Swivel Remote Sync Client

Contents

Overview

The Swivel Secure AD Agent (AD Agent) allows data from a data source (e.g. Active Directory) to be pushed to a Swivel Server. The AD Agent can be used with a Swivel Secure instance deployed within the Cloud. Users are added to the appropriate repository and appear in the User Administration on AuthControl Sentry. The AD Agent runs under Tomcat and requires JAVA. The Windows installer contains all the required software elements and configures the software to run.

Prerequisites

AD Agent Installer.exe file from the Downloads page

Windows OS with Java or Swivel appliance

Swivel Configuration

Configuring the Server Agent

On the AuthControl Sentry Administration console configure the Server Agent, see Agents How to Guide. The following settings need to be configured:

Name

Hostname/IP of the AD Agent

Shared Secret: same value entered on AD Agent server

Can Act as Repository: Yes

URL Check Repository: https://IP_of_the_SRSC_server:8080/adagent/adminxml

Encryption/Deccryption key: same value entered on AD Agent server

Enabling Session creation with username

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

AD Agent Installation

Windows Installation

Download the AD Agent installer to where the AD Agent is to be run from, and run the installer.

AD Agent Settings

Run the AD Agent configuration program, and enter in the Cloud details supplied by Swivel.

AD Agent Administration security

The AD Agent Administration console can be protected by IP source. Edit the file .swivel/srsc/security.properties. After editing, Tomcat will need to be restarted, or on Windows quit and restart the console.

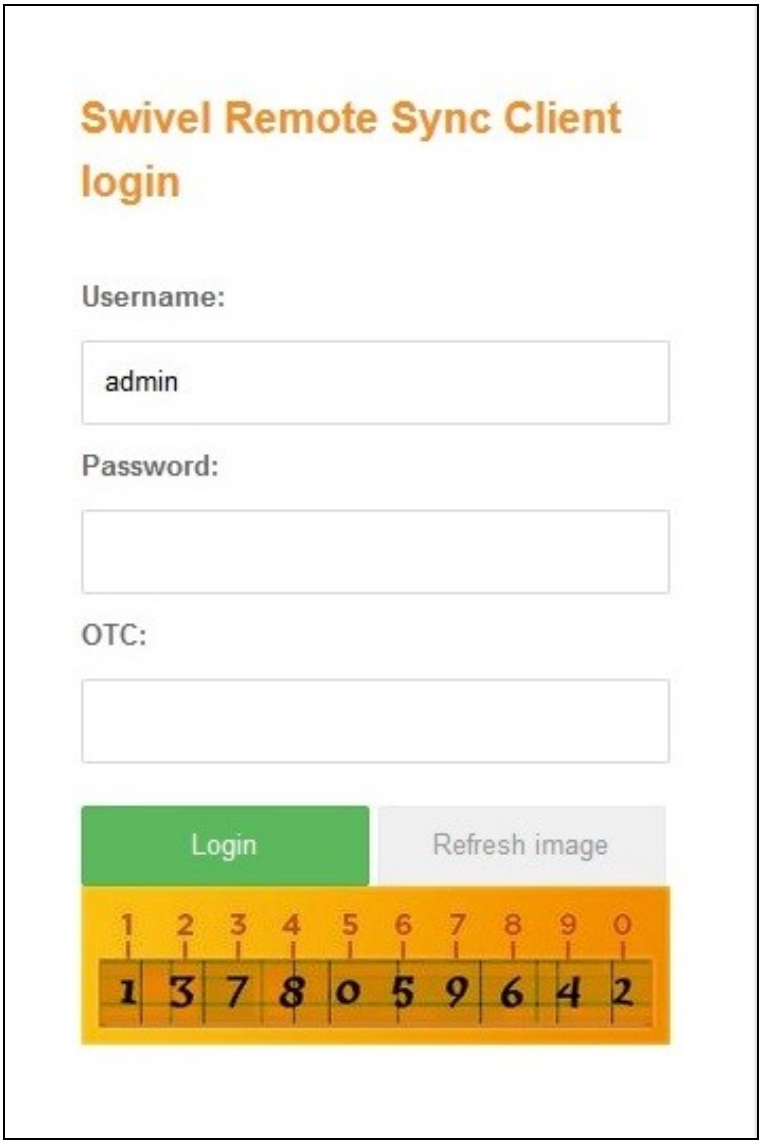
To allow access from any IP use 0.0.0.0/0

