

Table of Contents

1 Authcontrol Sentry v4 Admin Guide.....	1
2 Swivel Secure AuthControl Sentry Version 4.....	2
3 Getting Started.....	3
4 PIN Policies and Locking.....	8
5 Authcontrol v4 Sentry SSO and Adaptive Authentication.....	10
6 What is Adaptive Authentication?.....	11
7 Getting Started.....	12
7.1 Login to Sentry for the First Time.....	12
7.2 Settings.....	14
7.3 Accessing the Web Administration Console.....	14
7.4 Setup Sentry Keys.....	14
7.5 Viewing Certificate and Metadata.....	15
8 Defining Applications.....	18
9 Defining Authentication Methods.....	26
10 Defining Sentry Rules.....	31
10.1 IP Address (White List or Black List).....	32
10.2 Time Range.....	33
10.3 Certificate.....	34
10.4 Group Membership.....	35
10.5 Known IP.....	36
10.6 GeoIP.....	37
10.7 Geo Velocity.....	38
10.8 Compound Rules.....	39
11 Single-Sign-On.....	42
12 Setup Authentication for Start Page (Optional).....	43
13 General Operation and Diagnosis.....	46
13.1 Users Active Sessions.....	46
13.2 User History.....	46
13.3 Log Viewer.....	47
14 Azure AD as a Data Source.....	49
15 Overview.....	50
16 Prerequisites.....	51
16.1 Implementation.....	51
17 How To Configure OATH Mobile.....	52
17.1 Overview.....	52
17.2 Prerequisites.....	52
17.3 Swivel core configuration.....	52
17.4 Configuring OATH policy settings.....	52
17.5 Define a group of Mobile OATH users.....	54
17.6 Testing.....	54
17.7 Troubleshooting.....	54
18 How To Configure Push Mobile.....	56
18.1 Overview.....	56
18.2 Prerequisites.....	56
18.3 Swivel core configuration.....	56
18.4 Configuring Dual Channel settings.....	56
18.5 Define a group of Push Users.....	56
18.6 Define a Push Transport.....	57
18.7 PNA configuration.....	58
18.8 PNA V5 Configuration.....	59
18.9 iOS Users.....	60
18.10 Android Users.....	60
18.11 Testing.....	60
18.12 Troubleshooting.....	60
19 How To Provision Mobile Apps.....	62
19.1 Provisioning Mobile Apps.....	62
19.2 How it works.....	62
19.3 Site ID.....	62
19.4 Provision URLs.....	62
19.5 Quick Provision Link.....	63
19.6 QR Code.....	63
19.7 Policies.....	63
19.8 Troubleshooting.....	65
20 Licence key.....	66
20.1 Swivel Licence Keys.....	66
20.2 Entering Licence Keys.....	66

Table of Contents

20 Licence key	67
20.3 Updating Licence Information.....	67
21 Mobile App Privacy Policy.....	69
22 Notes.....	70
23 Privacy Policy.....	71
24 Need more help?.....	72
25 MobileIron Integration.....	73
26 Overview.....	74
27 Prerequisites.....	75
28 How does it work.....	76
29 SwivelSecure Configuration.....	77
29.1 Enabling Standard Federation - Sales Force.....	77
29.2 Enabling Standard Federation - Office 365.....	85
30 Related Articles.....	90
31 Additional Information.....	91
32 OATH Seed Conversion.....	92
32.1 Introduction.....	92
32.2 Pre-requisites.....	92
32.3 Python Script.....	92
32.4 Microsoft MFA Seed File Formatting Requirements.....	92
33 Pinsafe.....	93
33.1 PINsafe.....	93
34 Sentry.....	94
35 Sentry SSO with ADFS.....	95
36 Configuring ADFS Support for Sentry.....	96
36.1 Introduction.....	96
36.2 Requirements.....	96
36.3 Configuration Procedure.....	96
37 Sentry SSO with Cisco ASA.....	113
37.1 Introduction.....	113
37.2 Configure Cisco ASA.....	113
37.3 Configure Swivel Sentry.....	116
37.4 Configure RADIUS NAS on Swivel Core.....	118
37.5 SSO.....	118
37.6 Known Issues/Limitations.....	119
38 Sentry SSO with Cisco ASA using SAML.....	120
38.1 Introduction.....	120
38.2 Setup AuthControl Sentry Keys.....	120
38.3 Convert Sentry Keys to PFX.....	120
38.4 Download the Sentry SSO IdP metadata.....	120
38.5 Configure Cisco ASA.....	120
38.6 Configure AuthControl Sentry.....	121
39 Sentry SSO with CiscoASA.....	122
39.1 Introduction.....	122
39.2 Overview.....	122
39.3 Configure Cisco ASA Login.....	122
39.4 Configuring Sentry Login.....	123
39.5 Configuring Sentry RADIUS.....	123
39.6 SSO.....	123
39.7 Testing.....	123
39.8 Troubleshooting.....	123
40 Sentry SSO with Citrix Netscaler.....	124
40.1 Introduction.....	124
40.2 Setup AuthControl Sentry Keys.....	124
40.3 Setup SAML SSO on Citrix Netscaler.....	124
40.4 Configure Check Password with Repository on the Swivel Core.....	130
40.5 Setup AuthControl Sentry Application definition.....	130
40.6 Setup AuthControl Sentry Authentication definition.....	132
40.7 Testing authentication to Google via Swivel AuthControl Sentry.....	132
40.8 Troubleshooting.....	134
41 Sentry SSO with CitrixNetscaler.....	135
41.1 Introduction.....	135
41.2 Setup AuthControl Sentry Keys.....	135
41.3 Setup SAML SSO on Citrix Netscaler.....	135

Table of Contents

41 Sentry SSO with CitrixNetscaler	141
41.4 Configure Check Password with Repository on the Swivel Core	141
41.5 Importing your users into the Swivel Core	141
41.6 Setup AuthControl Sentry Application definition	141
41.7 Setup AuthControl Sentry Authentication definition	143
41.8 Testing authentication to Google via Swivel AuthControl Sentry	143
41.9 Troubleshooting	146
42 Sentry SSO with F5	147
42.1 Setup SSO on F5	147
42.2 Setup Sentry Application Definition	154
42.3 Testing authentication to Salesforce via Swivel Sentry	161
43 Sentry SSO with GoogleApps	163
43.1 Setup AuthControl Sentry Keys	163
43.2 Setup SSO on Google	163
43.3 Configure Check Password with Repository on the Swivel Core	164
43.4 Setup AuthControl Sentry Application definition	165
43.5 Setup AuthControl Sentry Authentication definition	167
43.6 Testing authentication to Google via Swivel AuthControl Sentry	167
43.7 Troubleshooting	171
44 Sentry SSO with GoToMeeting	172
44.1 Introduction	172
44.2 Setup AuthControl Sentry Keys	172
44.3 Setup SSO on GoToMeeting	172
44.4 Setup AuthControl Sentry Application definition	174
44.5 Testing authentication to Google via Swivel AuthControl Sentry	176
44.6 Troubleshooting	179
45 Sentry SSO with JIRA	180
45.1 Introduction	180
45.2 Setup AuthControl Sentry Keys	180
45.3 Setup SSO on JIRA	180
45.4 Setup AuthControl Sentry Application definition	185
45.5 Testing authentication to JIRA via Swivel AuthControl Sentry	194
45.6 Troubleshooting	196
46 Sentry SSO with Juniper	197
46.1 Introduction	197
46.2 Overview	197
46.3 Configure Juniper Login	197
46.4 Configuring Logout	199
46.5 Configure Juniper	199
46.6 Configuring Sentry Login	203
46.7 Configuring Sentry RADIUS	204
46.8 SSO	204
46.9 Authentication with AD/LDAP and Radius	204
46.10 Testing	205
47 Sentry SSO with Meraki Dashboard	207
47.1 Setup Sentry Keys	207
47.2 Enable SAML SSO in Meraki Dashboard	207
47.3 Setup additional role attribute in Swivel Core (if needed)	208
47.4 Setup Sentry Application	209
47.5 Testing authentication to Meraki Dashboard via Swivel Sentry	212
47.6 Troubleshooting	214
48 Sentry SSO with Mimecast	216
48.1 Setup AuthControl Sentry Keys	216
48.2 Setup SSO on Mimecast	216
48.3 Configure Check Password with Repository on the Swivel Core	221
48.4 Setup AuthControl Sentry Application definition	221
48.5 Setup AuthControl Sentry Authentication definition	223
48.6 Testing authentication to Mimecast via Swivel AuthControl Sentry	223
48.7 Troubleshooting	227
49 Sentry SSO with Netscaler	228
49.1 Introduction	228
49.2 Overview	228
49.3 Configure Netscaler Login	228
49.4 Configuring Netscaler	229
49.5 Configuring Sentry Login	234
49.6 Configuring Sentry RADIUS	236
49.7 SSO	236
49.8 Authentication with AD/LDAP and Radius	236
49.9 Testing	237
49.10 Troubleshooting	238
50 Sentry SSO with Office 365	239
50.1 Introduction	239
51 Sentry SSO with OneLogin	240
51.1 Introduction	240
51.2 OneLogin Setup	240

Table of Contents

51 Sentry SSO with OneLogin	242
51.3 Sentry Configuration	242
51.4 Testing	244
51.5 Troubleshooting	246
52 Sentry SSO with Palo Alto	247
52.1 Setup AuthControl Sentry Keys	247
52.2 Setup SSO on Palo Alto	247
52.3 Sentry	247
52.4 Login Steps	247
53 Sentry SSO with PHP	248
53.1 Setup SSO with PHP	248
54 Sentry SSO with PulseSecure	249
54.1 Contents	249
54.2 Introduction	249
54.3 Configuring the PulseSecure VPN	249
54.4 Configuring the Sentry Application	255
54.5 Testing authentication to PulseSecure via Swivel AuthControl Sentry	255
55 Sentry SSO with Salesforce	259
55.1 Setup Sentry Keys	259
55.2 Enable SAML on Salesforce.com	259
55.3 Create a new Single Sign-On Settings entry on Salesforce.com	259
55.4 Determine and configure your SSO username attribute	261
55.5 Configuring the federated ID in Salesforce.com	261
55.6 Configuring alternative username attributes in the Swivel Core	262
55.7 Configure Check Password with Repository on the Swivel Core	263
55.8 Setup Sentry Application definition	263
55.9 Setup Sentry Authentication definition	265
55.10 Assign the Salesforce domain to the SSO definition	265
55.11 Testing authentication to Salesforce via Swivel Sentry	265
55.12 Troubleshooting	267
56 Sentry SSO with ServiceNow	272
56.1 Introduction	272
56.2 Setup AuthControl Sentry Keys	272
56.3 Setup SSO on ServiceNow	272
56.4 Configure Check Password with Repository on the Swivel Core	275
56.5 Setup AuthControl Sentry Application definition	275
56.6 Setup AuthControl Sentry Authentication definition	277
56.7 Testing connection with ServiceNow tool	277
56.8 Testing authentication to ServiceNow via Swivel AuthControl Sentry	279
56.9 Troubleshooting	282
57 Sentry SSO with SonicWall	283
57.1 Setup AuthControl Sentry Keys	283
57.2 Setup SSO on SonicWall	283
57.3 Configure Check Password with Repository on the Swivel Core	285
57.4 Setup AuthControl Sentry Application definition	285
57.5 Setup AuthControl Sentry Authentication definition	288
57.6 Testing authentication to SonicWall via Swivel AuthControl Sentry	288
57.7 Troubleshooting	291
58 Sentry SSO with Thycotic Secret Server	292
58.1 Introduction	292
58.2 Setup AuthControl Sentry Keys	292
58.3 Convert Sentry Keys to PFX	292
58.4 Download the Sentry SSO IdP metadata	292
58.5 Setup SAML on Thycotic Secret Server	292
58.6 Setup Thycotic Secret Server as a Sentry SSO Application definition	293
58.7 Configure windowsusername attribute	294
58.8 Login Example	296
58.9 Troubleshooting	300
59 Site ID	301
60 Upgrade from v3 to v4	302
61 Upgrading notes	303
62 Before upgrade : License considerations	304
63 Upgrading procedure	305
64 Need more help?	308
65 User Portal	309
66 Overview	310
67 Prerequisites	311

Table of Contents

68 Upgrading User Portal.....	312
69 User Portal Installation.....	313
70 User Portal Configuration.....	314
70.1 settings.properties.....	314
70.2 portalconfig.properties.....	314
71 Language files.....	315
71.1 messages_en.properties.....	315
72 User Portal Menu options.....	316
73 User Portal Usage.....	317
73.1 User Portal Login.....	317
73.2 User Portal Menu.....	317
73.3 User Portal Mobile Provision.....	318
73.4 User Portal Mobile Provision On Screen.....	319
73.5 User Portal Mobile Provision by QR Code.....	319
73.6 User Portal ResetPIN.....	320
73.7 User Portal ChangePIN.....	321
73.8 User Portal Token Sync.....	322
74 Additional Configuration options.....	324
74.1 Creating a URL redirect from the root level.....	324
74.2 Using 443 instead of 8443.....	324
74.3 Changing the logo.....	324
75 Known Issues.....	325
76 Troubleshooting.....	326
76.1 Changes to xml files do not take effect.....	326
76.2 Error Messages.....	326
77 User Portal Administrator User Guide.....	327
77.1 Overview.....	327
77.2 Prerequisites.....	327
77.3 User Portal Configuration.....	327
77.4 Language files.....	327
77.5 User Portal Menu options.....	327
77.6 Additional Configuration options.....	328
77.7 Known Issues.....	328
77.8 Troubleshooting.....	328
77.9 Changes to xml files do not take effect.....	328
78 V3 & V4 Appliance Quick Start.....	329
78.1 Quick Start.....	329
78.2 Accessing Appliance Menus.....	329
78.3 Updating Appliance.....	329
78.4 Webmin.....	330
78.5 Setting Hostname IP Address.....	330
78.6 Starting and Stopping Tomcat.....	330
78.7 Accessing the Swivel Applications.....	330

1 Authcontrol Sentry v4 Admin Guide

2 Swivel Secure AuthControl Sentry Version 4

- A Tutorial for Administrators

This document describes how to administer Swivel Secure's AuthControl Sentry version 4, referred to herein simply as 'Sentry'. It assumes no previous knowledge of the product, so can be used by new users, as well as users upgrading from an earlier version.

This tutorial refers only to administration through the web consoles: it does not include administration of the Swivel Secure appliance itself, which is covered by a different document. It is therefore assumed that the appliance has been allocated an IP address and connected to the relevant network. Where instructions may be different for upgraded installations, as opposed to new ones, the upgrade instructions are preceded by the following heading:

- Upgrade

Instructions following this heading are for upgrades only, and are different from new installations. Upgrade instructions are indented.

3 Getting Started

- Logging In

To connect to the main Sentry web administration console, open a web browser and enter the following URL: https://<appliance_address>:8080/sentry. Here, replace <appliance_address> with the IP address of the appliance, or if it has been allocated a name by DNS, the host name. Upgrade Upgrading users may need to use the old path name, /pinsafe, rather than /sentry. You will be presented with the Sentry login page.

For a brand new installation, there is one user, named admin, so enter this in the username field. Now click on the Start Session button. An image will be shown with ten random digits.

This is known as a TURING image, and is one of the possible authentication methods supported by Sentry. For a new installation, it is the only method available. To use this image, you need to apply your PIN, which will be allocated to you, to the string of digits, selecting the digits corresponding to the indexes above the string. In this particular case, the initial PIN for the admin user is 1234, so you should enter the first 4 digits shown in the OTC field: in the example above, 2476, then click Login. If this is the first time you have logged in, you will be presented with the End User Licence Agreement, which you will be required to accept in order to proceed.

This agreement will not be displayed on subsequent occasions, although you can recall it if required, as explained below.

- Status Screen

This is normally the first screen you will see when you log in. It shows a summary of the current settings. Note that it also includes a link to the EULA. Although the Status Page is the default page shown after logging in, you can also enter the full URL of a different page, or bookmark a specific page, and after logging in, you will be taken directly to that page.

- Help

Notice that on nearly every page, there is a Help link. This links to the appropriate web page on <https://kb2.swivelsecure.com>, and provides more detail on the options contained within the page.

- Entering the Licence

The first thing you need to do when setting up your AuthControl Sentry server for the first time is to enter the licence information. You need to enter this information on the following pages, in this order.

- Server -> Name

When referring to specific pages in the administration console, we will always use the above notation. The first part of the page name, before the -> symbol, refers to a top-level menu item on the left-hand menu, in this case Server. Click on that menu to expand it to show the sub-menu. Now click on the second part of the name, in this case Name. The appropriate page will be displayed.

Enter the site ID you have been allocated by Swivel Secure. This is unique to your installation, and is required in order to install the licence. It identifies your company both to the licence key server and to the Swivel Secure Mobile Connection server. You can also enter the name of the server, which is displayed at the top of the page. This is optional, and mainly useful if you have more than one appliance, as a quick way of identifying them. The third field on this page will be explained later. Click Apply to save these settings.

- Server -> Licensing

Use this page to enter the licence details, after you have entered your site ID. If you attempt to enter the licence details before the site ID, it will fail.

You should have been provided with a License Key. This, together with the Site ID, is enough to extract the License Information from the Swivel Secure License Server. However, if your appliance has not been configured with internet access, you will need to request this information from Swivel Secure: contact supportdesk@swivelsecure.com to request this information. In this case, you should set the Online option to No, to prevent the appliance from attempting to contact the license server. Click Apply to save the licence information. If it is correct, your current entitlements will be displayed. If it is not, an error message will be displayed. NOTE: if you later upgrade your licence, and your appliance has internet access, all you need to do is to return to this page and click Apply to retrieve the updated license information. If your appliance does not have internet access, you will need to request the updated license information from Swivel Secure once again.

- Creating A Repository

First of all a note on what a repository is: put simply, a repository is a source of users. Every user belongs to exactly one repository. Taking the user information from the repository source (server) into the application database is referred to as User Synchronisation, or ?User Sync?. Your appliance is provided with one repository. This is an internal repository (different types of repository will be described later), and contains the single admin user. You could maintain all your users in this repository, but most administrators prefer to synchronise their users from the company?s user directory. The most common directory is Microsoft?s Active Directory, and we will describe adding an Active Directory as a source of users here. If your user repository is not Active Directory, please read the more detailed notes on Repositories, later on.

- Repository -> Servers

This page is where you create your repositories.

You will see the single repository, named ?Local XML? for reasons that will be explained later. Click on New Entry and enter the name of your repository. If you will have multiple repositories, you will want to give this a meaningful name. In this case, we will simply call it ?Active Directory?. Select Active Directory as the type, and click Apply.

You will notice that the name ?Active Directory?, or whatever you have named your repository, has been added to the Repository sub-menu. Click on it.

There are a number of details you might need to enter here, but typically all you will need is the address of a domain controller, and the username and password of an Active Directory user with rights to read the directory: the username should be qualified with the domain, either as domain\username or as username@domain. Note that, since Sentry does not modify the Active Directory, this account does not have to be an administrator account. Note also that the Hostname/IP can either be the name or IP address of a specific domain controller, or simply the domain name, assuming that your DNS will resolve that correctly. You may also wish to select the port as 636 (Domain LDAP SSL), for increased security. If you do, you should also set the option Allow self-signed certificates to yes, unless you have installed a commercial certificate on your domain controller. The other setting you may wish to set now is the Synchronization schedule. This determines how often Sentry connects to your domain controller to retrieve users. If you leave it at the default setting ?NEVER?, then you can still sync users manually from the User Administration page, as explained later. We will discuss the remaining options later, but for now, leave them as default. Click Apply to save the settings. You may want to try the Browse in window button to confirm that you can connect to your domain controller ? we will discuss the repository browser later. Repository -> Groups To quote the help page: ?Groups are used within Swivel to manage user rights, messaging and other features. A Swivel group can include users from multiple repositories, and each user can be a member of multiple groups?. Put simply, the Repository -> Groups page defines two things: What rights each group is allocated The mapping between

Sentry groups and Repository groups

Sentry comes with a number of groups pre-defined. You can use the groups provided, you can modify or delete them, or create your own. You do not have to use all the groups provided for all repositories (or indeed at all): any group for which you do not provide a definition for a given repository will be ignored. You will see across the top the list of rights that groups can be allocated. The first 4 and the last: Single, Dual, Push, Mobile App and OATH refer to the different authentication methods that Sentry supports. Admin indicates that the members of this group are system administrators, who are given full rights over the administration console. Helpdesk users have limited rights, mainly limited to user administration: the exact rights allocated to helpdesk users can be changed as required. The final right is PINless: members of groups with the PINless right will not be allocated PINs (but see later), and will use the PINless versions of the various authentication methods. Below the rights buttons are the mappings that associate Sentry groups with repository groups. Where Active Directory is concerned, you can use the Browse button to select the appropriate Active Directory group, rather than manually entering the full group name.

It is assumed that you have previously allocated Active Directory groups, and are sufficiently familiar with Active Directory structure to be able to locate the relevant groups.

- User Administration

You are now ready to start importing users. Click on the User Administration menu. This is probably the page that administrators, and certainly helpdesk users, will see most of.

First, a summary of the controls on this page: Max No. Users: this simply controls the maximum number of users that will be displayed. It does not relate to the number of licensed users, and can be altered as required. Users per page: this sets the number of users that will be displayed at one time. If there are more users than can fit on one page, page controls will be displayed to select different pages. Repository: this drop-down allows you to select which repository of users is displayed. State: allows you to limit the displayed users to those in a given state: user states will be discussed later. User Search: this allows you to search for users according to the value of a selected attribute, such as username, surname etc. Custom attributes will be discussed later. Members of group: allows you to restrict the display to members of a specified group. View: determines what information is displayed about the users. The categories in this drop-down will be described later. Next is a row of buttons: Search: applies the selected settings from the controls above: most drop-down selectors trigger this option automatically. Reset: resets the selected settings to the default. Purge: permanently removes all users marked as deleted. Undelete: removes the deleted mark from all users. Add User: (for editable repositories only: see later), display a screen to add a new user to the repository. Import: (for editable repositories only: see later), display a screen to import a list of users to the repository. User Sync: executes a manual user sync, to import or update users from the selected repository. Sync Count: executes a ?dummy? user sync, to determine how many users would be added, modified or deleted. All the above controls act on the entire user set. To administer a single user, click on that user

Edit allows you to change attributes for an editable user. We will talk about editable repositories in the next section. Policy allows you to modify certain policies regarding the user.

Reset PIN allows you to set the user's PIN directly. When set from here, policies regarding PIN composition are ignored, so for example, you can set a PIN of 1234 even if sequences are not allowed. View Strings allows you to view a user's current security strings. You can also request a new single channel string for a user. Possible uses for this are described later.

Send String will send a user a new dual channel string. The user must have the Dual right for this to show. Resend sends the user a randomly generated new PIN. It does not, despite the name, resend their existing PIN. App Provision sends the user a mobile app provision message. The user must have the Mobile App right for this to show. Lock locks the user's account. If the account is already locked, this button shows as Unlock. Remove for editable users only, removes the user from the repository. History shows the recent activity for a user. You can select from a list of activity types.

- Managing Repositories

We will now look in more depth at how repositories work and the different types of repository.

- Repository Types

There are several different types of repository: the two most common are XML and Active Directory.

- XML Repository

An XML repository is, behind the scenes, simply an XML file. The main advantage of an XML repository is that the users can be entered directly into the User Administration page. This is an example of a writeable repository, of which more later.

- Active Directory Repository

An Active Directory repository defines a connection between the application database and a Windows Active Directory (AD) Domain Controller (DC). Note that it is a defined Domain Controller: we are often asked if we can define multiple DCs, to which the answer is no. However, you can specify the domain name as the host, which can be resolved by DNS dynamically. The online help page goes into more detail on configuring AD repositories, but 2 features should be mentioned, which will be expanded on below: it is a read-only repository, as opposed to the XML repository being writeable, and it uses LDAP, in common with other repository types.

- Writeable and Read-Only Repositories

Repository types can be split into writeable and read-only repositories. ?Writeable?, means that the users can be created, edited and deleted directly within the user administration page. When you do this, the users are automatically synchronised with the database. Another feature is that you can import text files containing user details into writeable repositories, using either CSV or XML ? the XML import uses the same schema as the XML repository, which is defined in the online help page. XML, ADAM and LDAP Writeable are the writeable repositories, the others being read-only.

- LDAP

Lightweight Directory Access Protocol (LDAP) is a standard protocol used by Active Directory, and by a number of non-Microsoft operating systems, for managing users. When defining LDAP repositories, you need to be aware of the directory structure of the LDAP server. Users are defined within LDAP as being members of a group, and we use the group membership to define how users are imported. All the repositories types supported by Sentry use LDAP to communicate with the server, except for XML and Database.

- Database

A database repository is simply that: the users are imported directly from a database. It is flexible about the database structure, but it expects a single table (or view) for users, and another for user group membership. More information on defining a database repository can be found in the online help.

- ADAM

The name ADAM is now obsolete: the name that Microsoft now use is Active Directory Lightweight Directory Services, or AD-LDS, but we use the old name ADAM for convenience. It is, as the name implies, a lightweight version of Active Directory that can be installed on any Windows PC. It works in more or less the same way as AD, but has the advantage, in our implementation, of being writeable.

- Agents as Repositories

There is a final type of repository: Agent repositories. These are managed by Agents (of which more later), using the AgentXML API (again, of which more later). They are not defined within the repository configuration.

- Repository Definitions

You define repositories by adding them to the Repository -> Servers page. All you need to add here is the name and the type. This creates a new entry in the Repository menu, where you can define the repository details. Configuring repositories is covered in more detail in the online help.

- Repository Group Management

We have already discussed the uses of repository groups, and described how to set the group mapping for Active Directory. The same Browse feature is available for other LDAP repositories as well. For XML repositories, typically the repository group name is the same as the Sentry group name. For LDAP repositories, it is the fully-qualified domain name (FQDN) of the group. All members of the group, including members of contained groups, are imported into the Sentry group. For database repositories, the group mapping should contain the value in the Group column of the User Membership table or view. A quick note on non-standard features of Active Directory: AD allows inter-domain group membership, so members of groups in other domains within a forest can be members of a group. Unfortunately, the way it does this is not part of the LDAP standard, so this behaviour is not supported by Sentry. If you need to support inter-domain membership, you must use the AD Global Catalog, which is like a single-domain view of the entire forest. It uses different ports from single-domain LDAP.

- Helpdesk Group Rights

This menu can only be found from the Repository -> Groups menu. It offers a more fine-grained way of managing which helpdesk users are allowed to manage which users, for large companies with complicated structures. The online help page describes how it works.

- Custom Attributes

Custom attributes are miscellaneous additional information imported from the repository. They are used to define email addresses and phone numbers for messaging, can be used to search in the user administration page, and as alternative usernames in authentication ? of which more later.

As with groups, you need to define which attributes from the repository map to the Sentry attributes. A default set of attributes are provided, with default mappings dependent on the repository type. You can change or remove the mappings ? if there is no mapping, then no value will be stored for the attribute. You can also add your own custom attributes. Note the other settings for each attribute: Phone Number?: this is a Yes/No flag. The repository settings allow you to specify that phone numbers can be reformatted, removing or adding country prefixes, additional notation etc. Therefore, the phone numbers need to be indicated. Sync Rule: this indicates how a user sync treats a given attribute. The default, Synchronised, means that the attribute is always read on user sync. Initialised means that it is read for new users, but not updated for existing users. Local means that it is never read from the repository. The reason for this setting is that it is possible for external applications to modify attributes, using an API described later. This prevents user sync from overwriting the effects of the API changes. Add repository qualifier?: this option allows a prefix or suffix to be added to the attribute value. The qualifier is defined in the repository settings, and can be applied to the primary username as well, in the repository settings. This is typically used to create the Windows account name form domain\username, since there is no single attribute that returns that value.

- Messaging

This section defines how Sentry communicates with users, which essentially means by email or by mobile phone. As mentioned above, Sentry uses custom attributes to control messaging, and the Messaging -> General page defines how. It contains a list of available transports, which is how we refer to the different messaging mechanisms. You will not need the majority of these, but you may need to add transports that are not shown in the default list. Swivel Secure support can provide advice on which additional transports are available, and we can develop custom transports if you wish to use an SMS portal that is not currently supported. If you need to add a new transport class, be aware that the name must be different from all other classes, but otherwise is not significant. The class name must be entered in full and is case-sensitive. All class names start with the prefix com.swiveltechnologies.pinsafe.server.transport. For brevity, we will omit this prefix when referring to specific classes, and just give the unqualified class name. The online help page defines what information you need to enter into this page. You just need to be aware that messaging is used for 3 different things: Alerts ? basically any message to the user that doesn't come under the other categories Strings ? dual channel security strings, which will be discussed later Push notifications ? for Push / One Touch authentication, which will be discussed later The definitions require a single group for each transport. If you want to define multiple groups to use the same transport, you must create a new transport using the same transport class. Make sure the transport name is different from the original. You can define multiple transports for different alert groups (and strings groups), but if users are members of multiple transport groups, only the first one will be used. The Push repository group should only be set on the PNA transport. Once you have activated a transport by selecting an attribute and either a Strings or Alert group, a new menu item appears for you to enter the details of the transport. Most of the details are the contents of the various messages, but specific transports require specific additional information, such as gateway URLs for SMS gateways. A note on SMTP: SmtptTransport does not support secure SMTP, but there is an additional class, SecureSmtptTransport, that does. The default SmtptTransport uses the SMTP server defined by the system, but the secure SMTP transport defines its own SMTP server. It supports the StartTLS protocol, as used by mail servers like Gmail.

- Agents

Sentry uses a proprietary API called AgentXML as one protocol for user authentication. See the [Agent-XML](#) article for full details. For an external device to communicate with Sentry using the AgentXML protocol, it must be defined as an Agent, using the Server -> Agents page.

Note that one Agent, named ?local? is pre-defined. This is required, as it is used by all the other applications on the applications to communicate with the Core. Do not modify this Agent. The essential values for an Agent are the hostname or IP address and the Shared secret. Note that IP addresses can be specified as sub-nets: for example, 192.168.0.0/24 includes all IP addresses in the 192.168.0.x range. Also, multiple Agents can be defined for the same address, provided that the secret is different. The Agent device itself must send the secret as part of the AgentXML request for it to succeed. Agents can be used as repositories as well as for authentication. For this to happen, the Agent must have the option ?Can act as Repository? enabled. Once this is set, the Agent will appear in the list of repositories on the User Administration page. Note that an Agent can have the same name as a Repository. If they do, then the Agent acts on members of that repository. This can be useful, but can also have unexpected side effects. Also note that a User Sync potentially can wipe out the effects of API calls, hence the Sync Rule setting on attributes. This enables attributes to be set by API calls that are not overwritten by user sync. We will discuss the other Agent settings when we discuss authentication methods later.

- RADIUS

We will be discussing Remote Authentication Dial-In User Service in more detail later, but in brief is it a standard authentication protocol used by many VPNs and Gateways.

- RADIUS -> Server

The RADIUS server is enabled by default, but if you are not using Sentry to authenticate any RADIUS devices, you can disable it. Typically, you do not need to set an IP address: it will use any IP address available to the appliance. The authentication port is 1812 and accounting is 1813, although Sentry does not make use of the accounting information. You may need to change these if your device uses non-standard ports. The other options will be discussed in the section on authentication, later.

- RADIUS -> NAS

This page is used to configure the Network Authentication Server (NAS) devices that will use Sentry to authenticate. Typically, you will need the IP address or host name and the shared secret: the latter will need to be configured on the device as well. Unlike Agents, you cannot specify a NAS for a sub-net, only for single devices. The other settings will be discussed later.

- Authentication

Sentry provides several different ways for users to authenticate: Single Channel Methods The following methods are all categorised as Single Channel, and can be used by users with the Single right. Single channel methods always require some form of customisation to the authentication page of the integrated device or application. Swivel Secure have developed such customisations for a large range of products: see our KnowledgeBase or contact supportdesk@swivelsecure.com for more information. Single channel authentication is always Session-Based. That is to say, requesting a single channel image starts an authentication session on the Sentry appliance. This session is both exclusive and time-limited: when a user has an active session, they cannot authenticate using any other method, and the session is only valid for a limited time. By default, the time limit is 2 minutes, but methods to change the time limit will be described later.

- TURING

A ?Captcha? image containing 10 random digits or characters is displayed on screen, and the user selects the ones corresponding to their PIN. In the above example, if the user's PIN was 3974, then they would enter as their one-time code the digits corresponding to the indexes 3, 9, 7 and 4, i.e. 8317. The single-line TURING image is by far the most commonly used, but we do offer other formations, by selecting the Image file in Server -> Single Channel.

- Button

The indexes are not shown in this pattern, but they are the same as on a phone keypad, so for the PIN 3974, the OTC here is 6751.

- Pattern

Here the indexes go from top to bottom, left to right, so the OTC for 3974 is 2708. Pattern2

Again, the indexes go top to bottom, left to right, so the OTC for a PIN of 3974 is 8206. The image type selection is a global setting: it is not possible to choose different patterns for different users or different integrations.

- PINpad

PINpad provides an alternative input method for certain integrations:

The format may vary: some integrations display the numeric keys as rows of 3, 4 and 3 buttons, and the C and R buttons (for Clear and Refresh) are not always shown. The idea here is that you always click on the buttons corresponding to your PIN: the positions of the buttons vary at random. Clicking on the button enters the value corresponding to the position of the button, rather than the number on it.

- Dual Channel

An email or SMS is sent to the user containing 10 random digits or characters, as with TURING, except that the string is text, rather than an image. By default, the strings are sent in advance, so any user with the Dual right is sent a string as soon as their account is created, and when they use that one, a new one is sent ready for the next time. An alternative configuration is to enable On Demand Authentication on the Server -> Dual Channel menu. This means that strings are not sent out in advance, but only when requested. This means that the integration must be customised to allow a string to be sent out. The advantage here is that the user only receives the string when it's needed, reducing the probability of losing it. The disadvantage is that the user must always be able to receive their strings, whether by email or by SMS. On Demand Authentication is also session-based: see the discussion on Single Channel to understand what that means. By contrast, dual channel strings sent in advance have an indefinite lifespan, although they can only be used once. There is a compromise solution: enable On Demand Delivery, rather than On Demand Authentication. With this option enabled, users receive security strings in advance, but if they have lost their latest one, they can request a new one by the same method as On Demand Authentication. Strings requested using On Demand Delivery, however, are not session-based.

- OATH Tokens

These are physical tokens, which display random codes using the OATH standard. Swivel Secure can provide branded OATH-compliant tokens, but any such tokens can be used with Sentry authentication, provided that the token seeds are available. Sentry supports both event-based (HOTP) and time-based (TOTP) tokens. There are also applications that can act as ?virtual? tokens: Google Authenticator is probably the best-known example of this. In fact, with the release of version 4, Swivel Secure provides OATH authentication on its Mobile App.

- AuthControl Mobile App

Swivel Secure's AuthControl Mobile app is available for Android, iOS, Windows and Blackberry. Once a user has installed the Mobile App on their phone, it must be provisioned against the Sentry instance: instructions for this are provided elsewhere. 99 random strings are then downloaded to the phone, and displayed to the customer in order. When the strings run out, the user must request more. Alternatively, the app can be configured to use OATH, in which case there is no need to renew the strings. There is also a PC app that provides the same functionality on a Windows desktop. Push authentication uses the mobile app. When the user wishes to log in, a push notification is sent to the phone. The user must respond on the phone, either with a simple Yes/No, or a known code. This sends back a message, which results in a unique session ID being sent to the Agent. This also requires customisation to the authentication page.

- Authentication Protocols

We support 3 different protocols for authentication:

Agent XML ? our Proprietary API. This is used in many in-house apps, such as the IIS filter and Credential Provider. This has been mentioned previously, mainly in respect of using an Agent to modify user details, but the primary purpose of the Agent XML is to provide a means of authentication.

RADIUS ? used by many VPNs and Gateways. Sentry supports a limited range of RADIUS protocols. Only the PAP protocol is available for all authentication methods, but that is the most widely supported protocol. We also support CHAP, including MS-CHAP versions 1 and 2, but not EAP-MSCHAP. The only EAP-based protocols that we support are LEAP and EAP-MD5.

SAML ? this protocol is the basis of the Adaptive Authentication methodology. It is an industry standard, used by ADFS among others. The Adaptive Authentication solution also supports SAML over RADIUS, increasing the range of support for SAML to devices that do not support SAML natively. There is a separate tutorial on Adaptive Authentication that covers this in more detail.

- Other Configuration Settings

The online help provides details of every option on the administration menus. However, there are some features which warrant special mention. These are listed below.

- Changing the Session Validity

As mentioned previously, session-based authentication is time-limited, with a default timeout of 2 minutes. The setting that changes this timeout is on the Server -> Jobs menu. The setting is Session cleanup: the value is in seconds.

- Authenticating to Active Directory and Other Repositories

Swivel Secure's authentication solutions are targeted primarily as additional authentication: frequently they are used alongside Active Directory authentication or other username and password solutions, which we will refer to as 'Primary' authentication. However, in some cases, it is useful for Sentry to perform the authentication to the primary server as well as the Swivel Secure 'Secondary' authentication. We support this for both AgentXML and RADIUS: in both Server -> Agents and RADIUS -> NAS, there is an option 'Check Password with Repository?'. When enabled, this will expect to receive the AD or other repository password in addition to the one-time code. In the case of AgentXML, it is received as a separate field; for RADIUS, since it only supports one password field, the password and one-time code should be sent as a single value, the password first and no space between the values. As the one-time code has a known length, the split can be determined. This is the secondary use for repository servers, in addition to synchronizing users. In the case of LDAP (including Active Directory), a simple bind is performed. This may require the use of an alternative username to work: see the next section.

Use of this option can cause confusion in some cases, particularly in integrations which already require Active Directory authentication. You should pay close attention to whether the application you are integrating with connects directly to AD, or whether it passes the password through Sentry. For example, the Swivel Secure Credential Provider (the previous versions as well as the current), pass the password directly to Active Directory, so if the Agent is set up to handle a Credential Provider, 'Check Password with Repository?' should be set to No. Likewise, when using RADIUS as an additional authentication, alongside Active Directory, typically you will not use this option. The most common use for this option is with two-stage RADIUS authentication, which is covered in a later section.

- Support for Alternative Usernames

There are occasions when users need to be referenced by identifiers other than the primary username in Sentry. An example of this is mentioned above: when authenticating to Active Directory, the unqualified username (sAMAccountName) will not usually work: you need either domain\accountName, or userPrincipalName (name@domain). Alternative username support needs to work two ways: Sentry should recognise alternative usernames where appropriate, and it should also provide alternative usernames when authenticating to repositories, as in the previous section on authenticating to Active Directory. Recognising alternative usernames is useful when integrating with products that use Sentry as a secondary authentication solution. In this case, the primary authentication method may require the username in a specific format, such as userPrincipalName. It is inconvenient if the user has to enter two different usernames for the two authentication methods, so the ability for Sentry to recognise alternative usernames is useful here.

This is supported in both Server -> Agents and RADIUS -> NAS by the option 'Allow alternative usernames?'. If this option is enabled, you should also set 'Alternative username attributes?'. This is a comma-separated list of Sentry attributes that should be recognised as usernames for this Agent or NAS. Note that this is the Sentry attribute name, not the repository attribute name. The most common attribute used here is 'altusername?', which maps by default to userPrincipalName in Active Directory. When checking the repository password is enabled, you will probably also want to set the 'Username attribute for repository?' field. This determines which Sentry attribute to send to the repository with the password. Again, 'altusername?' is the most common value. If left blank, the primary username is sent. When requesting a single-channel image or dual-channel security string, you can also use alternative usernames. This is often necessary, since the same username is used to request the image/string as to authenticate. The settings to enable this are on Server -> Single Channel and Server -> Dual Channel respectively, and as before are labelled 'Allow alternative usernames?' and 'Alternative username attributes?'.

- RADIUS Two-Stage Authentication

Sentry supports authentication to RADIUS in two stages, usually referred to in RADIUS devices as 'Challenge-Response?'. Note that two-stage authentication is ONLY supported with the PAP protocol. It is enabled by the 'Two Stage Auth?' option on the NAS settings. In this case, the first stage expects only the password. The one-time code is sent at the second stage. Several other NAS settings also relate to two-stage authentication: Check password with repository? we have already discussed this above, but typically, when using two-stage authentication, the repository password is sent at stage 1. Allow blank password at Stage One? if the repository password is NOT used at stage 1, then the Sentry password is checked. Frequently, Sentry passwords are not used, so this option allows stage 1 to pass in just the username and no other information. Send Security String after Stage One? a typical scenario for two-stage authentication is with dual-channel on-demand authentication. In this case, the user enters the username and password at stage 1. Only if the password is correct is the user sent a security string from which to extract the one-time code for stage 2. Even if User has Valid String? if this option is set to No, and the user already has a valid security string, then a new string is not sent, even if the previous option is set to Yes. Send username in challenge? this option is typically only used where stage 2 displays a single channel image on the login page. Since the image requires the username in order to display, if there is no way to determine it from other information on the page, the username is sent as part of the challenge string sent back to the NAS, in the form username:challenge. Another use of challenge-response is when a user is required to change their PIN. The option 'Change PIN warning?', when enabled, returns a challenge message 'changePIN?' if the user's PIN is due to be changed. In this case, the response needs to be in the form cp1=<oldotc>cp2=<newotc>. Here, <oldotc> and <newotc> need to be replaced by the one-time code for the old PIN and the one-time code for the new PIN, both using the same security string.

- Using Security Strings Multiple Times

Both Server -> Single Channel and Server -> Dual Channel have the option 'Multiple Authentications per String?'. This is mainly needed for certain badly-behaved RADIUS NAS's that make multiple requests for the same user. However, it has also been used to provide temporary passwords: a sort of 'Multiple-Times Code?'. To make this useful, you typically should increase the session cleanup time to a much larger value? typically a day. A user can then be issued a security string, and from it extract a code that can be used repeatedly over a short period. Note that the View Strings option on User Administration has an Invalidate button to terminate this code before it expires, if required.

- Logging

Sentry logs most of the activity that occurs in the Sentry application. There is a Log Viewer that allows you to view those logs. However, we are aware that searching through these logs can be extremely slow, and occasionally fails to give the correct result. We therefore have alternative solutions. Logger messages can also be sent to Syslog devices, as controlled by the Logging -> Syslog menu. Certain messages can also be sent to a specific email address as well, as controlled by the Logging -> SMTP menu. You can decide what level of messages are sent by email, how many messages to accumulate before sending them, and whether to trigger an email on the occurrence of a higher-level log message. There is also a new, much faster log viewer. For technical reasons, this is a separate application, accessible using the URL path '/logviewer?', rather than '/sentry?'. You need to log into that separately from the main administration console. The new log viewer copies the logs to a database, which makes it much faster and more reliable. The down side of that is that it isn't always up to date, as it only reads completed log files: the logs are split into separate files, which are closed when they reach a certain size. You can control the size of the log files on the Logging -> XML menu.

4 PIN Policies and Locking

- Locking

You can control policies for locking user accounts on the Policy -> General menu. In particular: Maximum login tries determines how many successive failures a user can make before the account is locked. Account lockout time determines whether accounts are locked for a limited time, and if so, how long. Setting this value to 0 means that helpdesk intervention is required to unlock a user account. One thing to be aware of here is that the timed lockout only begins when the user attempts to log in one time too many. So, if the Maximum login tries is 3, and a user fails to login 3 times in succession, the timed lockout only starts when they attempt to login for a 4th time, or at least request an image or string for the 4th time. Inactive account expiry determines how long a user account must remain inactive, with no successful login attempts, before the account is deemed to be inactive, and locked out. Setting a value of 0 means that accounts are never locked due to inactivity.

- PIN Expiry

You can control requirements for users' PINs using options on the Policy -> PIN and OTC menu: PIN expiry indicates how long a user can keep the same PIN before they must change it. A value of 0 indicates that PINs never expire. You can also set a policy for individual accounts to override this option. PIN expiry after auto/admin reset is similar to the previous one, but applies to PINs that are reset by helpdesk, rather than by the user. PIN expiry warning sets a period during which the user is warned that their PIN is about to expire. Note that this is an interval before the actual expiry, so for example, if this value is set to 7, the first warning will occur 7 days before the PIN actually expires, and will recur daily until the user actually changes their PIN, or the PIN expires. PIN change grace period this setting applies for one specific scenario only: a user's PIN expires and their account is locked. The helpdesk then unlocks the PIN, but does not reset the PIN. In this case, this setting determines how long the user now has to reset their PIN. Require PIN change after auto setting means that the user must change their PIN immediately after first logging in, if they have been allocated a random PIN, either on account creation, or using the Resend button from User Administration. Require PIN change after admin reset is similar to the previous option, but applies after a user has had their PIN manually reset by the helpdesk. Only warn user, do not lock account if enabled, accounts are never expired because the PIN has expired: users are only warned that they have not changed their PIN. Auto-reset PIN on expiry when enabled, accounts are not locked when the PIN expires: instead, their PIN is automatically reset to a random value. The behaviour of this option in combination with the PIN expiry warning setting is noteworthy: if PIN expiry warning is greater than 0, the PIN is changed instead of sending the first warning, so before the PIN actually expires.

- PIN Composition

The following settings apply to PIN composition: Minimum PIN size is the minimum number of digits a PIN can have. Maximum repeated PIN digits is the number of times the same digit can occur in a PIN. So if 0, all digits must be different, etc. Allow numeric sequences for PIN if disabled, sequences such as 1234, 2468, 9753 are disallowed. Banned Credentials the Policy -> Banned Credentials menu allows you to specify PINs that are not permitted. You can use ??? to indicate any PIN, so for example, ?19??? prohibits any 4-digit PIN starting with 19.

- PINless

As mentioned previously, users can be designated as PINless. In this case, rather than extracting a one-time code from the security string using a PIN, they enter the entire security string as the one-time code. The following policies from Policy -> PIN and OTC affect PINless users: PINless OTC length determines the number of characters in a PINless security string (PINless security strings are always 10 digits). Always use PIN for single channel overrides the PINless flag when authenticating as single channel. In this case, users are actually allocated a PIN, but they only need to authenticate as PINless when authenticating using a single-channel authentication method. For all other methods, they are PINless.

- Mobile App Policies

This section describes settings relating to the AuthControl Mobile app. There is one setting on Policy -> General that relates to the Mobile app: Auto send provision code when enabled, provision codes are automatically sent to users with the Mobile App right, on account creation. Some Mobile App policies are actually on the Policy -> Self-Reset menu: Allow user self-provision of mobile app if enabled, allows the user to provision their mobile app using the user portal. If disabled, the helpdesk must initiate mobile app provisioning, unless auto-send is enabled.

Send provision code as security string if enabled, the provision code is sent as a security string. Otherwise, it is sent as an alert. Mobile App Local Mode if enabled provisions the mobile app with security strings that are generated using the OATH algorithm. This means that the mobile app does not need to connect to the Sentry server to provision. However, it also means that when the 99 strings are exhausted, the app must reprovision, rather than simply requesting more strings. Mobile App OATH Mode if enabled provisions the mobile app as a virtual OATH token. Provision Code Validity period determines how long a provision code is valid. The default is 1 day. URLs the last 4 options on this menu are URLs that are used for provisioning. You should not typically change these unless told to do so by Swivel Secure. There are also policies on the Policy -> Mobile App menu that determine what control the user has over the Mobile App.

- Custom Images

The default email messages include a number of images. You can use these default images, or you can provide your own. If you want to use your own, you must first change the Base URL setting on the Server -> Name menu. This should be the public URL for your Sentry appliance, and will typically be the same as that provided for your mobile apps. If you leave the default, <https://demo.swivelcloud.com>, you can continue to use the default images, but the custom images you upload will not be available. If you change the base URL to your own, all the default images will still be available, as they are installed on your appliance. You can upload your own images, or remove the default ones, using the menu Upload Email Images.

- Reporting

Reports can be generated on demand, or can be scheduled, as shown by the following menus: Reporting -> Instant

Reporting -> Schedule

We provide a small list of built-in reports, but if you want a report that is not there, please contact supportdesk@swivelsecure.com. New reports can be added without having to restart Sentry.

- Managing OATH Tokens

The OATH menus are provided for administrators to import lists of OATH token seeds, and to assign tokens to users.

Note that tokens come as HOTP and TOTP ? event-based and time-based. If you import a batch of tokens as the wrong type, the only option is to remove them and try again: however, the Import menu allows you to delete all users in a list, so removing an entire set is simple. TOTP tokens cannot be synchronised, but rely on the appliance clock being correct to within a minute.

This menu allows you to import tokens: make sure you have set the correct token type on the Policies page first. You can also allocate tokens to users. Only users with the OATH right can be allocated tokens.

This menu shows all users that have been or can be allocated tokens

- High Availability

High availability settings are largely configured on the appliance CMI, but there are two menus on the web administration that are used with high availability environments. These menus have no meaning for stand-alone appliances.

- Session Synchronisation

Session synchronisation is the process by which an authentication session generated on one appliance is also available on the other. This is managed by the Appliance -> Appliance Synchronisation menu

Here, you should enter the IP address or host name of the partner appliance in the first field. Typically, the context will be ?sentry?, port is ?8080? and Use SSL should be ?Yes?. ?Ignore SSL Cert Errors? will normally be ?Yes? as well. The Shared Secret should be the same on both appliances and Synchronise Sessions will be set to ?Yes?. Now every time an authentication session is generated on one appliance, it will be duplicated to the other. This ensures that it is possible to generate sessions on one appliance, but authenticate on the other. If you are not using session-based authentication, there is no need to configure this menu. Configuration Synchronisation

Config Sync controls which settings are replicated between appliances. Not all settings can be replicated, and certain ones, in particular scheduled tasks, should not be the same on both appliances. We always recommend that either customers disable scheduled syncs on the standby, or they offset them by at least half an hour. The settings here are slightly different from session synchronisation. Here you should set the broker IP to be the primary appliance IP or host address on BOTH appliances. On the primary ONLY, set ?Act as Broker? to yes: on the standby, leave it as No. The shared secret should again be the same on both. Enable ?Synchronise configuration? on both.

5 Authcontrol v4 Sentry SSO and Adaptive Authentication

6 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 Salesforce.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.

7 Getting Started

7.1 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 SWIVEL SECURE LIMITED (English company number 04068905) ("**SWIVEL**"). BY DOWNLOADING AND/OR INSTALLING THE ACCOMPANYING SOFTWARE ("**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 payment of the "**Licence Fee**") to either Swivel or a reseller appointed by Swivel (the "**Reseller**") for the Licensed Software and associated documentation (collectively, "**Licensed Products**").

LICENCE. Swivel grants Customer a personal, non-exclusive licence to use the Licensed Products subject to the terms set out in this Licence. Swivel shall have no obligation to provide maintenance or support for the Licensed Products except for 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 accordance with the usage 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 conclusively presumed a breach of this Licence);
- (iii) not to reverse engineer, disassemble, reverse translate, decompile, or in any other manner decode the Licensed Software or to derive the source code form or for any other reason (and any such action shall be conclusively presumed a material breach of this Licence);
- (iv) not to make full or partial copies of Licensed Products except such limited number of back up copies of the Licensed Software in object 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, except those Customer interactions with the Licensed Software associated with normal use and explained in the associated documentation;
- (vi) that the right to use the Licensed Software is restricted by a measure of usage based upon number of users or devices. If the specified usage level shall require payment to Swivel or a Reseller of an incremental charge or another licence, Customer shall pay the applicable price, following which payment Swivel shall provide Customer with an activation key or registration for the additional usage;
- (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, ¹³¹ distribute, sell or otherwise transfer the Licensed Products or any rights in the Licensed Software or Licence to any third party except as expressly permitted hereunder; and

