Shared Configuration

https://campus.barracuda.com/doc/54266807/

Overview

The Barracuda Web Application Firewall Control Center enables you to configure settings and share it with the connected devices. To share the configuration, you must first associate the object on the Barracuda Web Application Firewall Control Center with the object on the Barracuda Web Application Firewall device.

Understanding How the Shared Configuration Works

In this section, we use the object “Security Policy” as an example to explain how the configuration is shared between the Barracuda Web Application Firewall Control Center and the connected devices.

Initial Connect to the Barracuda Web Application Firewall Control Center

The Barracuda Web Application Firewall Control Center includes a predefined set of security policies. When the Barracuda Web Application Firewall is connected to the Barracuda Web Application Firewall Control Center, the configuration settings of the security policies on the connected device will automatically be overridden with the Barracuda Web Application Firewall Control Center configuration. This configuration synchronization happens because the **Association Mode** for the connecting devices is set to **Automatic** by default on the **ADVANCED > Settings** page. If you intend to manually associate the Barracuda Web Application Firewall Control Center security policies with the connected device, set the **Association Mode** to **Manual** before connecting the device.

For information on how to connect a device to the Barracuda Web Application Firewall Control Center, see **Connect a Device** section in the **Connecting and Disconnecting Devices** article.

Association Mode

The **Association Mode** determines whether to synchronize the configuration settings automatically or manually with the connected devices at the time the device is first connected to the Barracuda Web Application Firewall Control Center.

- **Automatic** – The security policies on the Barracuda Web Application Firewall Control Center will automatically be associated with the security policies of the connected device, and the Barracuda Web Application Firewall Control Center overrides the configuration of the security policies on the device with its configuration
- **Manual** – You should select the security policies and the devices to which the configuration needs to be synchronized.

Association Mode setting is used ONLY when the device is first connected to the Barracuda Web Application Firewall Control Center.

Creating a New Security Policy

The Barracuda Web Application Firewall Control Center provides a predefined set of policies that can be modified and applied to the connected devices. Additionally, you can create a new security policy and synchronize it with all connected devices, or associate the policy with the specific device(s) and synchronize the configuration. Perform the following steps to create and associate a new security policy:

1. Log into the Barracuda Web Application Firewall Control Center web interface.
2. Go to the **POLICIES > Security Policies** page.
3. In the **Create New Policy** section, do the following:
    1. **Policy Name**: Enter a name for the policy.
    2. **Based On**: Select an existing security policy based on which you want to create a new security policy, or select **Create New** to create a new security policy with custom settings.
    3. **Sync to All**: Specify whether or not to push the policy to the connected devices.
        1. **Yes** – The policy gets created and associates with all connected devices.
        2. **No** – The policy gets created and will be listed in the **Policy Manager** section. In this case, you should manually associate the policy with the device(s) to synchronize the configuration.
    4. Click **Add**.

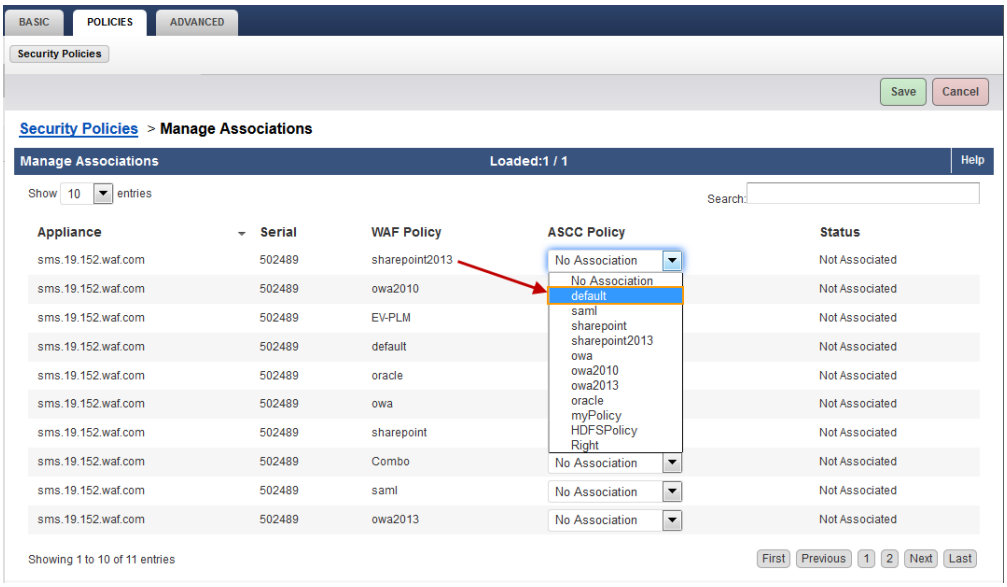
Synchronizing a Custom Policy with the Connected Devices

