With the implementation of the XPTR Cloud solution setting up security rules for
XPTR resources has changed. In the past, XPTR used RACF Dataset Rules to
control access to resources. With the Cloud solution, XPTR will use RACF
Resource Rules to control access to resources.

This document is intended for XPTR Administrators who will be controlling access
to their organizations XPTR resources.

All XPTR resource rules are contained in the RACF resource class CSRES.

There are important differences with the new Cloud security exit compared to the
old security exit:

1) In the access list for the RACF resource, do not use * READ rules to allow
any user to access the resource. Instead, use UACC(READ).

2) The new Cloud security exit loads a copy of all the CSRES resource rules
when the XPTR product comes up. Any changes to those rules must be
relayed to XPTR so it can reload the rules. DIT will automatically reload the
rules each morning. If an administrator needs to have the rules reloaded
outside of this window they can create a service request to the DIT
Mainframe team to have this done.

3) Since resource rules begin with #, instead of the department code, when an
administrator needs to create a new directory or report rule, they will need
to open a ticket to the DIT Mainframe team to create a skeleton rule with
their agency as the RACF owner. Once the skeleton rule is created the
agency will have the authority to manage the rule. Note that the skeleton
rule will have RACF group FSHXPTR granted access of ALTER. This is
necessary to allow the cloud logonid to synchronize report information
between the cloud and the mainframe.

4) If you want to create a new rule for a report or directory, e.g.
#.R$\ABC\CDE\FGHI, and there is a more generic resource rule that already
exists, say#.R$\ABC\CDE\*, the user will need to have access to both rules.
This is different than how the data set rule was processed in RACF with the
old security exit.

5) Note that Cloud security rules are delimited by a backward slash, \, instead
of a period as in a dataset name.

6) When creating a new rule only use access values of READ or ALTER. Do
not use UPDATE or CONTROL.

7) Under the old RACF data set rule format, users could audit all access
attempts to reports (using the RACF AUDIT(ALL) parameter) and run
standard RACF or Vanguard reports to print the results. The new security
exit determines access to reports internally, without calling RACF. All
access attempts to reports are now logged in a new Systemware SMF record.
Therefore, you no longer need to code AUDIT(ALL) in the rule itself. This means RACF and Vanguard reports will no longer show report access and violations. Contact the DIT Mainframe team to set up a batch job to create these reports now.

Administrators will need the following rules set up in resource class CSRES:

(1) For updating the User Profiles within XPTR:

ALTER access for: #.U$\dept\USR\*

Where:  
department code = three character department code  
USR = the literal value, ‘USR’  
# = the literal value, "#"  
U$ = the literal value, "U$"

Note: Remember to add READ access for the directory, too.

READ access for: #.D$\dept\USR\*

(2) For defining and updating report definitions and their break rules and indexing functions:

ALTER access for: #.R$\dept\bill\*

Where:  
department code = valid 3 character dept code  
bill code = valid 3 character bill code  
# = the literal value, "#"  
R$ = the literal value, "R$"

NOTE: Report definitions can be defined to the form level if necessary

ALTER access for: #.R$\dept\bill\form

However, do not extend the rule beyond the form id  
(e.g. #.R$\dept\bill\form\*)
(3) For viewing and deleting report versions:

```
ALTER access for: #.RV\dept code\bill code\*
```

Where:
- dept code = valid 3 character dept code
- bill code = valid 3 character bill code
- # = the literal value, "#"
- RV = the literal value, "RV"

**NOTE:** Reports can be defined to the form level if necessary

```
ALTER access for: #.RV\dept code\bill code\form id
```

However, do not extend the rule beyond the form id
(e.g. #.RV\dept code\bill code\form id\*)

(4) For defining directories:

```
ALTER access for: #.D$\dept code\bill code\*
```

Where:
- dept code = valid 3 character dept code
- # = the literal value, "#"
- D$ = the literal value, "D$"

(5) For defining sub-directories:

```
ALTER access for: #.D$\dept code\bill code\*
```

Where:
- dept code = valid 3 character dept code
- bill code = valid 3 character bill code
- # = the literal value, "#"
- D$ = the literal value, "D$"

(6) For report distribution and bundling:

```
ALTER access for: #.B$\dept code\bill code\*
```

Where:
- dept code = valid 3 character dept code
- bill code = valid 3 character bill code
- # = the literal value, "#"
- B$ = the literal value, "B$"
Users will need the following RACF rules set up in resource class CSRES:

(1) For viewing report versions:

READ access for: #.RV\dept\bill\*  

Where:  
\begin{align*}  
department code & = \text{valid 3 character dept code} 
\text{bill code} & = \text{valid 3 character bill code} 
# & = \text{the literal value, "#"} 
RV & = \text{the literal value, "RV"} 
\end{align*}

Note: Reports can be secured down to the form ID level. The format is:

READ access for: #.RV\dept\bill\form id

(2) For viewing directories:

READ access for: #.D$\dept\bill\*  

Where:  
\begin{align*}  
department code & = \text{valid 3 character dept code} 
\text{bill code} & = \text{valid 3 character bill code} 
# & = \text{the literal value, "#"} 
D$ & = \text{the literal value, "D$"} 
\end{align*}

READ access for: #.D$\dept*

Where:  
\begin{align*}  
department code & = \text{valid 3 character dept code} 
# & = \text{the literal value, "#"} 
D$ & = \text{the literal value, "D$"} 
\end{align*}

(3) For viewing report definitions and the report versions underneath:

READ access for: #.R$\dept\bill\*  

Where:  
\begin{align*}  
department code & = \text{valid 3 character dept code} 
\text{bill code} & = \text{valid 3 character bill code} 
# & = \text{the literal value, "#"} 
R$ & = \text{the literal value, "R$"} 
\end{align*}

Note: Reports can be secured down to the form ID level. The format is:

READ access for: #.R$\dept\bill\form id
For additional information in using RACF to secure X/PTR resources, please see the Common Security System chapter in the Content Server z/OS, JHS Security guide on the web site: http://www.state.nc.us/sysware.

Here are some example TSO commands (you can also run these commands in batch) to manipulate RACF resource rules.

1) To list the resource rule, access list, and audit settings

   RLIST CSRES ".R$dept code\bill code\* ALL

   *NOTE: If you issue this command in TSO it will be displayed as ".R$:dept code:bill code:*", with : replacing the \, which is a restriction of TSO.

2) To list all report rules for a specific department code

   SR CLASS(CSRES) MASK(#.R$dept code)

3) To give a RACF user or group read access to a resource

   PERMIT ".R$dept code\* CLASS(CSRES) ID(group) ACCESS(READ)

   To remove a RACF user or group from a resource

   PERMIT ".R$dept code\* CLASS(CSRES) ID(group) DELETE

4) To change the universal access value

   RALTER CSRES ".R$dept code\* UACC(READ)