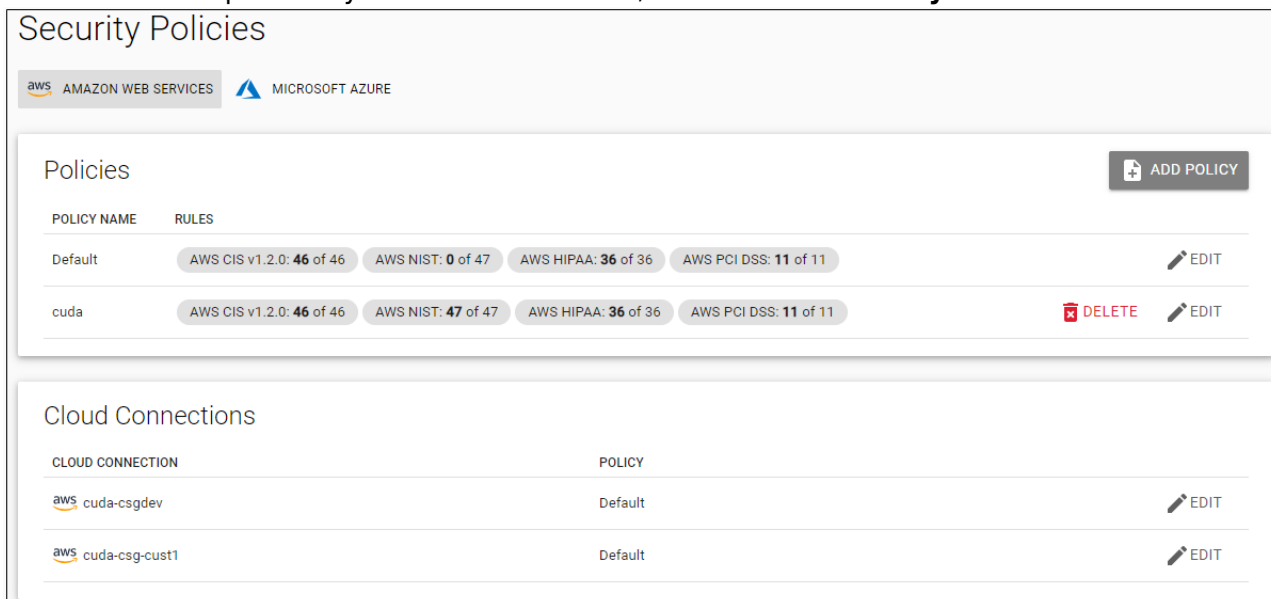


Creating a Security Policy

<https://campus.barracuda.com/doc/78808286/>

To create a new security policy in Barracuda Cloud Security Guardian:

1. In the left menu, navigate to **Security Policies**.
2. Select the cloud provider you want to work with, then click **Add Policy**.



The screenshot shows the 'Security Policies' page in the Barracuda Cloud Security Guardian interface. At the top, there are tabs for 'AMAZON WEB SERVICES' (selected) and 'MICROSOFT AZURE'. Below the tabs, the 'Policies' section contains a table with two rows: 'Default' and 'cuda'. Each row shows compliance scores for various standards (AWS CIS v1.2.0, AWS NIST, AWS HIPAA, AWS PCI DSS) and has an 'EDIT' button. A 'DELETE' button is also present for the 'cuda' policy. An 'ADD POLICY' button is located in the top right corner of the Policies section. Below the Policies section, the 'Cloud Connections' section contains a table with two rows: 'cuda-csgdev' and 'cuda-csg-cust1', both associated with the 'Default' policy and having an 'EDIT' button.

POLICY NAME	RULES	ACTIONS
Default	AWS CIS v1.2.0: 46 of 46 AWS NIST: 0 of 47 AWS HIPAA: 36 of 36 AWS PCI DSS: 11 of 11	EDIT
cuda	AWS CIS v1.2.0: 46 of 46 AWS NIST: 47 of 47 AWS HIPAA: 36 of 36 AWS PCI DSS: 11 of 11	DELETE EDIT

CLOUD CONNECTION	POLICY	ACTIONS
aws cuda-csgdev	Default	EDIT
aws cuda-csg-cust1	Default	EDIT

3. Type a unique **Policy Name**.

Add Policy

Policy Name*

[Azure CIS v1.1.0](#)
[Azure NIST](#)
[Azure HIPAA](#)
[Azure PCI DSS](#)

<input checked="" type="checkbox"/> BENCHMARK	DESCRIPTION	SEVERITY
<input checked="" type="checkbox"/> CIS 1.1	Ensure that multi-factor authentication is enabled for all privileged users	MEDIUM
<input checked="" type="checkbox"/> CIS 1.2	Ensure that multi-factor authentication is enabled for all non- privileged users	LOW
<input checked="" type="checkbox"/> CIS 1.3	Ensure that there are no guest users	HIGH
<input checked="" type="checkbox"/> CIS 1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled'	LOW
<input checked="" type="checkbox"/> CIS 1.5	Ensure that 'Number of methods required to reset' is set to '2'	MEDIUM
<input checked="" type="checkbox"/> CIS 1.6	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	MEDIUM
<input checked="" type="checkbox"/> CIS 1.7	Ensure that 'Notify users on password resets?' is set to 'Yes'	MEDIUM
<input checked="" type="checkbox"/> CIS 1.8	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes'	LOW
<input checked="" type="checkbox"/> CIS 1.9	Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No'	LOW
<input checked="" type="checkbox"/> CIS 1.10	Ensure that 'Users can add gallery apps to their Access Panel' is set to 'No'	LOW
<input checked="" type="checkbox"/> CIS 1.11	Ensure that 'Users can register applications' is set to 'No'	LOW
<input checked="" type="checkbox"/> CIS 1.12	Ensure that 'Guest user permissions are limited' is set to 'Yes'	LOW
<input checked="" type="checkbox"/> CIS 1.13	Ensure that 'Members can invite' is set to 'No'	LOW
<input checked="" type="checkbox"/> CIS 1.14	Ensure that 'Guests can invite' is set to 'No'	LOW
<input checked="" type="checkbox"/> CIS 1.15	Ensure that 'Restrict access to Azure AD administration portal' is set to 'Yes'	MEDIUM

CANCEL
ADD

- Select the standards and controls you want to use for this new policy.
 - Specify the standard by selecting its tab in the top line, including CIS, NIST, HIPAA, and PCI DSS.
 - Select all controls or just specific controls you want to include, and clear any check boxes for controls that you do not want to include. For example, you might want all of the CIS policies except one.
- At the bottom of the window, click **Add**.
- Your policy appears in the table of policies for your public cloud.

From this table of policies, you can choose to edit or delete any policy you create at any time. You can view and edit, but not delete the Default Policy.

After you create policies, assign the policies to your cloud connections. Refer to [Assigning a Security Policy to a Cloud Connection](#) for details.

Figures

1. policiesSec.png
2. policyList.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.