7.2 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

```
imagesssl=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

7.3 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.

7.3.1 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.

7.4 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

[Rules](#)[Applications](#)[Authentication Methods](#)[View IdP Metadata](#)[Keys](#)[Users Active Sessions](#)[User History](#)[Log Viewer](#)[General Configuration](#)[Application Images](#)

Keys

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

© 2017 Swivel Secure. All rights reserved.

7.5 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.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

AuthControl Sentry

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

8 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:

[Rules](#)[Applications](#)[Authentication Methods](#)[View IDP Metadata](#)[Keys](#)[Users Active Sessions](#)[User History](#)[Log Viewer](#)[General Configuration](#)[Application Images](#)

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.

Rules

Applications

Authentication Methods

View IDP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Application Types

RADIUS VPN - Cisco ASA

✓Select

RADIUS VPN - Citrix Netscaler

✓Select

RADIUS VPN - Juniper

✓Select

RADIUS VPN - Other

✓Select

SAML - ADFS

✓Select

SAML - Citrix Netscaler

✓Select

SAML - GoToMeeting

✓Select

SAML - Google

✓Select

SAML - Mimecast

✓Select

SAML - Office 365

✓Select

SAML - OneLogin

✓Select

SAML - Other

✓Select

SAML - PulseSecure

✓Select

Example SAML Application:

SAML Application



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not used in the 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

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"

Start Page

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users / Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application

Name

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

Format

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

Sentry Attribute

email

Save

Back

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.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History



Log Viewer

General Configuration

Application Images

Application Images

Hide Default Images

Image	Name	Actions
	ADFS.png	 Replace
	Cisco.png	 Replace
	CitrixNetscaler.png	 Replace
	GoToMeeting.png	 Replace
	Google.png	 Replace

9 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

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

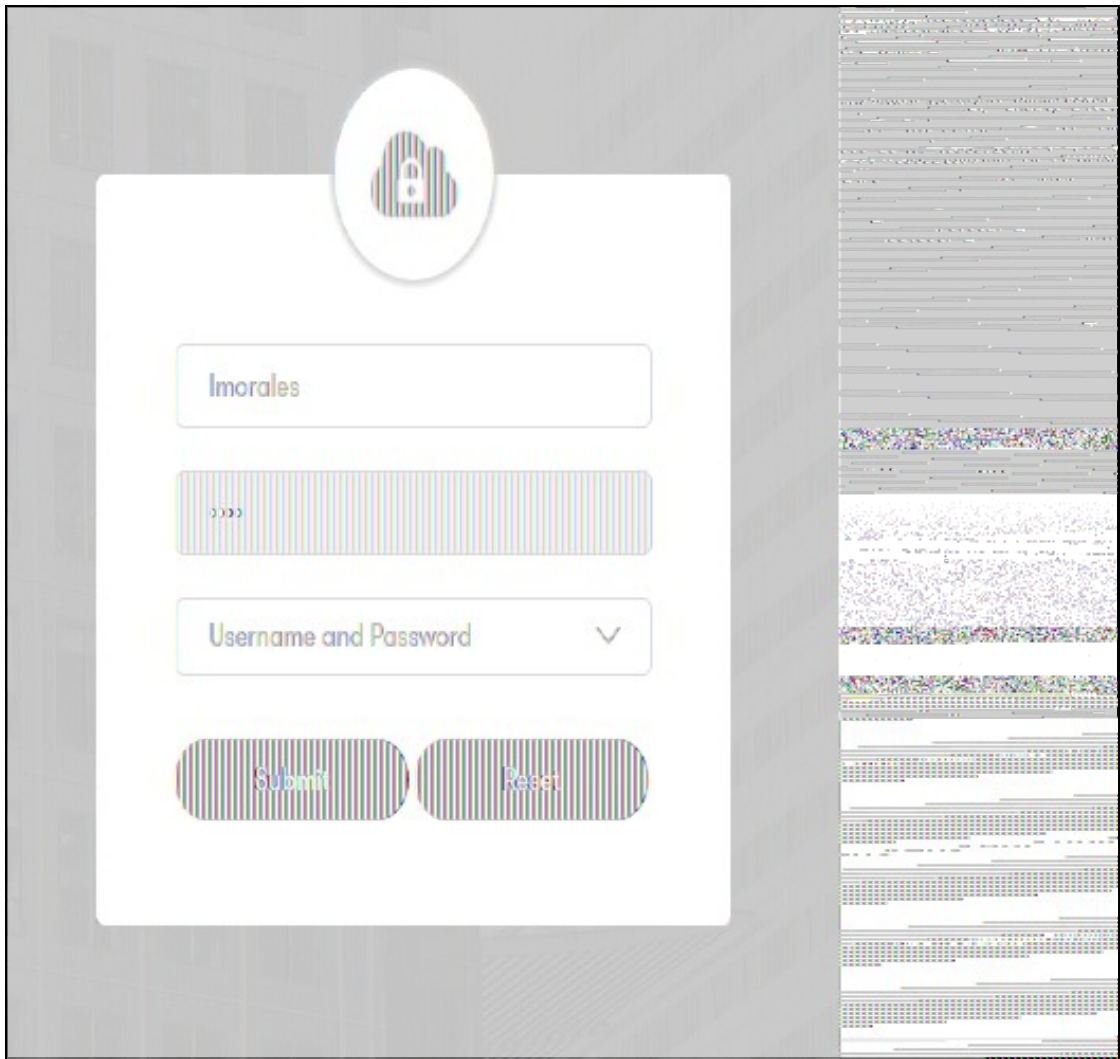
Application Images

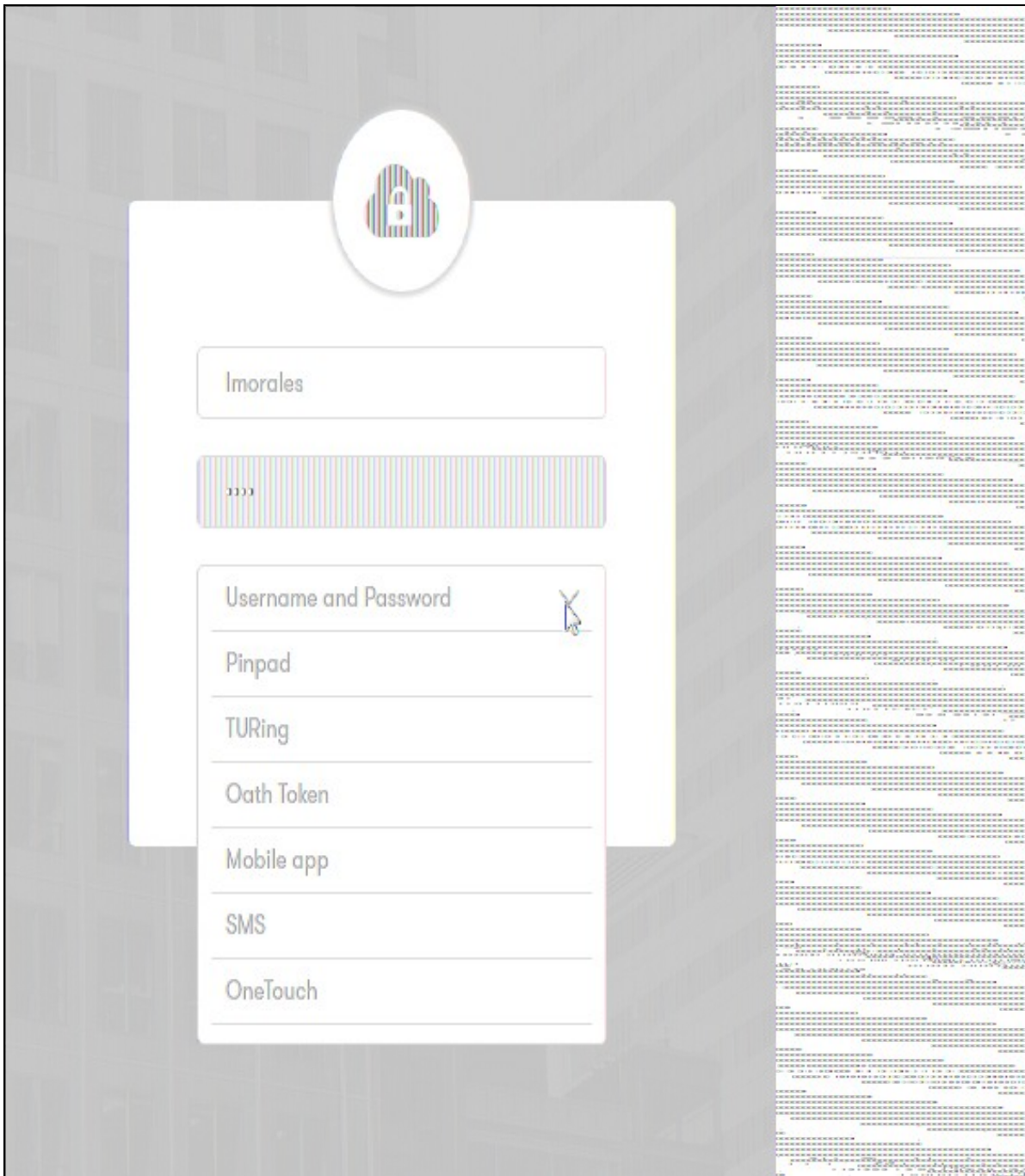
Authentication Methods

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.





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.

Rules

Applications

Authentication Methods

View IDP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

General Configuration

SSO Enabled☒

Log Level

TRACE

Show Allowed Authentication Methods By Rights☒

Delete Logs Older Than (days)

30

Show End User Licence Agreement

Save

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.

10 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

Applications

Authentication Methods

View ID Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Rules

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

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.

10.1 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

Rules

Applications

Authentication Methods

View IDP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

IP Range Rule

Name

Whitelist

Score When Valid

50

IP range

192.168.0.0/24

Save

Rules

Applications

Authentication Methods

View IDP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

IP Range Rule

Name

Score When Valid

IP range

Save

10.2 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:

Rules

Applications

Authentication Methods

View IoP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Time Range Rule

Name

Working Hours

Score When Valid

50

Start of time range

09:00

End of time range

17:00

Save

10.3 Certificate

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

Parameters:

None

Example:

Rules

Applications

Authentication Methods

View IDP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Certificate Rule

Name Managed Device

Score When Valid 50

Save

For further details on configuration, check [Client Authentication using Certificates](#)

10.4 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:

Rules

Applications

Authentication Methods

View IDP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Group Membership Rule

Name

Admins

Score When Valid

-50

Name of group

Administrators

Solve

10.5 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:

Rules

Applications

Authentication Methods

View IP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

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

Save

10.6 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:

Rules

Applications

Authentication Methods

View IP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Geo IP Rule

Name: Countries Where We have Offices

Score When Valid: 50

Country code: GB,US,ES,DE

Save

10.7 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:

Rules
Applications
Authentication Methods
View IDP Metadata
Keys
Users Active Sessions
User History
Log Viewer
General Configuration
Application Images

Geo Velocity Rule

Name
Area based

Score When Valid
-50

Speed Limit(MPH)
100

Save

10.8 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:

Rules

Applications

Authentication Methods

View IOP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Compound Rule

Name

Admin and not working hours

Score When Valid

-50

Rules

PulseSecure2

Office365

CiscoASA

Working Hours

Admins

AND

OR

XOR

AND NOT

PulseSecure2

Office365

CiscoASA

Working Hours

Admins

Save

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

40

Rules

Applications

Authentication Methods

View JSP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Compound Rule

Name

Admin and not working hours

Score When Valid

50

Rules

Pulse

PulseSecure2

Office365

CiscoASA

Working Hours

Admins

AND

OR

XOR

AND NOT

Mimecast

Salesforce

Google Apps

JuniperVPN

ServiceNow

Twitter

Save

11 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.

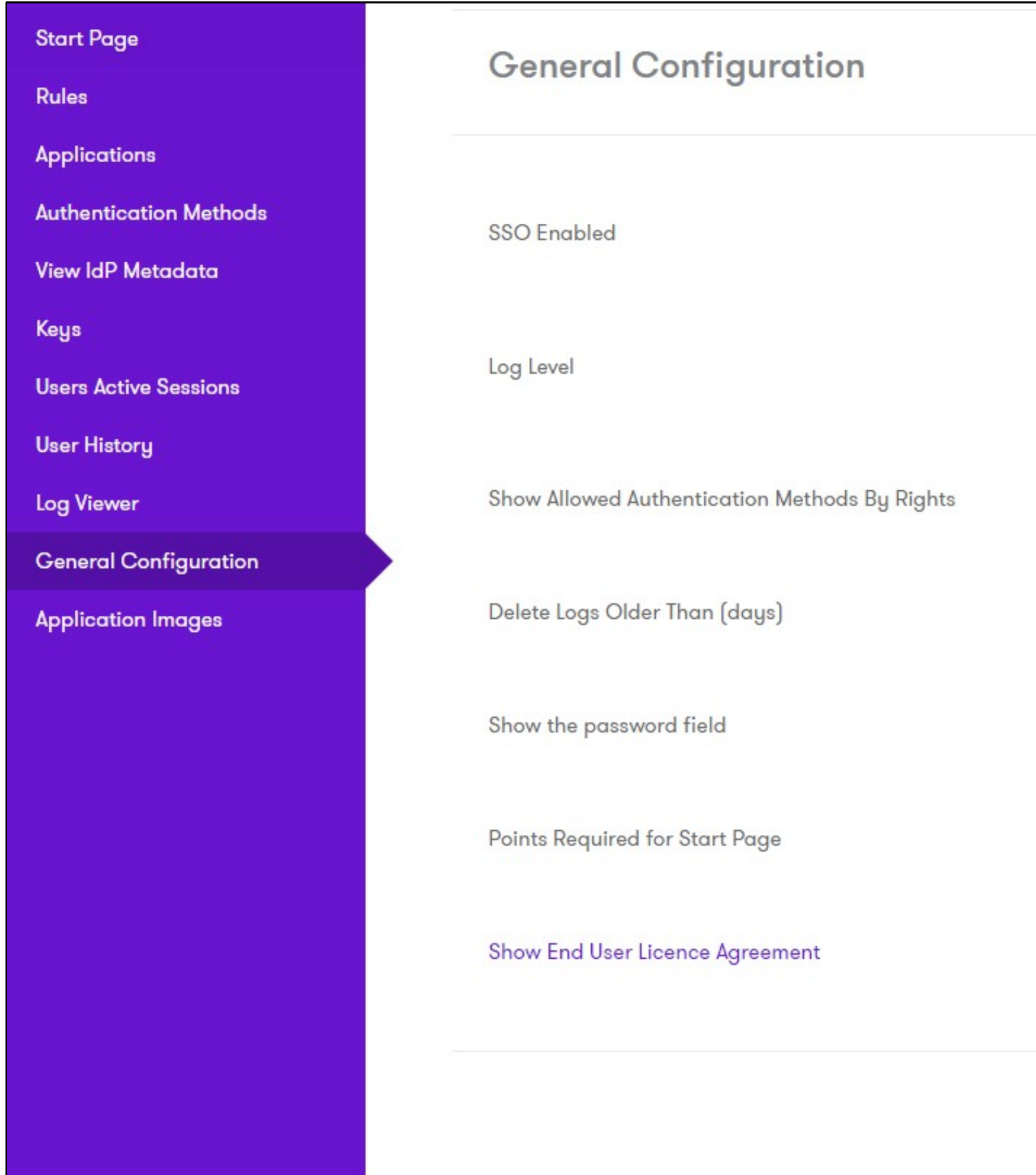
To enable single-sign-on select the SSO Enabled setting under General Configuration.

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

12 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.



The screenshot shows a web application interface with a purple sidebar on the left and a white main content area on the right. The sidebar contains the following navigation items: Start Page, Rules, Applications, Authentication Methods, View IdP Metadata, Keys, Users Active Sessions, User History, Log Viewer, General Configuration (highlighted with a white arrow), and Application Images. The main content area has the title 'General Configuration' and the following configuration options: SSO Enabled, Log Level, Show Allowed Authentication Methods By Rights, Delete Logs Older Than (days), Show the password field, Points Required for Start Page, and Show End User Licence Agreement.

Configuration Item	Value
SSO Enabled	SSO Enabled
Log Level	Log Level
Show Allowed Authentication Methods By Rights	Show Allowed Authentication Methods By Rights
Delete Logs Older Than (days)	Delete Logs Older Than (days)
Show the password field	Show the password field
Points Required for Start Page	Points Required for Start Page
Show End User Licence Agreement	Show End User Licence Agreement

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



Additionally, 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

Save

Back

13 General Operation and Diagnosis

13.1 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.

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

13.2 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.

Rules
Applications
Authentication Methods
View IdP Metadata
Keys
Users Active Sessions
User History
Log Viewer
General Configuration
Application Images

User History for admin

IP Address	Location	Points	Date
192.168.11.115		0	15:30
192.168.11.115		100	10:30
192.168.11.115		3553	16:30

Delete records

13.3 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 * * * * ?.

Rules

Applications

Authentication Methods

View IDP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

General Configuration

SSO Enabled



Log Level

TRACE

Show Allowed Authentication Methods By Rights



Delete Logs Older Than (days)

30

Show End User Licence Agreement

Save

14 Azure AD as a Data Source

15 Overview

This document describes how to use Azure AD as a Data Source.

16 Prerequisites

- Enable [Azure AD Domain Services](#).
- Enable [Secure LDAP](#).
- It is also necessary a connection between Swivel and Azure AD SLDAP

16.1 Implementation

You can follow the instructions on this article [here](#).

Please have a read in this instructions on this article [\[1\]](#) and also [\[2\]](#)

17 How To Configure OATH Mobile

17.1 Overview

OATH authentication allows a mobile device to be prompted a new OTC every 60 seconds without requiring the connection to AuthControl Sentry. Optionally, this can be changed to every 30 seconds for compatibility with Google and Microsoft Authenticators. See below for more details.

17.2 Prerequisites

Swivel AuthControl Sentry v4 onwards

Swivel Mobile Phone Client Version v4 for One Touch Mobile client based solution.

Swivel Server Details SSD for mobile client with OATH enabled.

17.3 Swivel core configuration

In order for a user to be able to use the mobile app as a OATH token they must be allocated the right to use the OATH mode of operation. This is done by ensuring that they are a member of a group that has this right.

Mobile client users must install the Swivel Mobile Phone Client from the app store.

17.4 Configuring OATH policy settings

On the Swivel Administration console select Policy -> Mobile App and ensure the below settings are configured:

Set **Mobile App OATH Mode** to Yes

Status

Log Viewer

▸ Server

▾ Policy

▸ General

▸ PIN and OTC

▸ Password

▸ Self-Reset

▸ Helpdesk

▸ Banned
Credentials

▸ Console Login

▸ Mobile App

▸ Reporting

▸
[policy_dualchannel]

▸ Logging

▸ Messaging

▸ Database

▸ Mode

▸ Repository

▸ RADIUS

▸ Migration

Policy / Mobile App ?

Set the polices to be downloaded to mobile app.

Allow user self-provision of
mobile app:

Yes ▾

Send provision code as
security string:

No ▾

Use long provision code:

No ▾

Use 30 second timestep for
OATH:

No ▾

Issuer for OATH token
label:

Enforce HTTP Header
Checking:

No ▾

Mobile App Local Mode:

No ▾

Mobile App OATH Mode:

No ▾

Base64 Encode Username
in provision URL:

No ▾

Other relevant options on this page are:

- Use 30 second timestep for OATH - if this is enabled, OATH codes are compatible with Google and Microsoft Authenticators. AuthControl Mobile Authenticator also supports this.
- Issuer for OATH token label - this only applies to 30-second OATH mode, and sets part of the label for authenticator display

Note that OATH mode (60 second timestep) is compatible with Push authentication provided that local mode is not also enabled.

17.4.1 Notes for 30 Second Mode

Note that if 30 second mode is enabled, provisioning can only be done using the QR code, in AuthControl Mobile Authenticator, Google Authenticator, Microsoft Authenticator or any other compatible authenticator app.

Please note that for 30 second mode, the URL placeholder needs to be url5, rather than url4. See the article on provisioning mobile apps for more details.

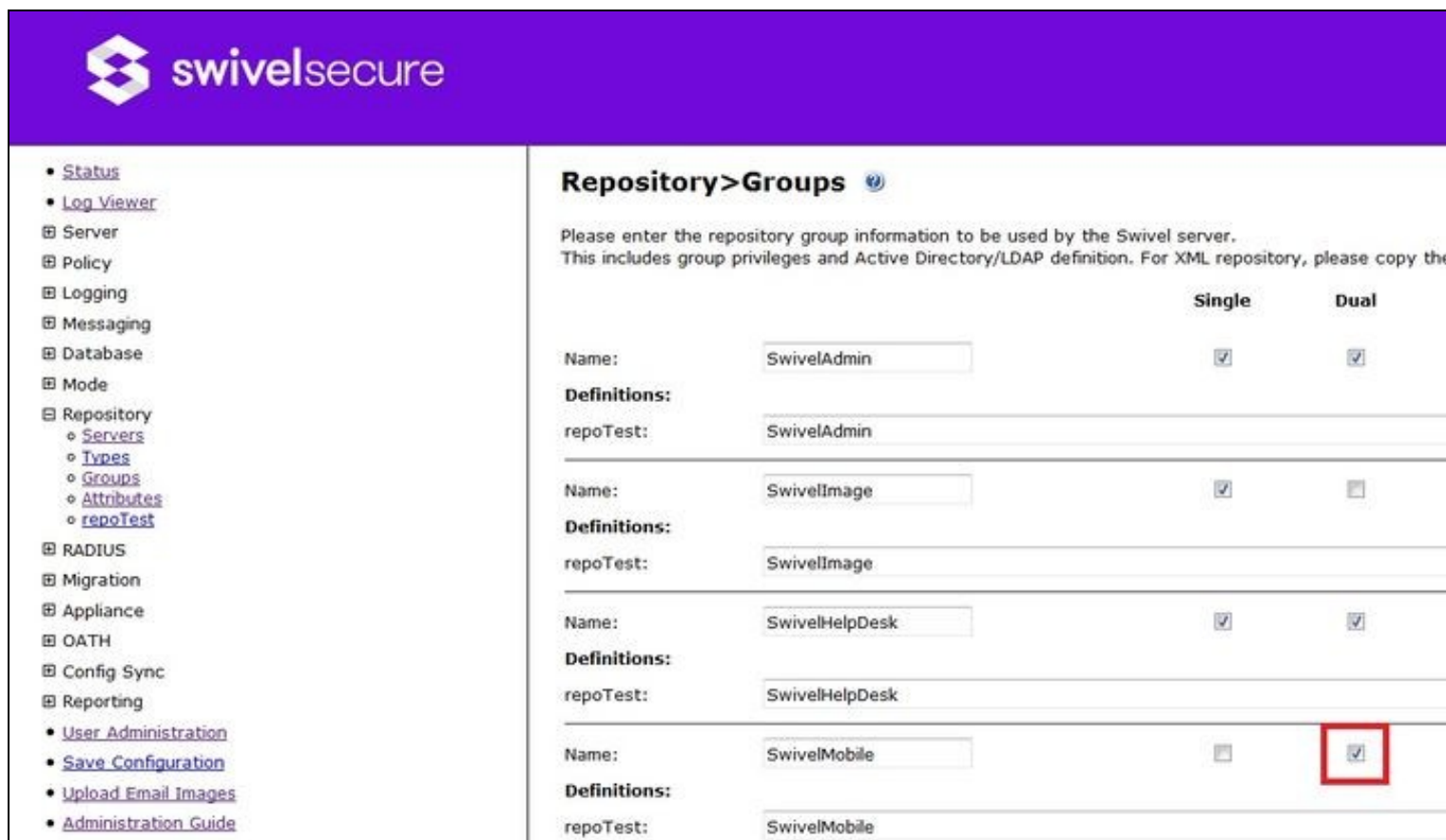
As 30-second timestep does not send any information back to Sentry, it is not compatible with Push authentication.

You can have both 30- and 60- second timestep tokens. Changing the setting only affects new tokens created after the change and does not change or invalidate tokens created before the change.

17.5 Define a group of Mobile OATH users

On the Swivel Administration console, select a group of users that will be using Mobile OATH authentication and ensure that the OATH box is ticked then click Apply.

OATH Mobile Users



The screenshot shows the SwivelSecure administration console. On the left is a navigation menu with options like Status, Log Viewer, Server, Policy, Logging, Messaging, Database, Mode, Repository (with sub-items Servers, Types, Groups, Attributes, repoTest), RADIUS, Migration, Appliance, OATH, Config Sync, Reporting, User Administration, Save Configuration, Upload Email Images, and Administration Guide. The main area is titled 'Repository > Groups'. It contains instructions: 'Please enter the repository group information to be used by the Swivel server. This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy the'. Below this is a table with columns for Name, Definitions, Single, and Dual. The table lists four groups: SwivelAdmin, SwivelImage, SwivelHelpDesk, and SwivelMobile. The 'SwivelMobile' group has its 'Dual' checkbox checked, which is highlighted by a red box.

Name:	Definitions:	Single	Dual
SwivelAdmin	SwivelAdmin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SwivelImage	SwivelImage	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SwivelHelpDesk	SwivelHelpDesk	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SwivelMobile	SwivelMobile	<input type="checkbox"/>	<input checked="" type="checkbox"/>

17.6 Testing

For testing OATH you can click App provision button on the user admin screen for the user that has been configured as a mobile OATH user and then provision the device with the URL or QR Code as explained:

Provision the device via URL. [Please read more on Provision URL page.](#)

Provision the device via QR code. [Please read more on QR Code page.](#)

17.7 Troubleshooting

Security code is showing instead of OATH Token

Please ensure that the SSD server for that Site ID has been configured as OATH and local mode is set to false. After changing the setting in SSD server, the users must be re-provisioned.

Check the Swivel logs for error messages

Error Messages:

CANNOT_CREATE_TOKEN for the <username> user does not belong to the OATH Group

This error can be seen where the button App Provision is clicked on the User Admin Console and the user does not have OATH permission. To solve that you need to add the OATH right to the group the user is member of.

OATH token does not allow the authentication.

When you click Provision App ensure that a token for that user has been created. For that you can go to the OATH/OATH Tokens screen and check that a new token has been created for that user.

- [Status](#)
- [Log Viewer](#)
- ▣ Server
- ▣ Policy
- ▣ Logging
- ▣ Messaging
- ▣ Database
- ▣ Mode
- ▣ Repository
- ▣ RADIUS
- ▣ Migration
- ▣ Appliance
- ▣ OATH
 - [OATH Policies](#)
 - [OATH Tokens](#)
 - [OATH Users](#)
- ▣ Config Sync
- ▣ Reporting
 - [User Administration](#)
 - [Save Configuration](#)
 - [Upload Email Images](#)
 - [Administration Guide](#)
 - [Logout](#)

OATH>OATH Users

Total number of users : 2

Users per page :

Search by username :

Search by serial ID :

Username	Allocated Token	
admin	..none..	<input type="button" value="Assign Token..."/>
Imorales	Imorales	<input type="button" value="Un-assign"/>

If the token has not been created, ensure that the policy Mobile App OATH Mode is set to Yes.

18 How To Configure Push Mobile

18.1 Overview

Push (or OneTouch) authentication allows a mobile device to be prompted by the Swivel server to let the user authenticate by pressing a confirm button on the mobile device screen, via a Swivel mobile application. You can see how that works on the following video:

18.2 Prerequisites

Swivel AuthControl Sentry v4 onwards

Swivel Mobile Phone Client Version v4 for One Touch Mobile client based solution.

Swivel Server Details SSD for mobile client with OneTouch enabled.

Swivel Server will need connection with Google and Apple servers: android.googleapis.com:443, fcm.googleapis.com:443, gateway.push.apple.com:2195, feedback.push.apple.com:2196

18.3 Swivel core configuration

In order for a user to receive the Push / OneTouch Mobile push message they must be allocated the right to use the OneTouch mode of operation. This is done by ensuring that they are a member of a group that has this right.

In addition they must be in a group associated with an Push / OneTouch transport. The transport must be the PNA (push notification authentication) Transport for Push / OneTouch Mobile client users.

Push / OneTouch Mobile client users must install the Swivel Mobile Phone Client from the app store. You can see how that works on the following videos:

18.4 Configuring Dual Channel settings

On the Swivel Administration console select Server/Dual Channel and ensure the below settings are configured:

Set **On-Demand Delivery** to Yes

Set **Allow message request by Username** to Yes

In Bound OTC Rule: Confirm key - enter the digits defined under Confirm Key to authenticate, example: if 1234 is entered then confirm by entering 1234 on the telephone keypad. OneTouch Mobile client solution currently only supports the confirm key mode of operation Confirmation key: (may be shown as [server_dualchannel_inboundconfirmkey]): The key(s) to be pressed to confirm authentication Call/Notification gap(s) (may be shown as [server_dualchannel_inboundcallgap]):

Domain Allowed to get OTC: Indicates the domain (e.g. <http://localhost:8080>, <http://domain>) authorized to get OTC. That is used by 2 way transport like Push Voice telephone or Push Mobile PNA (push notification authentication). The domain will correspond with the domain client (e.g. AuthControl Sentry, OnePushDemo, ...). If the value is * it will allow all the domains.

In Bound OTC Rule:	Confirm Key ▾
Confirmation key:	67890
Call/Notification gap (s):	10
In Bound SMS Timeout (ms):	500

18.5 Define a group of Push Users

On the Swivel Administration console, select a group of users that will be using Push authentication and ensure that the Push box is ticked then click Apply.

Push Mobile Users

Repository>Groups

Please enter the repository group information to be used by the Swivel server.

This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy

		Single	Dual
Name:	<input type="text" value="SwivelAdmin"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelAdmin"/>		
Name:	<input type="text" value="SwivelImage"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelImage"/>		
Name:	<input type="text" value="SwivelHelpDesk"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelHelpDesk"/>		
Name:	<input type="text" value="SwivelMobile"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelMobile"/>		
Name:	<input type="text" value="SwivelSMTP"/>	<input type="checkbox"/>	<input type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelSMTP"/>		
Name:	<input type="text" value="SwivelToken"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Definitions:			
repoTest:	<input type="text" value="SwivelToken"/>		

18.6 Define a Push Transport

On the Swivel Administration console, select or create a Push Transport

For OneTouch Mobile Client this will be the PNA (push notification authentication) Transport

Push Mobile Client Transport



Identifier:	<input type="text" value="PNA"/>
Class:	<input type="text" value="com.swiveltechnologies.pinsafe.server.transport.PNATransport"/>
Strings per message:	<input type="text" value="1"/>
Copy to alert transport:	<input type="button" value="No"/>
Destination attribute:	<input type="button" value="platformandpushid"/>
Strings Repository Group:	<input type="button" value="---NONE---"/>
Alert repository group:	<input type="button" value="---NONE---"/>
Push repository group:	<input type="button" value="SwivelMobile"/>

Configure Push Transports Configure a One Touch Mobile Client (PNA) Transport

The PNA (push notification authentication) Transport is preconfigured, no configuration changes are required unless requested by Swivel support

Timeout (ms): default 30000. Notification timeout. If the notification is pressed or arrives after the specified time, a message will be shown to the user to indicate that the Authentication Request has expired. 0 is no Timeout.

Notification title: Text displayed on the device notification.

Notification body: Text displayed on the authentication screen of the Swivel Mobile App.

iOS cert password: iOS certificate password which should correspond with the kind of certificate that is being used: production or development. The certificate used will depend of the attribute 'Production environment'.

BB URL: Push URL for BB10 Swivel Mobile App.

BB application id: BB10 Swivel Mobile App's identifier.

BB password: Push password for BB.

Android key: Key related with the Swivel Mobile app used.

Production environment: Indicates if the current environment is development or production. Depending of this value the certificate used to send the notification to the device will be the production one or the development one.

18.7 PNA configuration

Messaging>PNA

Please enter the details for the Push transport. Platforms supported: iOS, WP8, BB10, Android

Timeout (ms):	<input type="text" value="300000"/>
Notification title:	<input type="text" value="Authentication request received"/>
Notification body:	<input type="text" value="Do you want to continue with the authentication?"/>
iOS cert password:	<input type="password" value="....."/>
BB URL:	<input type="text" value="https://cp1253.pushapi.na.blackberry.com"/>
BB application id:	<input type="text" value="1253-8719a7580ri086467oooco209r60880oa86"/>
BB password:	<input type="password" value="....."/>
Android key:	<input type="text" value="AIzaSyAi-Kc1VQmQr7frgMeHWVqyg8RdWGc3Ow"/>
Production environment:	<input type="button" value="Yes"/> ▼

18.8 PNA V5 Configuration

Messaging>PNAV5 ?

Please enter the details for the Push transport. Platforms supported: iOS, WP8, BB10, Android

Timeout (ms):	<input type="text" value="300000"/>
Notification title:	<input type="text" value="Authentication request received"/>
Notification body:	<input type="text" value="Do you want to continue with the authentication?"/>
iOS cert password:	<input type="password" value="....."/>
BB URL:	<input type="text" value="https://cp1253.pushapi.na.blackberry.com"/>
BB application id:	<input type="text" value="1253-8719a7580ri086467oooco209r60880oa86"/>
BB password:	<input type="password" value="....."/>
Android key:	<input type="text" value="AIzaSyCWMrCle6zwXvpLWG-dxzzIwgklfiSCYUs"/>
Production environment:	<input type="button" value="No"/>

18.9 iOS Users

A renewal of the certificate might be due to happen from time to time as for now this is a non permanent certificate. Instructions and file: [APNS Push Certificates](#)

Bear in mind that v4 has an Update available but for internal database type we suggest that you either update the appliance and get the newer version (4.0.5) or if you decide to go for the manual option we strongly advise you to change from Internal to Appliance Database - there is a known bug when tomcat is restarted for v4.0.4 using the Internal database - check: https://kb.swivelsecure.com/w/index.php/Migrate_How_to_guide

18.10 Android Users

For AuthControl Mobile App v5 please ensure you create a PNA_V5 as Push Transport. Open it and replace the Android key by the following: AIzaSyCWMrCle6zwXvpLWG-dxzzIwgklfiSCYUs

18.11 Testing

For testing OneTouch you can use [AuthControl Sentry](#) adaptative authentication system or [RADIUS with OneTouch](#) enabled.

18.12 Troubleshooting

Check the Swivel logs for error messages

Error Messages:

Calling or sending notification to user "push" failed, error: The transport destination is empty.

This error can be seen where the user is authentication with the PNA and if the Mobile device has not been provisioned.

Authentication failure. Please Reprovision the device

The mobile device needs to be provisioned.

The authentication request expired

The authentication request took too long to reach the Mobile Client and is no longer valid. A large time difference between the mobile client and the Swivel server can cause this error. To increase the value, change the PNA Transport Timeout (ms): to a larger value or to 0 to prevent timeout.

PNA user id error

The wrong User is associated with the Provisioned mobile device. Provision with the correct user.

Calling or sending notification to user "gfield" failed, error: The transport destination is empty.

This can be caused where the SSD has a value of false for Push. To allow OneTouch Mobile this value needs to be true. To check this, verify on the Swivel Administration Console User Administration, View by Attributes to see platform and push id.

19 How To Provision Mobile Apps

19.1 Provisioning Mobile Apps

This article sets out how to set up your Swivel installation to provision the Swivel AuthControl Mobile App using the preferred Quick Provision Approach.

To be able to use quick provisioning you'll first need to contact Swivel Secure to enable this feature if it hasn't been enabled.

Please note that quick provisioning only works with SMTP transports. You cannot provision a mobile app with SMS.

19.2 How it works

The provisioning works in the following way.

1. User is sent a Provision Message
2. User accesses the provision url on their mobile (by clicking the link or scanning the QR code)
3. Mobile accesses the url, that takes the device to the Swivel Mobile Client Server
4. Mobile downloads the specific server settings required for that client
5. Mobile then uses those settings to access the Swivel Core Server to be provisioned

For this process to work the Swivel server needs to be allocated a Site ID and have a method of sending the required message to the user to be provisioned.

19.3 Site ID

When the mobile app is provisioned, it contacts the Swivel Mobile Configuration (SMC) server and presents its Site ID, and in return is given the server settings for that customer. To request a site ID you need to send a request to Swivel Support and include the following details:

- The public hostname/ip address of the Swivel server, along with the port number, context, and where the server is set to use SSL. A typical entry would be

```
Host:      swivel.company.com
Port:      8443
Context:   proxy
SSL:       true
```

You may also optionally state two other settings to define whether you wish the clients to work in Local Mode and if you want to use One Touch

```
One Touch: true
Local:      false
OATH:       false
```

Swivel support will inform you of your Site ID and this needs to be entered on the Site ID field on the Server - Name screen.

Server>Name

Please enter the name by which this Swivel server should be known.

Site ID:

Server Name:

19.4 Provision URLs

The URLs that will be used to contact the Swivel SMC server are set under Policy -> Self Reset.

URL provisioning:	https://smc.swivelsecure.net/smc/provision/
URL to get settings:	https://smc.swivelsecure.net/smc/getsettings/
URL complete:	https://smc.swivelsecure.net/smc/complete/
QR Code URL:	https://smc.swivelsecure.net/smc/qrcode?text=

19.5 Quick Provision Link

If the user can access their email on their mobile device they can be sent an email that contains a url that will instigate the provision process. Alternatively this url can be sent as a Text Message.

To use this method of provisioning you need to ensure that on the Messaging configuration screen, eg Messaging -> SMTP, the following text is included:

To automatically provision your device, click the following URL: %URL_COMPLETE%SITE_ID/%NAME/%CODE

When the message is sent to the user the %URL_COMPLETE%SITE_ID/%NAME/%CODE will be replaced by the SMC url, the site-id, the user's username and the user's provision code.

19.6 QR Code

The other option is for the provision message to include a QR code that the user can scan from their Swivel Mobile App in order to start the provision process.

The Swivel User Portal includes an application that will display the QR code relevant to the provision message. This needs to be available via the internet so that the provision message can include a link to it. For example if your userportal is deployed as <https://portal.domain.com:8443/userportal>, then the QR code should be available from <https://portal.domain.com:8443/userportal/getQRCode?text=>

To use this approach the provision message must be in html format include text along the lines of

Click here to view QR Code: url4

When this message is sent to the user, url4 is replaced by the html required to pull in the image.

19.6.1 Note for 30-second timestep

If you select 30-second timestep mode, you must change the placeholder to url5. The default provision template contains url4, so make sure you look for that and change it. You should also remove the provision link, as it is not compatible with 30-second timestep mode.

19.7 Policies

There are a number of policies you can set around the provision and use of the Swivel Mobile App.

19.7.1 Provision Policies

These policy settings define how the provision process operates and are on the Policy -> Self Reset page

Allow user self-provision of mobile client:	<input type="button" value="Yes"/> ▼
Send provision code as security string:	<input type="button" value="No"/> ▼
Log device information when provisioning:	<input type="button" value="Yes"/> ▼
Provision Code Validity period (seconds):	<input type="text" value="360000"/>

Allow user self-provision of mobile client

If set to yes the user can, at any time, request a new provision code via the user portal. If set to no then once a user has provisioned a mobile device, the only way to provision a new device is via the admin console.

Send provision code as security string

If this is set to No, then the provision message will be sent to the same destination as all other alert messages, usually an email address. If this is set to yes then the provision message will be sent to the same destination as their security strings, usually a mobile phone number. This option allows the system administrator to ensure that provision messages are only sent to the users registered mobile device

Log device information when provisioning

If set to yes, any http headers parameters sent by the mobile device will be logged against that user's device. If a mobile client attempts to download security strings and presents a different set of headers to that that was logged when the device was provisioned, the request will fail

Provision Code Validity period (seconds)

19.7.2 Usage Policies

When a mobile client is provisioned it downloads a set of policies from the Swivel Server. These policies are set on the Policy->Mobile Client screen

Policy>Mobile Client

Set the polices to be downloaded to mobile clients

Allow user to enter PIN:	Yes ▾
Allow user to choose how to extract OTC:	Yes ▾
Allow user to browse strings:	No ▾
Provision is numeric:	No ▾
Show Settings:	No ▾
Sync Index:	No ▾
Support Email Address:	support@domain.com
Support Phone Number:	+44 1234 5678
VPN URL Scheme:	

ApplyReset

These policies are

Allow user to enter PIN

If the user has a PIN they can enter that PIN into the mobile client and it will extract the associated one-time code. If this policy is set to Npo, the user will be shown the security string and the user will have to perform the one-time extraction mentally.

Allow user to choose how to extract OTC

If the user is allowed to enter their PIN, if this policy is set to yes, the user can opt to disable PIN entry

Allow user to browse strings

The mobile client will work sequentially through the security strings that it has downloaded, however if this policy is enabled the user can browse through strings, eg skip strings. This maybe required where the user has to use a specific string in order to authenticate (eg for MSCHAP authentication)

Provision is numeric

Should the user need to enter their provision code manually, by setting this you yes the mobile client will display a numeric only keypad on the provision code entry screen

Show Settings

If Quick Provision is being used, there should be no reason for a user to be able to view their settings. However this policy enables the user to see these settings

Sync Index

Some RADIUS protocols work in such a way that only a specific security string can be used to authenticate. Syncing the index means the Swivel Mobile Client will always use the security string that the server is expecting. To Read more about Sync please go [here](#)

Support Email Address, Support Phone Number

These support details will be shown to the user when they access the help screen on the mobile client

VPN URL Scheme

Certain versions of the mobile client may support the launching of a VPN client. This setting defines the format used to enable this

19.8 Troubleshooting

A key question when diagnosing provisioning issues is to determine if the Swivel Client is contacting the Swivel server or not. If there are no log entries in the Swivel logs when the provision fails, it implies the error is a configuration or network issue prior to this stage in the process/

User clicks the link or scans the QR Code and nothing happens This implies the settings for the SMC server are not correct

User sees the initial config screen then provision fails with connection error Check site is set and site id settings are correct Check that the urls are accessible. To test this you can paste

`http(s)://<site id settings>/AgentXML?xml=?xml version="1.0" ?><SASRequest><Version>3.6</Version><Action>ping</Action></SASRequest>`

Where site id settings represents the server, port and context set for your server ID

You should see a response

```
<?xml version="1.0" encoding="UTF-8"?>
<SASResponse>
<Version>3.6</Version>
<RequestID/>
<Result>PASS</Result>
</SASResponse>
```

Check the validity of the certificate and also check that there are no issues in relation to weak ciphers or encryption standards

Invalid Provision Code If the user gets an invalid provision code check when the code was sent and how long the validity of the code is sent to. If this is an HA pair, need to ensure that the same appliance that issue the provision code also received the provision request from the mobile or that Session Synchronisation has been enabled/

20 Licence key

20.1 Swivel Licence Keys

Since Version 3.11 the Swivel Licence keys work in a difference way. They differ from previous licence keys in the following ways.

- The licence is issued to a specific installation and therefore cannot be transferred from one server/installation to another
- The licence key is used to contact the Swivel Licence Key server to download details of the entitlements the customer has purchasded. This means when a customer wants to upgrade or renew their licence, they do not need to enter a new licence key, merely refresh the licence key they are given. See [License Key Update](#).

When an organisation become a Swivel customer they are allocated a Site ID. This uniquely identifies their installations and is used as part of the mobile device provisioning process and can also be quoted on support tickets etc.

It is also used as part of the key for encrypting licence keys, therefore licences will be issued for specific Site IDs. If, at the time of purchase, an organisation does not have a licence key, one will be allocated to them.

20.2 Entering Licence Keys

The licence information is sent in a document that contains both the **Site ID** and the **Licence Key**.

First you need to ensure that the Site ID has been set correctly. To do this go to the the Server->Name section and check that the site-id matches that on the licence document. If not then enter the Site-id procived and click apply.

Server>Name

Please enter the name by which this Swivel server should be known.

Site ID:

Server Name:

Then go to the Server -> Licence screen and ensure that on-line is set to yes and then enter the Licence Key into the Licence Key field.

Server>License



Please enter your Swivel license key below.

License key:

License information:

Online:

Then click apply

Server>License


Licence for 200 users. Started 03-Jan-2016, expires 03-Jan-2017.

Please enter your Swivel license key below.

License key:

License information:

Online:

The appliance will need access to the internet and to DNS to download the licence key information

You will see a message listing the licences associated with the licence key and the Licence Details will be populated.

20.2.1 Off Line Licence Key Entry

If, for any reason, it is not possible to allow the Appliance to contact the Swivel Licence Server then it is possible to set the On-Line mode to Off. In this case, the licence information needs to be entered manually. You can retrieve your current licence information from a browser, using the following URL:

<https://ssd.swivelsecure.net/slksext/licence/my-licence-key>

Replacing "my-licence-key" with your actual license key.

20.3 Updating Licence Information

With older versions of the software (prior to 3.11), requesting more users required a new licence key. With the new system, the licence key remains the same, but the license information changes.

20.3.1 Updating Licence Information Online

When you update your licence, it is not automatically updated in the appliance. However, if the appliance is online, all you need to do is to go back to the Server -> Licence page and click Apply for the latest licence information to be downloaded.

20.3.2 Updating Licence Information Offline

If your appliance is not able to connect to the internet, then you must retrieve your new licence information and replace it in the Server -> Licence page. Use the same URL as above:

<https://ssd.swivelsecure.net/slksext/licence/my-licence-key>

Replacing "my-licence-key" with your actual license key.

21 Mobile App Privacy Policy

22 Notes

This document refers to requisites of Authcontrol Mobile App.

23 Privacy Policy

Swivel Secure's mobile app requires access to:

- The Camera app to allow scanning of QR codes in our provisioning messages to ensure easy user provisioning.
- The Storage to save the information required to communicate with your AuthControl Sentry system and the storage of the security strings, that are downloaded as part of the provisioning process, allowing authentications even when no mobile phone signal is present.
- The Phone app to allow users to directly call their helpdesk from within the application for support and assistance.
- Your Email app to contact your company's helpdesk via email for support and assistance.

No other information is accessed, copied, collected or stored either within the app, on the phone or anywhere else.

24 Need more help?

Please contact your partner or create a support ticket in our support portal <https://supportdesk.swivelsecure.com/dashboard>

25 MobileIron Integration

AuthControl Sentry/Cloud to MobileIron
Integration Notes

26 Overview

Swivel Secure can provide strong and two factor authentication to the Mobile Iron. AuthControl Sentry is a linux based IdP for SAML federations. It is provided as on-prem or Cloud SaaS flavours, providing an adaptative authentication multifactor, managed by a system of points, depending on the factor used and the target app to access. This document outlines the details required to carry this out.

27 Prerequisites

Working MobileIron (MobileIron Sentry appliance) MobileIron Core 9.X and Connector 9.X AuthControl Sentry 4.x

28 How does it work

At App level we use conditional access to Cloud SaaS federated with SAMLv2. The Federated Identity works in 3-way trust with Access between Identity Provider (IDP), Service Provider (SP) and the Access provided by MobileIron AdminPortal/Access Gateway.

29 SwivelSecure Configuration

29.1 Enabling Standard Federation - Sales Force

The standard federation involves just this 3 fields:

- Portal URL: (this Endpoint URL can be found on the Setup -> Security Controls -> Single Sign-On

Settings page in Salesforce.com, listed as ?Salesforce Login URL? under the Endpoints section. It is unique to your Salesforce.com instance and domain.

- Entity ID:; Reflected on Salesforce SSO configuration for My Domain
- Federeated id: That needs to match with the attributed defined on Salesforce.com and Swivel

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application

i

Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) SAML (Security Assertion Markup Language) request.

Name

Salesforce

Image

Salesforce.png

Points

0

Portal URL

https://yourdomain.salesforce.com?

Endpoint URL

Entity ID

https://saml.sentry.salesforce.com

Federated Id

email

Once that we have a working federation from AuthControl Sentry and the SP, (in the example we will use Salesforce), this is just a standard Salesforce and Custom IdP federation on MI Access console, as the MFA part from Swivel will be triggered once the MI Access has approved the connection. AuthControl Sentry provides a metadata url to quickly get the XML from IdP. It uses POST method for federation.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images


Swivel + Salesforce

Demo

No description

Policy Name: Default Policy

SAML Customization of Mobile Iron settings, Portal URL, Entity ID and Federated ID:

Name	SalesForce secured by MI Access
Image	Salesforce secured.png 
Points	100
Portal URL	https://milabses-dev-ed.my.salesforce.com?so=00D0Y000001ktKL
Endpoint URL	
Entity ID	https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943
Federated Id	email

SAML Customization in the Sales Force Side. Settings for Mobile Iron.

SAML Single Sign-On Settings

[Back to Single Sign-On Settings](#)

[Edit](#) [Delete](#) [Clone](#) [Download Metadata](#) [SAML](#)

Name	SwivelAccess
SAML Version	2.0
Issuer	https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943-e816bccc2905/idp
Identity Provider Certificate	C=US, ST=California, L=Mountain View, O=MobileIron, OU=Support, CN=Signing Expiration: 12 Jul 2047 08:45:42 GMT
Request Signing Certificate	SelfSignedCert_12Jun2017_174925
Request Signature Method	RSA-SHA256
Assertion Decryption Certificate	Assertion not encrypted
SAML Identity Type	Username
SAML Identity Location	Subject
Service Provider Initiated Request Binding	HTTP POST
Identity Provider Login URL	https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943-e816bccc2905
Identity Provider Logout URL	https://ssauth.mi-labs.es:8443/sentry/singlelogout
Custom Error URL	

Just-in-time User Provisioning

User Provisioning Enabled ☐

Endpoints

Salesforce Login URL	https://milabses-dev-ed.my.salesforce.com?so=00D0Y000001ktKL
OAuth 2.0 Token Endpoint	https://milabses-dev-ed.my.salesforce.com/services/oauth2/token?so=00D0Y0000

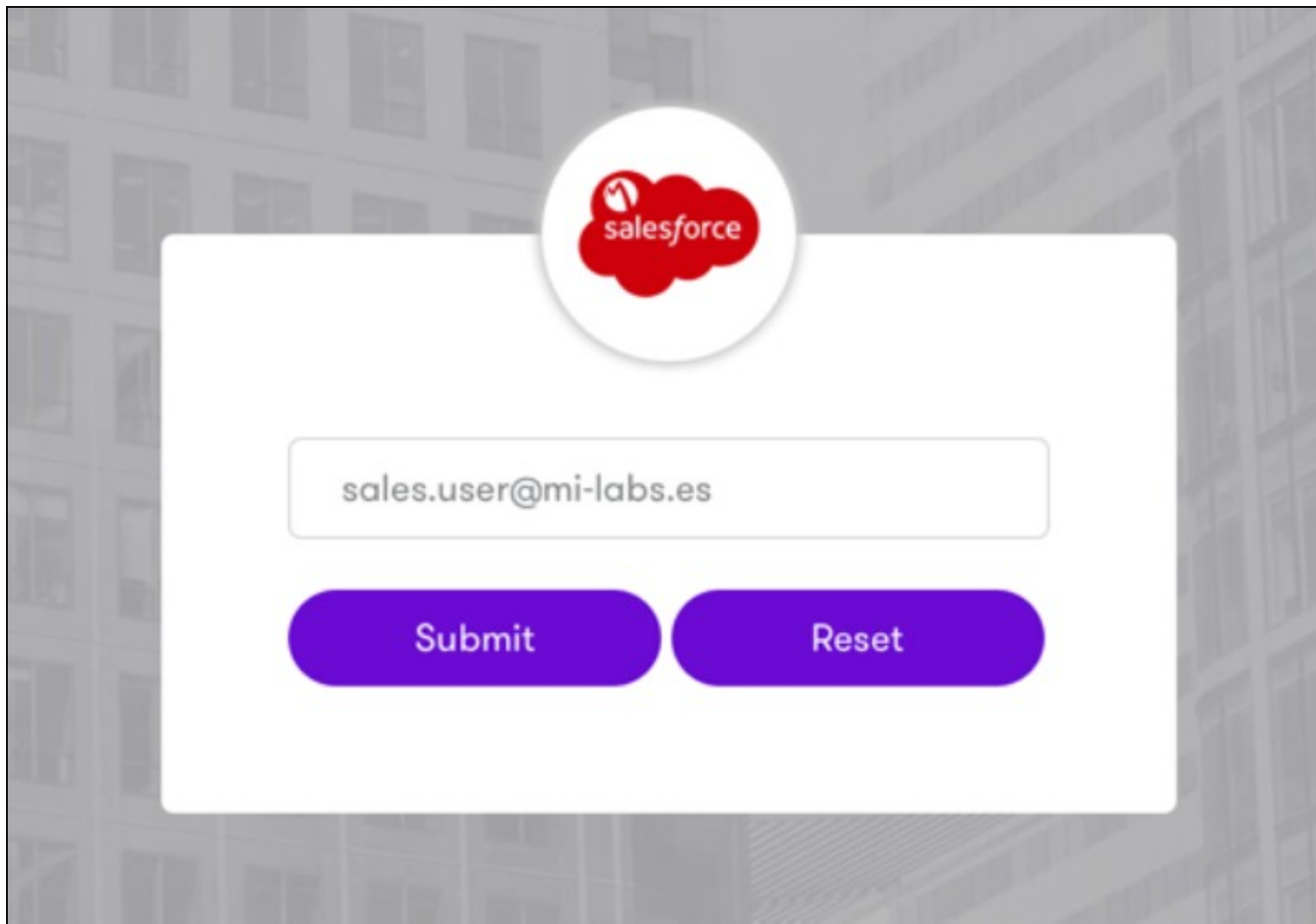
[Edit](#) [Delete](#) [Clone](#) [Download Metadata](#) [SAML](#)

After the application settings definitions have been applied the applications are available in AuthControl Sentry's web portal.

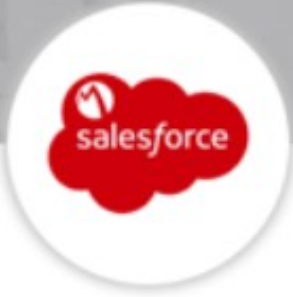


SalesForce secured by MI Access

User Login in Authcontrol Sentry with SalesForce using the MI Account




SSO for Salesforce using Mobile Iron and Turing image from SwivelSecure. This means that the user logs in using the Swivel Secure credentials, by the selected method (in this case Turing image) into the Sales Force (without the need of using Sales Force Credentials).



sales.user@mi-labs.es

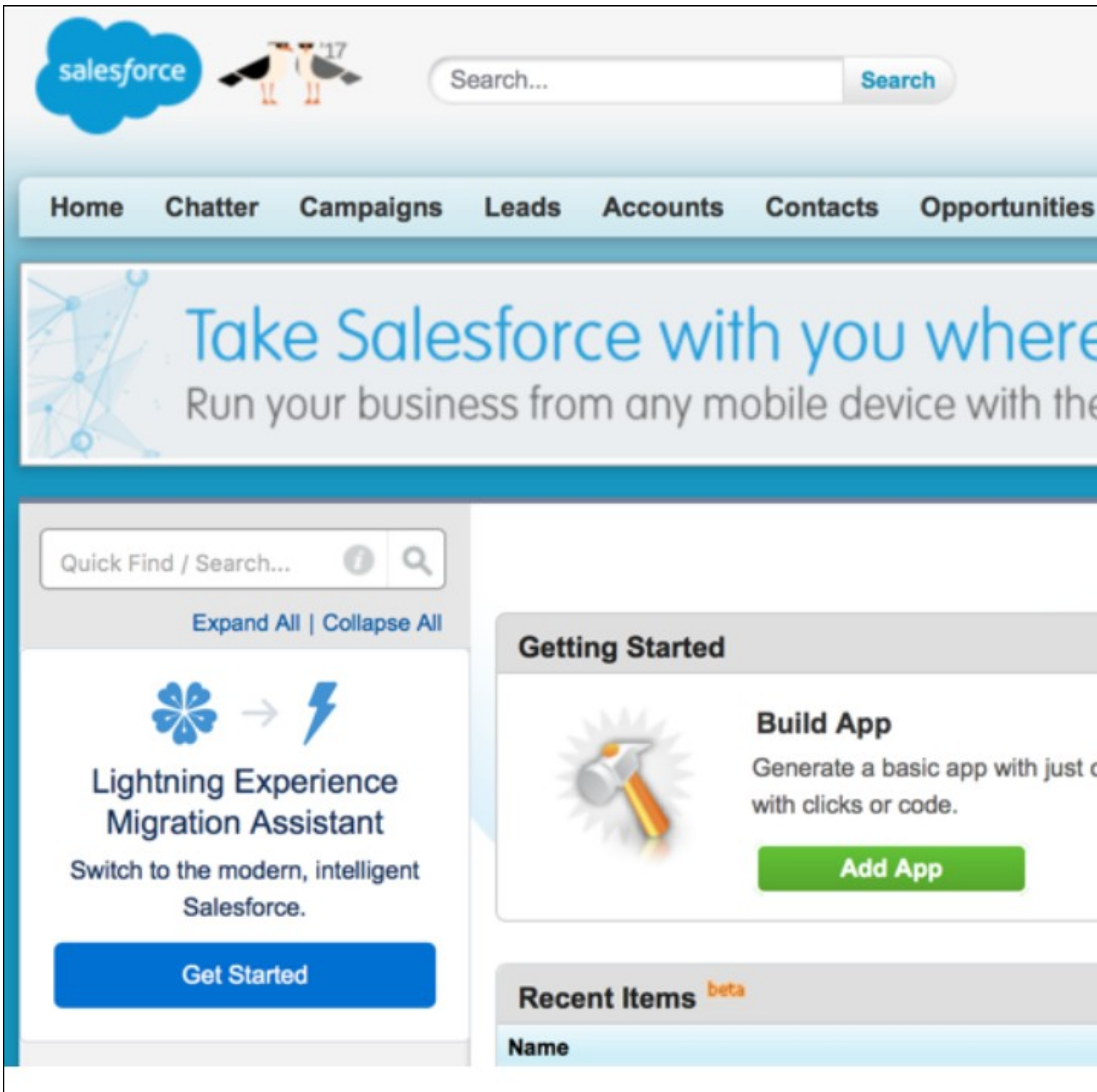
Password

10TC 

1	2	3	4	5	6	7	8	9	0
0	3	1	9	8	4	2	7	5	6

Login Refresh Image

Successfull login in Sales Force.



29.2 Enabling Standard Federation - Office 365

In the case of Office365, AuthControl requires that the main federation must be performed with ADFS. On a working federation, a complement has to be installed on ADFS 3.0 server.

Swivel Authentication Provider Configuration

Settings Languages Logging Advanced

Swivel URL: :// : /

☒ Allow self-signed certificates

Agent Secret:

Confirm Secret:

☐ Allow non-PINsafe users

☐ Ignore domain prefix

☐ Ignore domain suffix

Image Type: ☒ Auto-show Image

Image Source:

Turing URL:

Pinpad URL:

OK Cancel Save

Swivel ADFS Authentication Provider, version 1.0.6.2, Copyright © Swivel Secure Ltd 2015

There's a couple of choices depending if the customer is using ADFS Proxy servers or not.

This plugin installs Swivel Secure product as an MFA to be applied via ADFS Authentication Policy Settings.

Set AuthControl Sentry / Swivel Secure as Authentication Provider

Edit Global Authentication Policy

Primary

Multi-factor

Configure multi-factor authentication (MFA) settings.

Users/Groups

MFA is required for the following users and groups:

ES\Swivel-User-Group

Add...
Remove

Devices

MFA is required for the following devices:

☒ Unregistered devices

☒ Registered devices

Locations

MFA is required when accessing applications from the following locations:

☒ Extranet

☒ Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

☐ Certificate Authentication

☒ Swivel Authentication Provider

What is multi-factor authentication?

OK

Cancel

Apply

On AuthControl Sentry side, we will create an Application configuration with MI Access, IdP and Office365 endpoints:

87



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.

Name

Office365 secured by MI Access

Image

O365.png



Points

100

Portal URL

<https://login.microsoftonline.com/login.srf>

Endpoint URL

<https://access.mi-labs.es/MobileIron/acc/9b7ea0b6-e908-4111-8eb1-94c>

Entity ID

<https://access.mi-labs.es/MobileIron/acc/9b7ea0b6-e908-4111-8eb1-94c>

Federated Id

userPrincipalName

This way, ADFS will require PINPAD or Turing image in order to validate and access Office365, in addition to ADFS primary authentication policy.

MI LABS ES Login

Welcome ES\office.user

For security reasons, we require additional information to verify your account

OTC:

1	2	3	4	5	6	7	8	9	0
8	5	1	6	9	3	7	2	0	4

refresh

Continue

30 Related Articles

- ADFS configuration

https://kb.swivelsecure.com/w/index.php/Microsoft_ADFS_3_Authentication

31 Additional Information

For assistance in the Swivel Secure installation and configuration please firstly contact your reseller and then email Swivel Secure support at supportdesk@swivelsecure.com

32 OATH Seed Conversion

32.1 Introduction

This article explains how to convert the OATH Hard Token seeds from Base16 Hexadecimal to Base 32. This can provide ultimate flexibility for your Hardware token investment, if you intend to import the OATH tokens to other systems in conjunction with using them on the Swivel Secure platform.

32.2 Pre-requisites

- Swivel Secure OATH Token seeds in their original distribution format (*.txt file and fields separated by space)
- Some ability to use Python scripts
- Python version 3.7.3
- Python IDLE
- Microsoft Excel or Notepad for CSV file formatting and preparation

32.3 Python Script

```
import base64
import codecs
import csv

with open('C:\\Users\\admin\\Desktop\\seeds.txt','rt') as input, open('C:\\Users\\admin\\Desktop\\seeds32.txt','w') as output:

    csvin = csv.reader(input, delimiter=' ')
    csvout = csv.writer(output, delimiter=',')

    for row in csvin:
        hex = row[1]
        b32 = base64.b32encode(codecs.decode(hex, 'hex'))
        b32decoded = b32.decode("utf-8")
        csvout.writerow([row[0]] + [b32decoded])
```

32.4 Microsoft MFA Seed File Formatting Requirements

Note: If you want a stronger authentication solution, consider deploying [Sentry SSO with Office 365](#) to take advantage of [Authcontrol v4 Sentry SSO and Adaptive Authentication](#), with Single Sign On to your other corporate applications - instead of using Microsoft MFA.

Prepare a CSV file in the following format:

```
upn,serial number,secret key,timeinterval,manufacturer,model
```

e.g.

