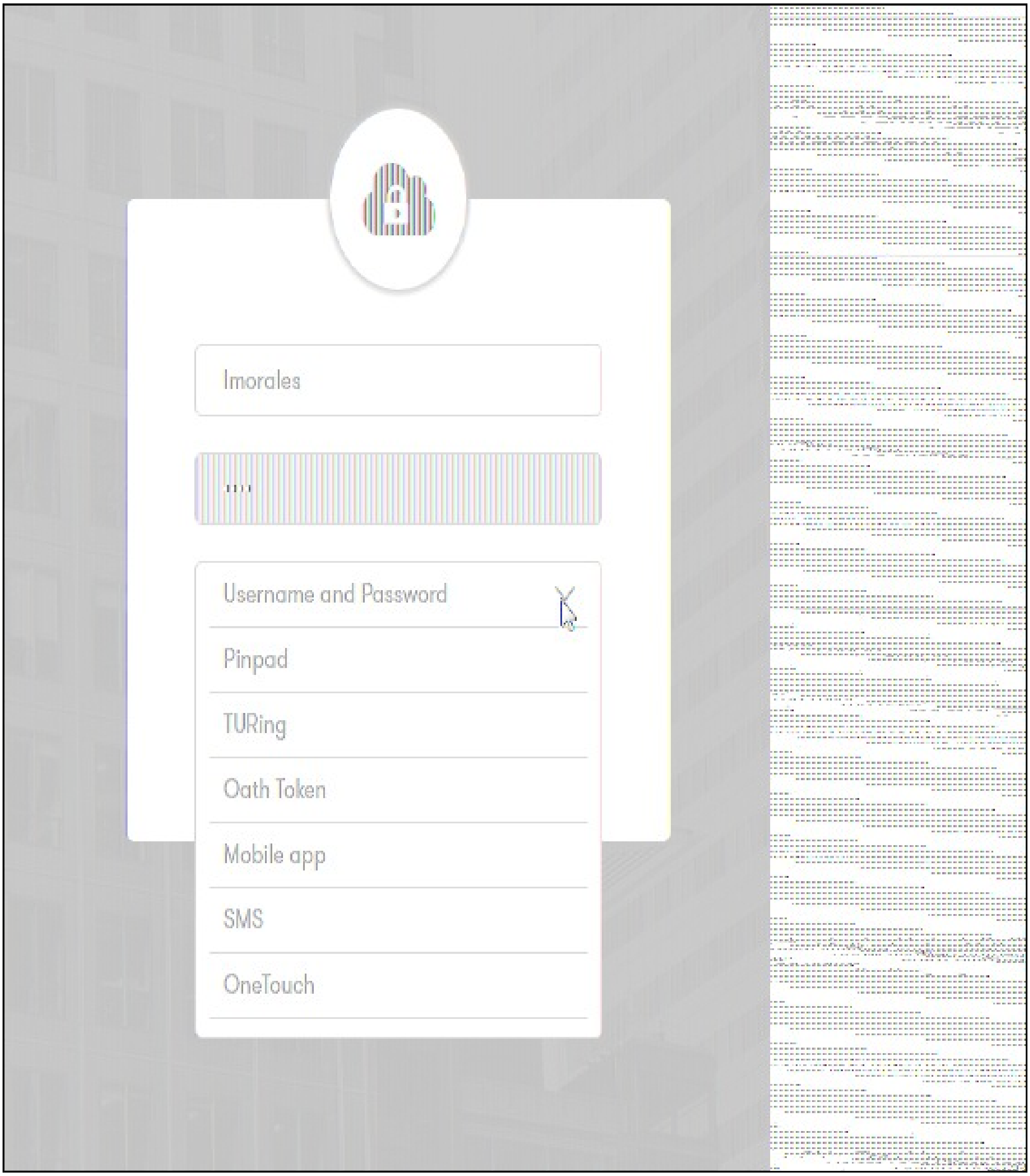
When a user tries to access an application, they will be offered the lowest point authentication method, although they can select an alternative method if they choose. By default, the user will be able to select all authentication methods.



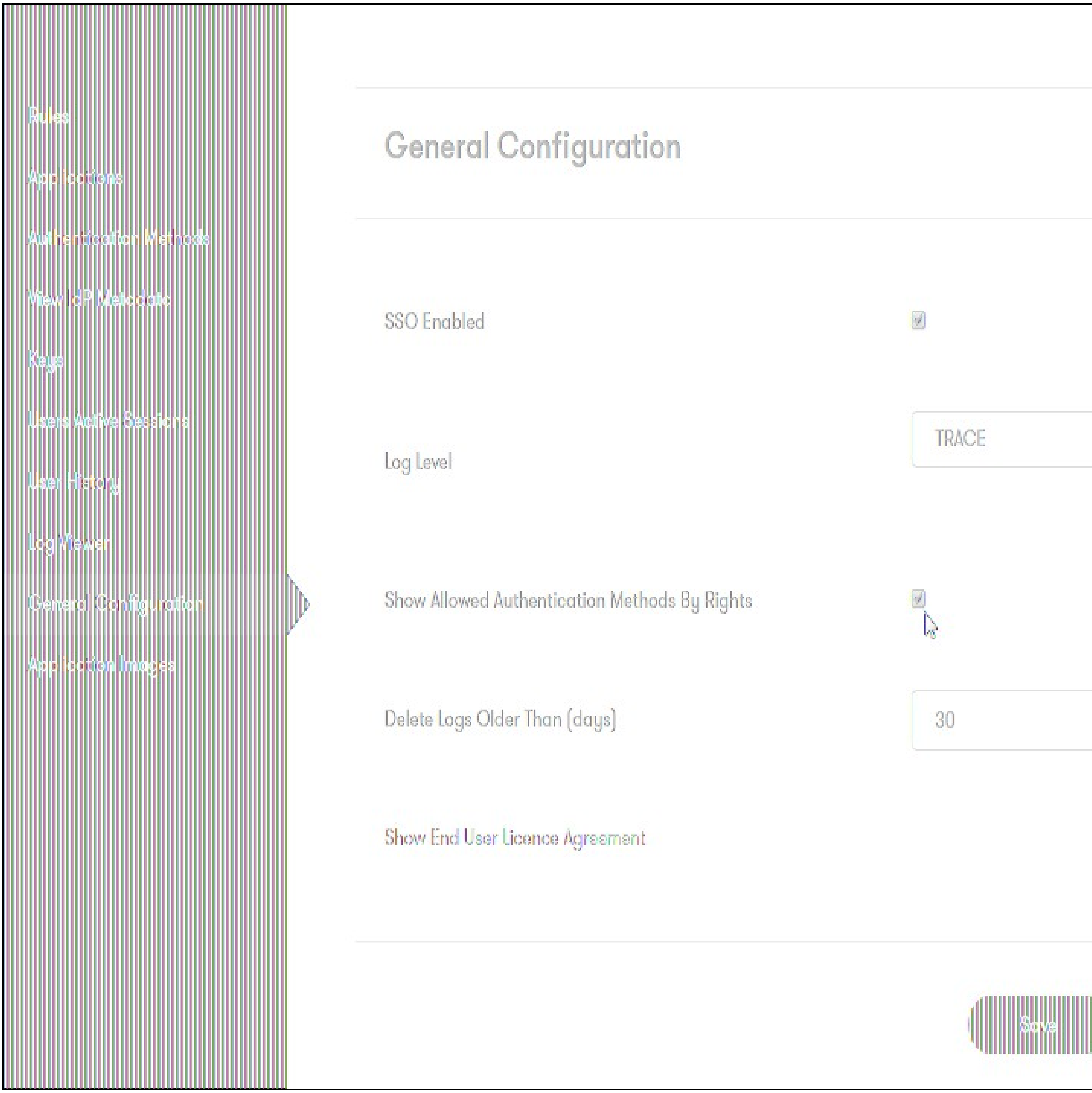
lmorales

••••

Username and Password



Alternatively, an administrator can select the option only to show authentication methods for which the user has the rights to use. To do so you have to go to General Configuration and tick Show Allowed Authentication Methods By Rights check-box. This way users will only see authentication methods that they can actually use.



