Templates Version 2

https://campus.barracuda.com/doc/45023981/

The **Templates Version 2** article is applicable to the *Barracuda Web Application Firewall Version 7.9* and above.

Managing application security policies over time and across multiple units manually can become cumbersome and error prone. Templates provide the ability to define baseline configuration settings that can be used as a model across policy revisions or across units. For example, by using templates, you can quickly create security policies designed to secure a specific application (e.g. SharePoint), web-portal, platform, framework or their constituents. Templates increase productivity, reduce manual errors and deployment time and ensure policy compliance.

A template is a reusable configuration file. It represents part of your Barracuda Web Application Firewall's existing configuration. The template framework provides a wizard-driven interface for creating templates from existing objects or applying created templates to an existing configuration. The configuration components can include a particular object or group of objects. Templates can be created to re-use one or more configuration components at a later time on the same unit or on another Barracuda Web Application Firewall. You can re-use a template by downloading, importing and applying the template to a unit.Templates allow you to:

- Migrate changes from the QA environment to the production environment.
- Import changes provided by the Barracuda Web Application Firewall expert community to refine policies on standard applications.
- Patch existing policies. For example, a new OWA template might need an additional "Allow Method" for a Global ACL, or a new pattern, like sql-tautology-conditions, might require a refinement to an existing pattern-group. An existing service might require a new keep-alive timeout, already tested and found optimal in the QA network.
- Take a backup of an application configuration.

Templates can also be used to:

- Create a new configuration on the Barracuda Web Application Firewall from a single unified web interface. For example, a new complete Security Policy can be created by modifying various security parameters in one shot.
- Replicate an object on the same or another Barracuda Web Application Firewall.

You can create three types of templates:

- **Full** - A Full template represents a configuration object (Refer to Object Type and Dependency Objects). You can create a new object with the desired settings using the **Full** template option. For example, a **Service** template includes all (selected) URL Profiles, Parameter Profiles, Rule Groups, URL ACLs, etc., associated with the service. Typically, a full template includes all

relevant information pertaining to an object. You can edit the values of parameters, if required, when creating a template.

- **Partial** - A Partial template represents part of an object configuration (refer to Object Type and Dependency Objects). With a Partial template, you can update the configuration of existing objects. Applying a partial template can be considered analogous to performing a Bulk Edit operation. For example, to update the **Session Timeout** value for multiple service, you can create a template with only the **Session Timeout** value modified. When this template is applied to the service(s), it only updates the Session Timeout value, keeping other parameter values intact.
- **Composite** - A Composite template is a group of full templates of the same type of objects (Refer to Object Type and Dependency Objects). You can use a Composite template to migrate multiple objects of the same type from the QA environment to the production environment. For example, to copy URL profiles of an application to another application, you can create a template with selected URL profiles and apply it to an application requiring configuration of these URL profiles. This creates URL profiles on the **WEBSITES > Website Profiles** page for the selected application.

You cannot edit the values of parameters when creating a Composite template. If you wish to edit the values of certain parameters, download the template, open the XML file and edit the values before importing it.

Creating a Template

To create a template, navigate to the **ADVANCED > Templates, Template Repository** section and click **Create Template**. Select a suitable Template Type, Template Format and specify which existing object you want to base the template on. You can create template for a particular object or object type. All configuration relevant to the chosen object gets loaded on the web interface, and you can modify the values before creating the template. Sub-objects can be included/excluded from the template at this time.

Editing Templates

You can edit and modify the configuration settings of a template by selecting the **Edit** option under the **Actions** column on the **ADVANCED > Templates** page. The following operations can be performed using the **Edit** option:

- Values can be modified (with an exception of few critical parameters, example: Service Type).
- Sub-objects can be excluded from the template.
- Associated objects like Certificates/Trusted Host Groups can be changed.

