AD Agent Version 1.5 Release Notes

Introduction

Version 1.5 of AD Agent differs from previous versions in several significant aspects:

- LDAP over TLS has been improved significantly – the previous version did not always work when LDAPS was invoked.
- Java and Tomcat are no longer embedded in the installer but must be installed separately. The versions used were old and updating to newer versions was difficult.
- The upload and download have been enhanced to backup and restore the entire configuration, rather than just the Sentry connection properties (as of 1.5.7).
- A new feature was added to allow two-way synchronisation with Sentry (as of 1.5.7).
- It has been rebranded in line with other Swivel Secure products

Requirements Prior to Installation

This product can be installed on most recent Windows operating systems: server or desktop. Testing has been performed on Windows Server 2016 and 2019 and Windows 10. However, we would expect it to work on Windows Server 2012 R2 as well. Earlier operating systems, such as Windows Server 2008 and Windows 7 may have problems supporting TLS protocols later than TLS 1.0.

This product requires Java 8 or later. It has been tested with Oracle Java version 8 and Open JDK version 15. It will work with Open JDK version 8 but be aware that the trusted certificate store in Open JDK 8 is empty, so you will need to provide your own. Should you choose to install Oracle Java, make sure you are aware of the licensing implications.

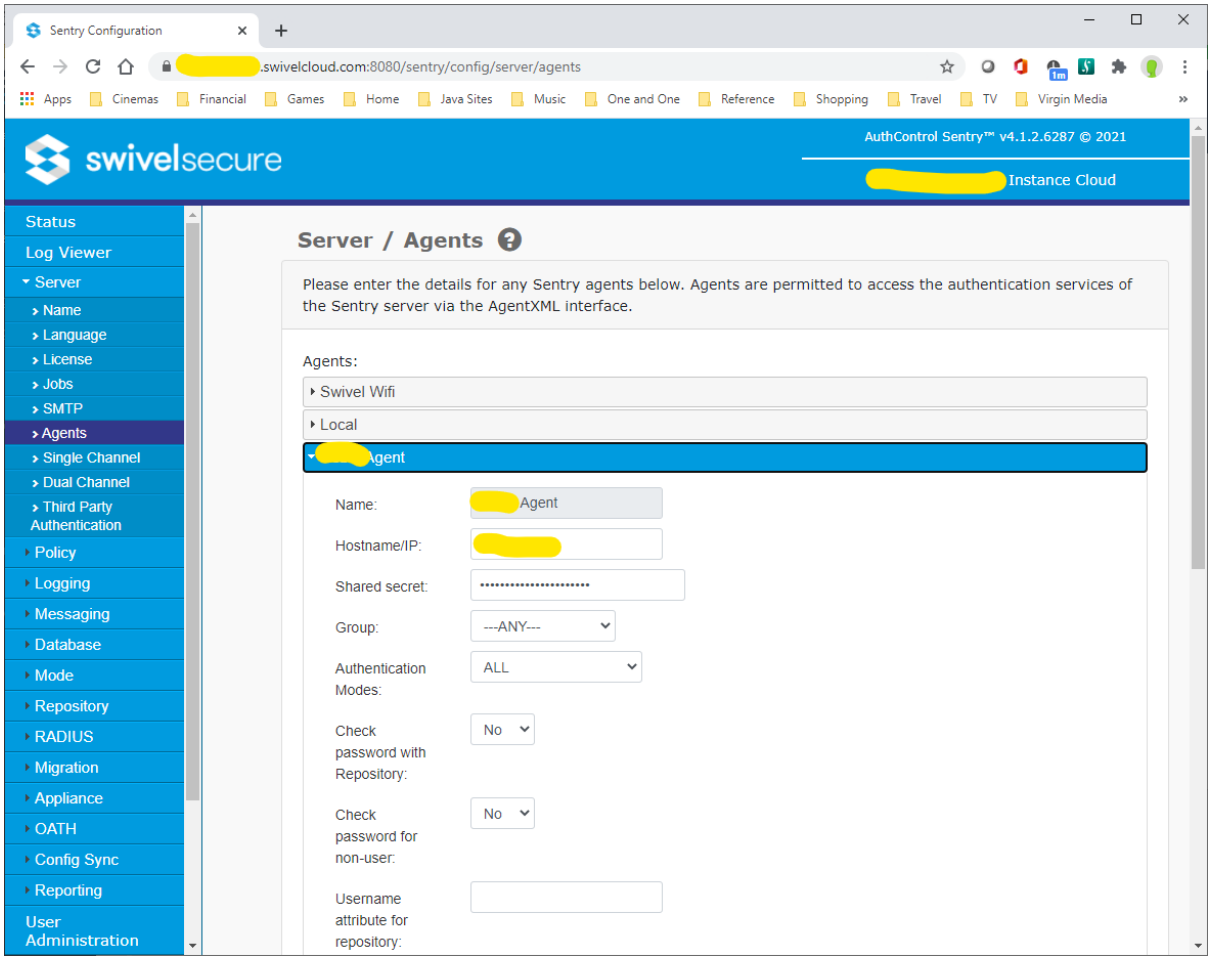
This product runs under Apache Tomcat. It has been tested with versions 7 and 9, so is assumed to work with version 8 as well. However, testing failed with Tomcat version 10, so you should not select that. You should select the Windows Service installer from the Tomcat website. If Tomcat is not installed as a service, the configuration program will not be able to stop and start Tomcat when required. You will need to do this manually instead. It is recommended when installing Tomcat to choose the Service Startup and Native options. You will not need any of the optional components, such as Documentation, Manager, Host Manager or Examples, so unless you are planning to use this installation for other products, it is recommended that you uncheck these.

Note that Java must be installed BEFORE Tomcat, as you will be asked to provide the location of the Java installation during the Tomcat installation process. If you are using Open JDK, there is no installer – the files are simply unzipped. Therefore, Tomcat will not be able to detect the location automatically and you will have to select it.

One final word of warning: you can use either 32-bit or 64-bit versions of Java and Tomcat, but make sure they are the same: 32-bit Tomcat will not run on 64-bit Java or vice versa.

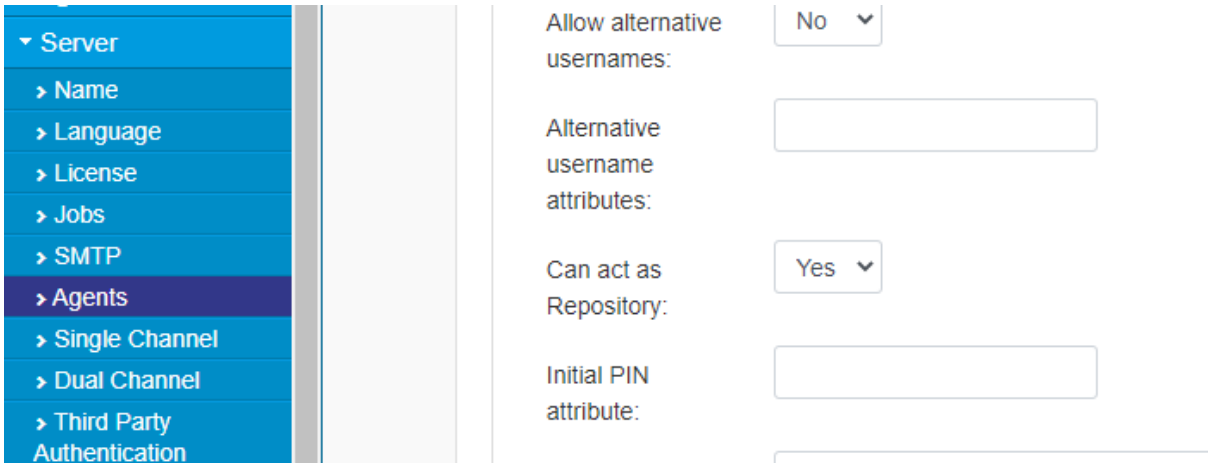
Preparing Sentry for AD Agent

The only requirement for Sentry to be able to connect to an AD Agent is that you create an Agent entry for the server that will be connecting.



The name can be anything, so long as it is unique among Agent names. Enter the public IP address of the server that will be acting as AD Agent. You should also enter a shared secret where indicated. This value will also need to be entered on the AD Agent later, so keep a note of it.

The other thing to check is that the Agent must be set to Act as Repository, for it to be able to import users:



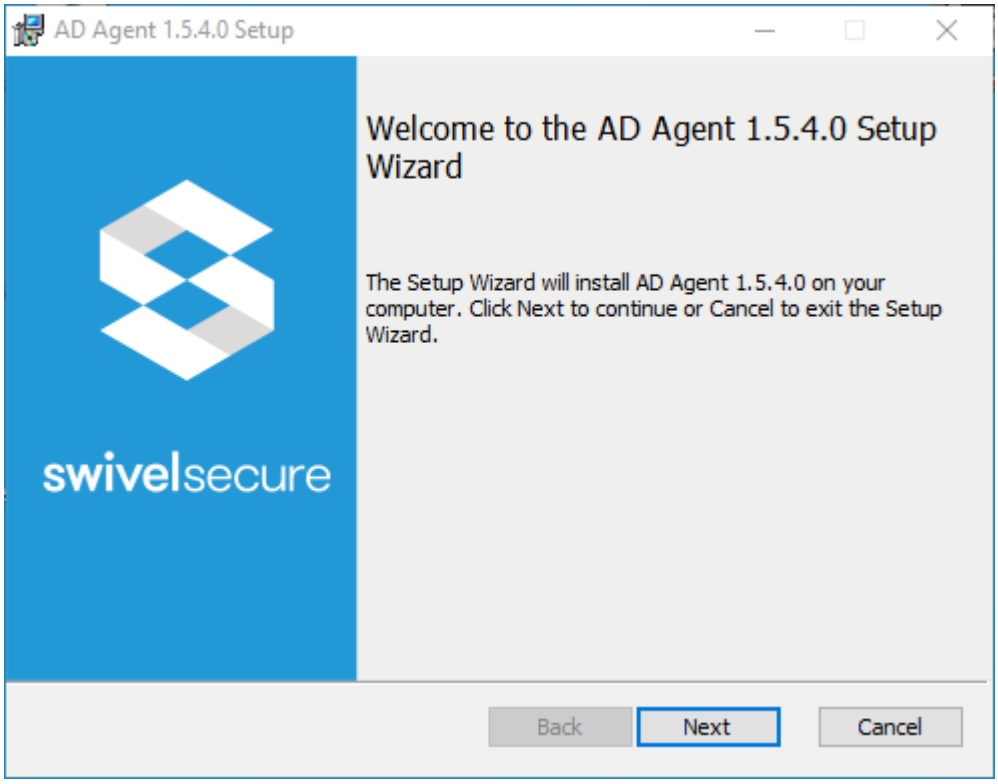
Upgrading from an Earlier Version

You should not install this version on top of an older one. As explained above, the requirements for version 1.5 are different from previous versions, and Java and Tomcat are not included in the installer. The preparation for upgrading is therefore as follows:

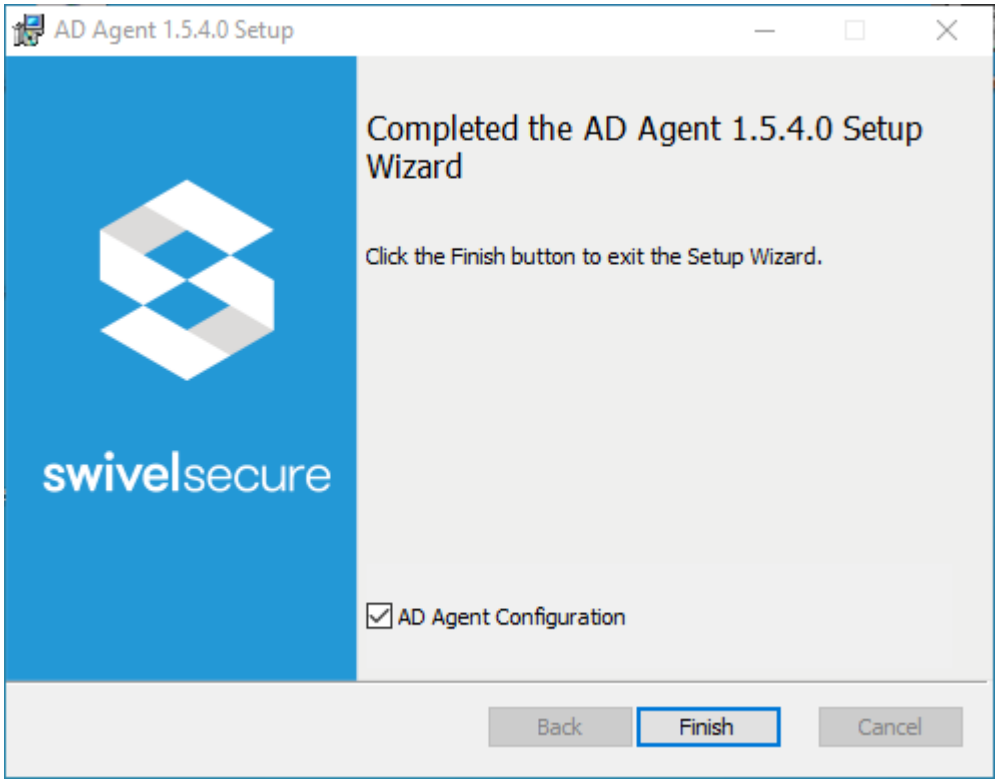
1. Stop the Tomcat service (which therefore stops AD Agent).
2. Locate the folder C:\ProgramData\Swivel Secure\.swivel. Be aware that ProgramData is hidden by default, so if necessary enable hidden folders in Explorer.
3. Back up the entire .swivel folder. Make sure Tomcat is stopped before you do this, or the backup will fail. This backup is for safety: the installer should not remove the current settings.
4. Optionally, uninstall the old version of Tomcat and Java. There is no problem with leaving these, so long as you ensure that you know which versions are being used for AD Agent. AD Agent 1.5 will run on the version of Tomcat 7 that was provided with earlier versions of AD Agent, but we recommend upgrading to a newer version. Also, AD Agent 1.5 will NOT run with Java 7 that was provided previously, so if you choose not to upgrade Tomcat, you will need to reconfigure it to use the newer version of Java.
5. Determine which account is running the Tomcat service, assuming you have installed a newer version of Tomcat. This will probably be “Local Service”. Check the security settings for C:\ProgramData\Swivel Secure\.swivel and ensure that this account has full control for this folder and all its contents.

Installation

It is recommended that you install AD Agent after Tomcat. The installation does not require Java or Tomcat, so installing will succeed, but you will not be able to configure it until Tomcat is available.

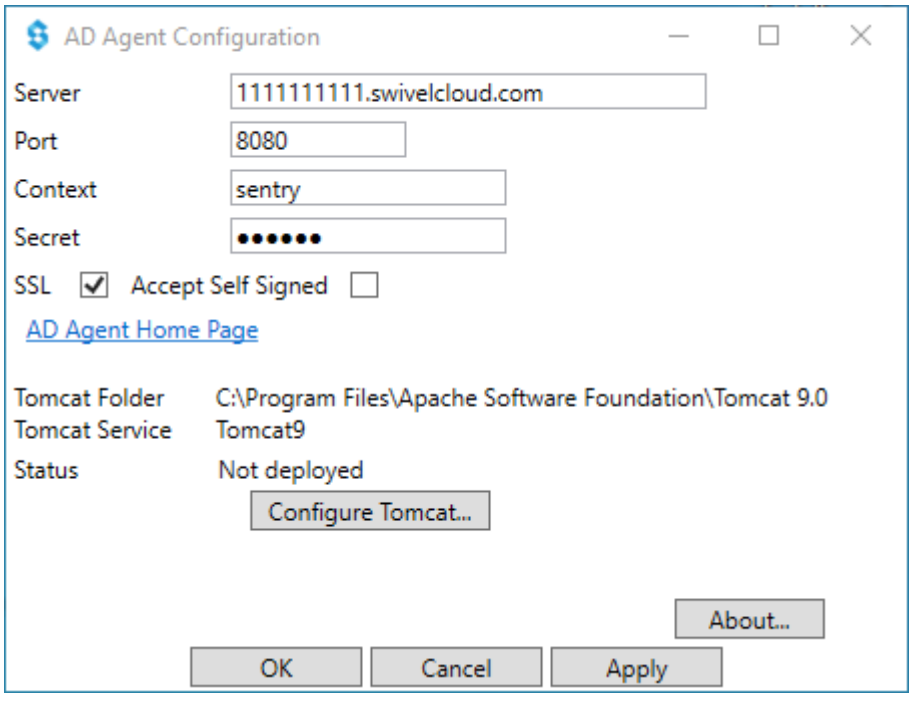


Installation is simply a matter of running the .msi file provided and stepping through the installation wizard.



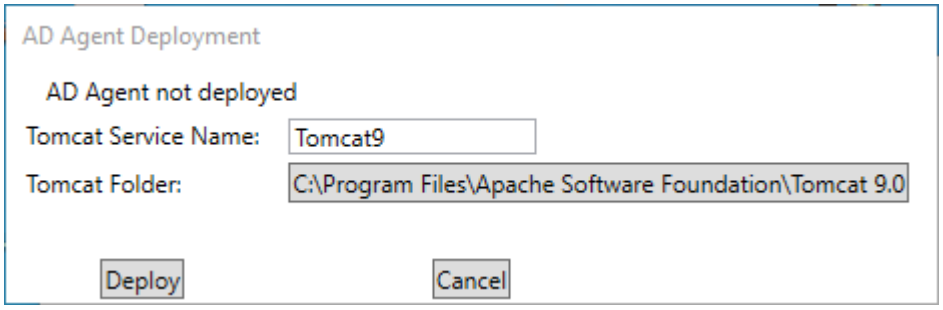
Once installed, you are given the option of running the configuration program, which you should do next. Note that the AD Agent Configuration is not selected by default.

Configuration



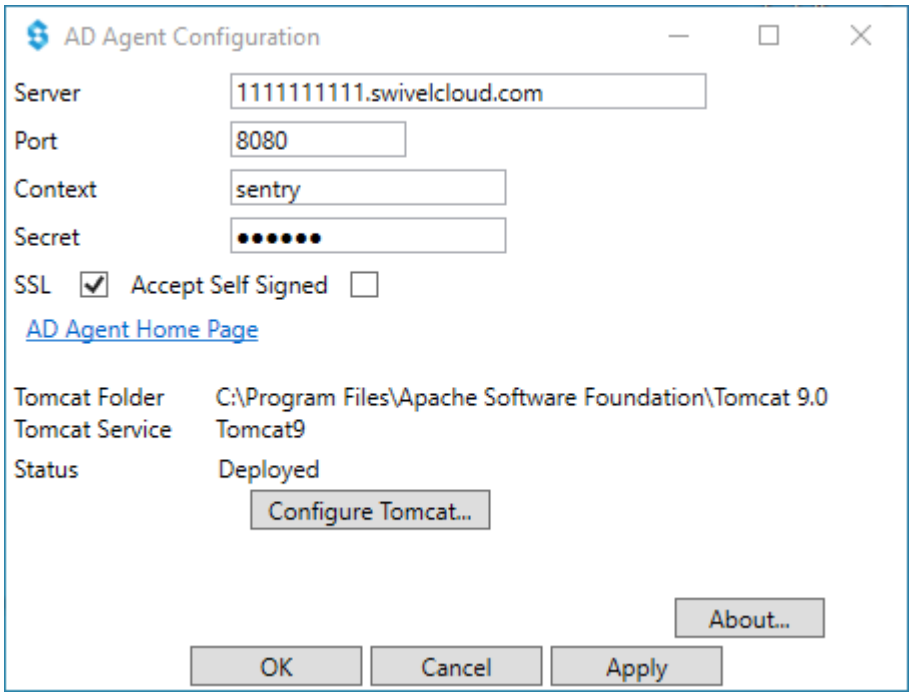
The configuration program allows you to configure the Sentry cloud instance to which you will be connecting. This must be done before you can run AD Agent itself. Enter the host name of the cloud instance you will be connecting to, and the Secret that you entered for the Agent earlier. Typically, you should not need to change the port or context, but you will need to select SSL.

Before you can run AD Agent, you must deploy it to Tomcat. If you used the service installation for Tomcat, the configuration program should have detected it and it will be displayed here. Otherwise, you will need to enter the location manually. Either way, you will need to select the Configure Tomcat button to deploy it. **Note that this is mandatory**: the installer does not copy the adagent application to Tomcat.



This dialog will allow you do deploy AD Agent to Tomcat. Assuming the settings are correct, simply click Deploy. If you need to change the location, click on it and select the Tomcat folder from the directory browser.

Once AD Agent has been deployed, the dialog will close

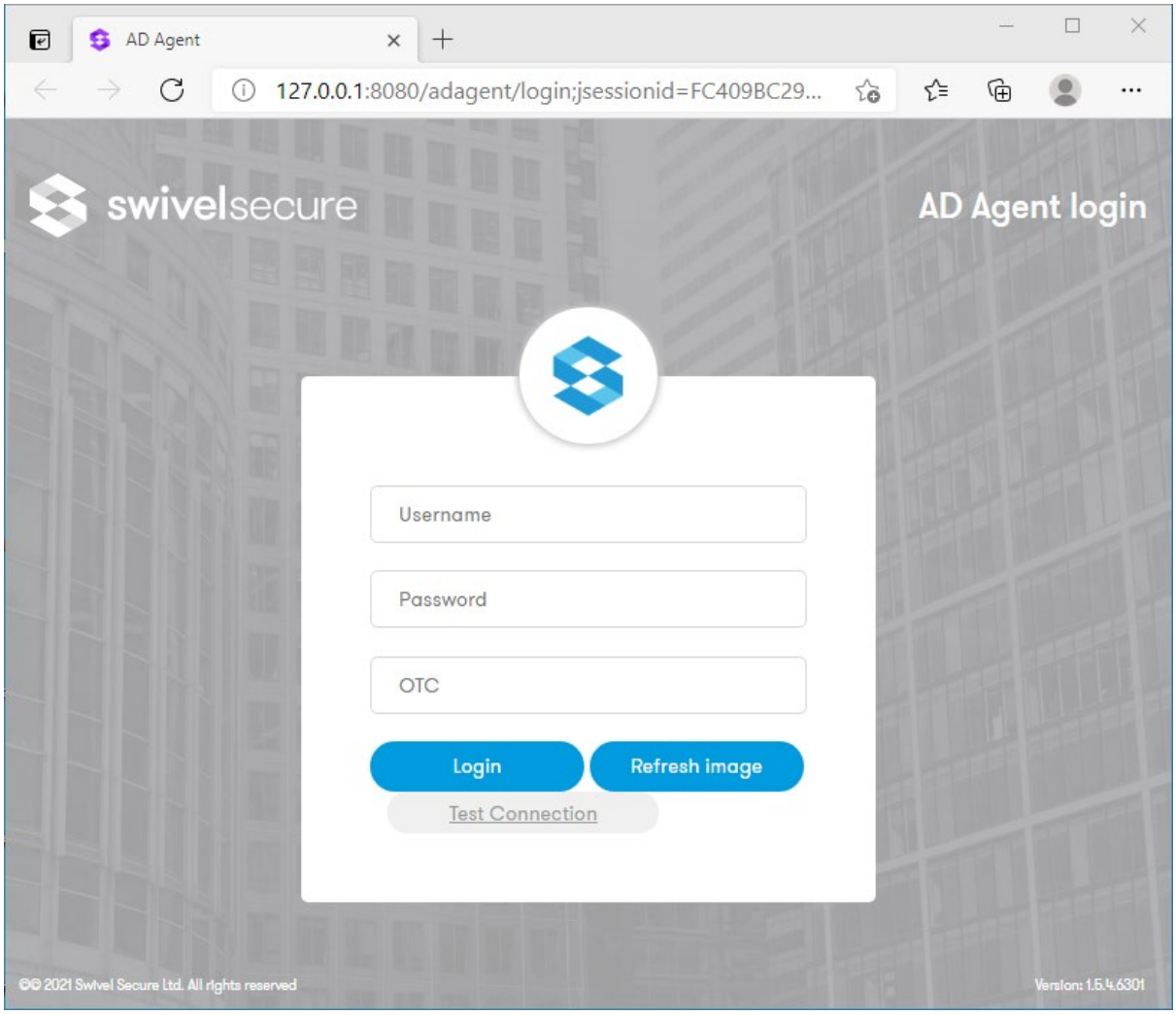


The dialog now shows that AD Agent is deployed. However, you will need to restart Tomcat to apply the Sentry settings. Clicking Apply will do this for you, provided Tomcat is running as a service. Otherwise, click Apply or OK to save the settings, then restart Tomcat manually.

