PUBLIC smof / RolesCreator

RolesCreator Quick Start Guide
v0.1 May 2013

Simon Moffatt

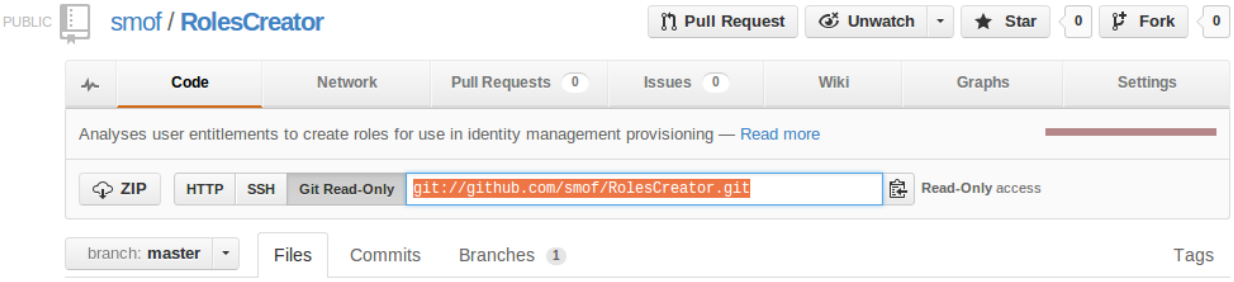
https://github.com/smof/RolesCreator

Table of Contents

1 – Download

Download the source or zip from Github into self contained directory.

If you have a github account simply “git clone git://github.com/smof/RolesCreator.git”. If not download the zip.



Analyses user entitlements to create roles for use in identity management provisioning — Read more

git://github.com/smof/RolesCreator.git

The main application module is located in rolescreator.rb, with supporting files in the lib/. The config.yml controls application parameters.

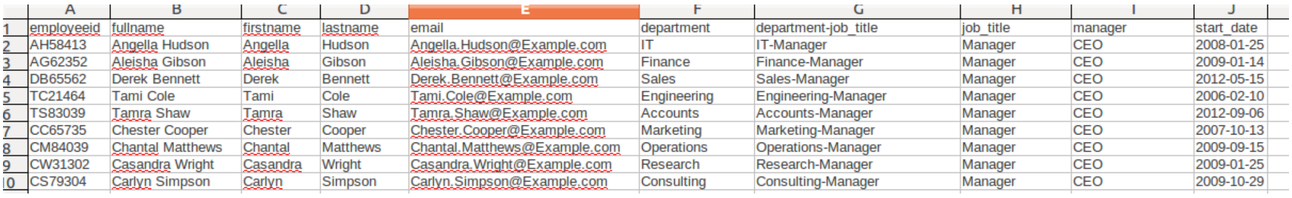
2 – Config

RolesCreator has an external Yaml configuration file. All parameters are accessed via this file, requiring zero changes to the source code.   The only changes to the source that may be required, are any changes to the logging verbosity. To change this, edit the logger.rb file in the lib/ directory.

3 – Use Case1 – Creating Roles

This will create a single output file, that contains a mapping between roles and identities. The location and format (XML, JSON, CSV) of this file is governed by the config.yml file.

Generate an authoritative source identities file that contains a list of users to analyse. This file needs to contain enough information in order to group the users. Eg. Functional mapping such as department, location, job-title etc. An example file is shown below:



	A	B	C	D	E	F	G	H	I	J
1	employeeid	fullname	firstname	lastname	email	department	department-job_title	job_title	manager	start_date
2	AH58413	Angella Hudson	Angella	Hudson	Angella.Hudson@Example.com	IT	IT-Manager	Manager	CEO	2008-01-25
3	AG62352	Aleisha Gibson	Aleisha	Gibson	Aleisha.Gibson@Example.com	Finance	Finance-Manager	Manager	CEO	2009-01-14
4	DB65562	Derek Bennett	Derek	Bennett	Derek.Bennett@Example.com	Sales	Sales-Manager	Manager	CEO	2012-05-15
5	TC21464	Tami Cole	Tami	Cole	Tami.Cole@Example.com	Engineering	Engineering-Manager	Manager	CEO	2006-02-10
6	TS83039	Tamra Shaw	Tamra	Shaw	Tamra.Shaw@Example.com	Accounts	Accounts-Manager	Manager	CEO	2012-09-06
7	CC65735	Chester Cooper	Chester	Cooper	Chester.Cooper@Example.com	Marketing	Marketing-Manager	Manager	CEO	2007-10-13
8	CM84039	Chantal Matthews	Chantal	Matthews	Chantal.Matthews@Example.com	Operations	Operations-Manager	Manager	CEO	2009-09-15
9	CW31302	Casandra Wright	Casandra	Wright	Casandra.Wright@Example.com	Research	Research-Manager	Manager	CEO	2009-01-25
10	CS79304	Carlyn Simpson	Carlyn	Simpson	Carlyn.Simpson@Example.com	Consulting	Consulting-Manager	Manager	CEO	2009-10-29

