Authentication Manager

Contents

SAML based Authentication

Swivel Secure is developing a new SAML integration provides a new range of capabilities that optimise the application of Swivel Authentication for accessing Cloud Applications.

This is now part of version 4 of the Swivel authentication platform, renamed as "Sentry". For more information, please see Sentry User Guide.

These capabilities include

1. Adaptive, Risk-based authentication: Enforcing the appropriate level of authentication depending on various risk factors

2. Single-Sign-On across multiple cloud applications

The mechanism behind these capabilities is a points system. Points are awarded to a user for successful authentication but also for other factors such as their IP address, the time of day etc etc.

The number of points awarded for different forms of authentication can be varies as can the number of points required to access each service or application.

This means a completely customised and optimised authentication system can be deployed.

Prerequisites

Swivel Version 3.10.3 or later

Swivel Authentication software (Product in development and not yet available)

Configuring the Swivel server

Configuring the Swivel Agent

On the Swivel Administration console configure the Swivel Agent, see Agents How to Guide. By default there is a local Agent, and if the Authentication manager and Swivel are on the server it can use this.

Enabling Session creation with username

To allow the TURing image, Pinpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

Configuring the Admin login

An Administrator account is required to login who is a member of the PINsafeAdministrators group, or group as defined below.

Authentication Manager Installation on a Swivel Appliance

The software comes as a web-archive (.war) file called swivelauthenticationmanager.war. Using WinSCP or similar copy the swivelauthenticationmanager.war file to /usr/local/tomcat/webapps2 folder.

This should automatically create the following folders:

/usr/local/tomcat/swivelauthenticationmanager

/home/swivel/.swivel/db/SwivelAuthenticationManagerDB

Configuring the Swivel Authentication Settings

Edit the settings.properties file in

/usr/local/tomcat/swivelauthenticationmanager/classes/settings.properties

The following values should be set for a Swivel hardware or virtual appliance:

```
pinsafessl=false
pinsafeserver=localhost
pinsafecontext=pinsafe
pinsafesecret=secret
pinsafeport=8181
imagessl=true
imageserver=Swivel_DNS_Public_Name
imagecontext=proxy
imageport=8443
selfsigned=true
certificateIssuer=SAML_SP
encryptionType=DSA
publicKeyFilePath=/keys/pinsafe/ssl/dsapubkey.der
privateKeyFilePath=/keys/pinsafe/ssl/dsaprivkey.der
certificateFilePath=/keys/pinsafe/ssl/dsacert.pem
administrationGroup=PINsafeAdministrators
timeoutPolling=60000
```

Note: Sentry's administrationGroup by default is set to Swivel Admin, after a migration this group must match the admin group set in the core, which by default was PINsafeAdministrators.

After saving the settings restart Tomcat, such as through the CMI

If you have changed the shared-secret for the local agent on the Swivel core server you need to set the secret on the authentication manager to match.

pinsafessl=false True/False, Comunication with the Swivel core, using SSL or not

pinsafeserver=localhost Comunication with the Swivel core, localhost if installed on the same server

pinsafecontext=pinsafe Comunication with the Swivel core, the Swivel installation name

pinsafesecret=secret Comunication with the Swivel core, the shared secret defined on the core

pinsafeport=8181 Comunication with the Swivel core, port used for communication, 8181 for the proxy

imagessl=true True/False Comunication with the Swivel core, using SSL for images

imageserver=Swivel_DNS_Public_Name Comunication with the Swivel core, The IP addrss used for Swivel images and usually publicly available through the Swivel proxy

imagecontext=proxy Comunication with the Swivel core, for obtaining authentication images, use proxy for an appliance

imageport=8443 Comunication with the Swivel core, for obtaining authentication images, use 8443 for an appliance

selfsigned=true True/False Comunication with the Swivel core, for obtaining authentication images, True to allow self signed certificates

certificateIssuer=SAML_SP

encryptionType=DSA

publicKeyFilePath=/keys/pinsafe/ssl/dsapubkey.der

privateKeyFilePath=/keys/pinsafe/ssl/dsaprivkey.der

certificateFilePath=/keys/pinsafe/ssl/dsacert.pem

administrationGroup=PINsafeAdministrators

timeoutPolling=60000

Additional settings

federatedIDAttribute=email The Federated ID Attribute can be defined, if it is not specified, it defaults to email.