General Configuration

SSO Enabled ☑

Log Level TRACE

Show Allowed Authentication Methods By Rights ☑

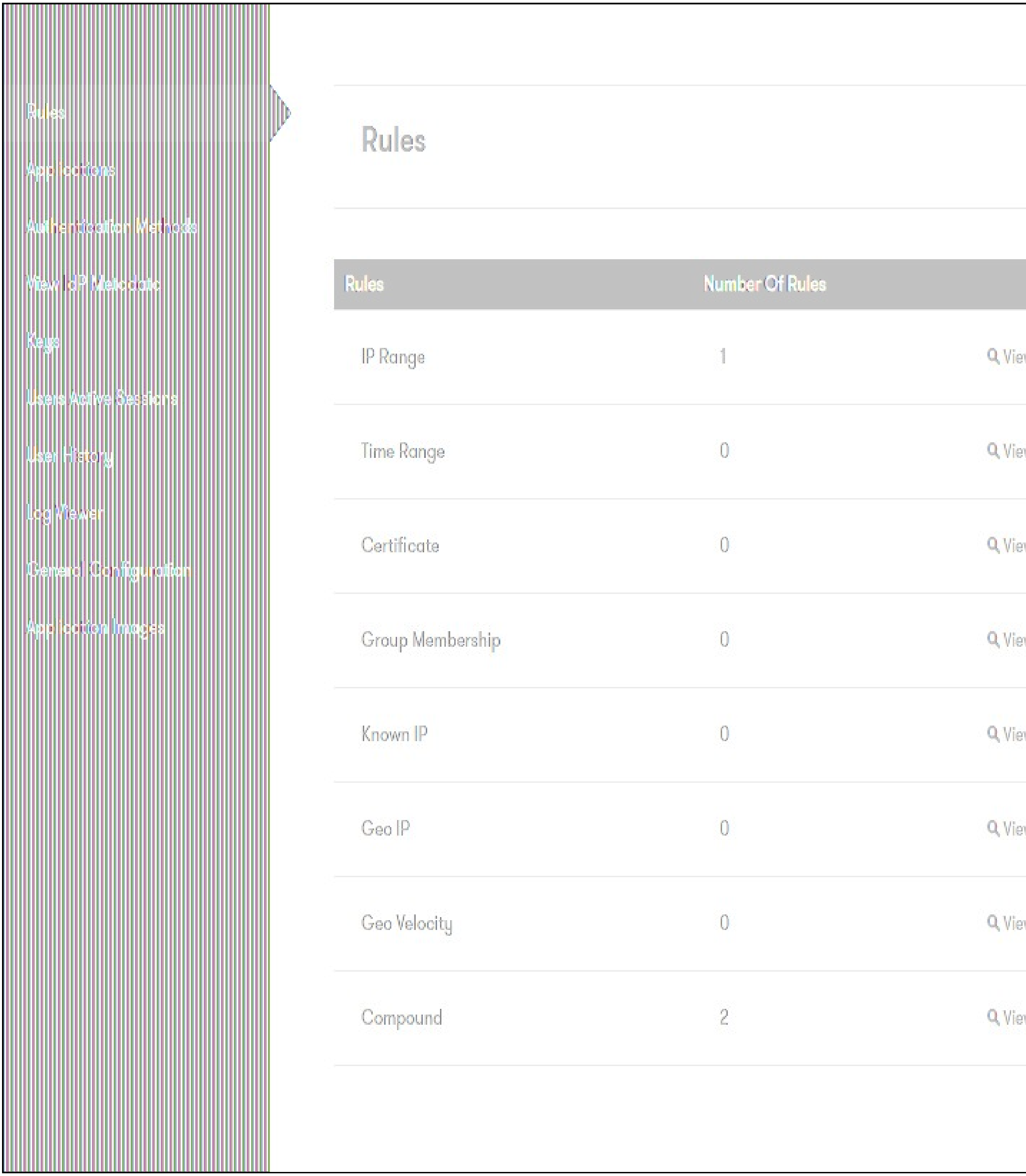
Delete Logs Older Than (days) 30

Show End User Licence Agreement

When a user accesses the service and is shown the authentication method, the authentication method will also show the service name / logo to indicate which service the user is trying to access.

Defining Sentry Rules

By allocating points to Services and Authentication Types, you can use Sentry to implement a set of static rules that dictate how a user needs to authenticate to certain services. Sentry rules allow you to add a dynamic element to user access, meaning that you can refine the access rules to reflect the specific risk elements of a user?s access.



Rules

Rules	Number Of Rules	
IP Range	1	🔍 Vie
Time Range	0	🔍 Vie
Certificate	0	🔍 Vie
Group Membership	0	🔍 Vie
Known IP	0	🔍 Vie
Geo IP	0	🔍 Vie
Geo Velocity	0	🔍 Vie
Compound	2	🔍 Vie

To define a rule, you set the parameter for that rule and then the score when that rule is valid. For example, for IP address you specify the IP address range and a score. The user will be allocated that score if their IP address is part of the specified range. Scores can be positive or negative.

You can specify multiple rules of each type

You can currently specify rules based on the following user and environmental attributes.

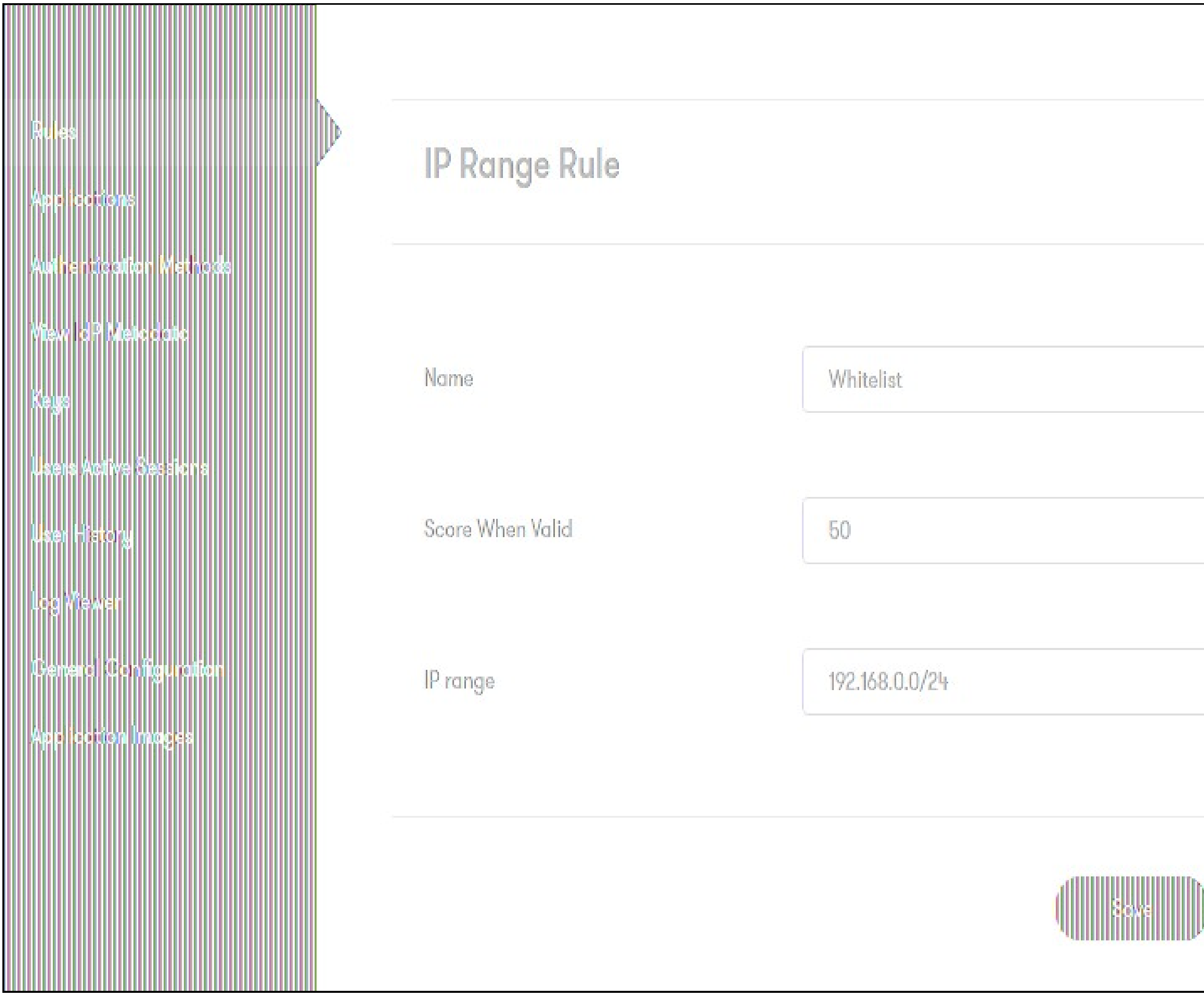
IP Address (White List or Black List)

These rules allow you to add trust points if the user is coming from a whitelist IP address or deduct points if the IP address is on a blacklist.

Parameters:

IP Address Range, e.g. 192.168.0.0/24

Examples

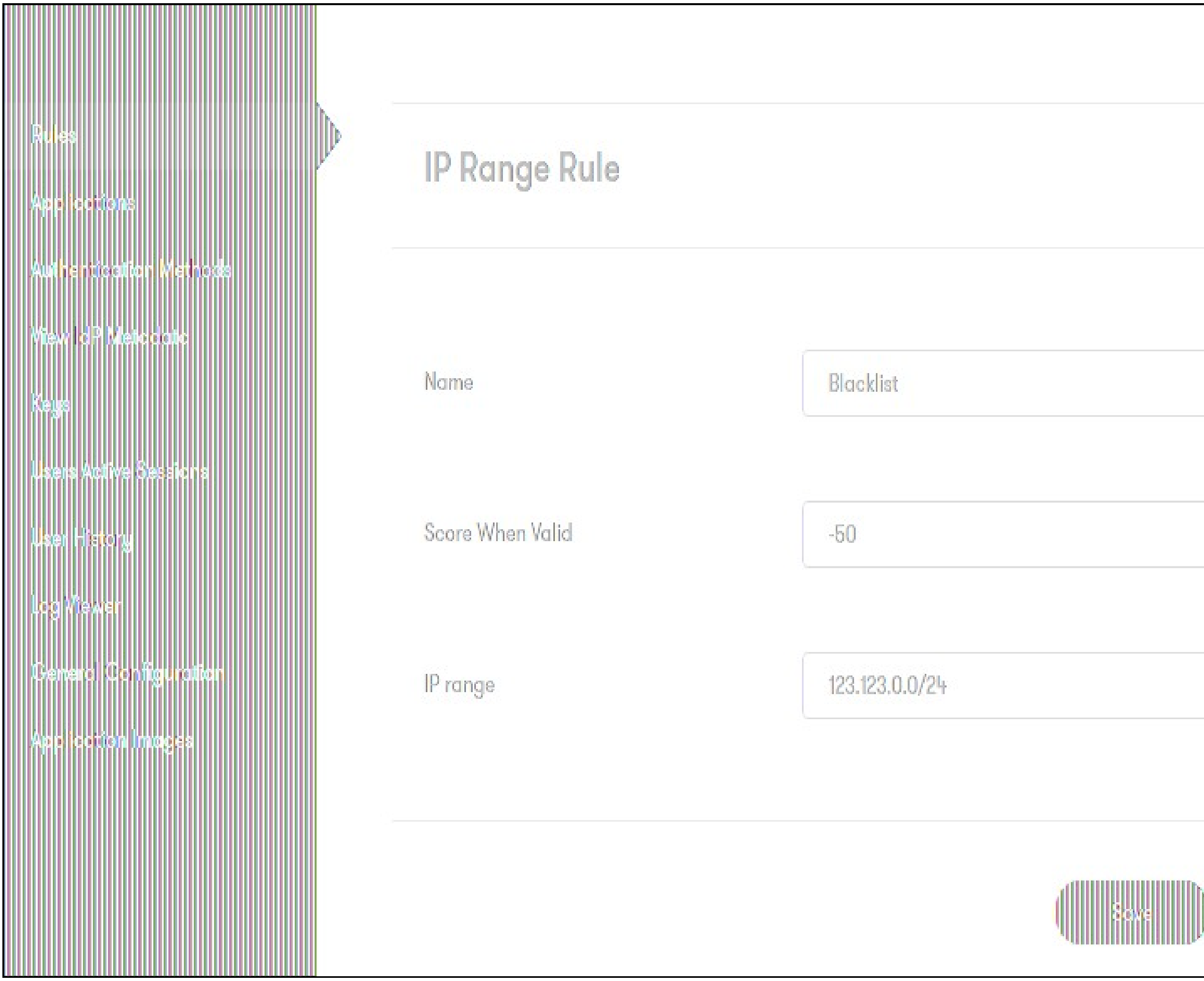


IP Range Rule

Name: Whitelist

Score When Valid: 50

IP range: 192.168.0.0/24



IP Range Rule

Name: Blacklist

Score When Valid: -50

IP range: 123.123.0.0/24

Time Range

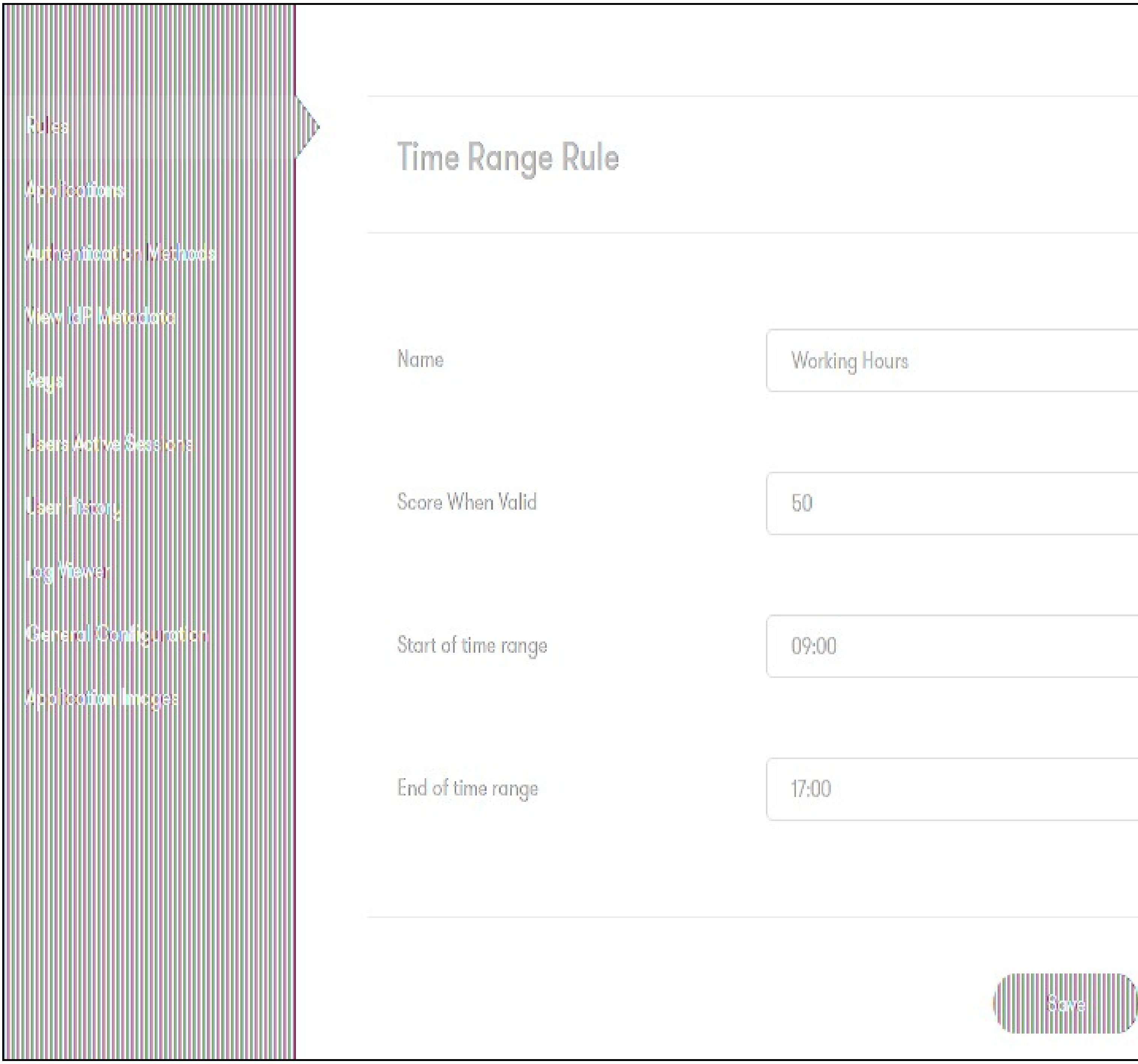
Allows you to add points or deduct points based on the time of day that the user is attempting access.

Parameters:

Start of Time Range: Start of time range of interest

End of Time Range: End of time range of interest

Example:



Time Range Rule

Name: Working Hours

Score When Valid: 50

Start of time range: 09:00

End of time range: 17:00

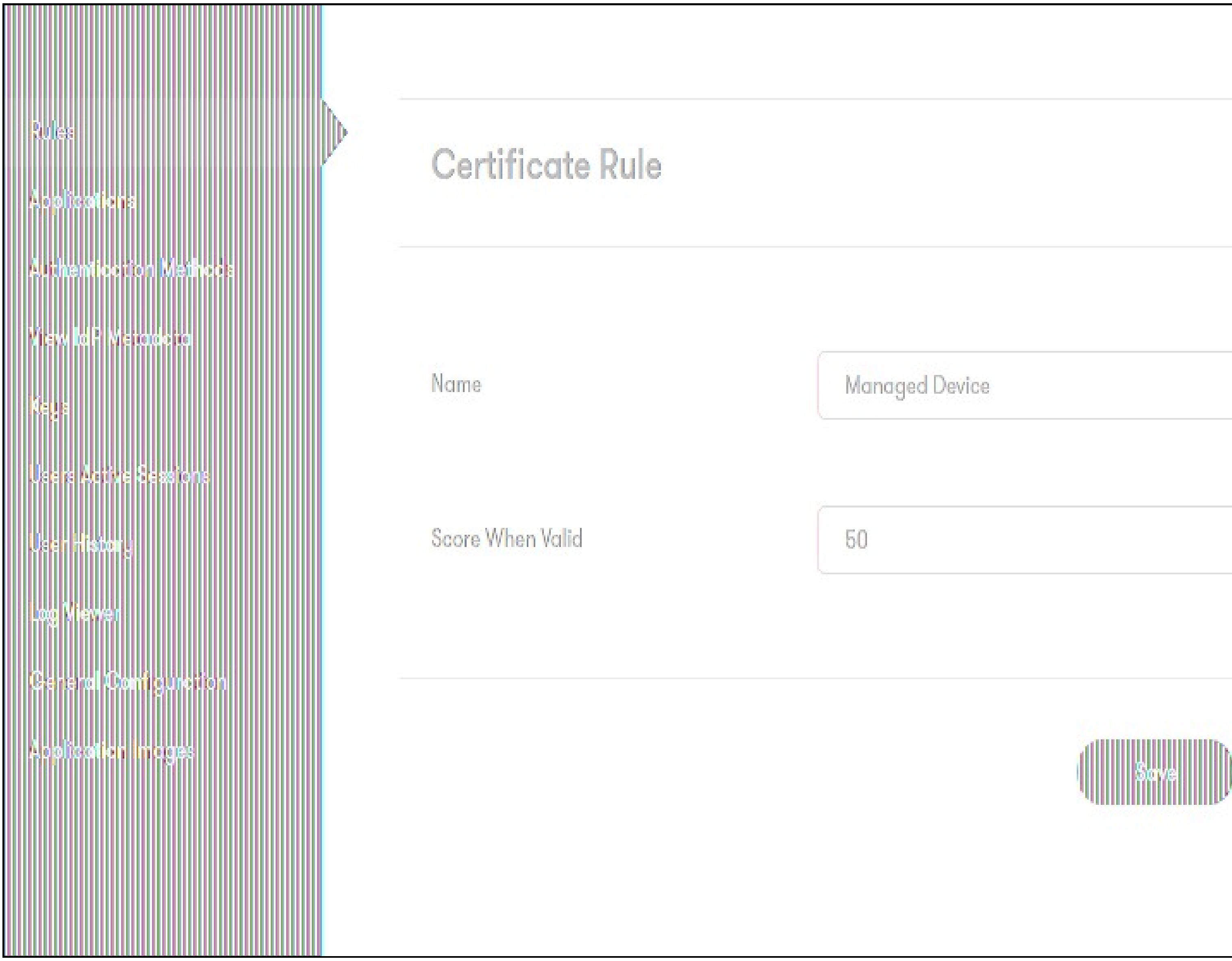
Certificate

Allows you to add points if the user has a valid client-side X509 Certificate installed

Parameters:

None

Example:



Certificate Rule

Name: Managed Device

Score When Valid: 50

For further details on configuration, check Client Authentication using Certificates