Edit the config.yml with the appropriate settings for your identities file. This will require field entries for the unique identifier and the functional mapping.

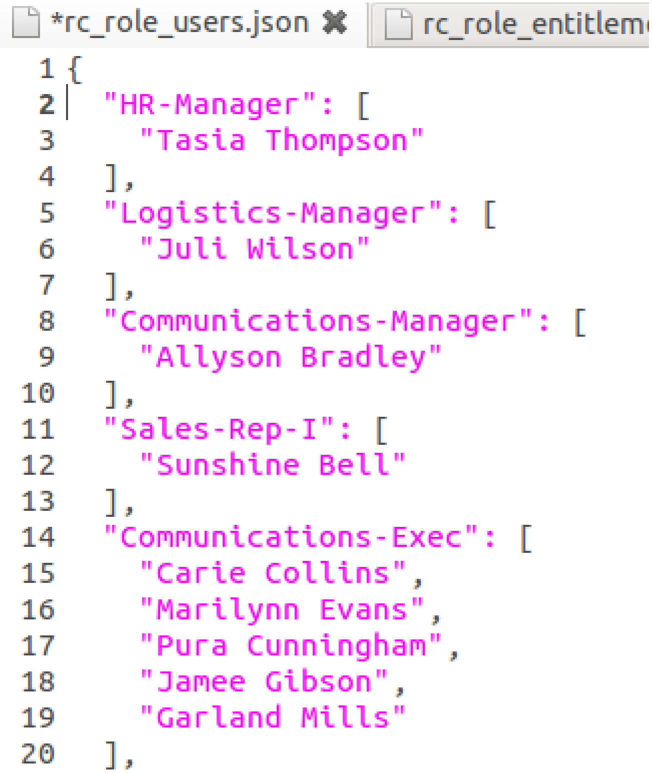
Config.yml settings:

create_role_users: true

input identities file location and format details

ouput role_users file location and format details

Running ./rolecreator.rb will result in a role:users output file in the format required:

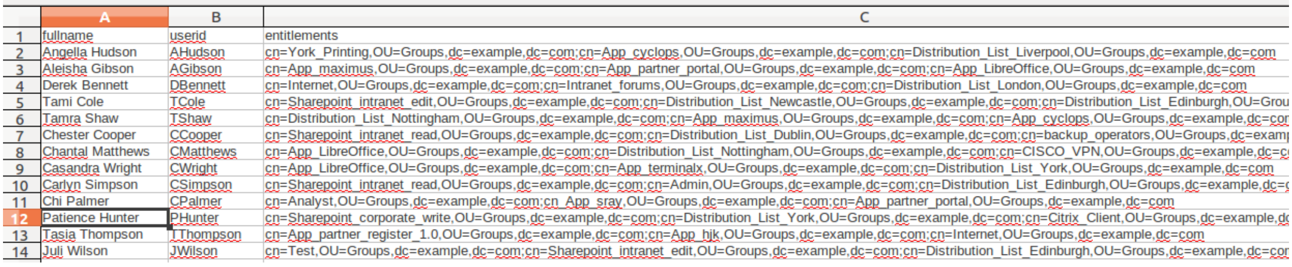


```
{
  "HR-Manager": [
    "Tasia Thompson"
  ],
  "Logistics-Manager": [
    "Juli Wilson"
  ],
  "Communications-Manager": [
    "Allyson Bradley"
  ],
  "Sales-Rep-I": [
    "Sunshine Bell"
  ],
  "Communications-Exec": [
    "Carie Collins",
    "Marilynn Evans",
    "Pura Cunningham",
    "Jamee Gibson",
    "Garland Mills"
  ],
```

4 – Use Case2 – Creating Role Entitlements

Adding entitlements to roles can either be done at the same time as use case 1 creating roles, or separately if roles have previously been created.