Key and Certificate generation

Key and Certificate Generation

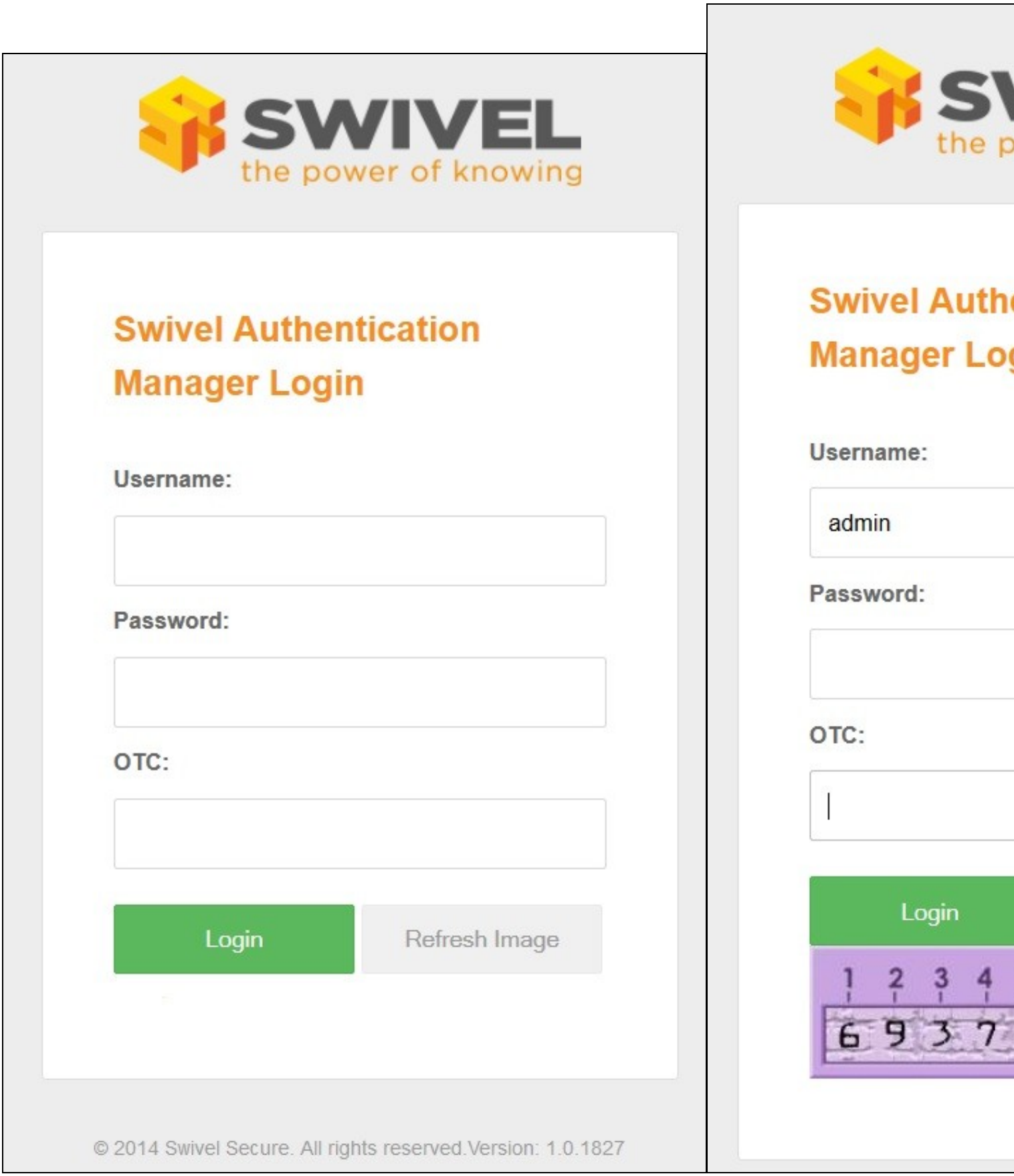
Swivel Authentication Manager Login

Using a web browser connect to the Swivel Authentication Manager:

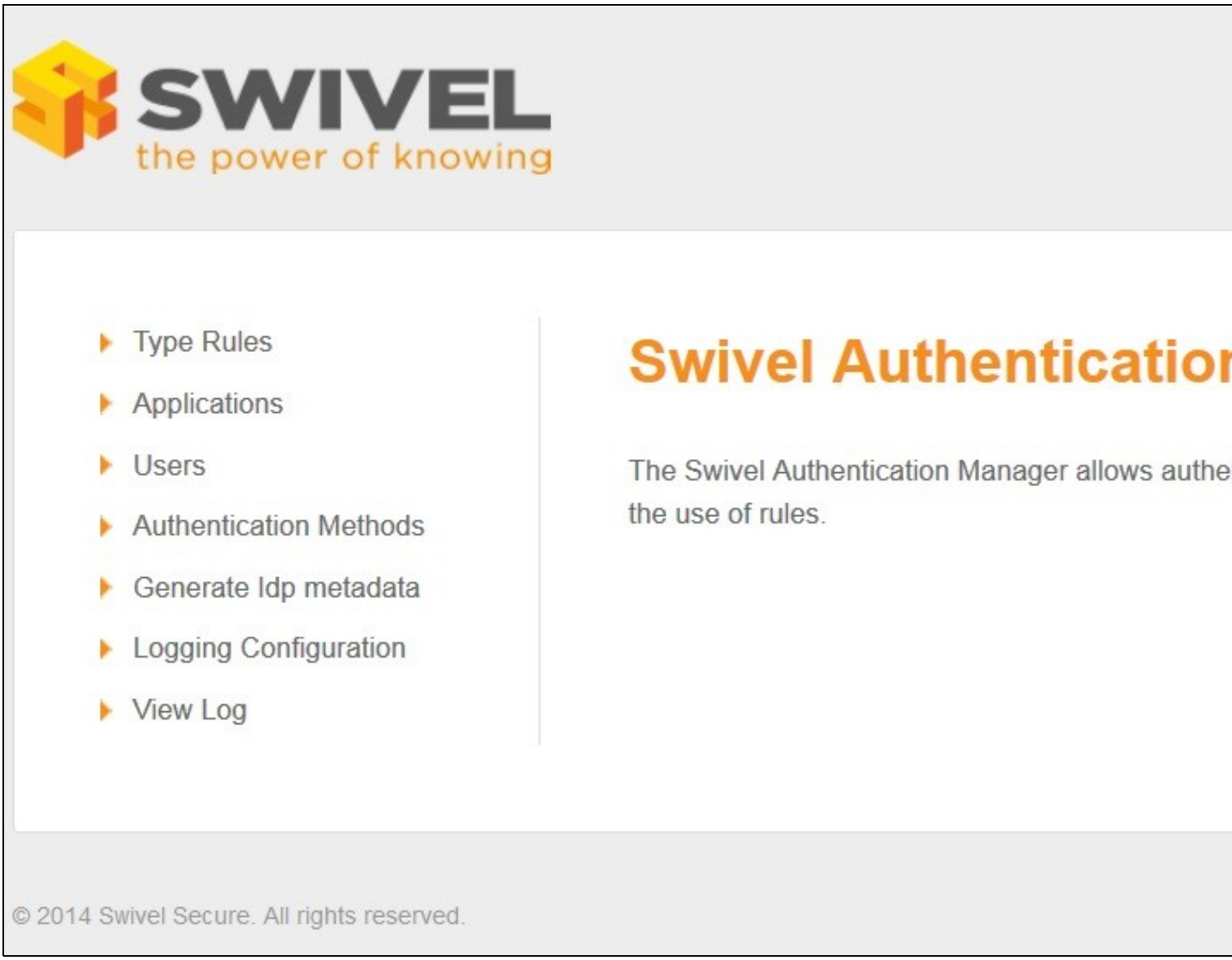
https://IP_or_Hostname:8443/swivelauthenticationmanager

Login with a user who is a member of the administrationGroup on the Swivel server, the default value for this is administrationGroup=PINsafeAdministrators, which is the default Swivel Administrators group.

Adinistrative login can also be restricted by IP source, see Filter IP How to Guide.



A succesful login should load the Swivel Authentication manager default page:



Integration

Integration of SAML-enabled services and applications will depend in detail on the applications themselves. However on the Authentication Manager side of the integration you need to

1) Give the service provider a name.