Using Templates

You can apply the template by selecting the **Use** operation in the **Available Templates** section. The **Use** operation allows you to apply a template to the selected destination. The **Use** template wizard

displays different key parameters for each object. The wizard layout is as follows:

- **Destination**: Select a destination to apply the template. For example, if you are applying a URL Profile template, the destination option would be a Service, because a URL Profile logically exists within a Service.
- Provide values for key parameters for each object and sub-objects.
- Review the summary details and click **Apply** to apply the template.

With the Use template wizard, you can use the same template and create different objects by providing unique values to key parameters.

Importing Templates

A saved template can be imported on to the same Barracuda Web Application Firewall or to another Barracuda Web Application Firewall by using the **Import Template** operation. This operation does not apply the configuration contained in the template, but only copies the template to the file system.

Steps to Create and Use a Template

To create and use a template, perform the following steps:

1. Go to the **ADVANCED > Templates** page, **Template Repository** section and click **Create Template**.
2. On the **Create Template** window:
    1. Enter a name for the template, select the template format, select the object type.
    2. Edit the values (if required), and click **Create**.
    3. If the template has any dependencies, a pop-up window displays the dependency objects.
        Ensure the dependency objects are configured on the destination system before the template is imported and used.
3. Once the template is created, it gets displayed in the **Template Repository** section.
4. You can edit the template (if required) by clicking **Edit** under **Actions**.
5. To use the template on the same unit, click **Use** under **Actions**. Select the destination and other subsequent settings based on the object type. Review your settings under **Summary,** and click **Apply**.
    Ensure the dependency objects (if any) are associated with the template before you **Apply** the template
6. To use the template on another Barracuda Web Application Firewall, do the following:
    1. Download the template to your local machine by clicking **Download** under **Actions**. The template downloads in ZIP format with the following two (2) files:
        1. An XML file containing the relevant configuration.
        2. An HDR file that can be recognized by the Barracuda Web Application Firewall and used for internal purposes.
    2. Log into the other Barracuda Web Application Firewall where you want to import and use the template, and do the following:
        1. Go to the **ADVANCED > Templates** page, **Template Repository** section and

click **Import Template**.

2. In the **Import Template** window, enter a name for the template and click **Browse** to select the downloaded template. Click **Import Template**.
3. Once the template successfully imports, it displays in the **Template Repository** section.
4. Now, click **Use** under **Actions**. Select the destination and other subsequent settings based on the object type. Review your settings under **Summary**, and click **Apply**.

   Ensure the dependency objects (if any) are associated with the template before you **Apply** the template

