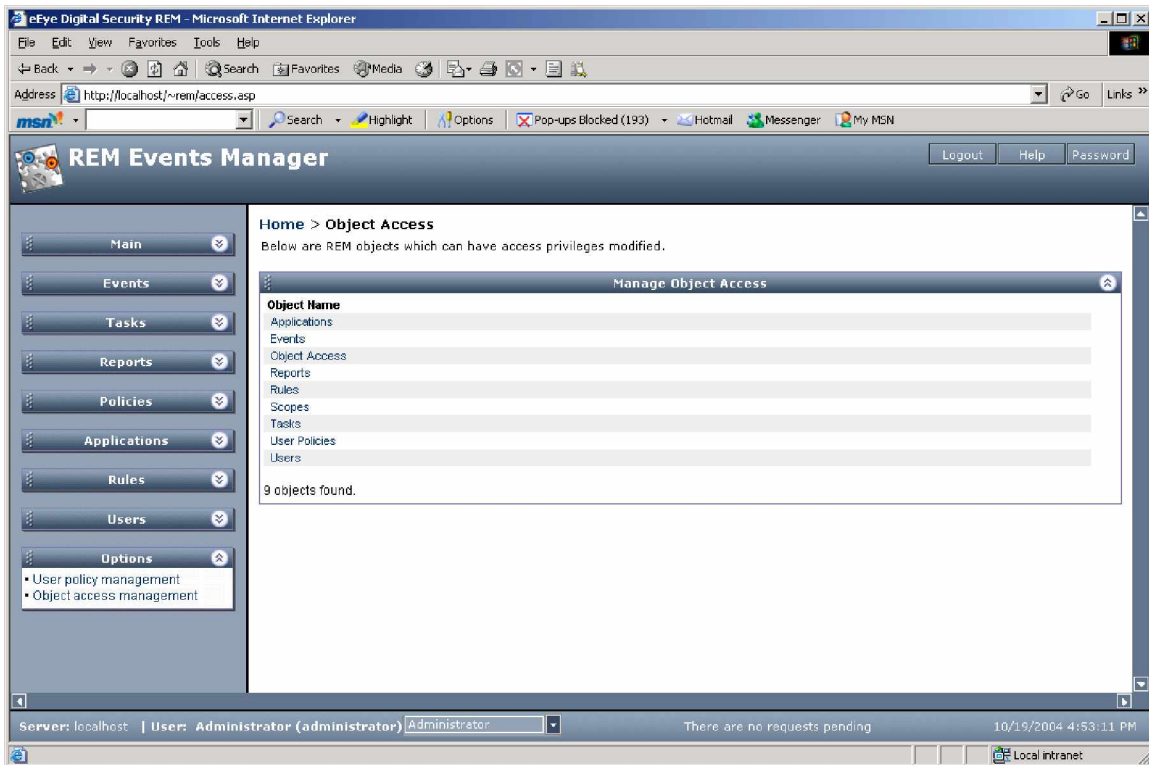


Enabling Policy Sub-Menu Access Control in REM

REM provides customers with the ability to restrict access to certain parts of the application. Managing user access is accomplished through the **Object access management** function located under the **options** menu.