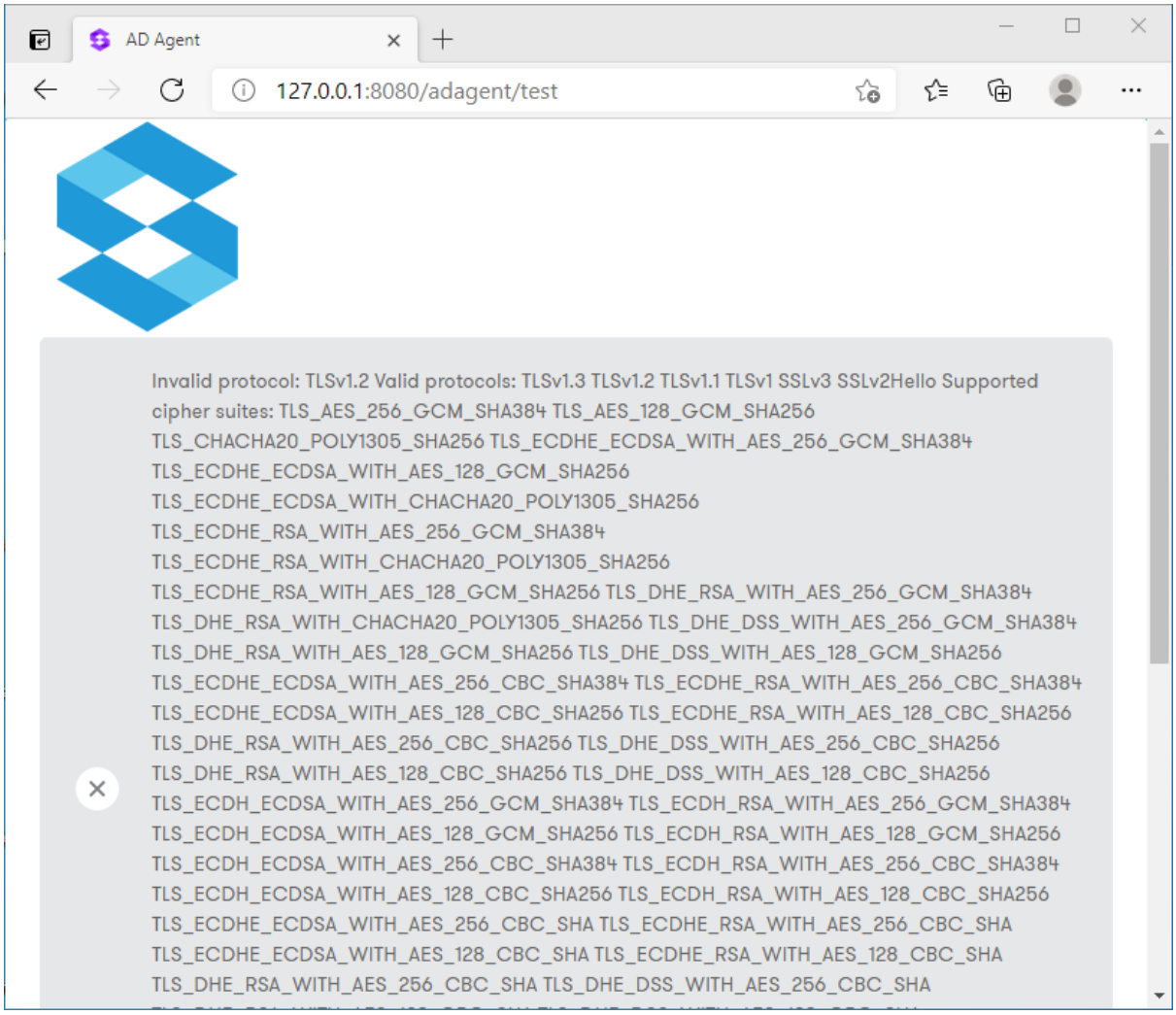
Testing AD Agent

You can open AD Agent by clicking on the “AD Agent Home Page” link, or simply enter http://localhost:8080/adagent in a browser.

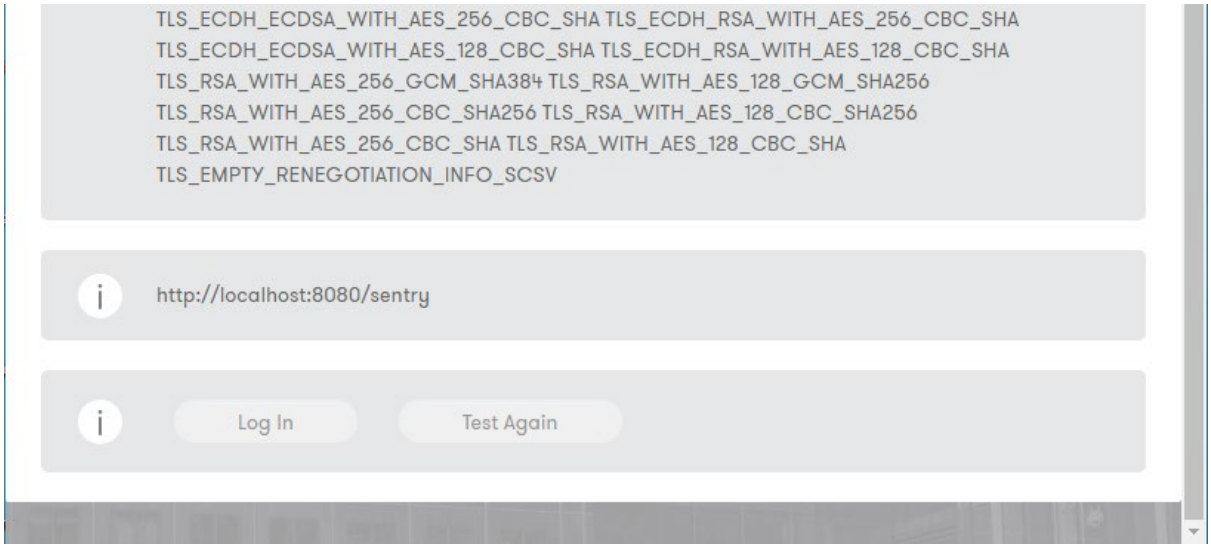
NOTE: if you prefer to run Tomcat as https, you will need to configure that within the Tomcat configuration. Instructions can easily be found online.



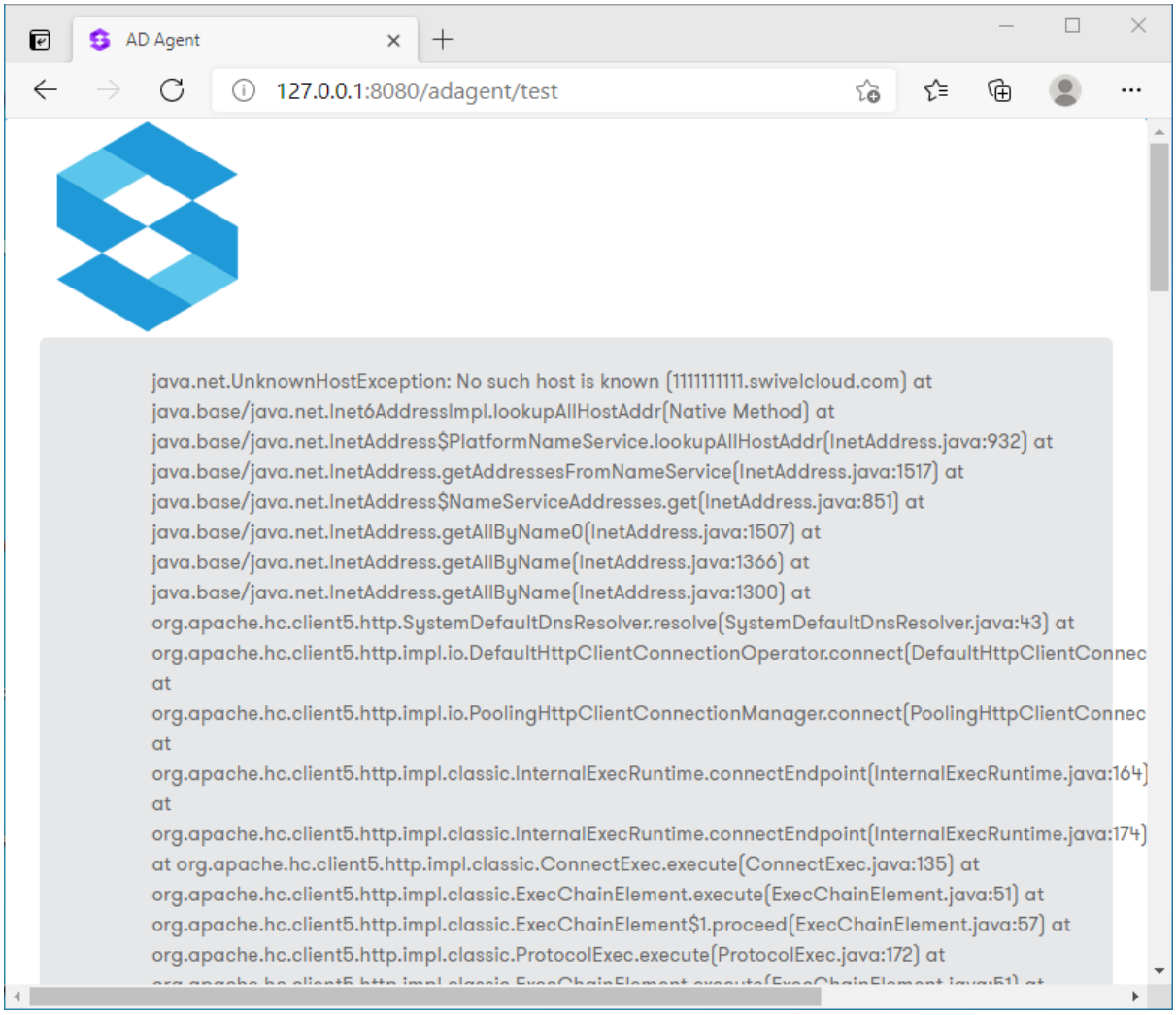
Here is the AD Agent login page. If you want to test that your settings are correct, simply click “Test Connection”. The following screens show some example results:



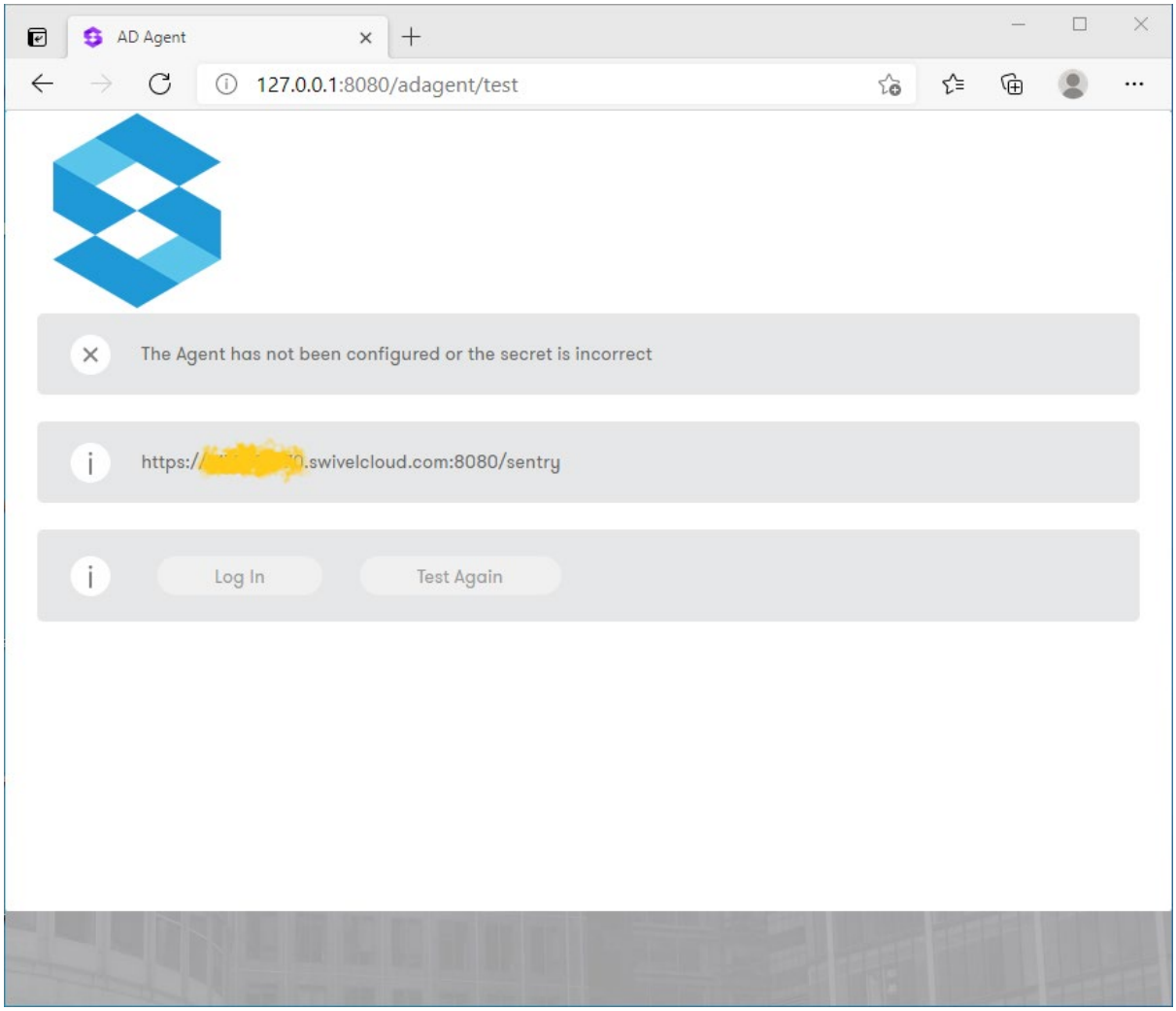
This is the screen you are likely to see if you have not configured the Sentry URL. It will be using the default localhost, so is attempting to connect to the local Tomcat instance.