To specify a range of IP's or a specific IP specify the IP and netmask

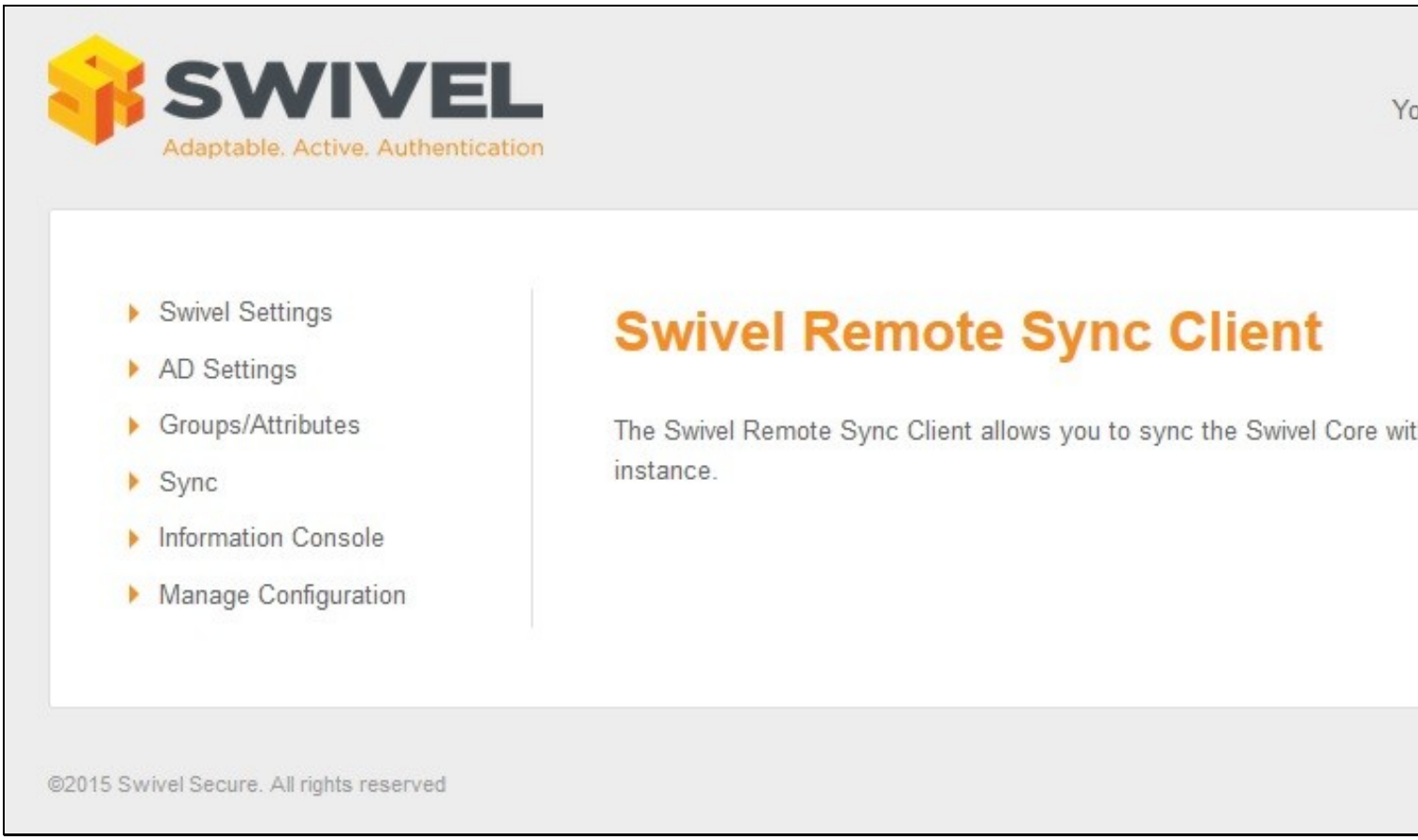
```
admin.iprange=192.168.11.0/24
core.iprange=192.168.11.115
```

AD Agent Login

In a web browser connect to http://local_server_ip:8080/adagent, a login screen should appear, allowing login from a Swivel Administrative user account.



A Successful login brings up the configuration options:



AD Agent Configuration - Swivel Settings

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.

URL check password: indicates the URL where the SRSC is listening for requests to check password

Note on Check Password

In the Swivel Settings screen there is a field to indicate the URL of SRSC 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?

AD Agent Configuration - AD Settings

Allows settings to configure ctive Directory data source

Server: IP/Hostname where the AD is running.

Port: Port where the AD is running.

Username: AD administrator username

Password: AD administrator 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 no 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 the good working is at the moment only covered for an AD.

- Swivel Settings
- AD Settings
- Groups/Attributes
- Sync
- Information Console
- Manage Configuration