```
daniel.croft@swivelcloud.net,2000123456789,QFA56K3C5CGFDQWCJCDJNNJHGXYD2DDC,60,SwivelSecure,TOTP
```

Note that timeinterval should be 60 and that manufacturer and model are just arbitrary text and can be anything.

Import your seed file into Azure AD under **Azure Portal > Azure Active Directory > MFA Server > OATH tokens**. With the seeds converted to Base 32 using the above Python script you should then be able to successfully activate and use the tokens.

33 Pinsafe

33.1 PINsafe

PINsafe is the former name of the Swivel Secure core authentication platform. As from version 4, it is known as **Sentry**. Specifically, we refer to **Sentry Core** where we need to distinguish the core authentication engine from the adaptive authentication and single-sign-on engine, **Sentry SSO**.

You can find a reference guide to the [Sentry Core Administration Console](#) [here](#).

34 Sentry

Sentry is the new context for Swivel Secure appliances. Before it used to be Pinsafe for v2 and v3 appliances.

35 Sentry SSO with ADFS

36 Configuring ADFS Support for Sentry

36.1 Introduction

This article describes how to configure an ADFS server to use Sentry to replace the standard Active Directory authentication. This allows a suitably configured environment to support Swivel authentication for Office 365, for example.

36.2 Requirements

ADFS integration requires version 4.x of Sentry.

36.3 Configuration Procedure

36.3.1 In Swivel Core

ADFS requires the username to be in the format domain\username. To do this, you need to create a Swivel attribute that includes the prefix.

In the Swivel admin console, under the repository details for the relevant AD repository, set the domain qualifier to be the short-form domain name, followed by "\" - don't forget the backslash at the end.

- [Status](#)
- [Log Viewer](#)
- ⊞ Server
- ⊞ Policy
- ⊞ Logging
- ⊞ Transport
- ⊞ Database
- ⊞ Mode
- ⊞ Repository
 - [Servers](#)
 - [Types](#)
 - [Groups](#)
 - [Attributes](#)
 - [Repos Admin](#)
 - [AD](#)
- ⊞ RADIUS
- ⊞ Migration
- ⊞ Windows GINA
- ⊞ Appliance
- ⊞ OATH
- ⊞ Config Sync
- ⊞ Reporting
- [User Administration](#)
- [Save Configuration](#)
- [Administration Guide](#)
- [Logout](#)

Repository>AD

Please enter the details for accessing Active Directory

Hostname/IP:

Username:

Password:

Port:

Allow self-signed certificates:

Synchronization schedule:

Username attribute:

Mark missing users as deleted:

Initial PIN attribute:

Initial password attribute:

Import disabled users:

Import disabled state:

Ignore FQ name changes:

Reformat Phone Number:

Prefix to remove:

Prefix to add:

Add domain qualifier:

Repository Domain Qualifier:

Allow expired passwords:

Under Repository -> Attributes, create an attribute - for example, call it "windowsaccountname". In the definition for the AD repository, put the AD attribute name "sAMAccountName", and under domain qualifier, select "As Prefix".

Name:	<input type="text" value="windowsusername"/>
Phone Number?	<input type="text" value="No"/>
Add repository qualifier?	<input type="text" value="As Prefix"/>
Sync Rule	<input type="text" value="Synchronised"/>
Attribute:	<input type="button" value="Delete"/>
Repos_Admin:	<input type="text"/>
AD:	<input type="text" value="sAMAccountName"/>

Finally, synchronise the AD repository, to ensure that all users have an attribute in the form domain\username.

36.3.2 In Swivel Sentry

36.3.2.1 Edit settings.properties

NOTE: this step is not usually necessary when using version 4.0.3 or later: the correct settings are chosen automatically for ADFS, and can be overridden in the configuration anyway. This assumes that you have added a domain prefix to the repository, and have created an attribute that uses it.

This file is located under /home/swivel/.swivel/sentry on an appliance. Check the following entries:

- certificateIssuer ? this must be in the form of a valid URI. It is recommended that you use the public URL of Sentry, but it doesn't have to be a real web location.
- windowsaccountnamefield=username. This configures the Swivel attribute field to be used to import the username for ADFS. If you have configured a prefixed attribute above, use the name of that attribute. Otherwise, use an attribute mapped to sAMAccountName without a prefix, and set the prefix below. This latter option is the only possibility for Swivel version 3.10.5 or earlier.
- windowsdomainprefix=domain. This configures the domain name to be prefixed to the ADFS username. If the attribute above already has a prefix, this should be blank. If not, make sure the \? is included. Do not set a prefix if your attribute is already prefixed.

36.3.2.2 Application settings

In the Sentry admin console, create a new application with the following settings:

- Service Provider = ADFS
- Endpoint URL = https://<ADFS_HOST>/adfs/ls/
- Entity ID = http://<ADFS_HOST>/adfs/services/trust

Replace <ADFS_HOST> with the public host name of your ADFS server / proxy. Other than that, the format should not be changed: Endpoint URL should have a / on the end, Entity ID should not. Also, note that Entity ID starts with "http", **NOT** "https".

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS is configured to use SAML (Security Assertion Markup Language) n

Name

ADFS

Image

ADFS.png

Points

0

Portal URL

https://<ADFS_HOST>/ad

Endpoint URL

https://<ADFS_HOST>/ad

Entity ID

http://<ADFS_HOST>/ad

Federated Id

windowsusername

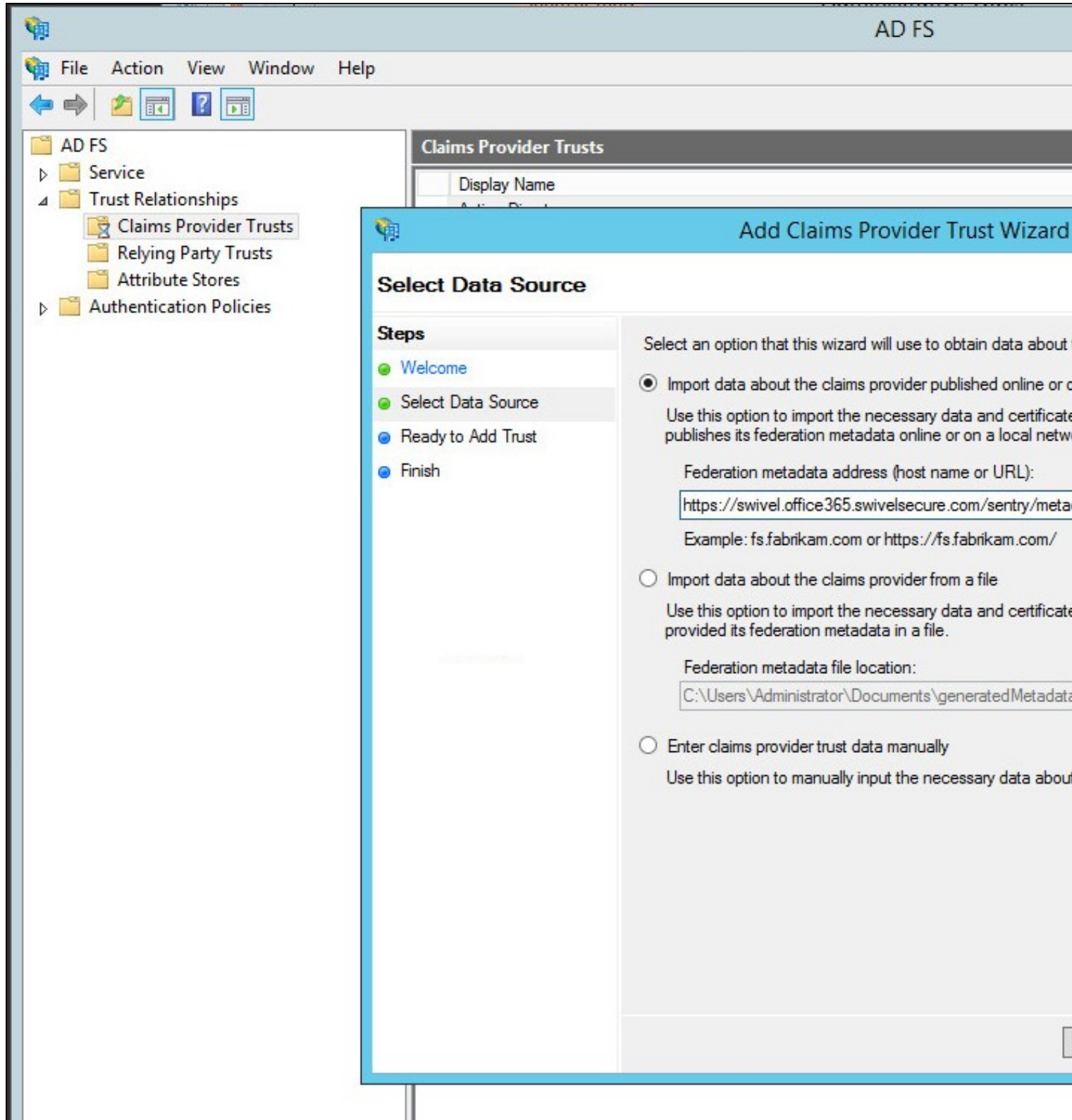
36.3.2.3 Certificates

Ensure that you generate a certificate for Sentry that is current.

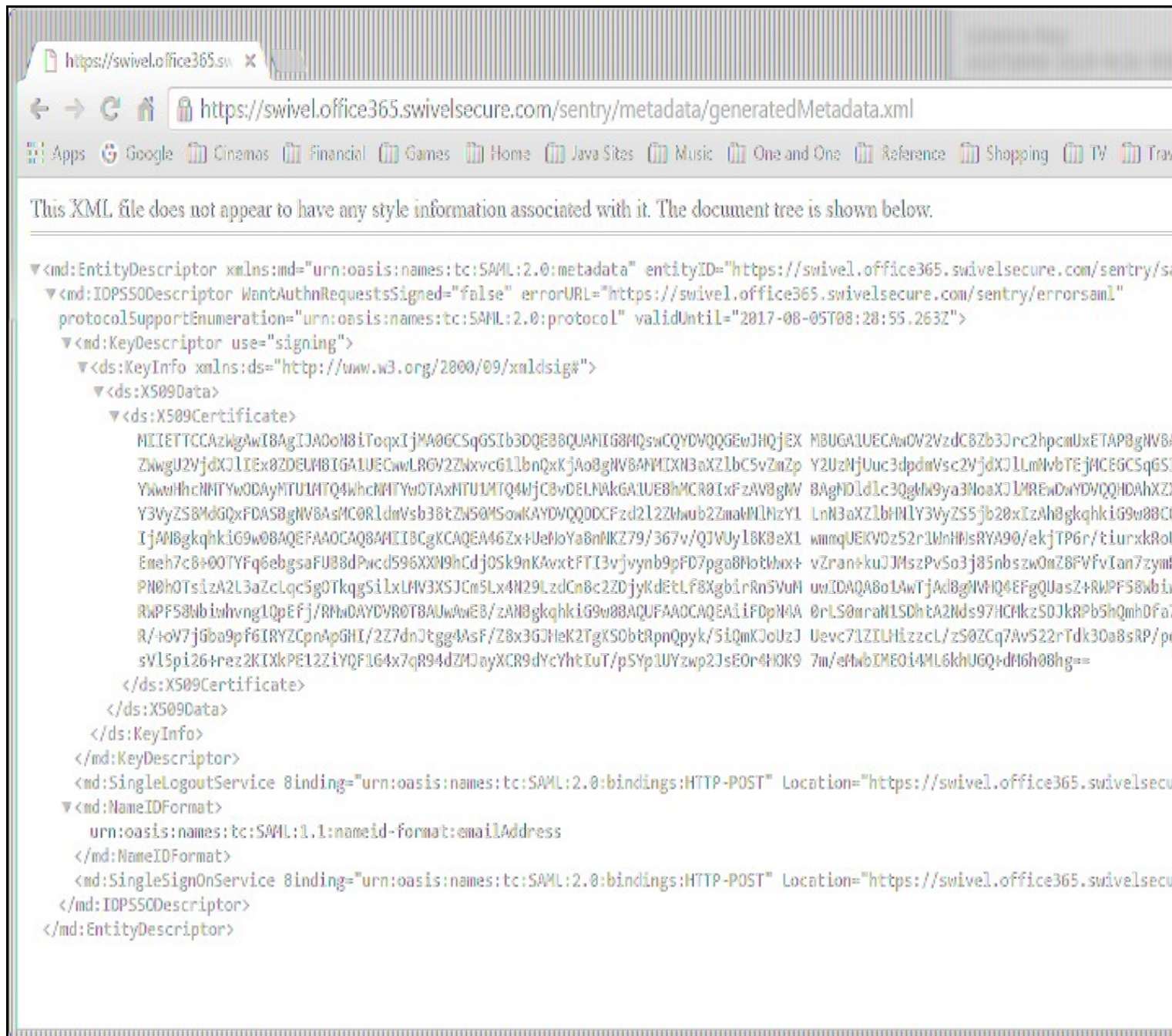
36.3.2.4 In ADFS Management

36.3.2.4.1 Claims Provider Trust

Create a new Claims provider trust.



If you can import the metadata directly from the Sentry URL: that is simplest, but it may not work, due to SSL handshaking issues. In which case, download the metadata to a file

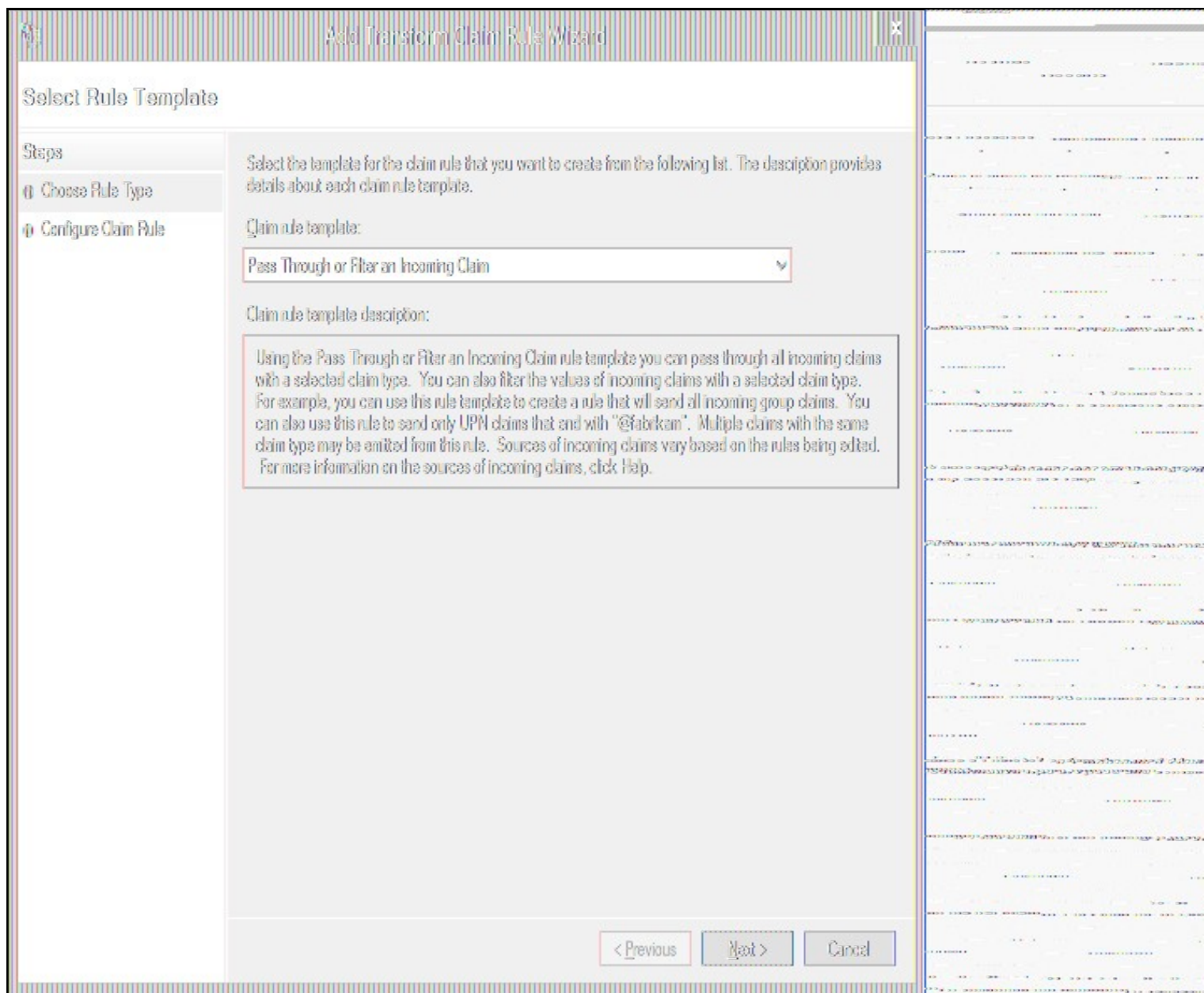


and import the settings from that file.

Once you have created the new trust, you will be given the opportunity to add claim rules:

Claim Rules:

Create two rules using the template ?Pass Through or Filter an Incoming Claim?, as follows:



- Incoming claim type = Name ID: it is recommended that you specify the format as Email, and only pass through claims matching your domain suffix.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- 1 Choose Rule Type
- 2 **Configure Claim Rule**

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name:

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type:

Incoming name ID format:

☐ Pass through all claim values
☐ Pass through only a specific claim value

Incoming claim value:

☒ Pass through only claim values that match a specific email suffix value:

Email suffix value:

Example: fabrikam.com

☐ Pass through only claim values that start with a specific value:

Starts with:

Example: FABRIKAM\

- Incoming claim type = Windows Account Name. There is no need to specify any other restrictions on this claim rule.

Edit Rule - Pass through Windows Account Name

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name:

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type:

Incoming name ID format:

☒ Pass through all claim values

☐ Pass through only a specific claim value

Incoming claim value:

☐ Pass through only claim values that match a specific email suffix value:

Email suffix value:

Example: fabrikam.com

☐ Pass through only claim values that start with a specific value:

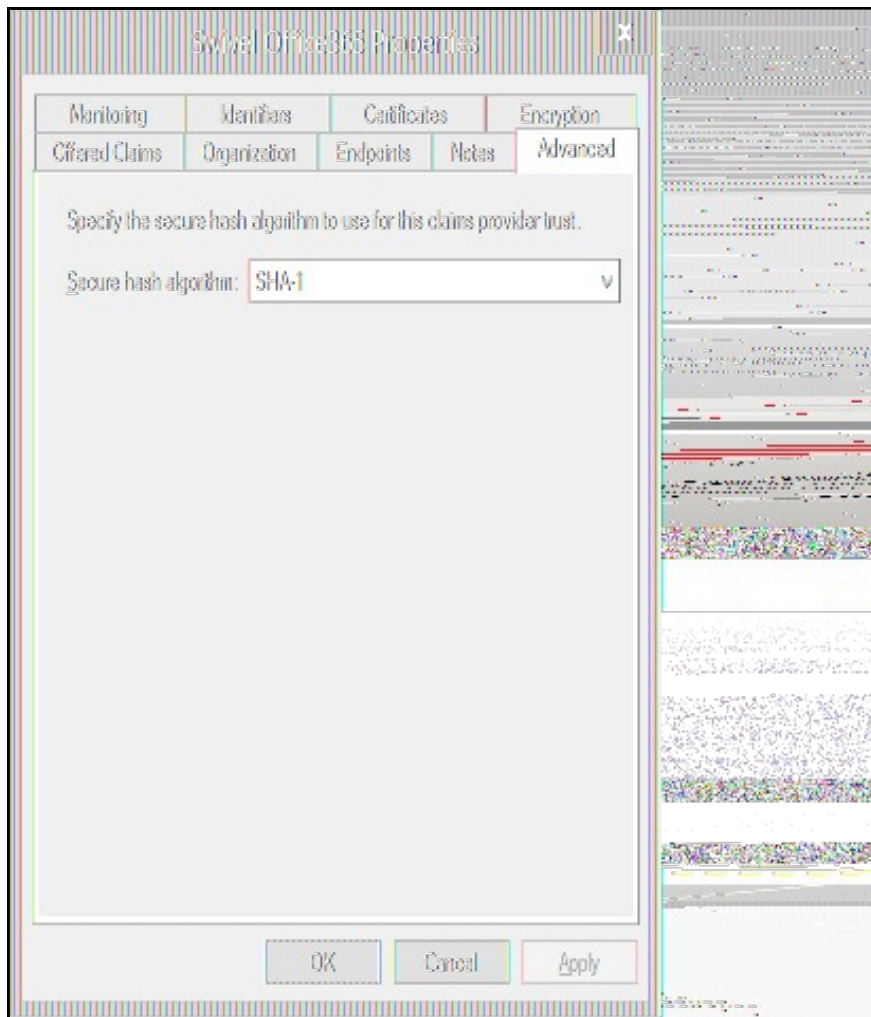
Starts with:

Example: FABRIKAM\

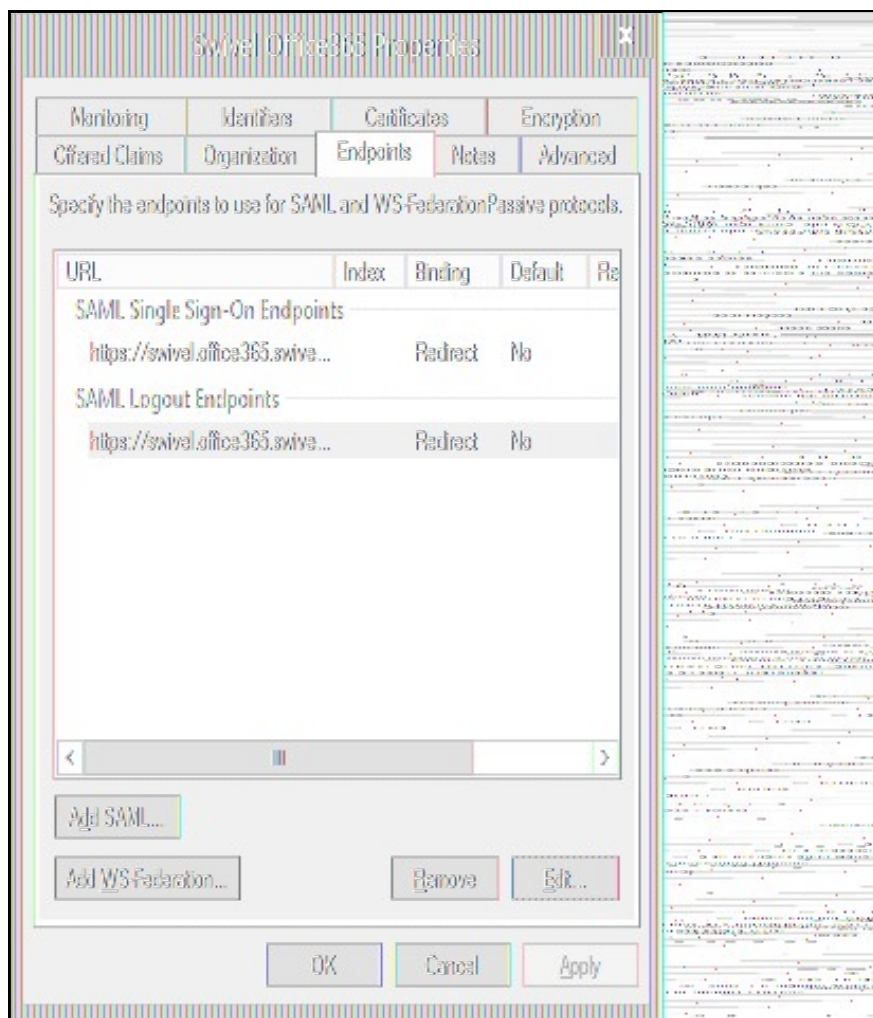
Settings:

You will need to edit the properties of this trust:

- Under Advanced, Secure hash algorithm must match the signing algorithm for the Sentry certificate. Version 4 supports SHA-256, but if you have an older version of Sentry SSO, you must select SHA-1.



- Under Endpoints, there should be two endpoints configured.



If not, create them as follows. If they have been created, check that they match the following. Both are SAML endpoints:

- Endpoint Type = SAML Single Sign-On, Binding = redirect, Trusted URL = https://<sentry_URL>/sentry/saml20endpoint

Endpoint type:
SAML Single Sign-On

Binding:
Redirect

☐ Set the trusted URL as default

Index: 0

Trusted URL:
https://swivel.office365.swivelssecure.com/sentry/saml20endpoint
Example: https://sts.contoso.com/aufrs/ls

Response URL:

Example: https://sts.contoso.com/logout

OK Cancel

- Endpoint Type = SAML Logout, Binding = redirect, Trusted URL = https://<sentry_URL>/sentry/singlelogout, Response URL = https://<sentry_URL>/sentry/singlelogout

Endpoint type:
SAML Logout

Binding:
Redirect

☐ Set the trusted URL as default

Index: 0

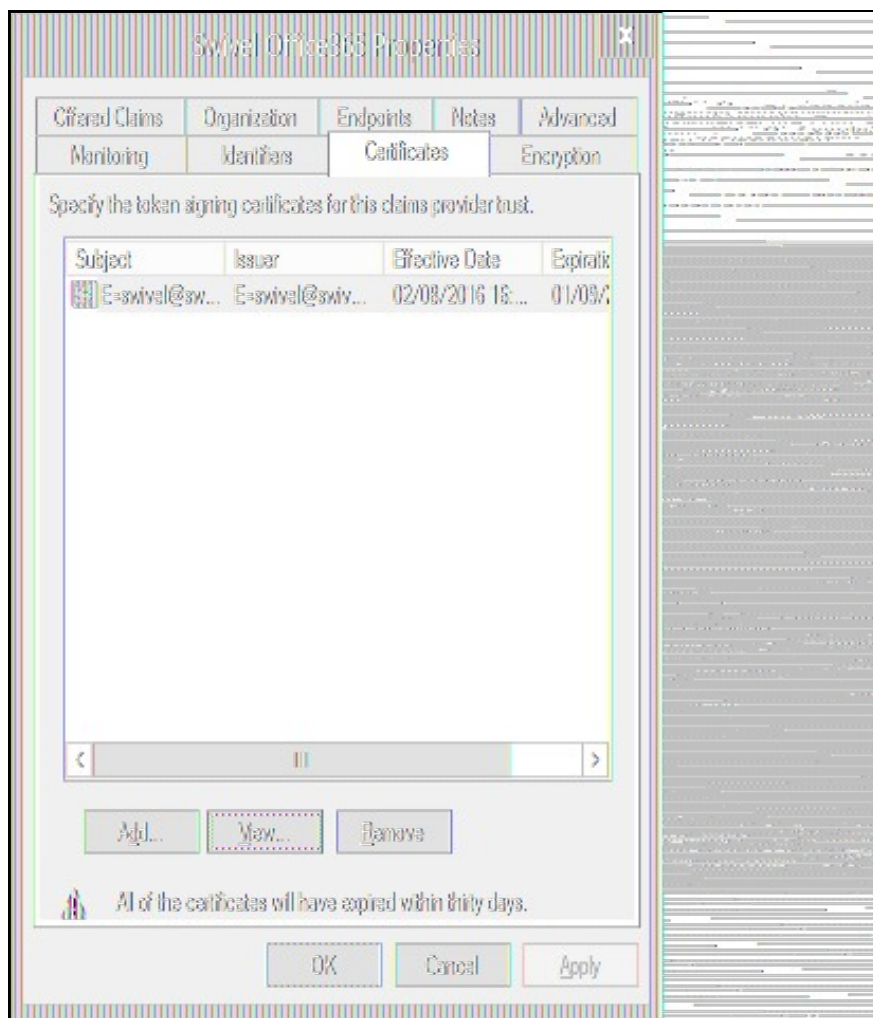
Trusted URL:
https://swivel.office365.swivelssecure.com/sentry/singlelogout
Example: https://sts.contoso.com/aufrs/ls

Response URL:

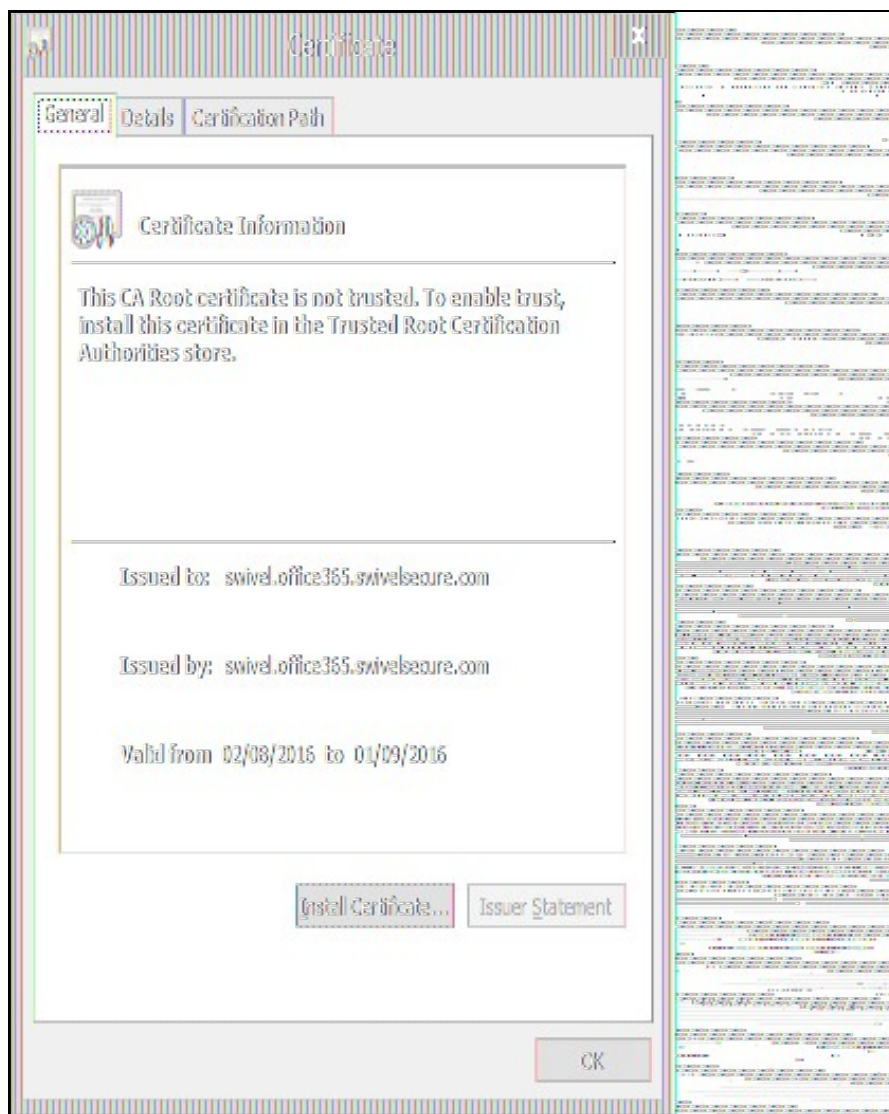
Example: https://sts.contoso.com/logout

OK Cancel

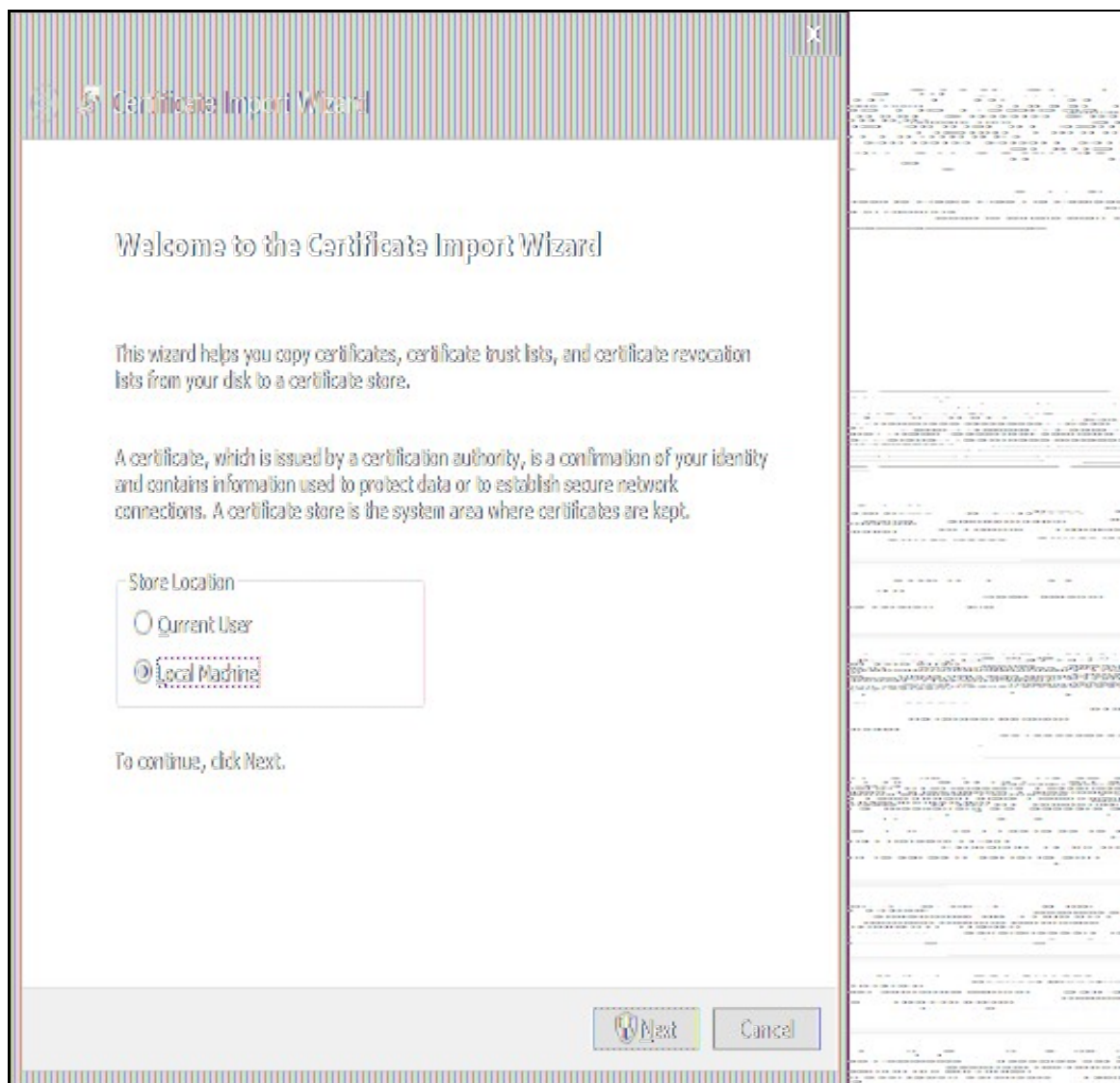
- Under Certificates,



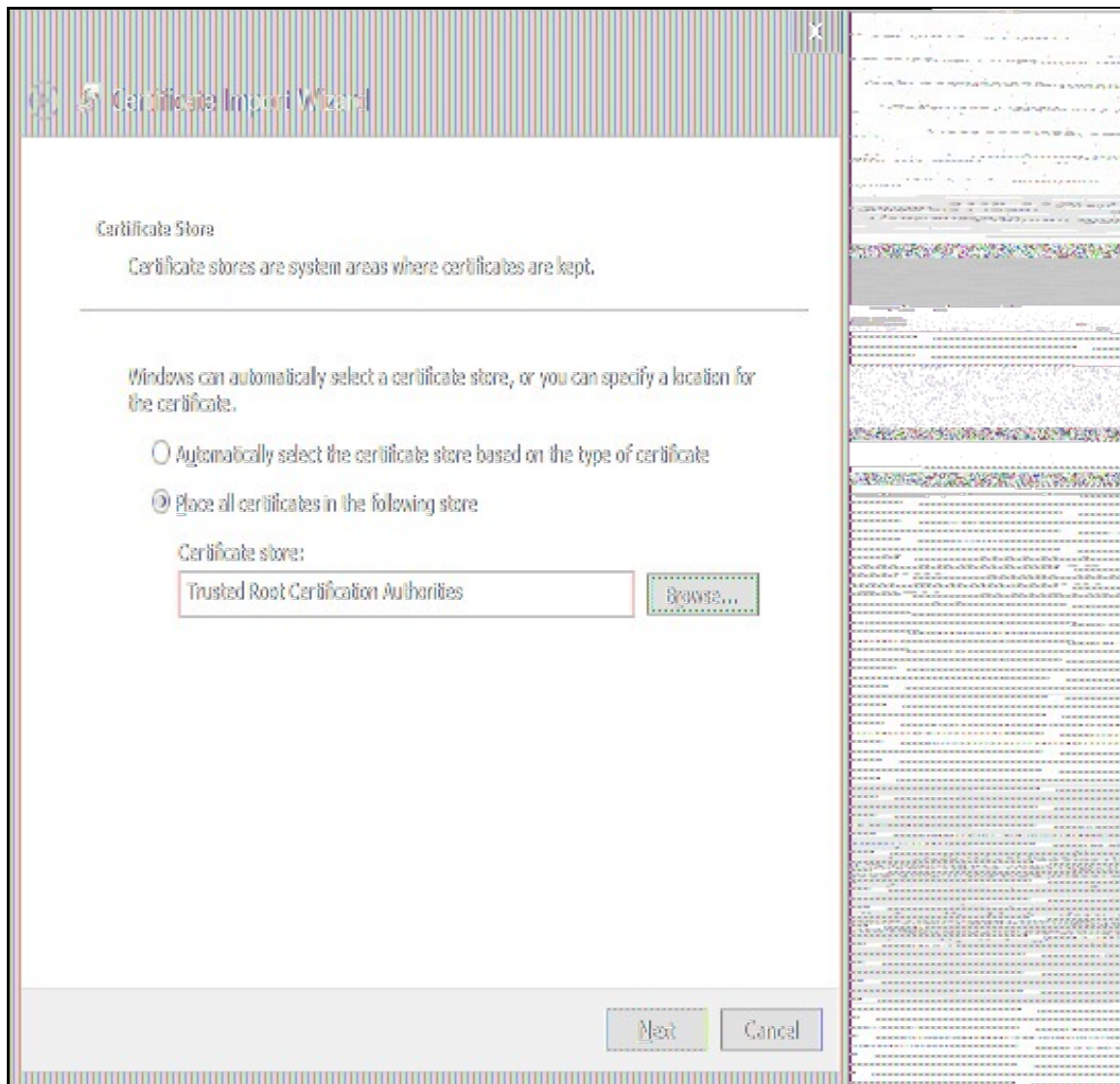
view the imported certificate,



then click on **Install Certificate**.



Select **Local Machine** on the next page,



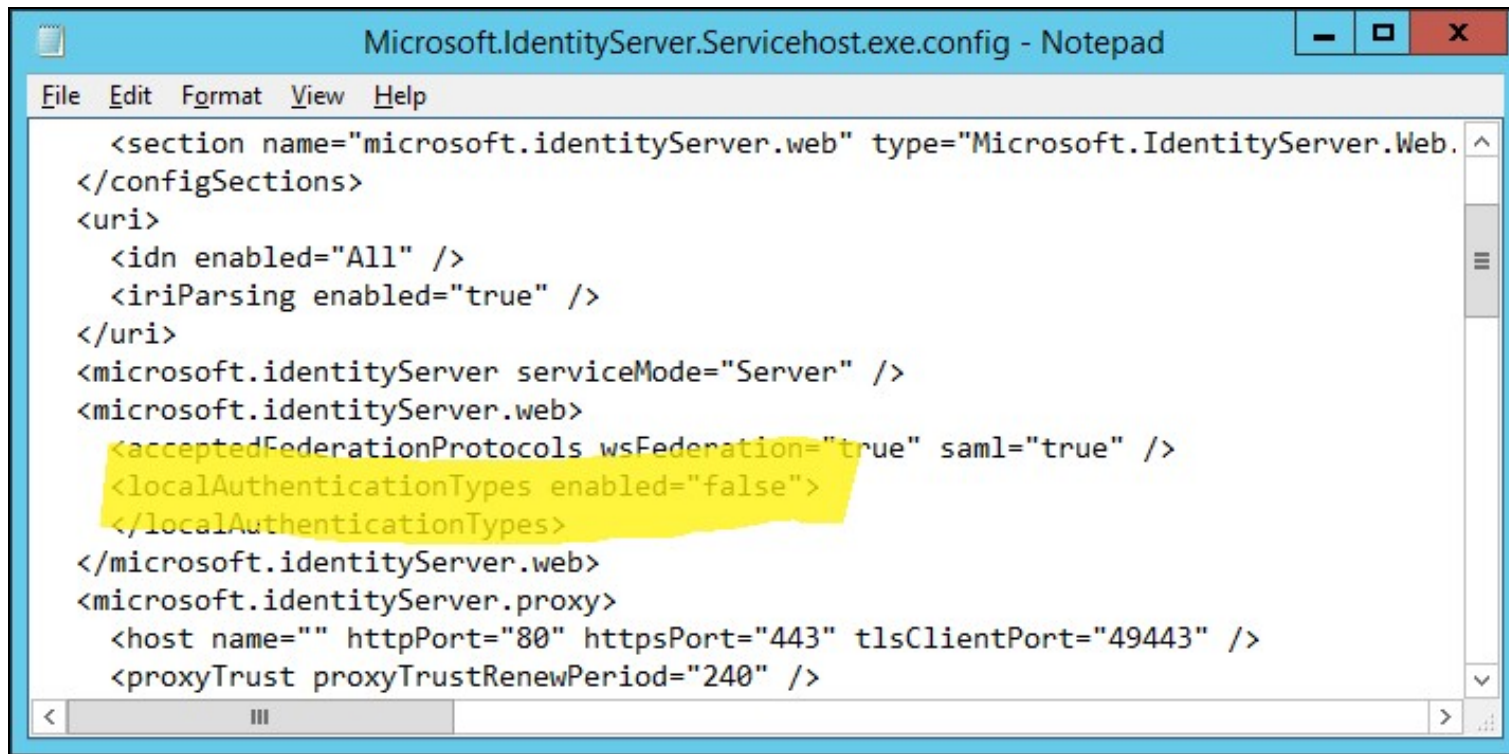
and on the following page, **Place all certificates in the following store**. Browse and select **Trusted Root Certification Authorities**.

36.3.3 Disable Active Directory Authentication

As ADFS is currently configured, you will now have a choice of Active Directory or Swivel authentication. To disable Active Directory authentication:

- Edit C:\Windows\ADFS\Microsoft.IdentityServer.Servicehost.exe.config.

Note that you must open your text editor (for example Notepad) as administrator, or you will not be able to save the changes.



```
Microsoft.IdentityServer.Servicehost.exe.config - Notepad
File Edit Format View Help
<section name="microsoft.identityServer.web" type="Microsoft.IdentityServer.Web.
</configSections>
<uri>
  <idn enabled="All" />
  <iriParsing enabled="true" />
</uri>
<microsoft.identityServer serviceMode="Server" />
<microsoft.identityServer.web>
  <acceptedFederationProtocols wsFederation="true" saml="true" />
  <localAuthenticationTypes enabled="false">
</localAuthenticationTypes>
</microsoft.identityServer.web>
<microsoft.identityServer.proxy>
  <host name="" httpPort="80" httpsPort="443" tlsClientPort="49443" />
  <proxyTrust proxyTrustRenewPeriod="240" />
</microsoft.identityServer.proxy>
```

- Search for ?<localAuthenticationTypes? and set enabled to ?false?.
- Restart ADFS.

36.3.4 Implement Sentry Authentication Selectively

If you don't want to use Sentry authentication for all ADFS applications, or in all scenarios, you can use the PowerShell cmdlets to control it. Some examples are given in the following link:

<https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/home-realm-discovery-customization>

Potentially the most useful scenarios would be to bypass Sentry for intranet login:

```
Set-AdfsProperties -IntranetUseLocalClaimsProvider $true
```

or to use Sentry for selected relying parties only:

```
Set-AdfsRelyingPartyTrust -TargetName "Office 365" -ClaimsProviderName @("Sentry SSO")
```


37 Sentry SSO with Cisco ASA

37.1 Introduction

This Document describes how to integrate a Cisco ASA with Swivel Sentry SSO. As Cisco ASA does not support SAML natively, this uses a custom login page to redirect to Sentry, and RADIUS to verify that the SAML claim is valid. Therefore, this solution is not suitable for use with AnyConnect.

37.2 Configure Cisco ASA

The first step is to create a RADIUS authentication server group, and associate it with a connection profile. We do not go into details on this, as we presume the customer is familiar with configuring a Cisco ASA. However, please ensure that the server is set to match the Swivel IP address or host name. Note that the Swivel appliance doesn't support using a virtual IP address with RADIUS. Also, check that the ports match those on the Swivel RADIUS server (the defaults are 1812 and 1813, which should be correct). Make a note of the Server Secret Key used, as this will need to be entered on the Swivel server. Do not enable the **Microsoft CHAPv2 Capable** option.

The screenshot shows the 'Edit AAA Server' configuration window. The 'Server Group' is set to 'Swivel'. The 'Interface Name' is 'OUTSIDE'. The 'Server Name or IP Address' field is empty. The 'Timeout' is set to '10 seconds'. Under 'RADIUS Parameters', 'Server Authentication Port' is '1812', 'Server Accounting Port' is '1813', 'Retry Interval' is '10 seconds', 'Server Secret Key' is '000000', 'Common Password' is empty, 'ACL Network Convert' is 'Standard', and 'Microsoft CHAPv2 Capable' is unchecked. The 'SDI Messages' section shows 'Message Table'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

You will now need to customize the web page, as follows:

Cisco ASDM 7.6(1) for ASA -

File View Tools Wizards Window Help

Home Configuration Monitoring Save Refresh Back Forward Help

Device List Bookmarks

Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Customization

Customization Objects

Configure Customization Objects that the security appliance displays for the Login page, Logout page, and main SSL portal page

This parameter is enforced by a [VPN group policy](#) or a [user policy](#) that controls the customization of the SSL VPN portal page, or a [connection profile](#) that controls the customization of the Login and Logout pages. You can click on Assign button to assign the selected one to them.

Add Edit Delete Import Export Assign

Customization	Group Policies/Connection Profiles/LOCAL Users Using the Customization
Template	Template
DfltCustomization	DfltCustomization
SwivelCustom	SwivelCustom

Find: Match Case

OnScreen Keyboard

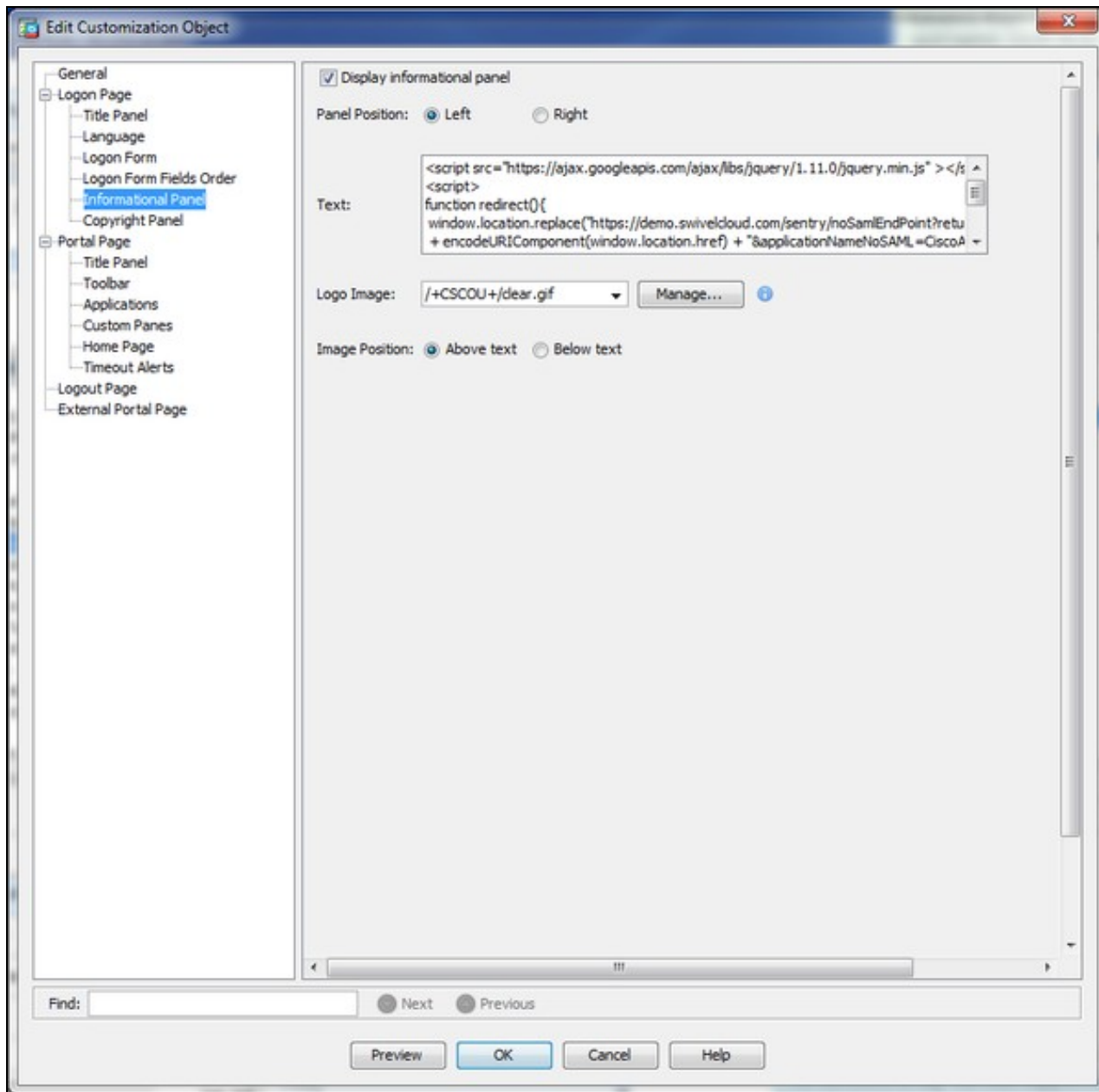
Specify when OnScreen Keyboard should be shown on portal pages.

☒ Do not show OnScreen Keyboard
☐ Show only for the login page
☐ Show for all portal pages requiring authentication

Apply Reset

swivel 15

Select the customization you intend to use, or create a new one. If you create a new one, make sure you associate it with the connection profile that uses the Swivel server, on the **General** tab.



Select **Informational Panel**. Make sure you check **Display informational panel**. Then paste the following code in the **Text** field:

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect() {
    window.location.replace("https://<swivel_server>/sentry/noSamlEndPoint?returnurlNoSAML="
        + encodeURIComponent(window.location.href) + "&applicationNameNoSAML=<EntityID>" );
}
var QueryString = function () {
    // This function is anonymous, is executed immediately and
    // the return value is assigned to QueryString!
    var query_string = {};
    var query = window.location.search.substring(1);
    var vars = query.split("&");
    for (var i=0;i<vars.length;i++) {
        var pair = vars[i].split("=");
        // If first entry with this name
        if (typeof query_string[pair[0]] === "undefined") {
            query_string[pair[0]] = pair[1];
        } // If second entry with this name
        else if (typeof query_string[pair[0]] === "string") {
            var arr = [ query_string[pair[0]], pair[1] ];
            query_string[pair[0]] = arr;
        } // If third or later entry with this name
        else {
            query_string[pair[0]].push(pair[1]);
        }
    }
    return query_string;
} ();

$(document).ready(function() {
    usernamePassedIn = QueryString["username"];
    passwordPassedIn = QueryString["password"];
    claimPassedIn = QueryString["claim"];
```



```

if(typeof claimPassedIn == 'undefined') {
    redirect();
} else {
    $('[name=password]').val(claimPassedIn);
    $('[name=username]').val(usernamePassedIn);
    // $('[name=user#2]').val(usernamePassedIn);
    // $('[name=password#2]').val(claimPassedIn);
    document.getElementById("unicorn_form").submit();
}
});
</script>

```

before you paste it, replace <swivel_server> with the public host name of your Swivel Sentry server. Also, replace <EntityID> with the Entity ID of the Sentry application you create - see below.

Secondly, go to the **Logout Page** tab and enter the following code:

```

<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect(){
    window.location.replace("https://<swivel_server>/sentry/singlelogout");
}
$(document).ready(function(){
    redirect();
});
</script>

```

Again, replace <swivel_server> with the public host name of your Swivel Sentry server.

37.3 Configure Swivel Sentry

Log into the Sentry administration console. Select **Applications**. Then click **Add Application** and select the type **RADIUS VPN - Cisco ASA**

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

RADIUS VPN Application



Note: The Endpoint URL is used only if it

Name

CiscoASA

Image

Cisco.png

Points

0

Portal URL

https://cisco.yourdomain.com

Endpoint URL

Entity ID

CiscoASA

Enter a name - it is recommended that the name is the same as the Entity ID below.

Portal URL should be the public URL of your Cisco server. It is recommended that you use the same address for **Endpoint URL**, although this will usually be overridden by the address sent by the Cisco login page.

Entity ID must be the same as the value shown as `<EntityID>` in the section above, so that Sentry will recognize the request as coming from this Cisco server.

37.4 Configure RADIUS NAS on Swivel Core

You need to create a new NAS entry on the Swivel Core application. Log into the Swivel web admin console, and go to RADIUS -> NAS.

The screenshot shows the Swivel Cloud Demo web admin console. The top header is purple with the Swivel logo and version 'Swivel v4.0.3.4756 © 2016'. Below the header is a navigation menu on the left with links like Status, Log Viewer, Server, Policy, Logging, Messaging, Database, Mode, Repository, RADIUS (with sub-links for Server and NAS), Migration, Windows GINA, Appliance, OATH, Config Sync, Reporting, User Administration, Save Configuration, Upload Email Images, Administration Guide, and Logout. The main content area is titled 'RADIUS>NAS' and contains a description: 'Please enter the details for any RADIUS network access servers. A NAS is permitted to access the authentication services of the Swivel server via the RADIUS interface.' Below this is a form for configuring a new NAS entry. The form has a 'NAS:' section with radio buttons for 'Juniper', 'Netscaler', and an empty box. The 'CiscoASA' radio button is selected. The form fields include: Identifier (CiscoASA), Hostname/IP (redacted), Secret (masked with dots), Group (---ANY---), EAP protocol (None), Authentication Mode (All), Vendor (Groups) (None), Change PIN warning (No), Two Stage Auth (No), Allow blank password at Stage One (No), Send Security String after Stage One (Yes), Even if User has Valid String (Yes), Check password with repository (No), One Touch Enabled (No), Authenticate non-user with just password (No), Username attribute for repository (empty), Allow alternative usernames (Yes), Alternative username attributes (altusername), OTC timeout (mins) (0), Internal IP ranges (empty), and Send username in challenge (No). A 'Delete' button is visible at the bottom right.

Identifier must be the same as the Entity ID from the Sentry application and the Cisco custom code, in order for authentication to succeed.

Hostname/IP should be the IP address (or hostname) of the Cisco ASA.

Secret must be the same as the one entered on the RADIUS server details on the Cisco.

Everything else should be left as default.

37.5 SSO

For RADIUS VPN applications the login page will be displayed although Sentry has been configured with SSO enabled. That attribute just applies for SAML applications.

37.6 Known Issues/Limitations

This method of authentication relies on the default policy for the Cisco portal requiring Swivel RADIUS authentication as the only authentication. It will not work if additional authentication is required, or if the user needs to select the Swivel authentication policy.

Because this method uses a custom login page, it cannot be used with AnyConnect or IPSEC - only with the Cisco ASA web login page.

38 Sentry SSO with Cisco ASA using SAML

38.1 Introduction

This Document describes how to integrate a Cisco ASA with Swivel Sentry SSO using SAML.

If your Cisco ASA does not support SAML or you are not licensed to do so, our Sentry SSO with Cisco ASA for RADIUS article can be used instead: it uses a custom login page to redirect to Sentry, and RADIUS to verify that the SAML claim is valid. The solution is not suitable for use with AnyConnect.

38.2 Setup AuthControl Sentry Keys

Before you are able to create a SAML configuration in Cisco ASA, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

38.3 Convert Sentry Keys to PFX

You will need to retrieve the keys generated above from the /home/swivel/.swivel/sentry/keys folder so that you are able to convert from PEM format to a PFX file containing the private key.

The openssl command to achieve a PEM to PFX conversion is as follows:

```
openssl pkcs12 -export -out Cert.pfx -in cert.pem -inkey key.pem
```

You will be prompted for a password for the private key and a password for the PFX you are creating This command assumes:

- Cert.pfx is the file being created
- cert.pem is the cert file downloadable from the AuthControl keys GUI
- key.pem is the private key you download from the /home/swivel/.swivel/sentry/keys folder using WinSCP

38.4 Download the Sentry SSO IdP metadata

In the Sentry SSO Web GUI (running on port 8443), right click on the 'View IdP Metadata' left hand menu option and 'Save As' an xml file e.g. SwivelIdPMetadata.xml. We will upload this to the Cisco ASA in a moment.

38.5 Configure Cisco ASA

We recommend you protect your SSL VPN endpoint with an SSL certificate and ensure that it is working prior to embarking on this integration.

The below steps all assume that you are administering the Cisco ASA using the ASDM client.

38.5.1 Import the AuthControl Sentry IdP Certificate

In the ASDM, go to Configuration -> Remote Access VPN -> Certificate Management -> Identity certificates.

Click Add. Give the certificate an arbitrary name. Import the PFX created earlier being sure to ensure a password was set and is entered in the Decryption Passphrase field. Browse to the file and finally, click Add Certificate to validate and import the PFX.

Don't forget to Apply the changes in the ASDM client.

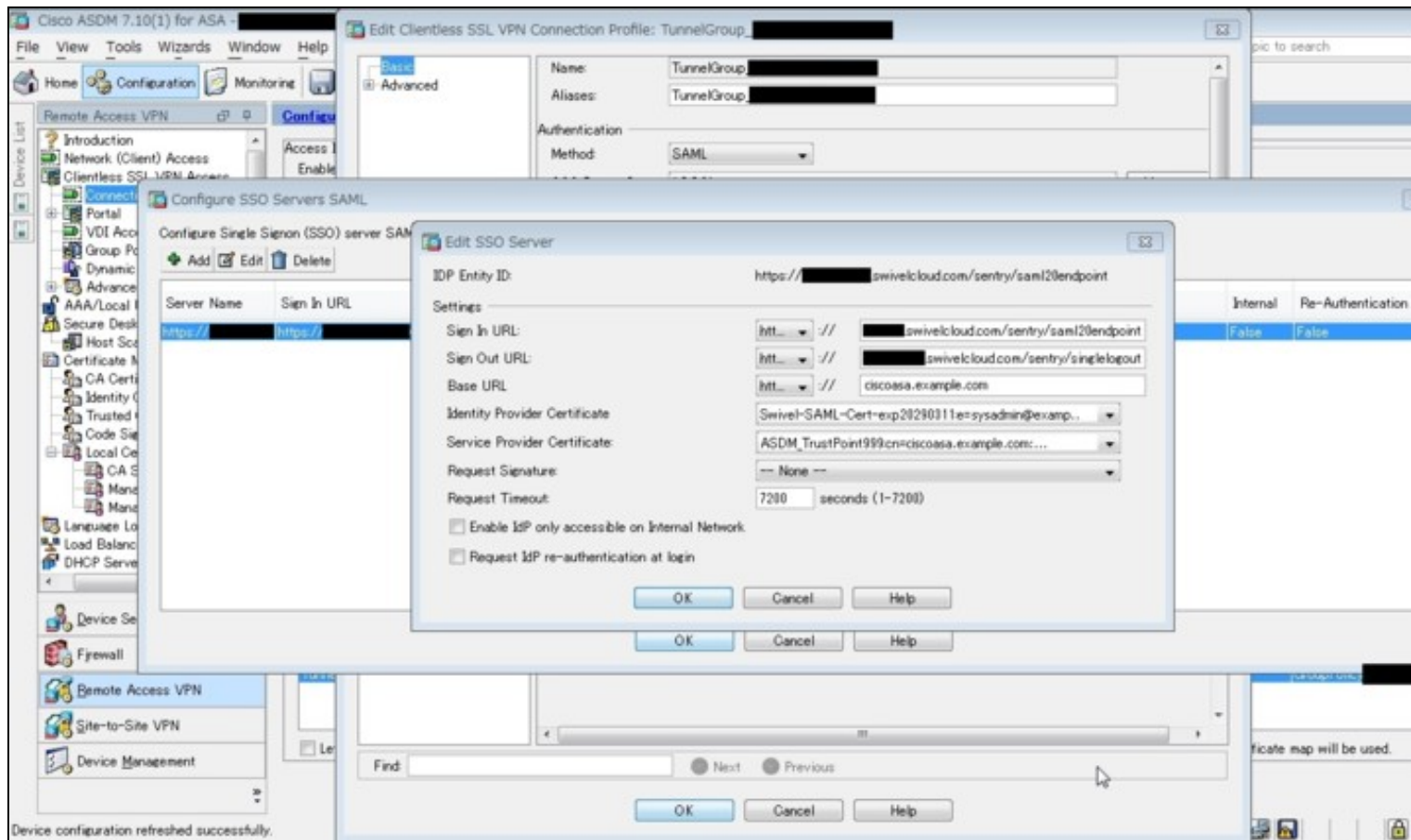
38.5.2 Setup the SAML IdP against the SSL VPN Connection Profile

In the ASDM, go to Configuration -> Remote Access VPN -> Clientless SSL VPN Access -> Connection Profiles, highlight the Connection Profile assigned to the SSL VPN and click the Edit button.

Under the Basic tab, SAML Identity Provider section, click Manage.

Add a new entry:

- IDP Entity ID: (needs to match the entity ID specified in Sentry SSO metadata XML file, in the AuthControl Sentry GUI -> View Metadata screen you will see the IDP's entity ID listed at the top) e.g. "**https://<AuthControlSentryHostname>/sentry/saml20endpoint**". The FQDN of this entity ID URL should be valid. If not, login to the Swivel Secure CMI -> Main Menu -> Appliance -> Sentry and set the Base URL to be correct and restart Tomcat. Then view and export the IdP metadata again.
- Sign In URL: **https://<AuthControlSentryHostname>/sentry/saml20endpoint**
- Sign Out URL: **https://<AuthControlSentryHostname>/sentry/singlelogout**
- Base URL: (the CiscoASA FQDN hostname) e.g. **https://ciscoasa.example.com**
- Identity provider certificate (select the one imported earlier)
- Service provider certificate (select the SSL certificate assigned to the SSL VPN endpoint)



38.6 Configure AuthControl Sentry

Log into the Sentry administration console. Select **Applications**. Then click **Add Application** and select the type **SAML - Other**

Enter an arbitrary name e.g. "Cisco ASA".

Portal URL should be the public URL of your Cisco server. It is recommended that you use the same address for **Endpoint URL**, although this will usually be overridden by the address sent by the Cisco login page.

Entity ID must be the same as the value shown as *IDP Entity ID* in the Add SSO Server window shown above, so that AuthControl Sentry will recognize the request as coming from this Cisco server.

39 Sentry SSO with CiscoASA

39.1 Introduction

This article explains how to integrate a Cisco ASA with Sentry.

It focusses on the setting up of Sentry and the modification of the login pages to support the Sentry integration.

It assumes knowledge of how to configure the Cisco ASA to use Sentry as a RADIUS authentication server. Details of these elements can be found in the existing integration guide [Cisco ASA Integration](#)

For this integration it is recommended that the Swivel Radius server is the only authentication required for this realm.

39.2 Overview

The integration works by

1. configuring the Cisco ASA login page to redirect the user to Sentry to authenticate
2. user authenticates at Sentry
3. user is redirected back to the Cisco ASA login page with a claim
4. Cisco ASA login page is submitted with username and claim
5. Username and claim are validated via RADIUS
6. User gains access

Therefore the following steps are required

1. Configure Cisco ASA Login
2. Configure Sentry to work with Cisco ASA login page
3. Configure Sentry to accept RADIUS requests from Cisco ASA

39.3 Configure Cisco ASA Login

In order to make the Cisco ASA page work in the desired way once the page has loaded the page must detect if the user has been redirected to this page from Sentry or if the user have come directly.

If the user has come directly they need to be redirected to Sentry. If they have been directed from Sentry the login form needs to be populated and submitted.

This is the required snippet that needs adding to the head section of the login pages.

The only modification required is to change SENTRYURL for the actual public url of your sentry install.

Note the **applicationNameNoSAML=CiscoVPN**. This is important as this application name must match the settings on Sentry

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect(){
  window.location.replace("https://SENTRYURL/noSamlEndPoint?returnurlNoSAML="
+ window.location.href + "&applicationNameNoSAML=CiscoVPN" );
}
var QueryString = function () {
  // This function is anonymous, is executed immediately and
  // the return value is assigned to QueryString!
  var query_string = {};
  var query = window.location.search.substring(1);
  var vars = query.split("&");
  for (var i=0;i<vars.length;i++) {
    var pair = vars[i].split("=");
    // If first entry with this name
    if (typeof query_string[pair[0]] === "undefined") {
      query_string[pair[0]] = pair[1];
      // If second entry with this name
    } else if (typeof query_string[pair[0]] === "string") {
      var arr = [ query_string[pair[0]], pair[1] ];
      query_string[pair[0]] = arr;
      // If third or later entry with this name
    } else {
      query_string[pair[0]].push(pair[1]);
    }
  }
  return query_string;
} ();

$(document).ready(function(){
  usernamePassedIn = QueryString["username"];
  passwordPassedIn = QueryString["password"];
  claimPassedIn = QueryString["claim"];
  if(typeof claimPassedIn == 'undefined') {
    redirect();
  } else {
    $('[name=password]').val(claimPassedIn);
    $('[name=login]').val(usernamePassedIn);
    document.getElementsByName("unicorn_form")[0].submit();
  }
});
</script>
</head>
```

39.4 Configuring Sentry Login

The Cisco ASA VPN needs to be added to Sentry as an Application.

The following entries are required.

- Name This must match the name in the redirect url, eg CiscoVPN
- Service Provider SwivelVPN. Indicates this is a VPN integration
- Points Number of points required to access the VPN, refer to Sentry User guide
- Endpoint URL This is the URL of the Cisco ASA login page configured to work with Sentry
- Entity ID Should match Name.

39.5 Configuring Sentry RADIUS

To complete the integration the Cisco ASA VPN must be added as a NAS on the Sentry server.

The key settings are

- Identifier Must match the Name on Sentry login, eg CiscoVPN
- Hostname Must match IP of Cisco ASA VPN

Two stage auth, Check Password with repository should be set to NO

39.6 SSO

If the Sentry login has been configured with SSO enabled then the Cisco ASA login page will work in the same way as other Sentry applications. If a user has authenticated already with more points than the Cisco ASA requires then the user will gain access to the Cisco ASA without needing to authenticate again.

39.7 Testing

- Goto to Cisco ASA login url
- User redirected to Sentry, user should be prompted for credentials
- Supply credentials

Should see Sentry logs including

```
Login successful for user: username  
SSO_CLAIM_CREATED_FOR_USER, username
```

- User should be redirected to Cisco ASA VPN
- User should gain access

Logs should include

