

AD Agent

Contents

- 1 Introduction
- 2 Installation
- 3 Pre-Configuration
- 4 Create an Agent
- 5 Configuration
- 6 Swivel Core Settings
- 7 Active Directory (AD) Settings
- 8 Groups/Attributes
- 9 Synchronisation
- 10 Scheduled sync
- 11 Sync (Manual sync)
- 12 Information Console
- 13 Manage Configuration
 - ◆ 13.1 Download configuration
- 14 Upload configuration
- 15 Check Password
- 16 Encryption
- 17 RADIUS
- 18 NAS

Introduction

The AD Agent is a Swivel Remote Sync Client application that allows the synchronisation of users between the Core and a remote Active Directory (AD) server. The communication between these 2 systems is done through XML messages. To allow the exchange of messages, the Core has to have the Agent configured and the option ?Can act as repository? has to be set to YES.

The AD agent reads the details from users stored in the Active Directory and sends the details of those users to the Swivel Core. In order to do this the AD Agent needs to be configured to know what data to read, where to read it from and where to send the results.

Installation

The installer for the AD Agent can be found [here](#). The zip file contains 2 files:

- AD Agent Installer.exe
- backupPreviousConfig.bat

The latter file is only required if you have already installed an earlier version of the AD Agent. The configuration is deleted on update, so this batch file will take a backup of them before running the installer, and will subsequently restore the saved configuration. If you do not have a previously-installed AD Agent, you can simply run AD Agent Installer.exe directly.

The installer will install the AD Agent and all other required software. To see to see how the installer operates refer to [this video](#)

Generally you can accept all the defaults, the only exception to this would be if you are installing the AD Agent on a server that already has a service running on port 8080, in which case you need to select a different, unused port. The Agent needs to be installed on a server that can access a domain controller via LDAP and can also access the associated Swivel Core server.

The default for the AD Agent is English locale. In order to make it work with another locale there is need to copy the file ?C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\adagent\WEB-INF\classes\messages_en.properties? to ?C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\adagent\WEB-INF\classes\messages_es.properties? and restarted Tomcat.

Pre-Configuration

To configure the AD Agent it is required to edit the files **settings.properties** and **security.properties** .

These 2 files will be by default on the directory <user.home>\.swivel\srsc\. If the system variable SWIVEL_HOME nor the swivelHome property in web.xml have been defined, <user.home> will be the home directory of the account the Tomcat service is running as - if it runs as **Local System**, which is the default, it will be the root of the C: drive. In that folder, will be the file configuration.properties. Those files will be created automatically when the application is launched the first time. The DB will be on \$user.home/.swivel/db