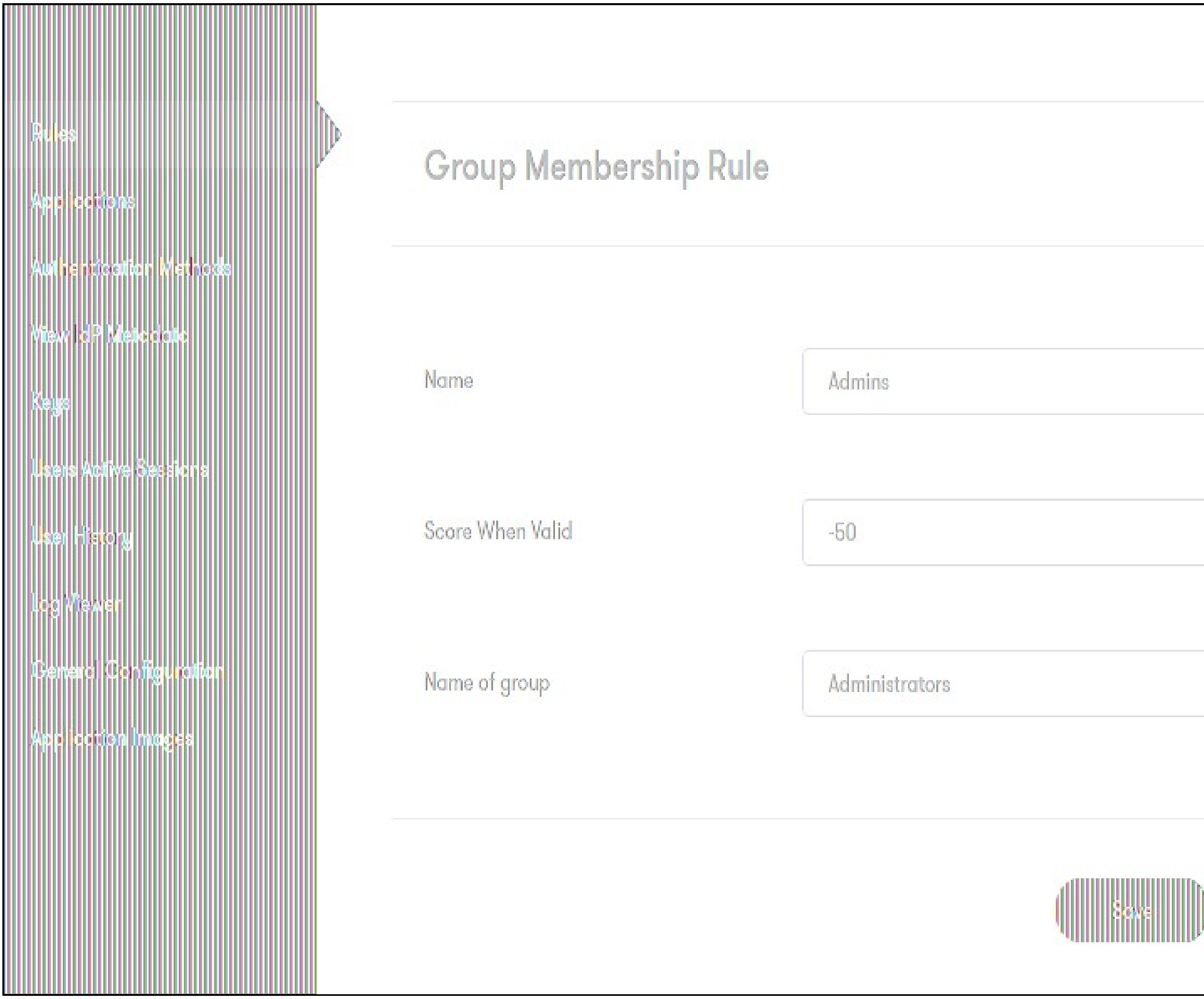
Group Membership

Allows you to add or deduct points based on whether a user is a member of a particular group.

Parameters:

Name of Group. The name of the Sentry Users group that is of significance.

Example:



Group Membership Rule

Name: Admins

Score When Valid: -50

Name of group: Administrators

Known IP

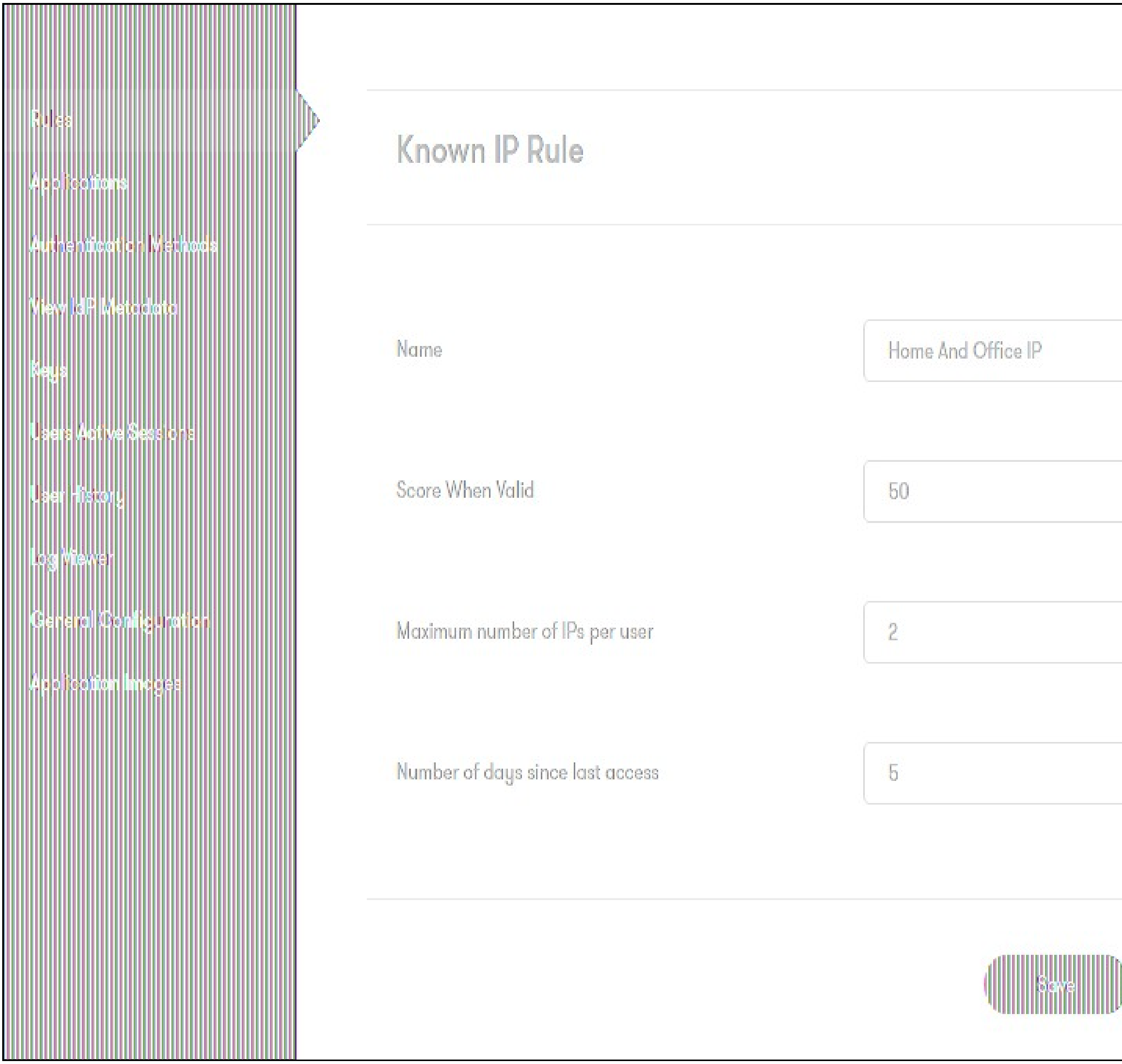
Allows you to add points if a user is attempting to access a service from an IP address that they have successfully accessed before.

Parameters:

Maximum Number of IP Address: Sentry will record up to a maximum number of IP addresses that a user has successfully authenticated from to cover for example home and office IP Addresses

Number of Days since Last Access: The number of days after the last successful authentication that an IP address will be treated as being significant.

Example:



Known IP Rule

Name: Home And Office IP

Score When Valid: 50

Maximum number of IPs per user: 2

Number of days since last access: 5

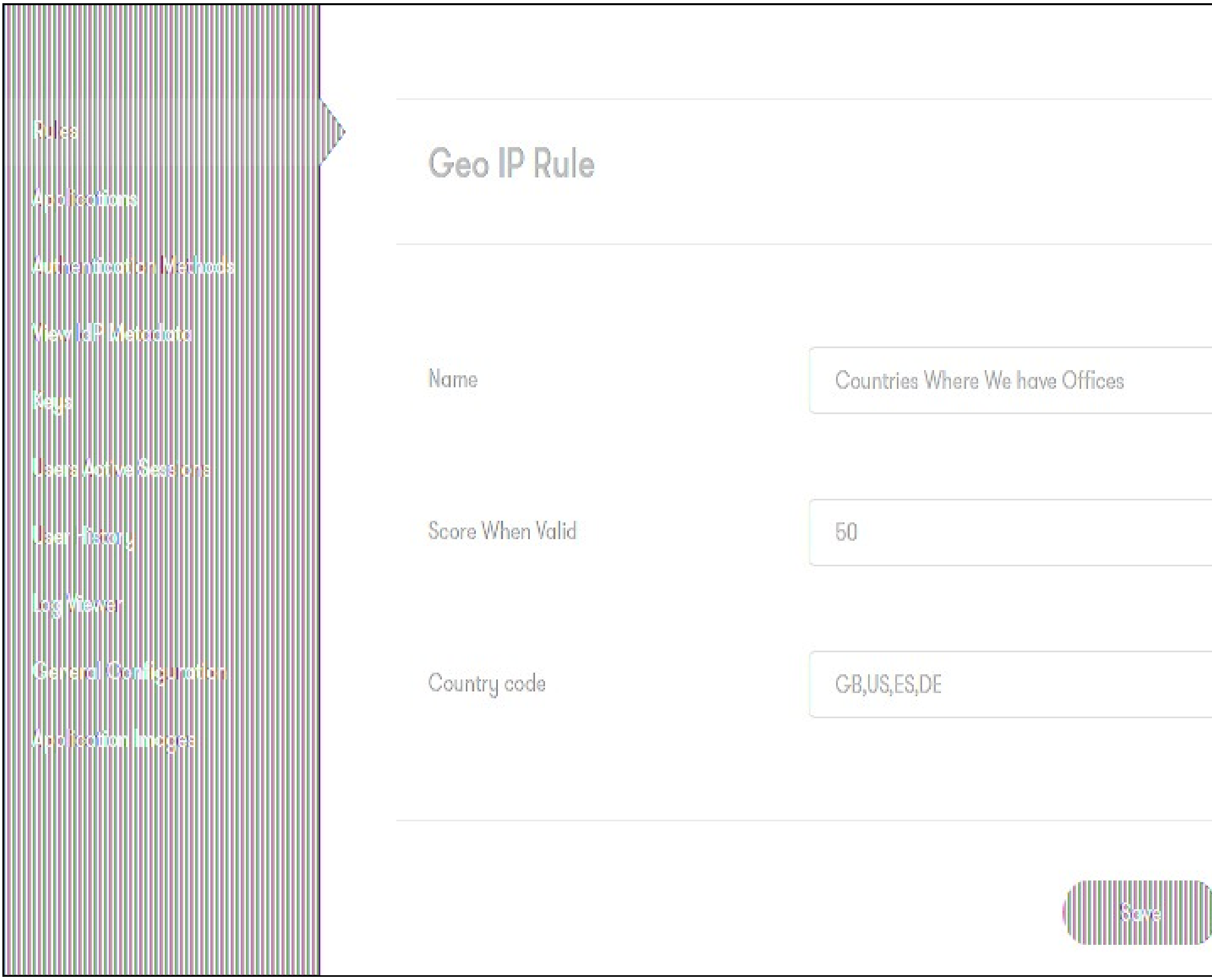
GeoIP

Allows you to add or deduct trust points based on from which country a user is attempting access, according to their Geo IP location.