```
CiscoVPN:Processing user username as channel CLAIM  
CiscoVPN:Login successful for user: username
```

39.8 Troubleshooting

The scripts on the login page work by injecting values into the login page and submitting this page. To work therefore the standard login page must have a form called unicorn_form that has an input field called login for the username and an input field called passwd for the password as shown in the javascript.

By "called" the html must have the name attribute set to this value

40 Sentry SSO with Citrix Netscaler

40.1 Introduction

This article explains how to integrate a Citrix Netscaler with Sentry via SAML.

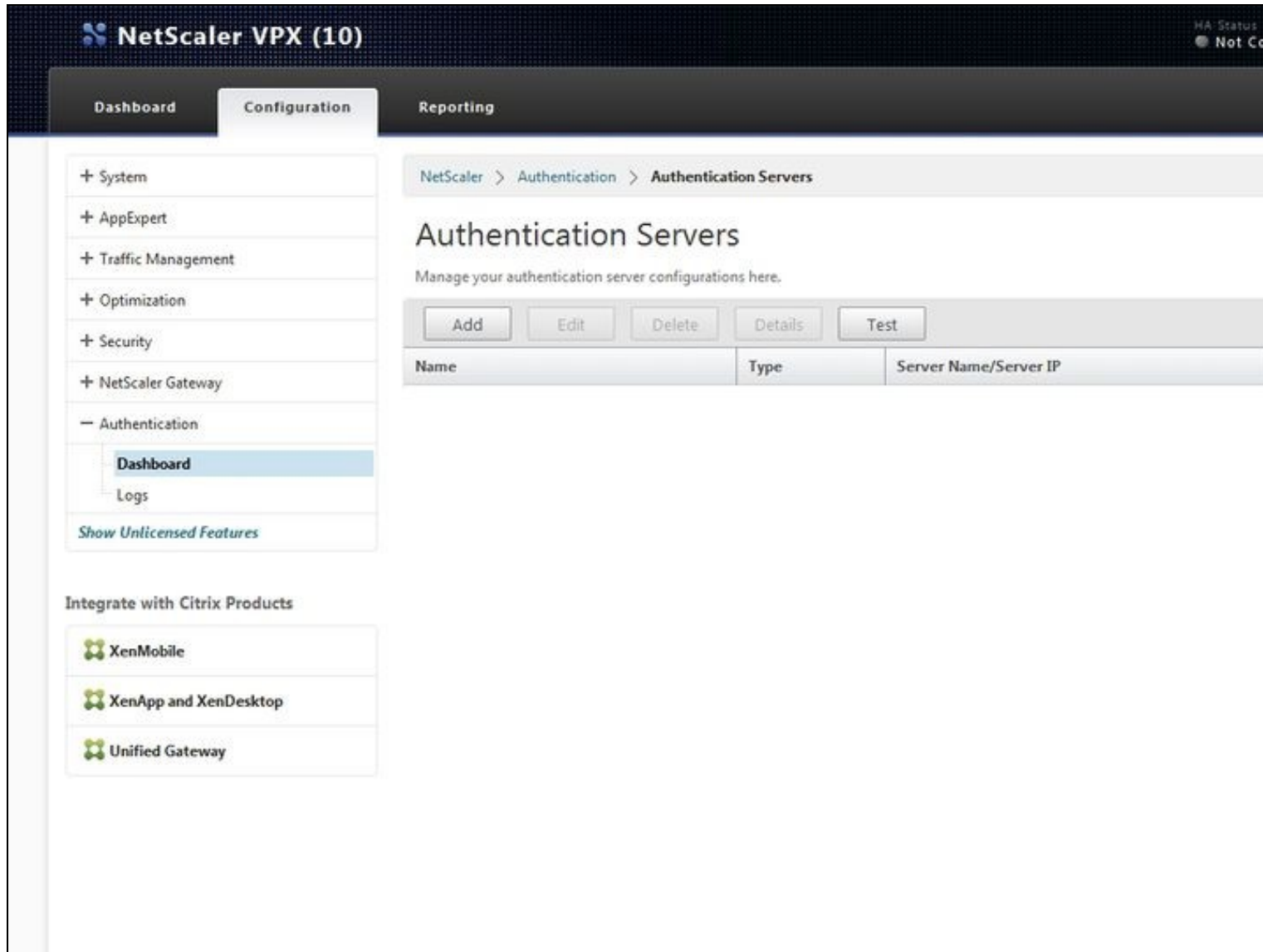
It assumes knowledge of how to configure the Netscaler and that a Virtual Server has been already created, missing just the SAML authentication configuration.

40.2 Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on your Netscaler Citrix account, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

40.3 Setup SAML SSO on Citrix Netscaler

To configure SAML SSO settings on your Citrix Netscaler account you have to access your Admin console. You should see an Admin console with an option "Authentication > Dashboard" similar to the one below:



On the Authentication Servers screen you have to click on the Add button. You will be shown a create authentication server screen with a Choose Server Type options where you have to click on "SAML".

DashboardConfigurationReporting

Back

Configure Authentication SAML Server

Name

SAML_test

Authentication Type

SAML

IDP Certificate Name*

sentry-rsa-cert

+

Redirect URL*

http://192.168.11.115:8084/sentry/sai

Single Logout URL

http://192.168.11.115:8084/sentry/sir

User Field

Signing Certificate Name

Issuer Name

citrix.swivelsecure.com

Reject Unsigned Assertion*

OFF

SAML Binding*

POST

?

Default Authentication Group

local

Two Factor

☐ ON ☒ OFF

Assertion Consumer Service Index

255

Attribute Consuming Service Index

255

Requested Authentication Context*

Exact

You will have to enter a name for the Authentication SAML Server and fill in the details for your AuthControl Sentry such as:

IDP Certificate Name - Click on + and a screen like the one displayed below should be displayed. Browse to the RSA PEM files created earlier to upload the certificate and select PEM as a Certificate Format:

Install Certificate

Certificate-Key Pair Name*

sentry-rsa-cert

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name*

rsacert.pem

Browse ▼ +

Key File Name

rsaprivkey.pem

Browse ▼ +

Certificate Format

☒ PEM ☐ DER

Password

••••••••

☐ Certificate Bundle

☒ Notify When Expires

Notification Period

30

Install Close

After you have entered all the certificate details click Install

Set the Redirect and Single Logout below, where <FQDN_OF_SENTRY_SERVER> is the public DNS entry of your Swivel AuthControl Sentry server, e.g. swivel.mycompany.com or if you do not have a redirect from port 443 to 8443 in place, you may need to include a port number e.g. swivel.mycompany.com:8443

Redirect URL - *https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint*

Single Logout URL - *https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout*

Issuer Name - *E.g. citrix.companyname.com*

(The value set in here will be used to configure the Citrix Netscaler application on AuthControl Sentry)

Signature Algorithm - RSA-SHA256

Digest Method - SHA1

After you have entered all the details as above click Create

Now the SAML authentication server has been created. To configure the Virtual Server used to log in to use SAML authentication, select Netscaler Gateway > Virtual Servers and click Edit. You should see a screen like the one below:

Dashboard

Configuration

Reporting

← Back

VPN Virtual Server

Basic Settings

Name Demo
IPAddress 10.40.242.185
Port 443
State ● Up
RDP Server Profile -
Login Once false
Double Hop false
Down State Flush true
DTLS false
AppFlow Logging false

Maximum Users 0
Max Login Attempts -
Failed Login Timeout -
ICA Only true
Enable Authentication true
Windows EPA Plugin Upgrade -
Linux EPA Plugin Upgrade -
Mac EPA Plugin Upgrade -
ICA Proxy Session Migration false
Enable Device Certificate false

Certificates

1 Server Certificate

1 CA Certificate

Authentication

Primary Authentication

1 SAML Policy

Profiles

Net Profile -
TCP Profile -
HTTP Profile nshttp_default_strict_validation

Published Applications

No Next HOP Server

1 STA Server

No Url

To add the SAML authentication server click + on the Authentication section. Select Policy as SAML and type Primary. Click the Continue button.

Choose Type

Choose Type

Policies

Choose Policy*

SAML

Choose Type*

Primary

Continue

Cancel

The below screen will be displayed. Click + to add Add Binding:

Choose Type

Choose Type

Policies

Choose Policy

SAML

Choose Type

Primary

Add Binding

Unbind

Edit

Priority

Policy Name

Expression

Click + add to add a new Policy Binding:

Choose Type > Policy Binding

Policy Binding

Select Policy*

Click to select

>

+

✍

Binding Details

Priority*

110

Bind

Close

Set a name for the SAML policy, select the SAML server configured before and add on Expression ns_true.

Choose Type > Policy Binding > Configure Authentication SAML Policy

Configure Authentication SAML Policy

Name
SAML_policy

Authentication Type
SAML

Server*
SAML_test

Expression*
Operators Saved Policy Expressions Frequently Used Expressions
ns_true

OK Close

After those parameters have been set click the Create button. Then the policy bind screen will be displayed again with the new policy selected.

Choose Type > Policy Binding

Policy Binding

Select Policy*
SAML_policy

More

Binding Details

Priority*
110

Bind Close

Click Bind. The below screen will be displayed.

Choose Type

Choose Type

Policies

Choose Policy

SAML

Choose Type

Primary

Add Binding

Unbind

Edit

Priority	Policy Name	Expression
110	SAML_policy	ns_true

Close

Click the Close button. The virtual server will have now the SAML authentication set. Click the back button and save the current configuration.

40.4 Configure Check Password with Repository on the Swivel Core

In order to check the user's Active Directory password, ensure that the local Agent is configured as explained [here](#)

40.5 Setup AuthControl Sentry Application definition

Please note: you must have setup a Citrix Netscaler SAML SSO prior to defining this Application entry within AuthControl Sentry. This is so that you are able to populate the Endpoint URL field. Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for Google, click the Add Provider button.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the AC SAML (Security Assertion Markup Language)

Name

CitrixNetscaler

Image

CitrixNetscaler.png

Points

0

Portal URL

https://citrix.yourdomain

Endpoint URL

Entity ID

citrix.yourdomain

Federated Id

email

- **Name:** Citrix Netscaler (Type an Arbitrary name for this Application)
- **Image:** CitrixNetscaler.png (selected by default)
- **Points:** 100 (the number of the points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)
- **Portal URL:** (this Portal URL is your companies Citrix Netscaler URL which you can usually access on: <https://citrix.mycompanyname.com>)
- **Endpoint URL:** N/A
- **Entity ID:** citrix.mycompanyname.com (This is the Issuer Name configured on Citrix Netscaler SAML server)

40.6 Setup AuthControl Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for Citrix Netscaler SAML authentication.

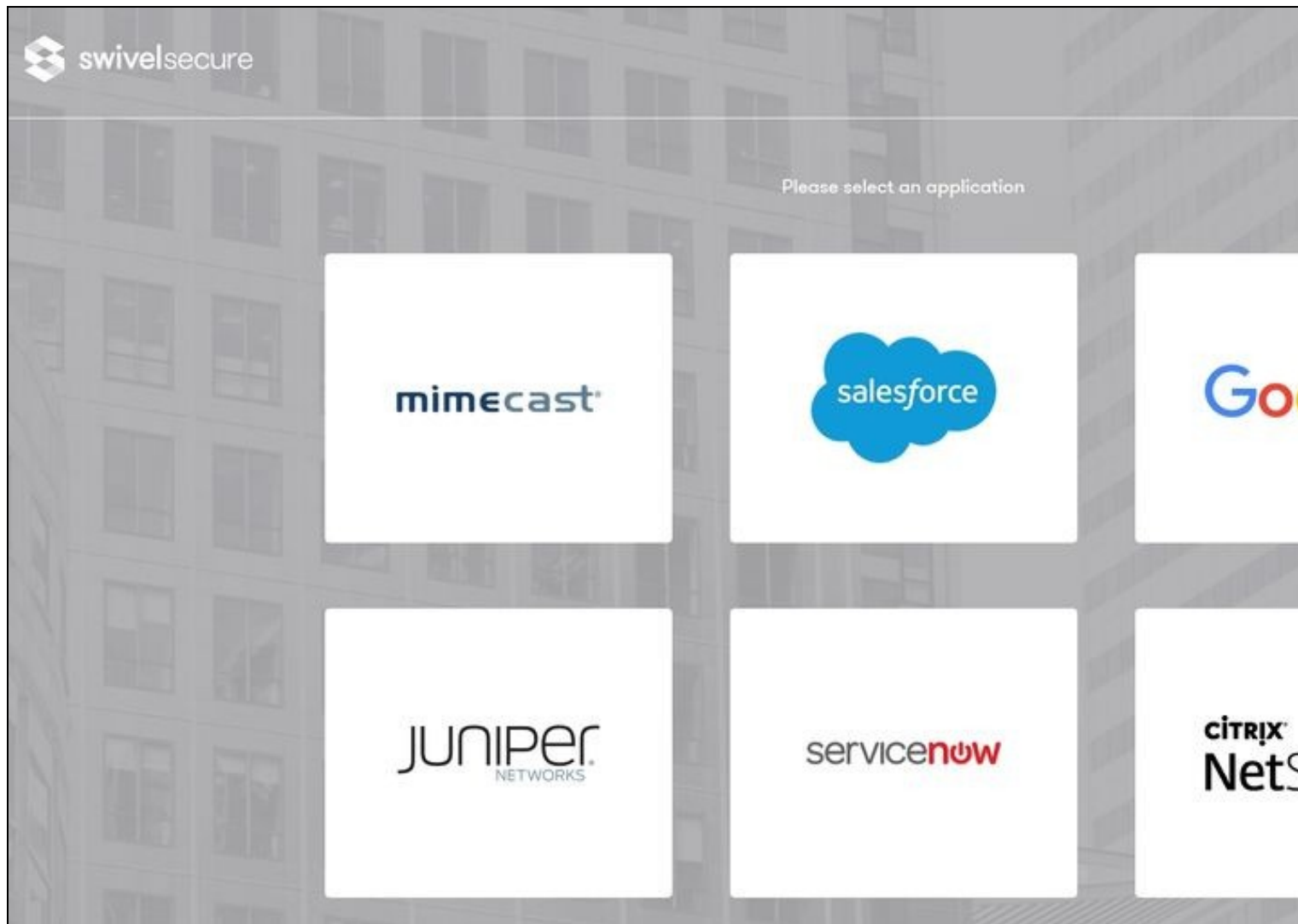
Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Google Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

40.7 Testing authentication to Google via Swivel AuthControl Sentry

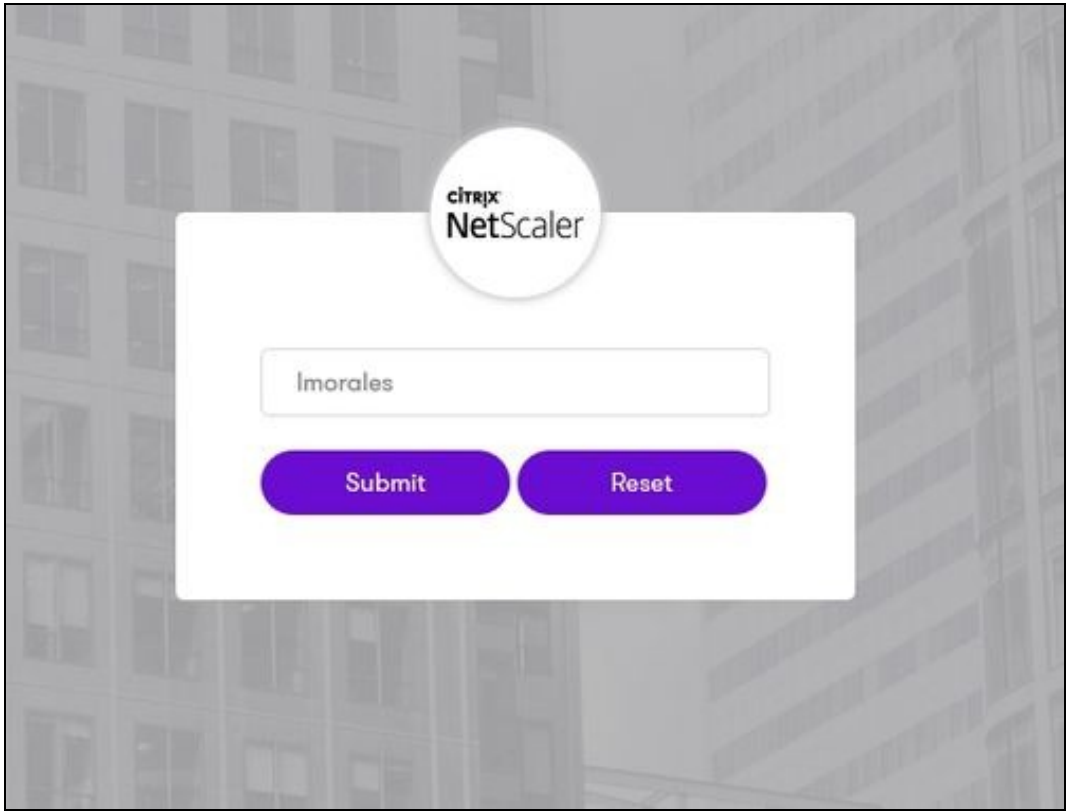
This should be the final step after all previous elements have been configured.

In a web browser, visit the the URL that you setup on AuthControl Sentry as Endpoint URL e.g. <https://citrix.mycompanyname.com>

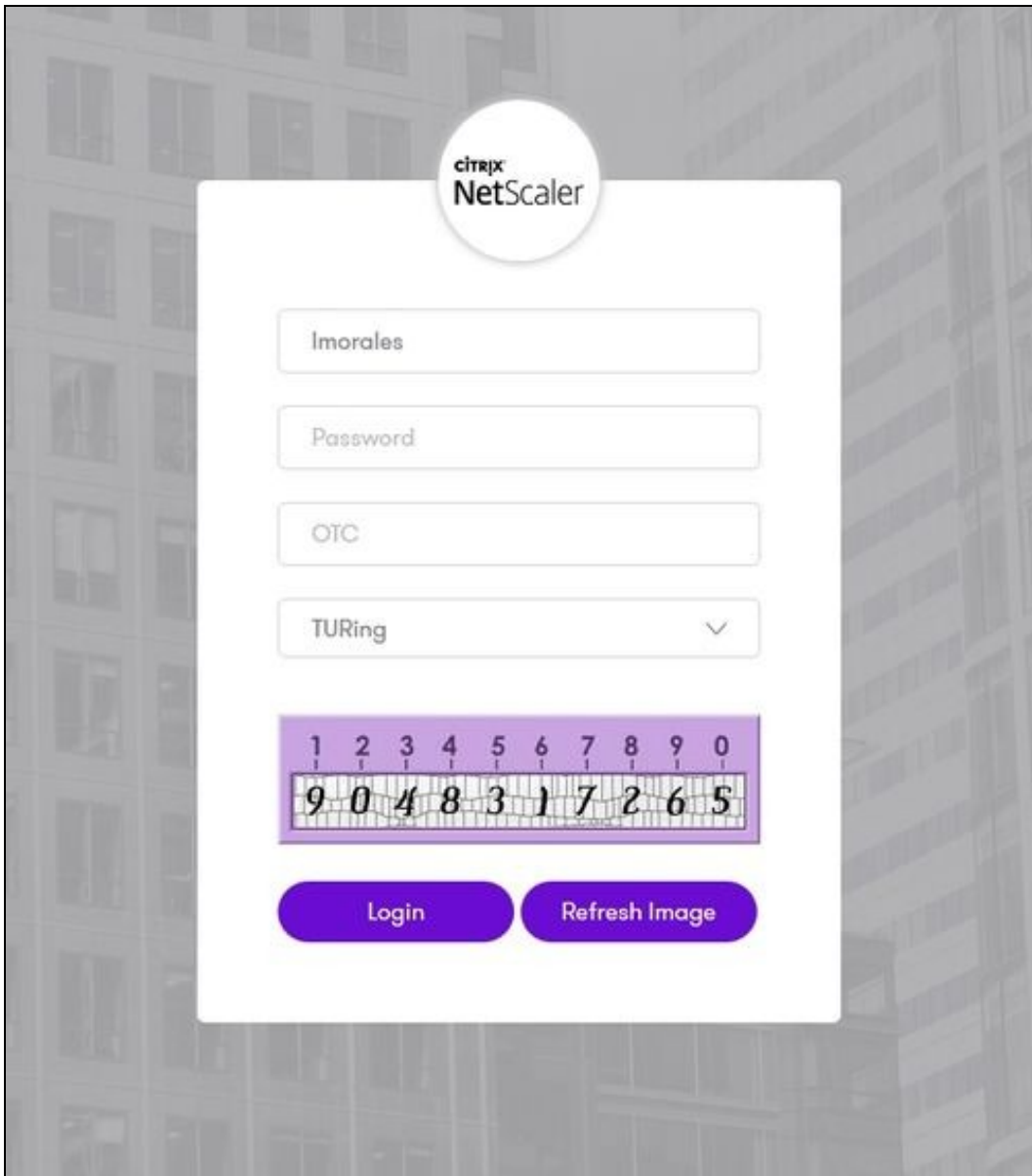
Alternatively you can visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. <https://mycompanysentrydomain/sentry/startPage> On a Start Page you will be able to see a new Google Icon on which you can click and proceed with authentication (as you would by going straight to the Citrix Netscaler page)



When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you have setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Citrix Netscaler Application definition.



After we enter the username we are prompted with another authentication method (in this example we use turing)



After we enter our authentication credentials we successfully will see the web app that we have tried to access.

40.8 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from Citrix Netscaler and can be useful for comparison with the Netscaler Citrix SAML Assertion Validator output;

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ◆ Can AuthControl Sentry find the Certificate locally, is it the correct one?
 - ◆ Has the correct Certificate been uploaded to Citrix Netscaler?
 - ◆ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?

41 Sentry SSO with CitrixNetscaler

41.1 Introduction

This article explains how to integrate a Citrix Netscaler with Sentry via SAML.

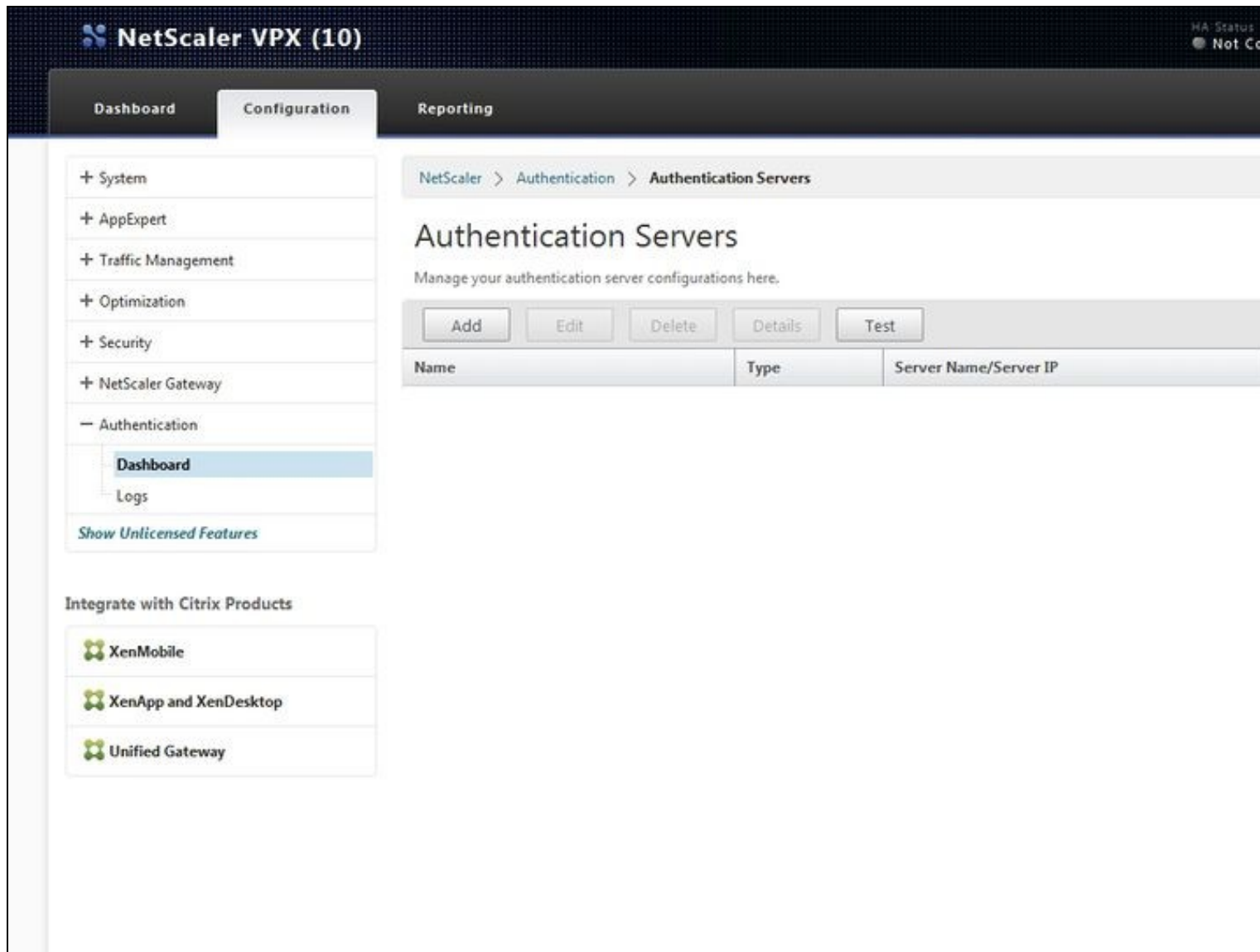
It assumes knowledge of how to configure the Netscaler and that a Virtual Server has been already created, missing just the SAML authentication configuration.

41.2 Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on your Netscaler Citrix account, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

41.3 Setup SAML SSO on Citrix Netscaler

To configure SAML SSO setting on your Citrix Netscaler account you have to access your Admin console. You should see an Admin console with an option "Authentication > Dashboard" similar to the one below:



On the Authentication Servers screen when you click on the Add button you will be shown a create authentication server screen with Choose Server Type options where you have to click on "SAML".

DashboardConfigurationReporting

Back

Configure Authentication SAML Server

Name

SAML_test

Authentication Type

SAML

IDP Certificate Name*

sentry-rsa-cert

+

Redirect URL*

http://192.168.11.115:8084/sentry/sai

Single Logout URL

http://192.168.11.115:8084/sentry/sir

User Field

Signing Certificate Name

Issuer Name

citrix.swivelsecure.com

Reject Unsigned Assertion*

OFF

SAML Binding*

POST

?

Default Authentication Group

local

Two Factor

☐ ON ☒ OFF

Assertion Consumer Service Index

255

Attribute Consuming Service Index

255

Requested Authentication Context*

Exact

You will have to enter a name for the Authentication SAML Server and fill in the details for your AuthControl Sentry such as:

IDP Certificate Name - Click on + and a screen like the one displayed below should be displayed. Browse to the RSA PEM files created earlier to upload the certificate and select PEM as a Certificate Format:

Install Certificate

Certificate-Key Pair Name*

sentry-rsa-cert

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name*

rsacert.pem

Browse ▼ +

Key File Name

rsaprivkey.pem

Browse ▼ +

Certificate Format

☒ PEM ☐ DER

Password

••••••••

☐ Certificate Bundle

☒ Notify When Expires

Notification Period

30

Install Close

After you have entered all the certificate details click Install

Set the Redirect and Single Logout below, where <FQDN_OF_SENTRY_SERVER> is the public DNS entry of your Swivel AuthControl Sentry server, e.g. swivel.mycompany.com or if you do not have a redirect from port 443 to 8443 in place, you may need to include a port number e.g. swivel.mycompany.com:8443

Redirect URL - *https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint*

Single Logout URL - *https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout*

Issuer Name - *E.g. citrix.companyname.com*

(The value set in here will be used to configure the Citrix Netscaler application on AuthControl Sentry)

Signature Algorithm - RSA-SHA1

Digest Method - SHA1

After you have entered all the details click Create

Now the SAML authentication server has been created. To configure the Virtual Server used to log in to use SAML authentication, select Netscaler Gateway > Virtual Servers and click Edit. You should see a screen like the below:

Dashboard

Configuration

Reporting

← Back

VPN Virtual Server

Basic Settings

Name Demo
IPAddress 10.40.242.185
Port 443
State ● Up
RDP Server Profile -
Login Once false
Double Hop false
Down State Flush true
DTLS false
AppFlow Logging false

Maximum Users 0
Max Login Attempts -
Failed Login Timeout -
ICA Only true
Enable Authentication true
Windows EPA Plugin Upgrade -
Linux EPA Plugin Upgrade -
Mac EPA Plugin Upgrade -
ICA Proxy Session Migration false
Enable Device Certificate false

Certificates

1 Server Certificate

1 CA Certificate

Authentication

Primary Authentication

1 SAML Policy

Profiles

Net Profile -
TCP Profile -
HTTP Profile nshttp_default_strict_validation

Published Applications

No Next HOP Server

1 STA Server

No Url

To add the SAML authentication server click + on the Authentication section. Select as Policy SAML and type Primary. Click the Continue button.

Choose Type

Choose Type

Policies

Choose Policy*

SAML

Choose Type*

Primary

Continue

Cancel

The below screen will be displayed. Click + to add Add Binding:

Choose Type

Choose Type

Policies

Choose Policy

SAML

Choose Type

Primary

Add Binding

Unbind

Edit

Priority

Policy Name

Expression

Click + add to add a new Policy Binding:

Choose Type > Policy Binding

Policy Binding

Select Policy*

Click to select

>

+

✍

Binding Details

Priority*

110

Bind

Close

Set a name for the SAML policy, select the SAML server configured before and add on Expression ns_true.

Choose Type > Policy Binding > Configure Authentication SAML Policy

Configure Authentication SAML Policy

Name
SAML_policy

Authentication Type
SAML

Server*
SAML_test

Expression*
Operators Saved Policy Expressions Frequently Used Expressions
ns_true

OK Close

After those parameters has been set click the Create button. Then the policy bind screen will be displayed again with the new policy selected.

Choose Type > Policy Binding

Policy Binding

Select Policy*
SAML_policy

More

Binding Details

Priority*
110

Bind Close

Click Bind. The below screen will be displayed.

Choose Type

Choose Type

Policies

Choose Policy
SAML

Choose Type
Primary

Add Binding

Unbind

Edit

Priority	Policy Name	Expression
110	SAML_policy	ns_true

Close

Click the Close button. The virtual server will have now the SAML authentication set. Click the back button and save the current configuration.

41.4 Configure Check Password with Repository on the Swivel Core

In order to check the user's Active Directory password, ensure that the local Agent is configured as explained [here](#)

41.5 Importing your users into the Swivel Core

Before we are able to proceed with testing SSO authentication to Citrix Netscaler via Swivel AuthControl Sentry we need to ensure that there are users imported that we can test with.

Ensure that you have setup and configured a repository under the Repository -> Server and Repository -> Name of your repository menus on the Swivel Core.

Select the Repository on the User Administration screen, and click the User Sync button. For the user you are going to test with, ensure that you have set their PIN using the Reset PIN button.

41.6 Setup AuthControl Sentry Application definition

Please note: you must have setup a Citrix Netscaler SAML SSO prior to defining this Application entry within AuthControl Sentry. This is so that you are able to populate the Endpoint URL field. Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for Google, click the Add Provider button.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is configured to use SAML (Security Assertion Markup Language) request.

Name

CitrixNetscaler

Image

CitrixNetscaler.png



Points

0

Portal URL

https://citrix.yourdomain

Endpoint URL

Entity ID

citrix.yourdomain

Federated Id

email

Save

Name: Citrix Netscaler(Type an Arbitrary name for this Application)

Service Provider: CitrixNetscaler(select from dropdown list)

Points: 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)

Endpoint URL: (this Endpoint URL is your companies Citrix Netscaler URL which you can usually access on: <https://citrix.mycompanyname.com>)

Entity ID: citrix.mycompanyname.com (This is the Issuer Name configured on Citrix Netscaler SAML server)

41.7 Setup AuthControl Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for Citrix Netscaler SAML authentication.

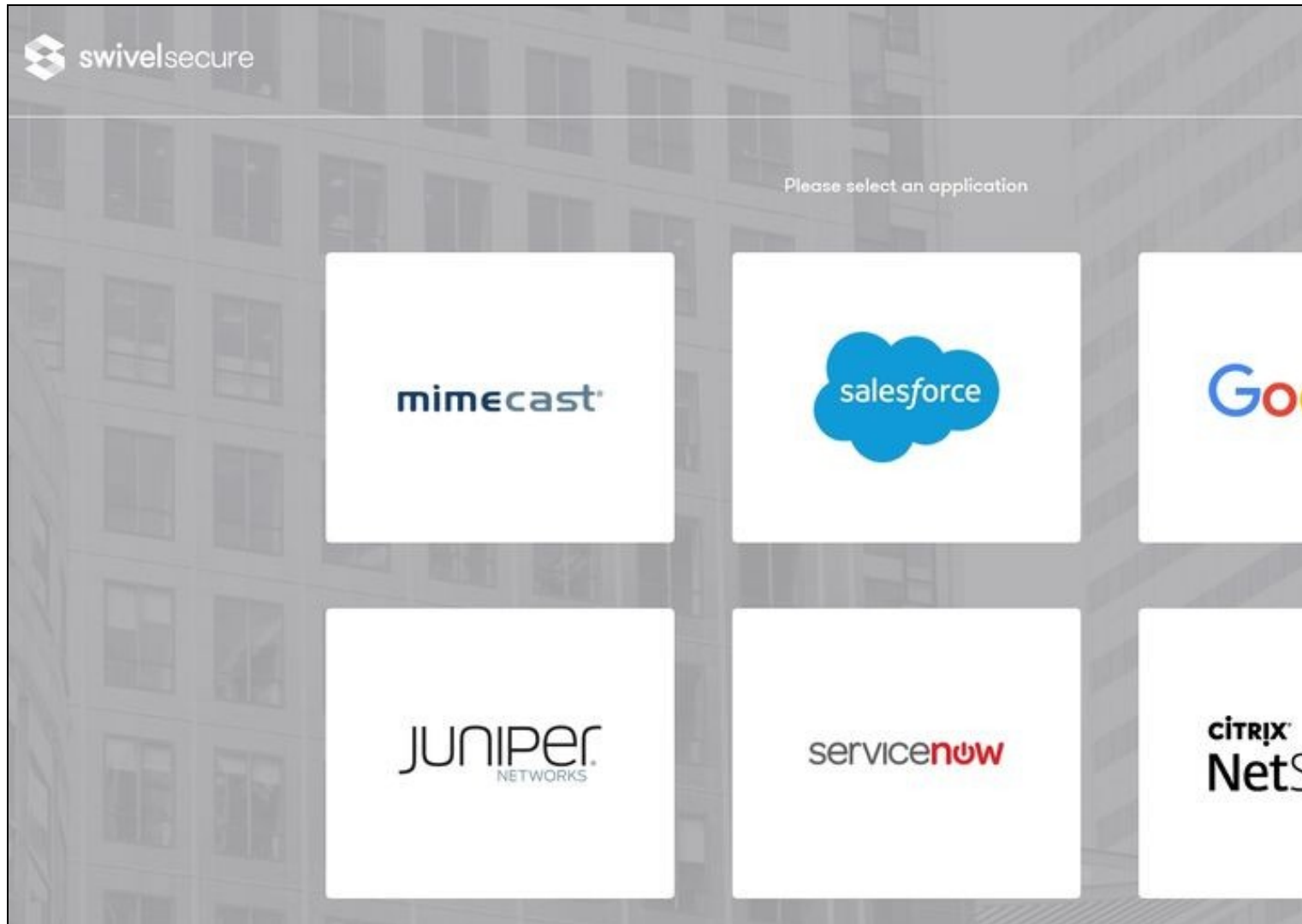
Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Google Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

41.8 Testing authentication to Google via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

In a web browser, visit the the URL that you setup on AuthControl Sentry as Endpoint URL e.g. <https://citrix.mycompanyname.com>

Alternatively you can visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. <https://mycompanysentrydomain/sentry/startPage> On a Start Page you will be able to see a new Google Icon on which you can click and proceed with authentication (as you would by going straight to the Citrix Netscaler page)



When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Citrix Netscaler Application definition.

The image shows a Citrix NetScaler login interface. At the top, there is a white circular logo with the text "CITRIX NetScaler". Below the logo is a white rectangular box containing a text input field with the username "lmorales". Underneath the input field are two purple buttons with white text: "Submit" and "Reset". The background is a grayscale image of a modern building with many windows.

CITRIX
NetScaler

lmorales

Submit

Reset

After we enter the username we are prompted with another authentication method (in this example we use turing)

Imorales

Password

OTC

TURing



1	2	3	4	5	6	7	8	9	0
9	0	4	8	3	1	7	2	6	5

Login

Refresh Image

After we enter our authentication credentials we successfully will see the web app that we tried to access.

41.9 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from Citrix Netscaler and can be useful for comparison with the Netscaler Citrix SAML Assertion Validator output;

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

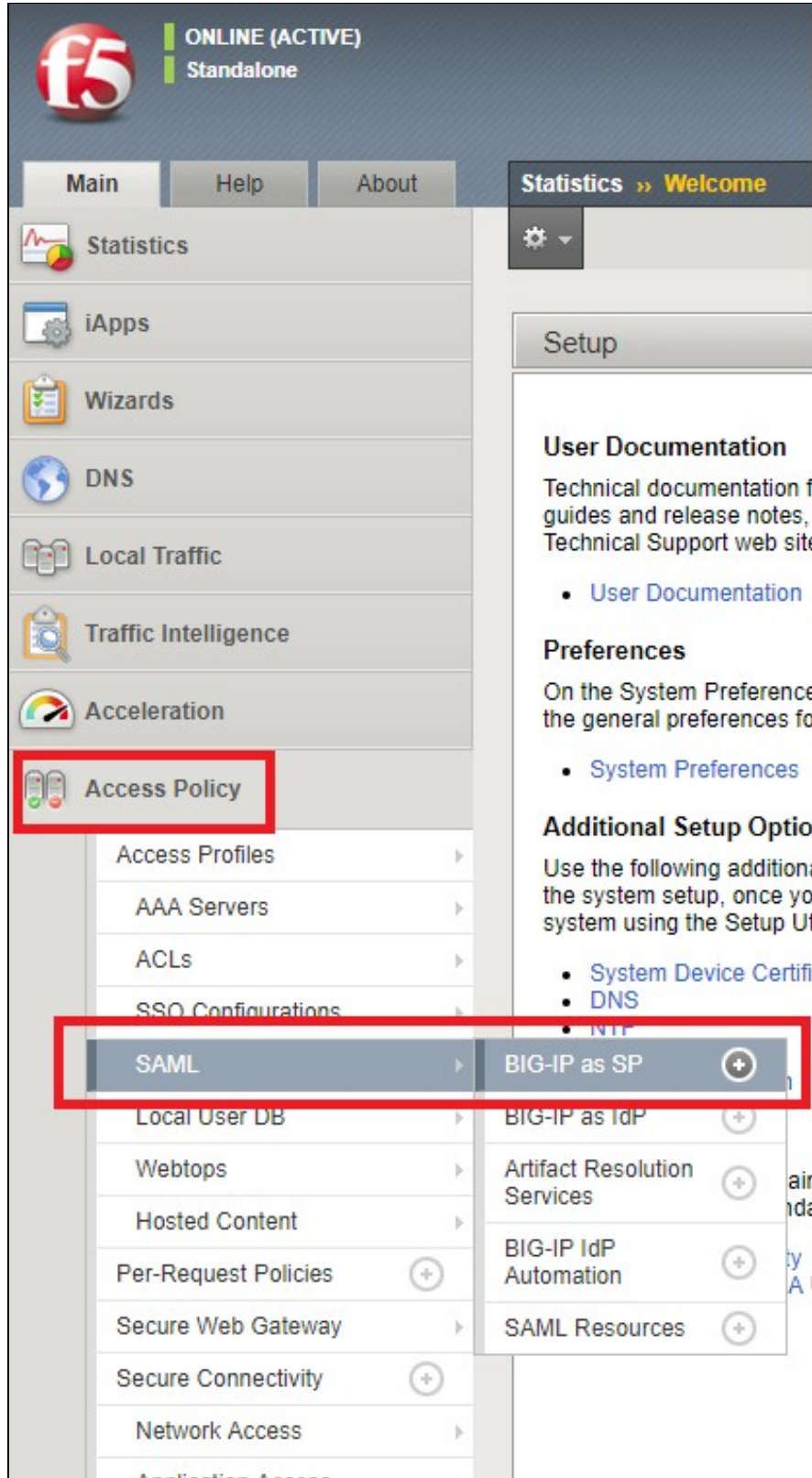
Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ◆ Can AuthControl Sentry find the Certificate locally, is it the correct one?
 - ◆ Has the correct Certificate been uploaded to Citrix Netscaler?
 - ◆ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?

42 Sentry SSO with F5

42.1 Setup SSO on F5

From the F5 BIG-IP Configuration page, select Access Policy -> SAML -> BIG-IP as SP.



Choose External IdP Connectors and click in Create -> From Metadata



Here you will need to import the IdP Metadata file that you can download from Sentry SSO administration console or directly from the url: https://<sentry_URL>/sentry/metadata.

Click browse to upload the file and enter a name for the Identity Provider Name.

Create New SAML IdP Connector

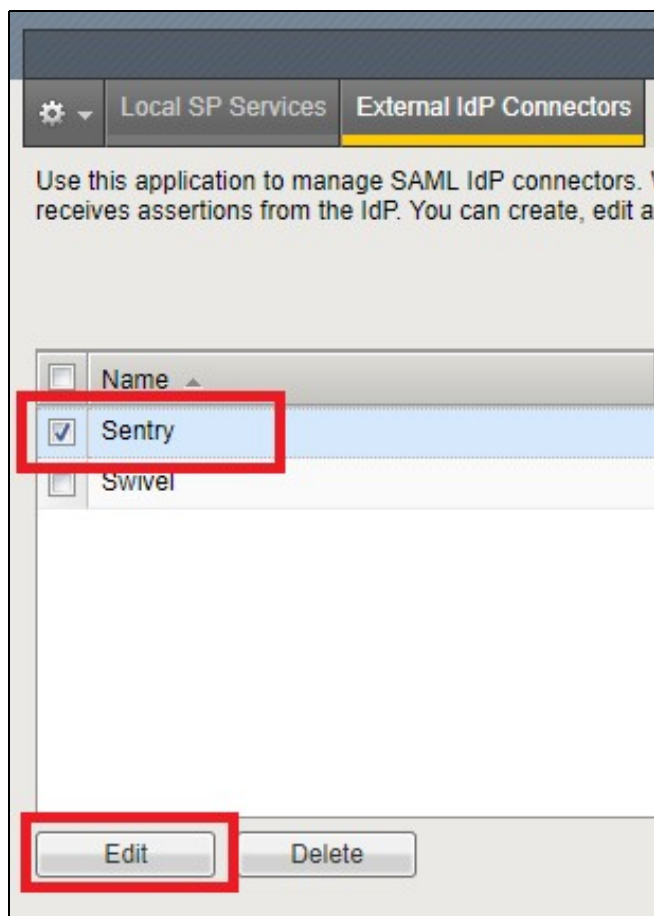
Select File*:
generatedMetadata.xml Browse

Identity Provider Name*:
Sentry

Select Signing Certificate :
Select a value...

OK Cancel

After the connector is created, select it from the list and click Edit.



Select Security Settings, activate 'Must be signed?', select the Signing Algorithm 'RSA-SHA256' and click OK.

Edit SAML IdP Connector

- General Settings
- Endpoint Settings
- Single Sign On Service ...
- Artifact Resolution Servi...
- Assertion Settings
- Security Settings**
- SLO Service Settings

Authentication Request sent by this device to IdP

☒ Must be signed
Signing Algorithm :
RSA-SHA256

Certificate Settings
IdP's Assertion Verification Certificate :
/Common/Sentry__saml_idp_metadata_cert.crt

☐ Detach signature when using redirect binding

OK

Select Local SP Services and click Create

Access Policy >> SAML : BIG-IP as SP

Local SP Services

External IdP Connectors

☐

Name ▲

SAML IdP Connectors

Description

Partition

Create

In General Settings, enter a name for the SP service, in the Entity ID enter your F5 URL e.g. https://F5_HOSTNAME, and click OK.

Create New SAML SP Service

☒ General Settings
 ☐ Endpoint Settings
 ☒ Security Settings
 ☐ Advanced Settings

Name*:
SwivelSentry

Entity ID*:
https://f5url.com

SP Name Settings

Scheme : Host :

Description :

Relay State :

After the SP Service is created, select it and click in Bind/Unbind IdP Connectors.

Access Policy » SAML : BIG-IP as SP

☒ Local SP Services
 ☐ External IdP Connectors

<input checked="" type="checkbox"/>	Name	SAML IdP Connectors	Description	Partition
<input checked="" type="checkbox"/>	SwivelSentry			Common

Click ?Add New Row? and select under SAML IdP Connectors, the one that you have previously created. For Matching Source, Select `%{session.server.landingurl}` and for Matching Value enter a custom path for the login url e.g. `/ or /PATH`. Click Update to save and then click Ok.

Edit SAML IdP's that use this SP

IdP Connectors associated with this SP Service

Add New Row

Create New IdP Connector

SAML IdP Connectors	Matching Source	Matching Value
/Common/Sentry	%{session.server.landinguri}	/

Edit

Delete

OK

Cancel

With the External IdP Connector and the Local SP Service configured, you can now change your existing Access Profile.

Go to Access Policy -> Access Profiles -> Access Profiles List and edit the Access Profile that you want to change or create a new one

Access Policy » Access Profiles : Access Profiles List

Access Profile List

Access Policy Sync

CAPTCHA Configuration List

NTLM

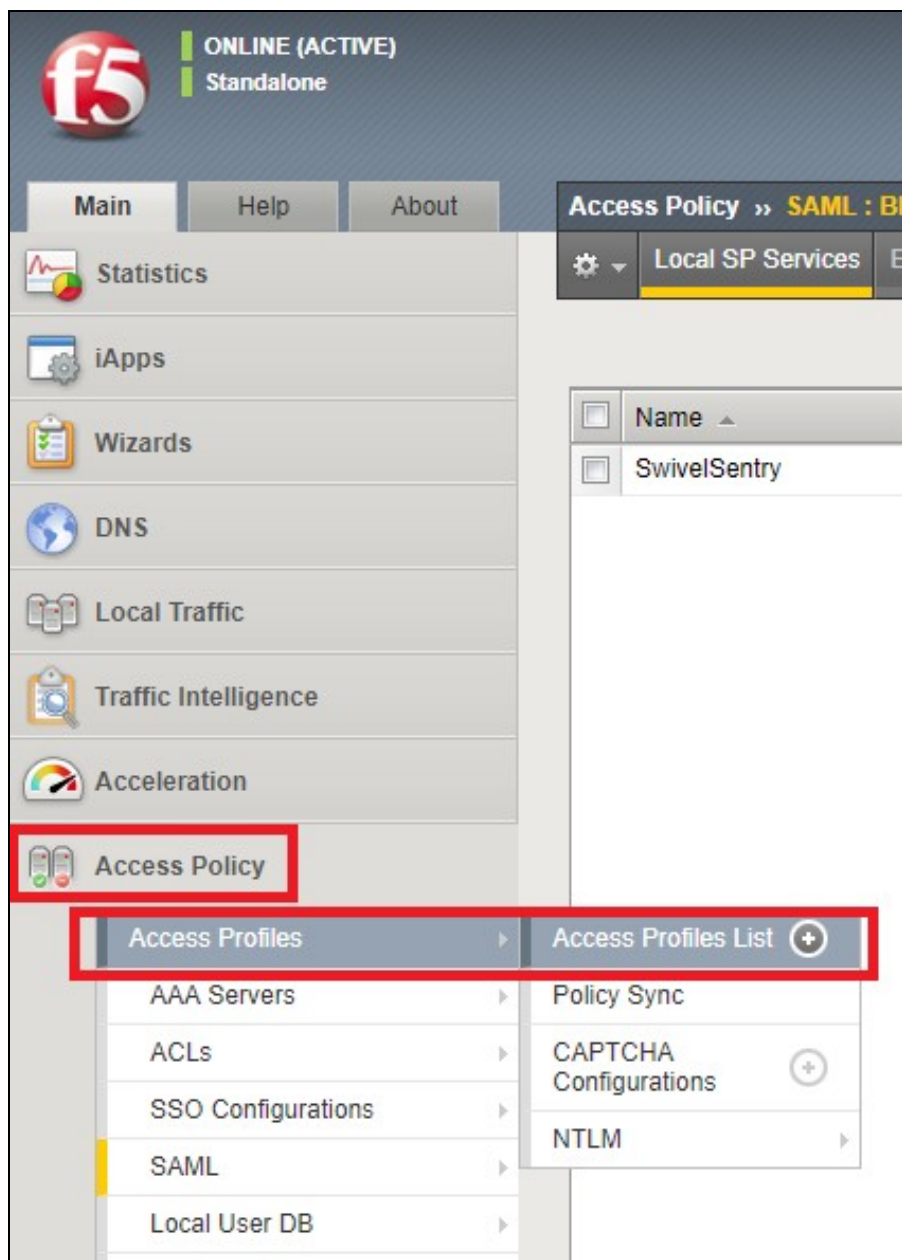
*

Search

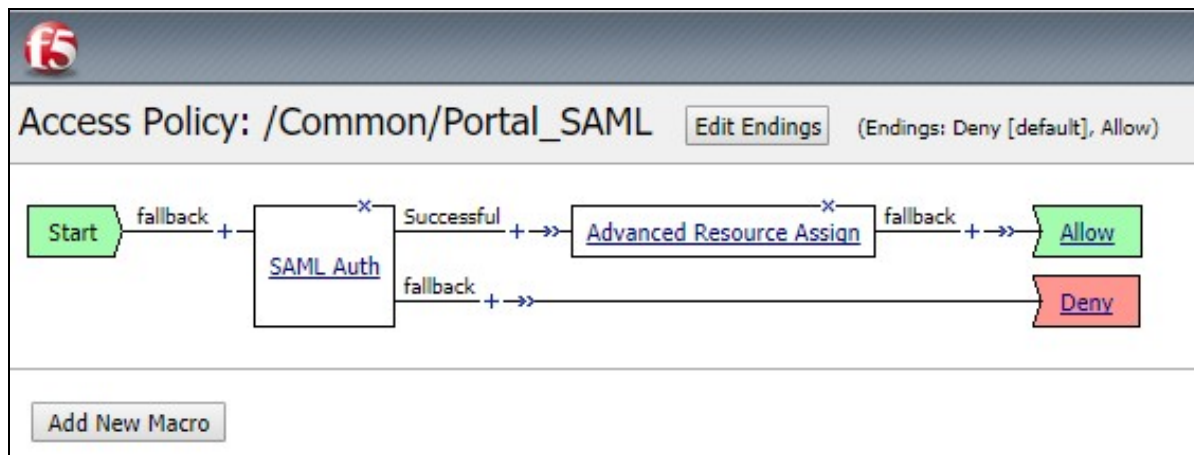
<input checked="" type="checkbox"/>	Status	Name	Application	Profile Type
<input type="checkbox"/>		Portal_SAML		All
<input type="checkbox"/>		Portal_demo		All
<input type="checkbox"/>		access		All

Delete...

Apply Access Policy



You need to configure your Access Policy in order to have the following actions:




Click in the SAML Auth Action to change the properties and change the AAA server to the previously created SP Service.

The screenshot shows the F5 configuration interface for SAML Authentication SP. The 'Branch Rules' tab is selected. The 'Name' field is 'SAML Auth'. The 'AAA Server' dropdown is set to '/Common/SwivelSentry'. The 'Save' button is highlighted with a red box.

42.2 Setup Sentry Application Definition

First we should upload the F5 logo. Find it using a Google Images search or copy it from here:



 swivelsecure

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions




User History

Log Viewer

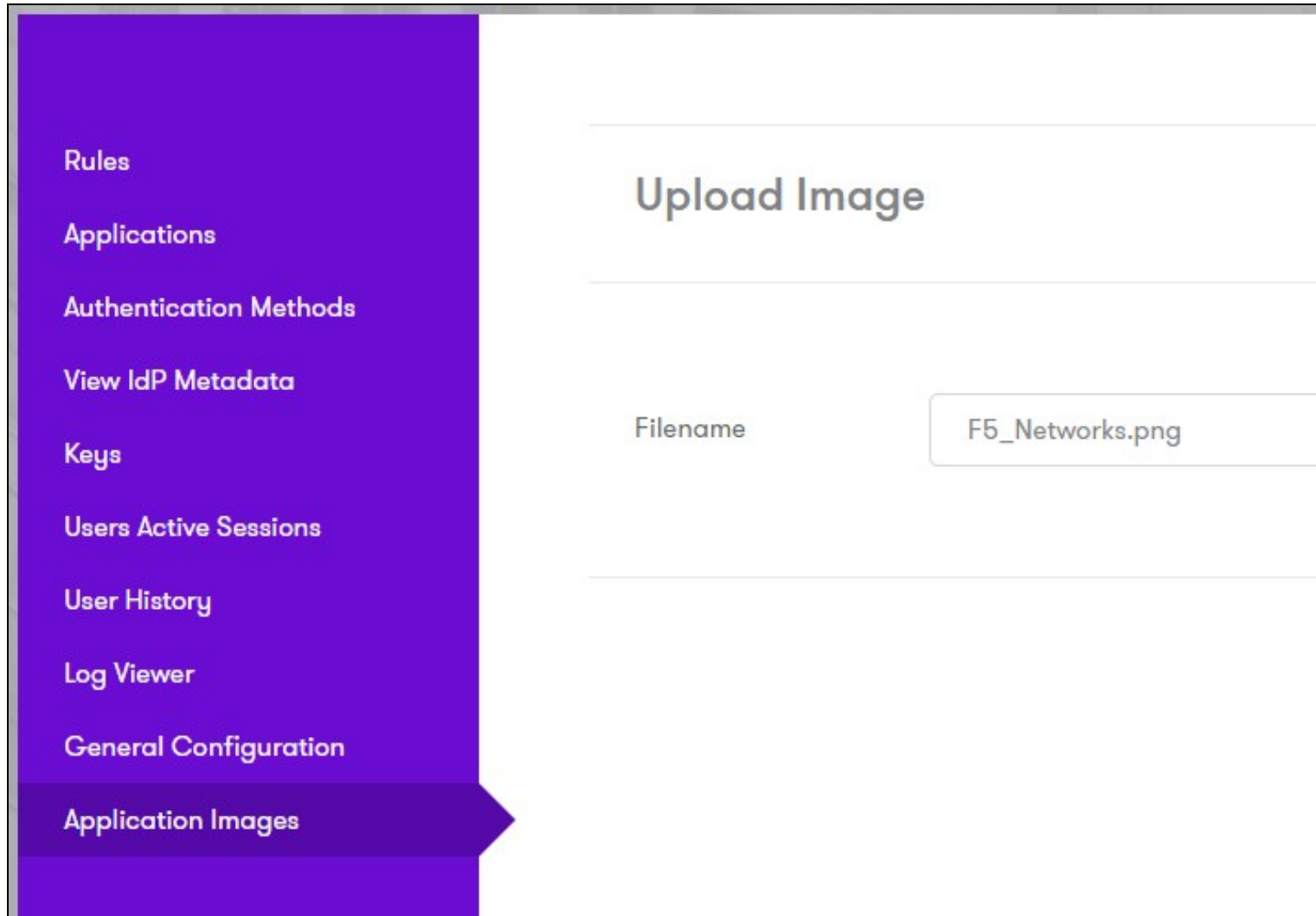
General Configuration

Application Images

Application Images

Image	Name
 <div>Microsoft Active Directory Federation Services</div>	ADFS.png
	Cisco.png
	CitrixNet.png

Browse to the Logo file you have saved:



Then upload the image to the Sentry application and the image should now be available to select, when we go to create a new Application definition for JIRA.

Login to the AuthControl Sentry Administration Console. Click Applications in the left-hand menu. To add a new Application definition for JIRA, click the Add Application button and select SAML - Other type.

[Rules](#)[Applications](#)[Authentication Methods](#)[View IdP Metadata](#)[Keys](#)[Users Active Sessions](#)[User History](#)[Log Viewer](#)[General Configuration](#)[Application Images](#)

Application Types

RADIUS VPN - Cisco ASA

✓Se

RADIUS VPN - Citrix Netscaler

✓Se

RADIUS VPN - Juniper

✓Se

RADIUS VPN - Other

✓Se

SAML - ADFS

✓Se

SAML - Citrix Netscaler

✓Se

SAML - GoToMeeting

✓Se

SAML - Google

✓Se

SAML - Mimecast

✓Se

SAML - Office 365

✓Se

SAML - OneLogin

✓Se

SAML - Other

✓Se

SAML - PulseSecure

✓Se

SAML - Salesforce

✓Se

SAML - ServiceNow

✓Se

SAML - SonicWall

✓Se

Name: **F5**

Points: 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)

Portal URL: URL to access to F5. The PATH needs to match the Matching Value for the previously created SP Service e.g.
`https://F5_HOSTNAME/PATH`

Endpoint URL: Leave blank - not required

Entity ID: Identifier of the F5 SAML request. It needs to match the Identifier for the previously created SP Service. e.g. `https://F5_HOSTNAME`

Federated Id: email

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is enabled for SAML (Security Assertion Markup Language) request.

Name

F5

Image

F5_Networks.png



Points

100

Portal URL

https://f5url.com/

Endpoint URL

Entity ID

https://f5url.com/

Federated Id

email

Save


42.3 Testing authentication to Salesforce via Swivel Sentry

This should be the final step after all previous elements have been configured.

Visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. <https://mycompanysentrydomain/sentry/startPage>. On a Start Page you will be able to see a new F5 Icon on which you can click and proceed with authentication (as you would by going straight to the F5 page)



When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup. You should be presented with the Sentry username page.



A login form for F5. It features a white rectangular box centered on a gray background with a faint building pattern. At the top of the box is the F5 logo, which consists of a red circle containing the white text 'f5'. Below the logo is a white rectangular input field with the placeholder text 'Username'. Underneath the input field are two purple rounded rectangular buttons. The left button is labeled 'Submit' and the right button is labeled 'Reset' in white text.

Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the F5 Application definition.

After you enter your authentication credentials you will login into the VPN.

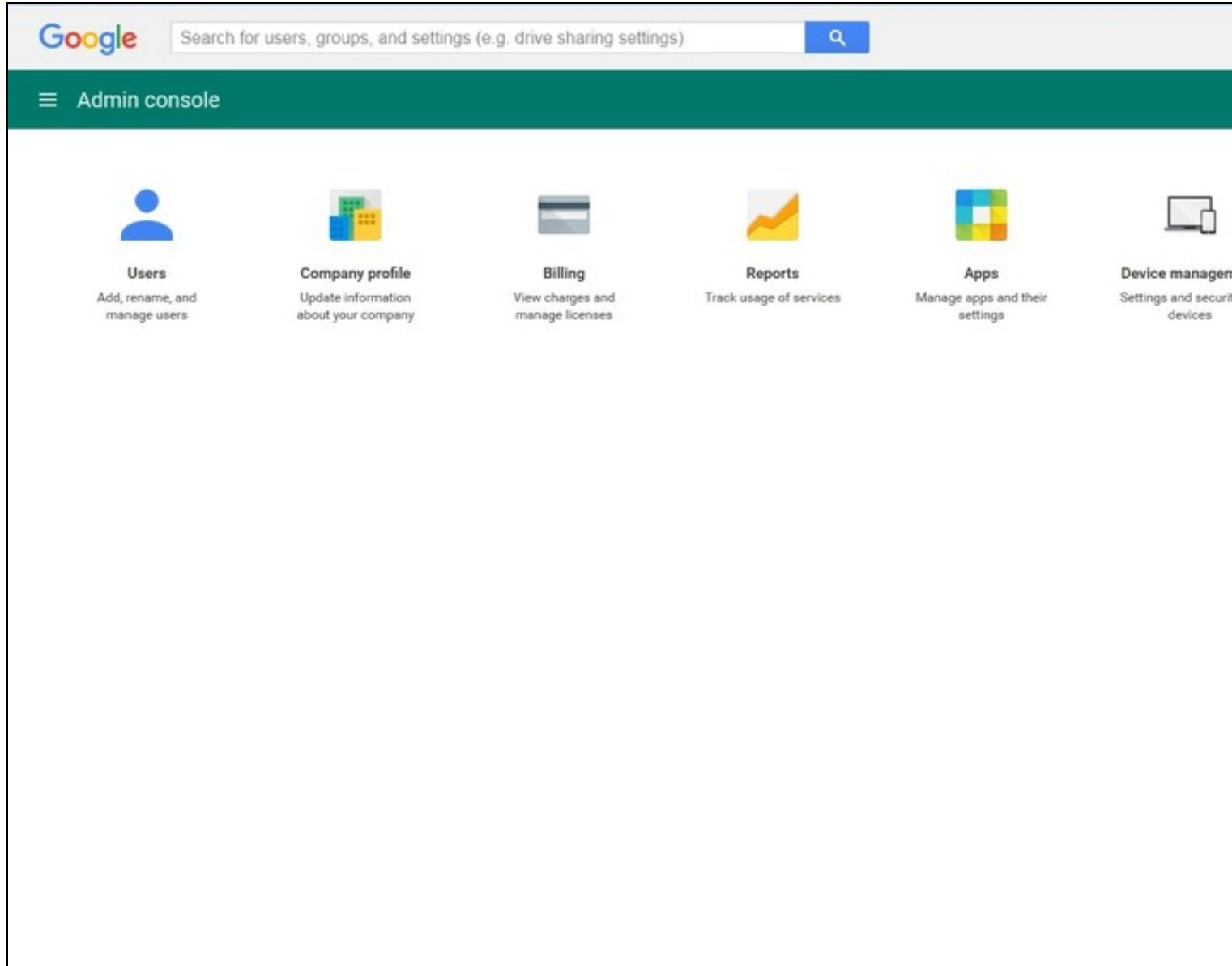
43 Sentry SSO with GoogleApps

43.1 Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on Google.com, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

43.2 Setup SSO on Google

To configure SSO setting on your Google Business account you have to access your Admin console by simply going to <https://admin.google.com/AdminHome> or by following https://google.co.uk/*Your Company Name*/ You should see an Admin console with an option "Security" similar to the one below:



When you click on the Security you will be shown security options where you have to click on "Set up single sign-on (SSO)".

The screenshot shows the Google Admin console's Security settings page. The left sidebar has a 'Security' header. The main content area is titled 'users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop POP access to Gmail, users must sign in directly with the username and password set up via the Admin console.' Below this, there are two main sections for SSO setup. The first section, 'Setup SSO with Google identity provider', is currently selected. It contains fields for 'SSO URL' (https://accounts.google.com/o/saml2/idp?idpid=C0184cgt4) and 'Entity ID' (https://accounts.google.com/o/saml2?idpid=C0184cgt4), both with 'DOWNLOAD' buttons. The second section, 'Setup SSO with third party identity provider', is marked with a checked checkbox. It contains fields for 'Sign-in page URL' (http://192.168.11.114:8083/sentry/saml20endpoint), 'Sign-out page URL' (http://192.168.11.114:8083/sentry/singlelogout), and 'Change password URL' (http://www.google.com). There is also a 'Verification certificate' section showing a message 'A certificate file has been uploaded. Replace certificate' and a checkbox for 'Use a domain specific issuer'. At the bottom, there is a 'Network masks' section with explanatory text.

You will have to click on the checkbox "Setup SSO with third party identity provider" and fill in the details for your AuthControl Sentry such as:

Set the Login, Logout and Change password URLs below, where <FQDN_OF_SENTRY_SERVER> is the public DNS entry of your Swivel AuthControl Sentry server, e.g. swivel.mycompany.com or if you do not have a redirect from port 443 to 8443 in place, you may need to include a port number e.g. swivel.mycompany.com:8443

Sign-in page URL - `https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint`

Sign-out page URL - `https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout`

Change password URL - `http://www.google.com`

Verification certificate - Browse to the RSA PEM file created earlier to upload the certificate. When you click save, if successfully imported you will see a popup message saying "Your settings have been saved."

After you have entered all the details as below click Save

43.3 Configure Check Password with Repository on the Swivel Core

In order to check the user's Active Directory password, ensure that the local Agent is configured as explained [here](#)

43.4 Setup AuthControl Sentry Application definition

Please note: you must have setup a Google SSO prior to defining this Application entry within AuthControl Sentry. This is so that you are able to populate the Endpoint URL field. Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for Google, click the Add Provider button.

Rules

Applications

Authentication Methods

View IDP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not enabled for the SAML (Security Assertion Markup Language) request.

Name

Google Apps Suite

Image

Google.png



Google

Points

0

Portal URL

https://docs.google.com/a/mycompanyname

Endpoint URL

Entity ID

google.com

Federated Id

email

- **Name:** Google
- **Image:** Google.png (selected by default)
- **Points:** 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)
- **Endpoint URL:** N/A
- **Portal URL:** (this Portal URL is your companies google docs URL which you can usually access on: <https://docs.google.com/a/mycompanyname>)
- **Entity ID:** google.com (at the time of writing this documentation, this settings is always the same when using Google, but may be subject to change by Google.com, so please review the online Google documentation if you find that this Entity ID no longer works)
- **Federated id:** email

43.5 Setup AuthControl Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for Google authentication.

Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Google Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

43.6 Testing authentication to Google via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

In a web browser, visit the the URL that you setup on AuthControl Sentry as Endpoint URL e.g. <https://docs.google.com/a/mycompanyname>

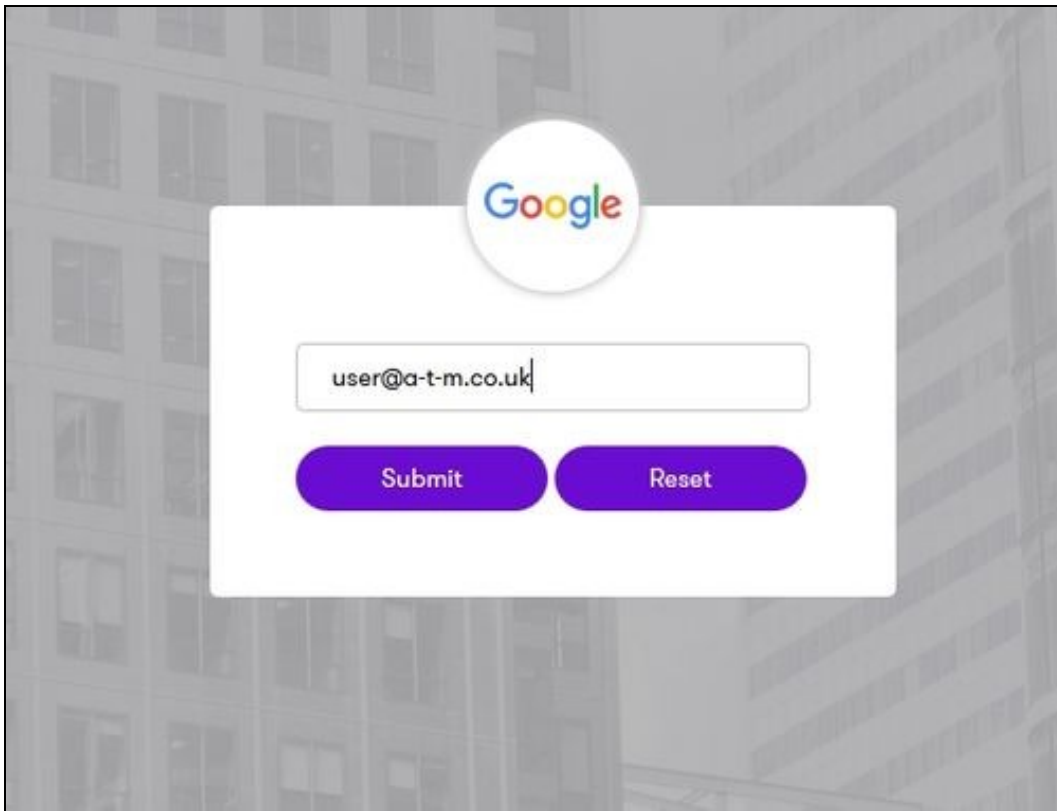
Alternatively you can visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. <https://mycompanysentrydomain/sentry/startPage> On a Start Page you will be able to see a new Google Icon on which you can click and proceed with authentication (as you would by going straight to the google page)

Please select an application

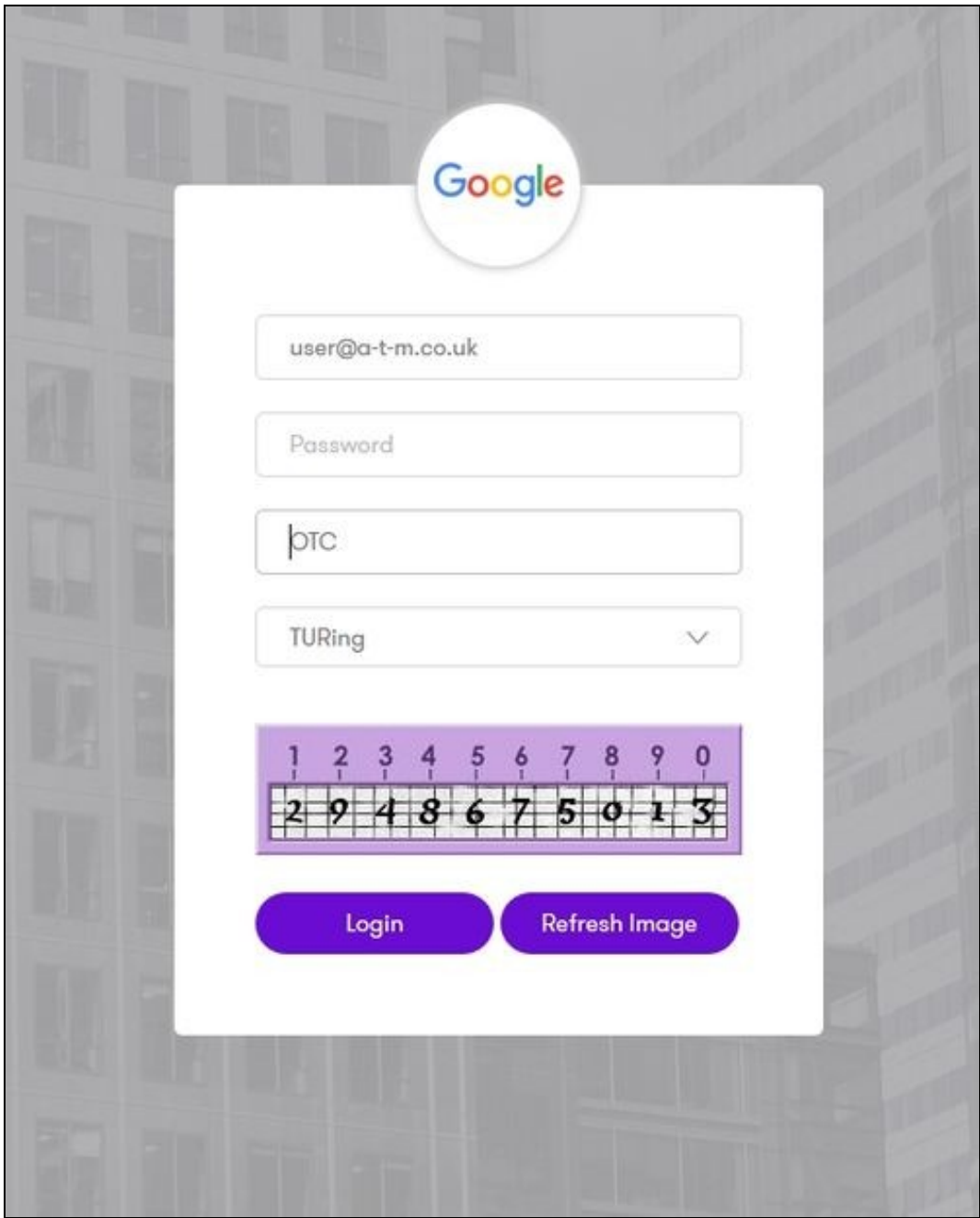
The Mimecast logo, consisting of the word 'mimecast' in a lowercase, sans-serif font.The Juniper Networks logo, with 'JUNIPER' in a large, bold, sans-serif font and 'NETWORKS' in a smaller, all-caps font below it.The ServiceNow logo, with 'servicenow' in a lowercase, sans-serif font, where 'now' is in red.

When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Google Application definition.

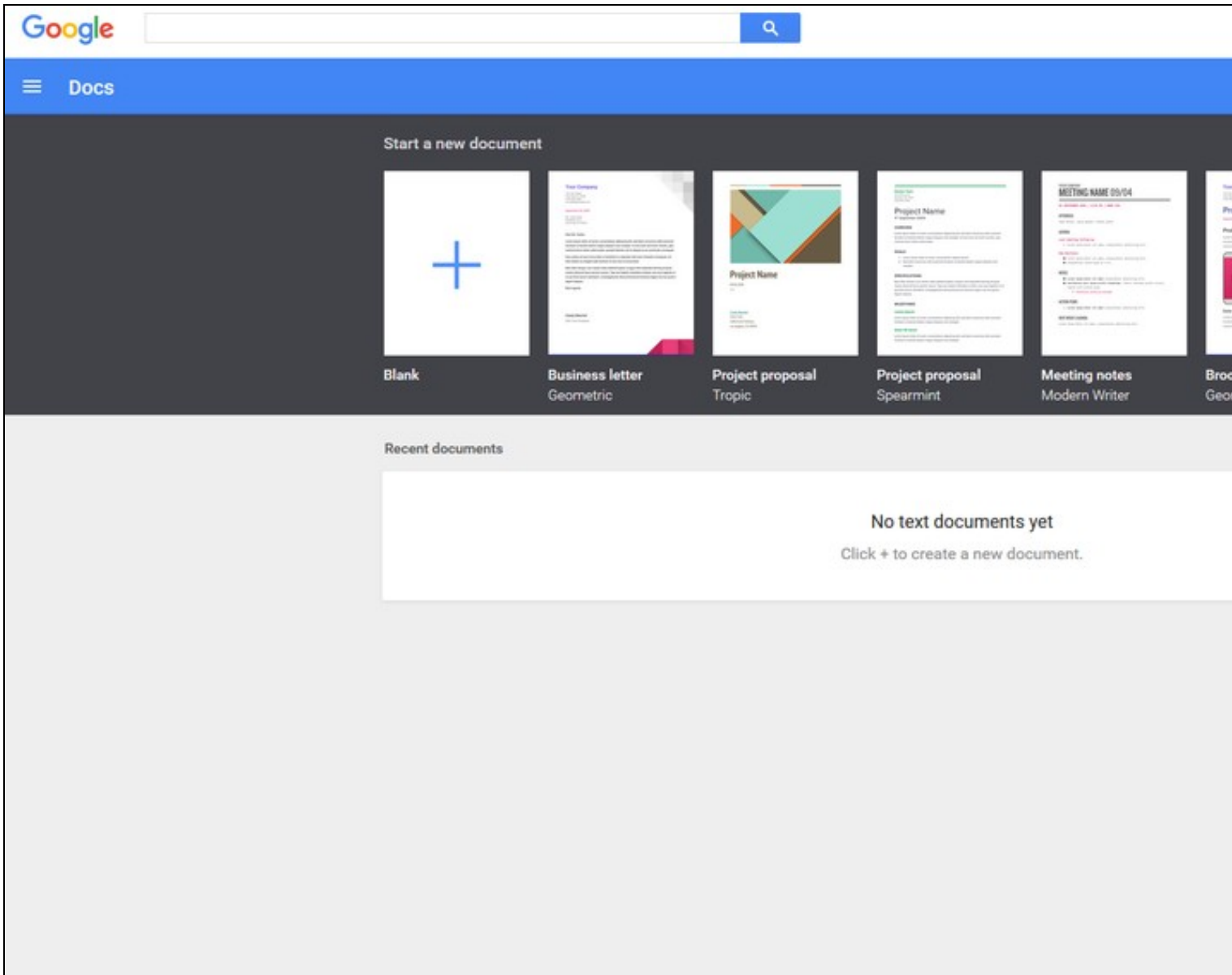
In this login example we are using the email as a username



After we enter the username we are prompted with another authentication method (in this example we use turing)



After we enter our authentication credentials we successfully will see the google docs that we tried to access.



43.7 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from Google and can be useful for comparison with the Google SAML Assertion Validator output;

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ◆ Can AuthControl Sentry find the Certificate locally, is it the correct one?
 - ◆ Has the correct Certificate been uploaded to Google.com?
 - ◆ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?

44 Sentry SSO with GoToMeeting

44.1 Introduction

This document describes how to configure GoToMeeting to work with Sentry SSO. Before following these instructions, you should be familiar with using Sentry - see the Sentry User Guide for more information.

44.2 Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on GoToMeeting.com, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

44.3 Setup SSO on GoToMeeting

To configure SSO setting on your GoToMeeting account you have to access your Admin console by simply going to <https://account.citrixonline.com/organization/administration/#identity>. You should see an Admin console with an option "Identity Provider" similar to the one below:

The screenshot shows the 'Identity provider' tab in the GoToMeeting Admin console. It features a header with 'Email domains' and 'Identity provider' tabs. Below the header, there is a descriptive paragraph about configuring SSO. A dropdown menu titled 'How would you like to configure your SAML IDP?' is set to 'Upload SAML metadata file'. Below this, there is a section titled 'Metadata file' with a text area labeled 'Paste or upload metadata xml'. At the bottom of the page, there is a footer with copyright information and links for Support, About Us, Terms of Service, and Privacy Policy.

Email domains Identity provider

To allow your users to log into Citrix products using sign in credentials you manage, you can configure your Identity Provider. Your users can log in either from the identity provider's website or from your Citrix product's website using the 'Use my credentials' form.

How would you like to configure your SAML IDP?

Upload SAML metadata file

Metadata file

Paste or upload metadata xml

© 2015 Citrix Systems, Inc. All rights reserved. Support | About Us | Terms of Service | Privacy Policy

Now navigate to your AuthControl Sentry View IdP Metadata page and copy the content of this page.

To allow your users to log into Citrix products using sign in credentials you manage, you can configure your Identity Provider. Your users can log in either from the identity provider's website or from your Citrix product's website using the 'Use my credentials' form.

How would you like to configure your SAML IDP?

Upload SAML metadata file



Metadata file

```
<?xml version="1.0" encoding="UTF-8"?>
<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="2017-10-11T14:16:57.864Z">
```

Click save. You will see something like the below. Click save again.

To allow your users to log into Citrix products using sign in credentials you manage, you can configure your Identity Provider. Your users can log in either from the identity provider's website or from your Citrix product's website using the 'Use my credentials' form.

How would you like to configure your SAML IDP?

Manual



Sign-in page url

https://192.168.11.114:8085/sentry/saml20endpoint

Sign-in binding: ☐ REDIRECT ☒ POST

Sign-out page url (optional)

https://192.168.11.114:8085/sentry/singlelogout

Sign-out binding: ☒ REDIRECT ☐ POST

Identity Provider Entity ID

https://192.168.11.114:8085/sentry/saml20endpoint

Verification certificate