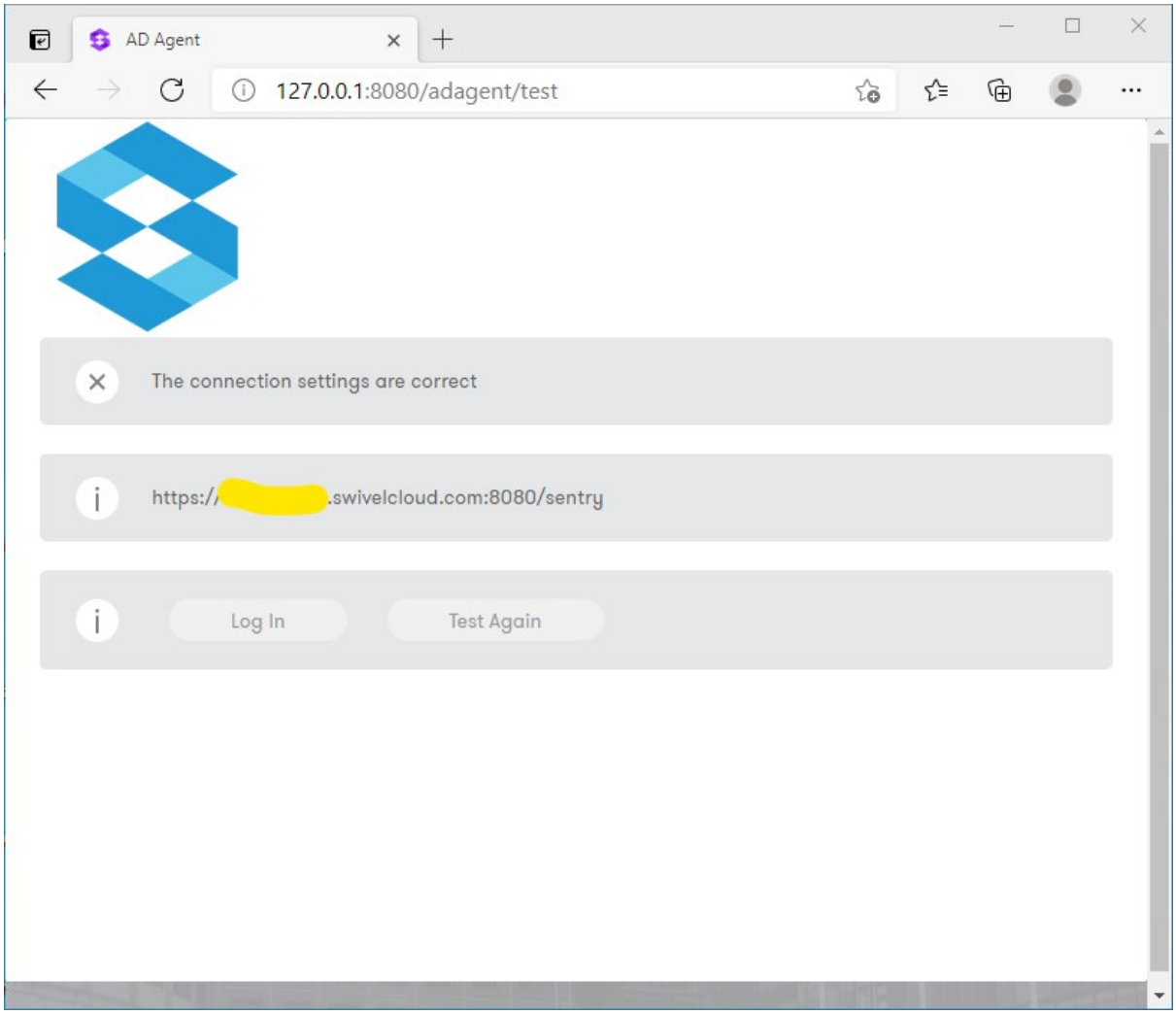
Scrolling down the screen, you will see that the URL is still http://localhost:8080.



This is the sort of error you will get if the host name is incorrect.



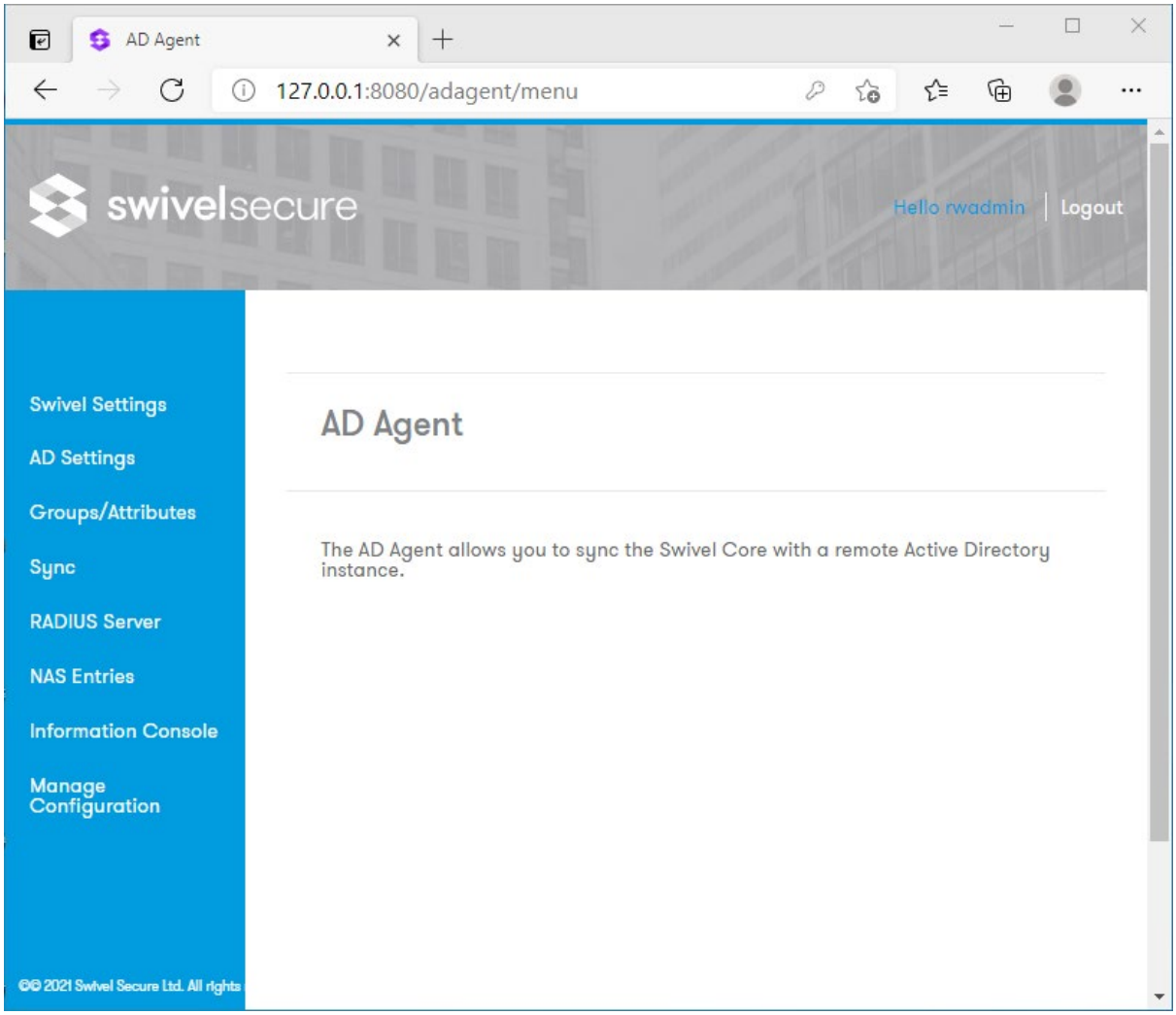
This is the error you will get if you have not configured an Agent in Sentry, or if the secrets do not match.



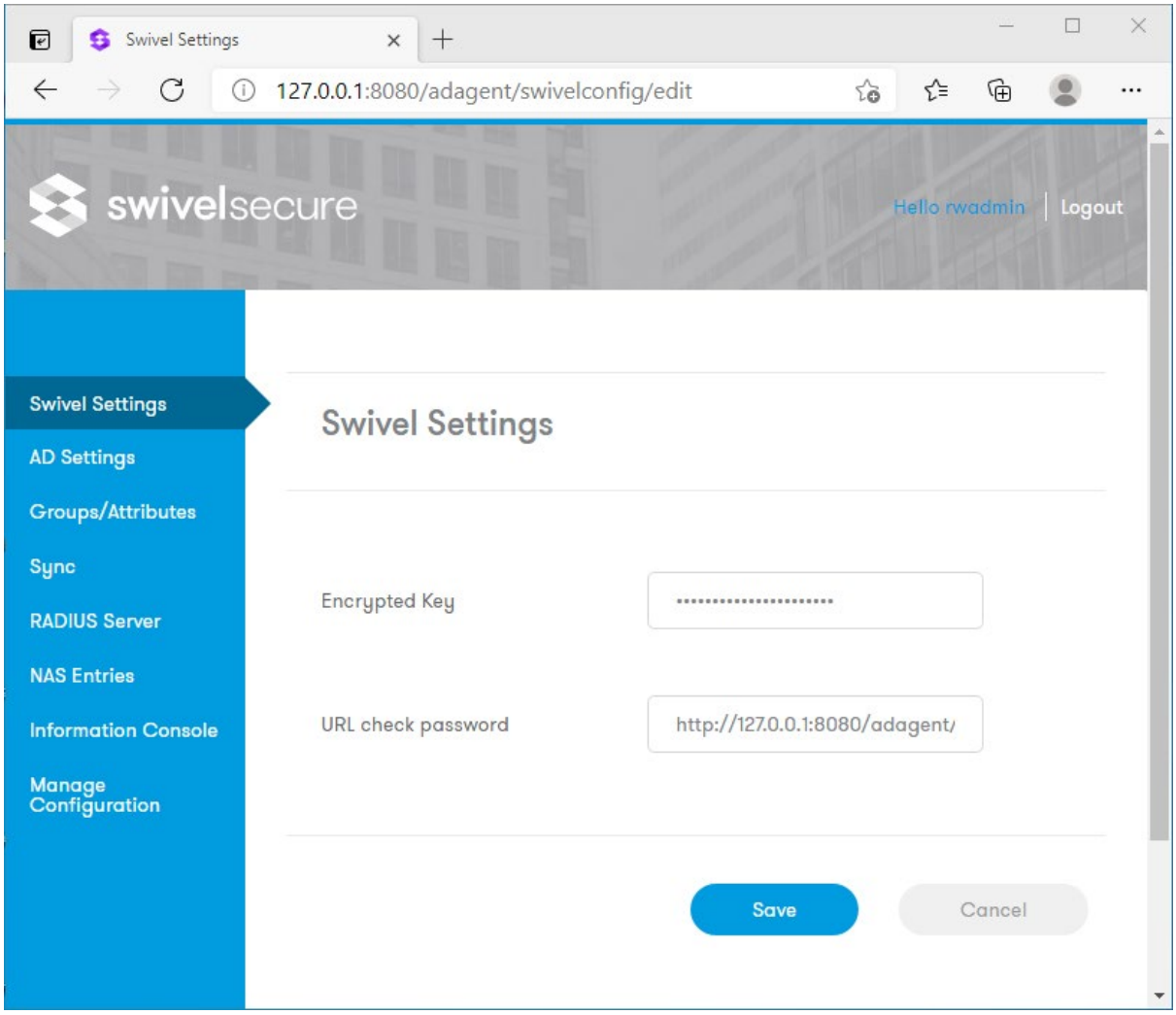
If the settings are correct, you should see this.