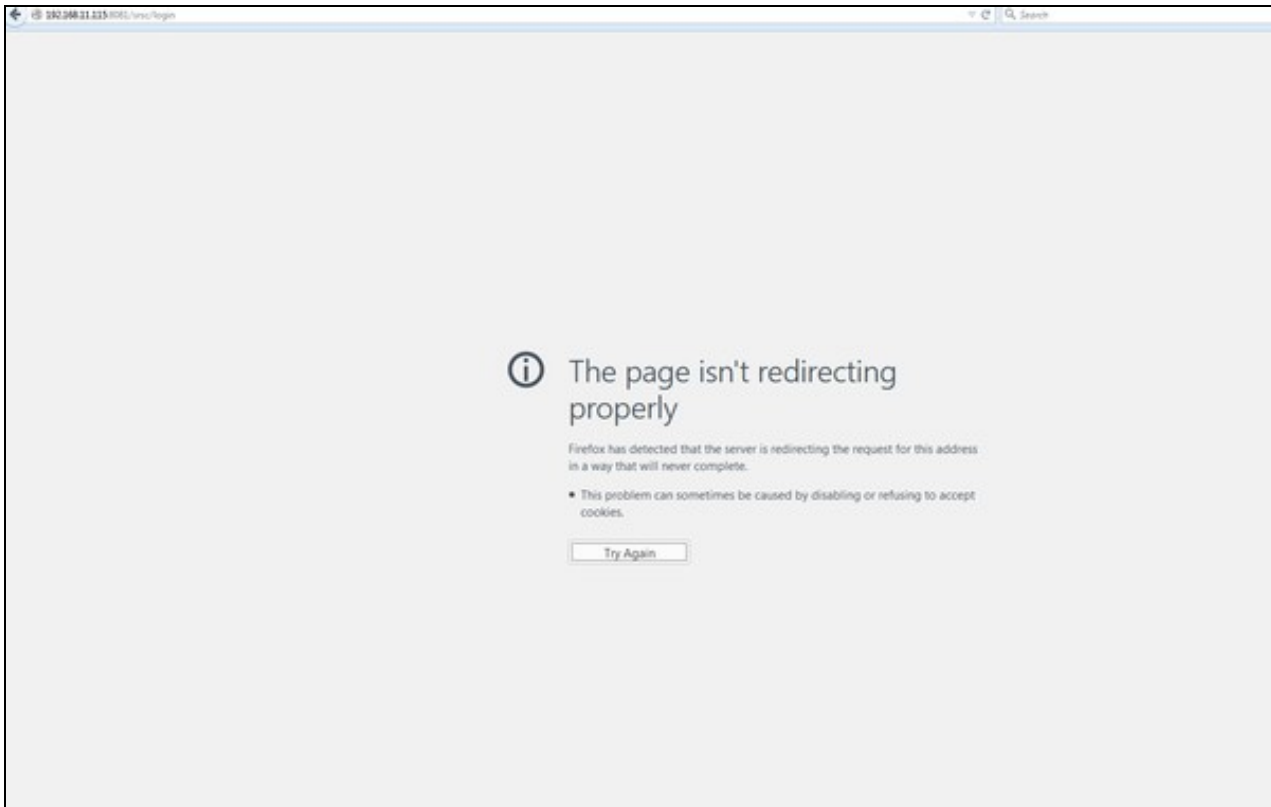
This will usually be achieved by using the configuration program (see installation) The file **settings.properties** is used to define the connection to the Swivel Core server that the AD Agent will communicate with has the following attributes:

pinsafessl=false	Whether the connection is via SSL (TLS)
pinsafeselfsigned=false	Are self-signed certificates supported
pinsafeserver=localhost	Core server hostname
pinsafecontext=pinsafe	Core server context. This will usually be pinsafe
pinsafeport=8080	Core server port, default would be 8080
pinsafesecret=secret	Shared secret, needs to match setting on the core
pinsafexmlversion=3.97	Version of Agent-XML used
imagesssl=false	Are self-signed certificates supported for images
imageserver=localhost	Core server hostname for getting TURING image
imagecontext=proxy	Core server context for getting TURING image
imageport=8443	Core server port for getting TURING image

The file **security.properties** allows to define the IP restrictions. It has the following two parameters:

core.iprange	Indicates the IP or IP range of the Core that will be allowed to check password. By default is 0.0.0.0/0
admin.iprange	Indicates the IP or IP range allowed to access to the app configuration screens.

Access will be denied for other IPs. Default is 0.0.0.0/0 (which allows access from all IPs) If access from non-allowed IP is attempted the following screen will be displayed.



Create an Agent

Create an Agent on the Swivel Core (port 8080), under Server Agents. The Hostname/IP should be the public or external address of the server in which the AD Agent is installed on. A Shared Secret must be set and it should match the secret which has been entered on the AD Agent installer.

Can act as Repository must be set to Yes which means the Agent will also be added as a Repository under User Administration, then under Repository drop down menu, you can select the AD Agent.

Encryption/Decryption key can be set but is optional. If it is set then it must match the Encryption Key set on the AD Agent configuration, under Swivel Core Settings - please see [Swivel Core Settings](#)

Configuration

NOTE: Due to the IP restriction, to access to the application use 127.0.0.1 or the correspondent IP instead of localhost. URL: <https://127.0.0.1:8080/adagent>

To access the main page you need to access using a valid Swivel Administrator account. I.e an account that has admin rights on the Swivel Core server the AD Agent is connecting to.

If a Domain prefix or Suffix is used, then enter this with the Username when logging into the AD Agent.



AD Agent login

Username:

Password:

OTC:

Login

Refresh image

The AD Agent's main page is the following:

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

AD Agent

The AD Agent allows you to sync the Swivel Core with a remote Active Directory.

Swivel Core Settings

This screen allows user to configure the following:

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

Swivel Settings

Encrypted Key:

.....

URL check password:

http://127.0.0.1:8080/a

Encrypted Key

Indicates if the messages sent/received will be encrypted/decrypted. The value has to be the same as the encrypted key configured in the 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 the Core so it knows to where to forward request to check AD passwords.