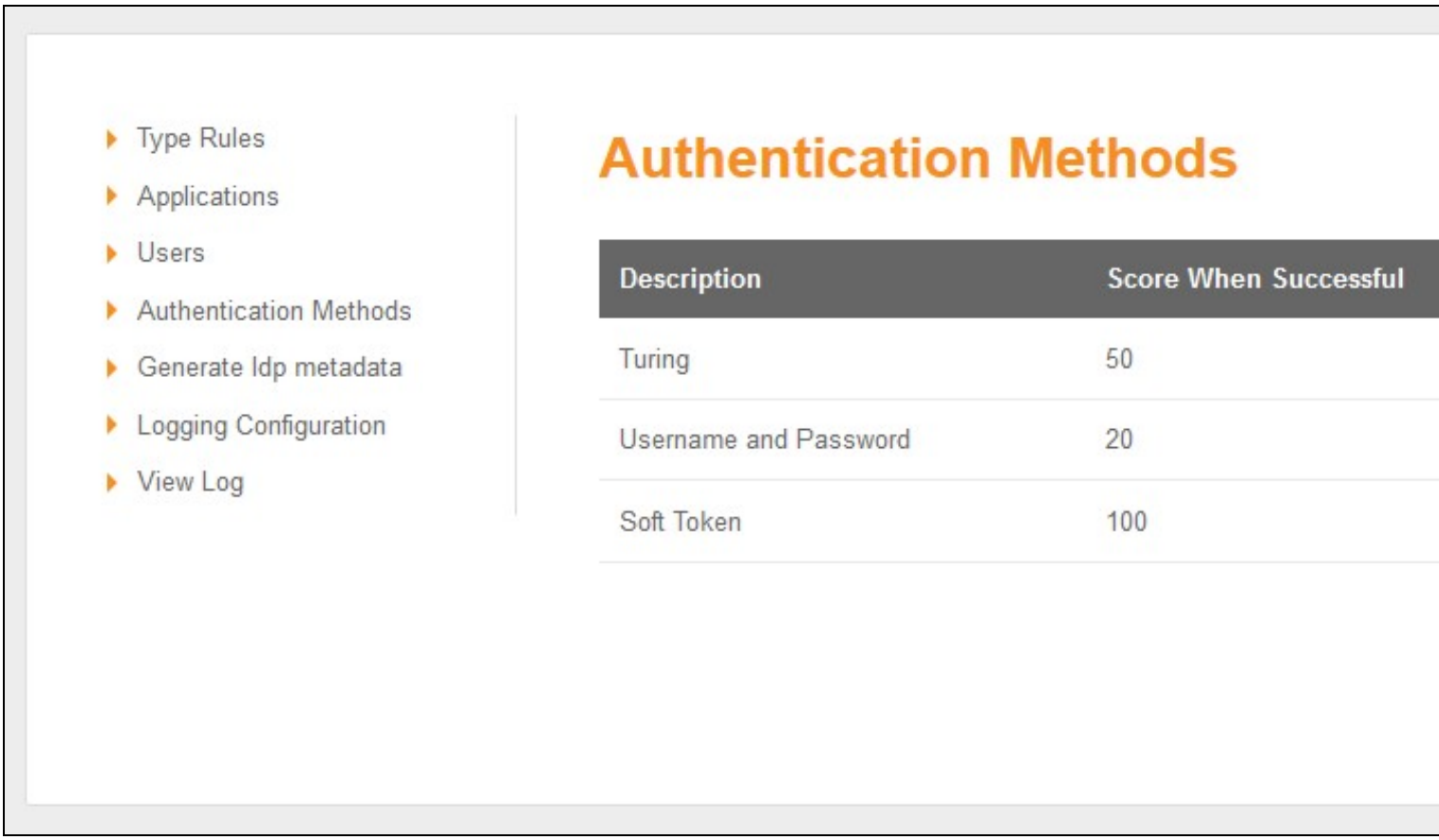
2) State the number of points required before the user can gain access.

3) The IP addess or host name of the cloud service, specically the SAML2.0 Endpoint for the service

4) The cloud servive URN, this will be part of the SAML Assertion that the cloud service will send

If required the Authentication Manager's metadata can be generated by using the Generate IdP metadata function.