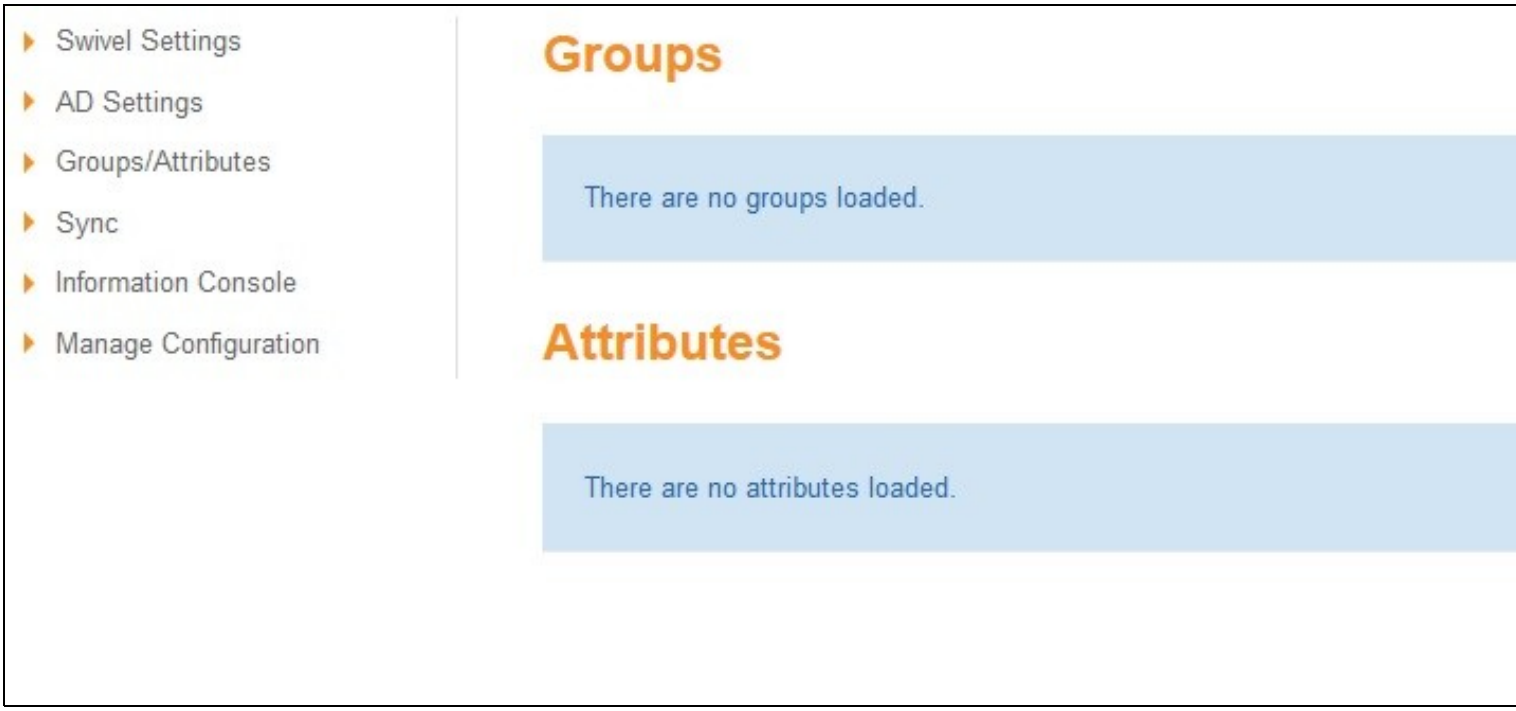
AD Settings

Server:	localhost
Port:	389
Username:	Administrator
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

S

AD Agent Configuration - Groups/Attributes

Get Config connects to the configured Swivel instance and loads the Groups and Attributes available.

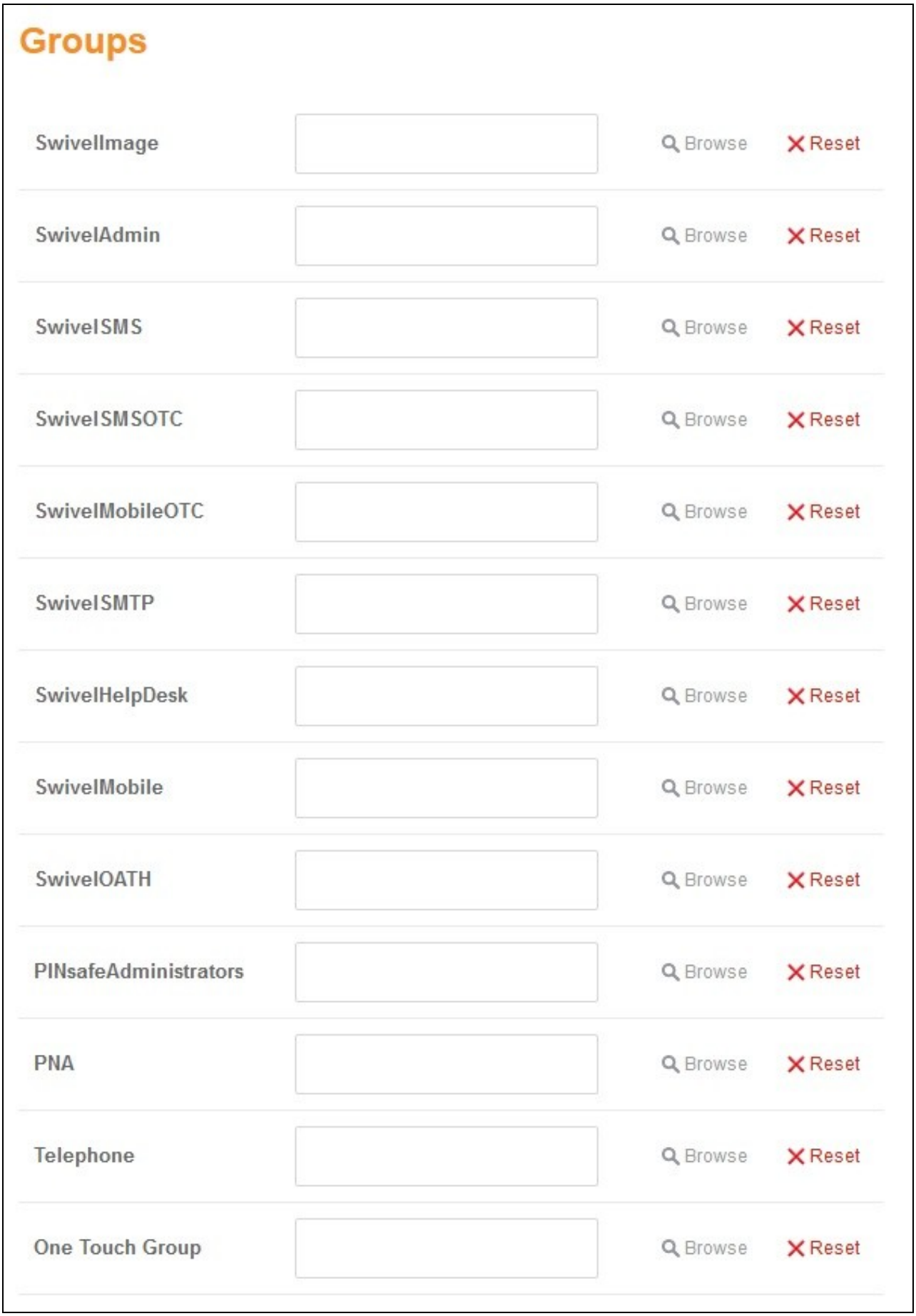


The **Browser** screen shows the current AD Path, the name of the group that the user wants to assign a value on and a list of Groups and Subcontainers of the current path. When an AD group is selected it is automatically assigned to the group.

