How to Configure SiteMinder Single Sign-On (SSO)

SiteMinder

The Barracuda Web Application Firewall integrates with CA/Netegrity SiteMinder to provide Single Sign-On and centralized management of Web applications using the predefined security policies. It uniquely identifies users before they are authenticated as named users, and manages user's privileges to ensure that they access only authorized applications or operations.

Support for SiteMinder has been deprecated. Also, SiteMinder feature will NOT be available from Version 9.1.

Components in SiteMinder Setup

The two significant components of SiteMinder are:

- **Web Agents** – Integrated with a standard Web server or application server that enables SiteMinder to manage Web applications based on the predefined security policies.
- **Policy Server** – Provides Policy management and AAA functions within the SiteMinder framework.

Single Sign-On (SSO) Setup

In SiteMinder Single Sign-On (SSO), a user successfully authenticates through one agent and does not have to re-authenticate when accessing a realm protected by a different agent. The two agents must be in the same cookie domain, for example: /abc.siteminder.com. CA SiteMinder supports both single and multi-domain Single Sign-On. For more information about Single sign-on functionality, refer to How to Configure Single Sign-On (SSO).

The **ACCESS CONTROL > Authentication** page provides two types of Single Sign-On:

Single Sign-On (SSO)

- Supports single and multiple domains.
- The Barracuda Web Application Firewall authenticates and authorizes users accessing the Web application.

SiteMinder SSO

- Supports single and multiple domains.
- Authentication and authorization is performed by the SiteMinder Policy Server. By default, the Barracuda Web Application Firewall is set as an authorization agent for all authentication services. To change the **Authorization Agent** to **SiteMinder**, navigate to the **ACCESS CONTROL > Authorization** page and click **Edit** next to the Service. See Configuring Authorization Policy.

How it works

The following steps describe how the Barracuda Web Application Firewall communicates with the Policy Server before granting access to the protected resource.

1. The Barracuda Web Application Firewall intercepts requests and communicates with the Policy Server to determine whether the requested resources are protected or not. For protected resources, users are

redirected to a login page, and challenged to provide credentials. If the resource is not protected, the user is allowed to access the requested resource instantly. **Note:** If a customized login URL is defined in **Auth Not Done URL** on the **ACCESS CONTROL > Authorization** page, the user is redirected to that page for authentication. If not, the user is redirected to the default login page.
2. User enters username and password.
3. The Barracuda Web Application Firewall transmits the credentials to the SiteMinder Policy Server for validation.
4. The SiteMinder Policy Server authenticates the user against the configured external user directories. The Policy Server supports LDAP, Oracle, Microsoft SQL Server and custom user directories.
5. After successful authentication, the Barracuda Web Application Firewall communicates with the Policy Server to authorize the user. During authorization, SiteMinder:
    1. Checks the rules and policies assigned to the users and groups.
    2. Generates an SSO token for the request.
6. On successful authorization, SiteMinder sends the SSO token along with other information such as user details, session expiration time and additional user attributes defined on the Policy Server if any.
7. The Barracuda Web Application Firewall uses the SSO token, appends the SMSESSION cookie to the request and allows access to the protected resource.
8. When the user attempts to access another protected resource:
    1. The Barracuda Web Application Firewall validates the user based on the contents of the SMSESSION cookie and communicates with the Policy Server for authorization, without challenging the user for credentials.
    2. If authorized, the user is allowed to access the protected resource and the information is stored in the cache.

Configuring SiteMinder SSO through Barracuda Web Application Firewall

The Barracuda Web Application Firewall requires the following configuration settings for SiteMinder SSO:

Pre-requisite:

1. Before enabling SiteMinder SSO on the Barracuda Web Application Firewall the administrator must configure the SiteMinder Policy Server as follows:
    1. **SiteMinder Agent** – Create an Agent with the **Agent Type** as **SiteMinder** and **Web Agent**. **Note**: The **Name** field in the **Agent Properties** window must match the **Agent Name** parameter in the Barracuda Web Application Firewall configuration for SITEMINDER server.
    2. **Agent Conf Objects** – In **Agent Configuration Objects Properties**, do the following:
        1. Add a new parameter **AcceptTPCookie** and set **Value** to **Yes**.
        2. Set **DefaultAgentName** to **Agent Name** parameter defined in **Step 1a**.
    3. **Host Conf Objects** – In **Host Configuration Object Properties**, ensure the IP address and port numbers assigned to **Policy Server** are correct. If the Policy Server is in a cluster, specify the IP addresses of all Policy Servers in the cluster.
    4. Create a user directory with all user names to be authenticated by SiteMinder.
    Create Realms and define rules and policies for the realm.You should create realms for each URL pattern you want to protect or unprotect instead of protecting the root directory (/). For example "/images/logo.jpg", "/images/banner.png" can be ignored from protection, and "/finance/report.html", "/server/login.html" can be configured to be protected. **Note**: The SiteMinder Realm is not related with the Realm on the Barracuda Web Application Firewall. A realm in SiteMinder is a cluster of protected and unprotected resources. The SiteMinder Realm and the corresponding policies determine the users and groups to be allowed for a protected resource. Refer CA SiteMinder Policy Design Guide for more information on how to configure these objects.The values configured on the Policy Server now need to be specified in the **SITEMINDER** tab under the **ACCESS CONTROL > Authentication Services** page.