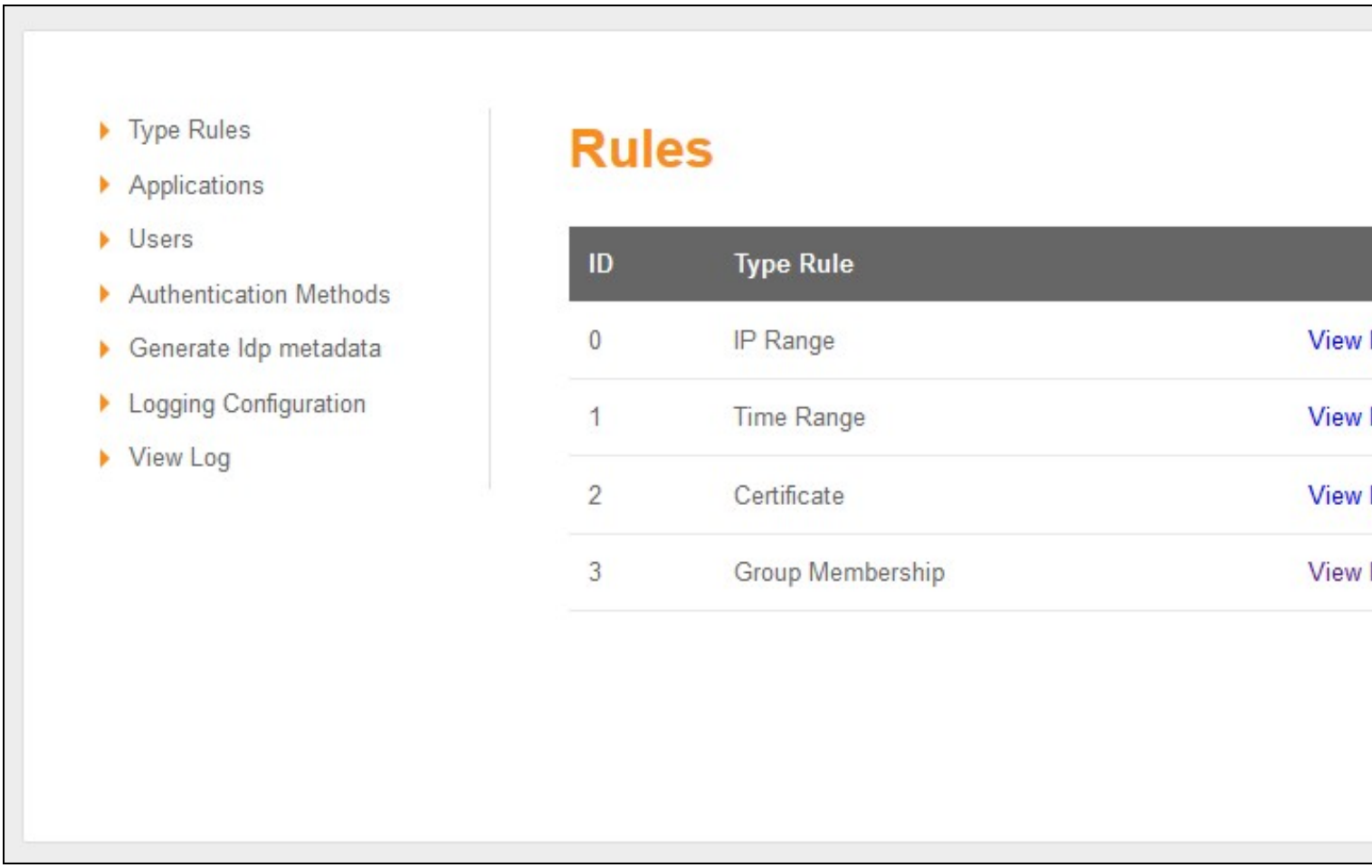
Authentication Methods



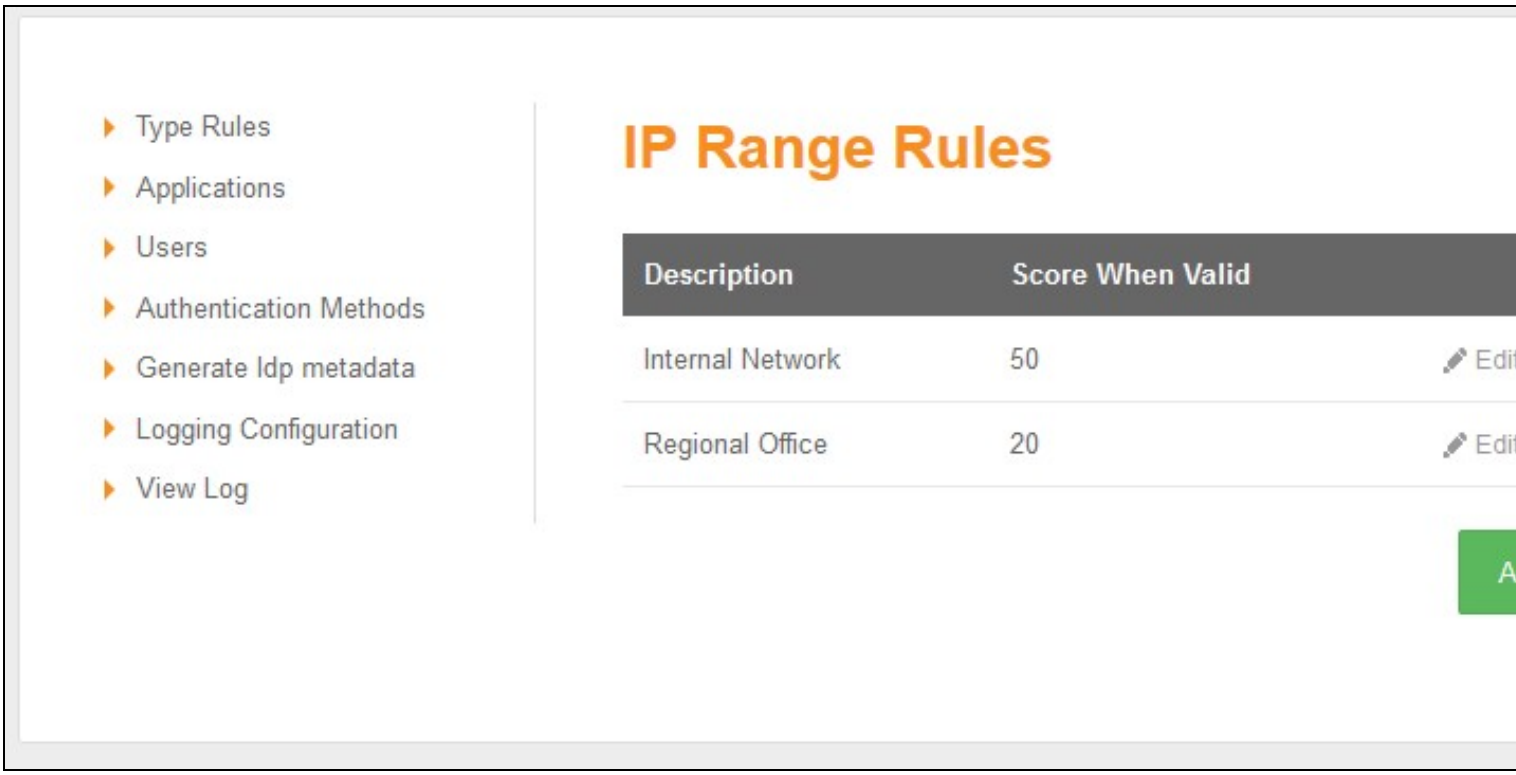
In order for a user to be allowed access to the cloud applications they must attain a significant number of points. Points can be attained by "rules" or by successfully authenticating to the Authentication Manager

The number of points awarded for each for of authentication is defined on the Authentication Methods Screen.