Perform the following steps to synchronize a custom policy with the connected devices:

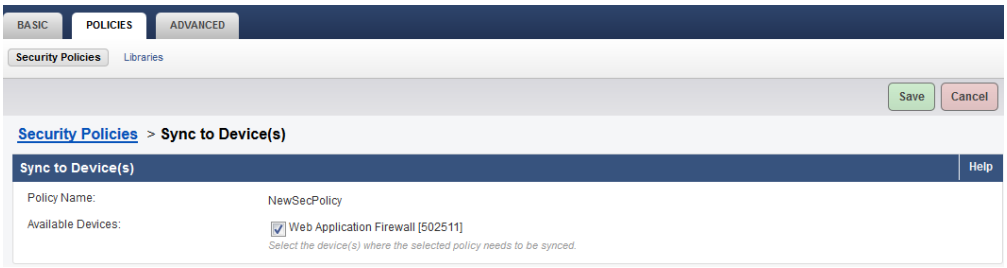
1. Log into the Barracuda Web Application Firewall Control Center web interface.
2. Go to the **POLICIES > Security Policies** page.
3. In the **Policy Manager** section, identify the policy that needs to be synchronized with the

device.

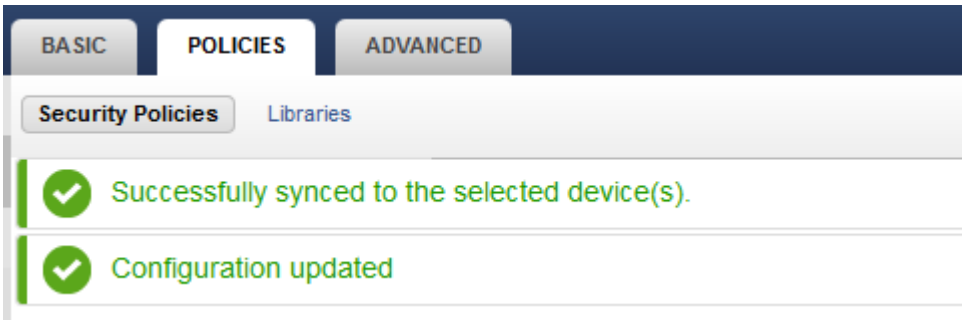
4. Select **Sync to Device(s)** from the **Actions** drop-down list next to the policy. The **Sync to Device(s)** page appears.



5. In the **Sync to Device(s)** section, select the device to which you want to associate the policy and click **Save**.



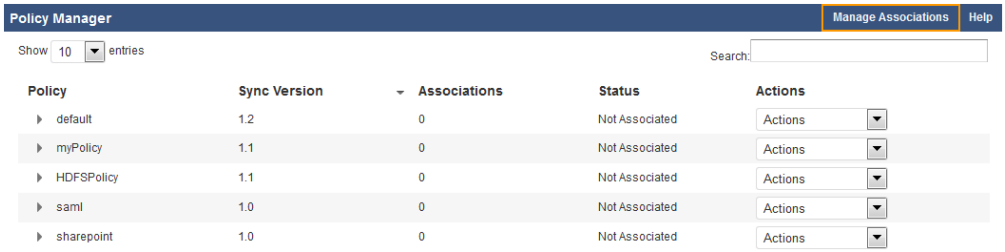
6. The policy gets synchronized with the selected devices.