You can now log in using your Sentry credentials. Note that any Sentry user can log in to this console, so you should control access to this server.

Configuring AD Agent



This is the page you should see when you first log into AD Agent.



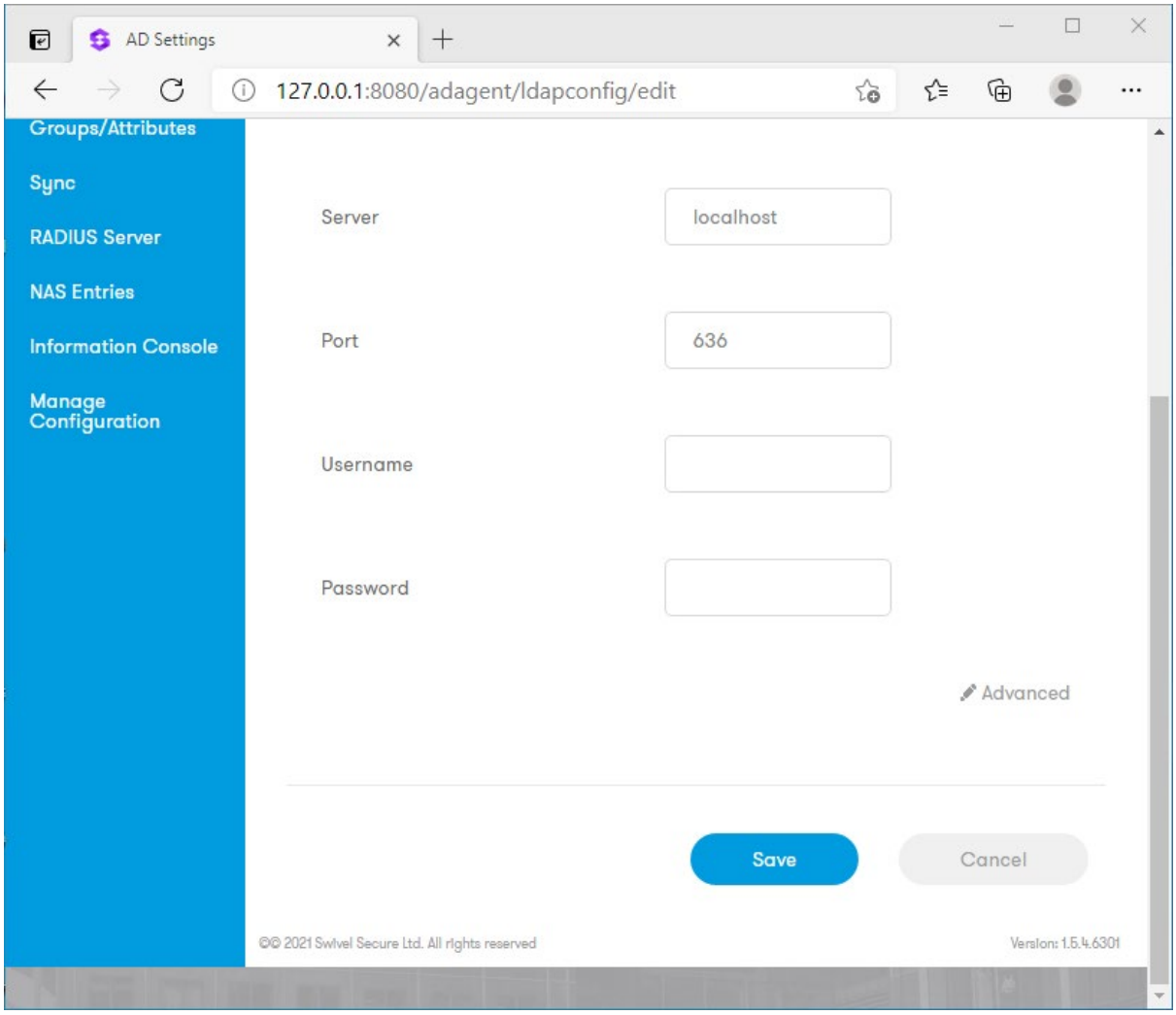
This is the Swivel Settings menu.

Encrypted Key

Indicates if the messages sent/received will be encrypted/decrypted. The value must be the same as the encrypted key configured in the Sentry Agent. If empty the messages won't be encrypted/decrypted other than via the standard encryption used on SSL.

URL check password

Indicates the URL where the AD Agent is listening for requests to check password. This value will be sent to Sentry so it knows to where to forward request to check AD passwords.



The AD Settings menu allows you to configure which domain controller is used connect to Active Directory.

Server

IP/Hostname where the AD is running.

Port

Port to use to connect to AD

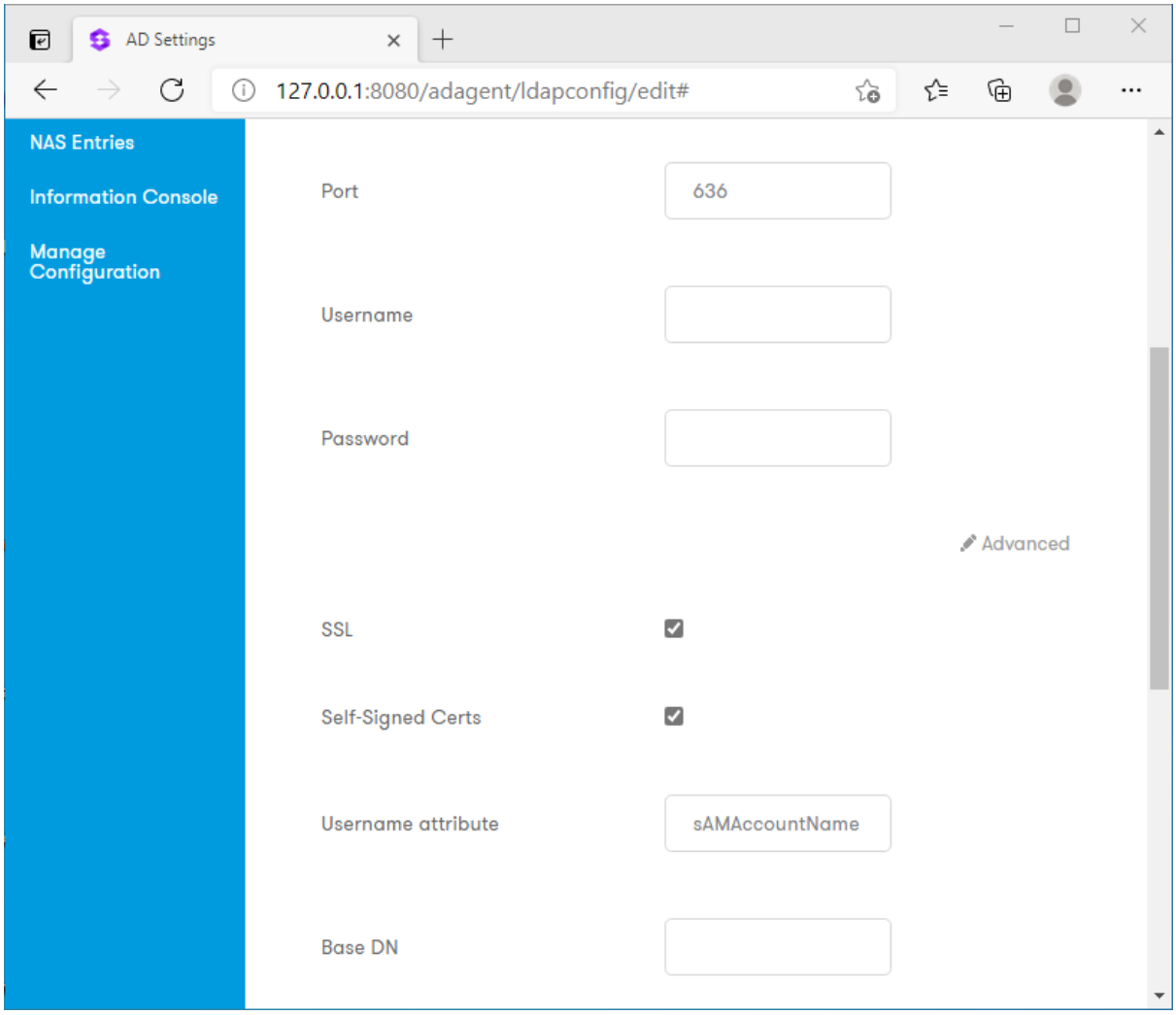
Username

AD's account username. This is the account used to read data from AD. Needs adequate read rights. Service accounts can be used. Typically, this will need to be the userPrincipalName.

Password

AD's account password

If you are connecting via secure LDAP (LDAPS) on port 636 (or 3269 for Global Catalog), you will need to expand the Advanced options:



SSL

Checked if the connection is SSL, unchecked otherwise.

Self-Signed Certs

If checked indicates that in an SSL connection, self-signed certs are accepted. It is important to note that this does not accept certificates if the hostname does not match the certificate. You must therefore ensure that the hostname on the certificate is used to connect to LDAPS. If necessary, you will need to add this name to the local hosts file.

Username attribute

Indicates the username's name attribute. By default: sAMAccountName

Base DN

Indicate the BaseDN, if empty will be root.

Group ObjectClass Name

Indicates the group object class name attribute. By default: group

User ObjectClass Name

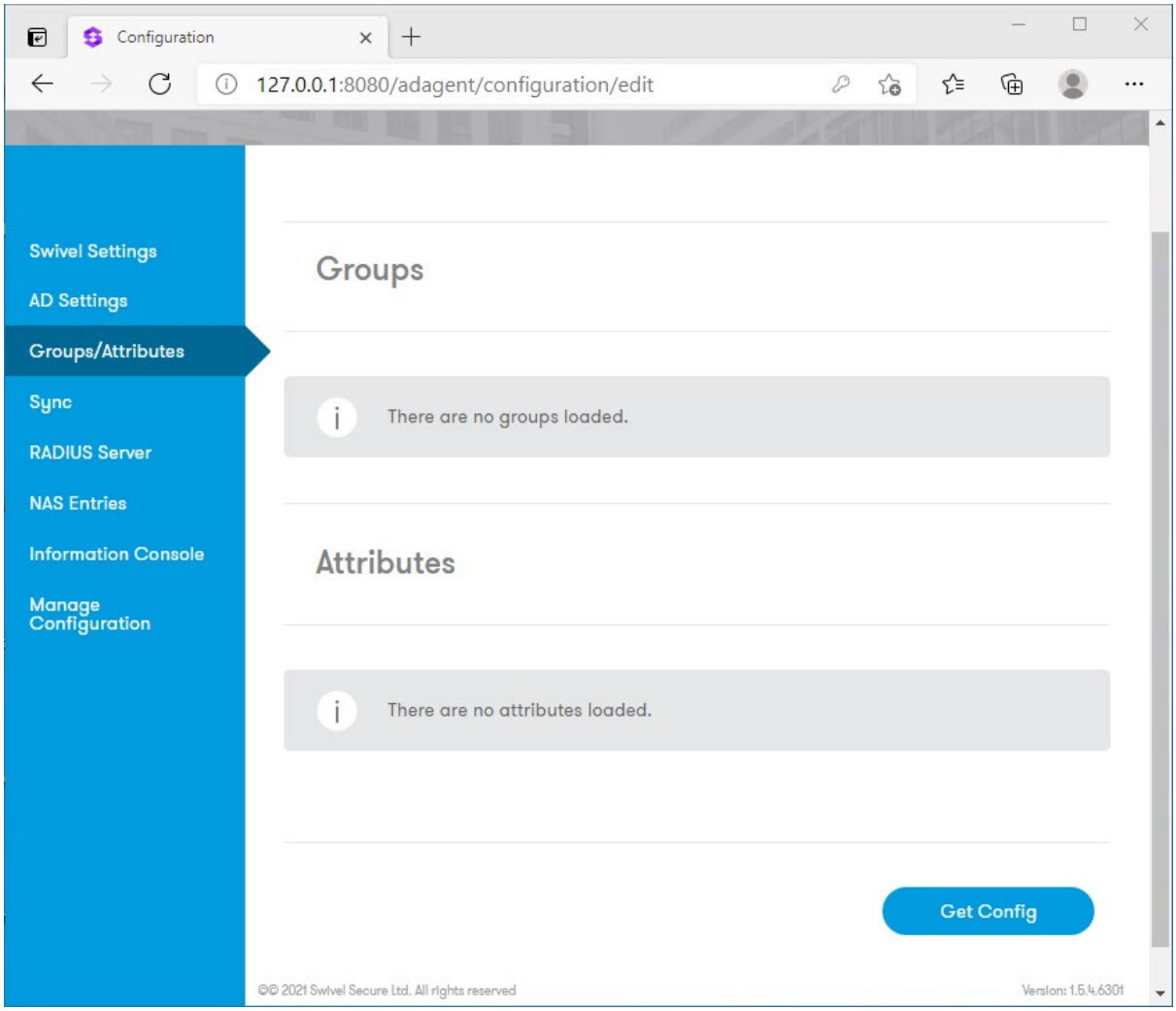
Indicates the group object class name attribute. By default: user