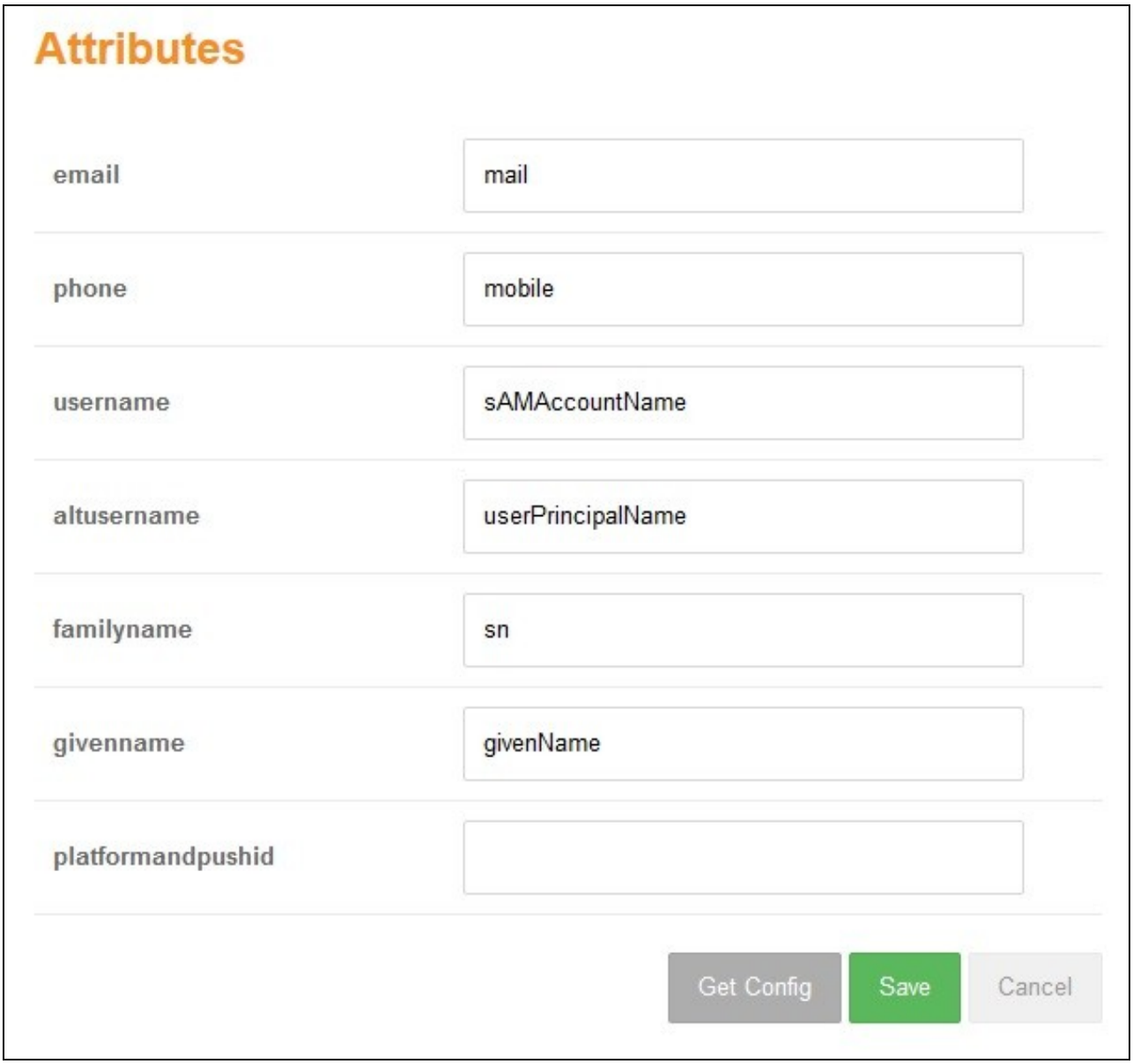
The second section on the Group/Attributes screen shows the attributes.