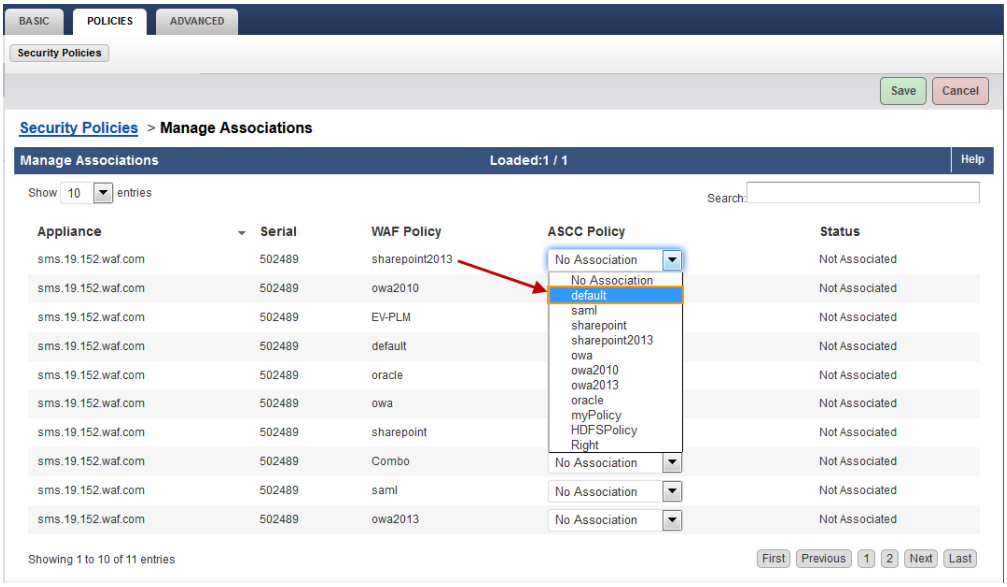
Steps to Manually Associate an Existing Policy on the Barracuda Web Application Firewall with the Policy on the Barracuda Web Application Firewall Control Center

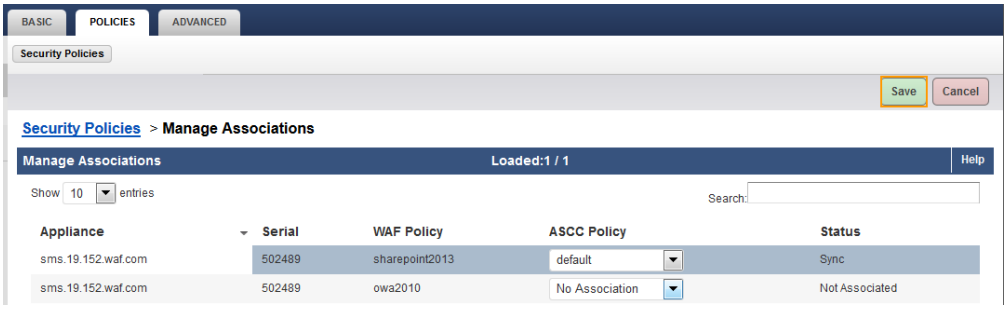
Perform the following steps to manually associate an existing security policy on the Barracuda Web Application Firewall with the Policy on the Barracuda Web Application Firewall Control Center:

1. Log into the Barracuda Web Application Firewall Control Center web interface.
2. Go to the **POLICIES > Security Policies** page.
3. In the **Policy Manager** section, click **Manage Associations**. The **Manage Associations** page appears.

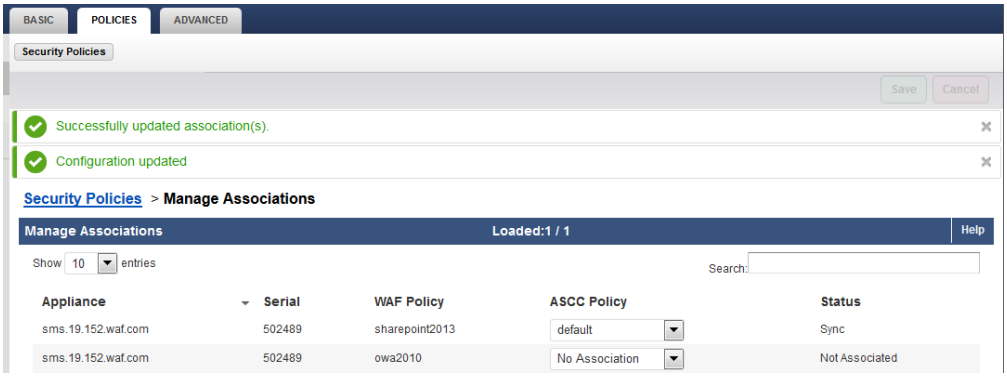


4. In the **Manage Associations** section, identify the WAF policy that needs to be associated with the policy on the Barracuda Web Application Firewall Control Center.
5. Select a policy from the **ASCC Policy** drop-down list next to the WAF policy, and click **Save**.