Active Directory (AD) Settings

A main purpose of the AD Agent is to read user data from a local Active Directory server and forward that information. To do this the AD Agent needs to be configured to read the correct information from the required AD server.

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

AD Settings

Server: localhost

Port: 389

Username:

Password:

SSL:

Self-Signed Certs:

Username attribute:

sAMAccountName

Base DN:

Group ObjectClass Name:

group

User ObjectClass Name:

user

Member attribute name:

memberOf

Last modification attribute name:

whenchanged

This screen requires the following information to be added.

- 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
- Password
AD's account password
- SSL
Checked if the connection is SSL, unchecked otherwise.
- Self-Signed Certs
If checked indicates that in a SSL connection self-signed certs are accepted.
- 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

NOTE: Currently AD Agent gets only non-disabled users, and to do that a rule has been added: ?!UserAccountControl:1.2.840.113556.1.4.803:2? this rule works for AD and it is something not configurable by the user in the application. This rule maybe is different for an OpenLDAP. So currently AD Agent is only known to work with AD.

Groups/Attributes

Once the Swivel Settings and AD settings have been configured the configuration of Groups/Attributes can be downloaded from the Core

If Swivel Settings are not configured and the user clicks ?Get Config? button an error message will be shown. Otherwise, attributes and groups will be loaded

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

Groups

SwivelAdmin	cn=pinsafeusers,ou=pinsafe,dc=te
SwivelImage	
SwivelHelpDesk	
SwivelMobile	
SwivelSMTP	
SwivelToken	

Attributes

email	mail
phone	mobile
username	sAMAccountName
altusername	userPrincipalName
familyname	sn
givenname	givenName
platformandpushid	

The groups on the core can then be mapped to the groups within the AD by using the browse version to find and select the group within AD. Groups appear in the first section, next to them 2 buttons appear, ?Browse? to assign an AD and ?Reset? to delete the current value.



- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

The configuration has been loaded correctly

Groups

SwivelAdmin

SwivelImage

SwivelHelpDesk

SwivelMobile

SwivelSMTP

SwivelToken

Get

The ?Browser? screen shows the current AD Path, the name of the group that the user wants to assign a value on and a list of Groups and Subcontainers of the current path.

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

LDAP Browser

Group: SwivelAdmin

Path: ou=Tony_Pinsafe,dc=test,dc=local

Groups

Tony_Group



Tony_Test



Subcontainers

Pin_Test_Tony



When an AD group is selected automatically is assigned to the group.

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

Groups

SwivelAdmin	<input type="text" value="cn=pinsafeusers,ou=pinsafe,dc=test"/>
SwivelImage	<input type="text"/>
SwivelHelpDesk	<input type="text"/>
SwivelMobile	<input type="text"/>
SwivelSMTP	<input type="text"/>
SwivelToken	<input type="text"/>

Get O

The same thing can then be performed for mapping the attributes.

Attributes section appears into the ?Advanced? section.

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

Groups

SwivelAdmin	cn=pinsafeusers,ou=pinsafe,dc=te
SwivelImage	
SwivelHelpDesk	
SwivelMobile	
SwivelSMTP	
SwivelToken	