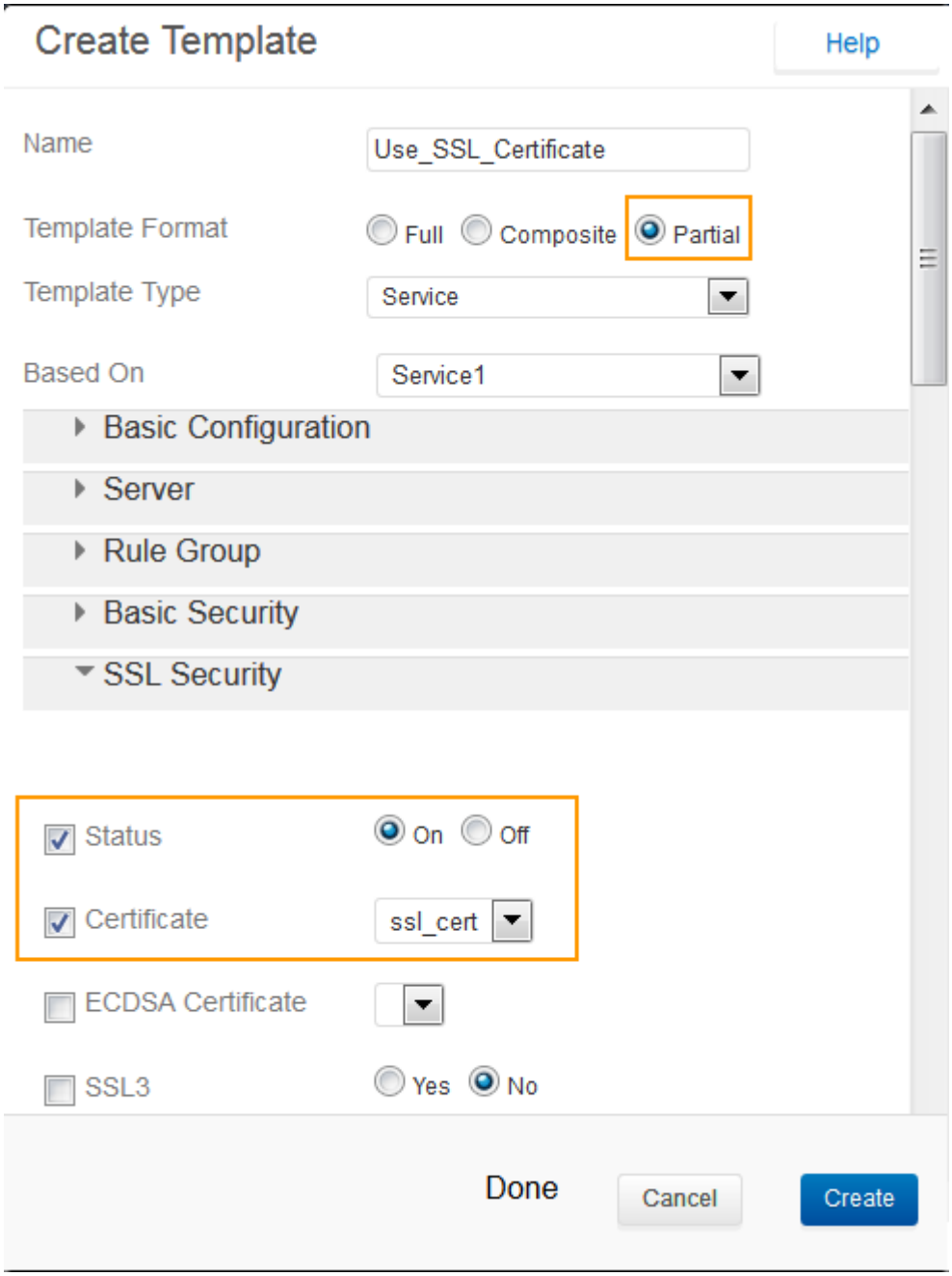
Use Case for Template

Use Case: Associate an SSL certificate used by a service to multiple services

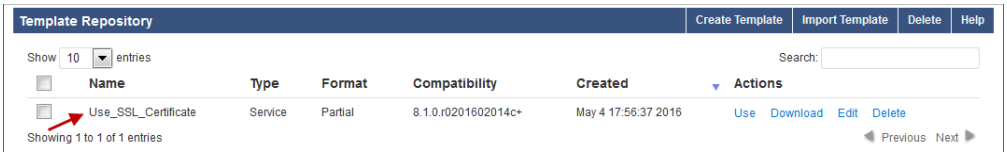
In this use case, let's assume you created an HTTPS service with an SSL certificate. You want to edit multiple services configured on the Barracuda Web Application Firewall, which should be SSL enabled and assigned the same SSL certificate. This can be achieved by using templates.

The steps below walks you through the use case:

1. Go to the **BASIC > Services** page, and create an HTTPS service with an SSL certificate. Example: *Service1*. For more information on how to create a service, click **Help** on the web interface.
2. Go to the **ADVANCED > Templates** page.
3. In the **Template Repository** section, click **Create Template**. The **Create Template** window appears.
4. In the **Create Template** window, do the following:
   1. **Name**: Enter a name for the template. **Example**: *Use_SSL_Certificate*
   2. **Template Format**: Select *Partial*.
   3. **Template Type**: Select *Service*.
   4. **Based On**: Select the service you want to base your template on. **Example**: *Service1*. This will display all configuration settings of the selected service.
   5. Click **SSL Security** and select **Status** and **Certificate** check boxes.
   6. Click **Create**.

