ESET Tech Center

Create a branch office structure in ESET Security Management Center 7.x

Anish | ESET Nederland - 2018-09-14 - Reacties (0) - ESET Security Management Center

Issue

- You have multiple high and low level ESET Security Management Center administrators that require varying levels of accesss. In this example, certain objects are made available to all administrators, while other objects are only accessible to high-level administrators.

Details

Solution

In this example, the following conditions exist:

- Two top-level administrators, *Admin1* and *Admin2* (with home group ALL)
- Two branch offices, *Tokyo Office* and *Sydney Office*
- Two local admins in each local office, *Tokyo_Admin_1* and *Tokyo_Admin_2*)
- Shared objects (policies) for admins on all levels
- Objects (policies) accessible only by top-level administrators
- Shared objects (client tasks) in the branch
- Objects accessible only by a single local admin and the Administrator
- Licenses distributed by top-level admins to each branch admin
- Shared installers among all admins

The Administrator must determine the branch structure that best suits the organization. This example shows how to build the following structure:

Figure 1-1

The tree structure in Figure 1-1 depicts the arrangement of static groups for this example. Complete each section to setup the structure.

1. Create static groups
2. Create permission sets
3. Create users
4. Distribute licenses
5. Create a shared policy
6. Create policies shared among top-level administrators
7. Create client task shared in the branch

8. Create a policy accessible only to a single branch administrator
9. Create installers shared among all level admins

Create static groups

1. Click **More → Groups**.

2. Click the gear icon next to the **All** group and select **New Static Group**.

Figure 2-1
Click the image to view larger in new window

1. Type the name of the static group in the **Name** field, optionally you can also type a description. For this example we use the name *Tokyo Office*.

2. Click **Finish** to create the group.

Figure 2-2
Click the image to view larger in new window

Repeat steps 1-4 for all static groups needed for your structure. This example will use the static group model shown in Figure 1-1.

Create permission sets

Each user must be assigned at least one permission set. In this example, we must create eight unique permission sets. "_PS", for "permission set" is appended to the name of each set. Figure 3-1 below illustrates permission assignments in this example.

Figure 3-1
Click the image to view larger in new window

A. Permissions for top-level administrators

To provide administrator access for *Admin1* and *Admin2* we have to create a permission set, follow these steps to do so:

1. Click **More → Permission Sets**.

2. Click **Permission Sets → New**.

Figure 3-2
Click the image to view larger in new window

1. Type the name of the permission set, optionally you can also type a description.

Figure 3-3
Click the image to view larger in new window

1. Click **Static Groups → Add static group(s)**.
   

   Figure 3-4
   Click the image to view larger in new window

2. Select a static group for this permission set. In this example, we will assign the *Admin_ps* permission set to the **All** group. Click **OK**.

Figure 3-5
Click the image to view larger in new window

1. Click **Functionality → Grant All Functionality Full Access** to give full access to users assigned this permission set. To assign a more specific set of permissions, select the corresponding check box for a given usage level to include it in this permissions set.

2. Click **Finish** to save the current permission set.

Figure 3-6
Click the image to view larger in new window

B. Permissions for branch level administrators

To create permission sets for branch level administrators, repeat steps from chapter **A.** using the following parameters:

Name	*Tokyo_ps*
Description	*Permission set for Tokyo branch administrators*
Static Groups	*Tokyo Office*
Functionality	Click **Grant All** and remove **Server Settings** (both **Read** and **Write**)

And another one for the other branch level administrator:

Name	*Sydney_ps*
Description	*Permission set for Sydney branch administrators*
Static Groups	*Sydney Office*
Functionality	Click **Grant All** and remove **Server Settings** (both **Read** and **Write**)

C. Permissions for home groups

To create permission sets for each branch level administrator's home group, repeat the steps from the chapter **A.** using the following parameters:

Name	*Tokyo_1_home_ps*
Description	*Permission set for Tokyo_Admin1*
Static Groups	*Tokyo_Admin_1*
Functionality	Click **Grant All** and remove **Server Settings** (both **Read** and **Write**)

Name	*Tokyo_2_home_ps*
Description	*Permission set for Tokyo_Admin2*
Static Groups	*Tokyo_Admin_2*
Functionality	Click **Grant All** and remove **Server Settings** (both **Read** and **Write**)