Member attribute name

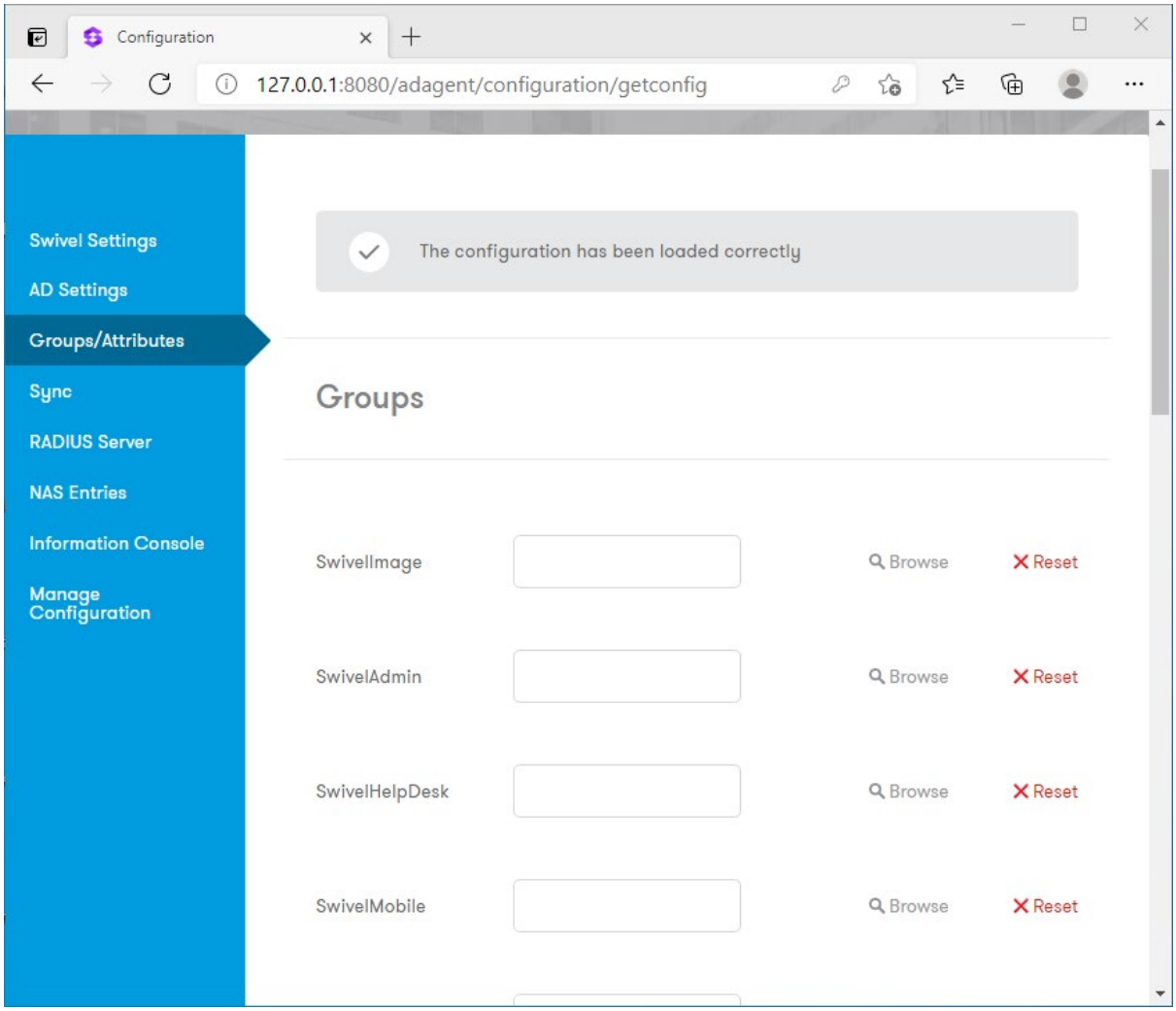
Indicates the member's name attribute. By default: memberOf

Last modification attribute name

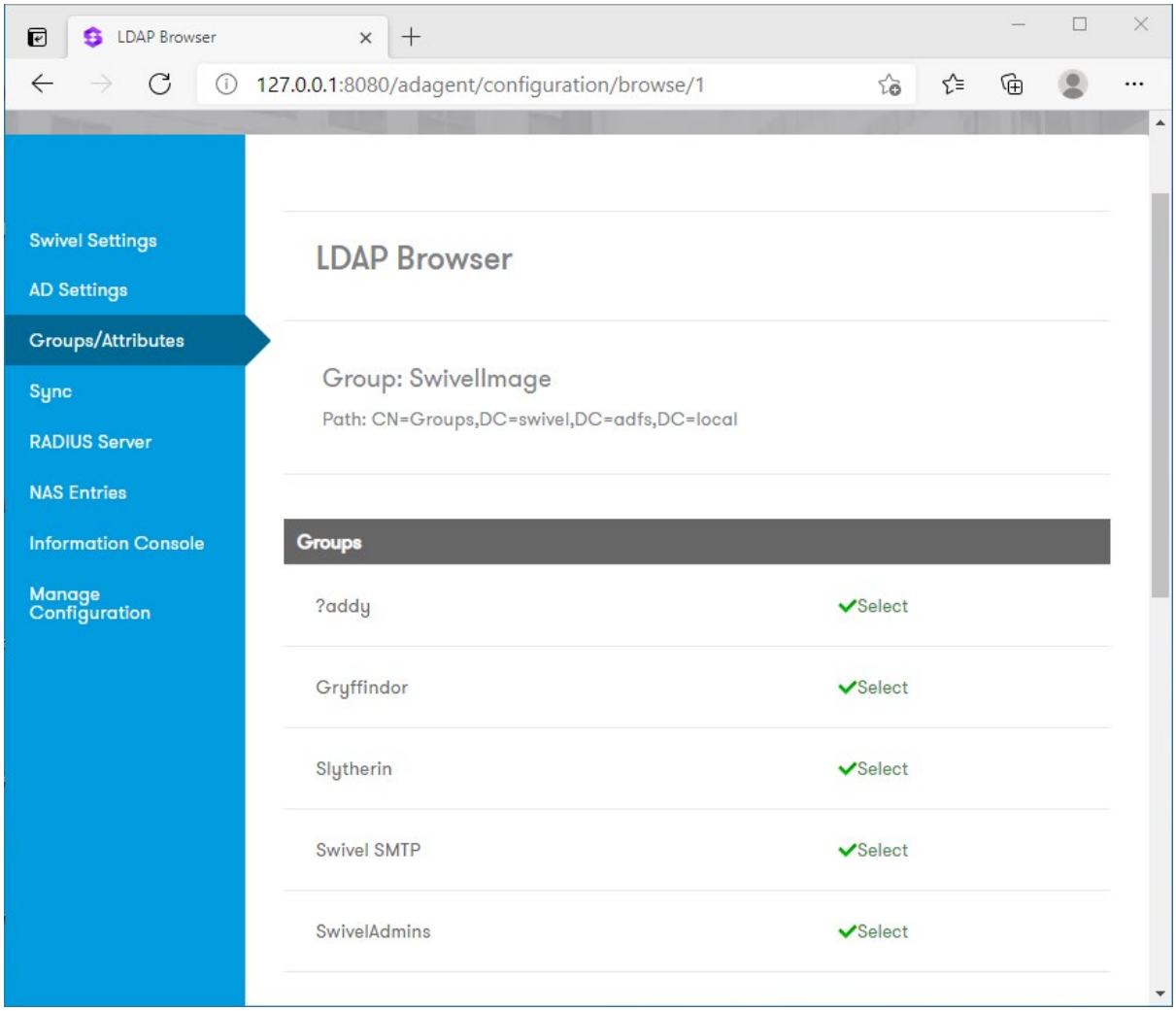
Indicates the last modification's name attribute. By default: whenchanged



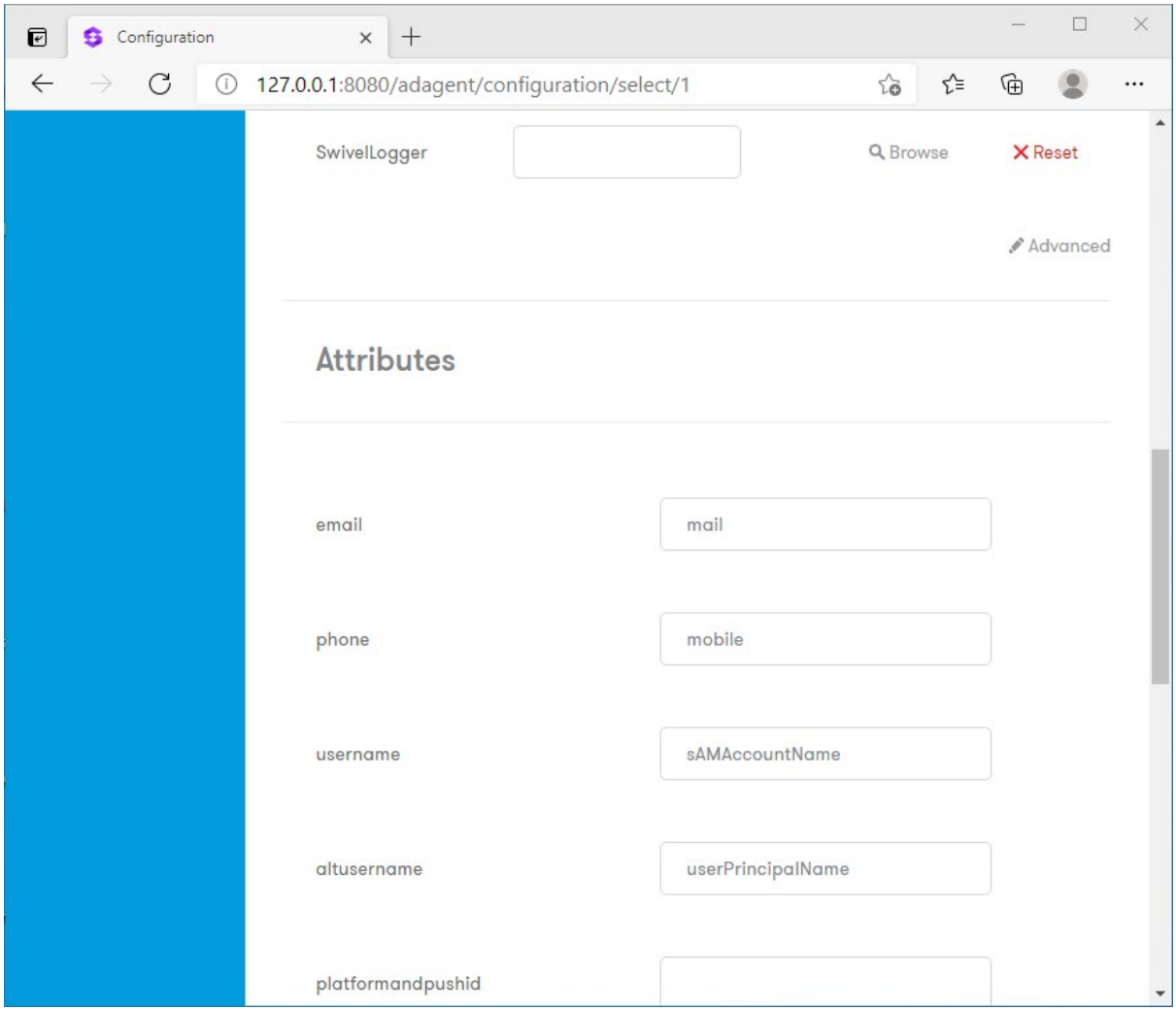
The Groups and Attributes menu allows you to configure which AD groups are used in Sentry, and which AD attributes are mapped to Sentry attributes. Before you can do this, you need to click on Get Config to download the known groups and attributes from Sentry.