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

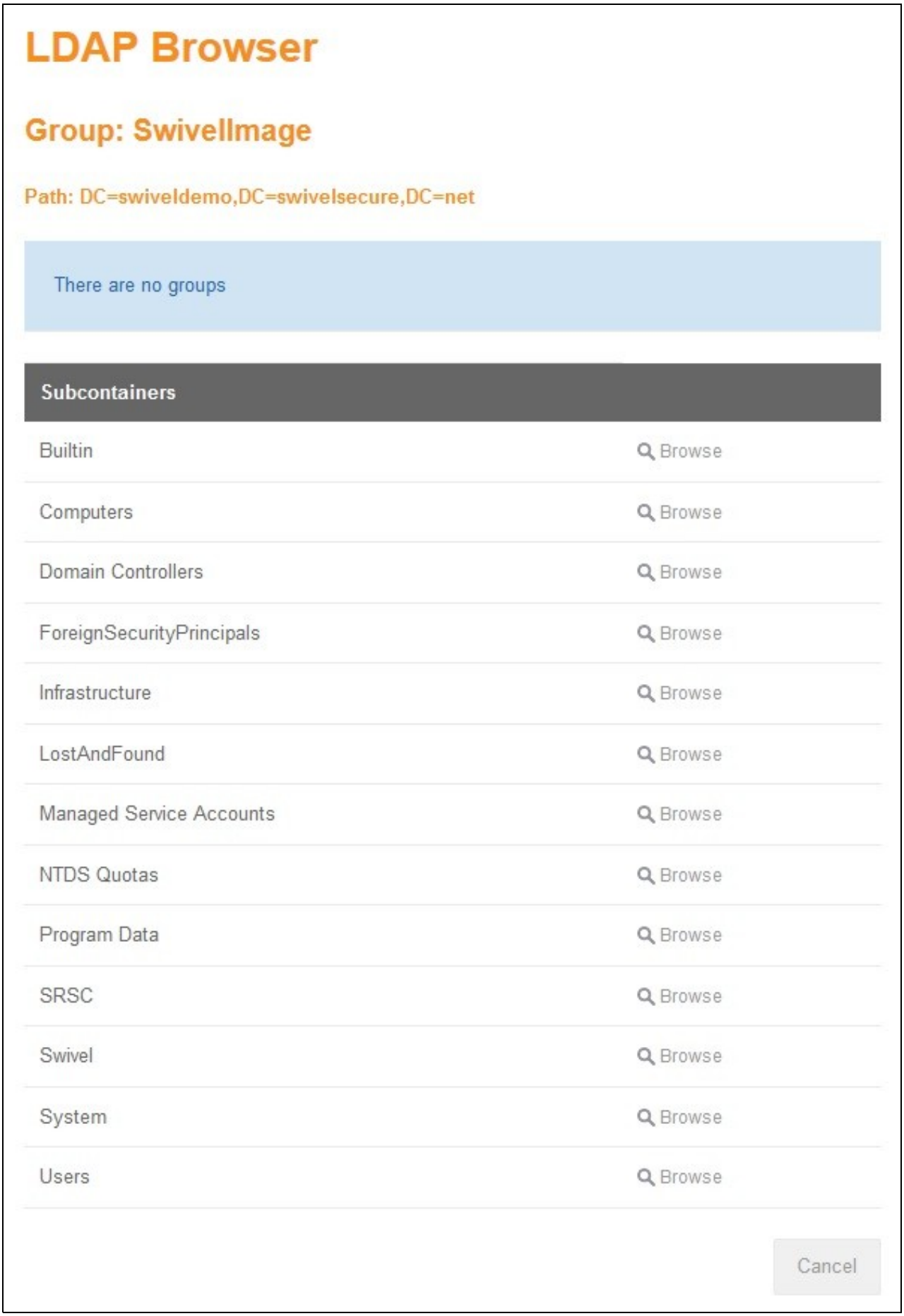
Browser Groups (imported from Swivel, values will depend n the Swivel setup)



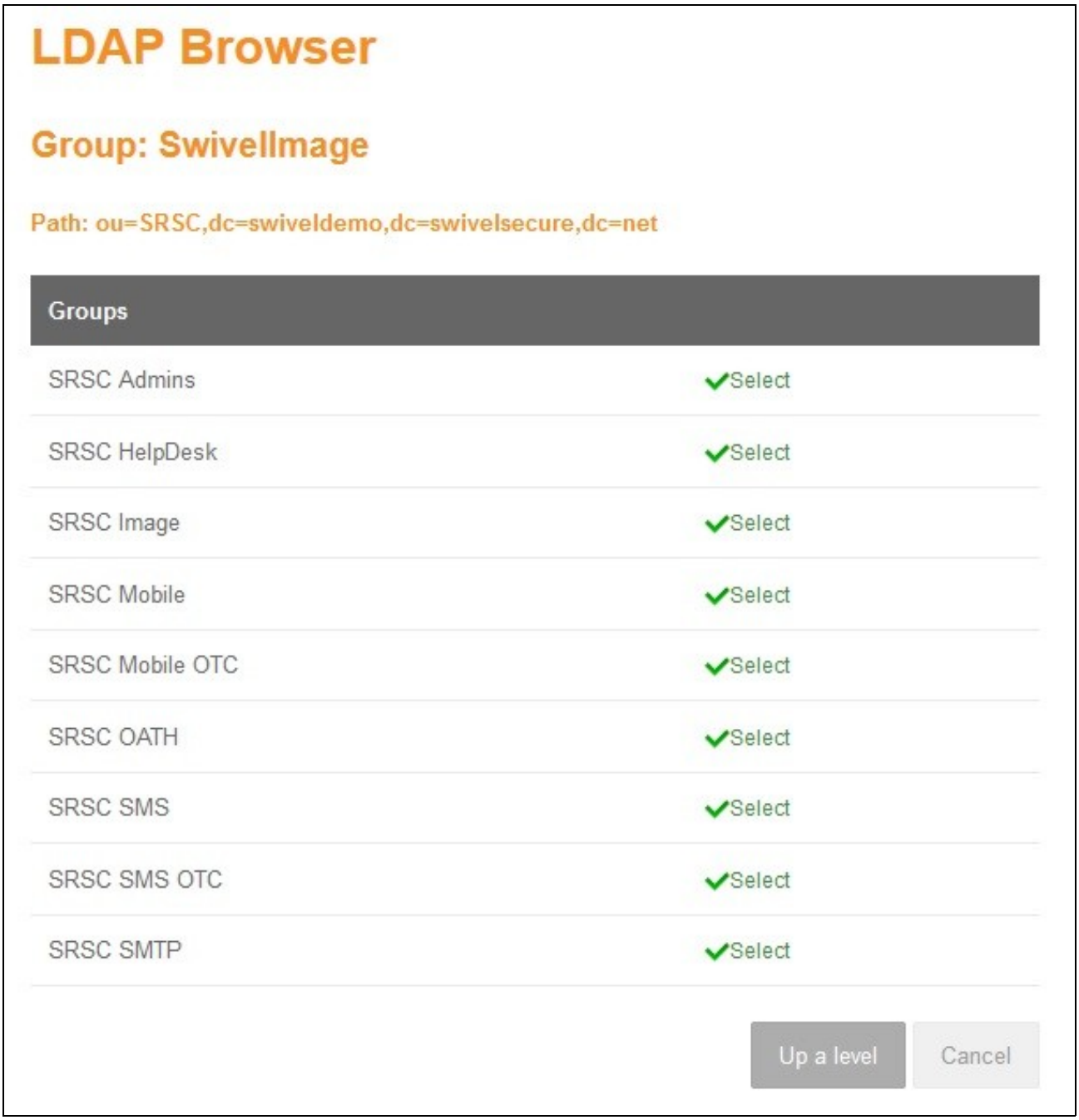
Browser Attributes (imported from Swivel, values will depend n the Swivel setup)