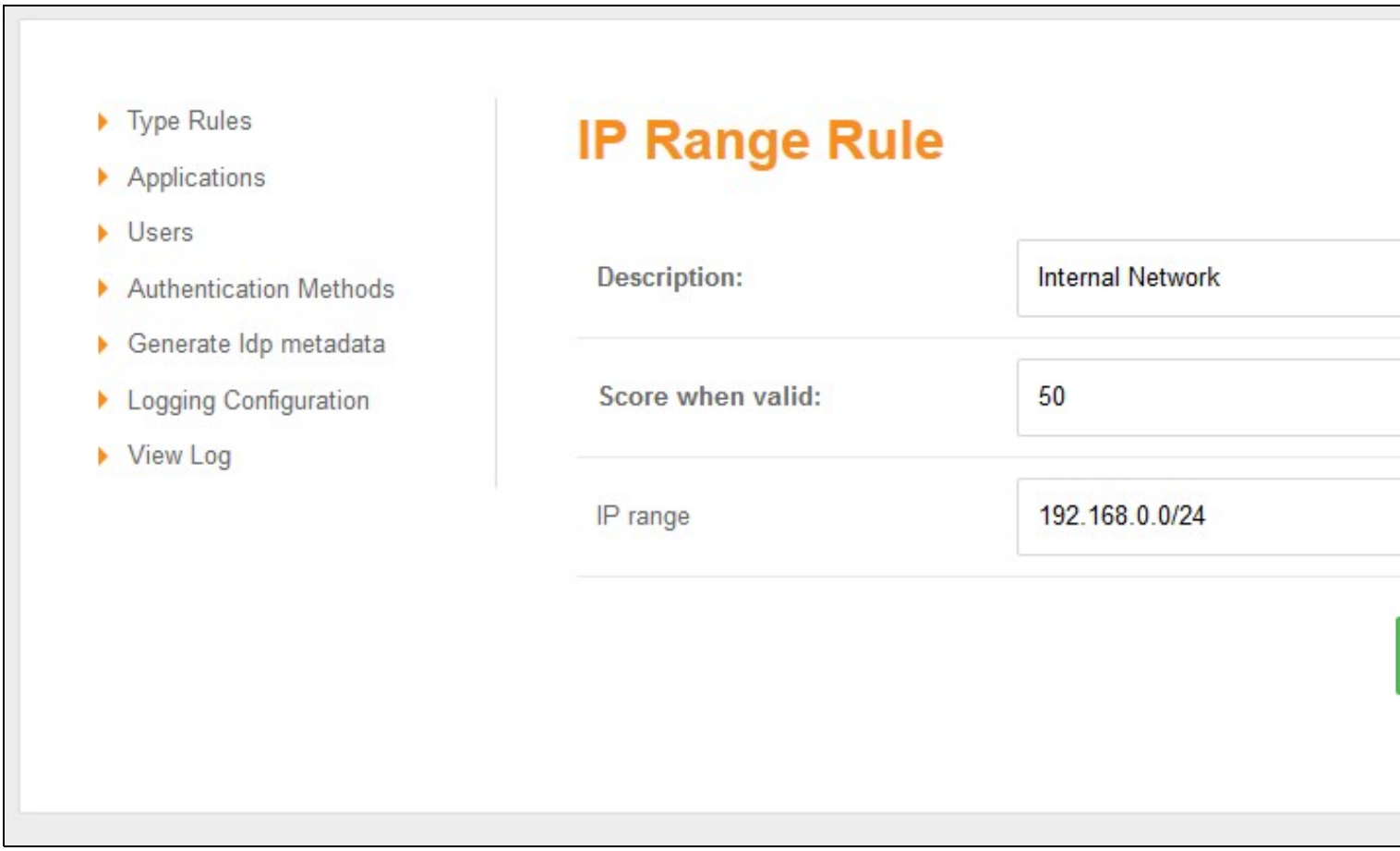
Rules



Rules are the means by which the system administrator can take into account a number of risk factors into account when deciding how a user should authenticate. The admin specifies the rule and then how many points the user is awarded (or penalised) should the rule be true for that user.



For example a user accessing from the local office network may be deemed to be less risky than from other IP addresses and therefore a rule may be defined that awards 50 points to a user that is accessing from the office.



New Rules are being made avaialable all the time. The current list of rules includes

IP address

If the user's IP address falls within a given range or ranges (since June 2014)

Time of Day

Points awarded (or subtracted) if the authentication takes place within a given time period (since June 2014)

X509 Certificate

Points awarded if the user has a valid X509 client installed on their computer (since July 2014)

Group Membership

Points awarded (or subtracted) if the user is a member of a defined group (eg Active Directory group) of users (since Sept 2014)

Known IP Address

Points awarded to a user if they are authenticating from an IP address from which they have previously successfully authenticated from (Due Dec 2014)

Location (Geo-IP)

Points awarded (or subtracted) based on a user's location as derived from their IP address(Due Q1 2015)

Users

Shows users who have made a log in displaying the following information:

Username

Points

Federated ID

IP

Applications

Logging

Logging Configuration

Log Level: default TRACE, options TRACE, DEBUG, ERROR, WARN, FATAL, The level to log, logs everything below the selected list

View Log

This Displays the Swivel Authentication manager login

Events Per Page: default 10, The number of events to display per page

Page Number: default 1, The page number of logs to display

Log Level: default TRACE, options TRACE, DEBUG, ERROR, WARN, FATAL, The log level to show, displays everything below the selected list

Ascending Date Order: default not ticked, Show as Ascending or descending date

Logging Out

The Authentiation manager will remember a users session for a period of time, not requiring them to login, unless a logout option has been enabled. For testing purposes it is useful to logout when the option is not available, and this can be done by deleting cookies, or some browsers such as firefox allow individual cookies to be deleted or removing them form the file system. The cookie name is usually that of the Authentication Manager URL.