Name	*Sydney_1_home_ps*
Description	Permission set for *Sydney_Admin1*
Static Groups	*Sydney_Admin_1*
Functionality	Click **Grant All** and remove **Server Settings** (both **Read** and **Write**)

Name	*Sydney_2_home_ps*
Description	*Permission set for Sydney_Admin2*
Static Groups	*Sydney_Admin_2*
Functionality	Click **Grant All** and remove **Server Settings** (both **Read** and **Write**)

D. Permissions for sharing objects

To create permission sets for sharing objects, repeat the steps from the chapter **A.** using

the following parameters:

Name	*Shared_ps*
Description	*Permission set for shared objects*
Static Groups	*Shared objects*
Functionality	Click **Grant All** and remove **Server Settings** (both **Read** and **Write**)

After successfully creating all permission sets your permission sets list will look like this:

Figure 3-7

Create users

Log in as an Administrator and follow these steps to create the desired users:

1. Click **More** → **Users** → **New**.

Figure 4-1
Click the image to view larger in new window

1. Type the username *Admin1* in the **User** field, optionally you can add a description. Click **Select**.

   

   Figure 4-2
   Click the image to view larger in new window

2. Select the **All** group as the home group for this user and then click **OK**.

Figure 4-3
Click the image to view larger in new window

1. Type a secure password into the **Password** field and confirm it in the field below. You have the option to define additional settings for this account if you desire.

Figure 4-4
Click the image to view larger in new window

1. Click **Permission Sets.** In the left menu select the permission set that will be assigned to this user (*Admin_ps* in this case). Click **Finish** to save the user.

Figure 4-5
Click the image to view larger in new window

1. Now when the first user is created, continue with other users. The procedure is the same, just the parameters of users are the following:

Name	*Admin2*
Description	*Top level administrator 2*
Home Group	*All*
Permission sets	*Admin_ps*

Name	*Tokyo_Admin1*
Description	*Tokyo office administrator 1*
Home Group	*Tokyo_Admin_1*
Permission sets	*Tokyo_ps, Shared_ps, Tokyo_1_home_ps*

Name	*Tokyo_Admin2*
Description	*Tokyo office administrator 2*
Home Group	*Tokyo_Admin_2*
Permission sets	*Tokyo_ps, Shared_ps, Tokyo_2_home_ps*

Name	*Sydney_Admin1*
Description	*Sydney office administrator 1*
Home Group	*Sydney_Admin_1*
Permission sets	*Sydney_ps, Shared_ps, Sydney_1_home_ps*

Name	*Sydney_Admin2*
Description	*Sydney office administrator 2*
Home Group	*Sydney_Admin_2*

Permission sets	*Sydney_ps, Shared_ps, Sydney_2_home_ps*

Distribute licenses

You can only import licenses to users with the home group **All**. In this example, the *Admin1* and *Admin2* users have the **All** home group, so you can import licenses to them and they can distribute licenses to other users. Follow the steps below to import a licenses to these users and then assign licenses to other users.

1. Click **More** → **License Management**.

2. Click **Add Licenses**.

Figure 5-1
Click the image to view larger in new window

1. Enter your license key or select one of the following:

- **ESET Business Account**
- **Offline License File**

1. Click **Add Licenses** to finish the process and save the license.

Figure 5-2

1. After the license is successfuly saved, a confirmation notice will be displayed:

Figure 5-3

1. In the License Management menu click the gear icon  next to the newly added license key, click **Access Group** in the menu.

2. Click **Move** in the side menu.

Figure 5-4
Click the image to view larger in new window

1. Select the group where the license will be moved. (In this case, the home group of *Sydney_Admin1*). Click **OK**to move the license.

Figure 5-5

Click the image to view larger in new window

1. A notification will be displayed notifying you that the license was moved.

2. Now the license is available only to top-level administrators (with home group *All*) and to the user whose home group was selected in the step 8.

Follow these steps to import and move licenses within different access groups.

Create a shared policy

When a policy is created it is automatically contained in the home group of the user who created it. You can move existing policies to other groups where your user has **Write** permissions (for **Policies**).

In this example we create a policy for Windows Endpoints and we move it to *Shared group*, weher all users can use it for their computers.

1. Log in as an administrator (*Admin1* or *Admin2*).

2. Click **Policies** → **New Policy**.

Figure 6-1
Click the image to view larger in new window

1. Type the name and description for the policy in the appropriate fields in the **Basic** section.

2. Click the **Settings** section.

3. Select the appropriate product from the drop-down menu. Set up the policy according to your needs.

4. Click **Finish** to save the policy.

Figure 6-2
Click the image to view larger in new window

1. The policy can now be moved to other access groups where it will be available for other users. In this example we will move it to the *Shared group*.