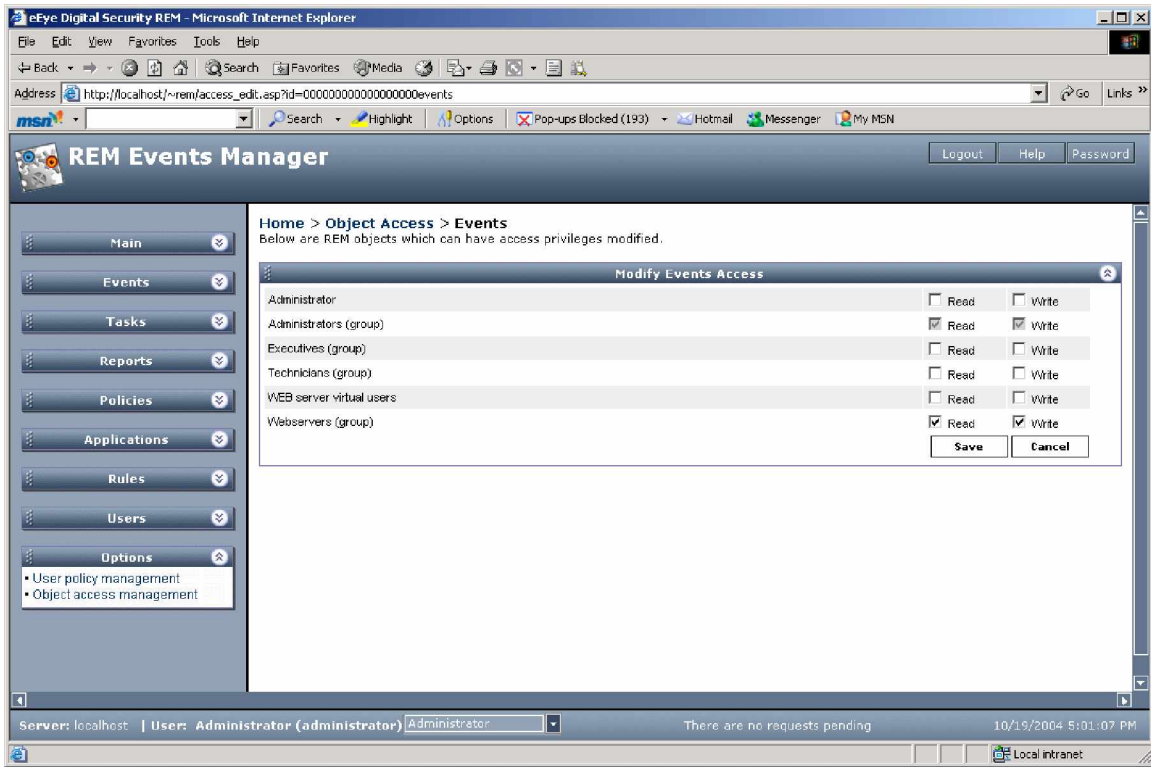
REM is divided into sections. A list of all access-controllable sections is provided within the **Object access management** function.

Architectural Overview



When following the link for any of the controllable sections a list with all the users and user groups defined within REM is displayed:

List of REM users and user groups with ‘r’ and ‘w’ check



For each user or user group a check box is displayed to enable “read” or “write” access to this particular object.

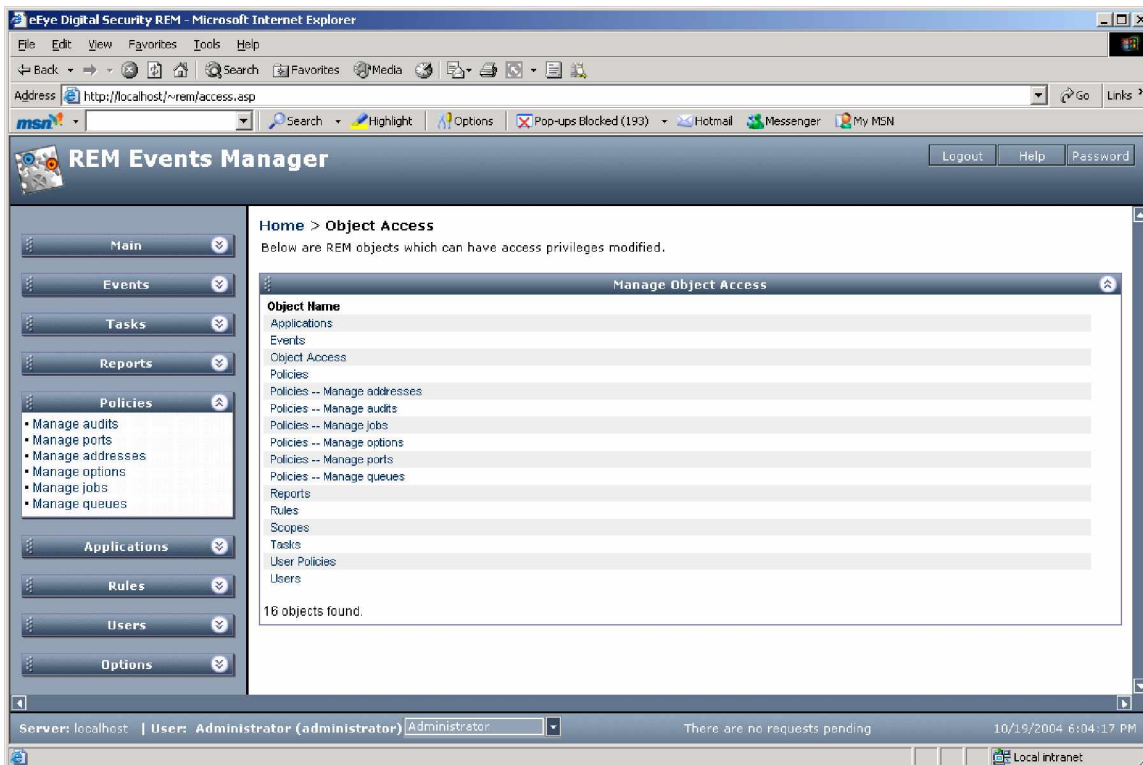
When a user logs into REM his/her access to any of the controllable sections is determined by the sum of the user’s set access with that of all the user groups this user belongs to. If access is not available the entire section will not be displayed.