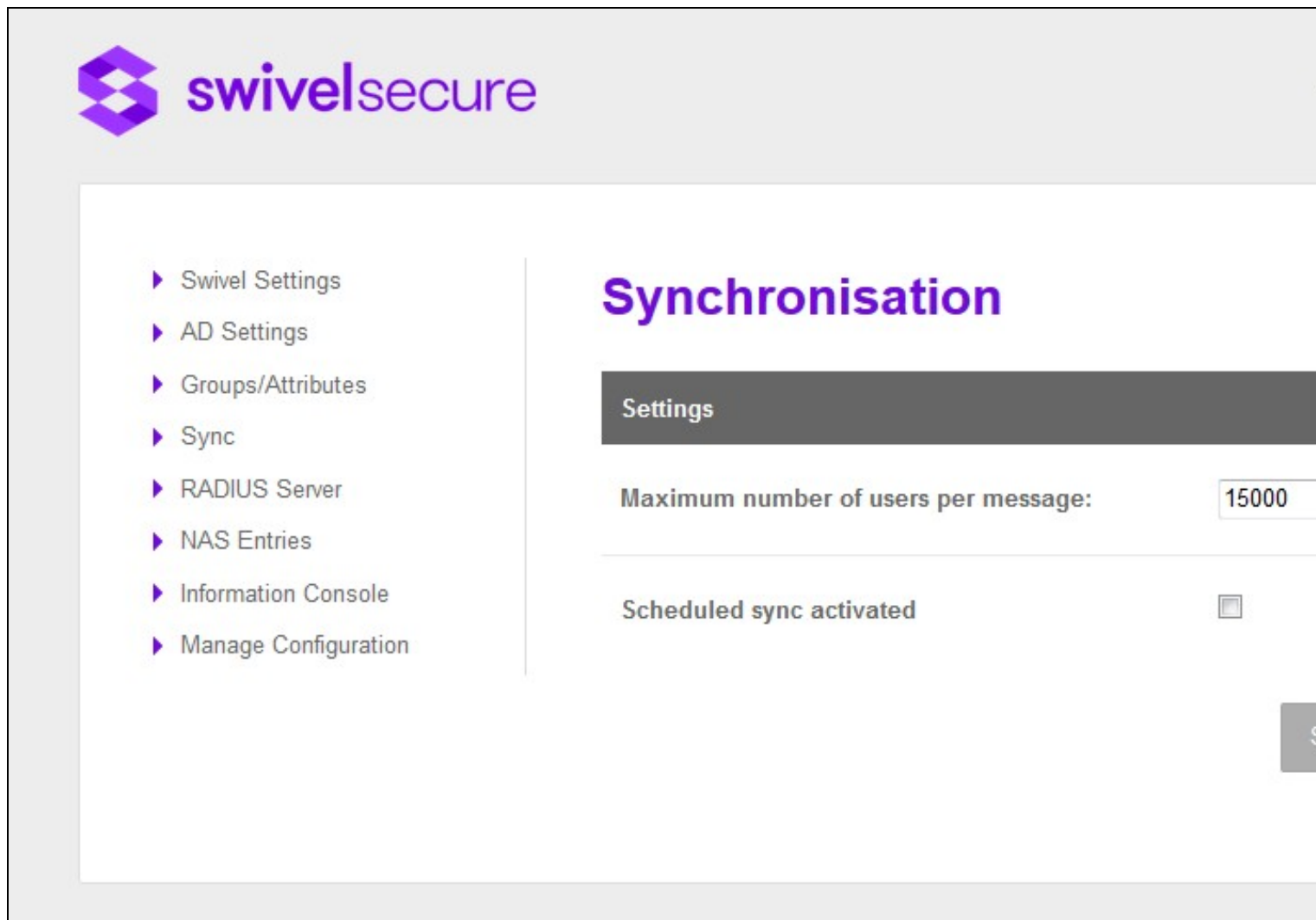
Attributes

email	mail
phone	mobile
username	sAMAccountName
altusername	userPrincipalName
familyname	sn
givenname	givenName
platformandpushid	

IMPORTANT: To save all the changes done in that screen ?Save? button has to be clicked.

Synchronisation

In the synchronisation screen, the user can indicate the maximum number of users that will be sent per message. If the number is 0 or less it will indicate that is no limit defined. Furthermore, the user can decide to do a Manual Sync clicking the Sync button that will resync all the users or an automatic synchronization where the user can specify when the synchronization will be executed.



The screenshot shows the Swivel Security web interface. At the top left is the Swivel Security logo. A navigation menu on the left lists: Swivel Settings, AD Settings, Groups/Attributes, Sync, RADIUS Server, NAS Entries, Information Console, and Manage Configuration. The main content area is titled 'Synchronisation' and contains a 'Settings' section. Under 'Settings', there is a field for 'Maximum number of users per message' with the value '15000'. Below that is a toggle for 'Scheduled sync activated', which is currently turned off.

When a synchronisation is started the AD Agent contacts the core and if all is ok compares the last sync time with the last modified time on AD and if changes are required, sends the new users details to the core.

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

Synchronisation

The synchronisation has finished correctly

Last sync date: 18/11/2016 13:38

Type: Manual

Some of the groups had not been defined: SwivelImage SwivelHe
SwivelSMTP SwivelToken

Created or updated users

OK: 0

FAIL: 3

Dele

OK:

FAIL

Settings

Maximum number of users per message:

15000

Scheduled sync activated



In this screen also appears information about the last synchronization (Manual or Scheduled). The information is the following:

Last sync date

Date and time of last sync

Type

Manual/Scheduled

If there are groups defined on the core that are not defined on AD Agent there will be a message showing the names of the groups not defined

Created or updated users
number of successes, number of failures

Deleted users
number of successful deletions, number of Failed deletions.