Browsing to the groups



Selecting the Groups



Selected Groups

Groups

SwivelImage	cn=SRSC Image,ou=SRSC,dc=	Browse	Reset
SwivelAdmin	cn=SRSC Admins,ou=SRSC,d	Browse	Reset
SwivelSMS		Browse	Reset
SwivelSMSOTC		Browse	Reset
SwivelMobileOTC		Browse	Reset
SwivelSMTP		Browse	Reset
SwivelHelpDesk	cn=SRSC HelpDesk,ou=SRSC	Browse	Reset
SwivelMobile		Browse	Reset
SwivelOATH		Browse	Reset
PINsafeAdministrators		Browse	Reset
PNA		Browse	Reset
Telephone		Browse	Reset
One Touch Group		Browse	Reset

AD Agent Configuration - Sync

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 not limit defined. Furthermore, the user can decide to do a Manual Sync clicking the corresponding button and/or define a scheduler for an automatic synchronisation. Also, there is a button to resync all the users.

The sync process involves the exchange of different types of messages as follows:

- AD Agent Request - Get Config / Response - Get Config (Groups and Attributes)

- AD Agent:

Groups not defined: Request - Error Groups / Response - Error Groups

All groups defined: No message

- AD Agent:

Get users members of the groups defined from AD

If there are users that have to be sync, the number of messages will depend of the maximum number of users per message

Request - Sync Users / Response - Sync Users

Update users last sync data if no error

No users to sync: no message sent

Information about the last synchronization (Manual or Scheduled) is shown. The information is as follows:

- Last sync date: date and time of last sync

- Type: Manual/Scheduled

- If there are groups not defined: Name of the groups not defined

- Created or updated users: number of OKs, number of FAILs

- Deleted users: number of OKs, number of FAILs

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

- Data of that user has been updated in the AD after last sync, e.g. whenChange > lastSyncTime

NOTE: clocks of AD server and the SRSC has to be synchronized.

- There has been a change in the groups/attributes screen after last sync so next sync all the users will be updated.

Scheduled sync

To define a scheduled sync, set 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?, in than moment a job of synchronization 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.

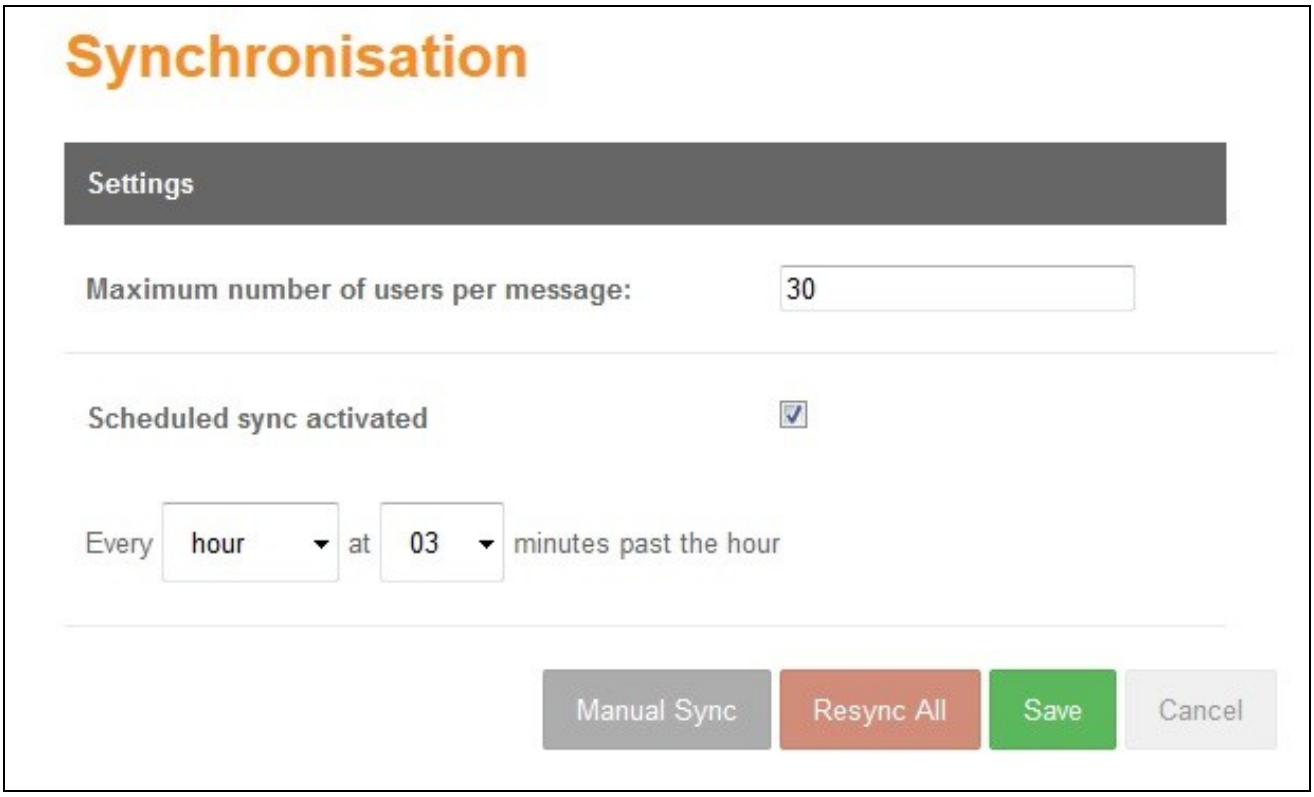
Manual Sync

When the user clicks ?Manual Sync? a confirmation dialog is shown, then if the user has accepted, a spinner overlap will be shown. That is useful to indicate to the user that the synchronization is working, mainly in synchronizations with a large amount of users that usually need more time and in addition, to avoid that the user clicks again Manual sync.