Testing

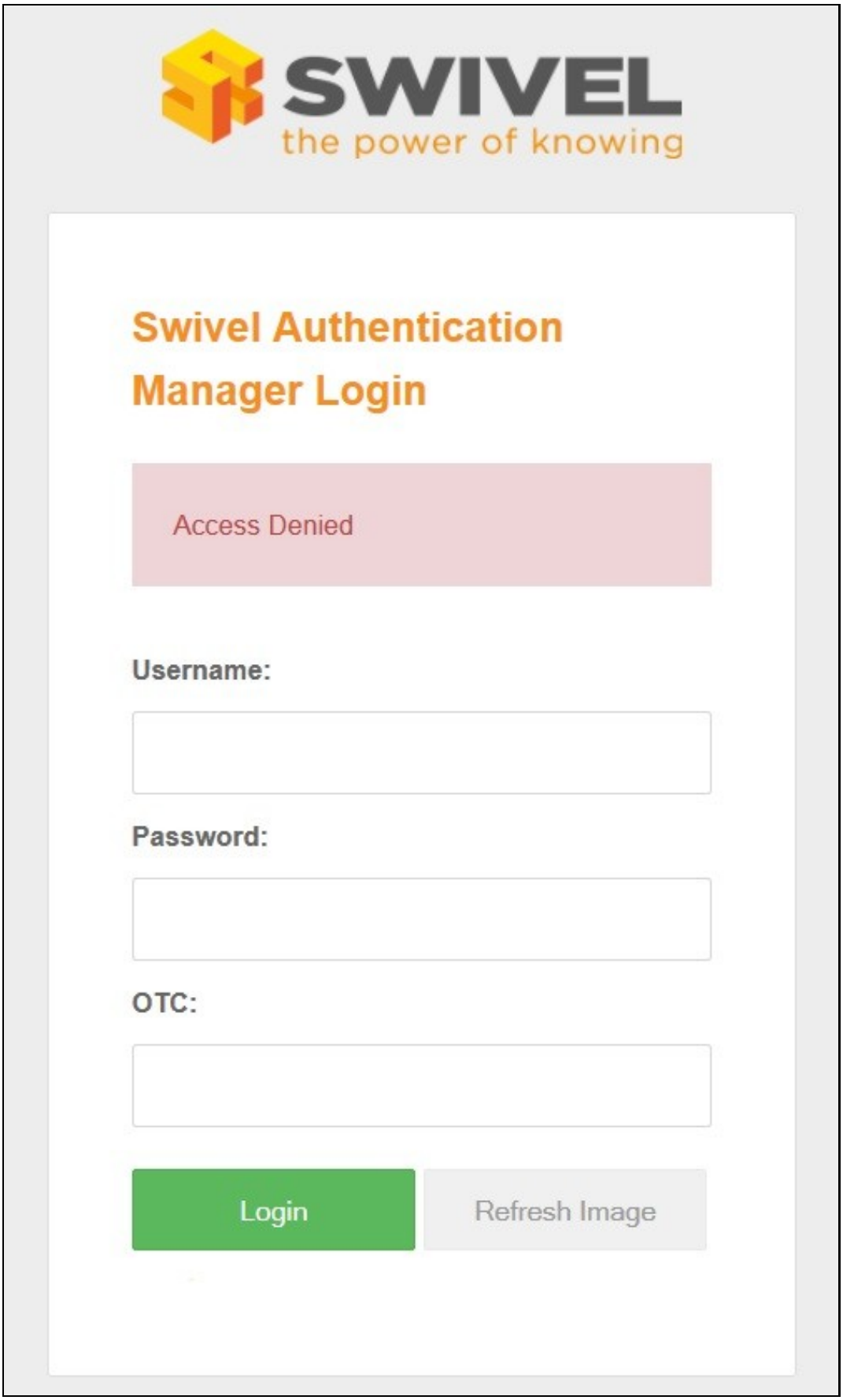
Known Issues

Troubleshooting

Check the Authentication Manager logs, the Swivel Administration Console logs and the Tomcat logs for any error messages

Swivel appliances /var/log/tomcat/catalina.out

No Username entered, or the application does not have permission. Check the logs.



Administrative User cannot login

This is usualy the admin user and by default on the Swivel core, they must be a member of the Swivel Repository Group PINsafeAdministrators, unless a different setting is configured in the settings.properties file, the default is: administrationGroup=PINsafeAdministrators. If it is different the Swivel core will show a successful authentication, but the Authentication Manager fails due to the incorrect group.

Sample Swivel core login information

```
Primary:Read user: admin.
Searching encryption key for the IP: 192.168.12.110, agent name found: Primary
Primary:Login successful for user: admin.
Pimary:Processing user admin as channel SINGLE
```

Error Messages

Authentication failed for username:

The login attempt failed for the user

Cannot find application for URN:

The application is not configured for authentication, check the Application settings. The URN is supplied to the Authentication manager, and check against the configured applications to find a matching Entity ID. To have the rule match a particular application set the Entity ID to the URN.

No LoggedUser in session, directing to username page

The user has not logged in so is directed to the authentication page.

Error XBM0H: Directory /home/swivel/SwivelAuthenticationManagerDB cannot be created.

java.lang.OutOfMemoryError: PermGen space

"ActiveMQ ShutdownHook" java.lang.OutOfMemoryError: PermGen space

These errors have been seen when there has not been enough memory available to run the Swivel Authentication Manager. See Heap Space Memory Management How to guide.