```
-----BEGIN CERTIFICATE-----
MIID8TCCAtmgAwIBAgIJAKrFR9TiEnRAMA0GCSqGSIb3DQEBCwUAMIGOMQswCQYDVQQGEwJHQAjER
MA8GA1UECAwIV2V0aGVyYnkxETAPBgNVBACMCFdldGhlcmJ5MQ8wDQYDVQQKDAZTd2I2ZWwxDDAK
BgNVBAsMA2RldjEPMA0GA1UEAwwGc2VudHJ5MSkxJwYJKoZIhvcNAQkBFhpsLm1vcmFsZXNac3dp
dmVsc2VjdXJlLmNvbTAeFw0xNjA5MjkxMzQxMzlaFw0xNjEwMjkxMzQxMzlaMIGOMQswCQYDVQQG
EwJHQAjERMA8GA1UECAwIV2V0aGVyYnkxETAPBgNVBACMCFdldGhlcmJ5MQ8wDQYDVQQKDAZTd2I2
```

44.4 Setup AuthControl Sentry Application definition

Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for GoToMeeting, click the Add Application button and select SAML - GoToMeeting type.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is configured for SAML (Security Assertion Markup Language) request.

Name

GoToMeeting

Image

GoToMeeting.png



Points

0

Portal URL

https://login.citrixonline.com/saml/sp/client?se

Endpoint URL

Entity ID

https://login.citrixonline.com/saml/sp

Federated Id

email

Save

Points: 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)

Portal URL: URL to access to goToMeeting (It does not require modification)

Entity ID: Identifier of the GoToMeeting SAML request (It does not require modification)

Federated Id: email

Setup AuthControl Sentry Authentication definition

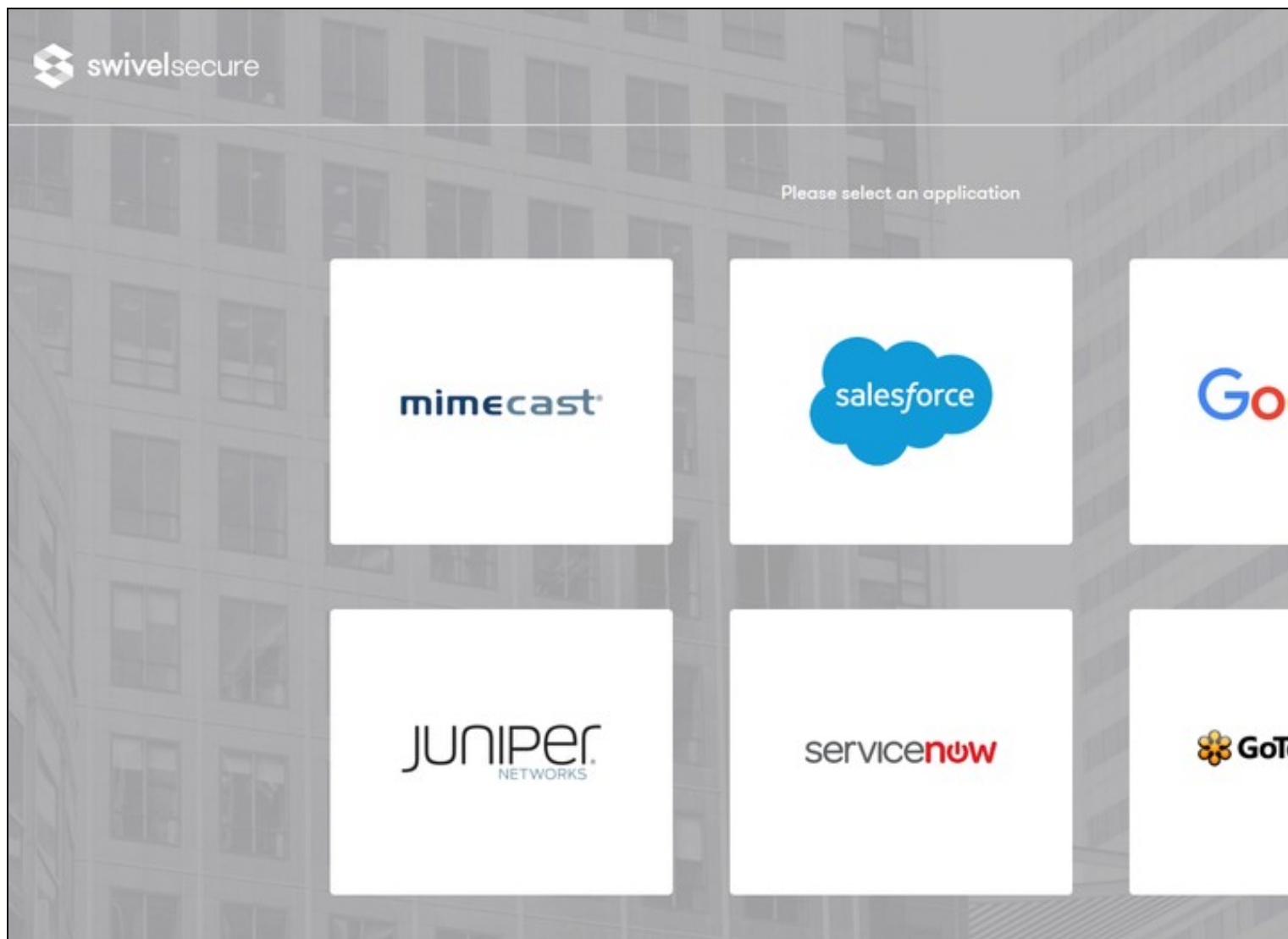
As an example here we will be using Turing authentication as the Primary method required for GoToMeeting authentication.

Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the GoToMeeting Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

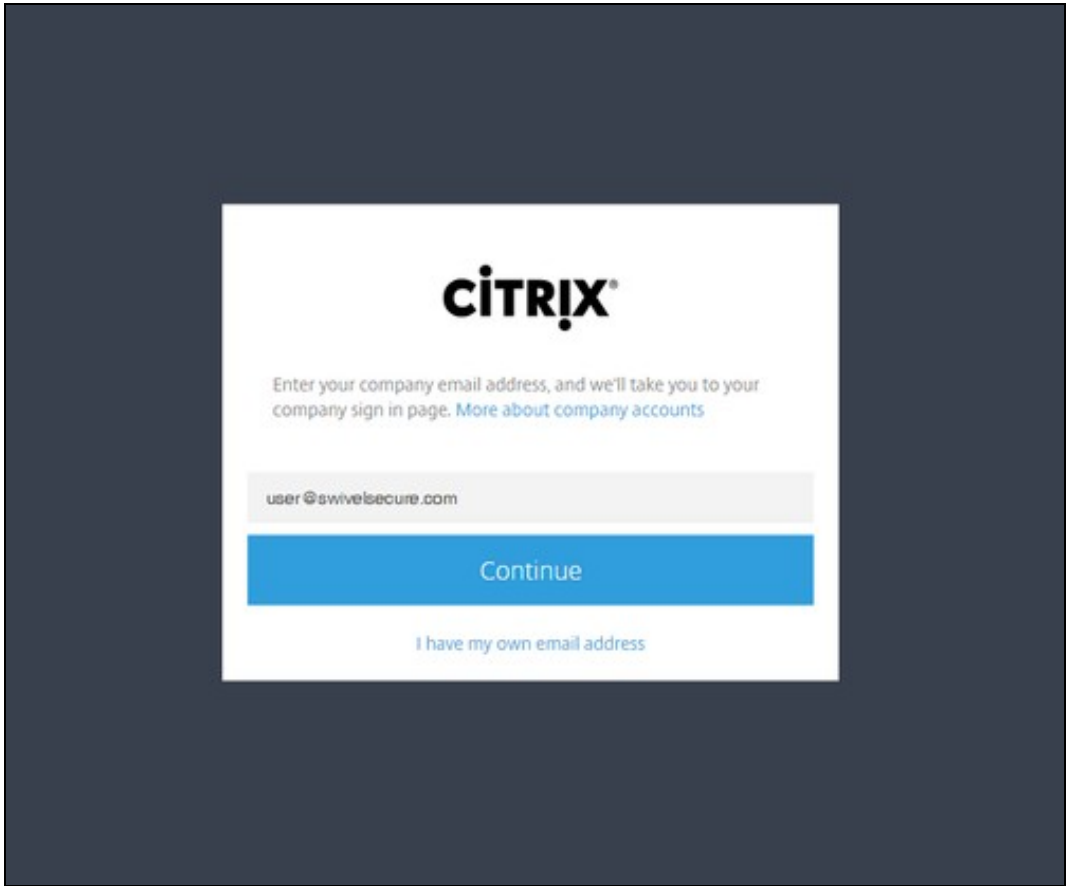
44.5 Testing authentication to Google via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

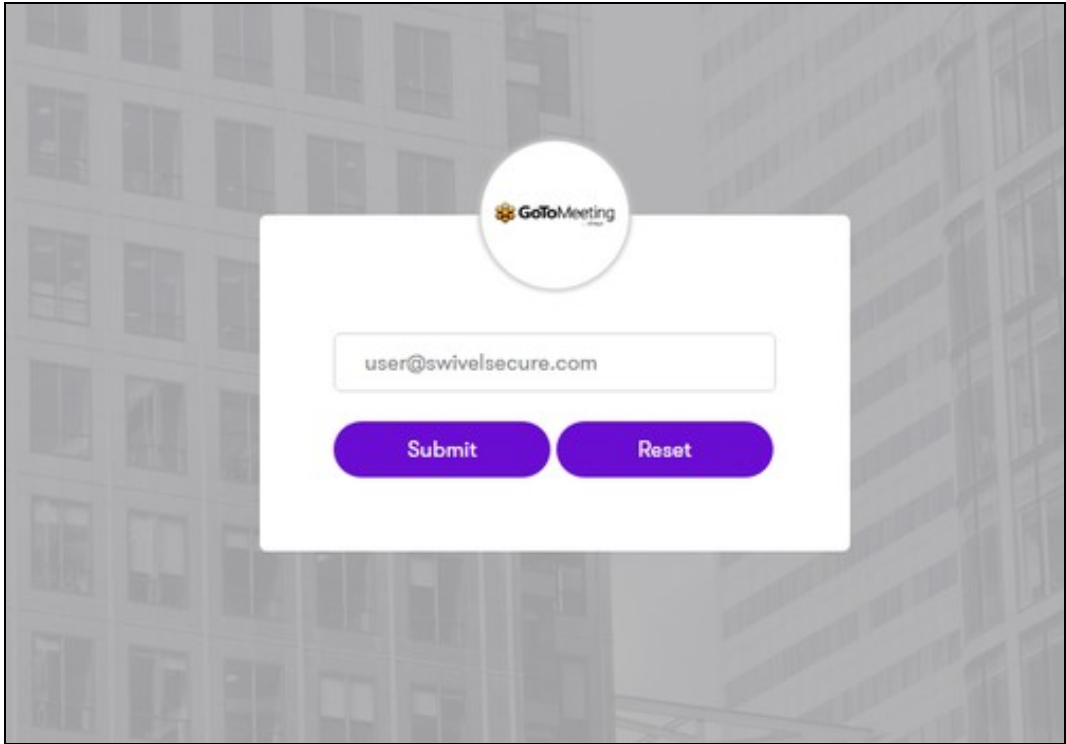
Visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. <https://mycompanysentrydomain/sentry/startPage>. On a Start Page you will be able to see a new GoToMeeting Icon on which you can click and proceed with authentication (as you would by going straight to the GoToMeeting page)



When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup.

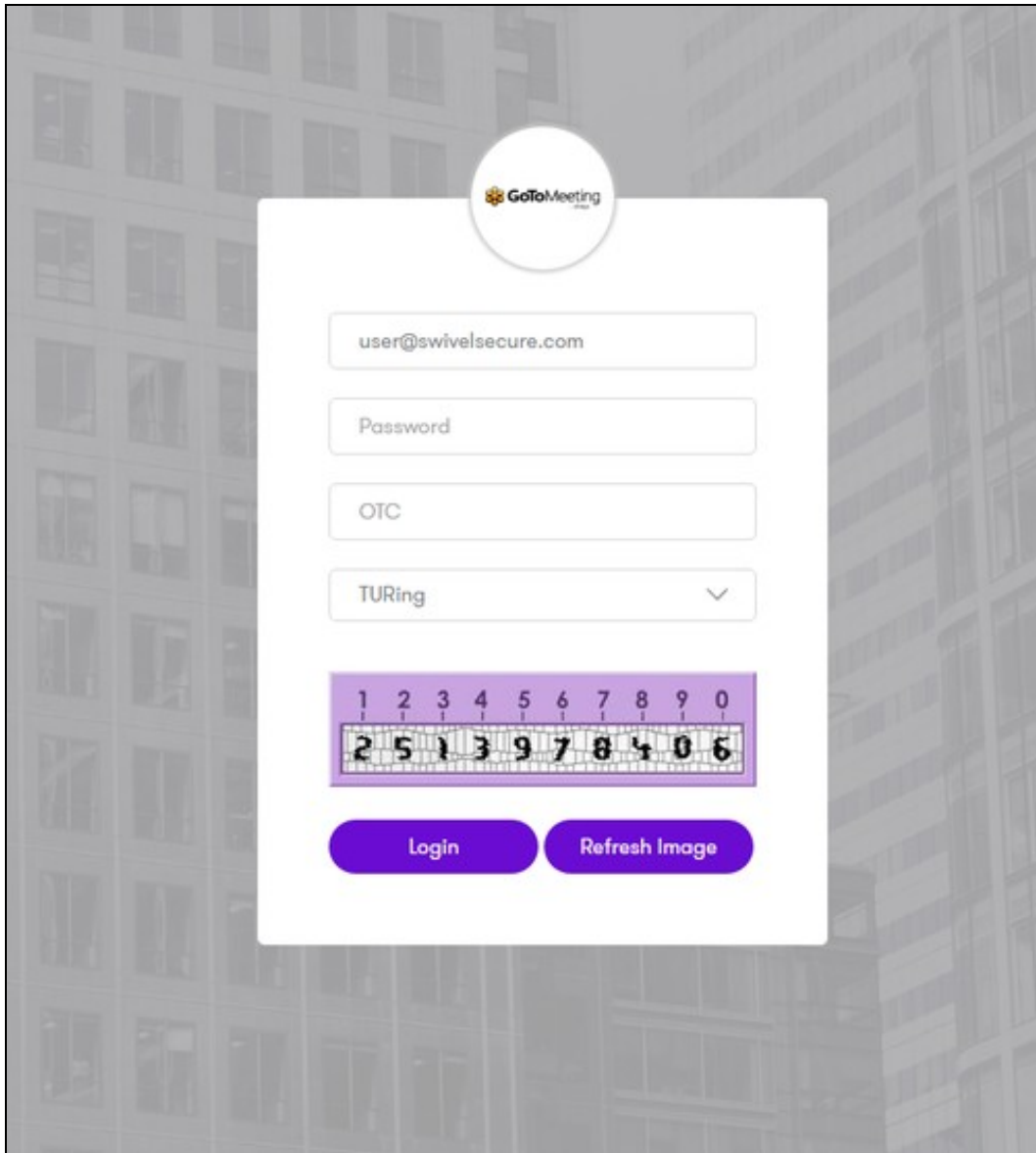


Once you have submitted your username. You should be presented with the Sentry username page.
In this login example we are using the email as a username.



Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match

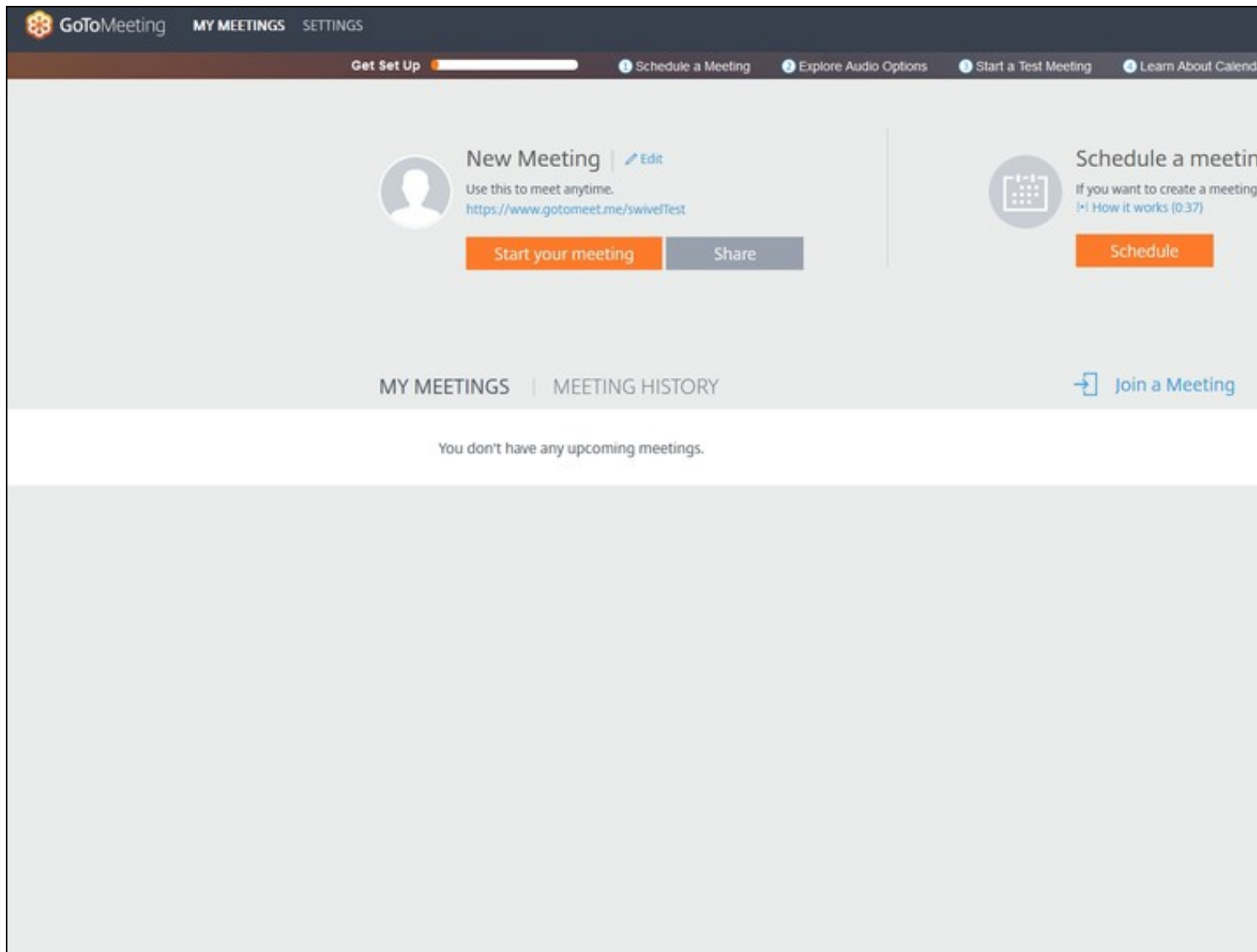
the points required by the GoToMeeting Application definition.



The image shows a GoToMeeting login interface overlaid on a background of a modern building. The login form is white and contains the following elements:

- GoToMeeting logo at the top.
- Input field for email: `user@swivelsecure.com`
- Input field for Password.
- Input field for OTC.
- Dropdown menu for TURing, currently showing "TURing" and a downward arrow.
- A 10-digit numeric keypad with digits 1-9 and 0. The digits entered are 2, 5, 1, 3, 9, 7, 8, 4, 0, 6.
- Two buttons at the bottom: "Login" and "Refresh Image".

After we enter our authentication credentials we successfully will see the GoToMeeting account that we tried to access.



44.6 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been
The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from GoToMeeting

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

Certificate or decryption issues;
Can AuthControl Sentry find the Certificate locally, is it the correct one?
Has the correct Certificate been uploaded to GoToMeeting?
Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core s

45 Sentry SSO with JIRA

45.1 Introduction

This document describes how to configure on-premise Atlassian JIRA to work with Sentry SSO. Before following these instructions, you should be familiar with using Sentry - see the Sentry User Guide for more information.

45.2 Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on your JIRA site, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

45.3 Setup SSO on JIRA

To configure SSO on JIRA a third party add-on is required. There are many SAML plugins available but the plugin that has been used by one of our partners and integrated successfully is the "SAML 2.0 Single Sign-On for JIRA" plugin by Bitium, Inc.

Goto the AddOns configuration page in JIRA. Search for Bitium and install the "SAML 2.0 Single Sign-On for JIRA" add-on:



SAML 2.0 Single Sign-On for JIRA

Bitium, Inc • Unsupported

ADMIN TOOLS

Easily configure JIRA to support SAML 2.0

★ ★

262

Free

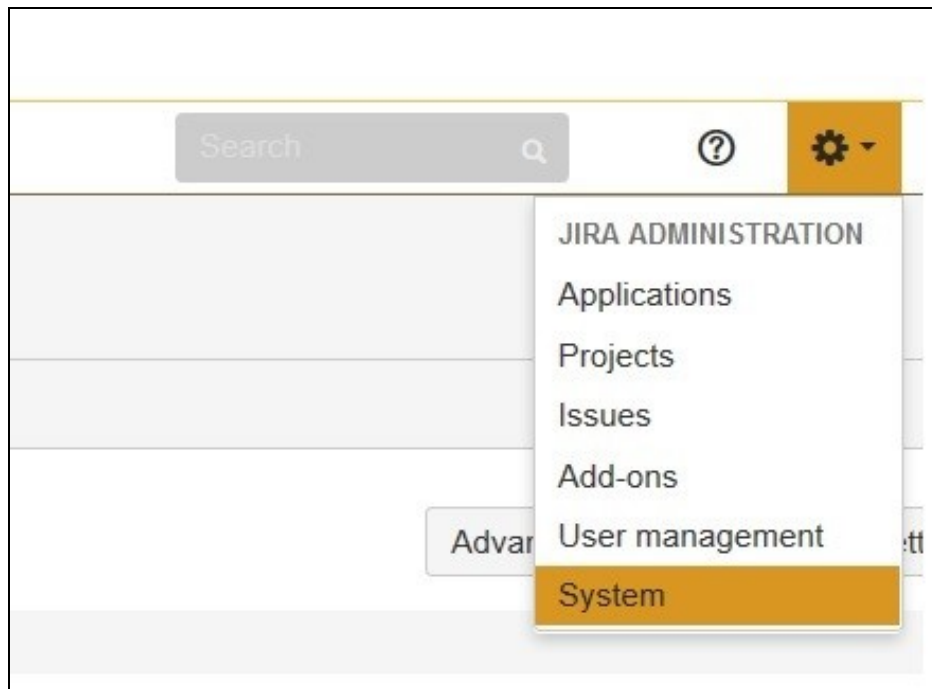
Installing

Installing SAML 2.0 Single Sign-On for JIRA...

Downloading... Installing...



Once installed, goto the System settings screen in JIRA, to begin the SAML configuration:



The plugin configuration screen is located on the left hand menu under Security:

https://[REDACTED]/plugins/servlet/sam

Login URL

<https://SITEID.swivelcloud.com:8443/sentry/saml20endpoint>

UID Attribute

NameID

The name of attribute that is used for user name (UID). Use special value of NameID to instead of attribute.

X.509 Certificate

[illegible]

Your IdPs X.509 certificate

Entity ID

<https://SITEID.swivelcloud.com:8443/sentry/saml20endpoint>

The EntityID that your IdP will use

Maximum Authentication Age

7200

Maximum Authentication Age (in Seconds)

☐ Force SSO login

If checked, all Jira logins will be made through SSO only. You are strongly encouraged to check this box before checking this box or else you may get locked out of Jira.

☐ Auto-create User

If checked, user will be automatically created on successful login, using data from

Default Group for Auto-created Users

jira-software-users

Auto-created users will automatically be added to the selected user group

Save



Configure the settings as shown in the screenshot, being careful to replace your hostname in the highlighted areas. Leave NameID as it is.

In the X.509 Certificate field, you will need to paste the Key from Swivel AuthControl Sentry. Navigate to your AuthControl Sentry Keys page and copy the certificate text into the SAML plugin in JIRA.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Keys

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

Opening RSAcert.rsa.pem

You have chosen to open:



RSACert.rsa.pem

which is: TXT file (1.2 KB)

from: https://192.168.40.35:84

What should Firefox do with this file?



Open with

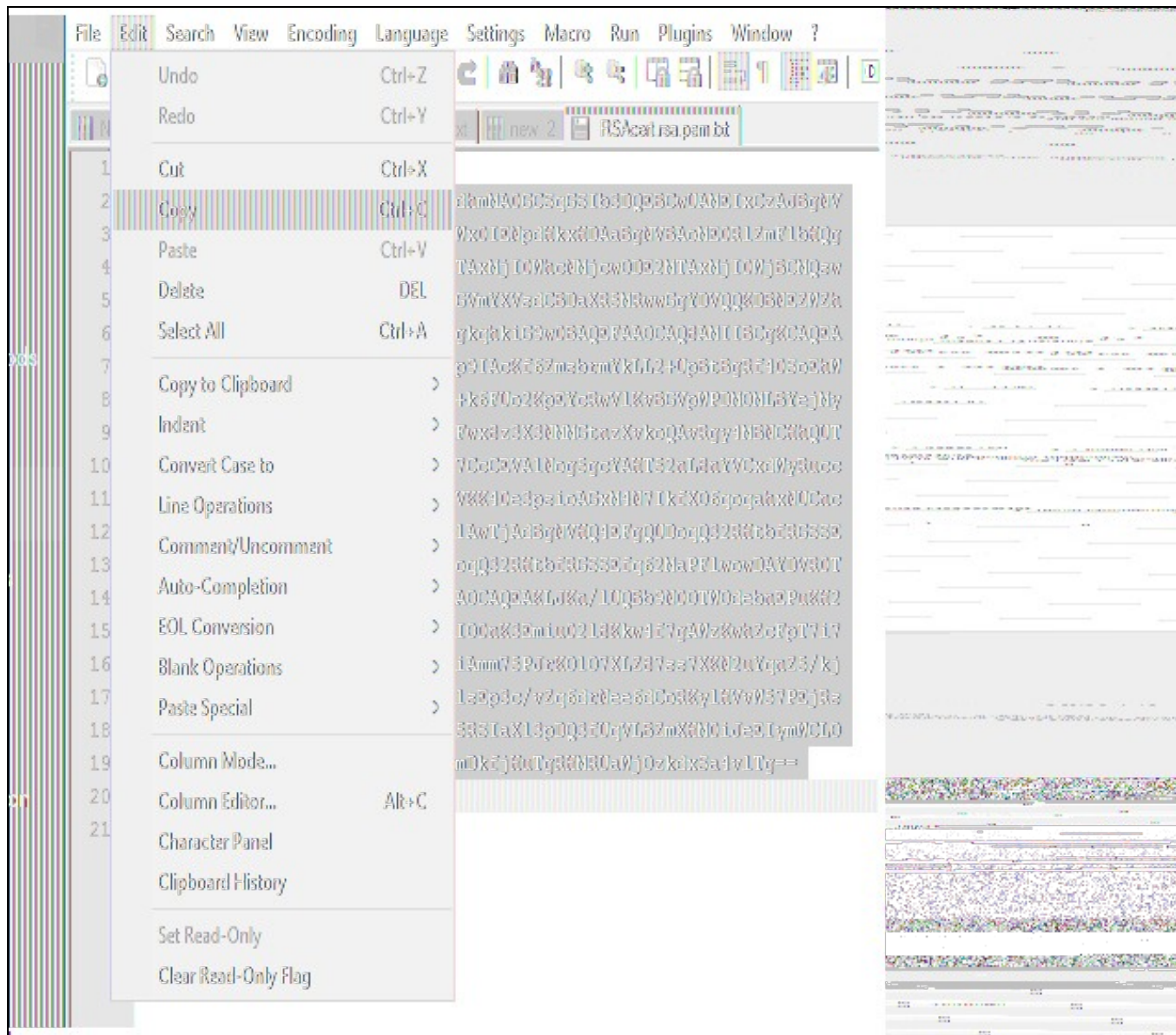
Notepad++ :



Save File



Do this automatically for files of this type



Once all the settings have been configured in the JIRA SAML plugin, save and apply the changes.

45.4 Setup AuthControl Sentry Application definition




First we should upload the JIRA logo. Find it using a Google Images search or copy it from here:



Login to the AuthControl Sentry Administration Console. Click Application Images in the left hand menu. Click the Upload Image button on the top right.

[Rules](#)[Applications](#)[Authentication Methods](#)[View IdP Metadata](#)[Keys](#)[Users Active Sessions](#)[User History](#)[Log Viewer](#)[General Configuration](#)[Application Images](#)

Application Images

Image	Name
 Microsoft Active Directory Federation Services	ADFS.png
 CISCO	Cisco.png
 CITRIX NetScaler	CitrixNet.png



Browse to the Logo file you have saved:

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Upload Image

Filename

jira_logo.png

© 2017 Swivel Secure. All rights reserved.

Then upload the image to the Sentry application:

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

Application Images



"jira_logo.png" uploaded

Image

Name



Microsoft

The image should now be available to select, when we go to create a new Application definition for JIRA:



Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for JIRA, click the Add Application button and select SAML - Other type.

[Rules](#)[Applications](#)[Authentication Methods](#)[View IdP Metadata](#)[Keys](#)[Users Active Sessions](#)[User History](#)[Log Viewer](#)[General Configuration](#)[Application Images](#)

Application Types

RADIUS VPN - Cisco ASA

✓Se

RADIUS VPN - Citrix Netscaler

✓Se

RADIUS VPN - Juniper

✓Se

RADIUS VPN - Other

✓Se

SAML - ADFS

✓Se

SAML - Citrix Netscaler

✓Se

SAML - GoToMeeting

✓Se

SAML - Google

✓Se

SAML - Mimecast

✓Se

SAML - Office 365

✓Se

SAML - OneLogin

✓Se

SAML - Other

✓Se

SAML - PulseSecure

✓Se

SAML - Salesforce

✓Se

SAML - ServiceNow

✓Se

SAML - SonicWall

✓Se

Name: **JIRA**

Points: 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)

Portal URL: URL to access to JIRA e.g. http://JIRA_HOSTNAME:8080/plugins/servlet/saml/auth

Endpoint URL: Leave blank - not required

Entity ID: Identifier of the JIRA SAML request e.g. http://JIRA_HOSTNAME:8080/jiraSAML

Federated Id: email

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is supplied in the SAML (Security Assertion Markup Language)

Name

JIRA

Image

jira_logo.png



Points

100

Portal URL

http://JIRA_HOSTNAME:8080/plugins/servlet/

Endpoint URL

Setup AuthControl Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for JIRA authentication.

Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the JIRA Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

45.5 Testing authentication to JIRA via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

Visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. <https://mycompanysentrydomain/sentry/startPage>. On a Start Page you will be able to see a new JIRA Icon on which you can click and proceed with authentication (as you would by going straight to the JIRA page)



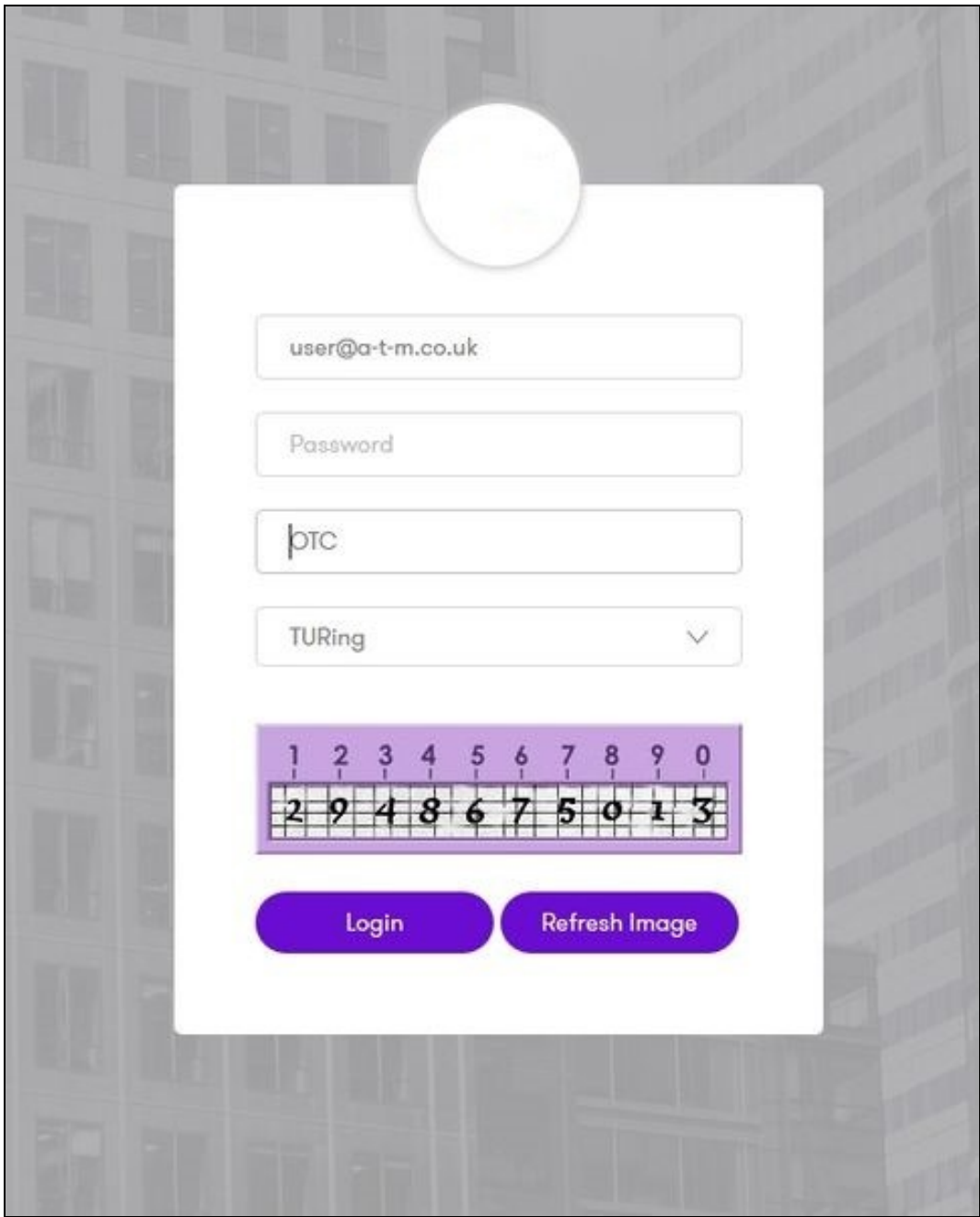
When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup.

Once you have submitted your username. You should be presented with the Sentry username page.

In this login example we are using the email as a username.



Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the JIRA Application definition.



After we enter our authentication credentials we successfully will see the JIRA account that we tried to access.

45.6 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been
The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from JIRA and

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

Certificate or decryption issues;
Can AuthControl Sentry find the Certificate locally, is it the correct one?
Has the correct Certificate been uploaded to JIRA?
Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core s

46 Sentry SSO with Juniper

46.1 Introduction

This article explains how to integrate a Juniper SSL VPN with Sentry.

It focusses on the setting up of Sentry and the modification of the login pages to support the Sentry integration.

It assumes knowledge of how to configure the Juniper to use Sentry as a RADIUS authentication server. Details of these elements can be found in the existing integration guides [Category:Juniper](#)

For this integration it is recommended that the Swivel Radius server is the only authentication required for this realm.

46.2 Overview

The integration works by

1. configuring the Juniper login page to redirect the user to Sentry to authenticate
2. user authenticates at Sentry
3. user is redirected back to the Juniper login page with a claim
4. Juniper login page is submitted with username and claim
5. Username and claim are validated via RADIUS
6. User gains access


Therefore the following steps are required

1. Configure Juniper Login
2. Configure Sentry to work with Juniper login page
3. Configure Sentry to accept RADIUS requests from Juniper

46.3 Configure Juniper Login

To modify the login pages download the sample.zip file from your Juniper and make the required changes to LoginPage.html. If you also wish to support mobile devices you will need to make the same changes to the other login pages, eg LoginPage-mobile-webtoolkit.html

sample.zip can be found on Upload Custom Sign-In Pages, which can be found on Signing-in -> Sign-in Pages -> Upload Custom Pages... There you will be able to see Sample Templates Files on the right side corner as shown below:



Junos Pulse Secure Access Service

System

Status

Configuration

Network

Clustering

IF-MAP Federation

Log/Monitoring

Authentication

Signing In

Endpoint Security

Auth. Servers

Administrators

Admin Realms

Admin Roles

Users

User Realms

User Roles

Resource Profiles

Resource Policies

Junos Pulse

Maintenance

System

Import/Export

Push Config

Archiving

Troubleshooting

[Signing In >](#)

Upload Custom Sign-In Pages

Custom sign-in pages allow you to provide customized templates for various pages that may appear during the sign-in process. Refer to the documentation for information about creating valid templates.

Sign-In Pages

Name:

Label to reference the custom sign-in pages.

Page Type:
☒ Access
☐ Meeting

Templates File:
No file chosen

Zip file containing the custom templates and assets.

Upload

☐ Skip validation checks during upload

In order to make the Juniper page work in the desired way once the page has loaded the page must detect if the user has been redirected to this page from the Sentry Auth Manager or if the user have come directly.

If the user has come directly they need to be redirected to Sentry Auth Manager. If they have been directed from Sentry Auth Manager the login form needs to be populated and submitted.

This is the required snippet that needs adding to the head (eg between the <head> and </head> tags) section of the login pages.

The only modification required is to change SENTRYURL for the actual public url of your sentry install.

Note the **applicationNameNoSAML=JuniperVPN**. This is important as this application name must match the settings on Sentry

```

<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect(){
    window.location.replace("https://SENTRYURL/noSamlEndPoint?returnurlNoSAML="
    + window.location.href + "&applicationNameNoSAML=JuniperVPN" );
}
var QueryString = function () {
    // This function is anonymous, is executed immediately and
    // the return value is assigned to QueryString!
    var query_string = {};
    var query = window.location.search.substring(1);
    var vars = query.split("&");
    for (var i=0;i<vars.length;i++) {
        var pair = vars[i].split("=");
        // If first entry with this name
        if (typeof query_string[pair[0]] === "undefined") {
            query_string[pair[0]] = pair[1];
            // If second entry with this name
        } else if (typeof query_string[pair[0]] === "string") {
            var arr = [ query_string[pair[0]], pair[1] ];
            query_string[pair[0]] = arr;
            // If third or later entry with this name
        } else {
            query_string[pair[0]].push(pair[1]);
        }
    }
    return query_string;
} ();

$(document).ready(function() {

```

198

```

usernamePassedIn = QueryString["username"];
passwordPassedIn = QueryString["password"];
claimPassedIn = QueryString["claim"];
if(typeof claimPassedIn == 'undefined') {
    redirect();
} else {
    $(' [name=password]').val(claimPassedIn);
    $(' [name=username]').val(usernamePassedIn);
    // $(' [name=user#2]').val(usernamePassedIn);
    // $(' [name=password#2]').val(claimPassedIn);
    document.getElementsByName("frmLogin")[0].submit();
}
});
</script>
</head>

```

46.4 Configuring Logout

So that when a user logs out of the Juniper they are also logged out of their Sentry session, the Juniper logout pages need to redirect the user to the Sentry single Logout page. This is a simpler version of the modifications made to the login page. The following code needs adding to the page in the logout.thtml file (and mobile device equivalents)

```

<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect(){
    window.location.replace("https://SENTRYURL/singlelogout");
}
$(document).ready(function(){
    redirect();
});

```

46.5 Configure Juniper

After you have set up the login and logout pages you should upload them to Juniper (as a zip file) like on the screen here [Sentry SSO with Juniper#Configure Juniper Login](#)

After you have uploaded the pages, you should configure the Authentication Realms for the new pages that you have created, to do so you have to click on the Signing In from the left menu. You will be shown the page as below:

Signing In

Sign-in Policies Sign-in Pages Sign-in Notifications

☐ Restrict access to administrators only

Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all rules on this page are disabled.

☐ Enable multiple user sessions

Select this check box and enter the maximum number of sessions per user per realm in Users > User Realms > [Realm Name] > Authentication Policy > Limits page. By default, this is 1, or

☒ Display open user session[s] warning notification

Check this option to notify users if they have other active session[s] in progress when they attempt to sign-in. The user has to follow the instructions on the warning notification page to proceed.

Select when to display a notification page to users

☒ Always

☐ If the maximum session limit per user for the realm has been reached

New URL... Delete... Enable Disable ↑ ↓

Administrator URLs

Sign-In Page

☐ */admin/

[Default Sign-In Page](#)

User URLs

Sign-In Page

☐ */dctest/

[DCTest2SA](#)

☐ */clientdemo/

[Swivel Sign In Page](#)

☐ */pulse/

[Pulse](#)

☐ */raytest/

[Swivel Sign In Page](#)

☐ */

[Swivel Juniper 7R13](#)

☐ */robintest/

[Robin's Custom Page](#)

☐ */pinsafe/

[PINsafe Demo v62R1](#)

☐ */WBY/

[PINSAFE-WBY](#)

☐ */ADdemo/

[PINsafe Demo v62R1 2 stage login](#)

☐ */grahamtest/

[Swivel Juniper 7R13](#)

☐ */sms/

[SMS](#)

☐ */remoteaccess/

[Swivel Juniper 7R13](#)

☐ */pinpad/

[pinpad](#)

☐ */onetouch/

[onetouch](#)

☐ */onetouch2stages/

[onetouch2stages](#)

☐ */inditex2stageDan/

[inditex2stageDan](#)

You have to click on the User URL and select the realm from the available realms box by clicking on it and clicking Add-> button. Refer to the screenshot below.

System

Status
Configuration
Network
Clustering
IF-MAP Federation
Log/Monitoring

Authentication

Signing In
Endpoint Security
Auth. Servers

Administrators

Admin Realms
Admin Roles

Users

User Realms
User Roles
Resource Profiles
Resource Policies
Junos Pulse

Maintenance

System
Import/Export
Push Config
Archiving
Troubleshooting

Signing In >

***/IljaSentry/**

Save Changes

User type:

☒ Users ☐ Administrators ☐ Authorization Only Access

Sign-in URL:

*/IljaSentry/

Format: <host>/<path>/; Use

Description:

Sign-in page:

IljaSentry

To create or manage pages, see [Sign-In pages](#).

Meeting URL:

*/meeting/

Authentication realm

Specify how to select an authentication realm when signing in.

☐ User types the realm name

The user must type the name of one of the available authentication realms.

☒ User picks from a list of authentication realms

The user must choose one of the following selected authentication realms when they sign in. If only one realm is selected, it is automatic.

Available realms:

ADSwivelUsers
authRealmLoreTest
AWSRealm
Chris
clientdemo_Realm

Add ->

Remove

Selected realms:

pinsafellja

Move Up

Move Down


Configure Sign-in Notifications

☐ Pre-Auth Sign-in Notification

☐ Post-Auth Sign-in Notification

Save changes?

Save Changes



Junos Pulse Secure Access Service

System

Status

Configuration

Network

Clustering

IF-MAP Federation

Log/Monitoring

Authentication

Signing In

Endpoint Security

Auth. Servers

Administrators

Admin Realms

Admin Roles

Users

User Realms

User Roles

Resource Profiles

Resource Policies

Junos Pulse

Maintenance

System

Import/Export

Push Config

Archiving

Troubleshooting

[User Authentication Realms >](#)
pinsafeIlja

General

Authentication Policy

Role Mapping

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

New Rule...

Duplicate

Delete

↑

↓

When users meet these conditions

☐
1.

username is "*"

When more than one role is assigned to a user:

☒ Merge settings for all assigned roles


☐ User must select from among assigned roles

☐ User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

Licensed to 0152M08YA0E9003E
Copyright © 2001-2011 Juniper Networks, Inc. All rights reserved.

After clicking on the Authentication Realm you should click on Role Mapping and add a new rule by clicking New Rule In the rule you have to set a rule like on the screenshot below. This rule will assign the users their role for your Juniper network.



Junos Pulse Secure Access Service

System

Status

Configuration

Network

Clustering

(F-MAP Federation)

Log/Monitoring

Authentication

Signing In

Endpoint Security

Auth. Servers

Administrators

Admin Realms

Admin Roles

Users

User Realms

User Roles

Resource Profiles

Resource Policies

Junos Pulse

Maintenance

System

Import/Export

Push Config

Archiving

Troubleshooting

[User Authentication Realms](#) > [pinsafellia](#) >

Role Mapping Rule

* Name:

Rule: (usernameisuser)

is

7

*

If more than one username should match, enter one username per line. You can use * wildcards.

...then assign these roles

Available Roles:

AccountsRemoteAccessRole

AnonyRole

bsmith-test

clientdemo_role

Custom Dan Role

Add ->

Remove

Selected Roles:

Users

☐ Stop processing rules when this rule matches

To manage roles, see the [Roles](#) configuration page.

Save changes?

Save Changes

Save as Copy

* indicates required field

Licensed to 0152M08YA0E9003E

Copyright © 2001-2011 Juniper Networks, Inc. All rights reserved.

After setting up Juniper you should be able to proceed by setting up the Sentry Auth Manager.

46.6 Configuring Sentry Login

The Juniper VPN needs to be added to Sentry as an Application.

The following entries are required.

- Name This must match the name in the redirect url, eg JuniperVPN

203

- Service Provider SwivelVPN. Indicates this is a VPN integration
- Points Number of points required to access the VPN, refer to Sentry User guide
- Endpoint URL This is the URL of the Juniper login page configured to work with Sentry
- Entity ID Should match Name.

46.7 Configuring Sentry RADIUS

To complete the integration the Juniper VPN must be added as a NAS on the Sentry server.

The key settings are

- Identifier Must match the Name on Sentry login, eg JuniperVPN
- Hostname Must match IP of Juniper VPN

Two stage auth, Check Password with repository should be set to NO

46.8 SSO

For RADIUS VPN applications the login page will be displayed although Sentry has been configured with SSO enabled. That attribute just applies for SAML applications.

46.9 Authentication with AD/LDAP and Radius

To be able to authenticate with both AD/LDAP and Radius when logging in you have to add few minor changes. You have to modify the script which you have added at this step [Sentry SSO with Juniper#Configure Juniper Login](#)

You have to uncomment two lines:

```
//$ ('[name=user#2]') .val (usernamePassedIn);
//$ ('[name=password#2]') .val (claimPassedIn);
```

by removing double forward slashes in front of the \$ sign, so it would look like below:

```
$ ('[name=user#2]') .val (usernamePassedIn);
$ ('[name=password#2]') .val (claimPassedIn);
```

And you have to change the password line above the uncommented code from.

```
$ ('[name=password]') .val (claimPassedIn);
```

To the line below, in the password field we will pass now the password and the claim in the password#2 which we have uncommented above.

```
$ ('[name=password]') .val (passwordPassedIn);
```

When you have updated the page, you have to re-upload it by following the same steps like previously on [Sentry SSO with Juniper#Configure Juniper Login](#)

After uploading the the index page you have to change settings on your authentication realm to do so, you have to select your authentication realm and first to add the authentication server to be your AD/LDAP. After selecting the authentication server you should select "Additional authentication server" check box and select a previously created Radius server authentication method. The Authentication Realm settings should look similar to the once on the screenshot below:

pinsafeIlja

General Authentication Policy Role Mapping

- ☐ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: SWIVEL-WBY-AD
Directory/Attribute: Same as above
Accounting: None

- ✓ **Additional authentication server**

You can specify an additional authentication server for single sign-on (SSO) purposes. The additional credentials can be specified by the user on the sign-in page (the labels for these inputs

Authentication #2:	<input type="text" value="pinsafelja"/>
Username is:	<div><input checked="" type="radio"/> specified by user on sign-in page <input type="radio"/> predefined as: <input type="text" value="<USER>"/></div>
Password is:	<div><input checked="" type="radio"/> specified by user on sign-in page <input type="radio"/> predefined as: <input type="text" value="<PASSWORD>"/></div> <div><input checked="" type="checkbox"/> End session if authentication against this</div>

- ☐ **Dynamic policy evaluation**

☐ Session Migration

Other Settings

Authentication Policy:	Password restrictions
Role Mapping:	1 Rule

Save changes?

Save Changes

* indicates required field

46.10 Testing

- Goto to Juniper login url
- User redirected to Sentry, user should be prompted for credentials
- Supply credentials

Should see Sentry logs including

```
Login successful for user: username
SSO_CLAIM_CREATED_FOR_USER, username
```

- User should be redirected to Juniper VPN
- User should gain access

Logs should include

JuniperVPN:Processing user username as channel CLAIM
JuniperVPN:Login successful for user: username

47 Sentry SSO with Meraki Dashboard

(This Article is under construnction)

(This integration has not been released yet)

47.1 Setup Sentry Keys

Before you are able to create a Single Sign On configuration on Meraki, you will need to setup some Keys if you haven't previously. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate from the View Keys menu option of Swivel Sentry. Download the Cert file and save it with the .crt extension name.

47.2 Enable SAML SSO in Meraki Dashboard

In Meraki Dashboard menu, go to Organization > Settings > SAML Configuration, enable SAML SSO and click "Add a SAML Idp"

The screenshot shows the Meraki Dashboard interface. On the left is a dark sidebar with the Cisco Meraki logo and a menu with options: ORGANIZATION, Customer testing org (selected), NETWORK, Select network, and Organization (highlighted with a green bar). The main content area is titled 'SAML Configuration'. It features a 'SAML SSO' toggle switch set to 'SAML SSO enabled'. Below this are three input fields: 'Consumer URL' with the value 'https://n151.meraki.com/saml/login/K3Ld5', 'X.509 cert SHA1 fingerprint' with the value 'bc:84:73:d8:bd:2b:71:76:a1:01:b5:58:7b:63', and 'SLO logout URL (optional)' with the value 'https://<FQDN_OF_SENTRY_SERVER>:8443'. A green link 'Add a SAML IdP' is located below these fields. At the bottom of the main content area, the word 'Administration' is visible.

SAML SSO = select "SAML SSO enabled"

X.509 cert SHA1 fingerprint = open the saved certificate from sentry and get the fingerprint/thumbprint from the Details. The fingerprint needs to have colons on every two characters. ex: 00:11:22:33:44...

SLO logout URL (optional) = set the logout url: https://<FQDN_OF_SENTRY_SERVER>:8443/sentry/singlelogout

47.2.1 Add SAML administrator roles

Go to Organization > Administrators > SAML administrator roles

This section is used to assign permissions to user groups in Dashboard. When SAML users log-in, they will be granted whatever permissions have been assigned to the 'role' attribute included in the SAML token provided by the IdP.

You can create roles based on the username or other attributes of the user.

To create a new role, click Add SAML role and specify the role.

SAML administrator roles

[SAML login history](#) ›

Delete

Search SAML roles... ▼

<input type="checkbox"/> Role ⓘ ▲	Privilege ⓘ
<input type="checkbox"/> ██████████_CUSTOMER	██████████ (Monitor-only)
<input type="checkbox"/> (██████████)_ADMIN	██████████ (Read)
<input type="checkbox"/> ██████████_██████████	██████████ (Monitor-only)

Create role

Role:

Organization access: None ▼

Note: Only administrators with Organization access can edit and/or view configuration template networks.

Target

Access

[+ Add access privileges](#)

[privacy](#)

Close

Create role

Current session started: 28 minutes ago
Session has named to shards: 7/1, 212

47.3 Setup additional role attribute in Swivel Core (if needed)

If you want to use specific roles for the Meraki User roles, you can create the attribute in Swivel Core > Repository > Attributes

Name:	<input type="text" value="merakirole"/>
Phone Number?	<input type="text" value="No"/>
Sync Rule	<input type="text" value="Synchronised"/>
Add repository qualifier?	<input type="text" value="None"/>
Attribute:	
Local:	<input type="text" value="custom"/>
Idap:	<input type="text" value="merakiRole"/>

47.4 Setup Sentry Application

You can select Application Images in the left hand menu to upload the Meraki Dashboard logo. (Optional)



Open the Sentry SSO administration page and Click Applications in the left hand menu. To add a new Application definition for Meraki, click the SAML - Other select button.

SAML - Other	✓Select
--------------	---------

SAML Application



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.

Name

Meraki

Image

cisco-meraki-logo.png



Points

0

Portal URL

<https://n151.meraki.com/saml/login/K3Ld5b/SKpuNaPW8kLb>

Endpoint URL

Entity ID

<https://dashboard.meraki.com>

Federated Id

email

Name = Meraki (Arbitrary name for the application)

Image = the meraki logo

Points = the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application

Portal URL = the Meraki Dashboard **Consumer URL** that is given when enabling SAML SSO

Entity ID = <https://dashboard.meraki.com>

Federated ID = email (That needs to match with the attributed defined on Swivel Core)

Save and click edit to be able to add SAML Assertion Attributes to the application. Add the two attributes required by Meraki:

<https://dashboard.meraki.com/saml/attributes/username> and <https://dashboard.meraki.com/saml/attributes/role>

SAML Application

Name	<input type="text" value="https://dashboard.meraki.com/saml/attributes/user"/>
Format	<input type="text"/>
Sentry Attribute	<input type="text" value="email"/>

SAML Application

Name

`https://dashboard.meraki.com/saml/attributes/role`

Format

Sentry Attribute

`merakirole`

Assertion Attributes

`https://dashboard.meraki.com/saml/attributes/username`

 Edit

 Delete

`https://dashboard.meraki.com/saml/attributes/role`

 Edit

 Delete

Add Attribute

47.5 Testing authentication to Meraki Dashboard via Swivel Sentry

In the Sentry Start Page, select Meraki Dashboard and login.

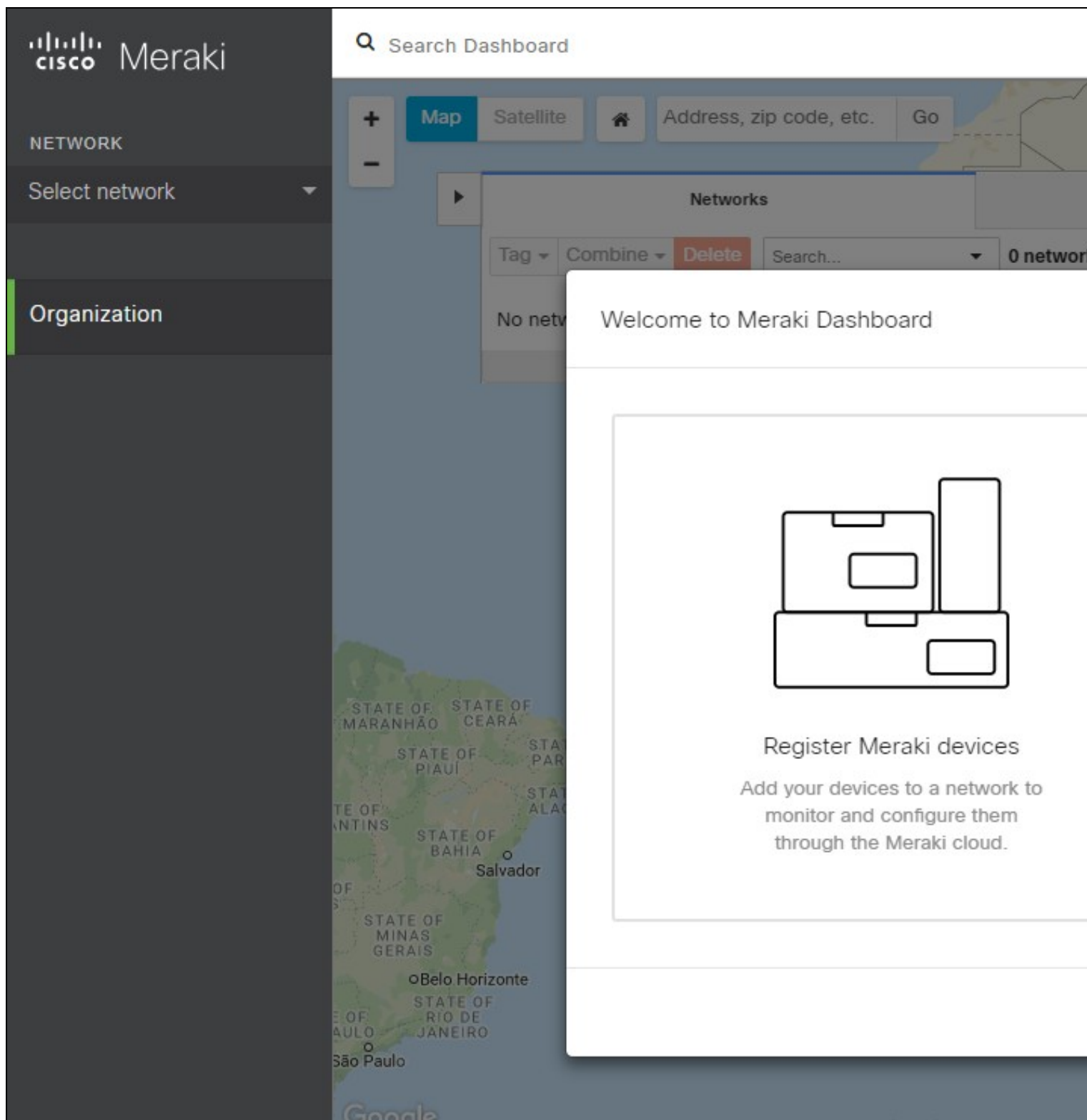
A login form for Cisco Meraki. At the top center is the Cisco Meraki logo, which consists of a circular icon with a stylized signal tower above the text "CISCO" in black and "Meraki" in green. Below the logo is a white rectangular box containing a text input field with the placeholder text "Username". Underneath the input field are two purple rounded rectangular buttons: "Submit" on the left and "Clear" on the right. The entire form is set against a background image of a modern building with many windows.



Username

Submit Clear

If the login is successful, you will login to the Meraki Dashboard and will see on the top right the username that was specified in the user attribute



47.6 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel Sentry has a View Log menu item which provides details about the SAML assertion and response received from Meraki and can be useful for comparison with the Meraki SAML Assertion Validator output;
- Meraki has a SAML login history which can provide diagnostics about the latest SAML authentication attempt. This can be particularly useful for verifying the SAML Attributes and various elements within the SAML assertion that takes place between the Swivel Sentry and Meraki. To get to the SAML Login history in Meraki select Organization -> Administrators -> SAML login history.

SAML administrator roles

[SAML login history](#) ›

Customer testing org SAML login history

‹ [Administrators](#)

Search... ▼

Status	Time ▼	Source IP	Username
✓	Nov 14 15:37:38 UTC	[REDACTED]	t.santos.meraki@swivelsecure.com
✓	Nov 14 15:19:44 UTC		t.santos.meraki@swivelsecure.com
✓	Nov 14 14:23:48 UTC		t.santos.meraki@swivelsecure.com
✓	Nov 14 12:29:54 UTC		t.santos.meraki@swivelsecure.com
✗	Nov 14 12:29:13 UTC	[REDACTED]	[REDACTED]
✗	Nov 14 12:28:11 UTC		[REDACTED]

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the Sentry logging or Meraki login history shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ◆ Can Sentry find the Certificate locally, is it the correct one?
 - ◆ Has the correct Certificate Fingerprint been set in Meraki?
- Attributes mismatch.
 - ◆ Has the Role been created in Meraki Dashboard?
 - ◆ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?

48 Sentry SSO with Mimecast

48.1 Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on Mimecast.com, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

48.2 Setup SSO on Mimecast

To configure SSO setting on your Mimecast accounts you have to access your Admin console by simply going to <https://console-uk-2.mimecast.com/mimecast/admin> You should see an Admin console with an option "Services" similar to the one below:

Service Notifications

All Mimecast services are operating normally. No recent service interruptions to report.

Product News

We are excited to announce global availability of the first phase of the updated Administration Console. If you aren't already, start using it today to benefit from the great new navigation and features. The location and guidance notes have been published on Mimecast Central

Activity Over 24 hrs

Held Email

n/a

Rejected Email

n/a

Bounced Email

n/a

Attachments Linked

n/a

Attachments Blocked

n/a

Policy Edits

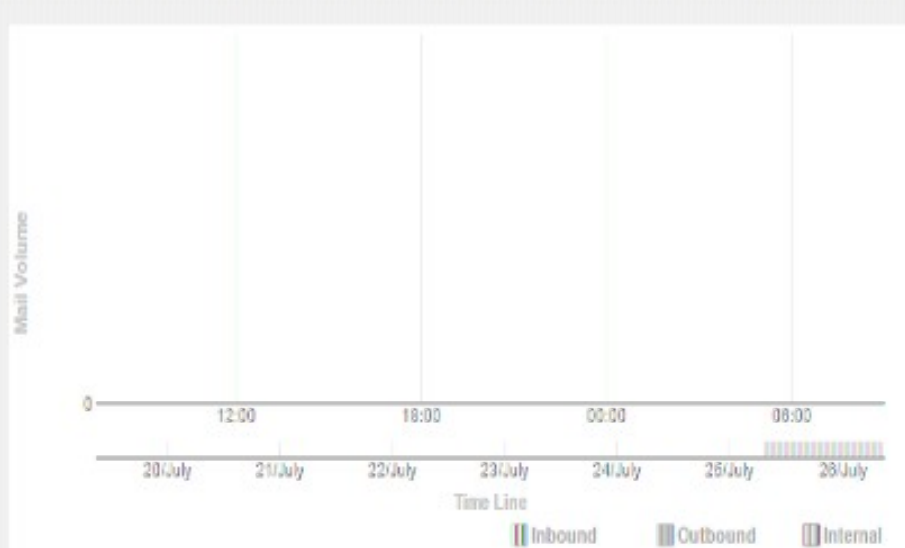
n/a

Last refreshed at 09:17 AM



Service Monitor

Total Email Traffic



Last refreshed at 09:07 AM

Directory Connectors

Service Not Configured

Last refreshed at 09:35 AM

Journal Connectors

n/a

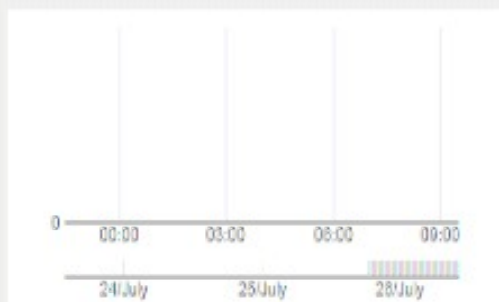
Last refreshed at 09:35 AM

Exchange Services

n/a

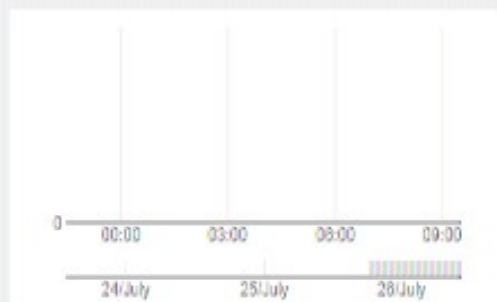
Last refreshed at 09:35 AM

Inbound Email Queue



Last refreshed at 09:30 AM

Outbound Email Queue



Last refreshed at 09:30 AM

Rejections

Open Relay Not Allowed

Recipient Address

Attempt Redirected to Primary MX

Administrative Lockout

Message Body Rejection

Last refreshed at 09:27 AM

Login Information

Account Name Swivel Secure

Logged In Since 2016-07-26 09:21:49

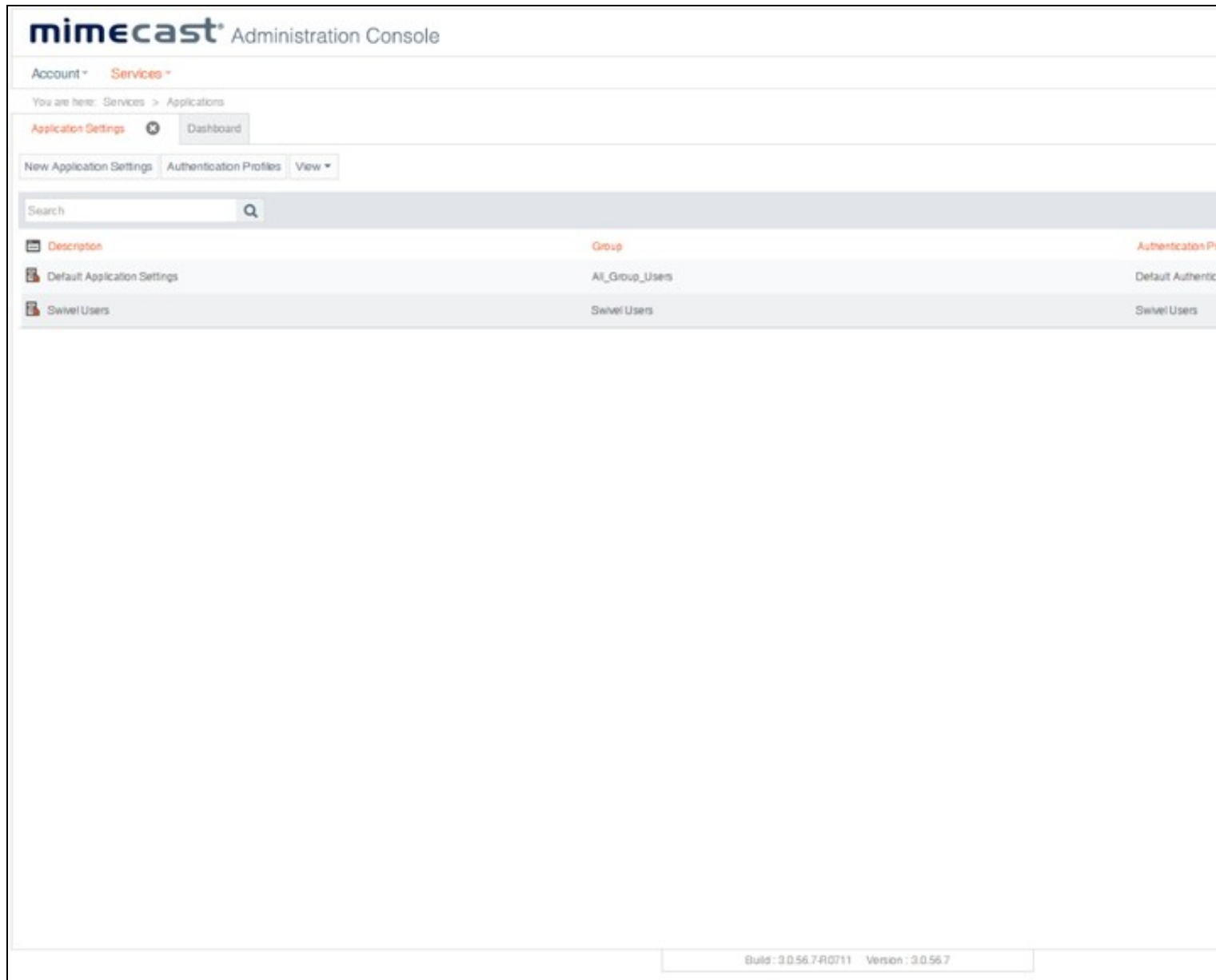
Security Passphrase

Account Code C75A125

Support Code

9BE6

When you click on the Services you will be shown different profiles. You have to click on the button "Authentication Profiles" and select the User group for which to use SSO. For this example we are using "Swivel Users".



The screenshot shows the Mimecast Administration Console interface. At the top, there's a header with the Mimecast logo and "Administration Console". Below this, there are tabs for "Account" and "Services". The "Services" tab is active, and the breadcrumb "You are here: Services > Applications" is shown. Under "Applications", there are buttons for "Application Settings" (highlighted in red), "Dashboard", "New Application Settings", "Authentication Profiles", and a "View" dropdown. A search bar is present below the buttons. The main content area displays a table with three columns: "Description", "Group", and "Authentication Profile". The table lists two entries: "Default Application Settings" with group "All_Group_Users" and "Swivel Users" with group "Swivel Users". The "Swivel Users" entry is highlighted. At the bottom right, a footer shows "Build: 3.0.56.7.R0711" and "Version: 3.0.56.7".

Description	Group	Authentication Profile
Default Application Settings	All_Group_Users	Default Authentication
Swivel Users	Swivel Users	Swivel Users

After clicking on the authentication profile you will have to fill in the details for your AuthControl Sentry such as:

Set the Login, Logout URLs below, where <FQDN_OF_SENTRY_SERVER> is the public DNS entry of your Swivel AuthControl Sentry server, e.g. swivel.mycompany.com or if you do not have a redirect from port 443 to 8443 in place, you may need to include a port number e.g. swivel.mycompany.com:8443

Sign-in page URL - https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint

Sign-out page URL - https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout

Now navigate to your AuthControl Sentry metadata page as below(https://<FQDN_OF_SENTRY_SERVER>/sentry/metadata/generatedMetadata.xml) and copy the content of this page.

Go Back

Save

Save and Exit

Description

Swivel Users ?

Allow Cloud Authentication

Allow Always ?

Domain Authentication Mechanisms

None ?

2-Step Authentication

None ?

Authentication TTL

3 days ?

Enforce SAML Authentication for Administration Console



Enforce SAML Authentication for Mimecast Personal Portal



SAML Configuration for Mimecast Personal Portal

Provider

Other ?

Metadata URL

Import

Monitor Metadata URL



Issuer URL

https://192.168.11.114:8085/sentry/saml20endpoint ?

Identity Mapping

EMAIL ?

Login URL

https://192.168.11.114:8085/sentry/saml20endpoint ?

Logout URL

https://192.168.11.114:8085/sentry/singlelogout ?

Identity Provider Certificate (Metadata)

MIIFVzCCBP2gAwIBAgIJAkS92WUrKu1yMA5GCWCGSAFlAwQDAjCBjzELMAkGA1UEBhMCR0IxETAQBgNVBAgMCV1vcmtzaGlyZTERMA8GA1UEBwwIV2V0aGVyYnkxDzANBgNVBAoMB1N3aXZlbDEMAAoGA1UECwwDRGV2MQ8wDQYDVQQDDAZTZH50cnkxKTANBgkqhkiG9w0BCQEWGmwubW9yYXxlc0Bzd212ZWxzZWNIcmUuY29tMB4XDTE2MDcvNTEzNTM0M1oXDTE2MDgvNDEzNTM0M1owgY8xC

Certificate will Expire on

2016-08-24 14:53

Certificate Last Checked

Allow Single Sign On



Use Password Protected Context



Use Integrated Authentication Context



Enforce Identity Provider Logout on Application Logging Out



Enforce SAML Authentication for End User Applications



48.3 Configure Check Password with Repository on the Swivel Core

In order to check the user's Active Directory password, ensure that the local Agent is configured as explained [here](#)

48.4 Setup AuthControl Sentry Application definition

Please note: you must have setup a Mimecast SSO prior to defining this Application entry within AuthControl Sentry. This is so that you are able to populate the Endpoint URL field. Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for Mimecast, click the Add Application button and select SAML - Mimecast.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS is SAML (Security Assertion Markup Language) n

Name

Mimecast

Image

Mimecast.png

Points

100

Portal URL

https://login-uk.mimecast.com

Endpoint URL

Entity ID

eu-api.mimecast.com.C75A

Federated Id

givenname

Name: Mimecast

Image: Mimecast.png(selected by default)

Points: 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)

Portal URL: (this Portal URL is Mimecast login URL which you can usually access on: <https://login-uk.mimecast.com/m/portal/login> note for different countries it might be a different URL)

Entity URL: N/A

Entity ID: eu-api.mimecast.com.ACCOUNT_NUMBER (Entity ID is a eu-api.mimecast.com. with an Account number such: eu-api.mimecast.com.C75A125)

Federated id: email

Account Number can be found on the Mimecast Admin Console [at the bottom left corner](#)

48.5 Setup AuthControl Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for Mimecast authentication.

Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Mimecast Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

48.6 Testing authentication to Mimecast via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

In a web browser, visit the the URL that you setup on AuthControl Sentry as Endpoint URL e.g. **<https://login-uk.mimecast.com/logon>**

Alternatively you can visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. **<https://mycompanysentrydomain/sentry/startPage>** On a Start Page you will be able to see a new Mimecast Icon on which you can click and proceed with authentication (as you would by going straight to the mimecast page)

Please select an application

The Mimecast logo, consisting of the word 'mimecast' in a lowercase, sans-serif font.The Juniper Networks logo, with 'JUNIPer' in a large, lowercase, sans-serif font and 'NETWORKS' in a smaller, uppercase, sans-serif font below it.The ServiceNow logo, with 'servicenow' in a lowercase, sans-serif font, where the 'now' part is in red.

When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup.



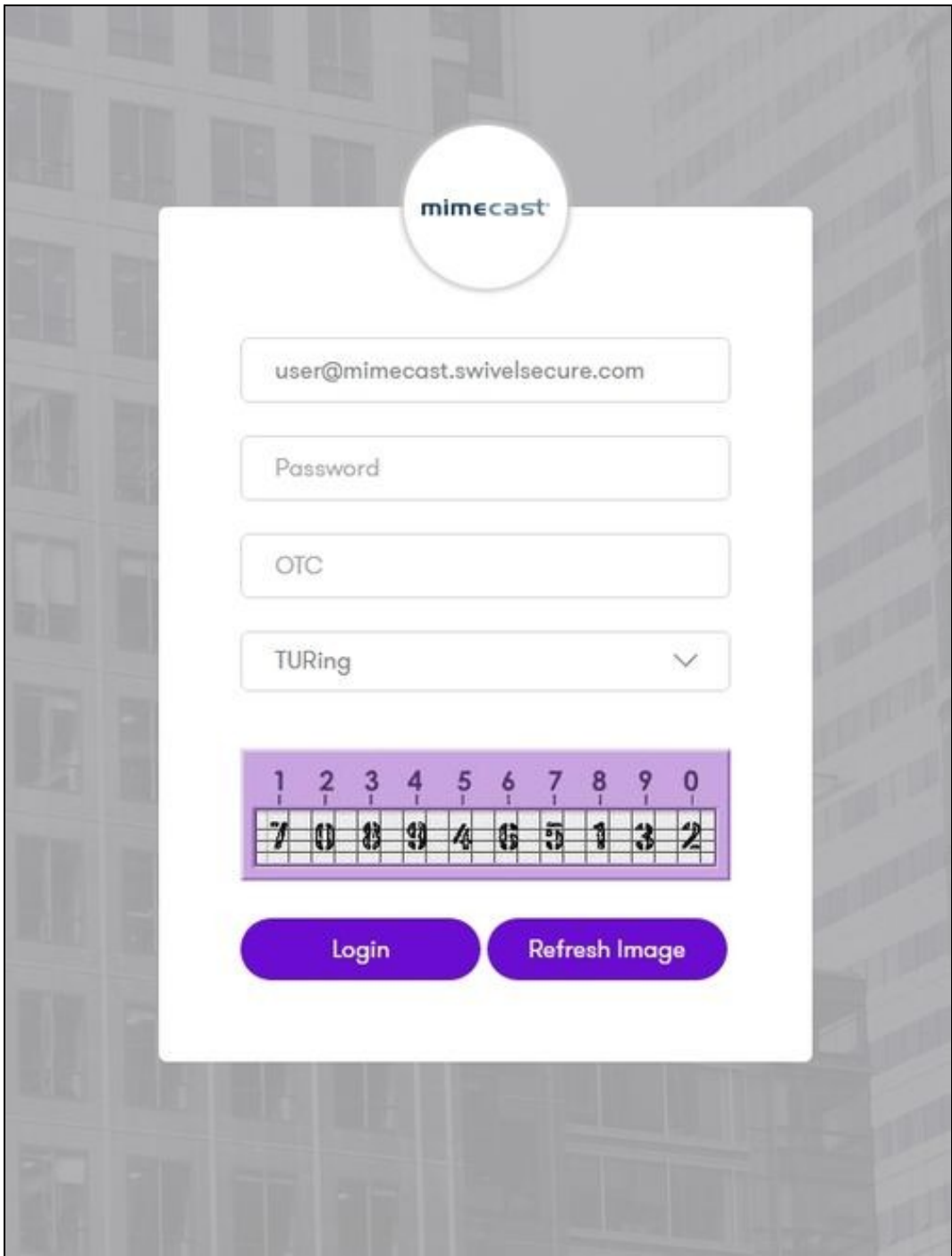
Personal Portal

Mimecast Personal Portal is a webmail portal that allows you to search your personal Archive, manage your PermitBlock lists, and continue to send and receive email in the event of a mail server outage, or for situations when you are unable to access your email.

Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Mimecast Application definition.

In this login example we are using the email as a username

After we enter the username we are prompted with another authentication method (in this example we use turing)



The image shows a login form for Mimecast. At the top is the Mimecast logo. Below it are four input fields: an email address field containing 'user@mimecast.swivelsecure.com', a password field, an OTC field, and a TURING field with a dropdown arrow. Below these fields is a CAPTCHA image showing a grid of numbers. At the bottom are two buttons: 'Login' and 'Refresh Image'.

mimecast

user@mimecast.swivelsecure.com

Password

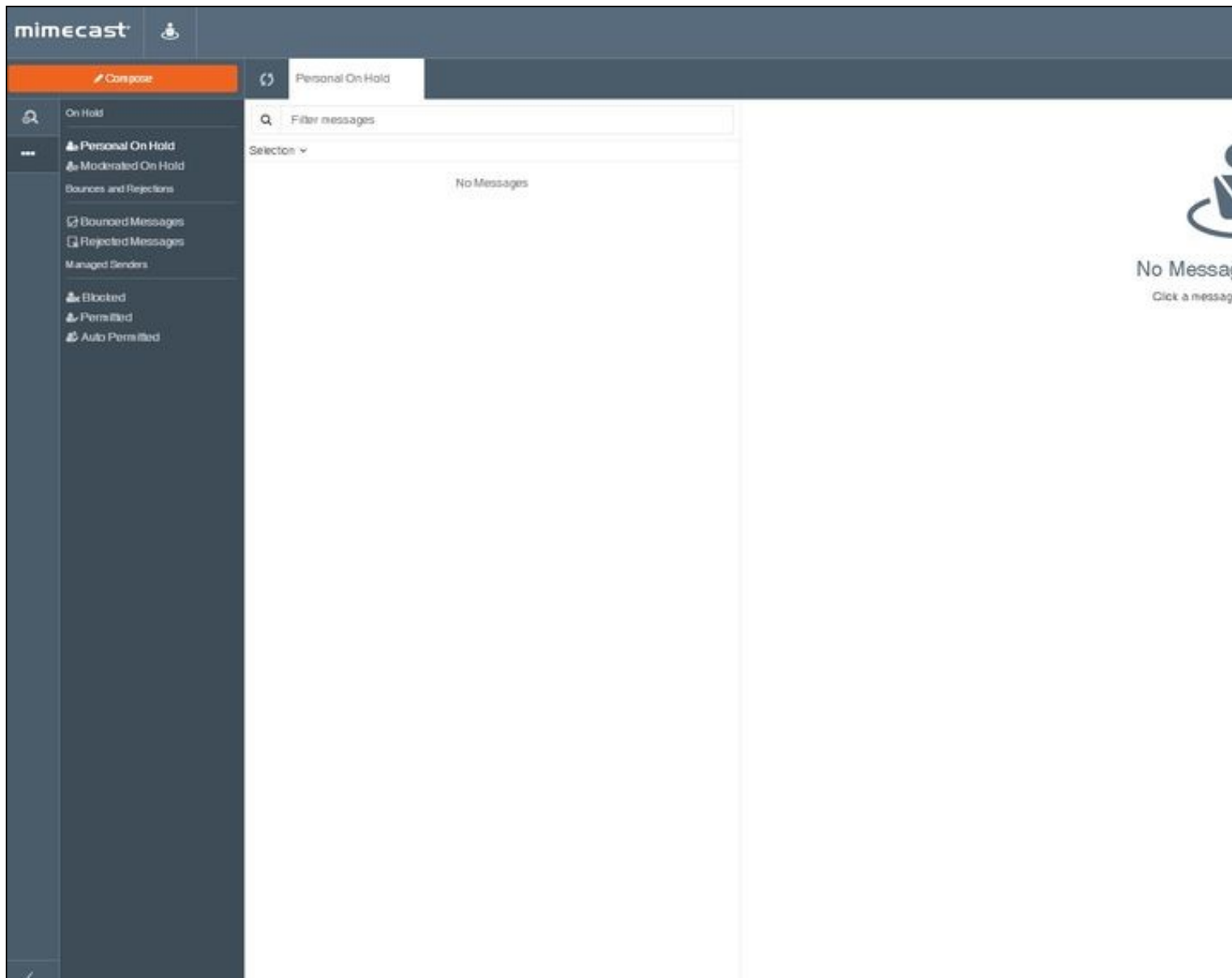
OTC

TURING

1	2	3	4	5	6	7	8	9	0
7	0	8	9	4	6	5	1	3	2

Login Refresh Image

After we enter our authentication credentials we successfully will see the Mimecast account that we tried to access.



48.7 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from Mimecast

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ◆ Can AuthControl Sentry find the Certificate locally, is it the correct one?
 - ◆ Has the correct Metadata been uploaded to the Mimecast?
 - ◆ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?

49 Sentry SSO with Netscaler

49.1 Introduction

This article explains how to integrate a Citrix Netscaler with Sentry.

It focusses on the setting up of Sentry and the modification of the login pages to support the Sentry integration.

It assumes knowledge of how to configure the Netscaler to use Sentry as a RADIUS authentication server. Details of these elements can be found in the existing integration guides [Category:Netscaler](#)

For this integration it is recommended that the Swivel Radius server is the only authentication required for this realm.

49.2 Overview

The integration works by

1. Configuring the Netscaler login page to redirect the user to Sentry to authenticate
2. User authenticates at Sentry
3. User is redirected back to the Netscaler login page with a claim
4. Netscaler login page is submitted with username and claim
5. Username and claim are validated via RADIUS
6. User gains access

Therefore the following steps are required

1. Configure Netscaler Login
2. Configure Sentry to work with Netscaler login page
3. Configure Sentry to accept RADIUS requests from Netscaler

49.3 Configure Netscaler Login

In order to make the Netscaler page work in the desired way once the page has loaded the page must detect if the user has been redirected to this page from Sentry or if the user have come directly.

If the user has come directly they need to be redirected to Sentry. If they have been directed from Sentry the login form needs to be populated and submitted.

This is the required snippet that needs adding to the head section of the login pages.

The only modification required is to change SENTRYURL for the actual public url of your sentry install.

Note the **applicationNameNoSAML=NetscalerVPN**. This is important as this application name must match the settings on Sentry