6. After successful association, the **Manage Associations** section displays the ASCC policy that you associated with the WAF policy.



Modifying an Existing Security Policy

When an existing security policy on the Barracuda Web Application Firewall Control Center is modified, the configuration is automatically synchronized with the associated security policy(s) on the connected device(s). If the security policy is not associated with the connected device(s), the policy will be saved in the **Policy Manager** section until it is manually synchronized with the connected device(s).

To modify an existing security policy on the Barracuda Web Application Firewall Control Center, perform the following steps:

1. Go to the **POLICIES > Security Policies** page on the Barracuda Application Control Center web interface.
2. In the **Policy Manager** section, identify the policy that you want to modify, and select **Edit** from the **Actions** drop-down list next to the policy. The selected policy page appears with all the sub-policies associated with it.
3. In the selected policy page, do the following:
    1. **Revision Control:** Mark the configuration changes as Major/Minor based on the number of changes/severity of changes. This will basically reflect on the sync version associated with the policy. For example, selecting **Minor** and modifying the request limit policy parameters would change the **Sync Version** from 1.0 to 1.1. If the same modification is done by setting the **Revision Control** to **Major**, the **Sync Version** changes from 1.0 to 2.0.
    2. **Request Limits:** The **Request Limits** policy defines the validation criterion for incoming requests by enforcing size limits on HTTP requests. The requests that exceed the defined length/limit are denied or allowed to pass through based on the **Mode** (**Passive** or **Active**) set for a Service. Modify the values if required and click **Save**. For more information, refer the Online Help.
    3. **Cookie Security**: The **Cookie Security** policy guarantees confidentiality of the cookie and avoids tampering of the cookie value. A shorter timeout interval can be configured for cookies to help minimize the chances of cookie stealing. This policy does not prevent cookie replay attacks. Modify the values if required and click **Save**. For more information,

refer the Online Help.

4. **URL Protection:** The **URL Protection** policy protects the service against web attacks. Modify the values if required and click **Save**. For more information, refer to the Online Help.
5. **Parameter Protection:** The **Parameter Protection** policy protects the service against attacks based on parameter values. Modify the values if required and click **Save**. For more information, refer to the Online Help.
6. **Cloaking:** The **Cloaking** policy prevents leakage of information about a Web site or service that is vulnerable for Web attacks. The HTTP headers and return codes are concealed before sending a response to a client. The response headers are filtered based on the headers defined in the **Headers to Filter** field. Modify the values if required and click **Save**. For more information, refer to the Online Help.
7. **URL Normalization:** This **URL Normalization** policy secures the websites from path traversal attacks, and specifies canonicalization policies for URLs found in the requests. Modify the values if required and click **Save**. For more information, refer to the Online Help.
8. **Protected Data Types:** The **Data Theft Protection** policy protects the sensitive information/data sent in responses from being exposed to unauthorized users. Modify the values if required and click **Save**. For more information, refer to the Online Help.
9. **Global ACLs:** The **Global ACL** policy defines the strict access control rules. You can add a new URL ACL or modify the existing URL ACL. Modify the values if required and click **Save**. For more information, refer to the Online Help.
10. **Action Policy:** The **Action Policy** is a collection of settings that determines the action to be enforced when a violation is detected. Modify the default attack action settings if required and click **Save**. For more information, refer to the Online Help.

Reconnecting to the Barracuda Web Application Firewall Control Center after Connection Failure

If the Barracuda Web Application Firewall disconnects from the Barracuda Web Application Firewall Control Center due to connection failure and reconnects to the Barracuda Web Application Firewall Control Center, the Barracuda Web Application Firewall Control Center validates the **Sync Version** with the connected device. If **the Sync Version** in the connected device is different, the Barracuda Web Application Firewall Control Center overrides the configuration on the connected device with its configuration. If the **Sync Version** is same, then the configuration is not synchronized with the connected device.

Disconnecting the Device Manually

When a device is disconnected manually, the Barracuda Web Application Firewall Control Center removes all the associations made with the device. If the same device is connected again with the

Barracuda Web Application Firewall Control Center, it is treated as a new device and configuration synchronization happens based on the Association Mode (Automatic or Manual).

Figures