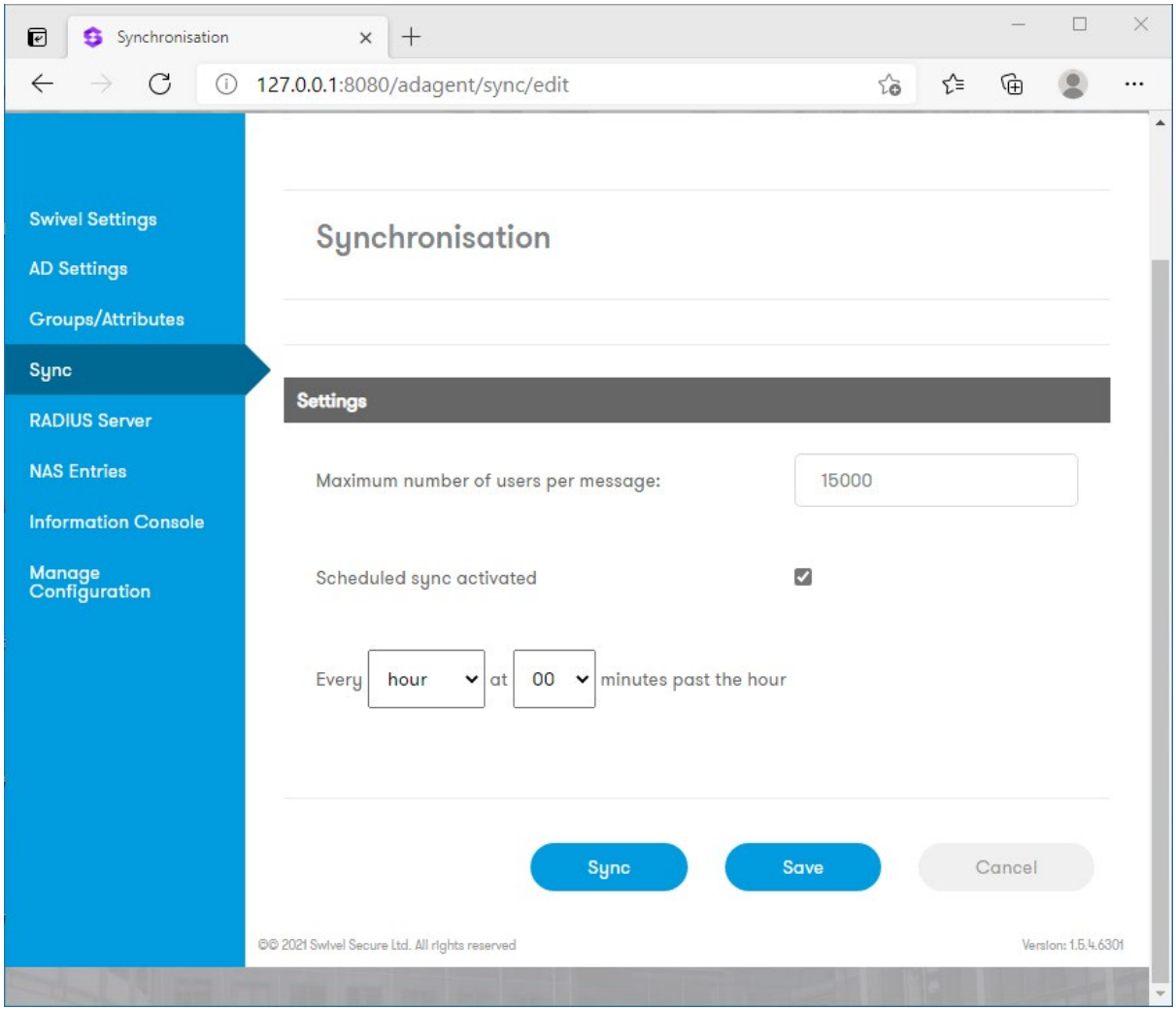
This page now shows all the groups known to Sentry. You do not have to fill in all of these, just the ones that you will be using. Click the Browse button next to a group to configure it, or you can type in the fully-qualified domain name manually.



This image shows the available groups from AD. Click Select to choose a group, or if any sub-containers are shown, you can Browse those further.



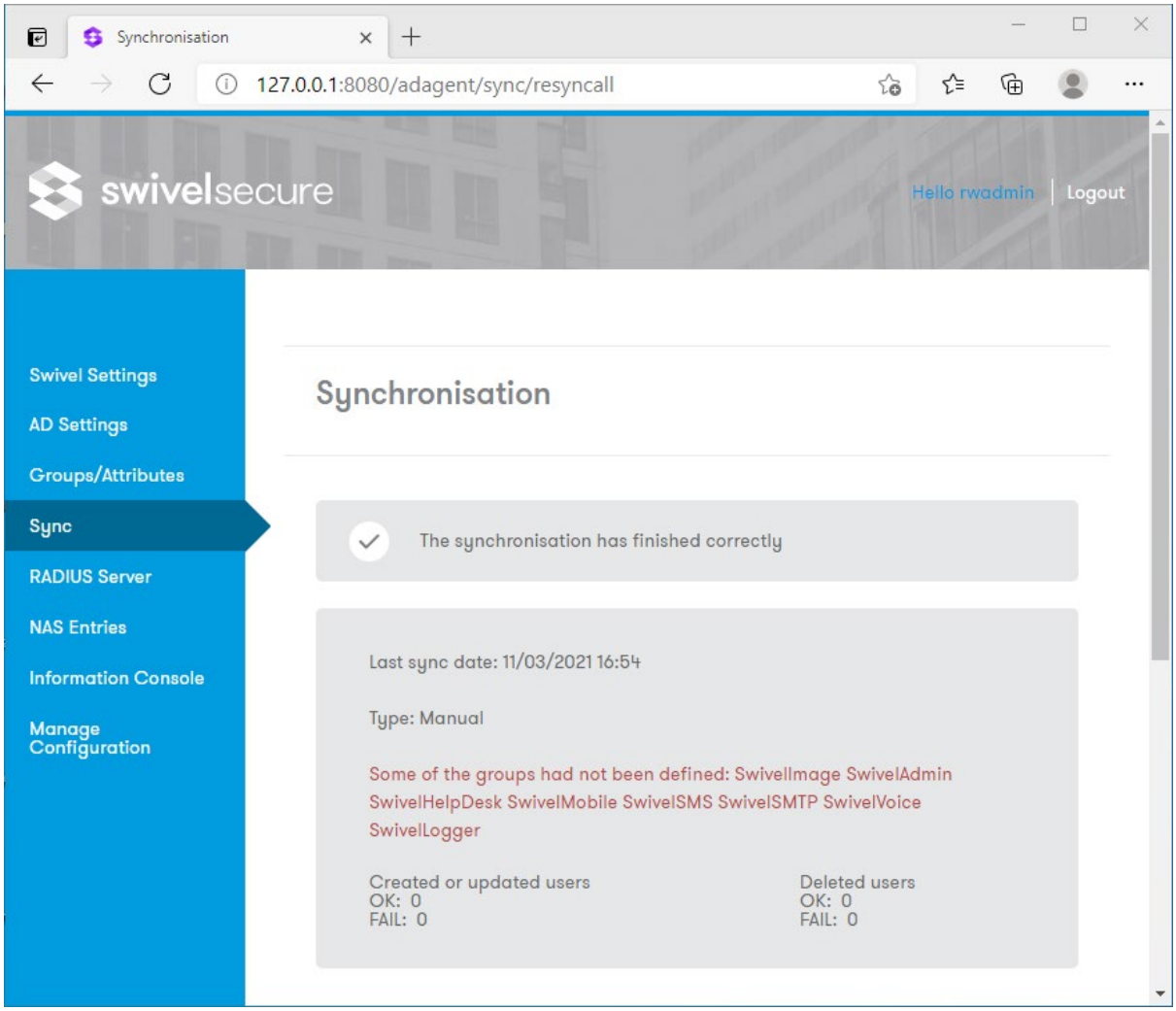
To configure custom attributes, click the Advanced button. The default settings will suffice in many cases, but you can change the attribute mappings as required.



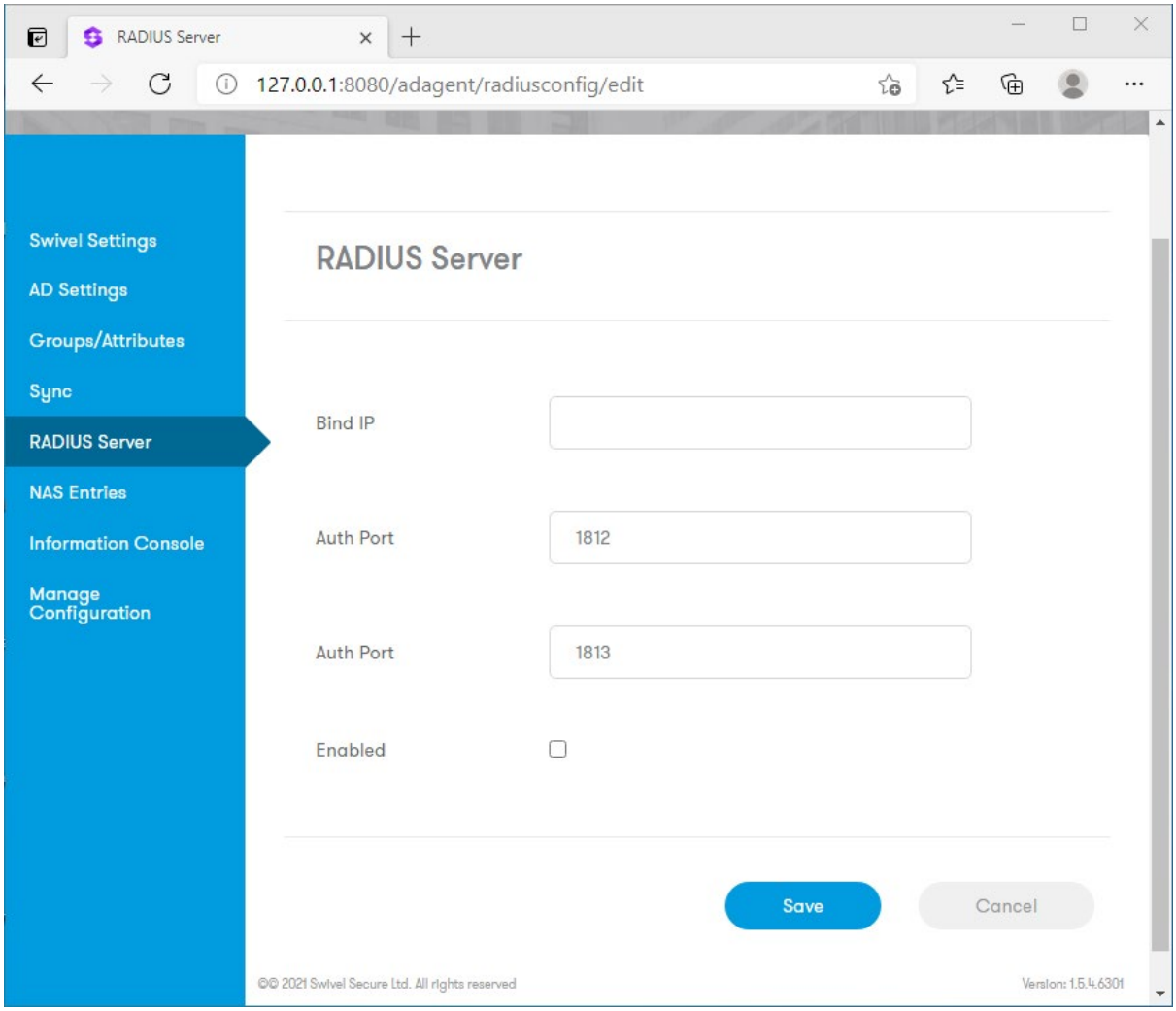
The Synchronisation tab allows you to configure synchronisation between Active Directory and Sentry.

