Barracuda Web Application Firewall Integration with Venafi

https://campus.barracuda.com/doc/96766281/

The Barracuda Web Application Firewall (WAF) protects web applications and performs SSL/TLS encryption/decryption for HTTPS applications. Integration with Venafi certificate life cycle management enables administrators to easily manage the certificate life cycle and prevent application outages or such incidents that may occur due to certificate expiration.

Venafi's Trust Protection Platform (TPP) integrates with the Barracuda WAF for the purposes of SSL/TLS certificate life cycle management. The primary benefit of this is to centrally manage the life cycle of an organization's SSL/TLS certificates.

Prerequisites

Before performing the steps in this integration guide, you must have or create the following:

- PowerShell 3.0 or higher
- Venafi Trust Protection Platform version 20.4 or higher
- Barracuda Web Application Firewall (WAF) firmware version 10.1.1 or higher
- Barracuda account credentials
- A policy folder for the Barracuda WAF device(s)
- A policy folder for the discovered Barracuda certificates

Barracuda WAF Integration with Venafi TPP

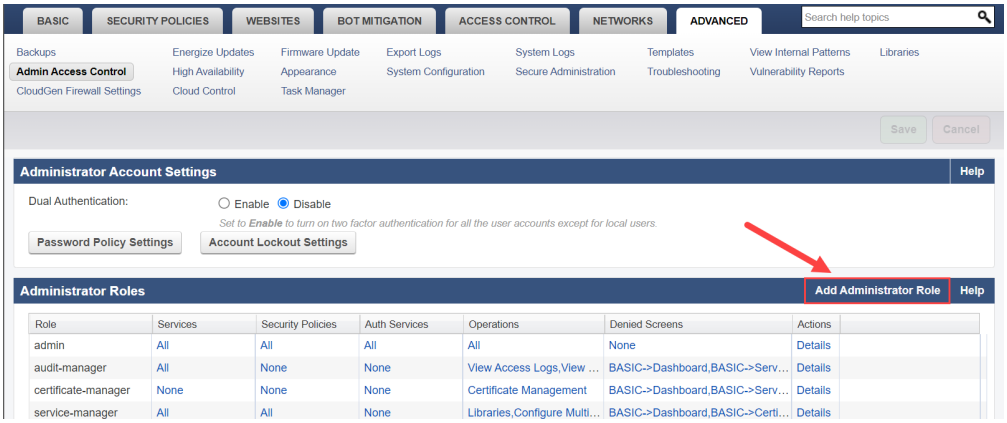
To enable Venafi TPP integration on the Barracuda WAF, do the following:

- Configure the Barracuda WAF with Access Credentials to Perform the API Operation
- Set Up the Barracuda WAF Connection Details and Credentials on the Venafi TPP
- Discover SSL/TLS Certificates on the Barracuda WAF
- Provision New SSL/TLS Certificates

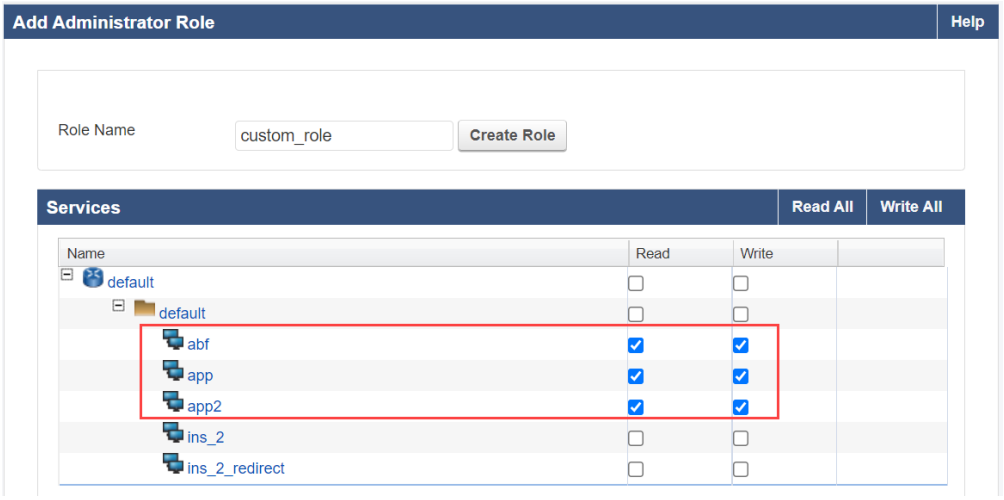
Configure the Barracuda WAF with Access Credentials to Perform the API Operation

On the Barracuda Web Application Firewall web interface, create a custom administrator role and do the following configuration:

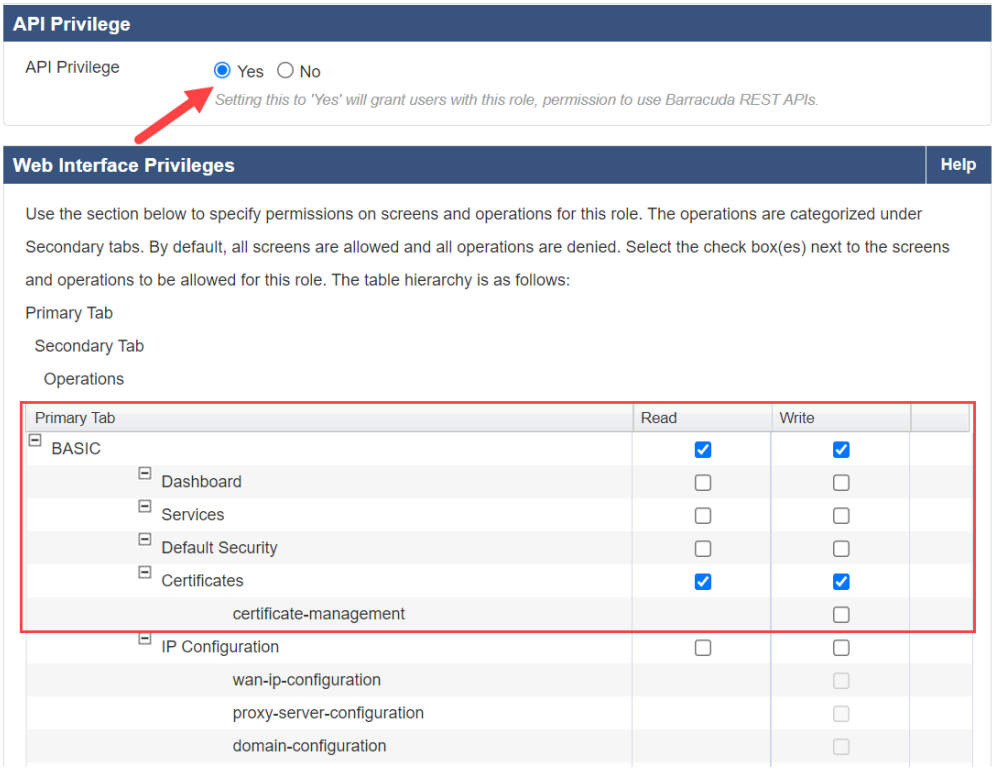
1. Go to the **ADVANCED > Admin Access Control** page, **Administrator Roles** section, and click **Add Administrator Role**.



2. On the **Add Administrator Role** window:
    1. Specify a role name.
    2. Under **Services**, select the services that need certificate management.

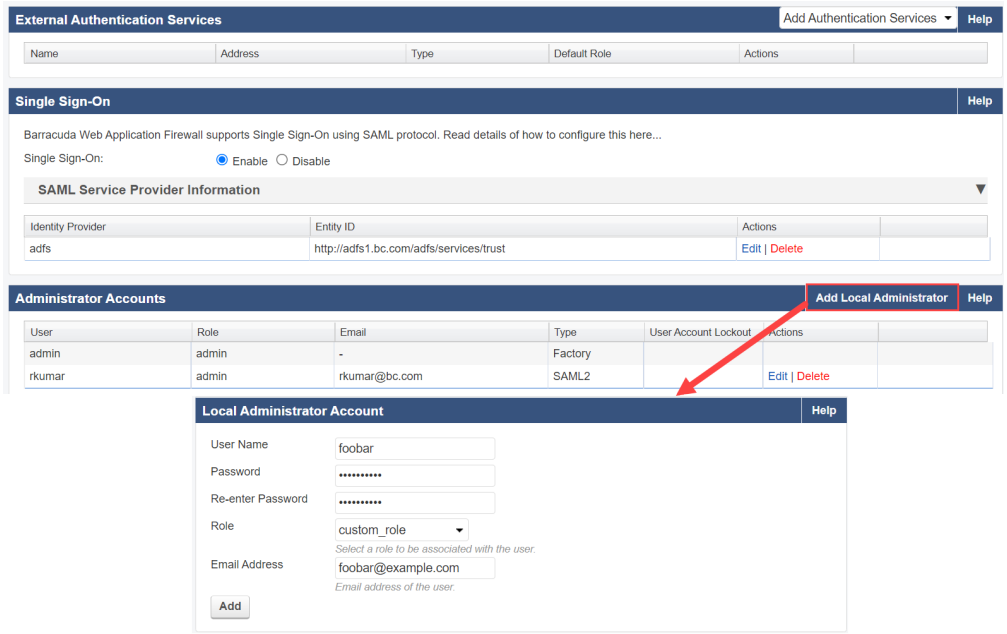


    3. Under **API Privilege**, set **API Privilege** to **Yes**.
    4. In the **Web Interface Privileges** section, select the **BASIC** (Primary Tab) and **Certificates** (Secondary Tab) **Read** and **Write** check boxes, and ensure that all other check boxes are cleared.