Parameters:

Country Code: List of ISO-3166 standard country codes related to this rule. List is comma separated, eg GB,FR

Example:



Geo IP Rule

Name: Countries Where We have Offices

Score When Valid: 50

Country code: GB,US,ES,DE

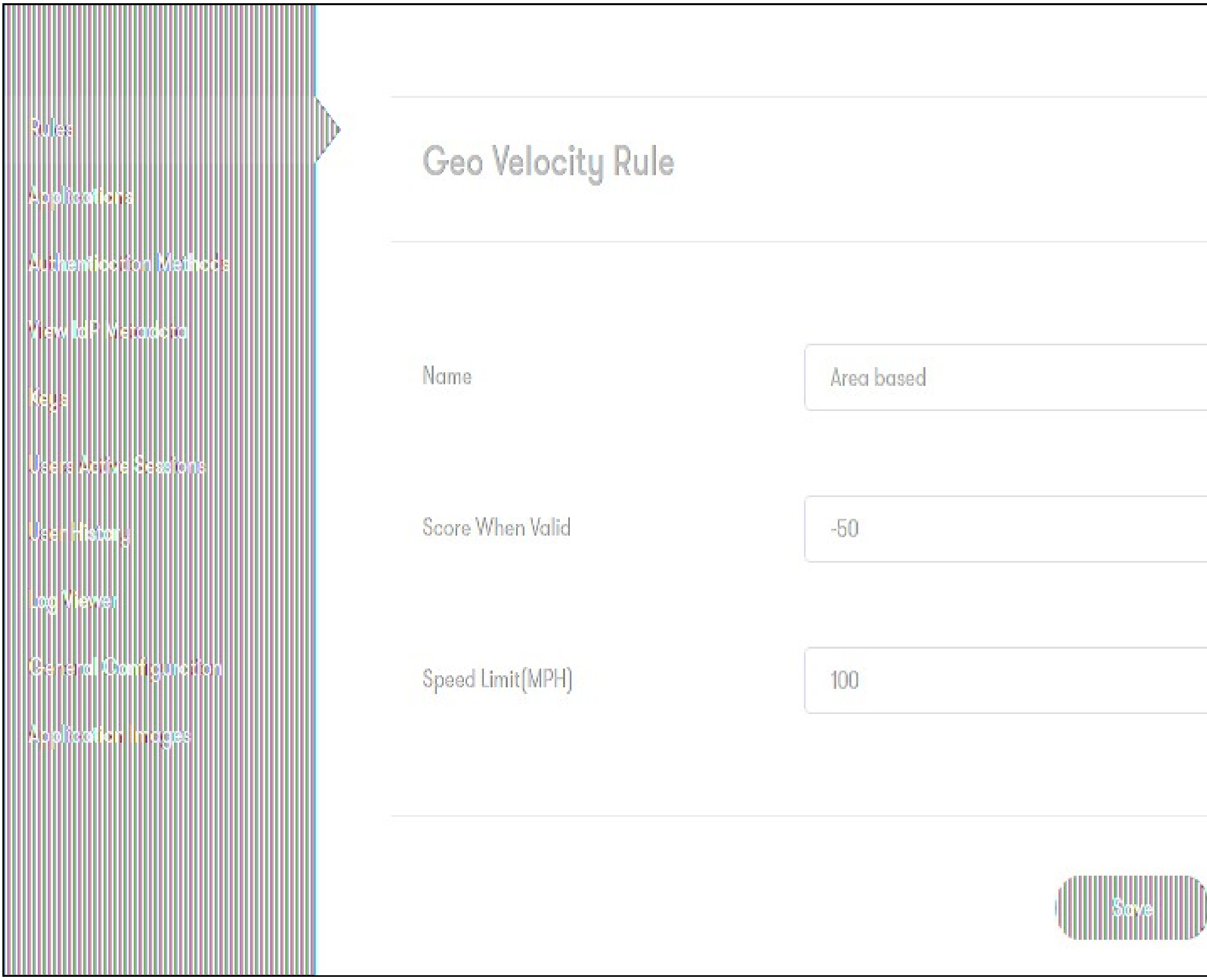
Geo Velocity

Allows you to add or more likely deduct points based on the user's apparent average speed since their last login. This uses their Geo-IP location at their current and previous location, and the elapse time. This rule is primarily designed to detect logins from someone other than the authorised user, at a geographically remote location.

Parameters:

Speed Limit (MPH): the average speed which must be exceeded for this rule to apply. Note that this is in miles per hour.

Example:



Geo Velocity Rule

Name: Area based

Score When Valid: -50

Speed Limit(MPH): 100

Compound Rules

Compound rules allow you to combine already created rules and accessing applications to add or deduct trust points for the user.

Rules can be combined to support both simple and complex set of access rules. For example you may decide that Username and Password from a Known IP Address in a safe country is as safe as two factor.

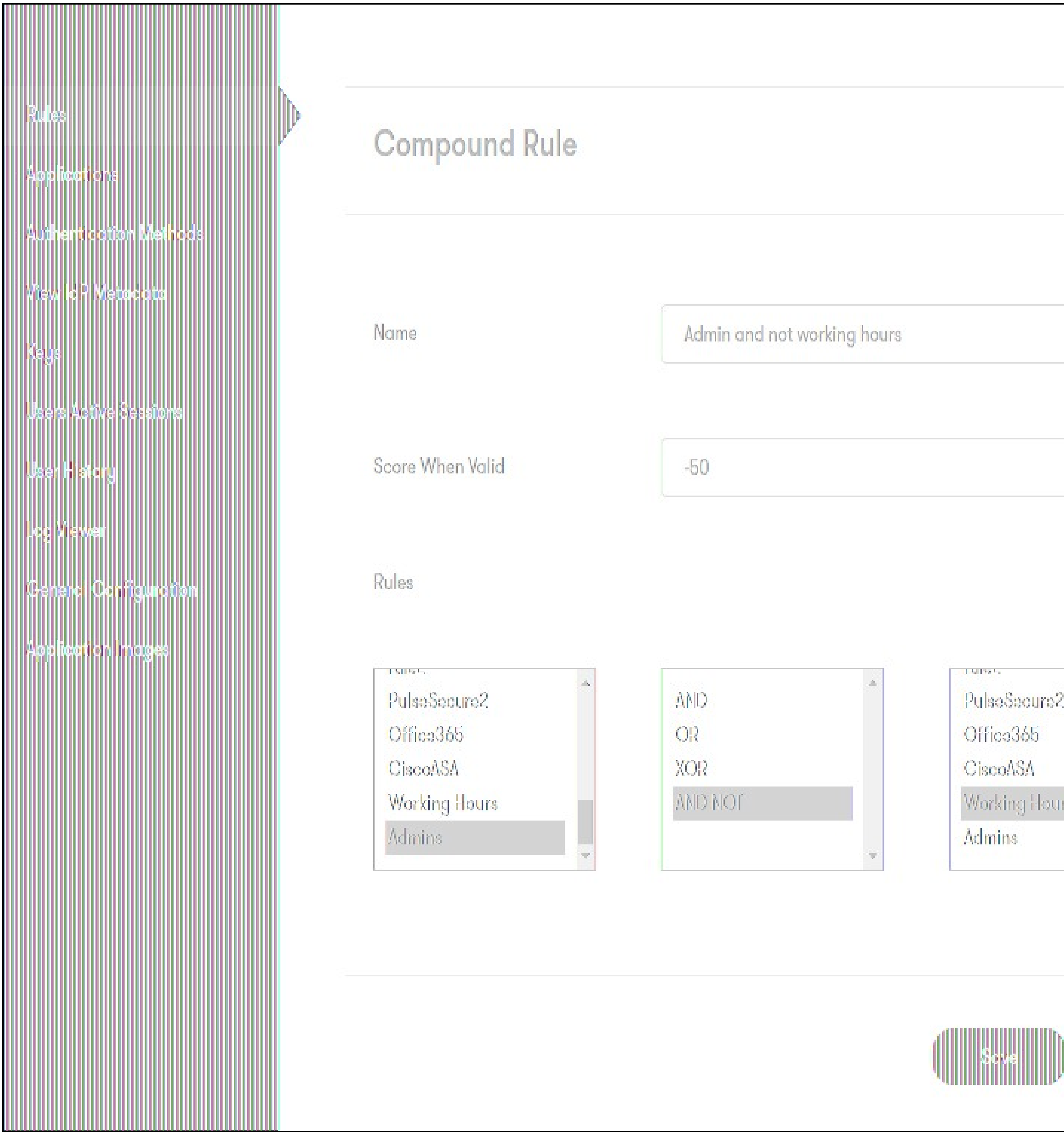
Parameters:

Rule/Application 1: A List of Rules and Applications

Operator: Operators AND,OR,XOR,AND NOT. Will allow to select if you want both rules/applications to be true to give or deduct trust points or one of to be true, or one has to be false etc.