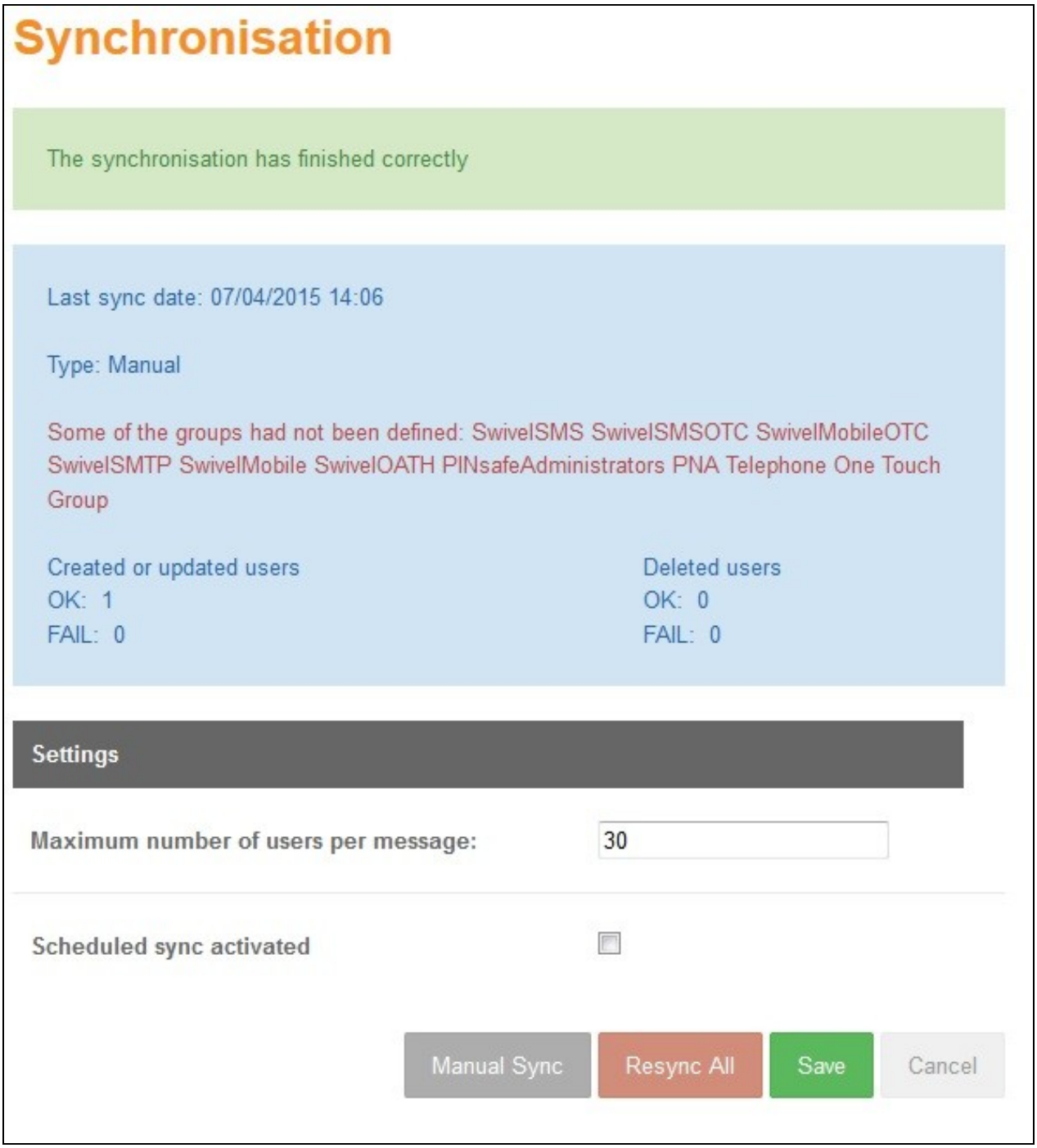
Resync All

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 resync all action has to be done to update the rights.


Synchronisation
Settings
Maximum number of users per message:
30
Scheduled sync activated
Every
hour
at
03
minutes past the hour
Manual Sync
Resync All
Save
Cancel

Manual Sync



AD Agent Configuration - Information Console

This shows the information about the messages exchanged between AuthControl Sentry and AD Agent. The messages can be deleted automatically using a schedule job that will be executed every day at 19:00. That configuration could be changed in the file distpatcher-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.

Example: Number of days 1 - the messages previous to the current day will be deleted.

AD Agent Configuration - Manage Configuration

The application allows download the current configuration or upload a configuration previously stored.

The configuration exported contains the following:

- Swivel Settings

- AD Settings

- Groups/Attributes

- Sync settings

- Information Console settings.

Testing

Known Issues

Troubleshooting

AD Agent:Message encrypted

Message seen on the Swivel Core Log Viewer for communication with the AD Agent.

Message decrypted

Message seen on the Swivel Core Log Viewer for communication with the AD Agent.