This requires a second input CSV file that contains the users and their respective entitlements form the target system. This file requires a unique identifier and multivalue separated list of their entitlements. One user per line. An example is below:



	A	B	C
1	fullname	userid	entitlements
2	Angella Hudson	AHudson	cn=York_Printing,OU=Groups,dc=example,dc=com;cn=App_cyclops,OU=Groups,dc=example,dc=com;cn=Distribution_List_Liverpool,OU=Groups,dc=example,dc=com
3	Aleisha Gibson	AGibson	cn=App_maximus,OU=Groups,dc=example,dc=com;cn=App_partner_portal,OU=Groups,dc=example,dc=com;cn=App_LibreOffice,OU=Groups,dc=example,dc=com
4	Derek Bennett	DBennett	cn=Internet,OU=Groups,dc=example,dc=com;cn=Intranet_forums,OU=Groups,dc=example,dc=com;cn=Distribution_List_London,OU=Groups,dc=example,dc=com
5	Tami Cole	TCole	cn=Sharepoint_intranet_edit,OU=Groups,dc=example,dc=com;cn=Distribution_List_Newcastle,OU=Groups,dc=example,dc=com;cn=Distribution_List_Edinburgh,OU=Grou
6	Tamra Shaw	TShaw	cn=Distribution_List_Nottingham,OU=Groups,dc=example,dc=com;cn=App_maximus,OU=Groups,dc=example,dc=com;cn=App_cyclops,OU=Groups,dc=example,dc=cor
7	Chester Cooper	CCooper	cn=Sharepoint_intranet_read,OU=Groups,dc=example,dc=com;cn=Distribution_List_Dublin,OU=Groups,dc=example,dc=com;cn=backup_operators,OU=Groups,dc=examp
8	Chantal Matthews	CMatthews	cn=App_LibreOffice,OU=Groups,dc=example,dc=com;cn=Distribution_List_Nottingham,OU=Groups,dc=example,dc=com;cn=CISCO_VPN,OU=Groups,dc=example,dc=c
9	Casandra Wright	CWright	cn=App_LibreOffice,OU=Groups,dc=example,dc=com;cn=App_terminalx,OU=Groups,dc=example,dc=com;cn=Distribution_List_York,OU=Groups,dc=example,dc=com
10	Carlyn Simpson	CSimpson	cn=Sharepoint_intranet_read,OU=Groups,dc=example,dc=com;cn=Admin,OU=Groups,dc=example,dc=com;cn=Distribution_List_Edinburgh,OU=Groups,dc=example,dc=
11	Chi Palmer	CPalmer	cn=Analyst,OU=Groups,dc=example,dc=com;cn_App_sray,OU=Groups,dc=example,dc=com;cn=App_partner_portal,OU=Groups,dc=example,dc=com
12	Patience Hunter	PHunter	cn=Sharepoint_corporate_write,OU=Groups,dc=example,dc=com;cn=Distribution_List_York,OU=Groups,dc=example,dc=com;cn=Citrix_Client,OU=Groups,dc=example,dc
13	Tasia Thompson	TThompson	cn=App_partner_register_1.0,OU=Groups,dc=example,dc=com;cn=App_hjk,OU=Groups,dc=example,dc=com;cn=Internet,OU=Groups,dc=example,dc=com
14	Juli Wilson	JWilson	cn=Test,OU=Groups,dc=example,dc=com;cn=Sharepoint_intranet_edit,OU=Groups,dc=example,dc=com;cn=Distribution_List_Edinburgh,OU=Groups,dc=example,dc=cor

The unique identifier must map directly to the unique identifier outlined in the identities or role user s file, as currently no regex correlation between systems and identifiers is enabled.

Config.yml settings

> create_role_entitlements: true
>
> input accounts location and format settings
>
> output role_entitlements format and location settings

Running ./rolecreator.rb will create another output file that contains a mapping between roles and the associated entitlements. These entitlements are the entitlements found across ALL users in the respective role.