When a user has been synced with the Core, the next synchronization will not be update that user again unless:

- * Data of that user has been updated in the AD after last sync, e.g. whenChanged is more recent than lastSyncTime
- * There has been a change in the groups/attributes screen after last sync so next sync all the users will be updated.
- * The sync all user option is used

NOTE: clocks of AD server and the AD Agent need to be synchronized.

Scheduled sync

To define a scheduled sync it is required to check the field ?Scheduled sync activated?, when this field is checked a new field/s appear under this field to defined the scheduler. When the scheduler is defined the user has to click ?Save?. A synchronization job will be started and executed every time that meet the time defined in the scheduler. If the job is already started and the user edit the scheduled time and press ?Save?, automatically the job will be rescheduled but if the user set unchecked the activated field the job will be stopped. The possible schedule times are shown below:

The screenshot displays a configuration interface for a scheduled sync job. It features six rows of dropdown menus and text labels to define the frequency and timing of the sync. Each row starts with the word "Every" followed by a frequency dropdown, then "at" followed by time-related dropdowns, and finally "minutes past the hour" or "of" followed by month and time dropdowns.

- Row 1: Every **minute** ▼
- Row 2: Every **hour** ▼ at **00** ▼ minutes past the hour
- Row 3: Every **day** ▼ at **00** ▼ : **00** ▼
- Row 4: Every **week** ▼ on **Sunday** ▼ at **00** ▼ : **00** ▼
- Row 5: Every **month** ▼ on the **1st** ▼ at **00** ▼ : **00** ▼
- Row 6: Every **year** ▼ on the **1st** ▼ of **January** ▼ at **00** ▼ : **00** ▼

Sync (Manual sync)

This action allows to the user resync all the users independently of they were synced before or not.

NOTE: If the rights of the groups are changed in the Core those changes are not communicate to the AD Agent and the users won't be updated. The next AD Agent synchronization won't update the users of those groups if the data on the AD for that users has not be modified. In that case the manual sync action has to be done to update the rights.

Information Console

This screen shows the information about the messages exchanged between Swivel Core and AD Agent. The messages can be deleted automatically thanks to a schedule job that will be executed every day at 19:00.

That configuration could be changed in the file dispatcher-servlet.xml if it was needed.

The user can customize the deletion indicating the number of days that the info message has to have to be considered old and the next execution of the job it will be deleted. If the number the days is less than 0 all the messages will be deleted.

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

Information Console

Date	Type Message	Description
18/11/2016 13:38:17	Response: Sync Users	Created/Updated FAIL: 3, Deleted
18/11/2016 13:38:17	Request: Sync users	Users to Create/U
18/11/2016 13:38:09	Response: Error Groups	
18/11/2016 13:38:09	Request: Error Groups	Groups not define SwivelHelpDesk, SwivelToken,
18/11/2016 13:38:09	Response: Get Config	Groups: 6 Attribu
18/11/2016 13:38:09	Request: Get Config	
18/11/2016 13:35:04	Response: Get Config	Groups: 6 Attribu
18/11/2016 13:35:04	Request: Get Config	

Settings

Delete records older than:

E. g.:

Number of days 1 would mean the messages previous to the current day will be deleted.

Manage Configuration

The application allows download the current configuration or upload a configuration previously stored. This allows for configurations to be copied across multiple installations or for when an AD Agent is moved from one server to another. The configuration exported contains the following:

- Swivel Settings
- AD Settings
- Groups/Attributes
- Sync settings
- Information Console settings

Download configuration

To download/export the current configuration (no swivel settings) the user should click ?Download?.

The screenshot displays the Swivel Secure web application interface. On the left, a navigation menu lists several options: Swivel Settings, AD Settings, Groups/Attributes, Sync, RADIUS Server, NAS Entries, Information Console, and Manage Configuration. The 'Manage Configuration' option is highlighted. The main content area is titled 'Manage Configuration' and features a 'Configuration file:' label next to an empty text input field. Overlaid on the right side of the interface is a file dialog box titled 'Opening configuration.properties'. The dialog shows that the user has chosen to open a file named 'configuration.properties', which is a Text Document (944 bytes) from the URL 'http://192.168.11.115:8084'. The dialog asks 'What should Firefox do with this file?' and provides three options: 'Open with Notepad (default)', 'Save File' (which is selected), and 'Do this automatically for files like this from now on.' (which is unchecked). 'OK' and 'Cancel' buttons are visible at the bottom right of the dialog.