Searching encryption key for the IP: 192.168.12.110, agent name found: AD Agent

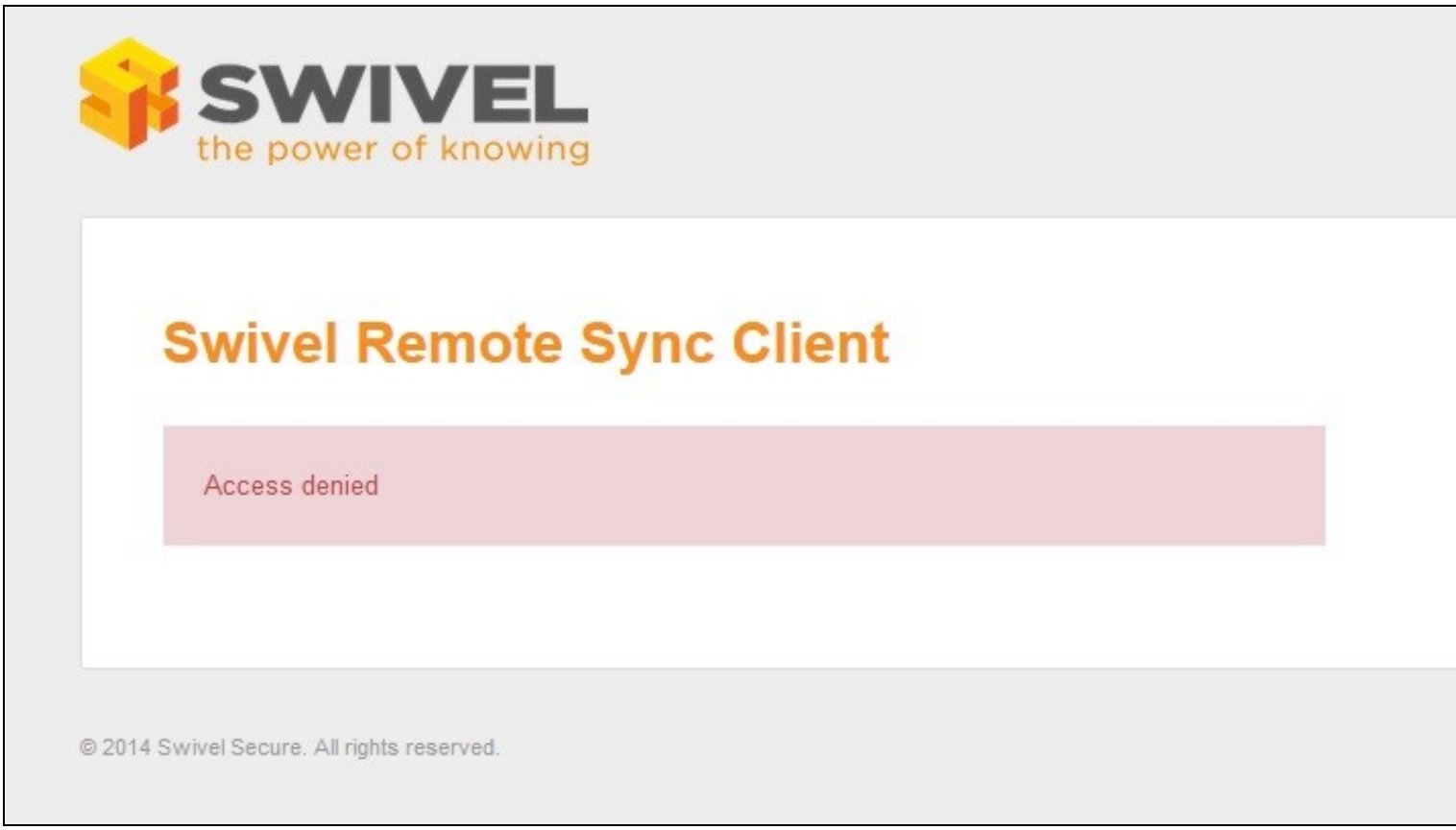
Message seen on the Swivel Core Log Viewer for communication with the AD Agent.

ERROR RestTemplateServiceImpl:72 - [MTD] sendPostMessage [MS G] Error: org.springframework.web.client.ResourceAccessException: I/O error on POST reques t for "https://192.168.12.111:8443/proxy/AdminXML": hostname in certificate didn't match: <192.168.12.111> != <*.swivelsecure.com>; nested exception is javax.net.ssl.SSLException: hostname in certificate didn't match: <192.168.12.111> != <*.swivelsecure.com>

Error seen in the AD Agent console for a certificate not matching the hostname. Select Self-Signed Certs.

ERROR ConfigurationController:81 - [MTD] getConfigRequest [MSG] Connection error

Error seen in the AD Agent console, unable to connect to the Swivel core.



Access Denied

If trying to access the login page goes straight to Access Denied, check the IP security filter addresses.

There was an error getting configuration In the AD Agent console

Response: Parse Error In the SRSC log

Check the AD data source configuration.

The '*Encrypted Key:* needs to be configured with the Swivel core to match that under Sever/Agents for the correspoding AD Agent.

ERROR EncryptionUtility:103 - [MTD] initCiphers [MSG] Error: javax.crypto.BadPaddingException: Given final block not properly padded in the AD Agent program console.

The '*Encrypted Key:* needs to be configured with the Swivel core to match that under Sever/Agents for the correspoding AD Agent.

AD Connection error in the AD Agent Administration console.

2015-04-07 12:57:18 ERROR ConfigurationController:148 - [MTD] ldapBrowser [MSG] Error: org.springframework.ldap.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903A9, comment: AcceptSecurityContext error, data 52e, v1db1]; nested exception is javax.naming.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903A9, comment: AcceptSecurityContext error, data 52e, v1db1] **in the SRSC program console.**

Use username@fqdn for the AD Settings