The list of controllable sections includes all high level menu items on the left side of the application.

Enhancement

Following the changes performed below, REM will now be able to control access to Policy sub menus items as well.

Policy sub menus are now controllable



This enhancement is a response to a request that came from several customers that wanted to segregate the responsibilities of running scans via REM to different individuals. For example, some should be able to define the scan components (address groups, port groups while others can schedule jobs but not change the scan elements.

Steps that need to be taken

The enhancement was designed in a way so that REM will behave exactly the same as it did for users who do not wish to take advantage of the new enhancement. However for REM to be able to manage access control to the Policy sub menu items the REM administrator needs to perform the following:

1. REM Events Manager (EM) needs to be at version 2.0.33 or above. The upgrade will replace several files that control the REM security features. REM's access control behavior will not change following this step
2. In the REM Events manager's home directory locate the `config.xml` file. Back it up, open it for edit and perform the following changes:

Locate the following section:

```
<object id="0000000000000000policies" serial="0">  
  <name>Policies</name>  
  <permissions>  
    <permission access="rw" type="group">0000000000000000Administrators</permission>  
  </permissions>  
</object>
```

Note: you may find additional lines of permission access for other users or user groups that have been previously given access to the "policy" object. Include these lines in the section you will replace in the following step)

Replace with the following section:

```
<object id="0000000000000000policies2" serial="0">  
  <name>Policies</name>  
  <permissions>  
    <permission access="rw" type="group">0000000000000000Administrators</permission>  
  </permissions>  
</object>  
<object id="0000000000000000P_audits" serial="0">  
  <name>Policies -- Manage audits</name>  
  <permissions>  
    <permission access="rw" type="group">0000000000000000Administrators</permission>  
  </permissions>  
</object>  
<object id="0000000000000000P_ports" serial="0">  
  <name>Policies -- Manage ports</name>  
  <permissions>  
    <permission access="rw" type="group">0000000000000000Administrators</permission>  
  </permissions>  
</object>  
<object id="0000000000000000P_addresses" serial="0">  
  <name>Policies -- Manage addresses</name>  
  <permissions>  
    <permission access="rw" type="group">0000000000000000Administrators</permission>  
  </permissions>  
</object>
```

```
<object id="000000000000000000P_options" serial="0">
  <name>Policies -- Manage options</name>
  <permissions>
    <permission access="rw" type="group">000000000000000000Administrators</permission>
  </permissions>
</object>
<object id="000000000000000000P_jobs" serial="0">
  <name>Policies -- Manage jobs</name>
  <permissions>
    <permission access="rw" type="group">000000000000000000Administrators</permission>
  </permissions>
</object>
<object id="000000000000000000P_queues" serial="0">
  <name>Policies -- Manage queues</name>
  <permissions>
    <permission access="rw" type="group">000000000000000000Administrators</permission>
  </permissions>
</object>
```

3. Go to the "Object access management" section under the "Options" menu. Configure your users according to your policy with access to the appropriate Policy sub menu items. Note that it is required to set each user with access to the Policy top level if any of the sub menu access is enabled.

Note: If you do not achieve the desired change replace the config.xml file with the saved copy. This will return REM to its pre-enhancement behavior. Contact technical support for additional assistance.