```
<script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.0/jquery.min.js" ></script>
<script>
function redirect(){
  window.location.replace("https://SENTRYURL/noSamlEndPoint?returnurlNoSAML="
+ window.location.href + "&applicationNameNoSAML=NetscalerVPN" );
}
var QueryString = function () {
  // This function is anonymous, is executed immediately and
  // the return value is assigned to QueryString!
  var query_string = {};
  var query = window.location.search.substring(1);
  var vars = query.split("&");
  for (var i=0;i<vars.length;i++) {
    var pair = vars[i].split("=");
    // If first entry with this name
    if (typeof query_string[pair[0]] === "undefined") {
      query_string[pair[0]] = pair[1];
      // If second entry with this name
    } else if (typeof query_string[pair[0]] === "string") {
      var arr = [ query_string[pair[0]], pair[1] ];
      query_string[pair[0]] = arr;
      // If third or later entry with this name
    } else {
      query_string[pair[0]].push(pair[1]);
    }
  }
  return query_string;
} ();

$(document).ready(setTimeout(function(){
  usernamePassedIn = QueryString["username"];
  passwordPassedIn = QueryString["password"];
  claimPassedIn = QueryString["claim"];
  if(typeof claimPassedIn == 'undefined') {
    redirect();
  } else {
    $('[name=password]').val(claimPassedIn);
    $('[name=login]').val(usernamePassedIn);
    // $('[name=password]').val(claimPassedIn);
    document.getElementsByName("vpnForm")[0].submit();
  }
},0));
</script>
</head>
```

After setting the Script on the index page (in the script tag) you have to also add a form with three input fields as below

```

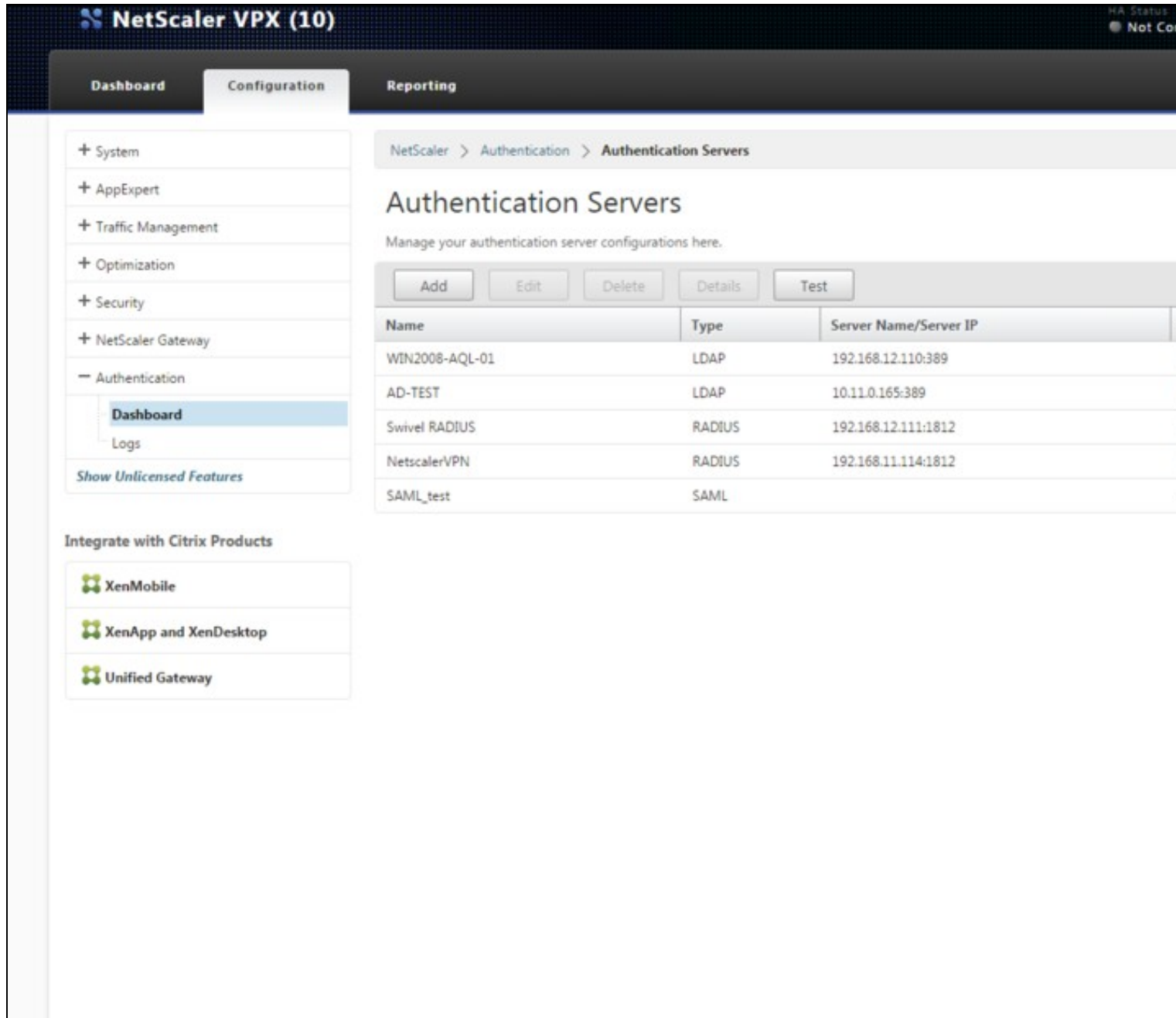
<form action="/cgi/login">
  <input id="login" name="login" data-swivel="username">
  <input id="passwd" name="passwd" data-swivel="password">
  <input id="passwd1" name="passwd1" data-swivel="claim">
</form>

```

This form has to be in the body of the page (in between <body> and </body>) The login page can be found on your Netscaler server usually at the path /netscaler/ns_gui/vpn/index.html

49.4 Configuring Netscaler

After you have successfully modified the login page, you should configure the Netscaler by adding a new Radius server. To do so you have to click on the Authentication -> Dashboard.



Click on the "Add" button and Add a RADIUS Server by adding an IP Address or Server Name Port, Time-out and secret (Secret should be the same as on the Sentry Core). It should look similar to the screenshot below:

NetScaler VPX (10)

HA Status
● Not Con

DashboardConfigurationReporting

← Back

Configure Authentication RADIUS Server

Name

NetscalerVPN

☐ Server Name

☒ Server IP

IP Address*

192 . 168 . 11 . 114

☐ IPv6

Port*

1812

Time-out (seconds)

3

Secret Key*

.....

Confirm Secret Key*

.....

► More

OK

Close

After you have added a radius server you should be able to see if Netscaler can connect to it (if you have created it prior to this) on the Authentication Servers screen in the Status column.

To set up the authentication servers to your Virtual Server or to create a Gateway Virtual Server you have to click on NetScaler Gateway -> Virtual Server

HA Status
● Not C

Dashboard

Configuration

Reporting

+ System

+ AppExpert

+ Traffic Management

+ Optimization

+ Security

- NetScaler Gateway

Global Settings

Virtual Servers

Portal Themes

+ User Administration

KCD Accounts

+ Policies

+ Resources

+ Authentication

Show Unlicensed Features

Integrate with Citrix Products

XenMobile

XenApp and XenDesktop

Unified Gateway

NetScaler > NetScaler Gateway > NetScaler Gateway Virtual Servers

Add

Edit

Delete

Statistics

Visualizer

Action

Name	State	IP Address	Port	Protocol
Demo	Up	10.40.242.185	443	SSL
Lore_DEv	Up	10.40.242.174	443	SSL
Robin	Up	10.40.242.173	443	SSL

On this screen (as above) you should be able to to edit or Add a new Gateway Virtual Server to Add a new server you have to click on the "Add" button, to edit the server you have to select the server by clicking on it once and clicking on the "Edit" button. In this example we are editing the already created Virtual server.

← Back

VPN Virtual Server

Basic Settings

Name	Demo	Maximum Users	0
IPAddress	10.40.242.185	Max Login Attempts	-
Port	443	Failed Login Timeout	-
State	Up	ICA Only	true
RDP Server Profile	-	Enable Authentication	true
Login Once	false	Windows EPA Plugin Upgrade	-
Double Hop	false	Linux EPA Plugin Upgrade	-
Down State Flush	true	Mac EPA Plugin Upgrade	-
DTLS	false	ICA Proxy Session Migration	false
AppFlow Logging	false	Enable Device Certificate	false

Certificates

1 Server Certificate

1 CA Certificate

Authentication

Primary Authentication

1 LDAP Policy

Secondary Authentication

1 RADIUS Policy

Profiles

Net Profile	-
TCP Profile	-
HTTP Profile	nshttp_default_strict_validation

Published Applications

No Next HOP Server

1 STA Server

You will see a screen similar to the one above, you have to set the Primary Authentication method to be your newly created Radius Server. To Do so you have to click on "+" on the Primary Authentication. On the new window that pops up you have to select the Policy as being RADIUS and type as being Primary.

On the next page you have to select the policy. You can click on the arrow button like on the screenshot below, and select your created Radius Server.

NetScaler VPX (10)

HA Status
● Not Configured

DashboardConfigurationReporting

← Back

VPN Virtual Server

Basic Settings

Name	Demo
IPAddress	10.40.242.185
Port	443
State	● Up
RDP Server Profile	-
Login Once	false
Double Hop	false
Down State Flush	true
DTLS	false
AppFlow Logging	false

Certificates

1 Server Certificate

1 CA Certificate

Authentication

Primary Authentication

1 LDAP Policy

Secondary Authentication

1 RADIUS Policy

Profiles

Net Profile	-
TCP Profile	-
HTTP Profile	nshttp_default_strict_validation

Published Applications

Choose Type

Choose Type

Policies

Choose Policy

RADIUS

Policy Binding

Select Policy*

policy_RADIUS_primary_ELITHEA...>+✎

More

Binding Details

Priority*

100

BindClose

After selecting the radius you have to click on the edit button (pencil) and on the edit screen you have to change the Expression to "ns_true" which might be selectable from the Saved Policy Expressions column as you can see from the screenshot below.

NetScaler VPX (10) HA Status: Not Configured Info: NS11.0 62.1

Dashboard Configuration Reporting Documentation

← Back

VPN Virtual Server

Basic Settings

Name	Demo
IP Address	10.40.242.185
Port	443
State	Up
RDP Server Profile	-
Login Once	false
Double Hop	false
Down State Flush	true
DTLS	false
AppFlow Logging	false

Certificates

- 1 Server Certificate
- 1 CA Certificate

Authentication

Primary Authentication

- 1 LDAP Policy

Secondary Authentication

- 1 RADIUS Policy

Profiles

Net Profile	-
TCP Profile	-
HTTP Profile	nshttp_default_strict_validation

Published Applications

- No Next Hop Server
- 1 STA Server

Choose Type > Configure Authentication RADIUS Policy

Configure Authentication RADIUS Policy

Name: policy_RADIUS_primary_ELITHEAWES

Server*: NetscalerVPN

Expression*: ns_true

OK Close

After setting the Expression click OK. Set Priority to 100 and click Bind. Now your Netscaler should be set up.

49.5 Configuring Sentry Login

The Netscaler VPN needs to be added to Sentry as an Application.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

RADIUS VPN Application



Note: The Endpoint URL is used only if it is not

Name

CitrixNetscaler

Image

CitrixNetscaler.png

Points

0

Portal URL

https://citrix.yourdomain

Endpoint URL

Entity ID

CitrixNetscalerVPN

The following entries are required.

- **Name:** This must match the name in the redirect url, eg NetscalerVPN
- **Image:** CitrixNetscaler.png (Selected by default)
- **Points:** Number of points required to access the VPN, refer to Sentry User guide
- **Portal URL:** This is the URL of the Netscaler login page configured to work with Sentry
- **Endpoint URL:** N/A
- **Entity ID:** Should match Name.

49.6 Configuring Sentry RADIUS

To complete the integration the Netscaler VPN must be added as a NAS on the Sentry server.

The key settings are

- Identifier Must match the Name on Sentry login, eg NetscalerVPN
- Hostname Must match IP of Netscaler VPN

Two stage auth, Check Password with repository should be set to NO

49.7 SSO

For RADIUS VPN applications the login page will be displayed although Sentry has been configured with SSO enabled. That attribute just applies for SAML applications.

49.8 Authentication with AD/LDAP and Radius

To be able to authenticate with both AD/LDAP and Radius when logging in you have to add few minor changes. You have to modify the script which you have added at [this step](#)

You have to uncomment one line:

```
//$( '[name=passwd1]' ).val (claimPassedIn);
```

by removing double forward slashes in front of the \$ sign, so it would look like below:

```
$( '[name=passwd1]' ).val (claimPassedIn);
```

You also have to change the password line above the uncommented code from.

```
$( '[name=passwd]' ).val (claimPassedIn);
```

To the line below, in the password field we will pass now the password and the claim in the password#2 which we have uncommented above.

```
$( '[name=passwd]' ).val (passwordPassedIn);
```

You have to re-upload/update the page to the Netscaler.

After updating the page, you have to configure AD/LDAP on the NetScaler. Follow to the Authentication -> Dashboard and click on Add. You have to enter your AD/LDAP settings and the page should resemble to something similar to the screenshot below.

[← Back](#)

Configure Authentication LDAP Server

Name

☐ Server Name
☒ Server IP

IP Address*

☐ IPv6

Security Type*

Port*

Server Type*

Time-out (seconds)

☒ Authentication

Connection Settings

Base DN (location of users)

Administrator Bind DN

☐ BindDN Password
Retrieve Attributes

Other Settings

Server Logon Name Attribute

Search Filter

Group Attribute

Sub Attribute Name

SSO Name Attribute

Default Authentication Group

☒ User Required
☐ Referrals

Maximum Referral Level

Referral DNS Lookup

☐ Validate LDAP Server Certificate
LDAP Host Name

[▶ More](#)

After adding an AD/LDAP you can check if NetScaler can connect to it (Status has to be Up on the Authentication Servers page)

You have to go to the Virtual Server and modify the settings for your virtual server to set AD/LDAP to be the primary authentication method and RADIUS to be Secondary. Follow the same steps to add the authentication methods [as on here](#) except that the Expression for AD-TEST should be "REQ.HTTP.HEADER User-Agent NOTCONTAINS Receiver" and Expression for RADIUS should be also "REQ.HTTP.HEADER User-Agent NOTCONTAINS Receiver".

This way when you will try to authenticate the password will be checked with AD/LDAP server and the One Time Code will be checked with the RADIUS Server (Sentry Core)

49.9 Testing

- Goto to Netscaler login url
- User redirected to Sentry, user should be prompted for credentials
- Supply credentials

Should see Sentry logs including

```
Login successful for user: username  
SSO_CLAIM_CREATED_FOR_USER, username
```

- User should be redirected to Netscaler VPN
- User should gain access

Logs should include