Rule/Application 2: A List of Rules and Applications

Example:



Compound Rule

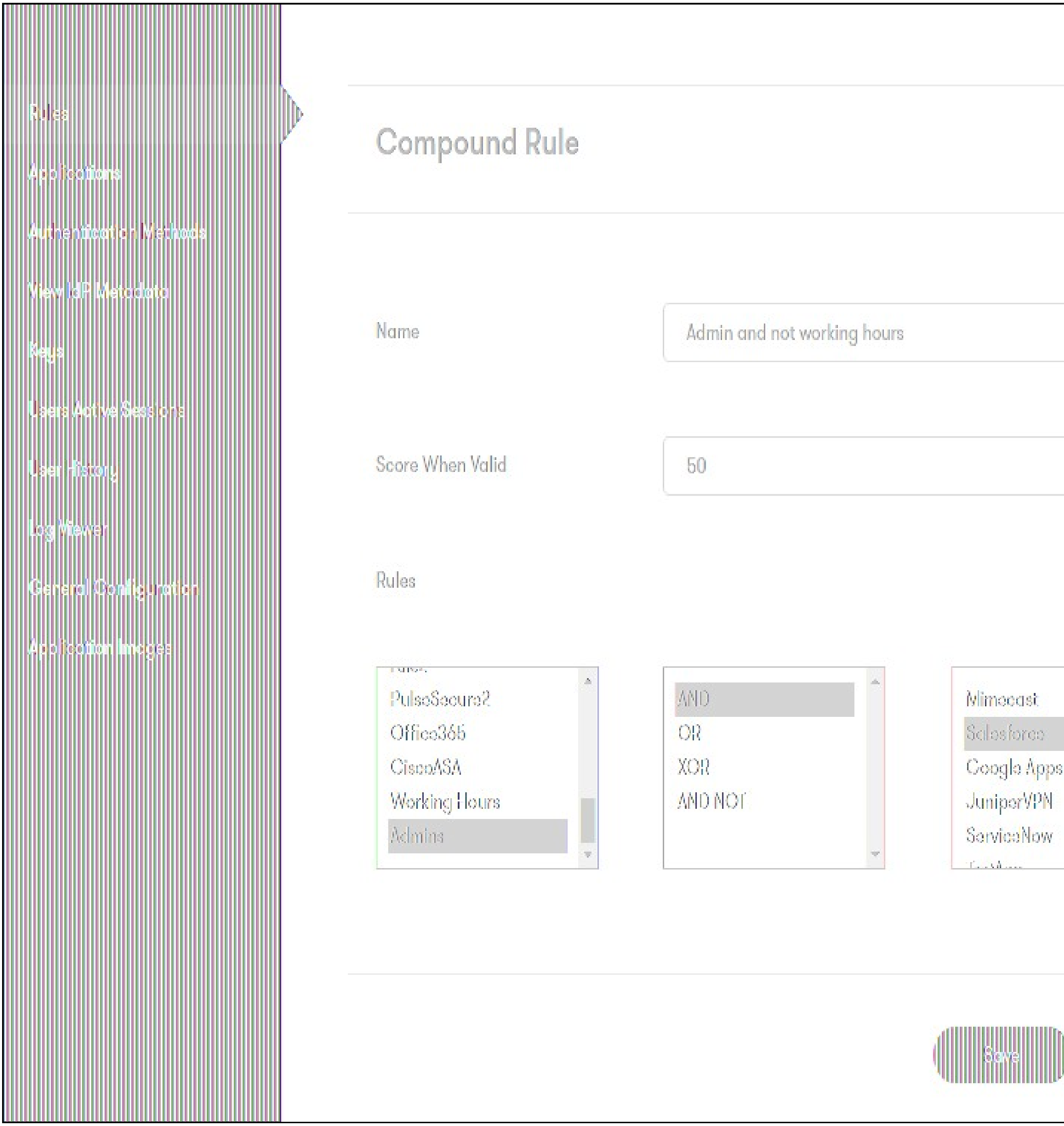
Name: Admin and not working hours

Score When Valid: -50

Rules

PulseSecure2	AND	PulseSecure2
Office365	OR	Office365
CiscoASA	XOR	CiscoASA
Working Hours	AND NOT	Working Hou
Admins		Admins

This also allows you to specify rules that only apply to specific applications e.g.



Compound Rule

Name: Admin and not working hours

Score When Valid: 50

Rules

PulseSecure2
Office365
CiscoASA
Working Hours
Admins

AND
OR
XOR
AND NOT

Mimecast
Salesforce
Google Apps
JuniperVPN
ServiceNow

Single-Sign-On

Single Sign-On allows a user to carry points that they have attained by authenticating to one application when authenticating to another application (within the same browser session).

This means that if a user has authenticated to one service they will be automatically logged-on to another service that has the same or lower required points value.

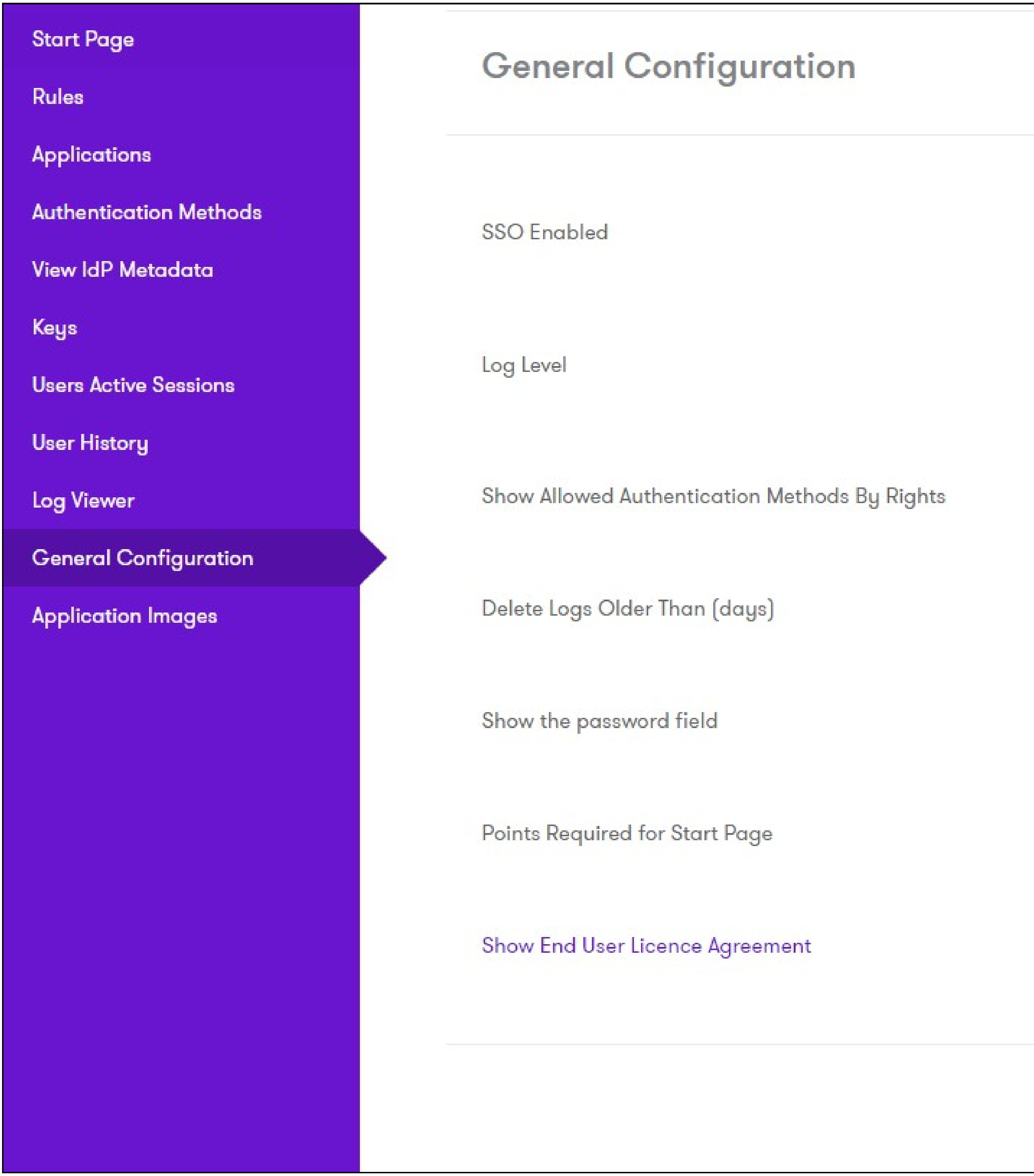
To enable single-sign-on select the SSO Enabled setting under General Configuration.

For RADIUS VPN applications the credentials will be required to access if the application does not have any session active.

Setup Authentication for Start Page (Optional)

If needed, from 4.0.5 onwards, you can configure the points required to authenticate before showing the start page.

In General Configuration, enter the Points Required for Start Page.