Example:

The manager-role contains three users: John, Bob and Alice and their entitlements on the target system are:

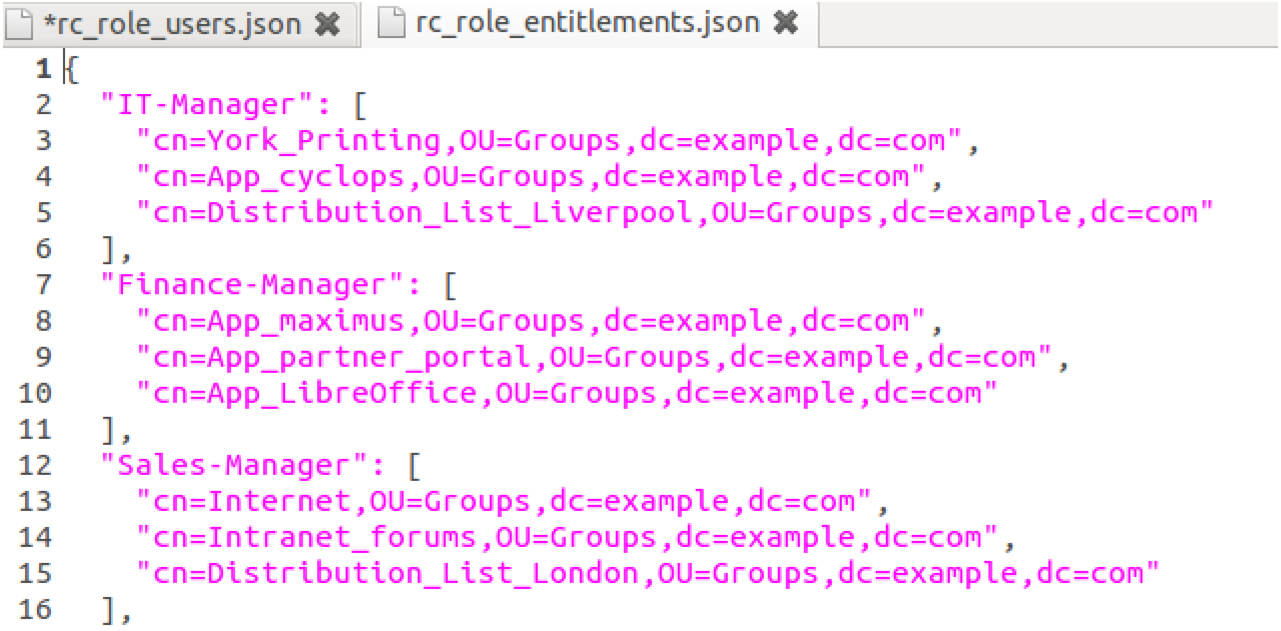
John – read, write, execute

Bob – read, write, full-control

Alice – read, write, create

The rolescreator will pull out only the entitlements that exist across ALL three users. This is akin to an array intersection ([] &[]). In this case the entitlements 'read' and 'write' will be added to the role. This is known as 'silent migration' as no entitlements are actually added or removed from the users. Simply grouped.

An example output file in JSON format would look like the following:



```
{
  "IT-Manager": [
    "cn=York_Printing,OU=Groups,dc=example,dc=com",
    "cn=App_cyclops,OU=Groups,dc=example,dc=com",
    "cn=Distribution_List_Liverpool,OU=Groups,dc=example,dc=com"
  ],
  "Finance-Manager": [
    "cn=App_maximus,OU=Groups,dc=example,dc=com",
    "cn=App_partner_portal,OU=Groups,dc=example,dc=com",
    "cn=App_LibreOffice,OU=Groups,dc=example,dc=com"
  ],
  "Sales-Manager": [
    "cn=Internet,OU=Groups,dc=example,dc=com",
    "cn=Intranet_forums,OU=Groups,dc=example,dc=com",
    "cn=Distribution_List_London,OU=Groups,dc=example,dc=com"
  ],
```

5 – Use Case3 – Identifying User Exceptions

User exceptions are any entitlements assigned to a user that are not assigned to a role. So in the example in Use Case 2 the following are exceptions:

Exist on target system:

John – read, write, execute

Bob – read, write, full-control

Alice – read, write, create

Added to manager-role:

manager-role: [read, write]

User exceptions (role – user):

John – execute

Bob – full-control

Alice – create

It is these exceptions that need to be checked by a compliance official to check if they are actually required by the individual user. The process to classify the entitlements as exceptions is based on the peer analysis assumption; that it's more efficient to analyse differences in peer behaviour than analyse the entire group individually.

Config.yml settings:

analyzer create_user_exceptions: true

output user_exceptions format and location settings

6 – Limits and Uses

Rolescreator is a standalone utility, not a full blown role mining engine. It is simple and robust. It has been tested with 100k identities on a Linux 64bit machine and ran in less than 10 seconds.

It can currently only analyse one application at a time. For multiple systems simply change the inputs and run again. Currently no regular expression mapping is available between identities and the system accounts, only direct mapping, so make sure extracts contain a unique identifier between the two.