Note: The Barracuda Web Application Firewall uses "***Custom Agent***" capabilities of SiteMinder to provide authentication and authorization in a Single Sign-On environment.

Configuring SiteMinder Authentication Service

The SiteMinder Policy Server must be specified as the authentication service on the **ACCESS CONTROL > Authentication Services > SITEMINDER** tab. The Barracuda Web Application Firewall uses this information to communicate with the SiteMinder Policy Server to authenticate a user.

To configure SITEMINDER authentication service:

1. From the **ACCESS CONTROL > Authentication Services** page select the **SITEMINDER** tab and specify values for the following:
    1. **Realm Name** – Enter a name for the realm to identify this server in the Web interface.
    2. **Server IP** – Enter the IP address of the SiteMinder Policy Server used for authenticating users.
    3. **Port** – Enter the port number associated with the IP address of the SiteMinder Policy Server.
    4. **Admin** – Enter the username of a user with privileges to access the SiteMinder Policy Server.
    5. **Password** – Enter the password associated with the above username (Admin).
    6. **Agent Name** – Enter the agent name of the SiteMinder Agent you configured in the SiteMinder Policy Server.
    7. **Host Conf Object** – Enter the corresponding Host Configuration Object defined in the SiteMinder Policy Server.
2. Click **Add** to save your settings.

Configuring Authorization Policy

By default, the Barracuda Web Application Firewall is the authorization agent for Services associated with the LDAP, RADIUS and RSA SECURID authentication services. If a Service is associated with the SITEMINDER authentication service, the authorization agent must be **SiteMinder** to authorize the users accessing SiteMinder protected resources. To change the **Authorization Agent**, click **Edit** next to the SiteMinder service on **ACCESS CONTROL > Authorization** and scroll down to the **Advanced** section. For more information on how to configure an authorization policy, see Configuring Authorization Policy.

Configuring SiteMinder Single Sign-On

Configure the following the parameters to set up single sign-on (SSO) using SiteMinder:

1. From the **ACCESS CONTROL > Authentication** page identify the Service to which you want to enable SiteMinder SSO. Ensure the Service is associated with the SiteMinder authentication service.
2. Click **Edit** next to the Service. The **Edit Authentication Policy** window appears.
3. Scroll down to the **SiteMinder SSO** section and specify values for the following:
    1. **Cookie Provider** – Set to *Yes* to enable this Service to act as a cookie provider agent to other agents that are in SiteMinder SSO setup.
    2. **Cookie Provider URL** – Specify the URL path of the cookie provider. This service acts as a cookie provider agent to other agents that are in SiteMinder SSO setup.
    3. **Source IP Check** – Set to *Yes* if you want to check the source IP address in the cookie while authenticating the user.
    4. **Session Validation Timeout** – Specify the time interval in seconds for the Barracuda Web Application Firewall to re-validate a session with the Policy Server.
    5. **Set-Cookie List** – Specify the list of cookies as comma separated regular expressions. If the regex matches the requesting URL, the corresponding cookie will be set in the redirect response to the Login page.
    6. **Idle Timeout URL** – Specify a URL to which the user will be redirected after **Idle Timeout** is exceeded.
    7. **Idle Timeout Cookie** – Specify a cookie name and value to be inserted in the redirect response to the client after the **Idle Timeout** is exceeded.
    8. **Extended Idle Timeout** – Set the maximum time (in minutes) that a user can remain idle, after which the user is redirected to the configured **Extended Idle Timeout URL**.
    9. **Extended Idle Timeout URL** – Specify a URL to which the user will be redirected once the

Extended Idle Timeout is exceeded.

10. **Extended Idle Timeout Cookie** – Specify a cookie name and value to be inserted in the redirect response to the client after the **Extended Idle Timeout** is exceeded.
11. **Single Session Per User** – Set to *Yes* to allow only one active session per user.
12. **Enable Debug Logs** – Set to *Yes* to enable debug logs.

4. Click **Save Changes** to save your settings.

References:

For more information about the SiteMinder Policy Server and Web Agent Configuration, refer to SiteMinder Bookshelf.

Related Articles

How to Configure Single Sign-On (SSO)