General Configuration

SSO Enabled

Log Level

Show Allowed Authentication Methods By Rights

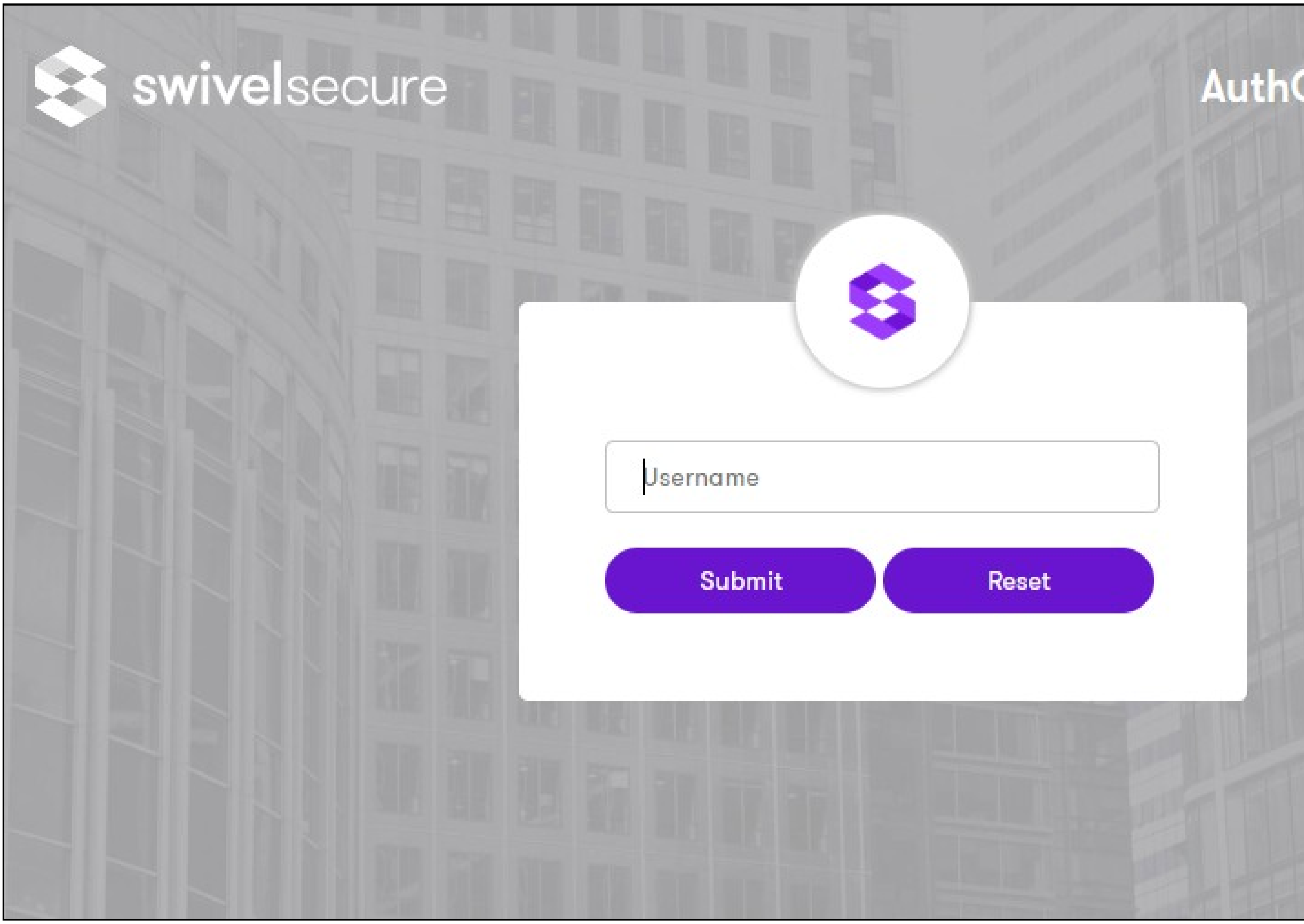
Delete Logs Older Than (days)

Show the password field

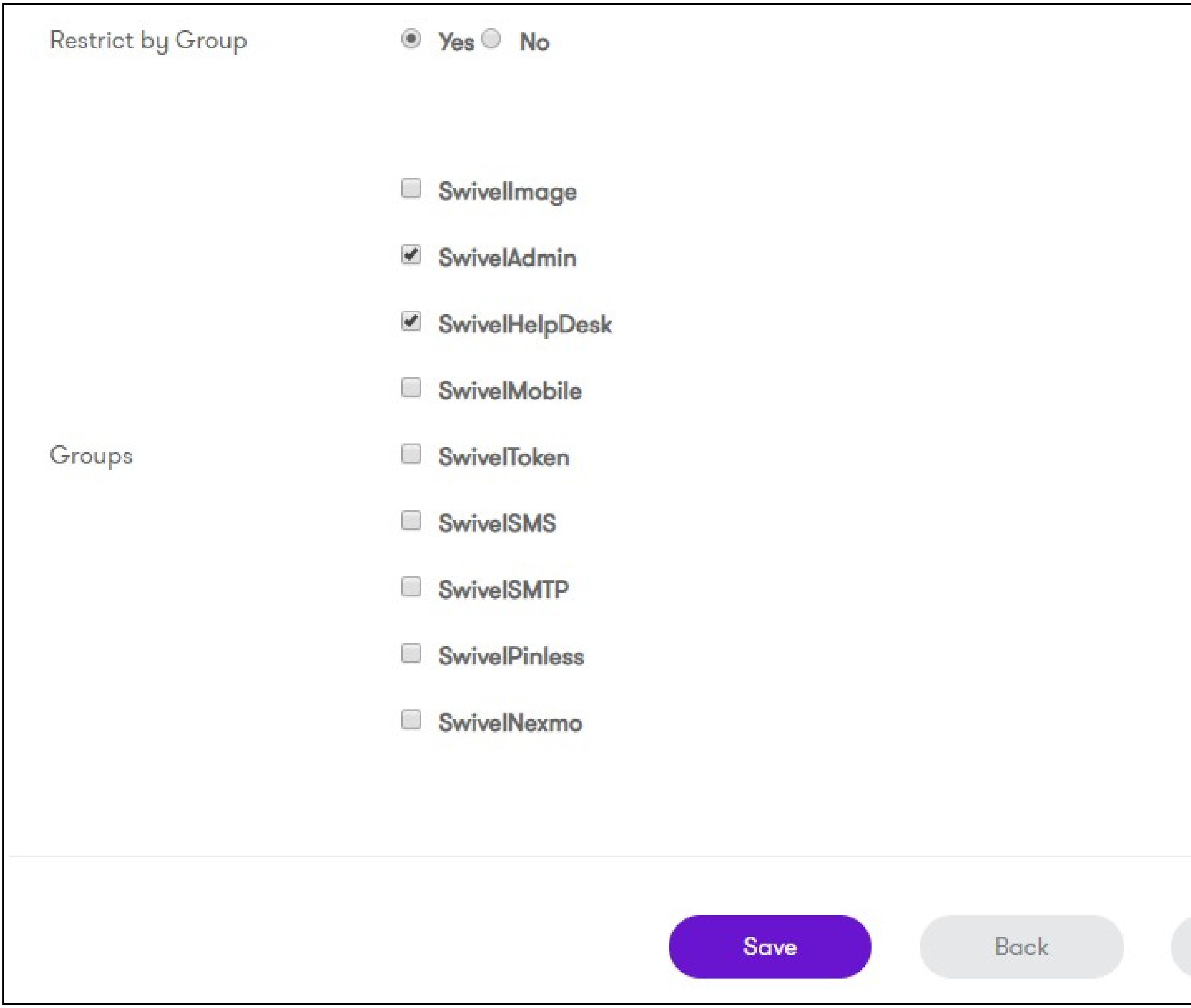
Points Required for Start Page

Show End User Licence Agreement

If you specify more than 0 points, you will get the RBA Login to enter the Start Page.



Additionaly, it's possible to configure what applications are shown in the Start page per user group, by going to the application page and selecting "Restrict by Group".



Restrict by Group ● Yes ○ No

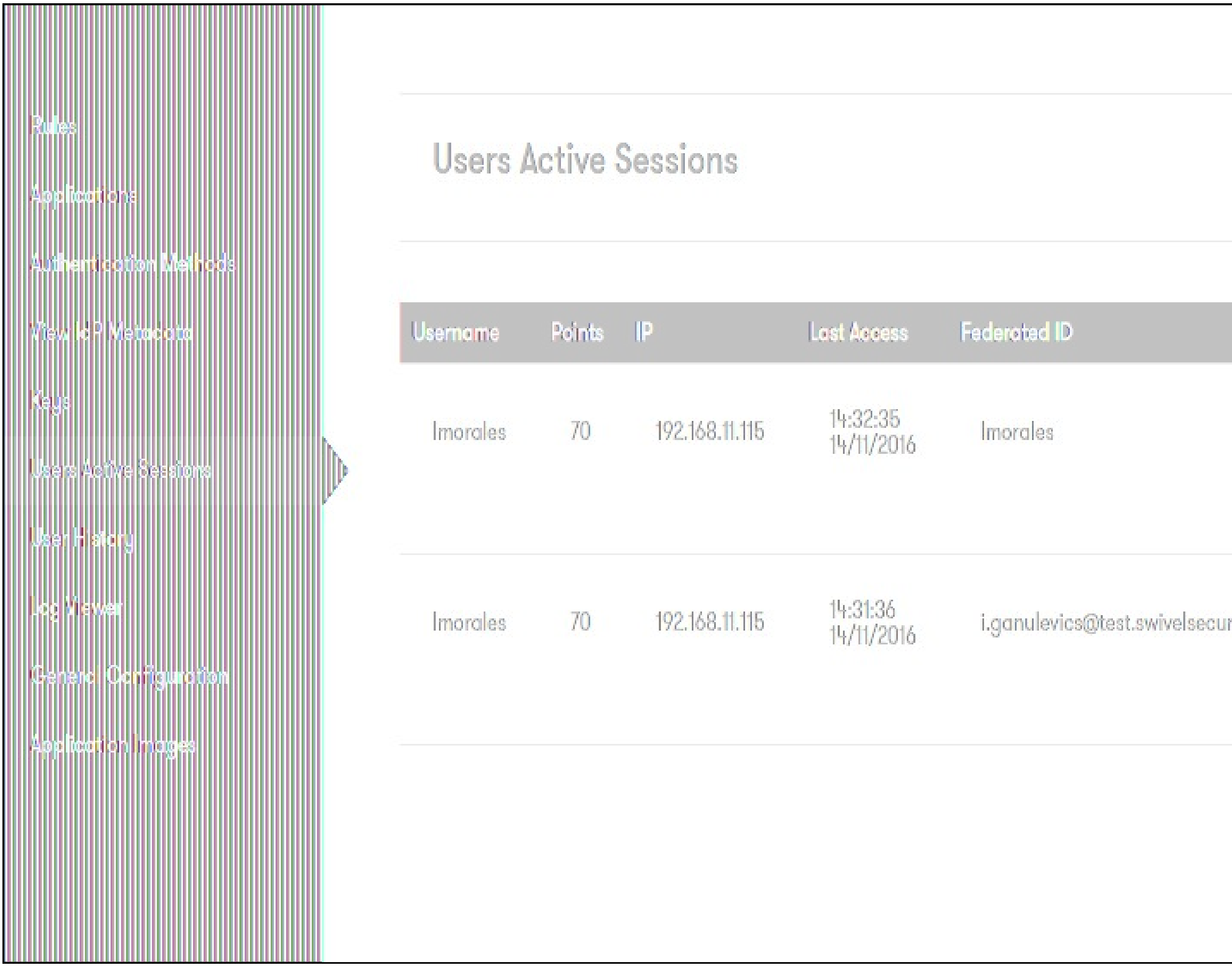
Groups

- □ SwivelImage
- ☑ SwivelAdmin
- ☑ SwivelHelpDesk
- □ SwivelMobile
- □ SwivelToken
- □ SwivelSMS
- □ SwivelSMTP
- □ SwivelPinless
- □ SwivelNexmo

General Operation and Diagnosis

Users Active Sessions

The Users Active Sessions Screen will display any users that are currently logged in via Sentry and it will indicate how many points they attained as part of that authentication.