To configure automatic synchronisation, click “Scheduled sync activated” and specify how often the sync is run.

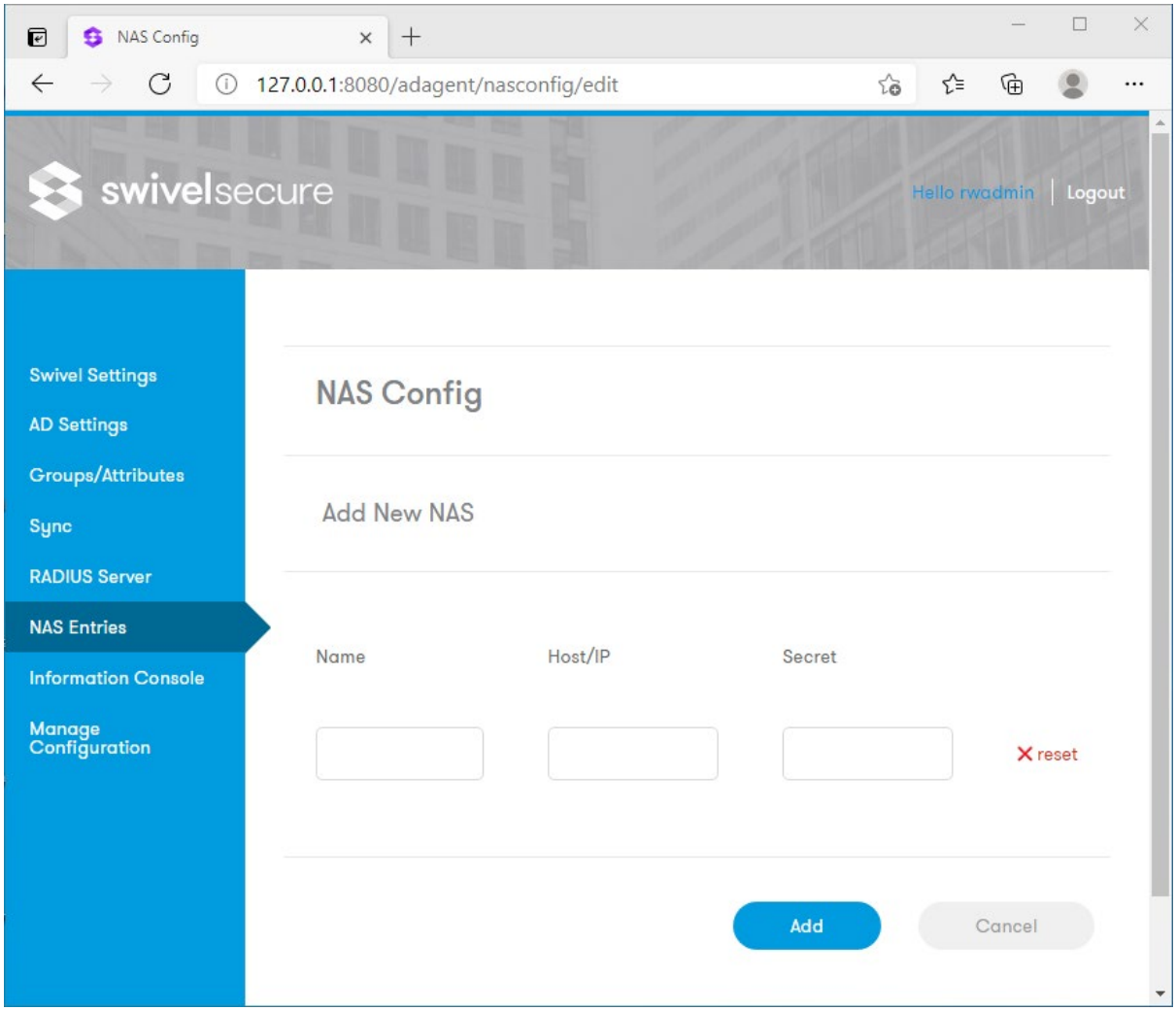
You can choose to do a Manual Sync by clicking the Sync button. This will resync all the users, while automatic/scheduled sync is incremental: accounts that have not been changed since the last sync will not be updated.



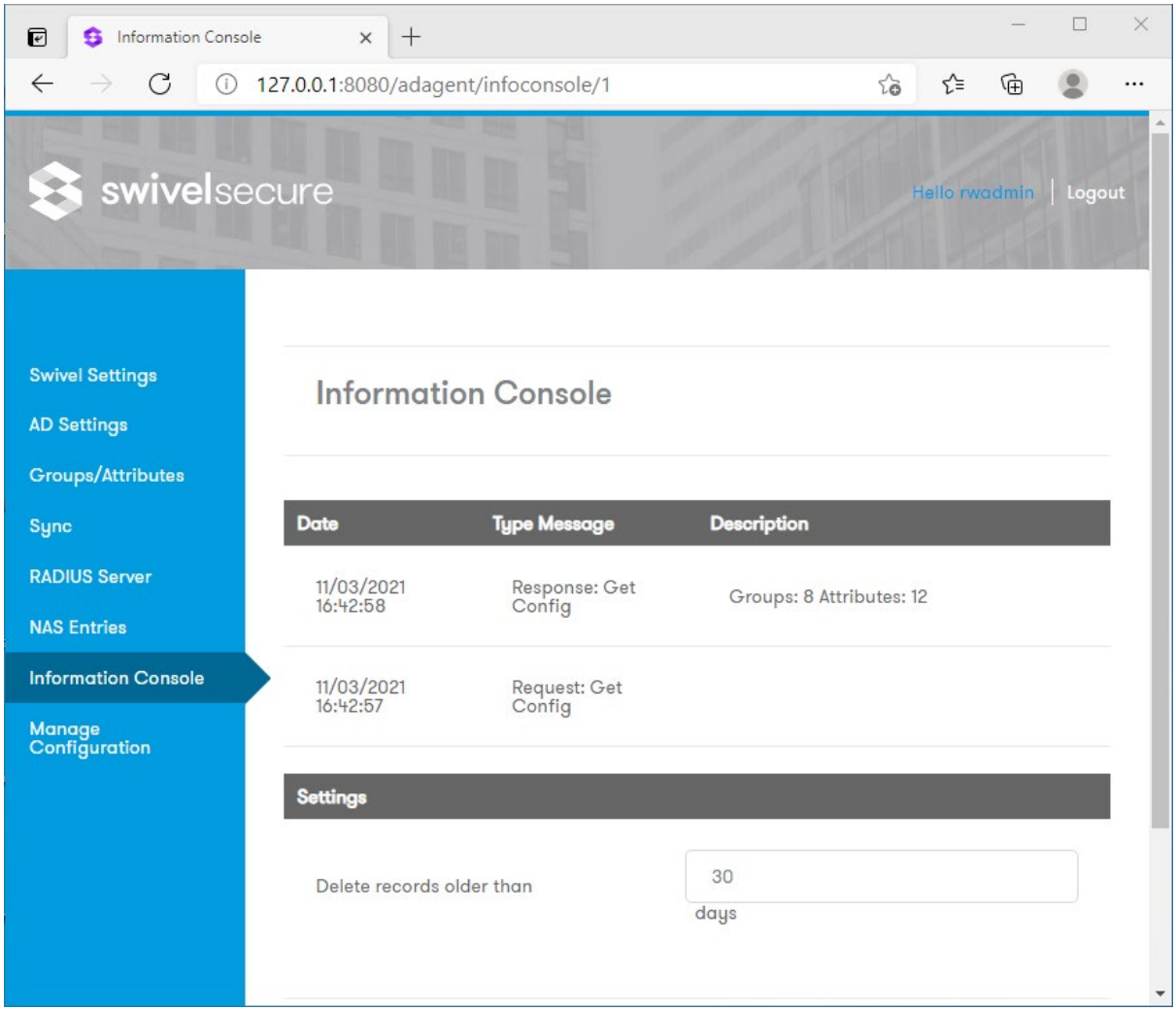
After a manual sync, any problems are shown and the number of changes indicated.



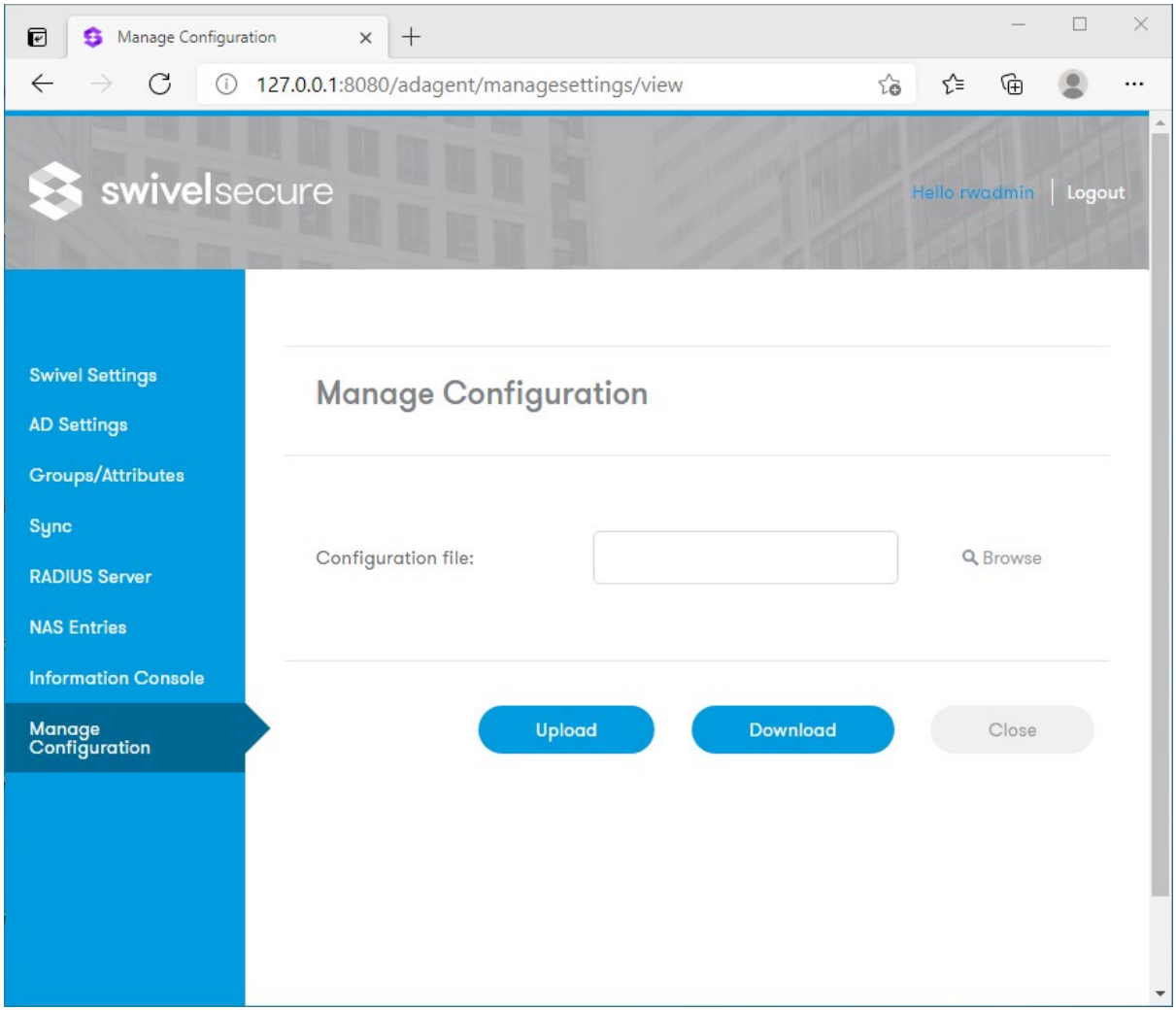
The RADIUS Server tab allows you to enable AD Agent to act as a local RADIUS server. As typically RADIUS is not used over the internet, RADIUS requests from the local network can be sent to this server, where they will be relayed to Sentry as AgentXML login requests.



To use the RADIUS server, you must configure any VPN gateways etc. as RADIUS NAS entries using the NAS Entries screen.



The Information Console tab shows the AD Agent log.



Finally, the Manage Configuration tab allows you to export (Download) or import (Upload) settings from this AD Agent, as a backup or to transfer to another device.