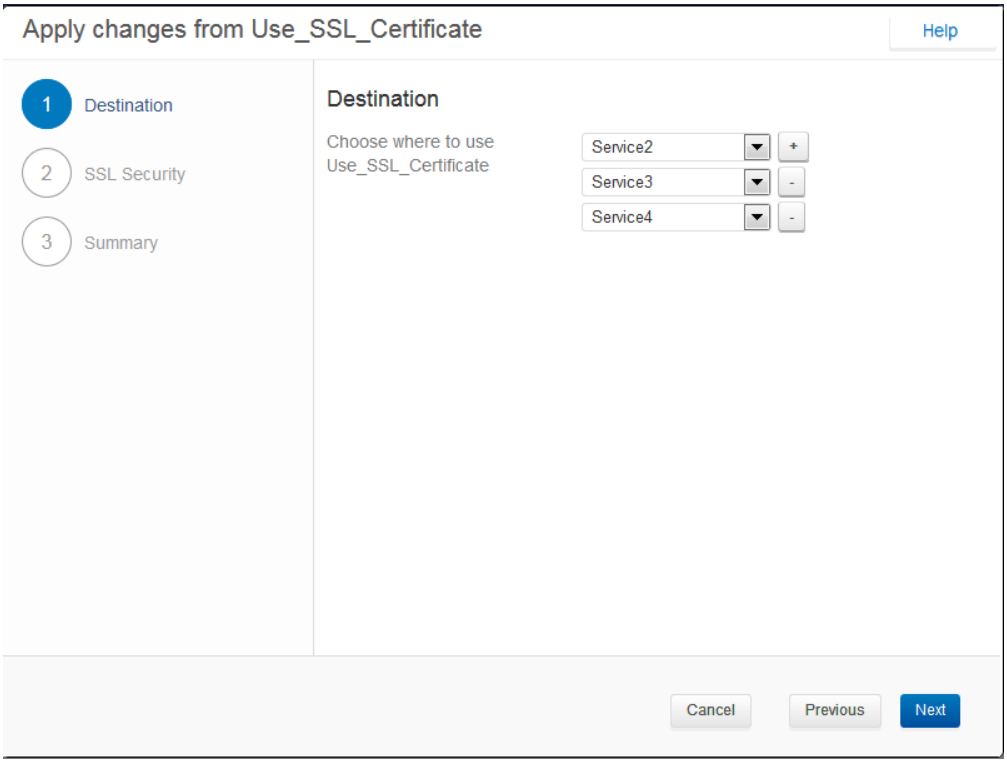


5. The template gets created and displayed in the **Template Repository** section.

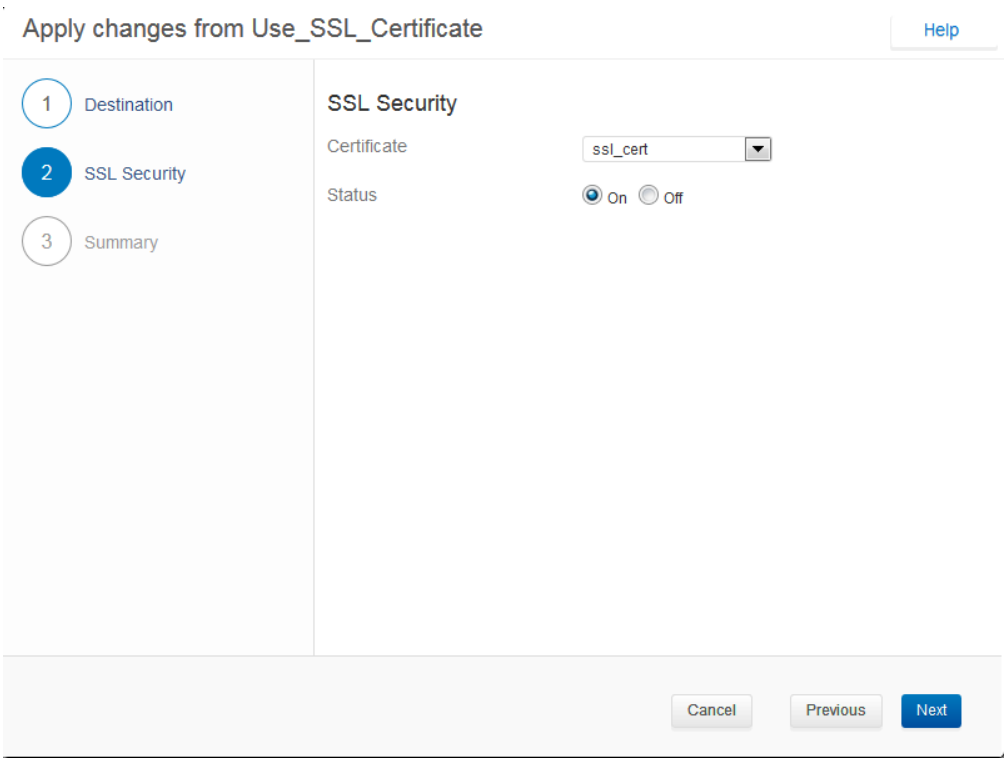


6. To associate the SSL certificate with other services, click **Use** under **Actions** in the **Template Repository** section. The **Apply changes from "Template-Name"** window appears. Example: *Apply Changes From Use_SSL_Certificate*.
7. In the **Apply Changes from Use_SSL_Certificate** window, do the following:

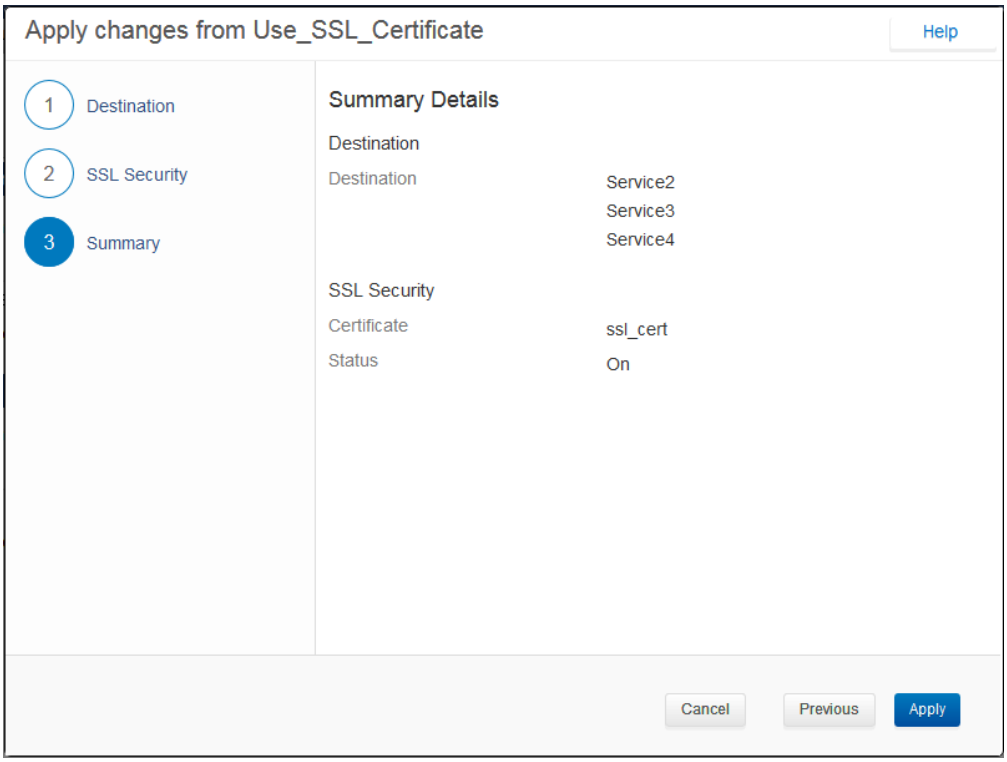
8. **1. Destination**: Choose the services to which you want to apply the *Use_SSL_Certificate* template, and click **Next**.



