How to Configure Permission Profiles

https://campus.barracuda.com/doc/73719363/

Permission profiles define how user sessions are handled by the SSH Proxy server. Although default permissions define setups that are valid for all users, you can also define custom permissions that apply only to special users. Follow the step-by-step instructions to configure default and custom permission profile settings.

Configure Default Permissions

Configure the default permission profile that applies to all users who connect to the SSH Proxy.

Step 1. Configure User Monitoring

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **SSH Proxy**.
2. In the left menu, select **Default Permission Profile**.
3. Click **Lock**.
4. In the left navigation menu, click **Default Permission Profile**.
5. For **Max. Illegal Inputs**, specify the maximum number of successive illegal inputs in the service menu after which a user is automatically disconnected. The default number of illegal attempts is 5.
6. Enable **Record Terminal Session** if terminal sessions of users should be recorded to a local file.
7. In the **Recorded Users** table, add the login names of the users whose sessions should be recorded.
8. In the **Inactivity Grace Time** field, specify the maximum inactivity time in seconds a user may spend within the proxy menu before being disconnected.
9. Click **Send Changes** and **Activate**.

Step 2. Configure Target Access Control

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **SSH Proxy**.
2. Click **Lock**.
3. In the left navigation menu, click **Default Permission Profile**.
4. In the **Target Access Control** section, enable **Allow Console Access** if local addresses on the firewall should be accepted as legitimate targets.
5. From the **Access Control Policy** list, specify how users should be granted access to certain destinations:
    1. **By Explicit Network Restriction** – Users are given access based on the list of addresses in the **Explicit Network ACL** table.
        - In the **Explicit Network ACL** table, add users who are not in the **Blocked User**

Groups table if you want to give them additional access rights due to source network restrictions.

2. **By Referenced Target Access List** – Users are given access to certain destinations based on destination hosts defined in an access list.
   - Select a configured list from the **Target Access List** menu. For more information on creating target access lists, see How to Configure the SSH Proxy.
6. In the **Custom Source IP** field, define the source IP address for outbound SSH connections.
7. If users are supposed to make X-Windows connections through the proxy service, enable **Forward X11 connections**.
8. If connecting users should be allowed to authenticate themselves at a target system with public key authentication, enable **Allow Public Keys**.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Configure Custom Permission Profiles

Configure custom permission profiles if some of the configurable settings should apply only to specific users. Configure the custom profile settings as described above in **Configure Default Permissions**.

Apply Custom Permission Profiles to Users

After configuring custom permission profiles, you can apply them to specific users.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > SSH Proxy**.
2. In the left menu, select **User Authorization**.
3. Click **Lock**.
4. In the **User Authorization** table, add profiles for your users. For each entry, configure the following settings:
   - **User Names** – In this table, add the names of users to which the profile settings will be applied.
   - **Applicable Permission Profile** – Select the permission profile to be applied to the users listed in the **User Names** table.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.