The contents of the configuration will look something like

```
apgroupobjclassname=groupOfNames
urlsrscserver=http\\://127.0.0.1\\:8081/adagent/adminxml
ldapssl=false
syncmaxuserspermessage=30
xmlencryptedkey=
schedulevalue=* * * * *
ldapuserobjclassname=inetOrgPerson
```

```
ldappassword=auuyhKPiTckfPIskDjAKS+
ldaplastmodifiedattributename=description
ldapselsigned=false
ldapbasedn=

GROUP.PINsafeAdministrators=
GROUP.PINsafeUsers=
GROUP.PNA=
ATTRIBUTE.familyname=
ATTRIBUTE.username=
ATTRIBUTE.phone=
ATTRIBUTE.altusername=
ATTRIBUTE.givenname=
ATTRIBUTE.email=
```

As we can see in the previous example, password is stored encrypted

Upload configuration

To upload a configuration file the user should click ?Browse? and selecting the configuration file previously downloaded

After that, the configuration file name is shown on the screen and then it should be clicked ?Upload? to load the file configuration. After clicking that button an information message will be shown.

Check Password

In the Swivel Settings screen there is a field to indicate the URL of AD Agent that is listening requests. This parameter is sent in the ?Get Config? message to the Core, and is saved as information of the Agent.

NOTE: if this value is changed directly in the Core when a synchronisation is done or a get config message is sent, it will be changed again with the value sent by AD Agent. That URL is used by the Core to check the password of the users created through this Agent ONLY if the Agent XML or RADIUS has been configured as ?Check password with repository?

Encryption

The messages exchanged between AD Agent and Core are XML messages. All those messages can be encrypted/decrypted if the encryption key is not empty. This encryption key can be defined in the AD Agent, on the Swivel Settings screen, and in the Core, in the correspondent Agent. Both systems have to have the same value. This value will be used as a key to encrypt/decrypt the messages.

NOTE: if there are 2 agents defined with the IP of AD Agent the encryption cannot be used. That is because if the message is encrypted the core only has the IP to identify the Agent so if there are more than one Agent on that IP they cannot be distinguished

?

RADIUS

Available since Version 1.2

The AD Agent can also act as a RADIUS server. (Currently PAP only) It can receive RADIUS requests from a VPN and forward the submitted credentials to the Swivel Core server for validation. The authentication requests will be sent to the same agent setting on the RADIUS core as used for account synchronisation, therefore any policies, eg Check Password With Repository, must be set as required on the core.

The RADIUS server is enabled and configured on the RADIUS screen.

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

RADIUS Server

Bind IP:

Auth Port:

1812

Auth Port:

1813

Enabled

You must specify the ports that the RADIUS server will bind to. You can also set an IP address. This setting is optional and if you leave this blank the RADIUS server will listen on all IP addresses.

If you change any of these settings the RADIUS server will be restarted.

NAS

In order to use the AD Agent to authenticate VPN users, you must enter the details of the VPN as a Network Access Server (NAS) on the AD Agent. You need to specify the IP address of the NAS and the shared secret.

- ▶ Swivel Settings
- ▶ AD Settings
- ▶ Groups/Attributes
- ▶ Sync
- ▶ RADIUS Server
- ▶ NAS Entries
- ▶ Information Console
- ▶ Manage Configuration

NAS Config

Add New NAS

Name	Host/IP	Secret
<input type="text"/>	<input type="text"/>	<input type="text"/>

Edit Existing NAS

Name	Host/IP	Secret
<input type="text" value="local"/>	<input type="text" value="127.0.0.1"/>	<input type="text" value="....."/>

If you specify a NAS by a hostname, the AD Agent must be able to resolve that hostname to a valid IP address. This means it must have access to DNS

Once a NAS has been added in can make RADIUS authentication requests to the AD Agent.

The AD Agent extracts the submitted credentials from the inbound RADIUS requests and passed them to the Swivel Core server for validation.

If the credentials are valid the SRSC returns a RADIUS Accept, if not a returns a RADIUS Reject