```
NetscalerVPN:Processing user username as channel CLAIM  
NetscalerVPN:Login successful for user: username
```

49.10 Troubleshooting

The scripts on the login page work by injecting values into the login page and submitting this page. To work therefore the standard login page must have a form called vpnForm that has an input field called login for the username and an input field called passwd for the password as shown in the javascript.

By "called" the html must have the name attribute set to this value

50 Sentry SSO with Office 365

50.1 Introduction

Support for Office 365 authentication is provided through ADFS. Therefore you should follow the guide for [ADFS](#). The only difference is, you should select the application type SAML - Office 365. This will set the portal URL to <https://portal.office.com>, and select a different logo by default, but everything else is exactly the same.

51 Sentry SSO with OneLogin

51.1 Introduction

This article explains how to integrate the One Login Web portal with Auth Control Sentry. This article does not cover the initial setting-up of Sentry and assumes that you have generated the required keys etc. These steps are covered in other articles , eg [Sentry_SSO_with_Salesforce](#)

The following article maybe a useful reference.

<https://support.onelogin.com/hc/en-us/articles/201173344-Trusted-IdP-Relying-Party-Trust->

NOTE OneLogin requires <http://www.w3.org/2001/10/xml-exc-c14n#> canonicalisation. Check your version supports this

51.2 OneLogin Setup

In order to set-up your Onelogin domain to use Auth Control Sentry as its Identity Provider you first need to log into the OneLogin Admin Console.

You then need to go to Settings->Security->Trusted IdPs

This will take you to a page where you can add an IdP by clicking the NEW TRUST button.

Create a new Trust called Swivel (or something of your own choosing) and complete the following settings

Settings

Trusted IdPs

Use SAML Service Providers to allow identity providers in your organization to sign in users to OneLogin and the applications.

For information on configuring and using trusted IdPs [click here](#).

Configurations

Issuer

The issuer name or URL of the remote identity provider

IdP Login URL

Where OneLogin redirects users to initiate SAML SSO

Email Domains

Automatically initiate Trusted IdP for users on these domains.



Sign users into OneLogin



Sign users into additional applications

Issuer

This is the issuer of the SAML assertion. This is set within settings.properties (refer to [Sentry Manual](#)) So this entry needs to match that set with settings.properties.

IdP Login Url

This will be the external URL of your Sentry login page. For example if the public hostname of your Sentry server is sentry.domain.com this value would be <https://sentry.domain.com:8443/sentry/saml20endpoint>

This can also be an IP address and need not be https, but for production hostname and https are recommended.

Email Domains If your one-login account covers multiple domains you can list the domains here that you want to use this IdP. If you only have one domain this field can be left blank.

Sign Users into .. You can configure this IdP to log users into their OneLogin account only or into this account and any applications that have been added to this account.

Trusted IdP Certificate	X.509 Certificate *
	<pre>-----BEGIN CERTIFICATE----- MIID4jCCAs6gAwIBAgIJA0nVM2M9uvvoMA0GCSqGSIb3DQEBBQUA VQQGEwJFTjESMBAGA1UECAwJWW9ya3NoaXJlMREwDwYDVQQHDAhX MA0GA1UECgwGU3dpdmVsMQswCQYDVQQLDAJJVDEMMAoGA1UEAwD KoZIHvcNAQkBFhpjLnJ1c3NlbGxAc3dpdmVsc2VjdXJlLnNvbTAe MzMzMzJaFw0yNjA2MTkxMzMzMzJaMIGLMQswCQYDVQQGEwJFTjES MA0GA1UECgwGU3dpdmVsMQswCQYDVQQLDAJJVDEMMAoGA1UEAwD</pre>
User attribute	User Attribute Mapping
	<div>Email ▼</div>

Trusted IdP Certificate This is the certificate that Sentry will use to sign the SAML assertion. You can get this information by logging onto to the Sentry admin console and using the view certificates option or view metadata option. You need to cut and past the certificate information, including the begin and end certifica header and footer by ensuring that no whitespace is added.

User Attribute This is an optional field to be used if, for example, users are logging in with attributes other than their email address.

51.3 Sentry Configuration

You need to add the OneLogin application to the Sentry admin console. If you have the option to add "OneLogin" as an application type use this option. If not then select the SwivelServiceProvider option.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS is SAML (Security Assertion Markup Language) n

Name

OneLogin

Image

OneLogin.png

Points

0

Portal URL

https://yourdomain.onelog

Endpoint URL

https://yourdomain.onelog

Entity ID

https://yourdomain.onelog

Federated Id

email

You need to specify

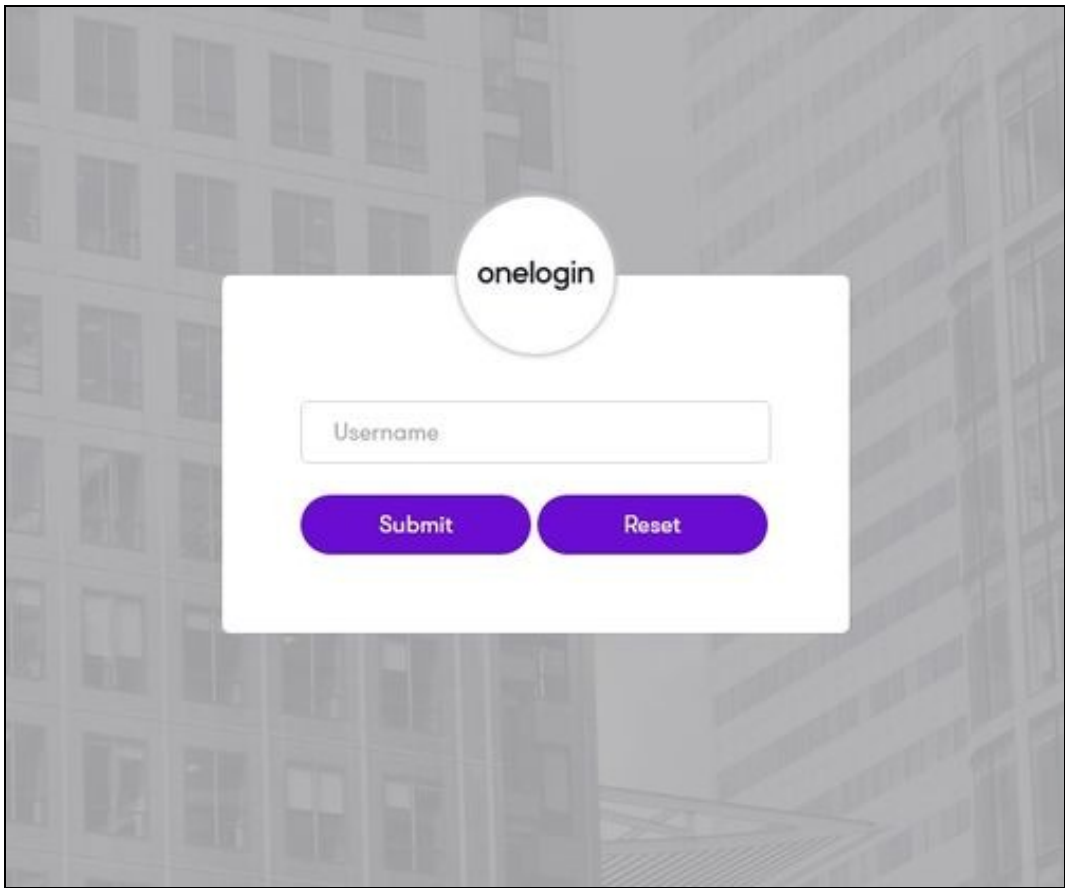
- **Name:** OneLogin
- **Image:** OneLogin.png (Selected by default)
- **Points:** The number of points required to access this service
- **Portal URL:** <https://yourdomain.onelogin.com>
- **Endpoint URL** This is the URL to which the Sentry server will redirect the user with their SAML assertion after authentication. This will be in the format of yourdomain.onelogin.com/sessions/saml. In this case domain is the domain you have registered with OneLogin.
- **Entity ID** This will be in the format of <https://yourdomain.onelogin.com>
- **Federated Id** email

51.4 Testing

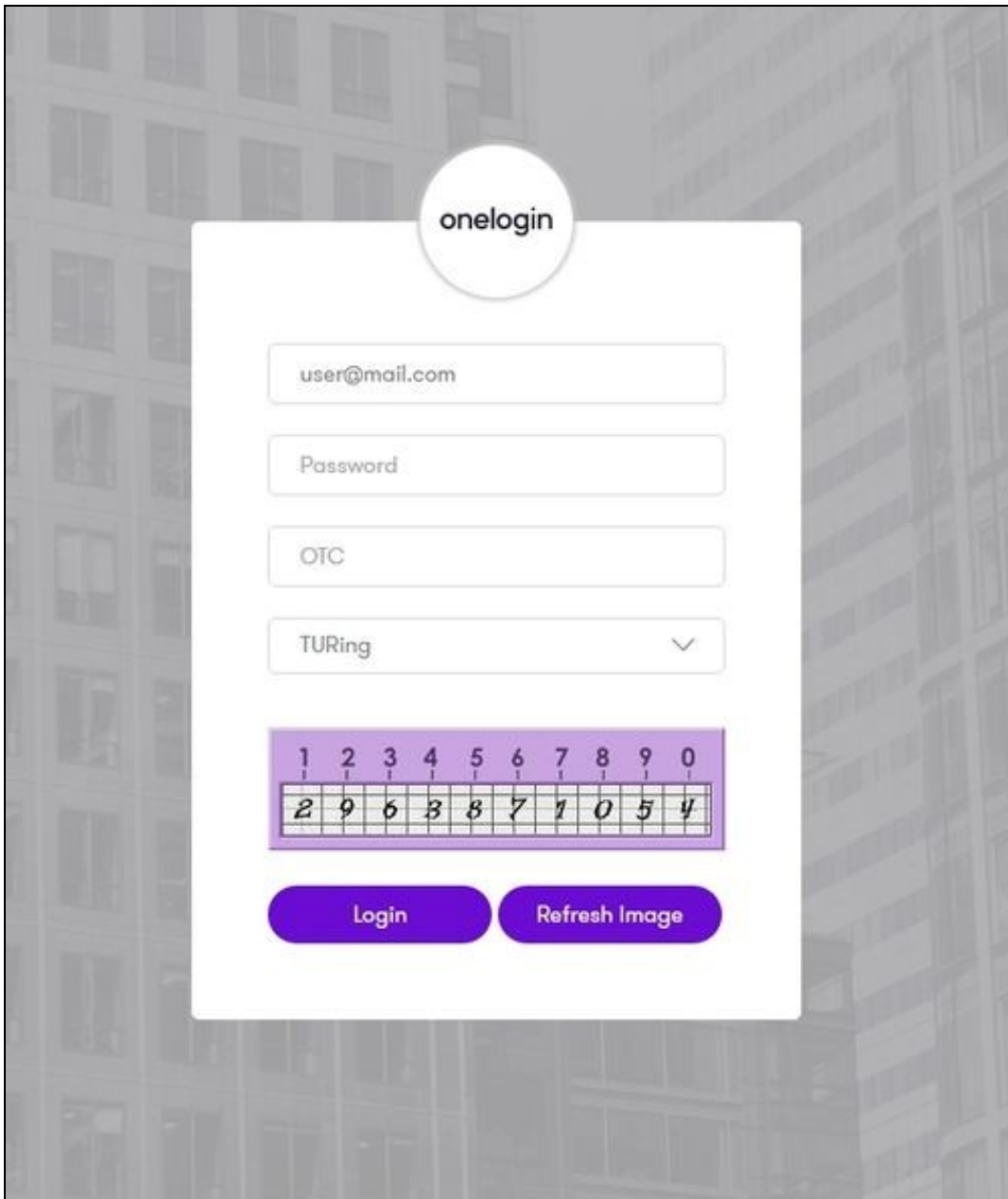
Visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. <https://mycompanysentrydomain/sentry/startPage> On a Start Page you will be able to see a new OneLogin Icon on which you can click and proceed with authentication (as you would by going straight to the OneLogin page)



You should be redirected to the Sentry Login Page.



After you enter the username we are prompted with another authentication method (in this example we use turing)



After you enter your authentication credentials you successfully will see the OneLogin account that you tried to access.

51.5 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from OneLogin

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- * Certificate or decryption issues;
 - * Can AuthControl Sentry find the Certificate locally, is it the correct one?
 - * Has the correct Metadata been uploaded to the OneLogin?
 - * Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core?

Most common issues are likely to be related to the SAML response and whether the OneLogin portal will accept it. To see the SAML response that Sentry is generating you can use a Firefox Plug-in called SAML Tracer <https://addons.mozilla.org/en-GB/firefox/addon/saml-tracer/> There are also some on-line tools you can use to validate the SAML assertion <https://www.samltool.com/>

52 Sentry SSO with Palo Alto

52.1 Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on Google.com, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

52.2 Setup SSO on Palo Alto

SAML IDENTITY PROVIDER SERVER PROFILE IMPORT

- Profile Name: Swivel_sentry (example)

Identity Provider Configuration

- Identity Provider Metadata : Copy the Metadata from Sentry and import it to Palo Alto

After this you should get :

SAML IDENTITY PROVIDER SERVER PROFILE

- Profile Name: Swivel_sentry

Identity Provider Configuration

- Identity Provider ID : <https://demo.swivelcloud.com/sentry/saml20endpoint>
- Identity Provider Certificate :
- Identity Provider SSO URL : <https://demo.swivelcloud.com/sentry/saml20endpoint>
- Identity Provider SLO URL : <https://demo.swivelcloud.com/sentry/singlelogout>
- SAML HTTP Binding for SSO Requests to IDP : Select Post
- SAML HTTP Binding for SLO Requests to IDP : Select Post
- Maximum Clock Skew (seconds) : 60

AUTHENTICATION PROFILE

- Name : SAML

TAB : Authentication

- Type : SAML
- IdP Server Profile : Swivel_sentry
- Certificate for Signing Requests :

Check : "Enable Single Logout"

- Certificate Profile : Swivel

User Attributes in SAML Messages from IDP

- Username Attribute : username

52.3 Sentry

- Name : Palo Alto VM
- Image : Palo Alto logo (png)
- Poits : 100 (example)
- Portal URL :
- Endpoint URL :
- Entity ID :
- Federated Id : username

52.4 Login Steps

Click : User Single Sign-On

Swivel username then click continue...

Insert username then click submit

Authenticate with Swivel authentication method (Turing / PINPad...)

53 Sentry SSO with PHP

53.1 Setup SSO with PHP

Please check the manual



54 Sentry SSO with PulseSecure

54.1 Contents

- 1 Introduction
- 2 Configuring the PulseSecure VPN
- 3 Configuring the Sentry Application
- 4 Testing authentication to PulseSecure via Swivel AuthControl Sentry

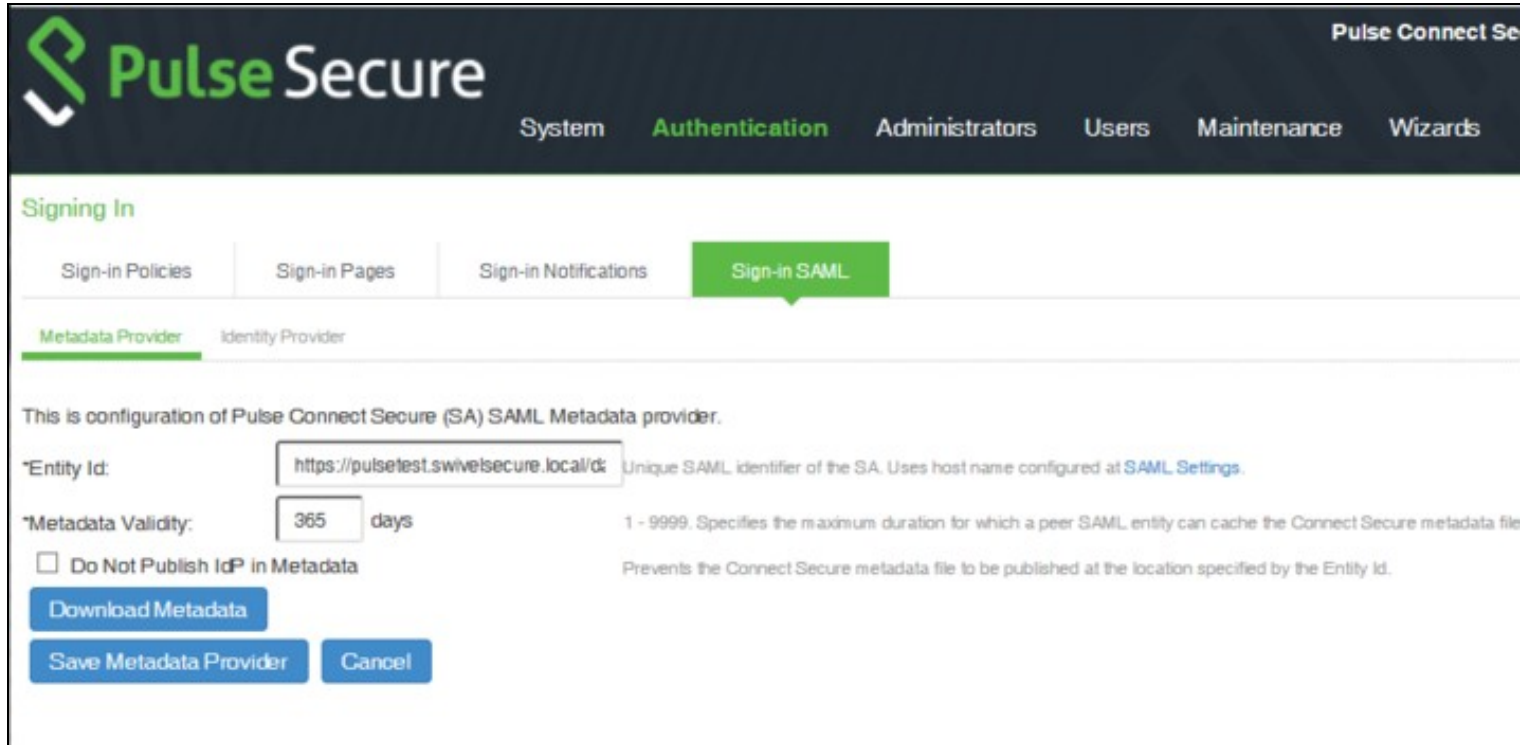
54.2 Introduction

This article explains how to integrate a PulseSecure SSL VPN with Sentry.

54.3 Configuring the PulseSecure VPN

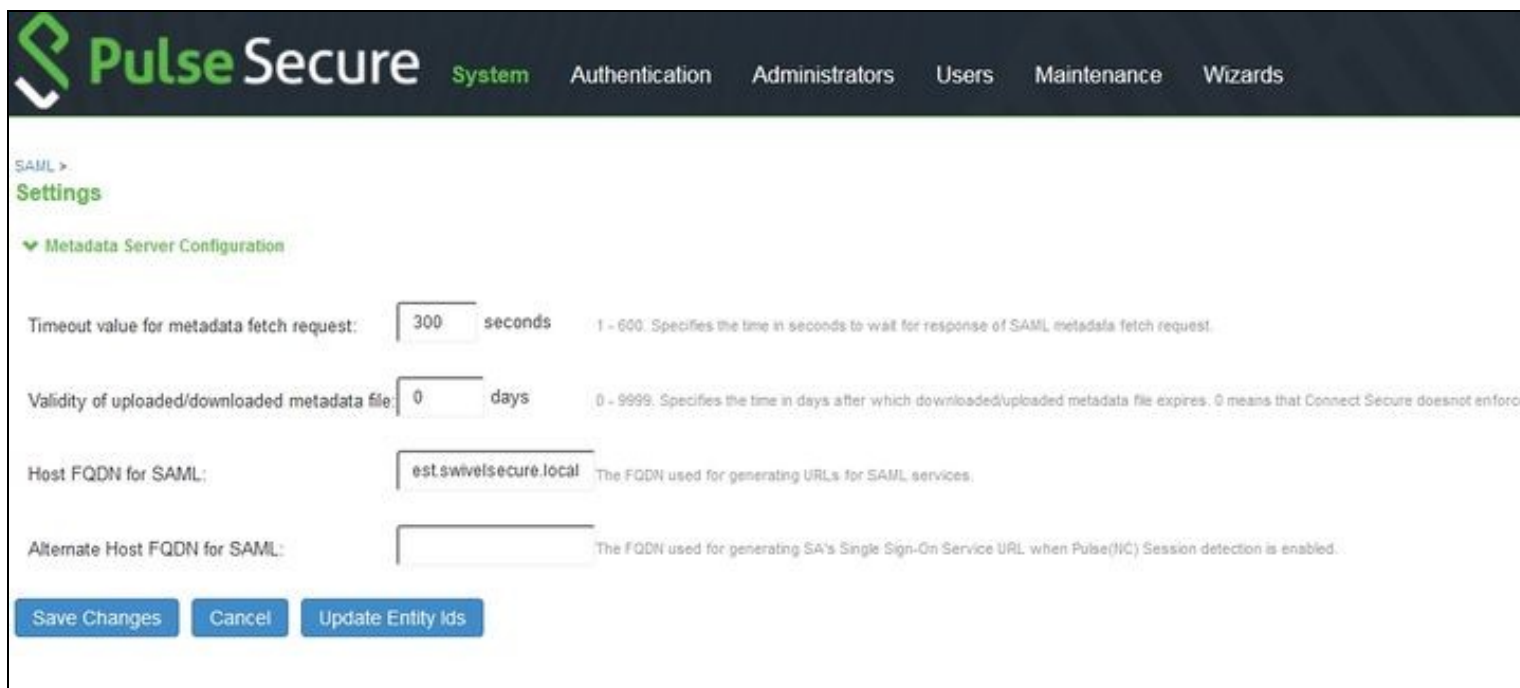
NOTE: It is assumed that your PulseSecure already has a basic, working configuration.

Log into the PulseSecure administration console. From the menu, select **Authentication**, then **Signing In** and **Sign-in SAML**.



The screenshot shows the Pulse Secure administration console interface. The top navigation bar includes the Pulse Secure logo and menu items: System, Authentication (highlighted), Administrators, Users, Maintenance, and Wizards. The 'Signing In' section is active, with sub-tabs for Sign-in Policies, Sign-in Pages, Sign-in Notifications, and Sign-in SAML (highlighted). Below the tabs, the 'Metadata Provider' tab is selected. The page title is 'This is configuration of Pulse Connect Secure (SA) SAML Metadata provider.' The configuration fields include: 'Entity Id' with a text input containing 'https://pulsetest.swivelsecure.local/dc' and a tooltip 'Unique SAML identifier of the SA. Uses host name configured at SAML Settings.'; 'Metadata Validity' with a text input containing '365' and a unit dropdown set to 'days', with a tooltip '1 - 9999. Specifies the maximum duration for which a peer SAML entity can cache the Connect Secure metadata file.'; and a checkbox labeled 'Do Not Publish IdP in Metadata' with a tooltip 'Prevents the Connect Secure metadata file to be published at the location specified by the Entity Id.' At the bottom, there are three buttons: 'Download Metadata', 'Save Metadata Provider', and 'Cancel'.

Click the link for **SAML Settings**, at the end of the line for **Entity Id**.



PulseSecure System Authentication Administrators Users Maintenance Wizards

SAML > Settings

▼ Metadata Server Configuration

Timeout value for metadata fetch request: seconds 1 - 600. Specifies the time in seconds to wait for response of SAML metadata fetch request.

Validity of uploaded/downloaded metadata file: days 0 - 9999. Specifies the time in days after which downloaded/uploaded metadata file expires. 0 means that Connect Secure doesnot enforce.

Host FQDN for SAML: The FQDN used for generating URLs for SAML services.

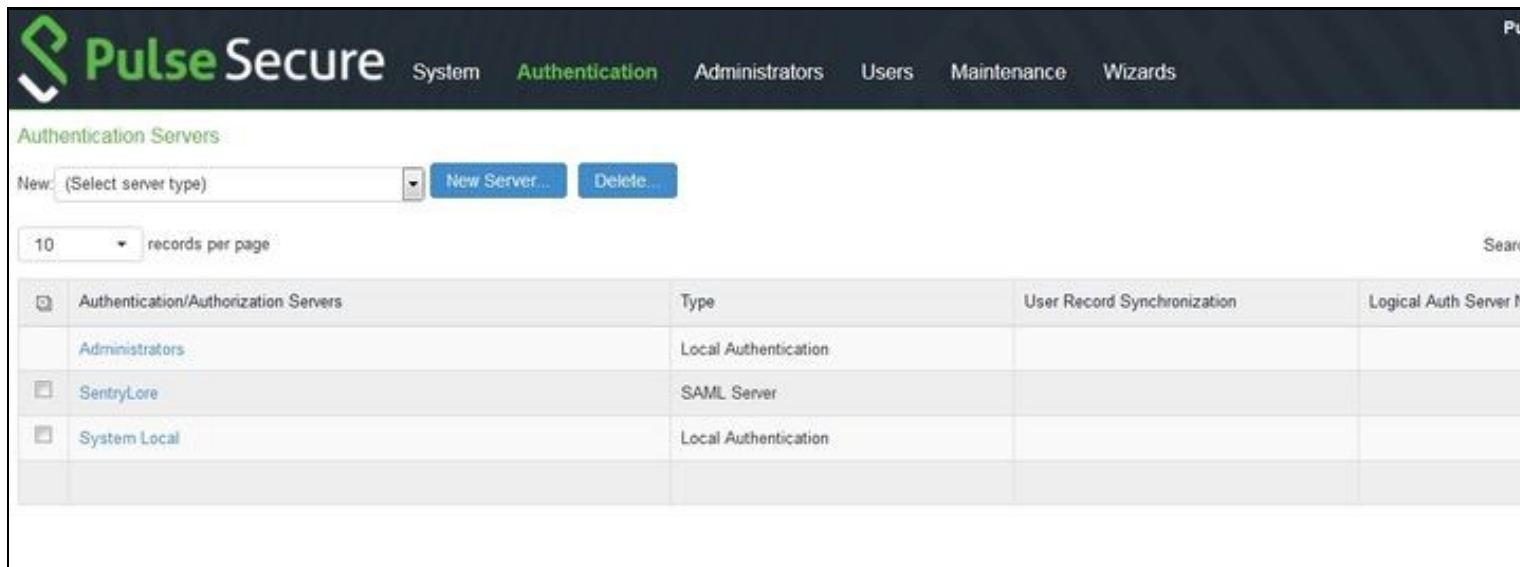
Alternate Host FQDN for SAML: The FQDN used for generating SA's Single Sign-On Service URL when Pulse(IIC) Session detection is enabled.

[Save Changes](#) [Cancel](#) [Update Entity Ids](#)

Enter the public host name of your PulseSecure server under **Host FQDN for SAML**, and click **Save Changes**.

Go back to the **Sign-in SAML** page, and ensure that the Entity Id is `https://<pulse_server>/dana-na/auth/saml-endpoint.cgi` - i.e. it should be exactly the same as the Entity ID you put on the Sentry application settings, except for `?p=sp1`.

Now go to **Authentication, Auth. Servers**



PulseSecure System Authentication Administrators Users Maintenance Wizards

Authentication Servers

New: (Select server type)

10 records per page

	Authentication/Authorization Servers	Type	User Record Synchronization	Logical Auth Server M
<input type="checkbox"/>	Administrators	Local Authentication		
<input type="checkbox"/>	SentryLore	SAML Server		
<input type="checkbox"/>	System Local	Local Authentication		

Select **SAML Server** from the drop-down, then click **New Server...**

System **Authentication** Administrators Users Maintenance Wizards

Auth Servers > SentryLore

SentryLore

Settings Users

Server Name: SentryLore

Settings

*SAML Version:

1.1

2.0

*Connect Secure Entity Id:

/dana-na/auth/saml-endpoint.cgi?p=sp1

Unique SAML identifier of the SAML Auth Server. Uses host name configured at [SAML Settings](#).

*Configuration Mode:

Manual

Metadata

Uses metadata files configured at [SAML Metadata](#) for metadata file based configuration.

*Identity Provider Entity Id:

168.11.115.8443/sentry/saml20endpoint

Unique SAML identifier of the Identity Provider.

Identity Provider Single Sign On Service URL:

168.11.115.8443/sentry/saml20endpoint

User is redirected to this URL in destination first scenario.

User Name Template:

Example: <assertionNameDN uid>, uid from X509SubjectName.
The entire assertion name identifier if not specified; Or
<userAttr attr>, attr from AttributeStatement attributes.

Allowed Clock Skew (minutes):

5

0 - 9999 minutes

☒ Support Single Logout

If checked, Connect Secure supports sending and receiving single logout requests.

*Single Logout Service URL:

192.168.11.115.8443/sentry/singlelogout

Location at Identity Provider to which the single logout request is sent.

Single Logout Response URL:

Location at Identity Provider to which the single logout response is sent. If not specified the response is sent to the same location as the request.

Sso Method

Artifact

Post

Response Signing Certificate:

Issued To: sentry

Issued By: sentry

Valid: Sep 29 13:41:39 2016 GMT - Oct 29 13:41:39 2016 GMT

Details: ▶ Other Certificate Details

Upload Certificate:

Browse

No file chosen

Delete

☐ Enable Signing Certificate status checking

(Uses configuration in Trusted Client CAs. This applies to the certificate configured above as well as the one comes along with the SAML response.)

Select Device Certificate for Signing:

Not Applicable

Certificate used for signing the Requests initiated by Connect Secure for the SAML Auth Server. Select "Not Applicable" if not applicable.

Select Device Certificate for Encryption:

Not Applicable

Certificate used by the IdP for wrapping encryption keys for the SAML Auth Server. Select "Not Applicable" if encryption is not required.

Set a name for the server. Ensure that **SAML Version** is set to 2.0.

Connect Secure Entity Id will be set as the unique entity ID for this server. Make a note of it, as you will be entering it in the Sentry configuration page.

For **Identity Provider Entity Id** and **Identity Provider Single Sign On Service URL**, enter `https://<swivel_server>/sentry/saml20endpoint`. Here, `<swivel_server>` is the public URL of the Swivel sentry server.

Check **Support Single Logout**, and enter `https://<swivel_server>/sentry/singlelogout` as the **Single Logout Server URL**. The **Single Logout Response URL** is the same, so can be left blank.

NOTE: for the next part, you will need a copy of the metadata from the Swivel Sentry server. If you do not already have one, open your browser to `https://<swivel_server>/sentry/metadata/generatedMetadata.xml`. When the metadata is displayed in your browser, save it to disk.

▼ SSO Method

☐ Artifact
☒ Post

Response Signing Certificate:

Issued To: sentry
 Issued By: sentry
 Valid: Sep 29 13:41:39 2016 GMT - Oct 29 13:41:39 2016 GMT
 Details: ▶ Other Certificate Details

Upload Certificate: No file chosen

☐ Enable Signing Certificate status checking
(Uses configuration in Trusted Client CAs. This applies to the certificate configured above as well as the one comes along with the SAML response.)

Select Device Certificate for Signing: ▼ Certificate used for signing the Requests initiated by Connect Secure for the SAML Auth Server. Select "Not Applicable" if encryption is not required.

Select Device Certificate for Encryption: ▼ Certificate used by the IdP for wrapping encryption keys for the SAML Auth Server. Select "Not Applicable" if encryption is not required.

Select Requested Authn Context Classes to be sent in the AuthRequest:

Available:

- InternetProtocol
- InternetProtocolPassword
- Kerberos
- MobileOneFactorUnregistered
- MobileTwoFactorUnregistered

Selected:

(none)

Comparison Method for Authentication Classes: ▼

▼ Service Provider Metadata Settings

Metadata Validity: days 1 - 9999. Specifies the time in days after which metadata for the SAML Auth Server should be refreshed by the Identity Provider. This is used to populate the cache duration field in the metadata.

☐ Do Not Publish Connect Secure Metadata Prevents the Metadata for the SAML Auth Server to be published at the location specified by the Connect Secure Entity Id.

▼ User Record Synchronization

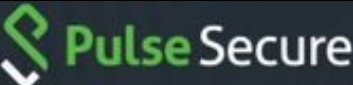
☐ Enable User Record Synchronization
 Logical Auth Server Name:

Ensure that **Post** is selected as the **SSO Method**. Click **Browse** next to **Upload Certificate** and select the metadata file you downloaded earlier.

Set a valid value for **Metadata Validity**.

Click **Save Changes**.

Now Select **Users**, then **User Realms**.


PulseSecure
System
Authentication
Administrators
Users
Maintenance
Wizards
Pulse Connect

User Realms > General

General

User Realms

User Roles

Resource Profiles

Resource Policies

Pulse Secure Client

Enterprise Onboarding

User Realms

New User Realm...

Name:

Description:

☐ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the Servers page.

Authentication:

User Directory/Attribute:

Accounting:

Device Attributes:

SentryLore

None

None

None

Specify the server to use for authenticating users.

Specify the server to use for authorization.

Specify the server to use for Radius accounting.

Specify the server to use for device authorization.

Additional Authentication Server

☐ Enable additional authentication server

Dynamic policy evaluation

☐ Enable dynamic policy evaluation

Session Migration

Other Settings

Authentication Policy:

Role Mapping:

Save Changes

Password restrictions

1 Rule

* indicates required field

Click **New** to create a new user realm.

253

General

General Authentication Policy Role Mapping

* Name: Label to reference this realm

Description:

☐ When editing, start on the Role Mapping page

▼ Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the [Servers](#) page.

Authentication: Specify the server to use for authenticating users.

User Directory/Attribute: Specify the server to use for authorization.

Accounting: Specify the server to use for Radius accounting.

Device Attributes: Specify the server to use for device authorization.

▼ Additional Authentication Server

☐ Enable additional authentication server

▼ Dynamic policy evaluation

☐ Enable dynamic policy evaluation

▼ Session Migration

▼ Other Settings

Authentication Policy: Password restrictions

Role Mapping: 1 Rule

[Save Changes](#)

* indicates required field

Add a name, then under **Authentication**, select your new authentication server. Click **Save Changes**.

Now under **Role Mapping**, select the role(s) that users will be assigned. For example, in the following role mapping, all users are assigned to the Role **Users**.

User Realms > sentryLoreRealm > Role Mapping

Role Mapping

General Authentication Policy Role Mapping

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

[New Rule...](#) [Duplicate](#) [Delete](#) [↑](#) [↓](#)

	When users meet these conditions	assign these roles
<input checked="" type="checkbox"/> 1.	username is "any"	→ Users

When more than one role is assigned to a user:

- ☒ Merge settings for all assigned roles
- ☐ User must select from among assigned roles
- ☐ User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

Finally, go to **Authentication, Signing In, Sign-in Policies**. Click **New URL....** Enter the **Sign-in URL**, then select **User picks from a list of authentication realms** and add the user realm created above. Click **Save Changes**.

54.4 Configuring the Sentry Application

Log into the Sentry administration console. Select **Applications**. Then Click **Add Application** and select **SAML - PulseSecure**

The screenshot shows the Sentry Administration Console interface. On the left is a purple sidebar with navigation links: Rules, Applications (highlighted), Authentication Methods, View IdP Metadata, Keys, Users Active Sessions, User History, Log Viewer, General Configuration, and Application Images. The main content area is titled 'SAML Application'. Below the title is a note: 'Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.' The configuration form includes the following fields: Name (PulseSecure), Image (PulseSecure.png with a dropdown arrow and a PulseSecure logo), Points (0), Portal URL (https://yourdomain/yourcontext), Endpoint URL (https://yourdomain/dana-na/auth/saml-consumer.cgi), Entity ID (https://yourdomain/dana-na/auth/saml-endpoint.cgi?p=sp1), and Federated Id (email). At the bottom right are three buttons: Save (purple), Back (grey), and Info (grey).

NOTE: for all the following, replace `<pulse_server>` with the public host name for your Pulse server.

Under **Portal URL**, enter the URL for the PulseSecure portal that will be authenticated using Sentry, for example `https://<pulse_server>/saml`.

Under **Endpoint URL**, enter `https://<pulse_server>/dana-na/auth/saml-consumer.cgi`.

Under **Entity ID**, enter the unique Entity ID you recorded from the PulseSecure authentication server.

Under **Federated Id**, enter `email`.

54.5 Testing authentication to PulseSecure via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

Visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g.

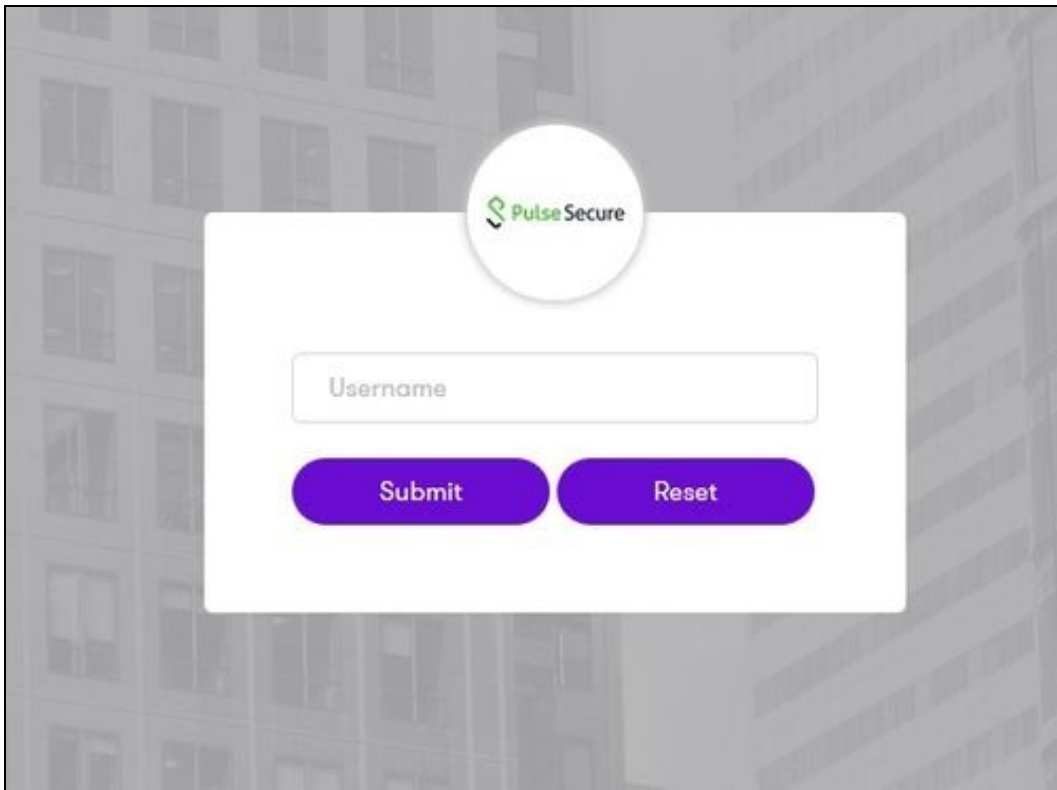
`https://mycompanysentrydomain/sentry/startPage` On a Start Page you will be able to see a new PulseSecure Icon on which you can click and proceed with authentication (as you would by going straight to the PulseSecure page)

Please select an application

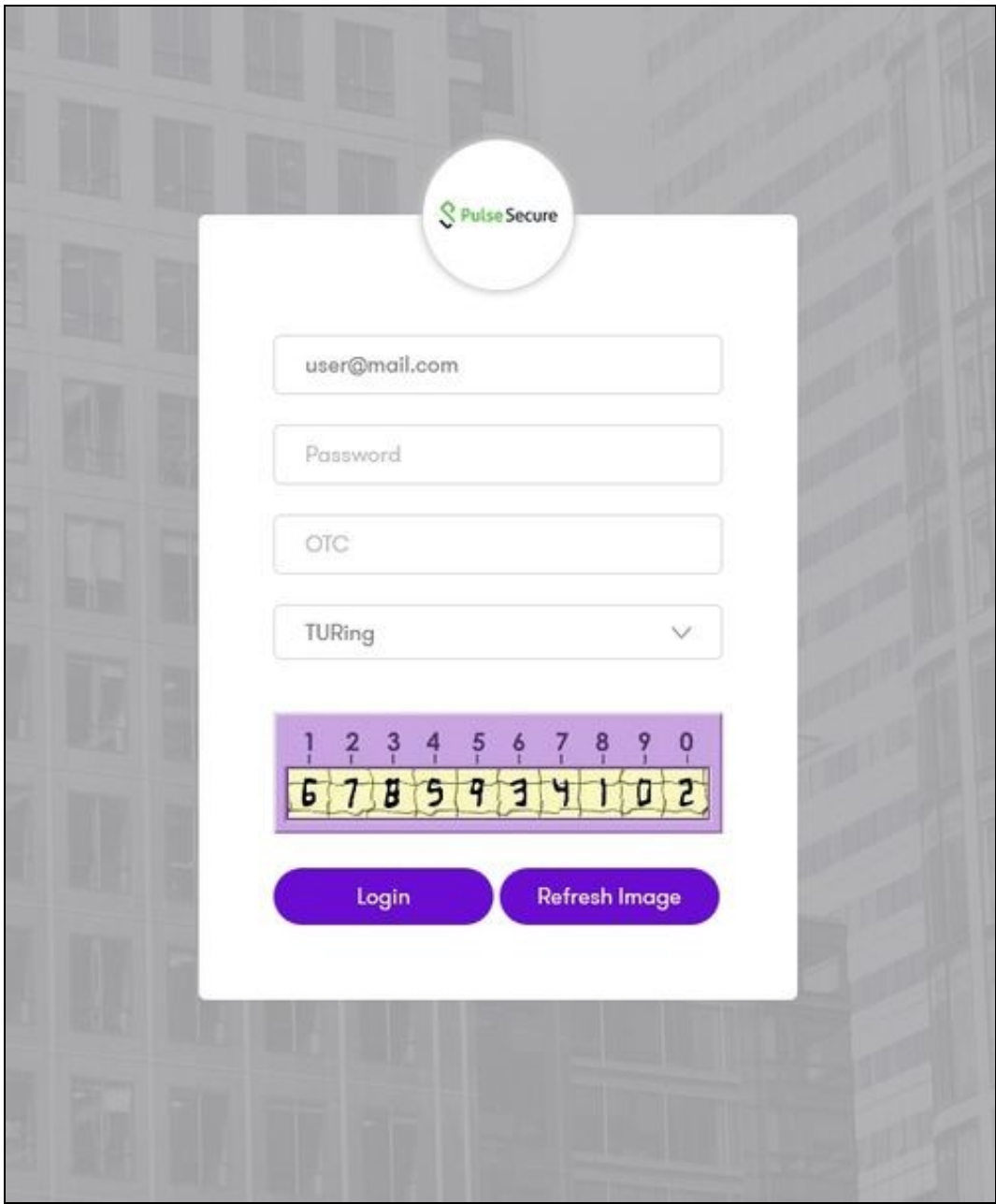


When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the PulseSecure Application definition.

In this login example we are using the email as a username



After we enter the username we are prompted with another authentication method (in this example we use turing)



After we enter our authentication credentials we successfully will see the PulseSecure that we tried to access.

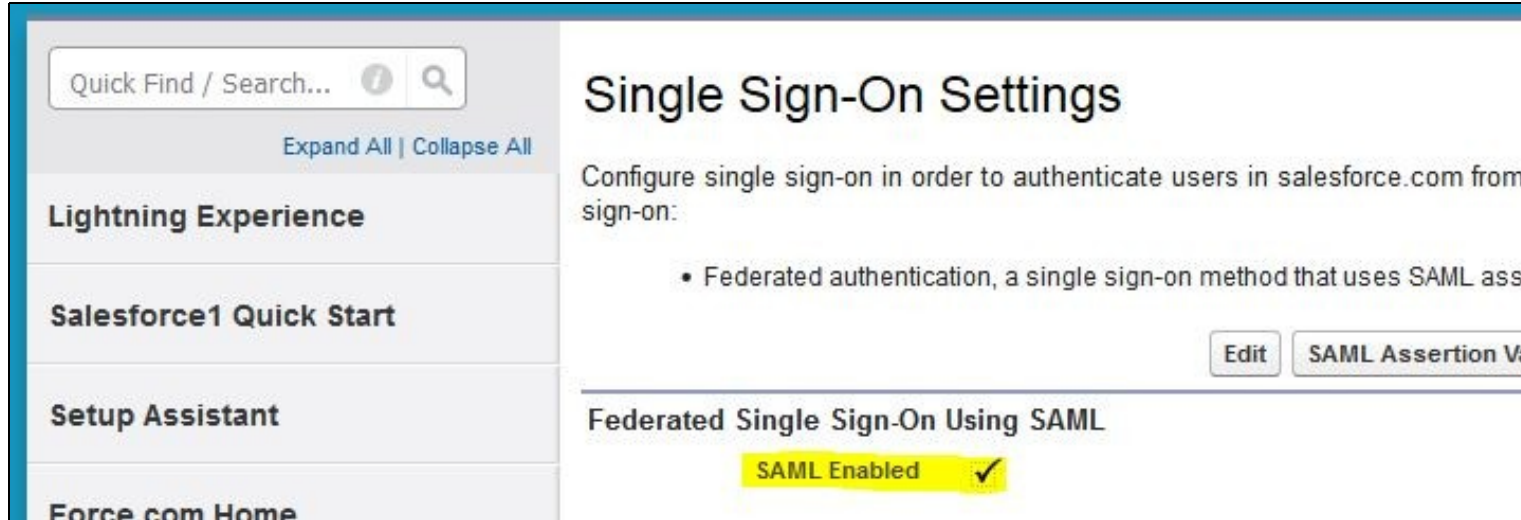
55 Sentry SSO with Salesforce

55.1 Setup Sentry Keys

Before you are able to create a Single Sign On configuration on Salesforce.com, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel Sentry.

55.2 Enable SAML on Salesforce.com

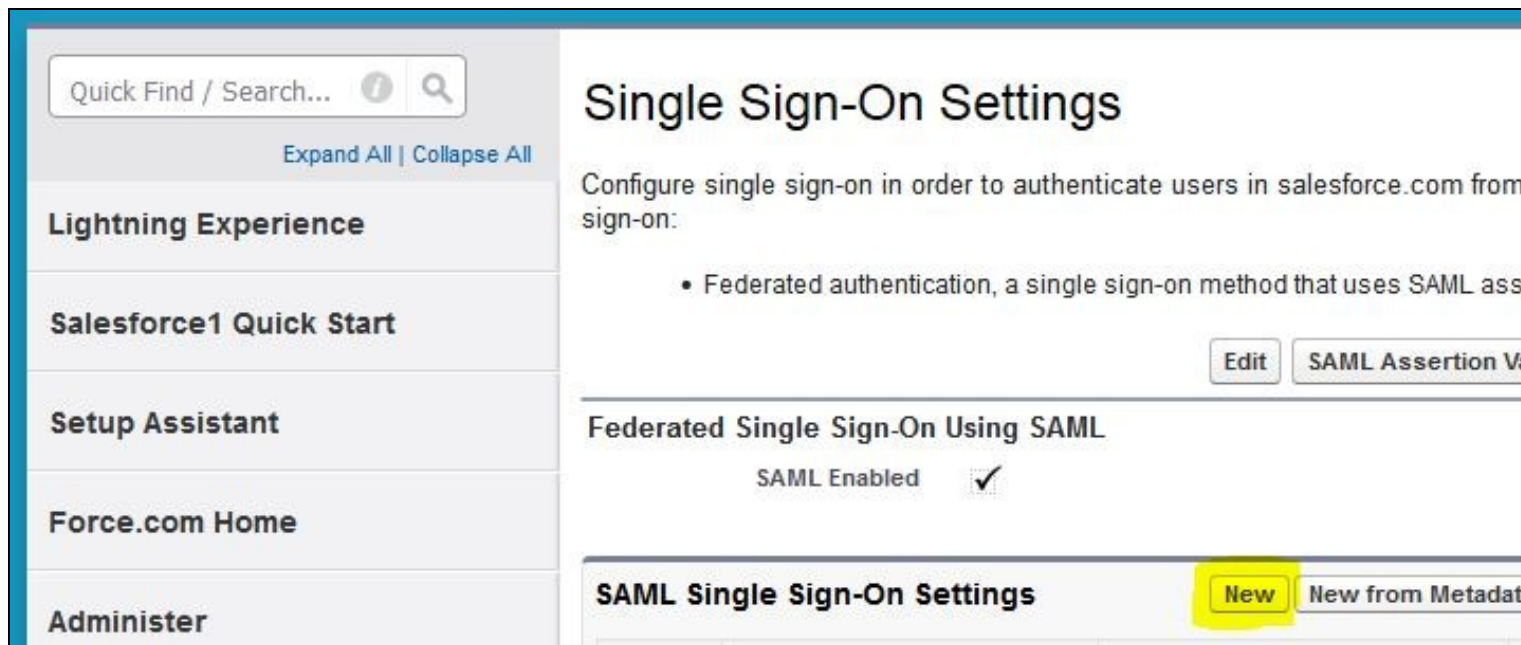
Enable SAML. A checkbox option entitled ?SAML Enabled? should be available in Salesforce under the menu Setup -> Security Controls -> Single Sign-On Settings.



If this option is not available, then you will need to request this feature from Salesforce support or your Salesforce reseller partner.

55.3 Create a new Single Sign-On Settings entry on Salesforce.com

Under the menu Setup -> Security Controls -> Single Sign-On Settings, create a new SAML Single Sign-On Settings entry by clicking the New button.



Populate all required fields and **upload the certificate you generated earlier** (this can be retrieved from the View Keys menu option of Swivel Sentry):

SAML Single Sign-On Settings

SaveSave & NewCancel

Name

Swivel Sentry

SAML Version

2.0

Issuer

SAML_SP

Identity Provider Certificate

Browse...

No file selected.

Request Signing Certificate

Default Certificate

Request Signature Method

RSA-SHA1

Assertion Decryption Certificate

Assertion not encrypted

SAML Identity Type

☐ Assertion contains User's salesforce.com username

☒ Assertion contains the Federation ID from the User object

☐ Assertion contains the User ID from the User object

SAML Identity Location

☒ Identity is in the NameIdentifier element of the Subject statement

☐ Identity is in an Attribute element

Service Provider Initiated Request Binding

☒ HTTP POST

☐ HTTP Redirect

Identity Provider Login URL

https://dc.dev.swivelsecure.net:8443/sentry/saml20endpoint

Identity Provider Logout URL

https://dc.dev.swivelsecure.net:8443/sentry/singlelogout

Custom Error URL

https://dc.dev.swivelsecure.net:8443/sentry/error

Just-in-time User Provisioning

User Provisioning Enabled

☐ i

SaveSave & NewCancel

Name = Swivel Sentry (arbitrary value)

Issuer = Sentry endpoint URL (<https://yourdomain/sentry/saml20endpoint>)

Identity Provider Certificate = Browse to the RSA PEM file created earlier to upload the certificate. When you click save, if successfully imported, the details of the certificate will appear on the right hand side under the ?Current Certificate? field.

Request Signing Certificate = Default Certificate

Request Signature Method = RSA-SHA1

Assertion Decryption Certificate = Assertion not encrypted

SAML Identity Type = Assertion contains the Federation ID from the User object

SAML Identity Location = Identity is in the NameIdentifier element of the Subject statement

Service Provider Initiated = HTTP POST

Set the Login, Logout and Error URLs below, where <FQDN_OF_SENTRY_SERVER> is the public DNS entry of your Swivel Sentry server, e.g. swivel.mycompany.com or if you do not have a redirect from port 443 to 8443 in place, you may need to include a port number e.g.

swivel.mycompany.com:8443

Identity Provider Login URL = `https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint`

Identity Provider Logout URL = `https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout`

Custom Error URL = `https://<FQDN_OF_SENTRY_SERVER>/sentry/error` (ensure that the firewall 443 to 8443 port redirect and open port is in place for these URLs)

API Name = `Swivel_Sentry`

Entity ID = `https://saml.salesforce.com`

55.4 Determine and configure your SSO username attribute

Prior to configuration, you will need to determine which username attribute will be used for authentication and single sign on. For example you may wish to use the email attribute, or the sAMAccountName (default Active Directory username) or something else like an employee or security ID.

Username attribute examples:

Email attribute: email e.g. j.smith@mycompany.net

AD username: sAMAccountName e.g. jsmith

When a user attempts to authenticate to the Salesforce Application or any other configured application, they will need to enter this username in the Login page presented by the Swivel Sentry.

55.5 Configuring the federated ID in Salesforce.com

Against the User's profile there is an area when you can configure the user's federated ID. This could be their email address or Active Directory username for example.

Mailing Address

Street	<input type="text"/>
City	<input type="text"/>
State/Province	<input type="text"/>
Zip/Postal Code	<input type="text"/>
Country	<input type="text"/>

Single Sign On Information

Federation ID	<input type="text" value="dcroft"/>
---------------	-------------------------------------

Additional Information

Can Delete Opportunities ☐

Locale Settings

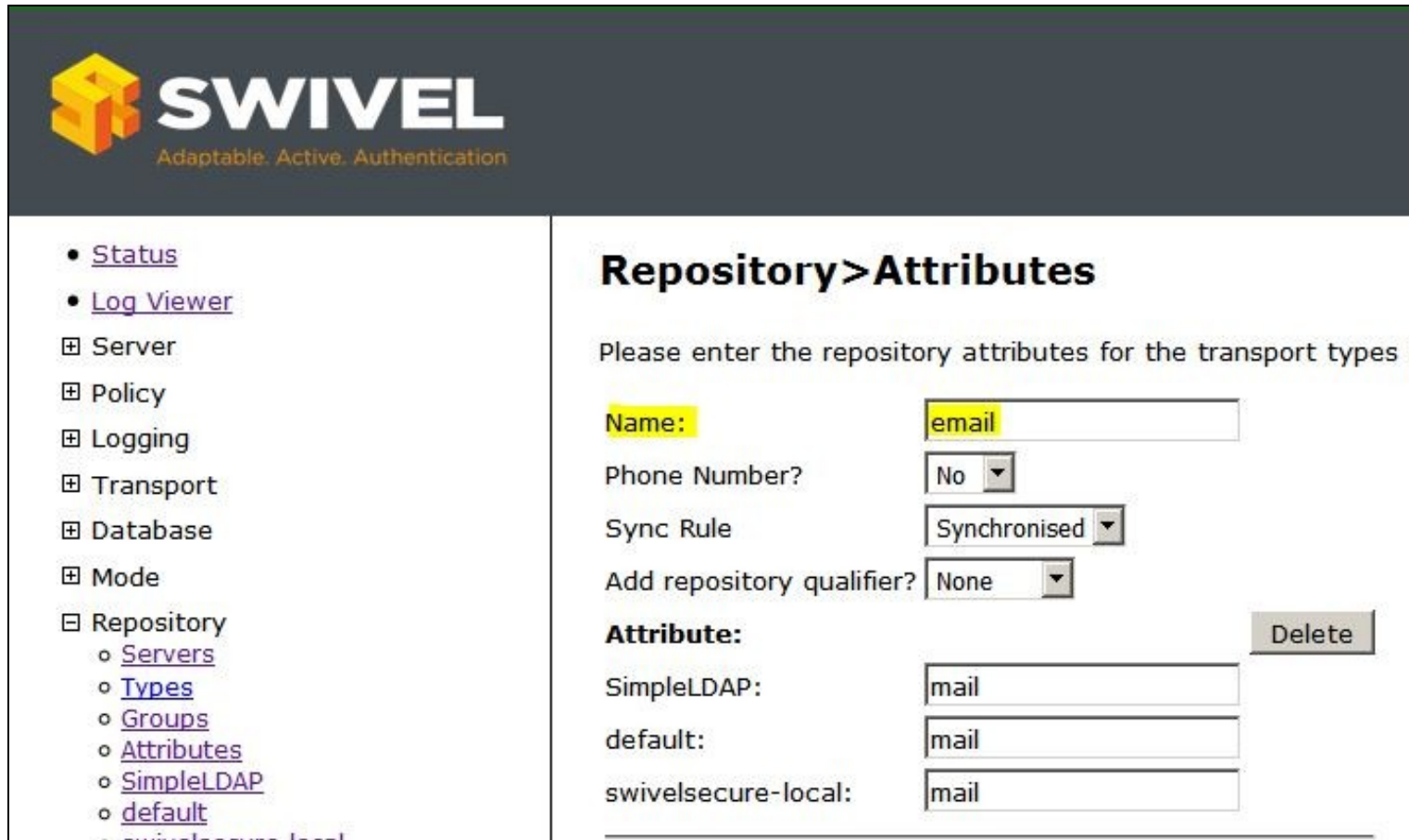
Time Zone	<input type="text" value="(GMT+01:00) British Summer Time (Europe/London)"/>
Locale	<input type="text" value="English (United Kingdom)"/>
Language	<input type="text" value="English"/>
Currency	<input type="text" value="GBP - British Pound"/>

55.6 Configuring alternative username attributes in the Swivel Core

If you have already imported the users into the Swivel Core with a particular username attribute, but wish to use another attribute for SSO and authentication, then you will need to configure an alternative attribute or delete and import the users into the Swivel Core again with the correct attribute.

The Swivel Core allows the use of any attribute for the username provided that it is imported into the Swivel Core database during User Sync. The use of alternative attributes can be configured upon the Server -> Agent definition in the Swivel Core.

Below you can see an example of email attribute.



SWIVEL
Adaptable. Active. Authentication

- [Status](#)
- [Log Viewer](#)
- ▣ Server
- ▣ Policy
- ▣ Logging
- ▣ Transport
- ▣ Database
- ▣ Mode
- ▣ Repository
 - [Servers](#)
 - [Types](#)
 - [Groups](#)
 - [Attributes](#)
 - [SimpleLDAP](#)
 - [default](#)
 - [swivelsecure-local](#)

Repository > Attributes

Please enter the repository attributes for the transport types

Name:

Phone Number?

Sync Rule

Add repository qualifier?

Attribute:

SimpleLDAP:	<input type="text" value="mail"/>
default:	<input type="text" value="mail"/>
swivelsecure-local:	<input type="text" value="mail"/>

As another example, here is another attribute you might consider, on the Repository -> Attributes screen (altusername) which maps to the userPrincipalName on the Active Directory repository:

- [Administration Guide](#)
- [Logout](#)

Name:	<input type="text" value="username"/>	
Phone Number?	<input type="text" value="No"/>	
Sync Rule	<input type="text" value="Synchronised"/>	
Add repository qualifier?	<input type="text" value="None"/>	
Attribute:		<input type="button" value="Delete"/>
SimpleLDAP:	<input type="text" value="cn"/>	
default:	<input type="text"/>	
swivelsecure-local:	<input type="text" value="sAMAccountName"/>	

Name:	<input type="text" value="altusername"/>	
Phone Number?	<input type="text" value="No"/>	
Sync Rule	<input type="text" value="Synchronised"/>	
Add repository qualifier?	<input type="text" value="None"/>	
Attribute:		<input type="button" value="Delete"/>
SimpleLDAP:	<input type="text" value="uid"/>	
default:	<input type="text"/>	
swivelsecure-local:	<input type="text" value="userPrincipalName"/>	

Again you need to be careful to enter the ?Name? such as username or altusername (highlighted) and not one of the repository mappings such as sAMAccountName or userPrincipalName.

55.7 Configure Check Password with Repository on the Swivel Core

In order to check the user?s Active Directory password, ensure that the local Agent is configured as explained [here](#)

55.8 Setup Sentry Application definition

Please note: you must have setup a Salesforce domain prior to defining this Application entry within Swivel Sentry. This is so that you are able to populate the Endpoint URL field. Login to the Swivel Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for Salesforce, click the Add Provider button.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACO is SAML (Security Assertion Markup Language)

Name

Salesforce

Image

Salesforce.png

Points

0

Portal URL

https://yourdomain.salesforce.com

Endpoint URL

Entity ID

https://saml.salesforce.com

Federated Id

email

- **Name:** Salesforce (Type an Arbitrary name for this Application)
- **Image:** Salesforce.png (selected by default)
- **Points:** 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)
- **Portal URL:** (this Endpoint URL can be found on the Setup -> Security Controls -> Single Sign-On Settings page in Salesforce.com, listed as ?Salesforce Login URL? under the Endpoints section. It is unique to your Salesforce.com instance and domain. Example: <https://companyname.my.salesforce.com?so=00E32000000cx70>. This requires that you have previously setup a Salesforce domain under Setup -> Domain Management -> Domains and that it is at least listed as ?Domain Ready for Testing? status on Salesforce.com)
- **EndPoint URL:** N/A
- **Entity ID:** <https://saml.salesforce.com> (at the time of writing this documentation, this settings is always the same when using Salesforce, but may be subject to change by Salesforce.com, so please review the online Salesforce documentation if you find that this Entity ID no longer works)
- **Federated id:** email (That needs to match with the attributed defined on Salesforce.com and Swivel Core)

55.9 Setup Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for Salesforce authentication.

Login to the Swivel Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Salesforce Application, this Authentication Method will be offered during login.

55.10 Assign the Salesforce domain to the SSO definition

On Salesforce, select Domain Management -> My Domains. Under the **Authentication Configuration** section, click Edit.

Deselect the **Login Page** checkbox and enable the checkbox of the authentication service that you created on the SAML SSO Settings screen. Click the Save button.

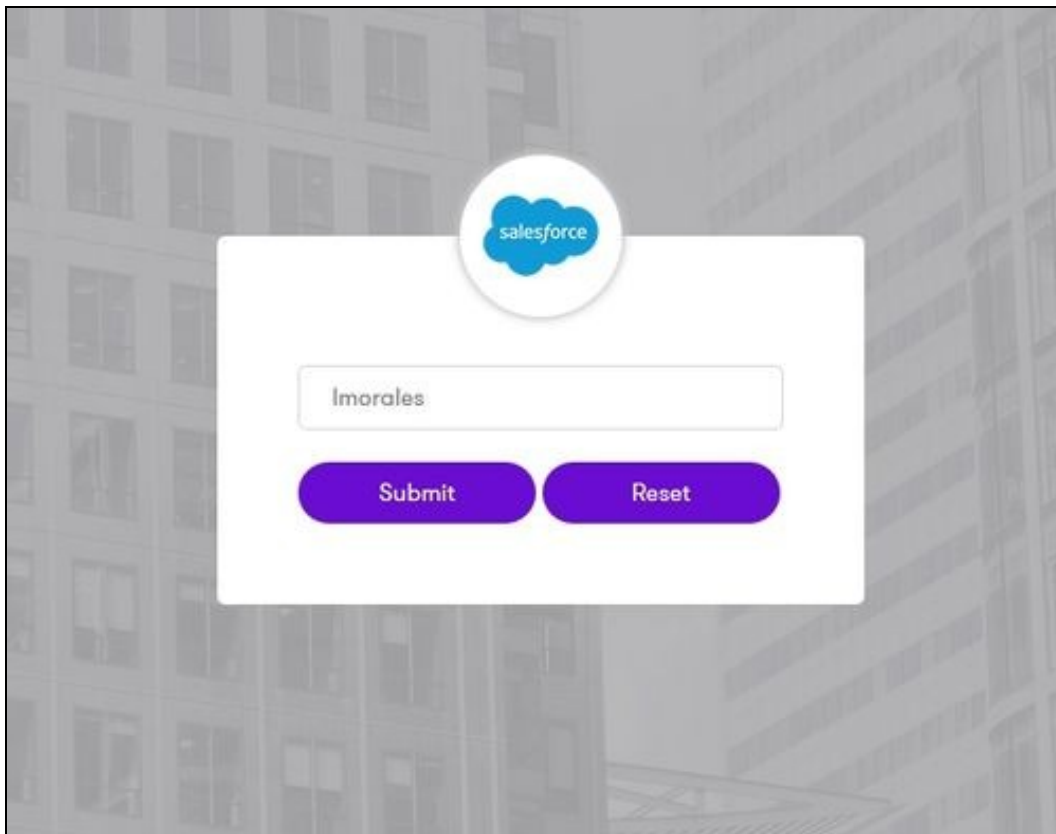
55.11 Testing authentication to Salesforce via Swivel Sentry

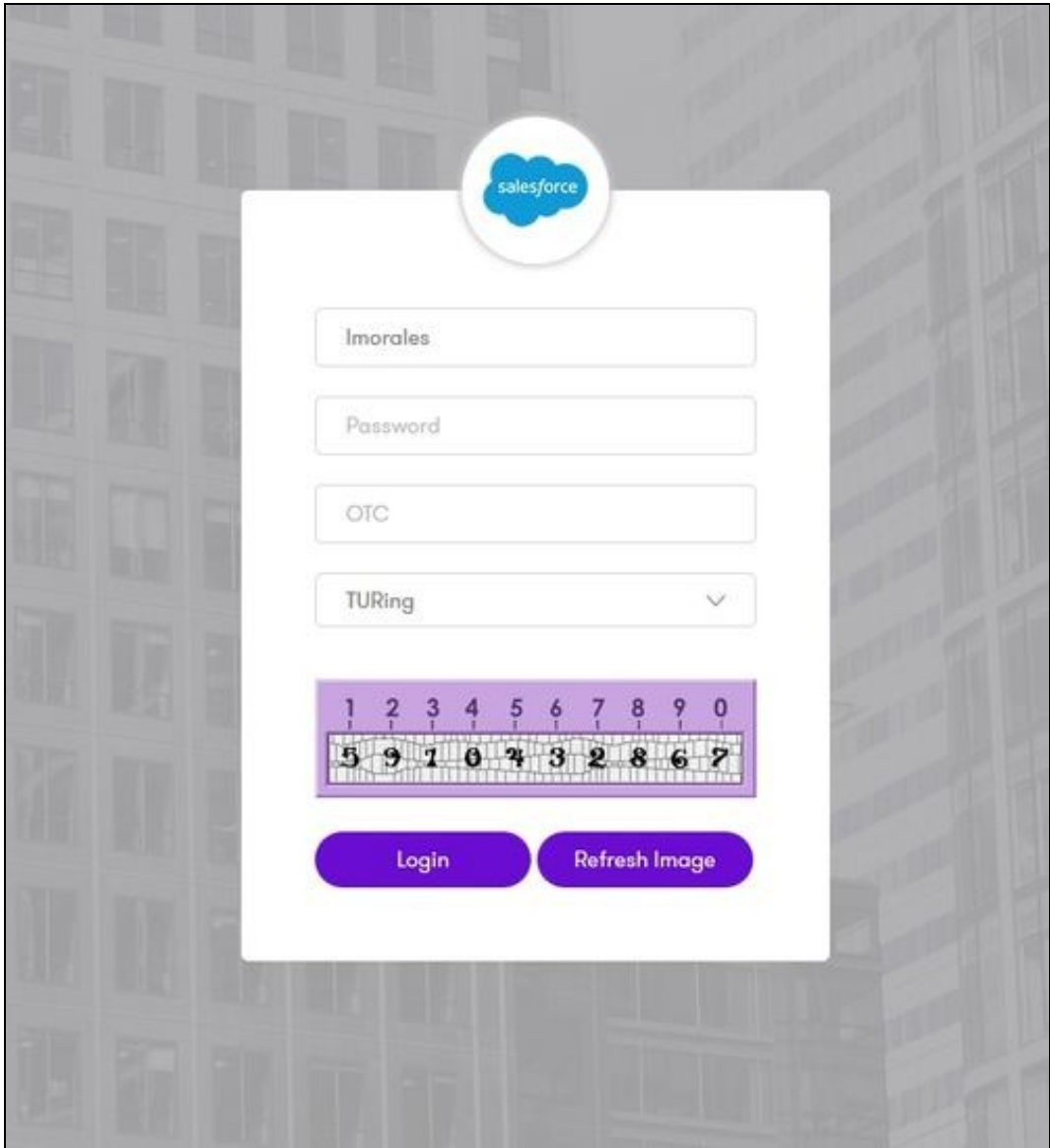
This should be the final step after all previous elements have been configured.

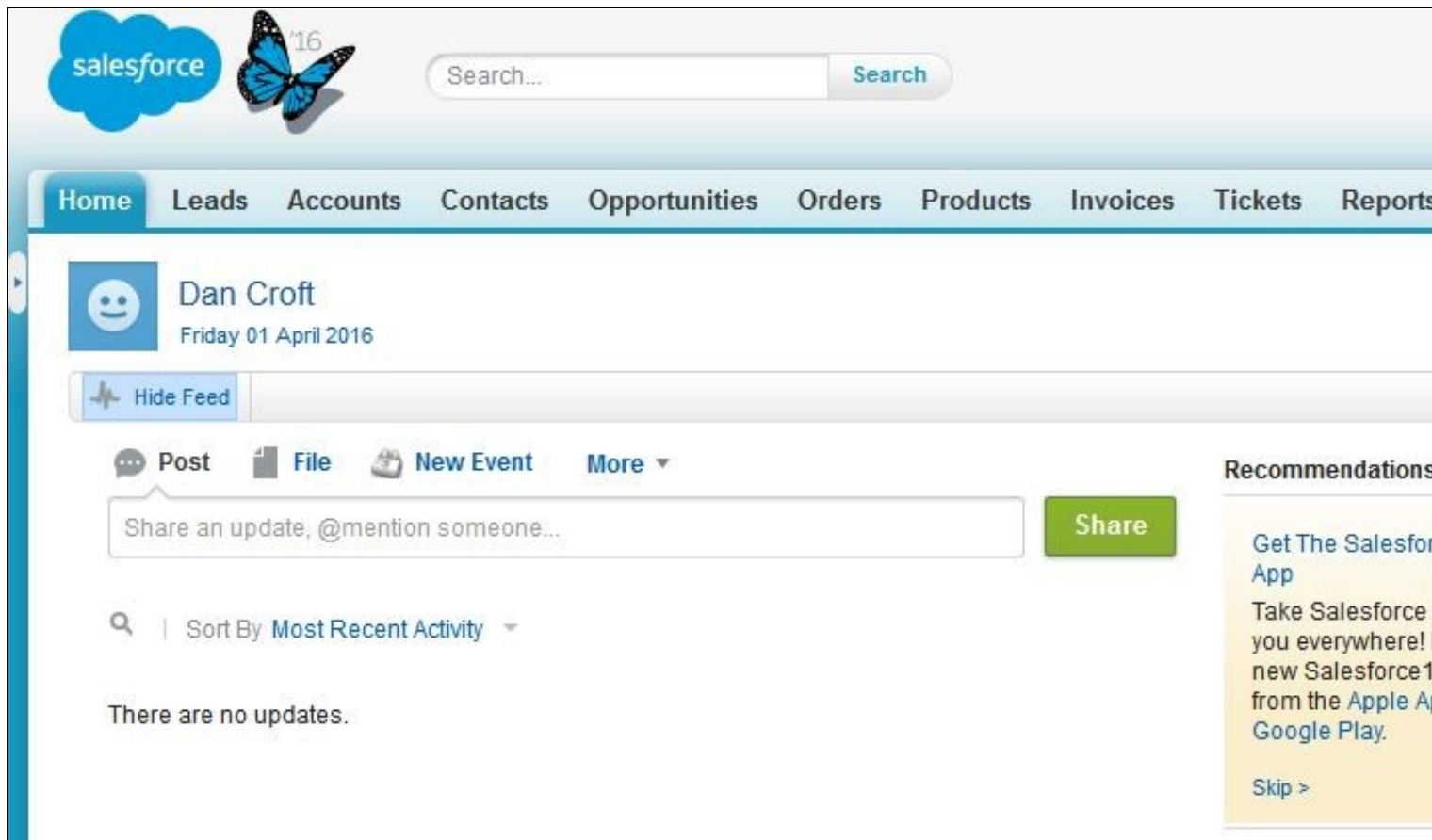
In a web browser, visit the Domain URL that you setup in Salesforce.com which also constitutes the FQDN part of your Endpoint URL e.g. <https://companyname.my.salesforce.com>

When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Salesforce Application definition.

In this login example we are using the username attribute as the federated ID.







55.12 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel Sentry has a View Log menu item which provides details about the SAML assertion and response received from Salesforce and can be useful for comparison with the Salesforce SAML Assertion Validator output;
- Salesforce has a SAML Assertion Validator which can provide diagnostics about the latest SAML authentication attempt. This can be particularly useful for verifying the federated ID and various elements within the SAML assertion that takes place between the Swivel Sentry and Salesforce.com. To get to the SAML Assertion Validator in Salesforce.com select Setup -> Security Controls -> Single Sign-On Settings. At the top of the page you will see the SAML Assertion Validator button:

Quick Find / Search...

[Expand All](#) | [Collapse All](#)

Lightning Experience

Salesforce1 Quick Start

Setup Assistant

Force.com Home

Administer

▸ Manage Users

▸ Manage Apps

▸ Company Profile

▣ Security Controls

Health Check **New!**

Sharing Settings

Field Accessibility

Password Policies

Session Settings

Login Flows

Network Access

Activations

Session Management

Login Access Policies

Certificate and Key Management

Single Sign-On Settings

Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from

- Federated authentication, a single sign-on method that uses SAML as

EditSAML Asses

Federated Single Sign-On Using SAML

SAML Enabled ☒

SAML Single Sign-On Settings

NewNew from M

Action	Name	SAML Version
Edit Del	Swivel Sentry	2.0

Click the button and you will be taken to a screen when you select the name of your Single Sign-On Setting and click Validate:

268

SAML Validator

Enter your SAML response in base64-encoded, deflated and base64-encoded, or plain xml format into the field below, and click V

You can select a config to use to validate the response, or you can automatically detect the config from the response. If the page i manually selecting the appropriate config.

The validator will try to continue validation even if it finds an error. However, the validator cannot recover from some errors. More e errors not related to the assertion itself will not be detected by this validator. Please refer to the login history for more information

Your organization is configured to use SAML Version 2.0

SAML Response

Validate

Swivel Sentry



Once you have clicked the validate button, the Results screen will appear and show some diagnostics.

Results

Unexpected Exceptions

Unable to parse the response
Premature end of file.

1. Validating the Status

Unknown

2. Looking for an Authentication Statement

Unknown

3. Looking for a Conditions statement

Unknown

4. Checking that the timestamps in the assertion are valid

Unknown

5. Checking that the Attribute namespace matches, if provided

Unknown

6. Miscellaneous format confirmations

Unknown

7. Confirming Issuer matches

Unknown

8. Confirming a Subject Confirmation was provided and contains valid timestamps

Unknown

9. Checking that the Audience matches

Unknown

10. Checking the Recipient

Unknown

11. Validating the Signature

Unknown

12. Checking that the Site URL Attribute contains a valid site url, if provided

Unknown

13. Looking for portal and organization id, if provided

Unknown

14. Checking if session security level is valid, if provided

Unknown

Subject:

Unable to map the subject to a Salesforce.com user

AssertionId:

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the Sentry logging or Salesforce.com validator shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ◆ Can Sentry find the Certificate locally, is it the correct one?
 - ◆ Has the correct Certificate been uploaded to Salesforce.com?
- Federated ID mismatch.
 - ◆ Has the Federated ID value been added to the user's Salesforce.com profile?
 - ◆ Has Tomcat been restarted after populating the Sentry settings.properties file with the federated ID username attribute?

- ◆ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?

56 Sentry SSO with ServiceNow

56.1 Introduction

This document describes how to configure ServiceNow to work with Sentry SSO. Before following these instructions, you should be familiar with using Sentry - see the Sentry User Guide for more information.

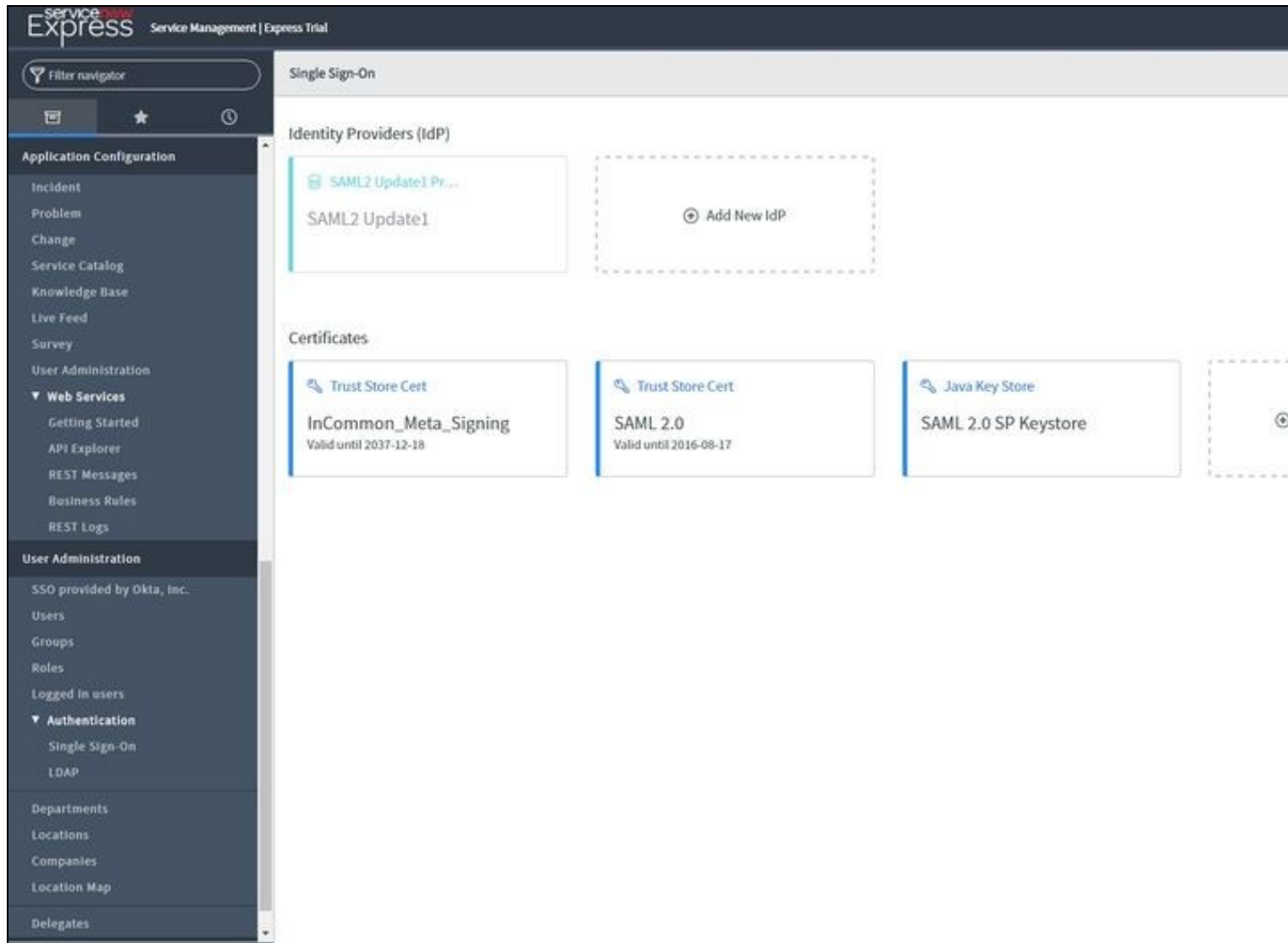
56.2 Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on yourdomain.servicenow.com, you will need to setup some Keys if they were not set up already. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

56.3 Setup SSO on ServiceNow

To configure SSO setting on your ServiceNow accounts you have to access your Admin console by simply going to <https://yourdomain.servicenow.com> You should see an Admin console.

On the left menu you will see a User Administration section. When you click on the Single Sign-On you will be see the following screen. You have to enable the options displayed on the right, which are: "Enable multiple provider SSO" and "Enable Auto Importing of users from all identity providers into the user table" . Click on the button "Add New IdP" and select the User group for which to use SSO. For this example we are using "Swivel Users".



Click on the button "Add New IdP" and click "Manually enter metadata XML".

Filter navigator

Application Configuration

Incident

Problem

Change

Service Catalog

Knowledge Base

Live Feed

Survey

User Administration

Web Services

Getting Started

API Explorer

REST Messages

Business Rules

REST Logs

User Administration

SSO provided by Okta, Inc.

Users

Groups

Roles

Logged in users

Authentication

Single Sign-On

LDAP

Departments

Locations

Companies

Location Map

Delegates

Add New Identity Provider

Configure Identity Provider

IdP Metadata URL

Ex. <http://idp.sso.cisco.com>

Manually enter metadata XML

Fetch

Cancel

Name

Identity Provider URL

Identity Provider's AuthnRequest

Identity Provider's SingleLogoutRequest

Identity Provider Certificate

Active

Default

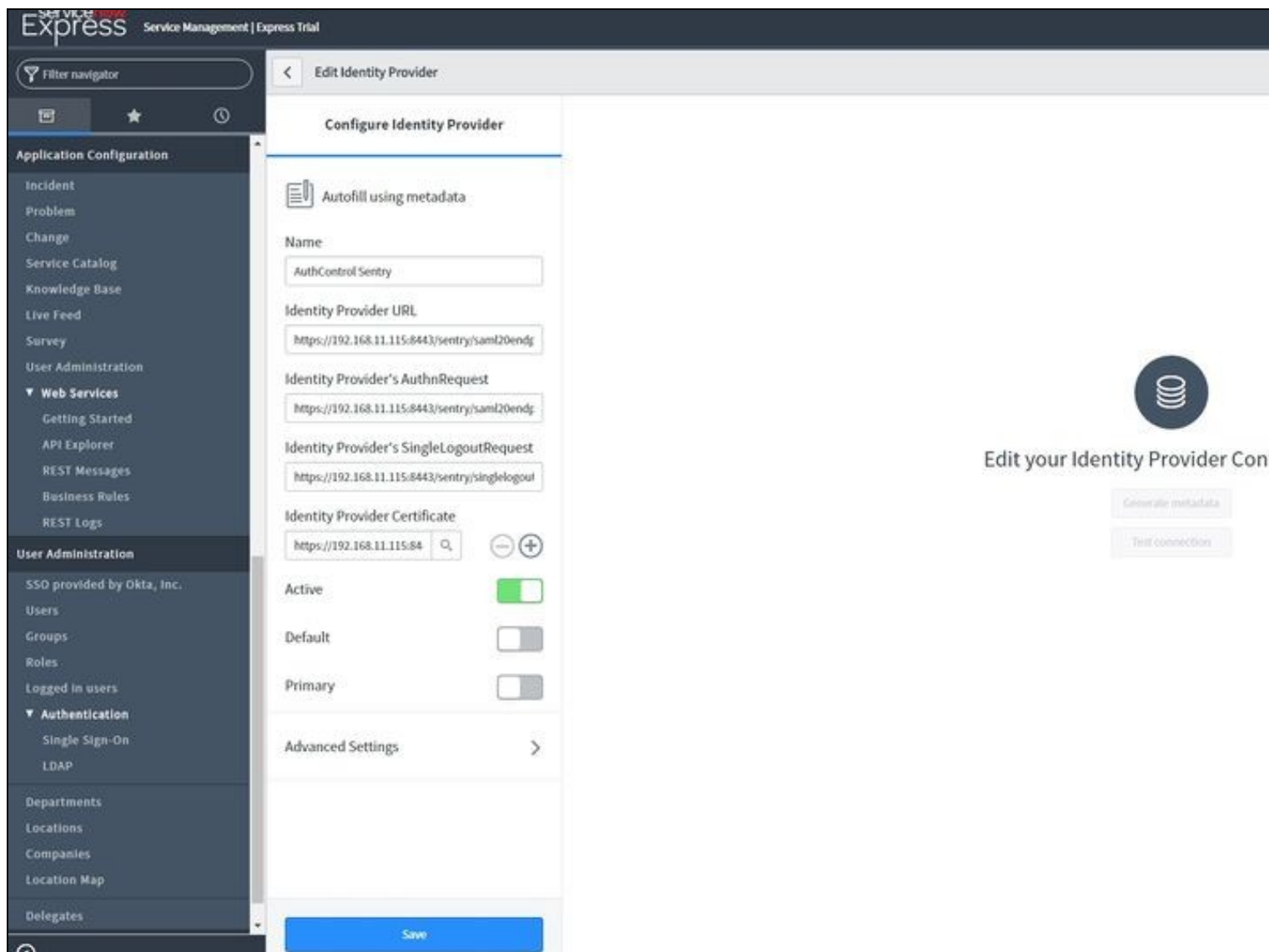
Primary

Advanced Settings

Save

Configure your Identity Provider

Now navigate to your AuthControl Sentry metadata page as below(https://<FQDN_OF_SENTRY_SERVER>/sentry/metadata/generatedMetadata.xml) and copy the content of this page.



After you have entered all the details as above click Save. You can test the connection after setting up Auth Control Sentry

56.4 Configure Check Password with Repository on the Swivel Core

In order to check the user's Active Directory password, ensure that the local Agent defined under Server -> Agents has got the Check Password with repository checkbox enabled. When an authentication occurs in AuthControl Sentry, the Active Directory password will then be passed to Active Directory for verification.

56.5 Setup AuthControl Sentry Application definition

Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for ServiceNow, click the Add Provider button and select ServiceNow SAML.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is enabled for the SAML (Security Assertion Markup Language) request.

Name

ServiceNow

Image

ServiceNow.png



Points

0

Portal URL

https://yourdomain.service-now.com/navpage.s

Endpoint URL

Entity ID

https://yourdomain.service-now.com

Federated Id

email

Save

Name: ServiceNow(Type an Arbitrary name for this Application)

Image: ServiceNow.jpg(selected by default)

Points: 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)

Portal URL: (this Portal URL is ServiceNow login URL which you can usually access on: <https://yourdomain.service-now.com/navpage.do>)

Endpoint URL: N/A

Entity ID: <https://yourdomain.service-now.com> (Entity ID is the one defined on ServiceNow > User Administration > Single Sign-On > AuthControl Sentry Idp > Advanced Settings: Entity ID)

Federated Id: email

56.6 Setup AuthControl Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for ServiceNow authentication.

Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the ServiceNow Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

56.7 Testing connection with ServiceNow tool

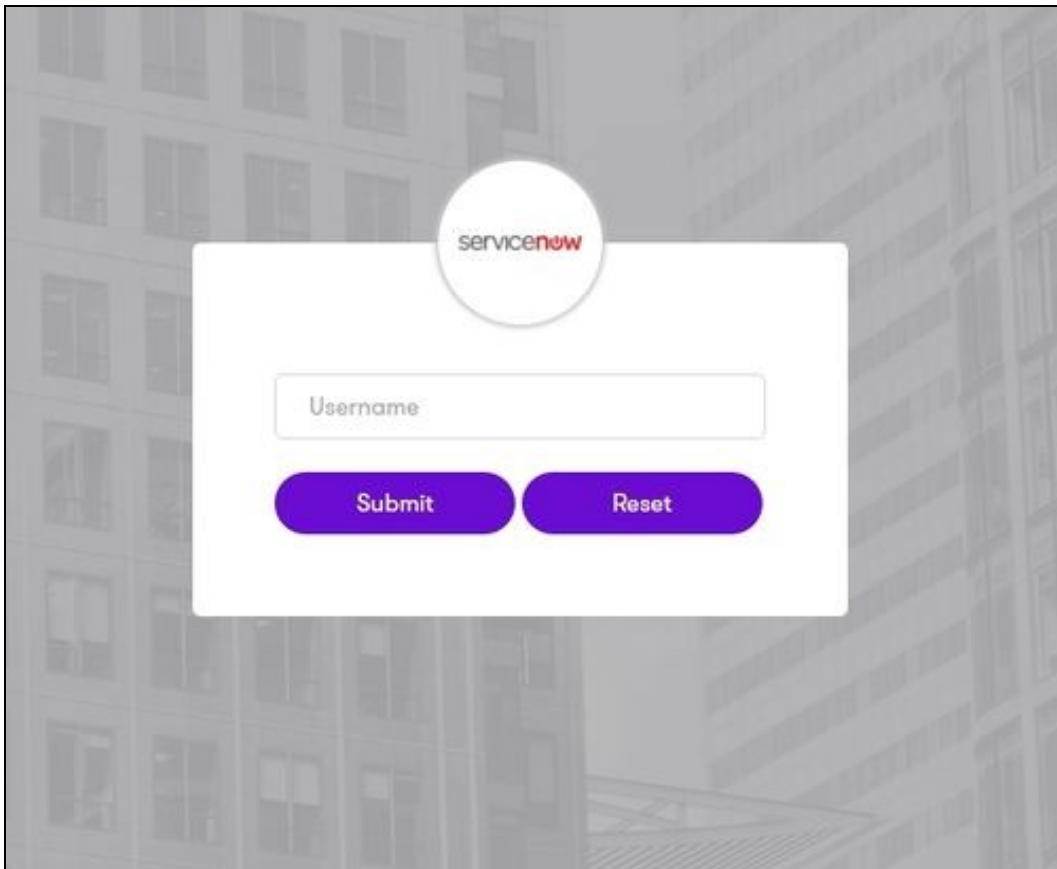
ServiceNow provides a tool to test the connection. Go to User Administration > Single Sign-On and click AuthControl Sentry Idp. After that click Test connection.

The screenshot displays the 'Edit Identity Provider' configuration page in the AuthControl Sentry Administration Console. The left sidebar shows the navigation menu with 'Web Services' expanded, and 'Authentication' > 'Single Sign-On' selected. The main content area is titled 'Configure Identity Provider' and includes the following fields:

- Name:** AuthControl Sentry
- Identity Provider URL:** <https://192.168.11.115:8443/sentry/saml2oendp>
- Identity Provider's AuthnRequest:** <https://192.168.11.115:8443/sentry/saml2oendp>
- Identity Provider's SingleLogoutRequest:** <https://192.168.11.115:8443/sentry/singlelogout>
- Identity Provider Certificate:** <https://192.168.11.115:84>

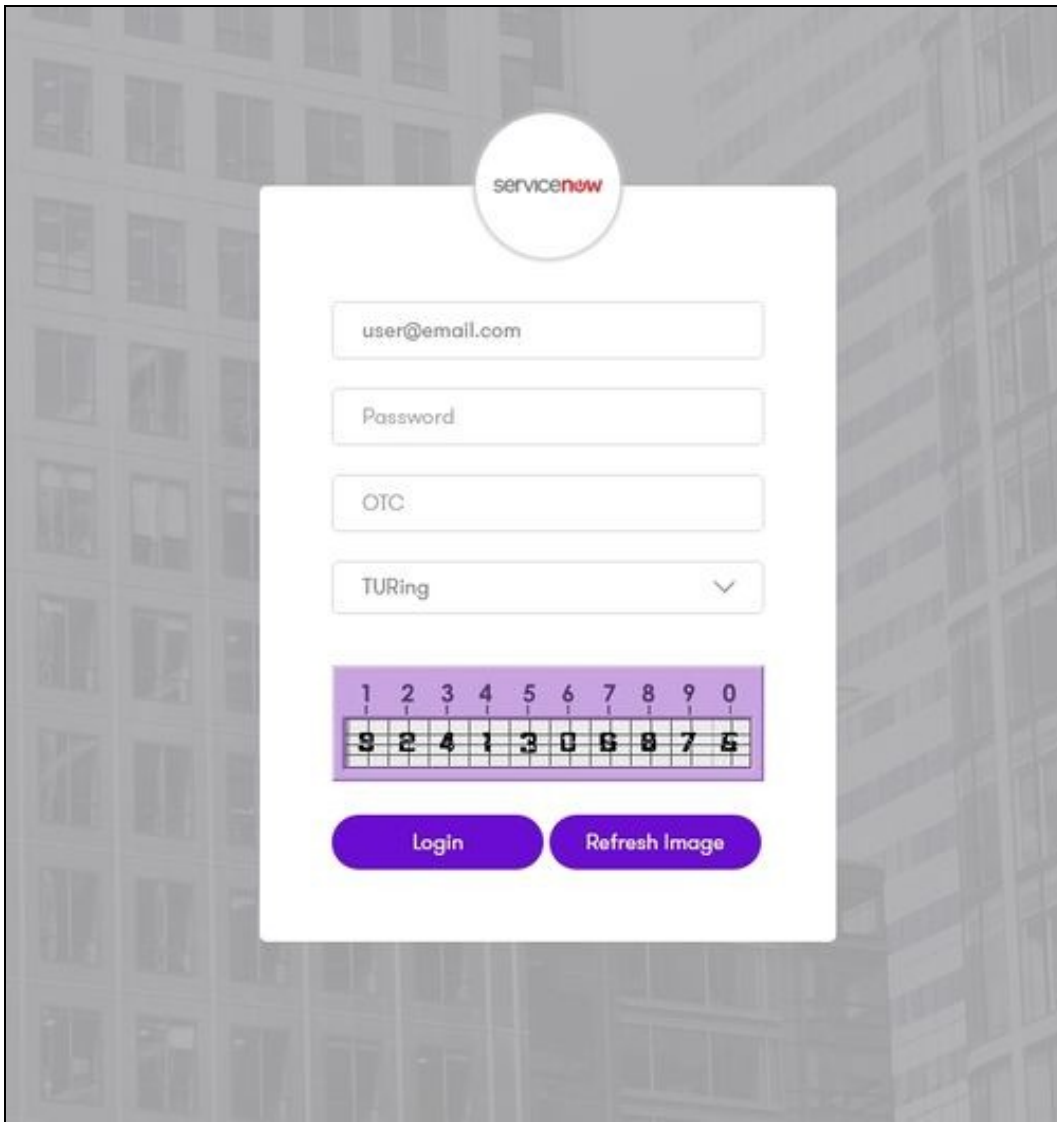
Below the fields are three toggle switches: 'Active' (checked), 'Default' (unchecked), and 'Primary' (unchecked). An 'Advanced Settings' link with a right arrow is also present. At the bottom is a blue 'Save' button. On the right side of the page, there is a circular icon with a database symbol and the text 'Edit your Identity Provider Con'. Below this are two buttons: 'Generate metadata' and 'Test connection'.

A new window will be displayed that will redirect to AuthControl sentry username page.



Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the ServiceNow Application definition.

In this login example we are using the email as a username



After we enter our authentication credentials we will see a logout screen. Close that window and on the ServiceNow page click View Log. Check that the logs indicate that the SAML authentication was successful.

56.8 Testing authentication to ServiceNow via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

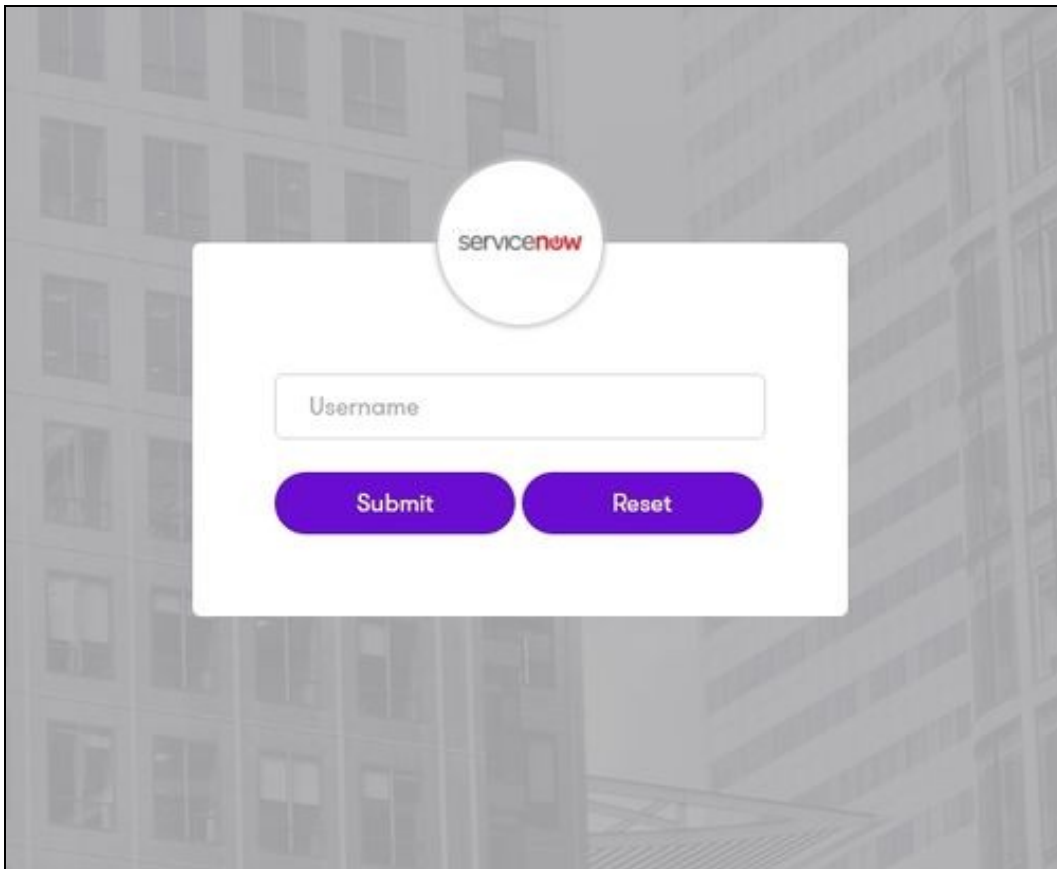
In a web browser, visit the the URL that you setup on AuthControl Sentry as Endpoint URL e.g. <https://yourdomain.service-now.com/navpage.do>

Alternatively you can visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. <https://mycompanysentrydomain/sentry/startPage> On a Start Page you will be able to see a new ServiceNow Icon on which you can click and proceed with authentication (as you would by going straight to the ServiceNow page)

Please select an application

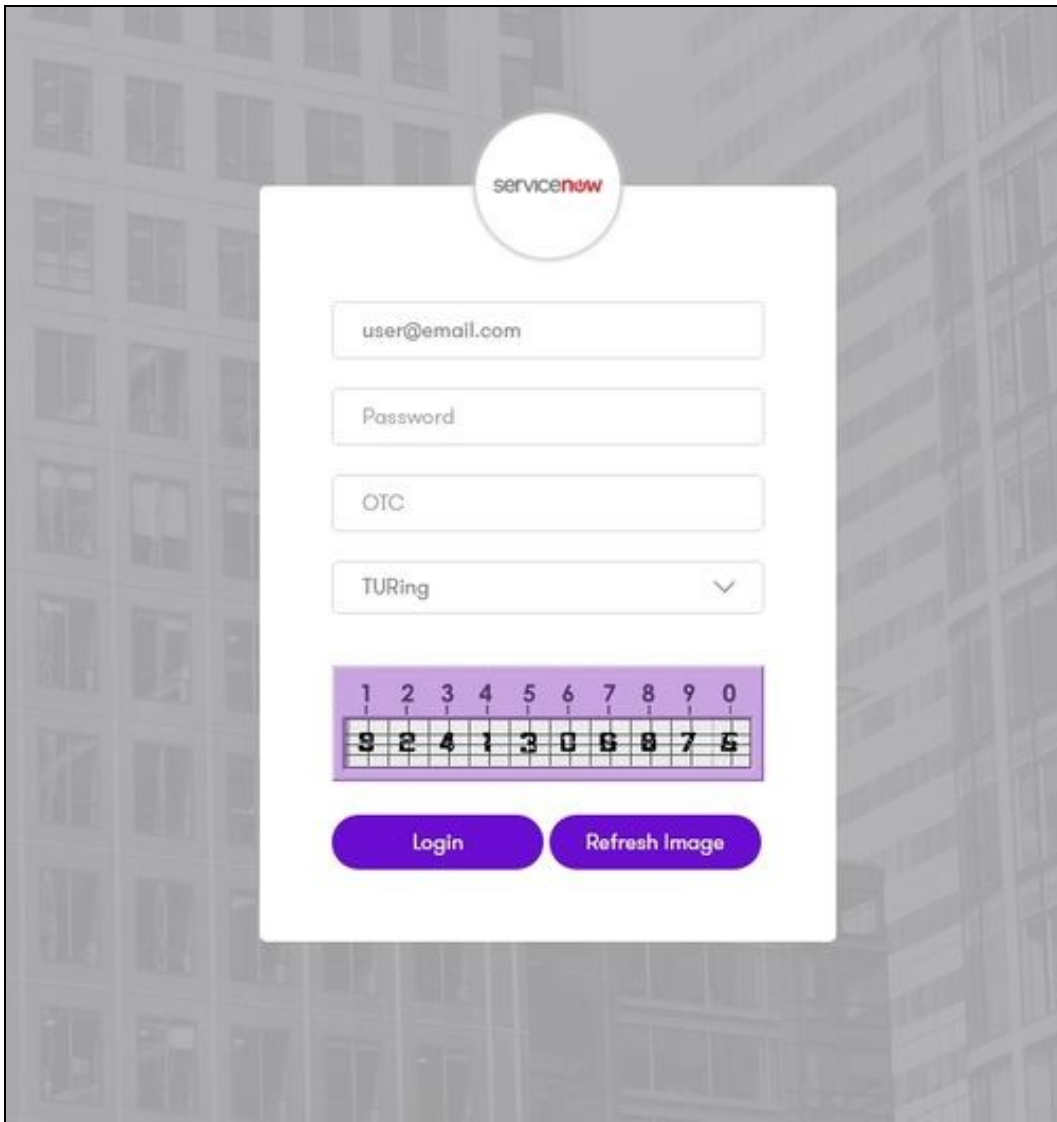
The Mimecast logo, consisting of the word 'mimecast' in a lowercase, sans-serif font.The Google logo, showing the letters 'Go' in blue and 'o' in red.The Juniper Networks logo, with 'JUNIPER' in a large, stylized font and 'NETWORKS' in a smaller font below it.The ServiceNow logo, with 'servicenow' in a lowercase font where 'now' is in red.The GoTo logo, featuring a stylized orange flower icon followed by the text 'GoTo'.

When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup.



Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the ServiceNow Application definition.

In this login example we are using the email as a username



After we enter our authentication credentials we successfully will see the ServiceNow account that we tried to access.

56.9 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from ServiceNow
- The ServiceNow has a Test Connection feature that provides details about the SAML response received from AuthControl Sentry

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

If you have issues login in with then SAML authentication to the admin console you can always access by https://yourdomain.service-now.com/side_door.do

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ♦ Can AuthControl Sentry find the Certificate locally, is it the correct one?
 - ♦ Has the correct Metadata been uploaded to the ServiceNow?
 - ♦ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?

57 Sentry SSO with SonicWall

57.1 Setup AuthControl Sentry Keys

Before you are able to create a Single Sign On configuration on SonicWall, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

57.2 Setup SSO on SonicWall

To configure SSO setting on your SonicWall account you have to create a new authentication server on your Admin console. You should see an screen similar to the one below:

Security Administration

Access Control

Resources

Users & Groups

User Access

Realms

WorkPlace

Agent Configuration

End Point Control

System Configuration

General Settings

Network Settings

SSL Settings

Authentication Servers

Services

Virtual Assist

Maintenance

Monitoring

User Sessions

System Status

Logging

Troubleshooting

New Authentication Server

Authentication Servers > New Authentication Serv

Choose the protocol used to access your user store, and specify how users will authenticate. Click Continue to configure the authentication server.

User store

Choose the directory type or authentication method:

Authentication directory

☒ Dell Defender

☐ Microsoft Active Directory (Basic)

A single domain.

☐ Microsoft Active Directory (Advanced)

Multiple domains in a tree or forest.

☐ LDAP

☐ RADIUS

☐ RSA Authentication Manager

☐ Public key infrastructure (PKI)

☒ SAML 2.0 Identity Provider

Single sign-on server

☐ RSA ClearTrust

Sign-on to ClearTrust is supported only from a Web browser.

Local user storage

☐ Local users

Credential type

Specify how users will authenticate:

☐ Digital certificate

☐ Token/SecurID

☒ Username/Password

Continue...

Cancel

You will need to select SAML 2.0 and Username/Password as Credential Type. Then click Continue.

284

Security Administration

Access Control

Resources

Users & Groups

User Access

Realms

WorkPlace

Agent Configuration

End Point Control

System Configuration

General Settings

Network Settings

SSL Settings

Authentication Servers

Services

Virtual Assist

Maintenance

Monitoring

User Sessions

System Status

Logging

Troubleshooting

Configure Authentication Server

Authentication Se

Configure settings for a SAML 2.0 Identity Provider (IdP) authentication

Name:*

SAML_Test

Appliance ID:*

https://sslvpn.companyname.com

Server ID:*

demo.swivelcloud.com/sentry/

Authentication service URL:*

https://demo.swivelcloud.com/sentry/saml20endpoint

Logout service URL:

https://demo.swivelcloud.com/sentry/singlelogout

Trust the following certificate:*

demo.swivelcloud.com

☒ Sign AuthnRequest message using this certificate:

sslvpn.companyname.com

Save

Cancel

Name - Type an arbitrary name

Appliance ID - `https://YOURDOMAIN` That value will need to match with the Entity ID attribute specified on the SonicWall application configured on Sentry
 Set the Login, Logout and Change password URLs below, where `<FQDN_OF_SENTRY_SERVER>` is the public DNS entry of your Swivel AuthControl Sentry server, e.g. `swivel.mycompany.com` or if you do not have a redirect from port 443 to 8443 in place, you may need to include a port number e.g. `swivel.mycompany.com:8443`
 Authentication service URL - `https://<FQDN_OF_SENTRY_SERVER>/sentry/saml20endpoint`

Logout service URL - `https://<FQDN_OF_SENTRY_SERVER>/sentry/singlelogout`

Trust the following certificate - You will need to import the RSA PEM file created earlier on Sentry

After you have entered all the details as below click Save

57.3 Configure Check Password with Repository on the Swivel Core

In order to check the user's Active Directory password, ensure that the local Agent is configured as explained [here](#)

57.4 Setup AuthControl Sentry Application definition

Please note: you must have setup a SonicWall SSO prior to defining this Application entry within AuthControl Sentry. This is so that you are able to populate the Endpoint URL field. Login to the AuthControl Sentry Administration Console. Click Applications in the left hand menu. To add a new Application definition for SonicWall, click the Add Provider button.

Rules

Applications

Authentication Methods

View IdP Metadata

Keys

Users Active Sessions

User History

Log Viewer

General Configuration

Application Images

SAML Application



Note: The Endpoint URL is used only if the ACS SAML (Security Assertion Markup Language) re

Name

SonicWall

Image

SonicWall.png

Points

0

Portal URL

https://sonicwall.yourdomain.com

Endpoint URL

https://sonicwall.yourdomain.com

Entity ID

https://sonicwall.yourdomain.com

Federated Id

email

- **Name:** SonicWall
- **Image:** SonicWall.png (selected by default)
- **Points:** 100 (the number of points the user needs to score from their Authentication Method in order to successfully authenticate to this Application)
- **Endpoint URL:** https://sonicwall.yourdomain/saml2ssoconsumer
- **Portal URL:** (this Portal URL is your companies google docs URL which you can usually access on: https://sonicwall.yourdomain)
- **Entity ID:** https://sonicwall.yourdomain (it needs to match with the value defined on SonicWall Appliance ID attribute)
- **Federated id:** email

57.5 Setup AuthControl Sentry Authentication definition

As an example here we will be using Turing authentication as the Primary method required for Google authentication.

Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the Turing option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the SonicWall Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

57.6 Testing authentication to SonicWall via Swivel AuthControl Sentry

This should be the final step after all previous elements have been configured.

You can visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g.

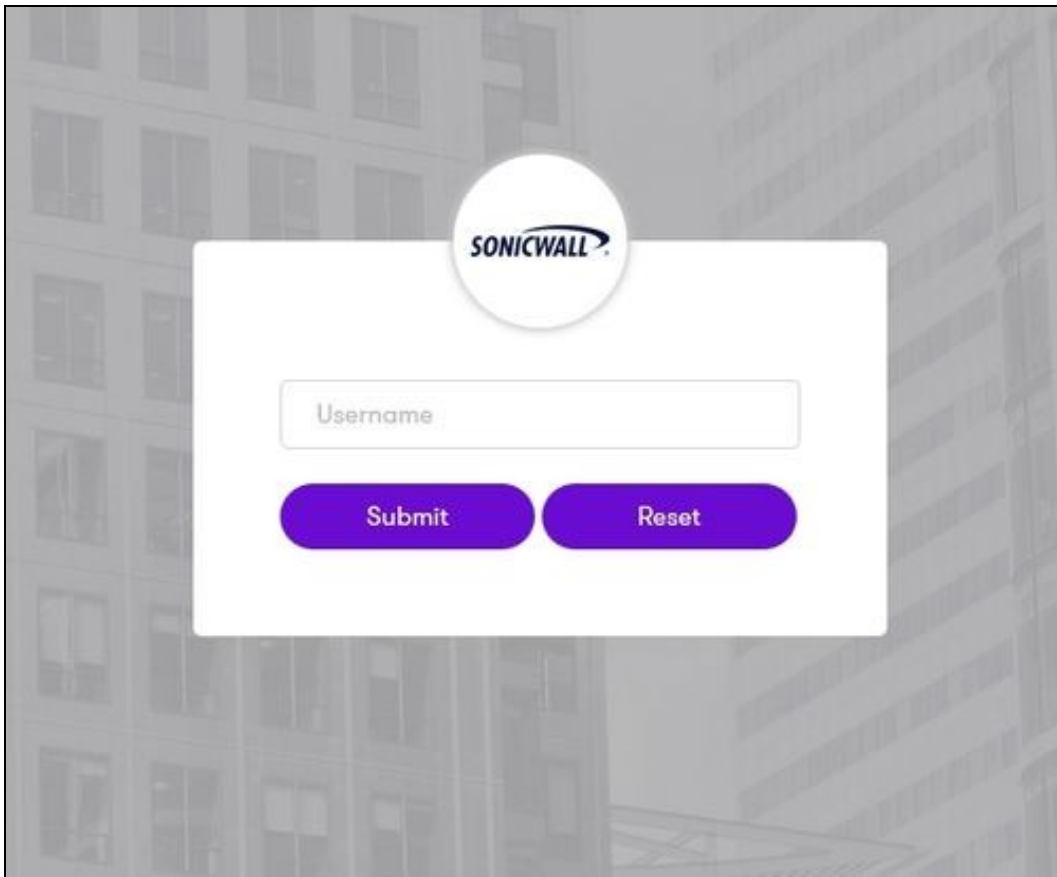
https://mycompanysentrydomain/sentry/startPage On a Start Page you will be able to see a new SonicWall Icon on which you can click and proceed with authentication (as you would by going straight to the google page)

Please select an application

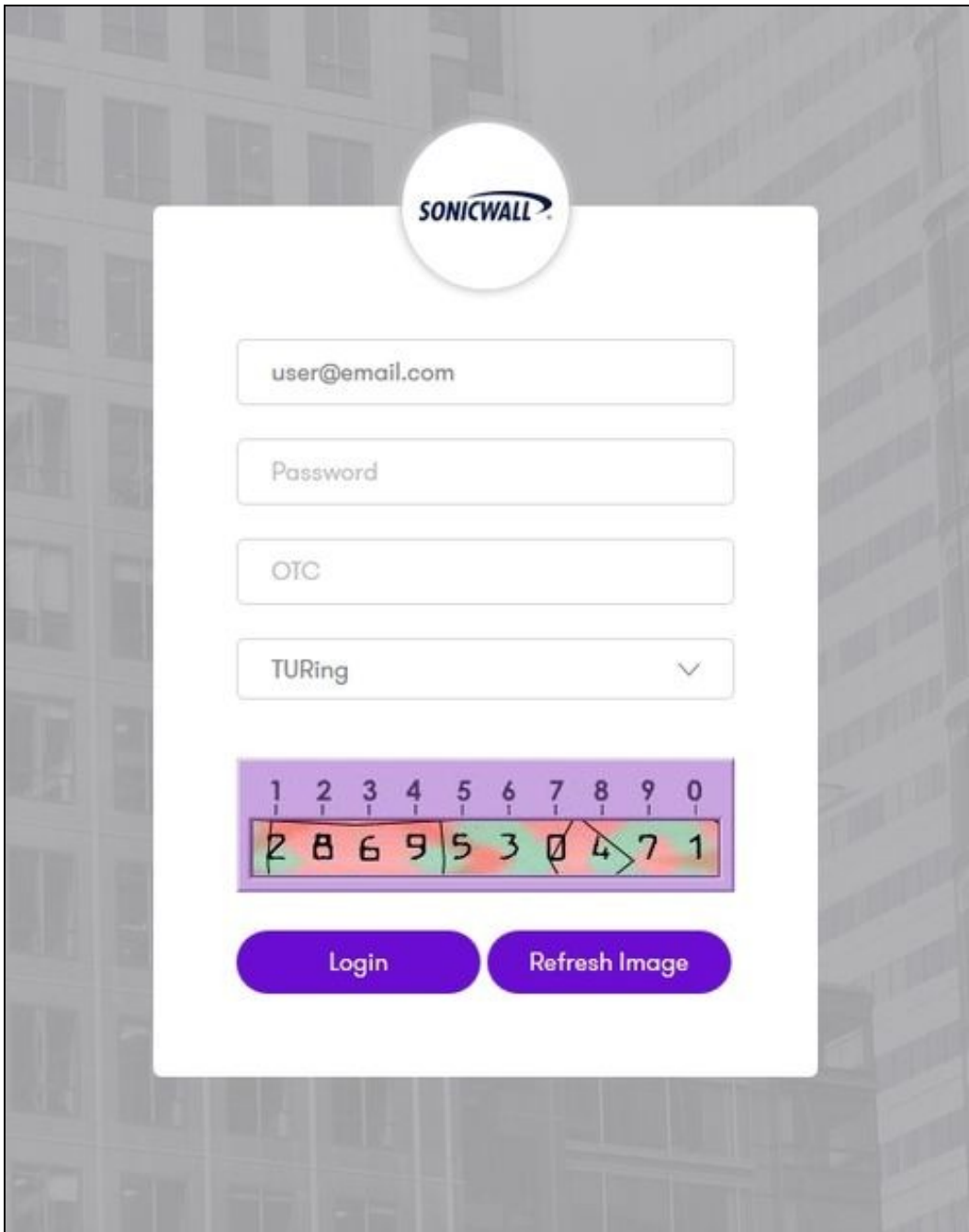
The Mimecast logo, consisting of the word 'mimecast' in a lowercase, sans-serif font.The Juniper Networks logo, with 'JUNIPER' in a large, thin, sans-serif font and 'NETWORKS' in a smaller, bold, sans-serif font below it.The ServiceNow logo, with 'service' in a lowercase sans-serif font and 'now' in a bold, lowercase sans-serif font, both in a dark red color.

When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup, once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the SonicWall Application definition.

In this login example we are using the email as a username



After we enter the username we are prompted with another authentication method (in this example we use turing)



After we enter our authentication credentials we successfully will see the SonicWall that we tried to access.

57.7 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

- The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been started for the image request;
- The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from SonicWall and can be useful for comparison with the SonicWall SAML Assertion Validator output;

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTC correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

- Certificate or decryption issues;
 - ◆ Can AuthControl Sentry find the Certificate locally, is it the correct one?
 - ◆ Has the correct Certificate been uploaded to SonicWall?
 - ◆ Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core since modifying this?

58 Sentry SSO with Thycotic Secret Server

58.1 Introduction

This document describes how to configure Thycotic Secret Server to work with AuthControl Sentry SSO. Before following these instructions, you should be familiar with using Sentry - see the Sentry User Guide for more information.

Also refer to the official Thycotic SAML integration guide for Secret Server version 10.5+:
<https://thycotic.force.com/support/s/article/SS-SAML-Config-Guide>

58.2 Setup AuthControl Sentry Keys

Before you are able to create a SAML configuration in Thycotic Secret Server, you will need to setup some Keys. Please see a separate article: [HowToCreateKeysOnCmi](#). You will need the certificate you generate in a later section of this article. This can be retrieved from the View Keys menu option of Swivel AuthControl Sentry.

58.3 Convert Sentry Keys to PFX

You will need to retrieve the keys generated above from the /home/swivel/.swivel/sentry/keys folder so that you are able to convert from PEM format to a PFX file containing the private key.

The openssl command to achieve a PEM to PFX conversion is as follows:

```
openssl pkcs12 -export -out Cert.pfx -in cert.pem -inkey key.pem
```

You will be prompted for a password for the private key and a password for the PFX you are creating This command assumes:

- Cert.pfx is the file being created
- cert.pem is the cert file downloadable from the AuthControl keys GUI
- key.pem is the private key you download from the /home/swivel/.swivel/sentry/keys folder using WinSCP

58.4 Download the Sentry SSO IdP metadata

In the Sentry SSO Web GUI (running on port 8443), right click on the 'View IdP Metadata' left hand menu option and 'Save As' an xml file e.g. SwivelIdPMetadata.xml. We will upload this to the Thycotic Secret Server in a moment.

58.5 Setup SAML on Thycotic Secret Server

Login to Thycotic Secret Server as an administrator. You should see a SAML tab where you can perform the SAML configuration:

Thycotic Secret Server 10.6
Platinum Edition

Search Secrets Search HOME TOOLS ADMIN REPORTS

An update is available (10.6.000001)

SAML Configuration

General Login **SAML** Folders Local User Passwords Security Ticket System Email Session Recording HSM

SAML General Settings

SAML Enabled Yes
Use Legacy SAML No

[Edit](#)

SAML Service Provider Settings

Name [Redacted]
Certificate Friendly Name
Subject CN=[Redacted], O=[Redacted] C=GB
Thumbprint [Redacted]
Expiration Date [Redacted]

[Edit](#) [Download Service Provider Metadata \(XML\)](#)

Identity Providers

[Create New Identity Provider](#)

Display Name	Name	Description	Certificate
https://[Redacted]:8443/sentry/saml20endpoint	https://[Redacted]:8443/sentry/saml20endpoint		[Redacted]

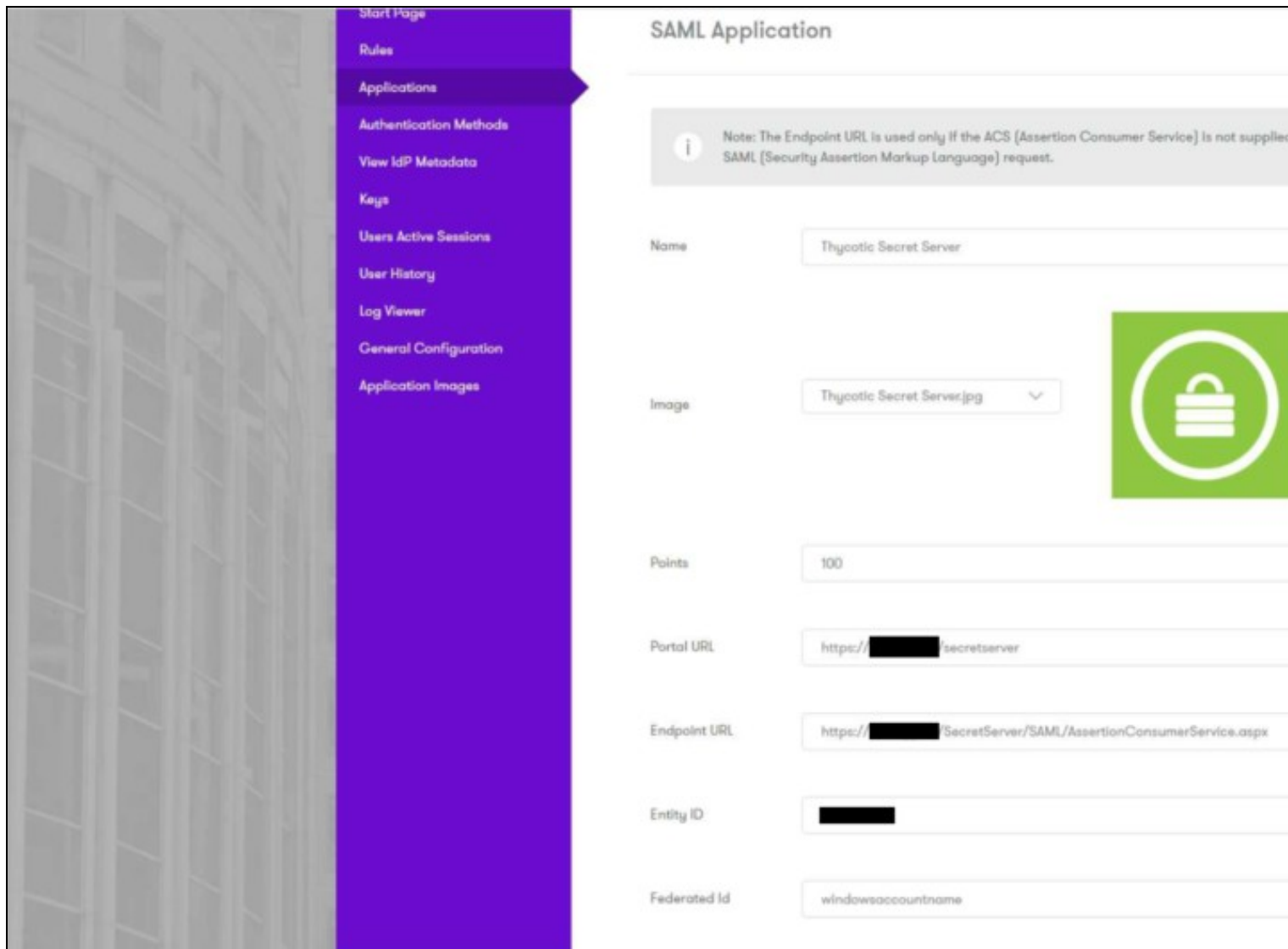
[View Log](#) [View Audit](#)

Get Help Status
Copyright © Thycotic, 2019

thycotic

- Enable SAML by checking the checkbox. Note: it's worth noting that there is a URL to facilitate a local login in the event that SAML is not configured correctly. We recommend you read the Thycotic user manual to have this as a backup option prior to your SAML implementation attempt.
- Under SAML -> Service Provider settings, select a certificate and browse to the PFX certificate created earlier.
- Under Identity Providers, select 'Create New Identity Provider'. This is where you will upload the IdP metadata file from earlier (e.g. SwivelIdPMetadata.xml that you saved from the 'View IdP Metadata' menu option in the Sentry SSO Web GUI). This should import successfully and populate all the endpoint URLs. The FQDN of these URLs should be valid. If not, login to the Swivel Secure CMI -> Main Menu -> Appliance -> Sentry and set the Base URL to be correct. Then export the IdP metadata again and repeat these steps to attempt to create a new identity provider.
- Download the Service Provider metadata and open this in a text editor such as Notepad. Locate the entityID. This will be used in the Sentry SSO Application definition in a moment.

58.6 Setup Thycotic Secret Server as a Sentry SSO Application definition



In the Sentry SSO Web GUI (running on port 8443):

- Locate a Thycotic logo online and upload this via the Application Images option
- Create a new Application definition using the SAML -> Other option
 - ◆ Name: Thycotic Secret Server
 - ◆ Image: (select the image you just uploaded)
 - ◆ Points: 100 - or whatever fits your risk profile if you have already deployed Sentry session
 - ◆ Portal URL: https://<thycoticsecretserverhostname>/secretserver
 - ◆ Endpoint URL: https://<thycoticsecretserverhostname>/SecretServer/SAML/AssertionConsumerService.aspx
 - ◆ Entity ID: enter the EntityID you copied from the Service Provider metadata (just the value from the XML without quotes)
 - ◆ FederatedID: (this will vary according to your installation) windowsusername
 - ◊ windowsusername will need to be setup as a username attribute in the Sentry Core GUI running on port 8080 under Repository -> Attributes if it does not exist already. See section below.

58.7 Configure windowsusername attribute

58.7.1 In Swivel Core

Thycotic Secret Server requires the username to be in the format domain\username if integrated with AD. To do this, you need to create a Swivel attribute that includes the prefix.

In the Swivel admin console, under the repository details for the relevant AD repository, set the domain qualifier to be the short-form domain name, followed by "\" - don't forget the backslash at the end.

- [Status](#)
- [Log Viewer](#)
- ⊞ Server
- ⊞ Policy
- ⊞ Logging
- ⊞ Transport
- ⊞ Database
- ⊞ Mode
- ⊞ Repository
 - [Servers](#)
 - [Types](#)
 - [Groups](#)
 - [Attributes](#)
 - [Repos Admin](#)
 - [AD](#)
- ⊞ RADIUS
- ⊞ Migration
- ⊞ Windows GINA
- ⊞ Appliance
- ⊞ OATH
- ⊞ Config Sync
- ⊞ Reporting
- [User Administration](#)
- [Save Configuration](#)
- [Administration Guide](#)
- [Logout](#)

Repository>AD

Please enter the details for accessing Active Directory

Hostname/IP:

Username:

Password:

Port:

Allow self-signed certificates:

Synchronization schedule:

Username attribute:

Mark missing users as deleted:

Initial PIN attribute:

Initial password attribute:

Import disabled users:

Import disabled state:

Ignore FQ name changes:

Reformat Phone Number:

Prefix to remove:

Prefix to add:

Add domain qualifier:

Repository Domain Qualifier:

Allow expired passwords:

Under Repository -> Attributes, create an attribute - for example, call it "windowsaccountname". In the definition for the AD repository, put the AD attribute name "sAMAccountName", and under domain qualifier, select "As Prefix".

Name:	<input type="text" value="windowsusername"/>
Phone Number?	<input type="text" value="No"/>
Add repository qualifier?	<input type="text" value="As Prefix"/>
Sync Rule	<input type="text" value="Synchronised"/>
Attribute:	<input type="button" value="Delete"/>
Repos_Admin:	<input type="text"/>
AD:	<input type="text" value="sAMAccountName"/>

Finally, synchronise the AD repository, to ensure that all users have an attribute in the form domain\username.

Click save. You will see something like the below. Click save again.

58.8 Login Example

As an example here we will be using OATH authentication as the Primary method required for Thycotic Secret Server authentication.

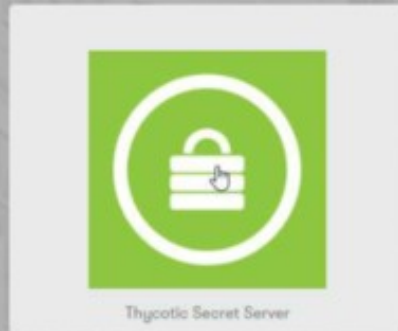
Login to the AuthControl Sentry Administration Console. Click Authentication Methods in the left hand menu. Click the Edit button against the OATH option in the list of Authentication Methods. Give this Authentication Method 100 points. This will mean that when a login attempt is made to the Thycotic Secret Server Application, this Authentication Method will be offered during login. (Please read about AuthControl Sentry Rules and familiarize your self with AuthControl Sentry [here](#))

58.8.1 Testing authentication to Thycotic Secret Server via Swivel AuthControl Sentry

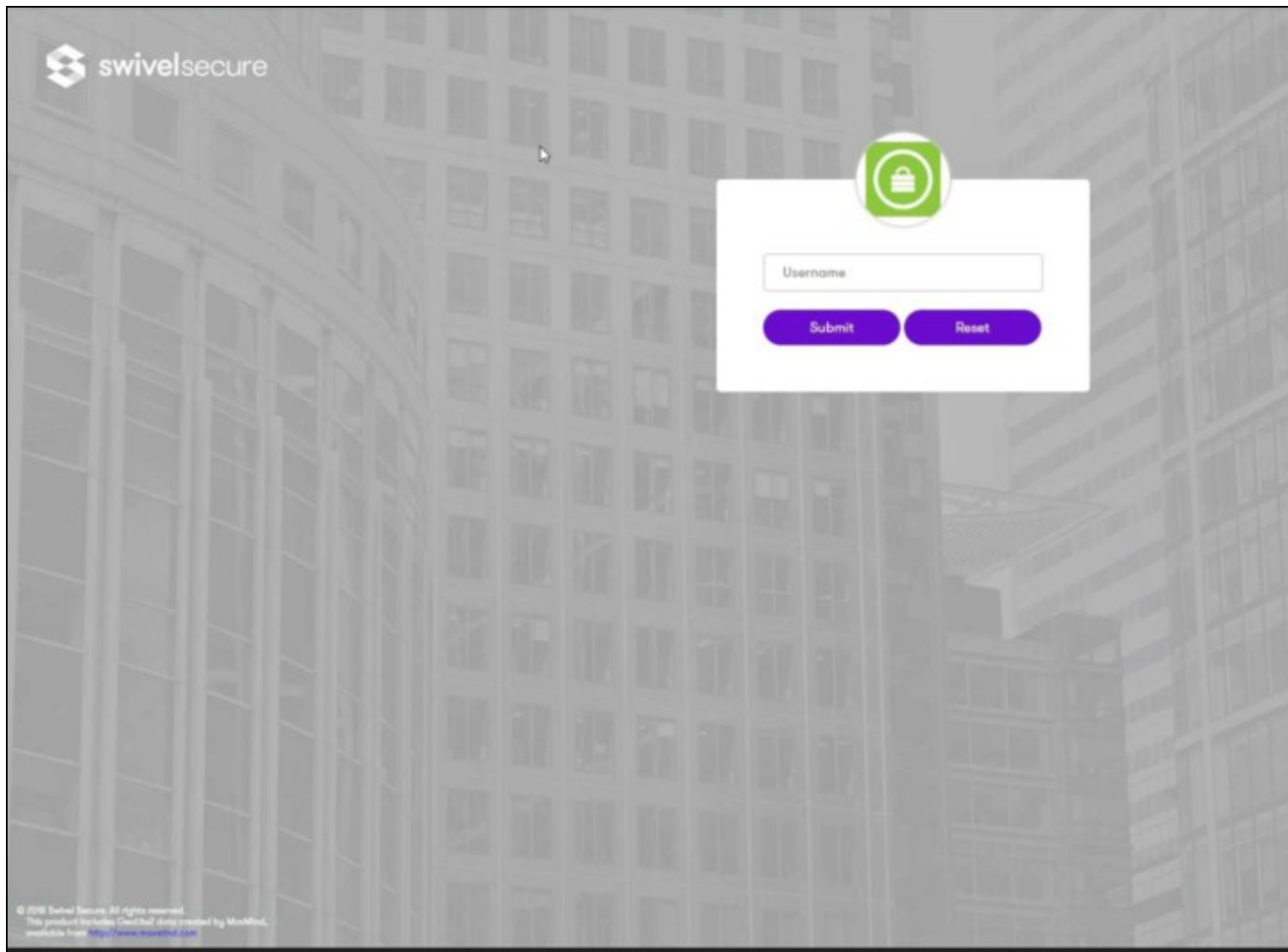
This should be the final step after all previous elements have been configured.

Visit your AuthControl Sentry Page with your public DNS entry of your Swivel AuthControl Sentry server, e.g. <https://mycompanysentrydomain/sentry/startPage>. On a Start Page you will be able to see a new Thycotic Secret Server Icon on which you can click and proceed with authentication (as you would by going straight to the Thycotic Secret Server page)

Please select an application

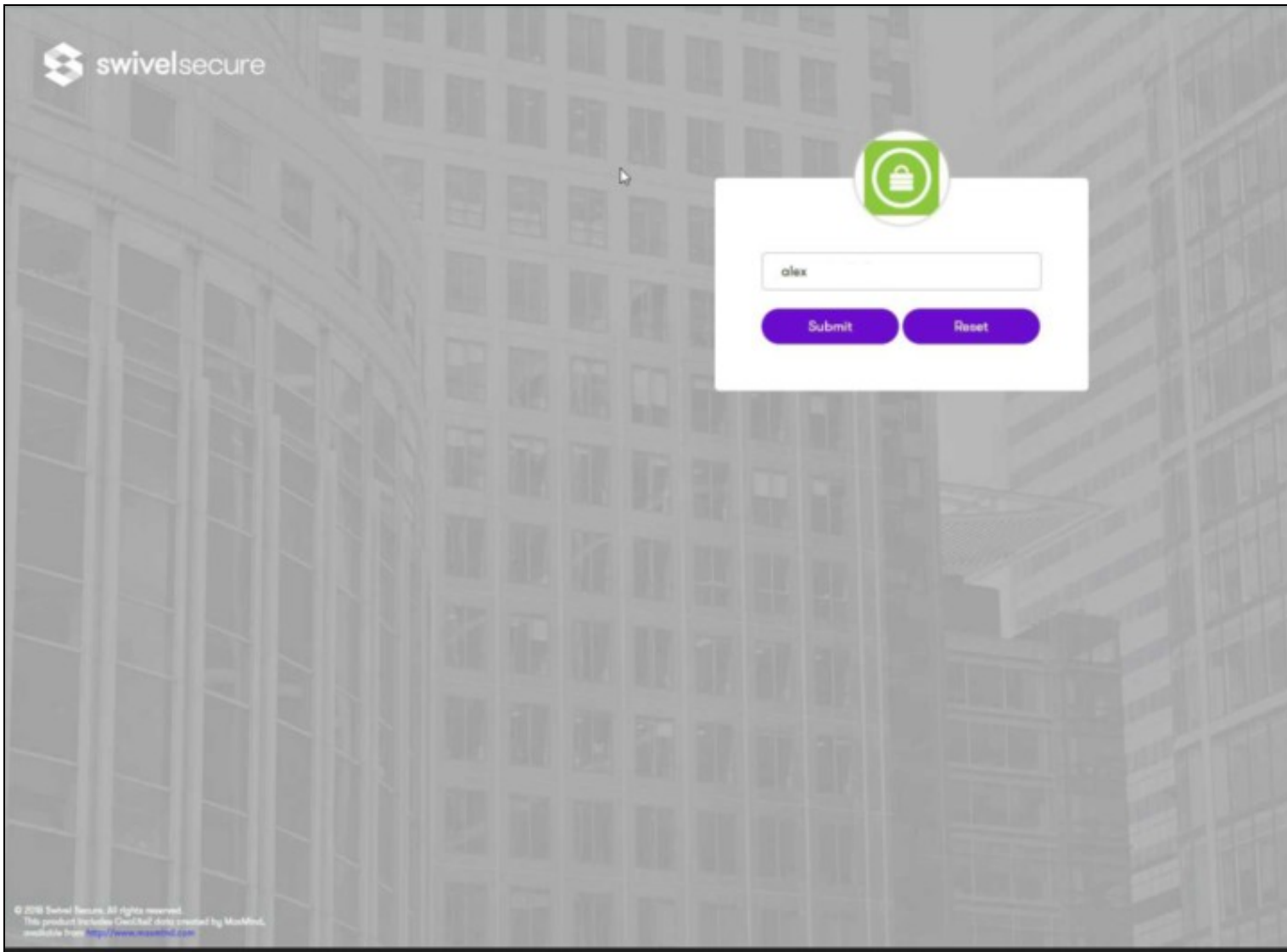


When you visit this URL you will notice that the domain should redirect to the identity provider login URL that you setup.

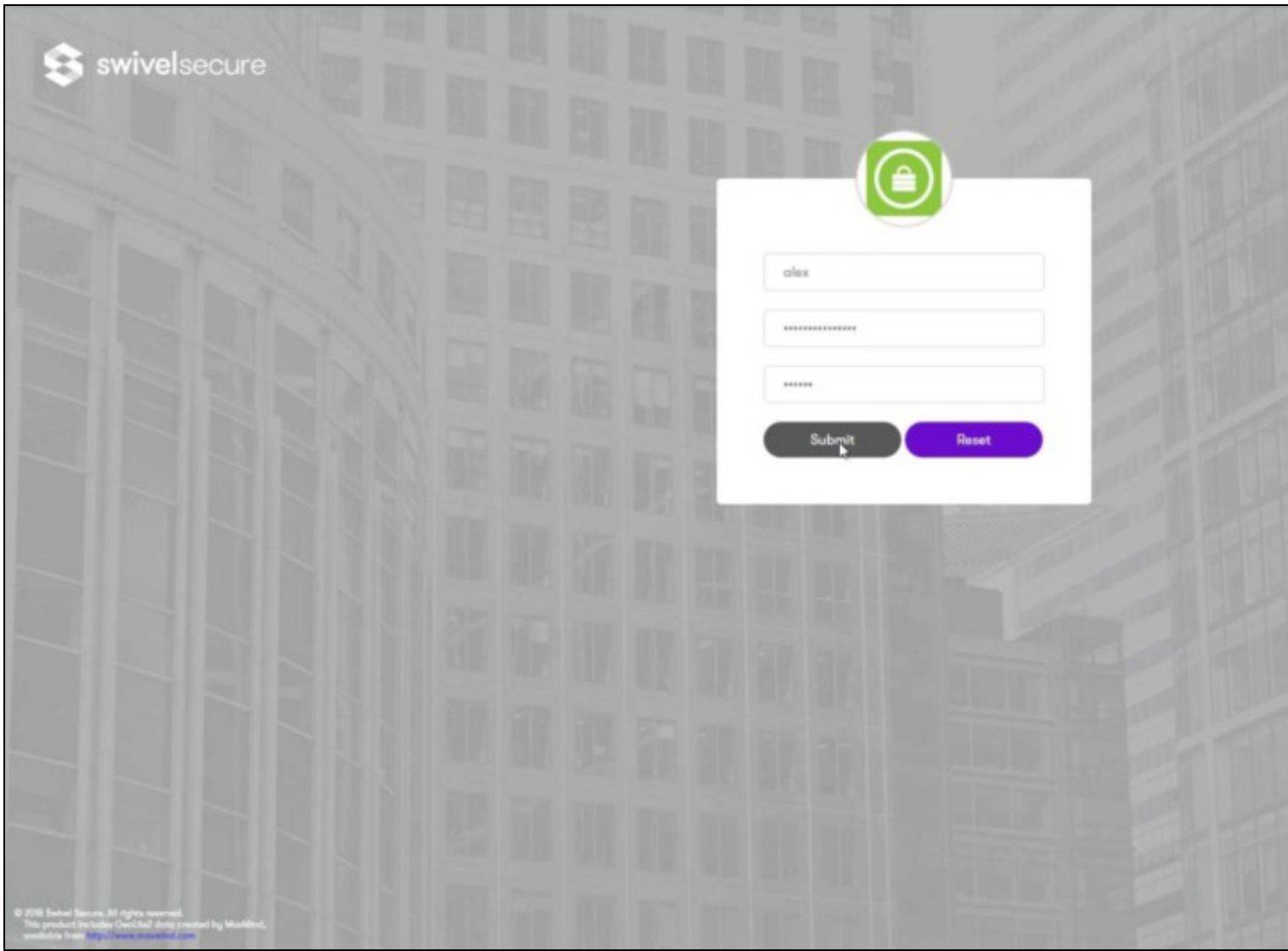


Once you have submitted your username. You should be presented with the Sentry authentication page.

In this login example we are using the sAMAccountName as a username and the fully qualified domain\username is being passed at the back end.



Once you have submitted your username. You should be presented with the page of the Authentication Method which can score enough points to match the points required by the Thycotic Secret Server Application definition.



After we enter our authentication credentials we successfully will see the Thycotic Secret Server account that we tried to access.

58.9 Troubleshooting

There are various logging components available for this particular integration which can aid in diagnosis at different points during authentication.

The Swivel Core has a Log Viewer menu item which can reveal information concerning user status e.g. is the user locked, has a session been
The Swivel AuthControl Sentry has a View Log menu item which provides details about the SAML assertion and response received from Thycotic

It is crucial when troubleshooting, to pinpoint where the authentication is failing. For example, you may find that the Swivel Core logs show a successful authentication (which would indicate that the user has entered their Password and OTP correctly), but the AuthControl Sentry logging shows that there is a problem with the SAML assertion.

Two common issues which can be diagnosed with the validator are:

Certificate or decryption issues;
Can AuthControl Sentry find the Certificate locally, is it the correct one?
Has the correct Certificate been uploaded to Thycotic Secret Server?
Does the Repository -> Attribute name being used actually map to a Repository attribute? Has a User Sync occurred in the Swivel Core s

59 Site ID

When creating a Site ID the customer will be asked to provide some information on how they intend to use Swivel Secure: see [SSD](#)

Other features are directly linked to the use of AuthControl Mobile App and its available options:

- PUSH (One Touch) authentication.
- PIN indicates whether or not the user enters their PIN in the mobile app and is shown the OTC, or has to extract the OTC from the security string.
- LOCAL - security strings are generated in the mobile app using TOTP, and are not requested from the appliance.
- OATH means that the mobile app generates one-time codes using TOTP.

60 Upgrade from v3 to v4

61 Upgrading notes

This document tells the procedure of upgrading from version 3 to version 4 sentry Authcontrol using the CMI

62 Before upgrade : License considerations

To access the latest AuthControl Sentry V4.04 features you will need to upgrade your appliance as well as request a V4 license key and Site ID, please contact your local Swivel Secure representative who can arrange this for you.

Please note some features like Single Sign On are chargeable.

63 Upgrading procedure

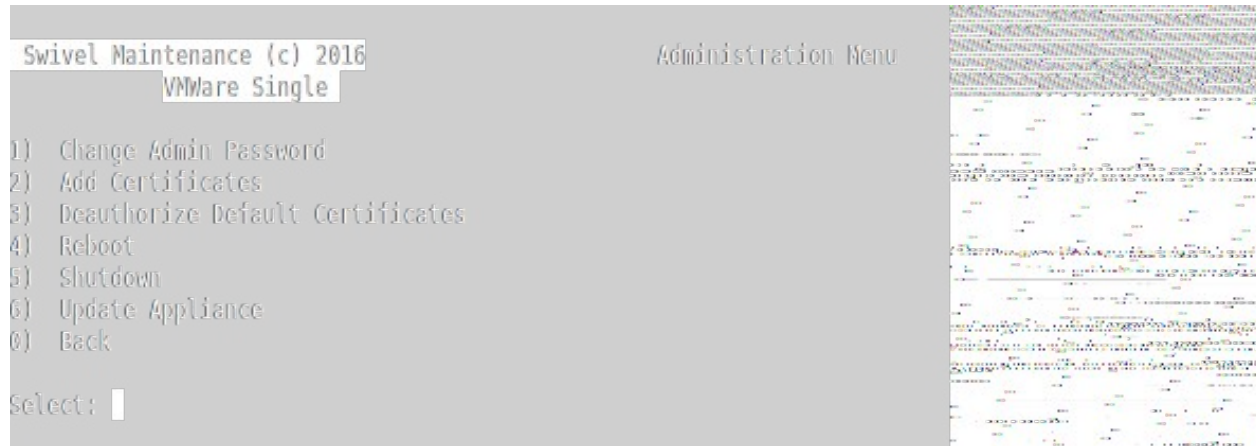
- Updating v3 to v4

1. Update swivel-cmi to at least 2214.

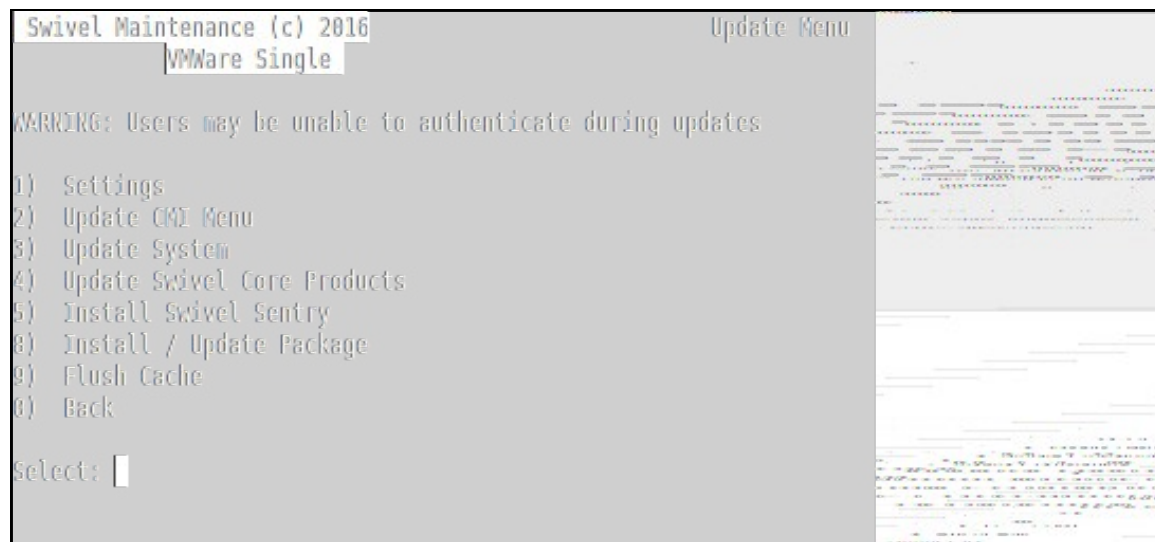
Update System or CMI from the update menu.

2. Logout.

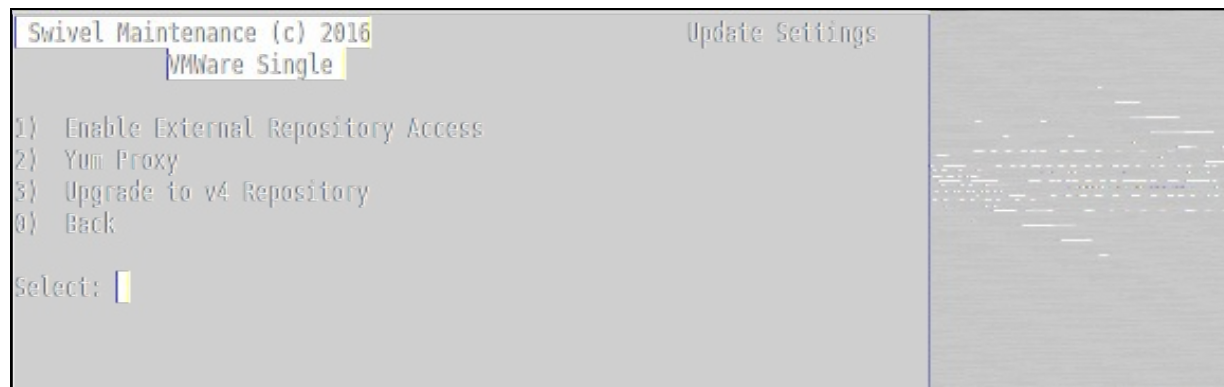
3. Login into Administration Menu



4. Select update menu and Select "Settings"



5. Select "Upgrade to v4 Repository"



```
Select: 3
INFO: Changed to take updates from v4 repositories.
Press RETURN to continue: 
```

6. Update System, Swivel Core Products.

```
Swivel Maintenance (c) 2016                               Update Menu
VMWare Single

WARNING: Users may be unable to authenticate during updates

1) Settings
2) Update CMI Menu
3) Update System
4) Update Swivel Core Products
5) Install Swivel Sentry
6) Install / Update Package
9) Flush Cache
0) Back

Select: 
```

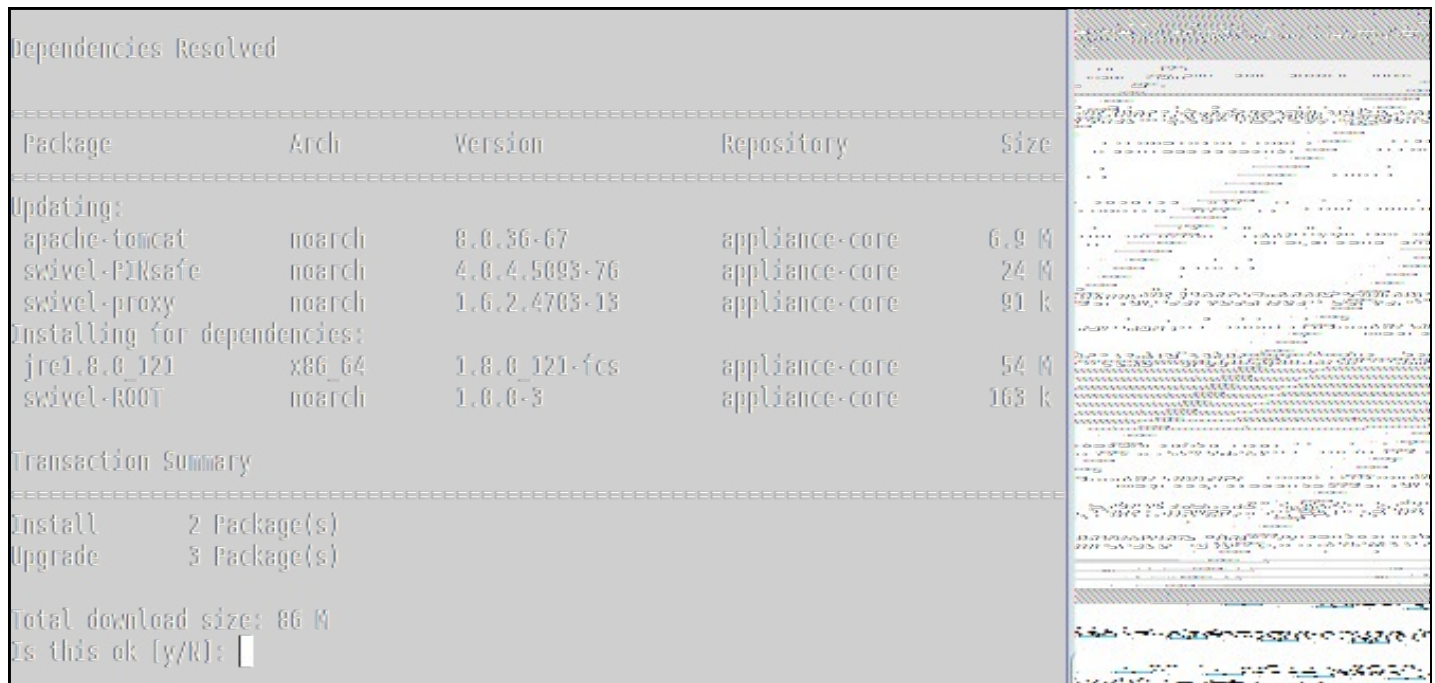
```
Resolving Dependencies
--> Running transaction check
--> Package swivel-cmi.noarch 0:3.0.2228-22 will be updated
--> Package swivel-cmi.noarch 0:4.0.2227-955 will be an update
--> Package swivel-mon.noarch 0:1.0.1841-16 will be updated
--> Package swivel-mon.noarch 0:1.0.2192-18 will be an update
--> Package swivel-mysql.noarch 0:1.0.2143-46 will be updated
--> Package swivel-mysql.noarch 0:1.0.2231-48 will be an update
--> Package swivel-release.noarch 0:1.0.1743-39 will be updated
--> Package swivel-release.noarch 0:4.0.1983-47 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch      Version      Repository      Size
=====
Updating:
swivel-cmi              noarch    4.0.2227-955 appliance       117 k
swivel-mon              noarch    1.0.2192-18  appliance       21 k
swivel-mysql            noarch    1.0.2231-48 appliance       20 k
swivel-release          noarch    4.0.1983-47 appliance       21 k
=====

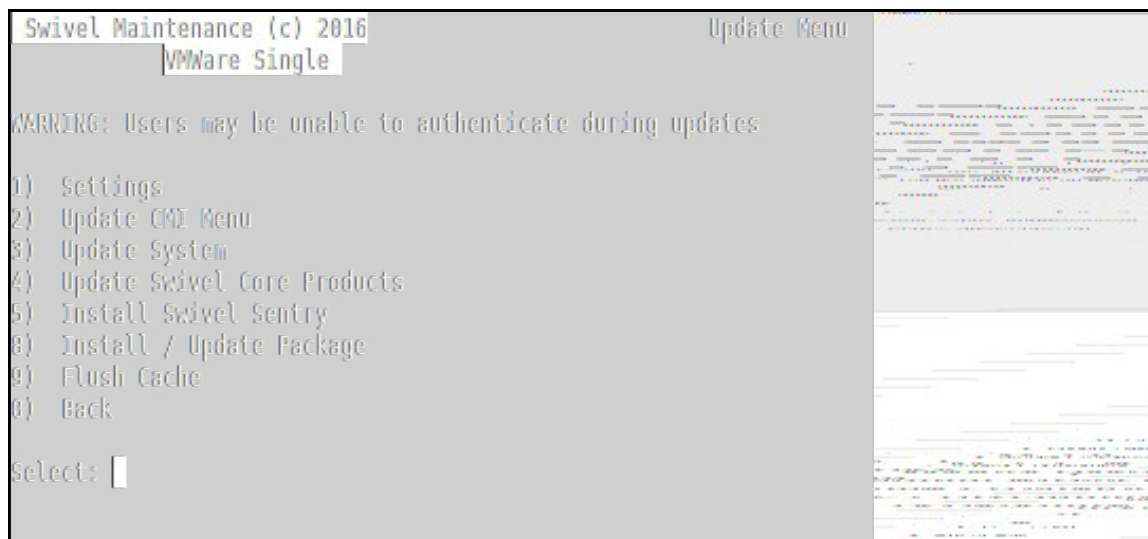
Transaction Summary
=====
Upgrade      4 Package(s)

Total download size: 179 k
Is this ok [y/N]: 
```



Select Y

7. Select "Install Swivel Sentry" in update Menu.



8. (opt) Select "Install / Update Package", then enter "swivel-logviewer" without quotes.

64 Need more help?

Please contact your partner or create a support ticket in our support portal <https://supportdesk.swivelsecure.com/dashboard>

65 User Portal

66 Overview

The user portal version 3 places all the self-service application in one place and allows the customer to decide what pages to make available to users and how those pages are to be used. This can replace the current changepin , resetpin and proxy applications.

The following applications are available.

- Change PIN
- Reset PIN (The ResetPIN needs to be enabled on the Swivel Administration console). See also [ResetPIN How To Guide](#)
- Provision a Mobile device
- Sync a [Token](#)

67 Prerequisites

For v4, see [User Portal Administration Guide](#) and [User Portal User Guide](#):

Swivel v3.9.5 to v3.11.5.

Appliance v2.0.16 onwards.

[QR Code Provision](#) Provisioning 3.10.4 onwards.

[Token](#) See link for Token prerequisites.

Swivel appliance with user portal see [Downloads](#).

68 Upgrading User Portal

The combined appliance patch gives the option to uninstall previous versions of the User Portal.

To manually remove it, backup the old user Portal, then with Tomcat running remove the `/usr/local/tomcat/webapps2/userportal.war` or whatever it has been called, this should remove the userportal folder. If using WinSCP refresh the folder to see if it has been removed.

69 User Portal Installation

If the User Portal is not installed on a Swivel appliance, it can be installed on an appliance running Swivel 3.9.1 onwards. WinSCP can be used to install this, see [WinSCP How To Guide](#).

Copy the userportal.war file to /usr/local/tomcat/webapps2

70 User Portal Configuration

Config files are located in: /home/swivel/.swivel/user-portal/ (or .swiveluser-portal on some versions)

70.1 settings.properties

Communication settings for a local Swivel instance. Restart Tomcat after making any changes.

```
pinsafessl=false
pinsafeserver=127.0.0.1
pinsafecontext=pinsafe
pinsafesecret=secret
pinsafeport=8181
imagessl=true
imageserver=YourSwivelURL.com
imagecontext=proxy
imageport=8443
```

Communication settings for a remote Swivel instance. Restart Tomcat after making any changes.

```
pinsafessl=false
pinsafeserver=RemoteSwivelIP or VIP
pinsafecontext=pinsafe
pinsafesecret=secret
pinsafeport=8080
imagessl=true
imageserver=YourSwivelURL.com
imagecontext=proxy
imageport=8443
```

70.2 portalconfig.properties

Controls the behaviour of changePIN. Restart Tomcat after making any changes.

```
#valid settings: directEntry turingEntry pinpadEntry
changePIN.page=turingEntry
```

71 Language files

These are located in `/usr/local/tomcat/webapps2/userportal/WEB-INF/classes`

71.1 messages_en.properties

This file contains the text and language which may be customised

72 User Portal Menu options

The options available to portal users can be edited to remove menus that are not required. Edit the file `/usr/local/apache-tomcat/webapps2/userportal/WEB-INF/view/template/leftpanel.jsp`

To remove an item, add at the start " example

The following removes the ChangePIN link

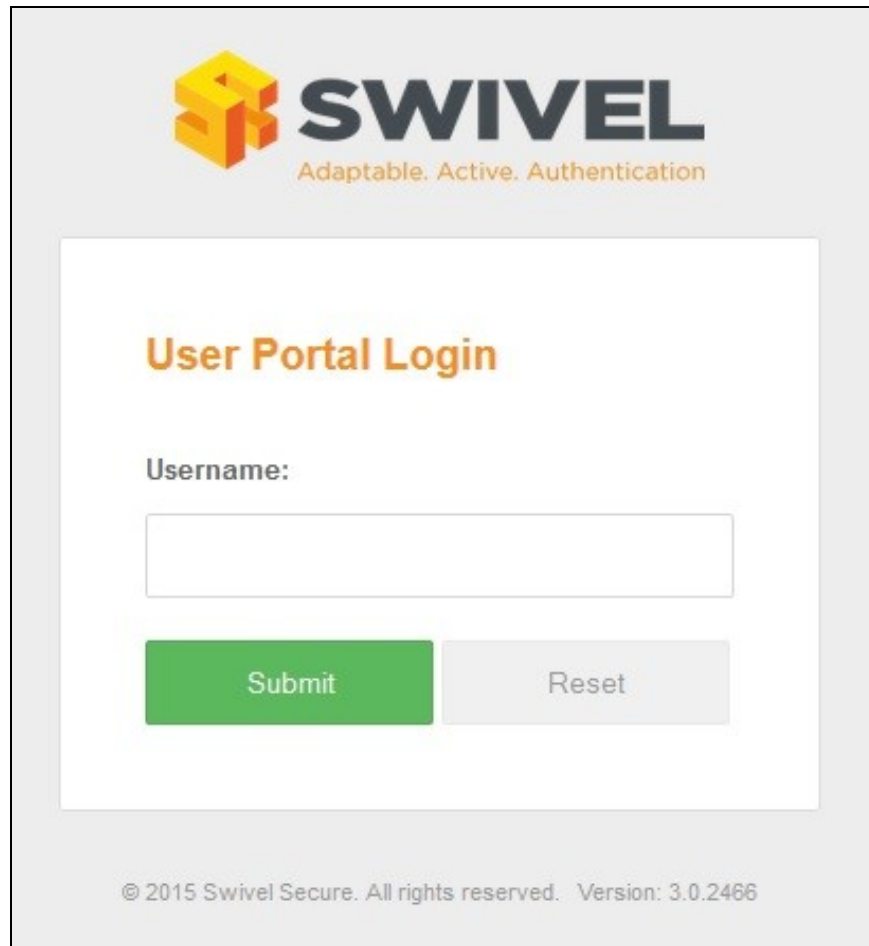
```
<li><a href="${mobileProvisioningUrl}"><spring:message code = "mobile_provisioning.title" /></a></li>
<li><a href="${selfResetUrl}" onclick="return confirmDialog(event);"><spring:message code = "reset.title" /></a></li>
<li><a href="${tokenManagementUrl}"><spring:message code = "tokenmanagement.title" /></a></li>
```

73 User Portal Usage

Navigate to the userportal page; <https://IP:8443/userportal> The userportal should be displayed.

73.1 User Portal Login

Here you can enter a user name and click [submit to access the User Portal.



The image shows a web browser window displaying the Swivel User Portal Login page. At the top, there is a logo for 'SWIVEL' with the tagline 'Adaptable. Active. Authentication'. Below the logo, the title 'User Portal Login' is displayed in orange. Underneath, there is a label 'Username:' followed by a text input field. Below the input field, there are two buttons: a green 'Submit' button and a grey 'Reset' button. At the bottom of the page, there is a footer that reads '© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466'.

73.2 User Portal Menu

The below screen will show once the username has been submitted.

- ▶ Mobile Provisioning
- ▶ Reset PIN
- ▶ Change PIN
- ▶ Token Management

User Portal

The User Portal allows users to administer themselves

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

73.3 User Portal Mobile Provision

The Mobile provision option allows a message to be sent to the user or to use [QR Code Provision](#).

- ▶ Mobile Provisioning
- ▶ Reset PIN
- ▶ Change PIN
- ▶ Token Management

Mobile Provisioning

Select the appropriate option

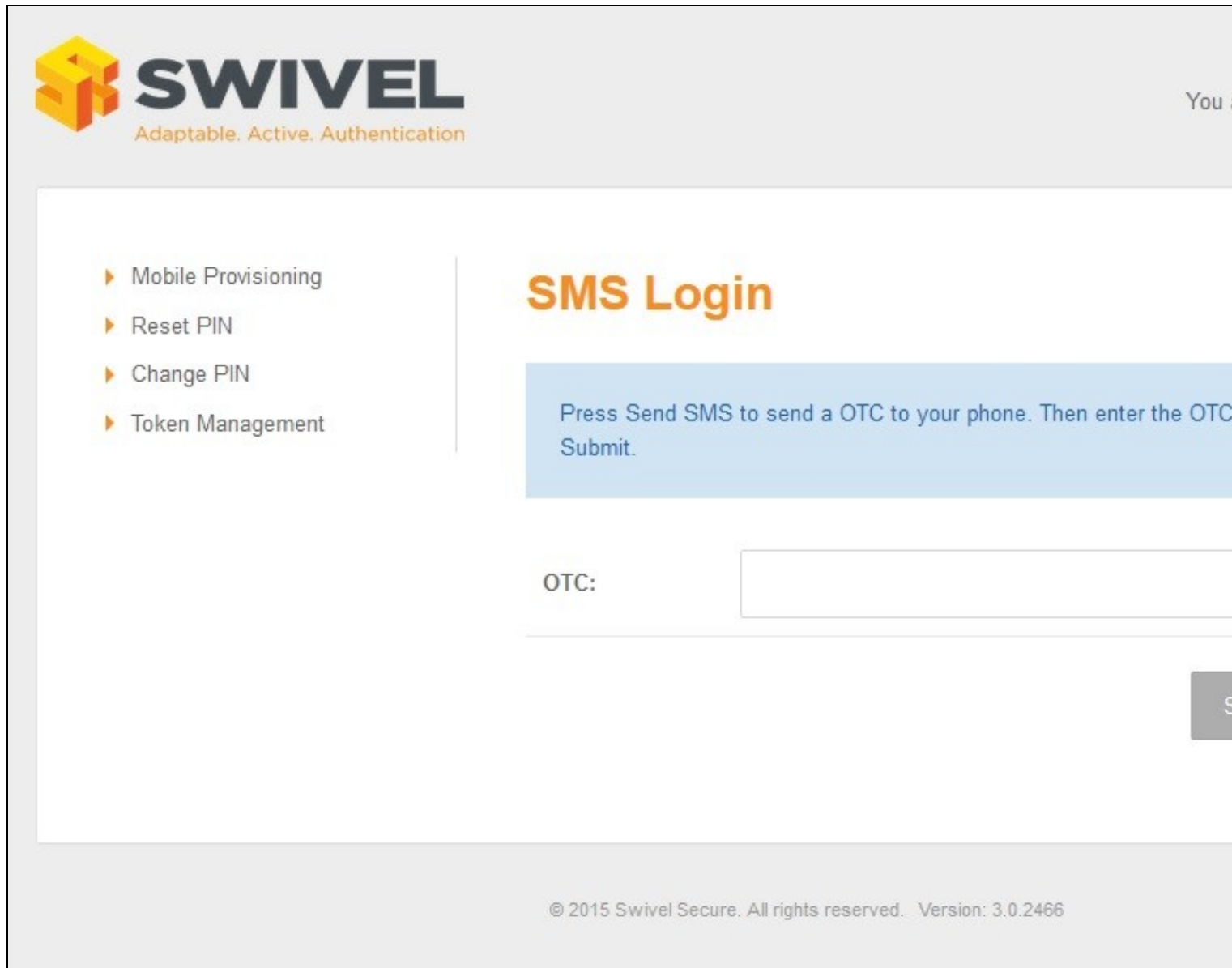
Send code via e-mail

Display code on screen

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

73.4 User Portal Mobile Provision On Screen

To use the [QR Code Provision](#) the user needs to authenticate by entering an [OTC](#), this screen allows the SMS to be sent to the user.



The screenshot shows the Swivel User Portal interface. At the top left is the Swivel logo with the tagline "Adaptable. Active. Authentication". On the right, the text "You" is partially visible. A left-hand navigation menu contains four items: "Mobile Provisioning", "Reset PIN", "Change PIN", and "Token Management". The main content area is titled "SMS Login" in large orange text. Below this title is a light blue instruction box that reads: "Press Send SMS to send a OTC to your phone. Then enter the OTC Submit." Underneath the instruction box is a label "OTC:" followed by a text input field. A "Send SMS" button is partially visible on the right edge. At the bottom of the page, the footer text reads: "© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466".

73.5 User Portal Mobile Provision by QR Code

A valid [OTC](#) will display the [QR Code Provision](#).

- ▶ Mobile Provisioning
- ▶ Reset PIN
- ▶ Change PIN
- ▶ Token Management

Mobile Provisioning

Please scan the QR code using the Swivel Mobile phone application



© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

73.6 User Portal ResetPIN

ResetPIN allows a user to be sent a new PIN number. The user is sent a reset code to enter into the below page, which if correct when submitted will create a new PIN and send it to the user.

- ▶ Mobile Provisioning
- ▶ Reset PIN
- ▶ Change PIN
- ▶ Token Management

Reset PIN

Reset PIN message sent

Please check your e-mail for the reset link.

Confirmation Code:

73.7 User Portal ChangePIN

ChangePIN allows a user to change their PIN number. Different options such as by using the [TURING](#) or [Pinpad](#) or direct entry of the PIN are available by modifying the configuration files above.

- ▶ Mobile Provisioning
- ▶ Reset PIN
- ▶ Change PIN
- ▶ Token Management

Change PIN

Please change your PIN by extracting OTCs from the following Tur



Current OTC:

....

New OTC:

....

Refresh Image

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

73.8 User Portal Token Sync

Token Sync allows a user to synchronise a new or existing token by entering two consecutive OTC from the token.

- ▶ Mobile Provisioning
- ▶ Reset PIN
- ▶ Change PIN
- ▶ Token Management

Token Management - Synchron

Enter the next two OTPs from your token and then click 'Submit' to count

First Code

637542

Second Code

734569

74 Additional Configuration options

74.1 Creating a URL redirect from the root level

See [Redirect link](#)

74.2 Using 443 instead of 8443

See [How to run PINsafe on non-default ports](#)

74.3 Changing the logo

You can change the User Portal logo by navigating to `/usr/local/tomcat/webapps2/userportal/img` and there is an image called `swivel-logo.png` (Not to be mistaken for `swivel_logo.png`). Import the required image and rename it to `swivel-logo.png`.

75 Known Issues

The User Portal ONLY supports the UTF-8 Character Code Set.

76 Troubleshooting

A Reset code could not be requested.

The Swivel server does not allow Account Resets

The ResetPIN needs to be enabled on the Swivel Administration console.

76.1 Changes to xml files do not take effect

76.1.1 Cached files

You may find you need to clear the cached compiled files for User Portal before the new settings will take effect. You can find these in /usr/local/tomcat/work/Catalina-proxy/localhost/userportal. Delete the contents of this folder **only when Tomcat is stopped**.

This folder will be automatically re-created the next time it is required, so it is safe to delete.

76.1.2 File locations

Ensure the correct locations are being edited: Config files will be stored in ~/.swivelportal/conf or as stated by stated in env variable SWIVEL_PORTAL_HOME or web.xml ?portalHome"

Editing the configuration files under <path to Tomcat>\webapps2\userportal\WEB-INF (Example: C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps2\userportal\WEB-INF) will not be used.

76.2 Error Messages

There was an error please check your username and pin code if the problem persists contact your systems administrator.

Contact the Administrator to see verify the error. This error should be logged on the Swivel server that the User Portal uses.

Change PIN failed for user: graham, error: The use of a static password is mandatory

The user is required to use a static Password

Change PIN failed for user: graham, error: The one-time code was missing or malformed.

Incorrect OTC entered

In the Swivel log viewer

AgentXML request failed, error: The XML request sent from the agent was malformed.

and in the User Portal

Something went wrong. Please try again or contact your system administrator.

This can be seen when a token is synced and the token is already synced.

Dual channel message request failed, error: On-demand dual channel delivery is disabled

When sending an SMS/Email to a user the On-demand dual channel delivery needs to be enabled on the Swivel Administration console under Server/Dual Channel.

77 User Portal Administrator User Guide

77.1 Overview

The user portal version 3 and 4 places all the self-service application in one place and allows the customer to decide what pages to make available to users and how those pages are to be used. This can replace the current changepin , resetpin and proxy applications.

The following applications are available.

- Change PIN
- Reset PIN (The ResetPIN needs to be enabled on the Swivel Administration console). See also ResetPIN How To Guide
- Provision a Mobile device
- Sync a Token

77.2 Prerequisites

User Portal

Swivel v3.9.5 onwards.

Appliance v2.0.16 onwards.

QR Code Provision Provisioning 3.10.4 onwards.

Token See link for Token prerequisites.

77.3 User Portal Configuration

Config files are located in: /home/swivel/.swivel/user-portal/ (or .swiveluser-portal on some versions)

settings.properties

Communication settings for a local Swivel instance. Restart Tomcat after making any changes.

```
pinsafessl=false
pinsafeserver=127.0.0.1
pinsafecontext=pinsafe
pinsafesecret=secret
pinsafeport=8181
```

Communication settings for a remote Swivel instance. Restart Tomcat after making any changes.

```
pinsafessl=false
pinsafeserver=RemoteSwivelIP or VIP
pinsafecontext=pinsafe
pinsafesecret=secret
pinsafeport=8080
```

The following attribute indicates if on the ResetPIN screen the user can choose if the Password needs to be reset with the PIN or not. By default it is set to false.

```
showresetpasswordfield=false
```

From 4.0.5, the following attribute indicates if authentication in user portal requires a confirmation code. By default it is set to false.

```
showconfirmationcode=false
```

portalconfig.properties

Controls the behaviour of changePIN. Restart Tomcat after making any changes.

```
#valid settings: directEntry turingEntry pinpadEntry
changePin.page=turingEntry
```

77.4 Language files

These are located in /usr/local/tomcat/webapps2/userportal/WEB-INF/classes

messages_en.properties

This file contains the text and language which may be customised

77.5 User Portal Menu options

The options available to portal users can be edited to remove menus that are not required. Edit the file /usr/local/tomcat/userportal/WEB-INF/view/template/leftpanel.jsp

To remove an item, add at the start " example

The following removes the ChangePIN link

```
<li><a href="${mobileProvisioningUrl}"><spring:message code = "mobile_provisioning.title" /></a></li>
<li><a href="${selfResetUrl}" onclick="return confirmDialog(event);"><spring:message code = "reset.title" /></a></li>
<li><a href="${tokenManagementUrl}"><spring:message code = "tokenmanagement.title" /></a></li>
```

77.6 Additional Configuration options

Creating a URL redirect from the root level

See Redirect link

Using 443 instead of 8443

See How to run PINsafe on non-default ports

Changing the logo

You can change the User Portal logo by navigating to `/usr/local/tomcat/webapps2/userportal/img` and there is an image called `swivel-logo.png` (Not to be mistaken for `swivel_logo.png`). Import the required image and rename it to `swivel-logo.png`.

For v4 the available option is the `logo-mark--purple.png` which is the logo on top of the Username.

77.7 Known Issues

The User Portal ONLY supports the UTF-8 Character Code Set.

77.8 Troubleshooting

A Reset code could not be requested.

The Swivel server does not allow Account Resets

The ResetPIN needs to be enabled on the Swivel Administration console.

77.9 Changes to xml files do not take effect

Cached files

You may find you need to clear the cached compiled files for User Portal before the new settings will take effect. You can find these in `/usr/local/tomcat/work/Catalina-proxy/localhost/userportal`. Delete the contents of this folder only when Tomcat is stopped.

This folder will be automatically re-created the next time it is required, so it is safe to delete.

File locations

Ensure the correct locations are being edited: Config files will be stored in `~/.swivelportal/conf` or as stated by `SWIVEL_PORTAL_HOME` or `web.xml ?portalHome`

Editing the configuration files under `<path to Tomcat>\webapps2\userportal\WEB-INF` (Example: `C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps2\userportal\WEB-INF`) will not be used.

Error Messages

There was an error please check your username and pin code if the problem persists contact your systems administrator. Contact the Administrator to see verify the error. This error should be logged on the Swivel server that the User Portal uses.

Change PIN failed for user: graham, error: The use of a static password is mandatory The user is required to use a static Password

Change PIN failed for user: graham, error: The one-time code was missing or malformed. Incorrect OTC entered

In the Swivel log viewer

AgentXML request failed, error: The XML request sent from the agent was malformed.

and in the User Portal

Something went wrong. Please try again or contact your system administrator. This can be seen when a token is synced and the token is already synced.

Dual channel message request failed, error: On-demand dual channel delivery is disabled When sending an SMS/Email to a user the On-demand dual channel delivery needs to be enabled on the Swivel Administration console under Server/Dual Channel.

78 V3 & V4 Appliance Quick Start

78.1 Quick Start

```
Swivel Maintenance (c) 2019 Main Menu VMware Single
Hostname      : test.single.name
Interface : eth0      : 192.168.0.25
Tomcat Status  : Running

WARNING: Password still default. This can be changed in Administration
WARNING: No alert email set. This can be set in Tools -> Alerts

1) Tomcat
2) Network
3) Appliance
4) Backup and Restore
5) Tools and Utilities
6) Administration
8) System Status
9) Version Information
0) Exit

Select: _
```

This guide is a quick start guide to the **Version 3 and 4** Swivel Secure Appliances.

A reference guide that describes the meaning for all the menus is also available [here for version 3](#) and [here for version 4](#).

The appliance will come with a pre-configured IP address depending on appliance type:

Stand-alone (192.168.0.35)

HA Primary (192.168.0.36)

HA Standby (192.168.0.37)

Amazon/Cloud (DHCP)

If this IP address is compatible with your network you can plug an ethernet cable into eth0 (labelled Gb1) and access the appliance via SSH.

Alternatively you can access by plugging in an ethernet cross-over cable into eth0

78.2 Accessing Appliance Menus

To access the appliance menu you secure-shell onto the appliance. From a Windows machine you can use a terminal emulator capable of SSH connections, such as putty. From a Linux machine you can simply use the ssh command. SSH access is via the standard port 22.

When you access the appliance you will be prompted for a username and password. The default settings for this are:

- V3 and V4.0 appliances:

username:admin

password:lockbox

- V4.1 and later appliances:

username:admin

password:securebox

Once you have logged on you will be presented with the top level menu. Sub-menus are accessed by simply pressing the number of the item required followed by <Enter>

On certain actions you will be asked to enter Y to continue. Entering any other character or just entering return will cause the action to be cancelled. To maintain compatibility with v2, entering ?yes? will also work.

NOTE Refer to our [PuTTY How To Guide](#) for detailed instructions and screenshots.

78.3 Updating Appliance

Important You should update an appliance prior to installation to ensure it is running the optimum versions and settings

A [reference guide that details the options available for Appliance updating](#) is available.

78.4 Webmin

You can find the [Webmin guide here](#).

78.5 Setting Hostname IP Address

If you are using an Cloud-based appliance, IP addresses must be set by DHCP.

You will need to set the IP address(es) of the appliance. To do this use the access the Network Menu and do the following

1. Use the change hostname to set the hostname. Recommended to make this a meaningful, eg swivel.yourcompany. If this appliance is part of an HA installation include the appliance type eg primary.swivel.yourcompany.
2. Set the Network settings for ETH0. This is the main interface, you may not need to change the ETH1 settings as this is used for database replication (ref Setting up HA)
3. Set DNS servers. This may not be required at this stage but will be required if the Swivel Appliance will need to perform DNS resolution, eg for sending emails or SMS messages via named hosts.

78.6 Starting and Stopping Tomcat

Swivel applications run within Tomcat so you will only be able to access them when Tomcat is running. Tomcat will start automatically when the appliance starts and the status of Tomcat is shown on the main screen and on the Tomcat menu screen.

Should you need to manually start or stop Tomcat, this is possible from the Tomcat menu.

78.7 Accessing the Swivel Applications

With the ETH0 address set to <IP Address> you will be able to access the following applications from a browser:

Swivel Core admin console <https://<IP Address>:8080/pinsafe>. For version 4, this should be <https://<IP Address>:8080/sentry>.

Swivel User (Self Service) Portal <https://<IP Address>:8443/userportal>

Swivel Proxy <https://<IP Address>:8443/proxy>

- The Swivel Proxy has no user interface but acts as a proxy for image and message requests e.g. <https://<IP Address>:8443/proxy/SCImage?username=test> should result in a TURING image being displayed.