2. Expand **Custom Policies** in the policies menu and find the policy you created earlier.

3. Click the gear icon next to it and select **Access Group → Move**.

Figure 6-3
Click the image to view larger in new window

1. Select the destination group (*Shared group*) and click **OK**.

The policy will be moved to the shared group and all users with the appropriate permissions set (*Shared_ps*) will be able to use it on computers/devices.

Create policies shared among top-level administrators

To create a policy which will only be available only to top-level administrators, Create a policy in the group **All** to make it available only to top-level administrators (other users in our setup do not have access to the group **All**).

Create client task shared in the branch

Create a client task that will be shared in the Tokyo office branch. It will be accessible to Tokyo administrators and top-level administrators.

1. Log in as *Tokyo_Admin1* (administrator of desired branch).
2. Navigate to **Client Tasks → New**.
3. Type in the name and description of the task.
4. Select the **Task Category** and **Task** (according to your needs).
5. Click **Settings** and set up the task.
6. Review the task in the **Summary** section and click **Finish** to save the task.
7. When asked if you want to add a trigger now, click **Close**.

   Figure 7-1
8. The task will automatically be created in the home group of current user (*Tokyo_Admin1* has the home group *Tokyo_Admin_1*). To make the task shared in the branch, move it to the shared static group, *Shared group,* in this example. Click the new task in the **All Tasks** menu and click **Access Group → Move**.

Figure 7-2

1. In the new window select the group which is shared in the branch and click **OK**.

Figure 7-3
Click the image to view larger in new window

1. The task will be moved to the shared group for the branch, allowing all branch administrators to use it.

Create a policy that is only accessible to a single branch administrator

This procedure is similar to the shared policy; only a few details are modified.

1. Log in as a branch administrator (eg. Tokyo*_Admin1*).
2. Click **Policies**.
3. Click **New Policy**.
4. In **Basic** section type a name and description of the policy.
5. Click the **Settings** section.
6. Select the appropriate product from the drop down-menu. Set up the policy according to your needs.
7. Click **Finish** to save the policy.

The policy will be saved in the home group of the current user, which means it will only be accessible to this user and top-level administrators. This branch administrator can apply this policy to all computers and devices to which they have access.

Create installers shared among all level admins

Any user with sufficient permissions over their home group, the target group and certificates can create an installer that is shared between all level admins.

1. Click **Quick Links → Other Deployment Options**.

Figure 8-1

1. Select **Create All-in-one Installer** and click **Create Installer**.


Figure 8-2

2. Deselect the check box **Participate in product improvement program** if you do not agree to send crash reports and telemetry data to ESET.

3. Select the product for which you want to create an installer.

4. Select the check box I accept the terms of the application End User License Agreement and acknowledge the Privacy Policy.

5. Select the language for this installer from the drop-down menu.

Figure 8-3
Click the image to view larger in new window

1. Click **Certificate**. In the **Peer Certificate** field, you can select whether to use a custom certificate from a *.pfx*file, or a certificate from ESMC. Choose the certificate to be used for the installer and if needed, type in the **Certificate passphrase**.

Figure 8-4
Click the image to view larger in new window

1. Click **Advanced**. Type in the **Name** and **Description** of the installer.

2. Select a parent group where the newly installed clients will be stored. For a shared installer, you should use a shared group where all users of the installer have access. (In this example use *Shared objects*)

3. If you want to use AV Remover, select the check box next to **Enable ESET AV Remover**.

4. Optionally, under **Configuration type** you can select whether the policy should be applied to clients following installation.

5. Make sure the **Server Hostname** is correct (the IP address of your ESMC Server).

6. Optionally you can change the **Port**, however this is not recommended.

7. Click **Finish** to create the installer.

Figure 8-5
Click the image to view larger in new window

1. Do not download the installer now. Click **Close**.

2. Click **Installers** and select the new installer. Click **Access Group → Move**.

Figure 8-6

1. Select a static group where all desired users have access (in this case the *Shared objects*) and click **OK**.

The installer will be moved to the shared group and will be available for all users with permissions over this group.

KB Solution ID: KB6881 |Document ID: 25873|Last Revised: August 17, 2018