5. Click **Create Role**.

3. On the **ADVANCED > Admin Access Control** page, use the **Administrator Accounts** or **External Authentication Services** section to add a local administrator or an LDAP/RADIUS authentication service. Associate the custom role created in Step 2 with the local administrator or the authentication service that you create.



For more information on creating users, see the "Create Users" section in the Role-Based Administration (RBA) article.

Set Up Barracuda WAF Connections Details and Credentials on Venafi TPP

Perform the following steps to set up the Barracuda WAF on Venafi TPP:

1. Log into the Venafi Trust Protection Platform (TPP).
2. On the Venafi WebAdmin, open the **Policy** tree and add a new policy folder for the Barracuda Networks devices.
3. On the newly added policy page:
    1. Select **Applications** and do the following configuration under **Adaptable**:
        1. Select the **Application Credential** path and provide the **Port** number under **Application Information**. Note: Port number should be 8443 for the cloud instance, 443 for the hardware. If there is any specific port number for the device, provide the port details.
        2. Under **Adaptable Settings**, select **Barracuda-Waf** as the adaptable driver from the **PowerShell Script** drop-down list.
        3. Specify values for other parameters as required and click **Save**.
    2. Select **Settings > Certificates** and do the following configuration:
        1. Set the **Management Type** as **Provisioning** and **Managed By** as **Aperture**.
        2. Specify values for other parameters as required and click **Save**.
4. Right-click on the policy you created and select **Add > Credential > Username Credential**.
5. On the **Add New : Username Credential** page:
    1. Add the credentials (**User Name** and **Password**) of the administrator that you created in Step 3 under **Configuring the Barracuda WAF with Access Credential to Perform the API Operation**.
    2. Specify values for other parameters as required and click **Save**.
6. Right-click on the policy you created and select **Add > Devices > Device**.
7. On the A**dd New : Device** page, add the device details, such as device name, IP address, credential, and click **Save**.

Usage

This section provides information on how to properly use the integration after the initial configuration is complete.

Discover SSL/TLS Certificates on the Barracuda WAF

1. On the Venafi Aperture page, use the menu option and select **Jobs**.
2. Click **Create New Job**.
3. On the **Create New Job** page, select **Onboard Discovery** and click **Start**.

4. On the **New Onboard Discovery Job** page, configure the following:
    1. **Details**
        1. Specify the job details and select **Adaptable** as the **Installation Type**.
        2. Select the **Enable Debug Logging** check box.
        3. Click **Next**.
    2. **Targets**
        1. Specify the device that needs be discovered/scanned, or select the folder to discover/scan all devices located in the folder. If you want to add a new device or add a new device and new credentials, select **Create New Devices**.
        2. Click **Next**.
    3. **Placement Rules**
        1. Select the location where you want to save the discovered certificates.
    4. **Occurrence**
        1. Set the **Frequency** to **Manually**.
    5. Click **Create Job**.
5. Select the job you created and click **Run Now**.
6. After the successful discovery, all applications available on the Barracuda WAF along with the associated certificate objects will be visible on the Venafi TPP.

> Note: If certificates are already on Venafi TPP, the "Discover" operation discovers applications and the existing certificates gets associated with it.

Provisioning New SSL/TLS Certificates

1. On the Venafi TPP WebAdmin, open the **Policy** tree.
2. Right-click on the policy that you created and select **Add > Certificates > Server Certificate**.
3. On the **Add New : Server Certificate** page, specify the certificate details and click **Save**.
4. After the certificate is added successfully, click **Associations** on the certificate page.
5. Click **Add** and select the application(s) to which you want to associate the certificate.
6. Click **Push** to push the certificate to the selected applications.

Automatic Renewal of SSL/TLS Certificates

1. By default, the auto-renewal window for created and discovered certificates is set to 30 days prior to expiration.
2. Choose the CA template that can be used while performing the renewal of the certificate.
3. At the renewal time, Venafi TPP generates the new key and gets CSR signed from the specified CA.
4. After the certificate is renewed, it is installed on devices and then associated with the applications.

Troubleshooting

Error Messages

When troubleshooting error messages, providing the entire message displayed by Trust Protection Platform can speed the diagnosis and resolution.

Error Message	Description
User does not have privilege to perform task	A general error that resulted due to lack of permissions for that particular task.
Unable to connect	When an incorrect port is configured, or the device is not accessible from the Venafi TPP

Known Issues

- Custom role with services access - With the "Custom" role, if new services are created, certificate-related operations on the new services will fail because the account will not have the required permissions. When a new service is added, the role should be edited, and the new service(s) should be selected for the role to function properly.

  Alternatively, the default "Admin" role can be used to get full privileges.

- On Venafi TPP, the certificate life cycle can be managed only for the RSA or ECDSA certificate(s) associated with the service(s).
- Only Created and Uploaded Server certificates associated with the service(s) are supported.
- Trusted (CA) Certificate(s) and Trusted Server Certificate(s) are not supported.
- SNI certificates associated with the services are not discovered on Venafi TPP.

Figures