9. **2. SSL Security**: Select the certificate that you want to associate with the service, set the status and click **Next**.

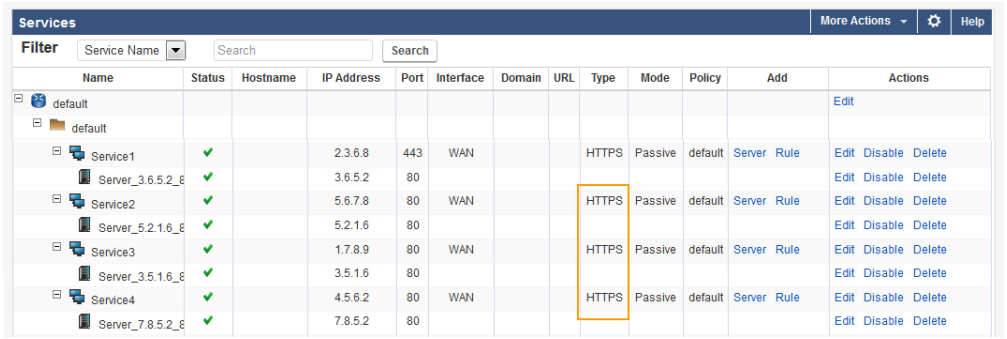


10. **3. Summary:** Review the summary details and click **Apply** to apply the template.



11. The template is now applied to the specified services.

12. Go to the **BASIC > Services** page. You can see that the template is applied to the services.



Points to Remember

While template generation includes configuration data of the sub-objects, it does not include the configuration of external entities/dependencies that the object or sub-object refers to. For example, if you have a policy associated to a service, make sure the policy exists on the destination unit before importing the service. The most common cases of objects like these within a service are: Security Policy, Response Pages, Certificates, Parameter Classes, Rate Control pool, Trusted Hosts, etc.

Object Type and Dependency Objects

A template only contains a reference to dependency objects. This means that when the template is downloaded and imported on another Barracuda Web Application Firewall, the dependencies are not imported. In this case, all dependencies appear as key parameters in the **Use Template** wizard and so appropriate dependencies can be referenced before applying the template. For example, when importing a template HTTPS service, the certificate is not imported. While applying the template, the certificate appears as a key parameter in the wizard and an existing certificate on the unit can be associated with the service.

The following table lists each object with its dependency objects:

Object Type	Objects on which the Object Type is dependent
Service	Rate Control Pool
	Authentication Service
	Trusted Hosts Group
	Session Identifiers
	Web Firewall Policy
	Certificate
Server	Client Certificate
URL Profile	Custom Blocked Attack Types
Parameter Profile	Custom Parameter Class
Rule Group Server	Client Certificate
URL Policy	Rate Control Pool
Secure Browsing Policy	Credential Server
URL ACL	Response Page
Header ACL	Custom Blocked Attack Types
Security Policy	Custom Blocked Attack Types
Global ACL	Response Page
Data Theft Protection	Custom Identity Theft Type
Custom Parameter Class	Custom Blocked Attack Types
	Custom Input Type Validation
Rule Group	
JSON Profile	JSON Security Policy
DDoS Policy	
Authorization Policy	
URL Encryption Rule	
URL Translation	

Adaptive Profiling Rule	
Request Rewrite Policy	
Response Rewrite Policy	
Response Body Rewrite Policy	
Allow/Deny Client	
SSL CRL	
Trusted Host Group	
Trusted Host	
LDAP Authentication Service	
RADIUS Authentication Service	
SiteMinder Authentication Service	
Kerberos Authentication Service	
RSA SecurID Authentication Service	
JSON Security Policy	
Rate Control Pool	
Preferred Client	
Response Page	
Credential Server	
Syslog Server	
Custom Identity Theft Protection	
Identity Theft Pattern	
Custom Attack Type	
Attack Type Pattern	
Custom Input Type	
Input Type Pattern	
Static Route	

Figures