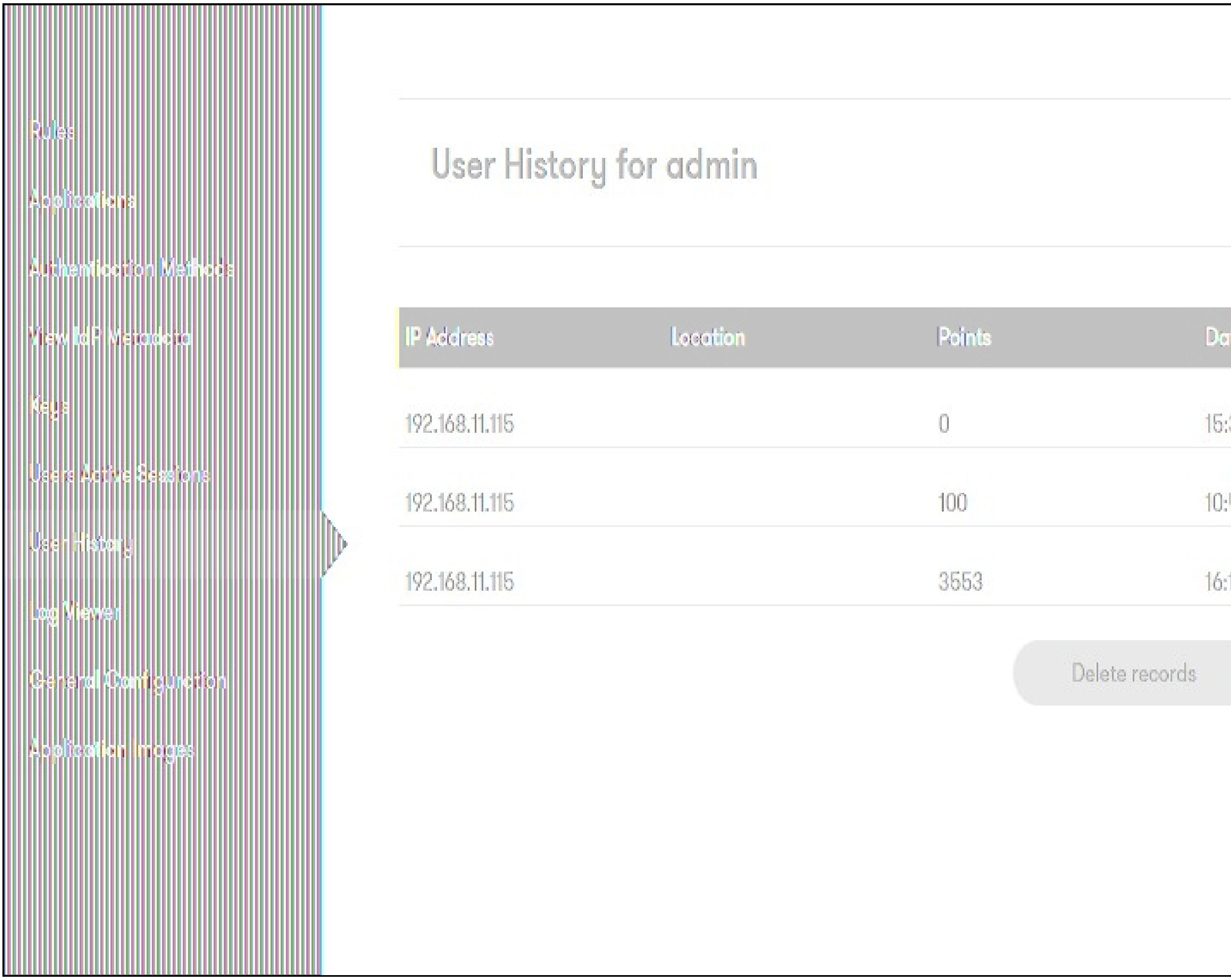
Users Active Sessions

Username	Points	IP	Last Access	Federated ID
lmorales	70	192.168.11.115	14:32:35 14/11/2016	lmorales
lmorales	70	192.168.11.115	14:31:36 14/11/2016	i.ganulevics@test.swivelsecur

User History

The User History Screen will display a user?s recent login history, including IP address, access date and points. If there is any GEO IP rule defined, the location of the user?s authentication will be displayed as well.

The user history information is used by the known IP rule, so if a Known IP has been defined, the number of last logins stored will depend on the information set on the rule. This screen also allows an administrator to remove the records associated with a user.



User History for admin

IP Address	Location	Points	Da
192.168.11.115		0	15:
192.168.11.115		100	10:
192.168.11.115		3553	16:

Log Viewer

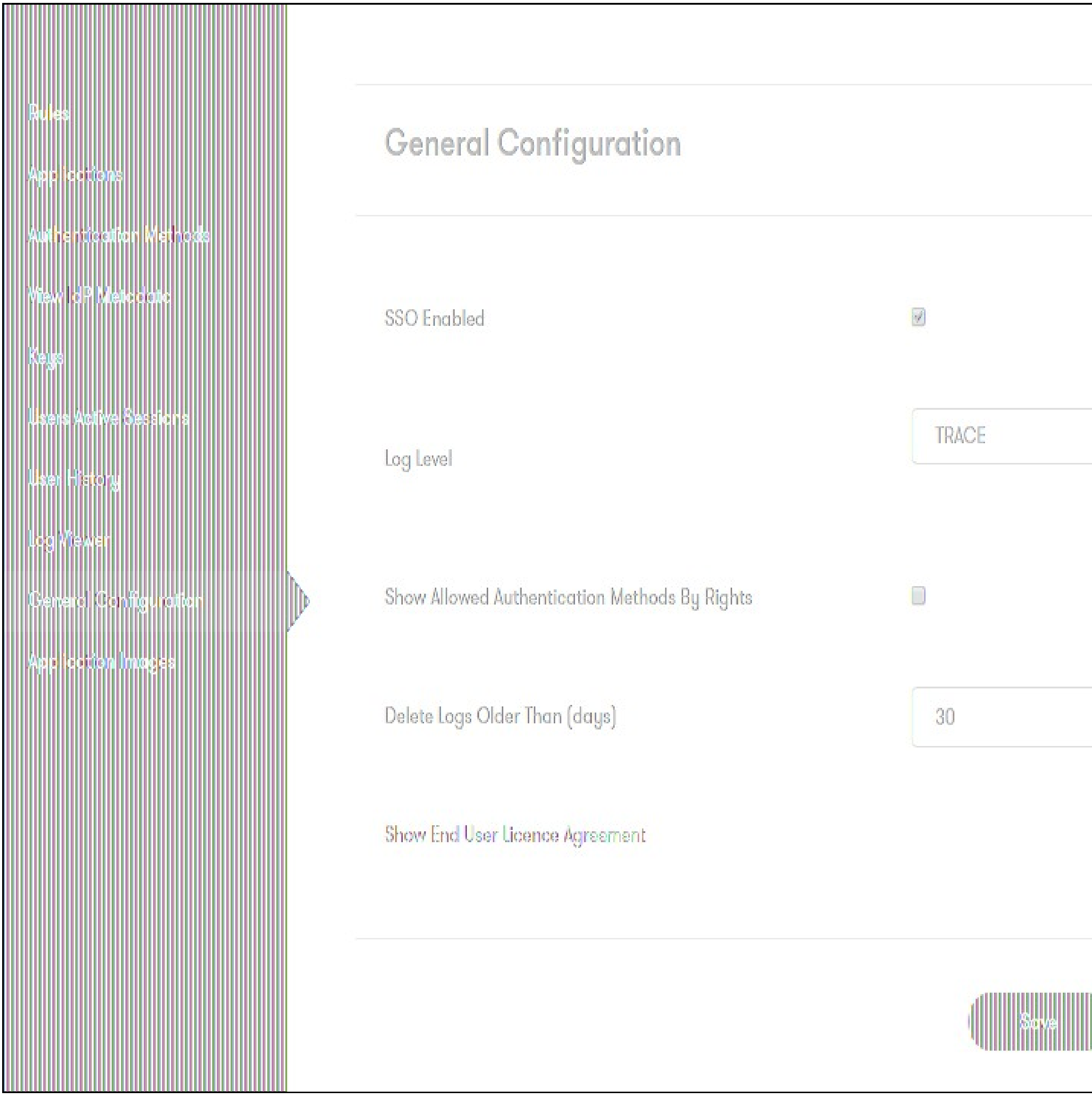
The Sentry server logs authentication and other events, which can be viewed on the Log Viewer page.

You can choose what level of logs to view from the drop-down list.

On General Configuration, you can select if you want to delete the logs and if so, how long to keep the logs.

By default Delete Logs Older Than (days) is set to 30. If that value is set to 0 the logs will not be deleted. If it is set to 1 it means that the logs will be deleted that are older than 1 day.

The scheduled task to delete logs by default will run every day at 23:00. This can be changed if the attribute deleteLogsJobCronExpression is added into settings.properties, e.g. deleteLogsJobCronExpression=0/5 * * * * ?.



General Configuration

SSO Enabled ☑

Log Level TRACE

Show Allowed Authentication Methods By Rights ☐

Delete Logs Older Than (days) 30

Show End User Licence Agreement