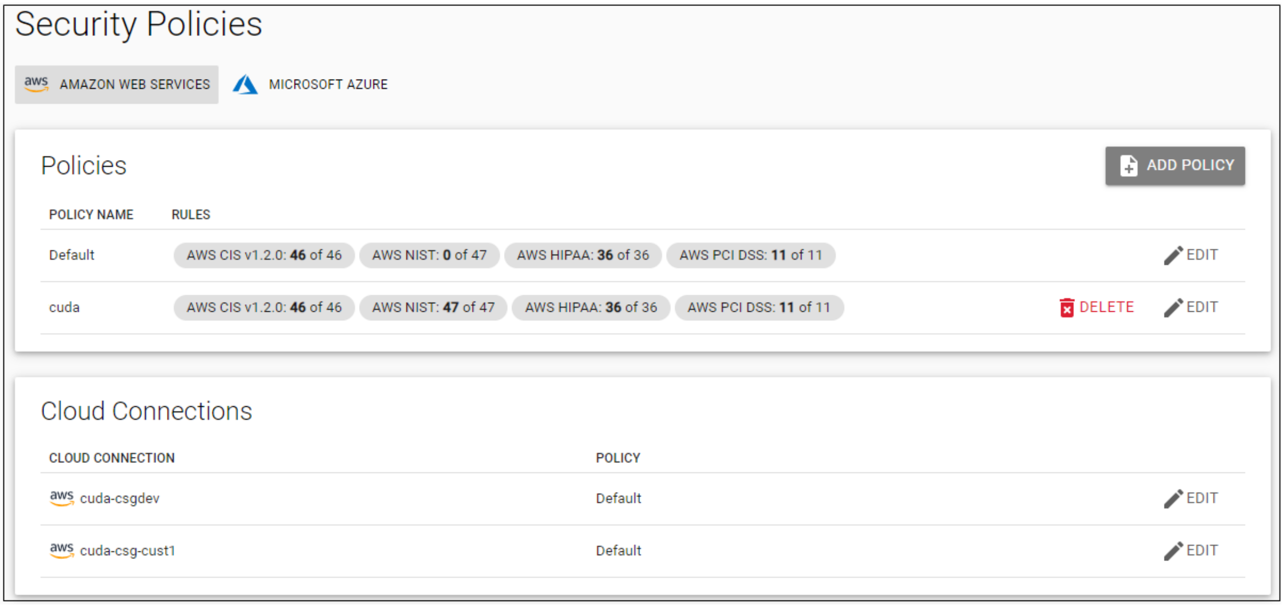
Creating a Security Policy

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**.

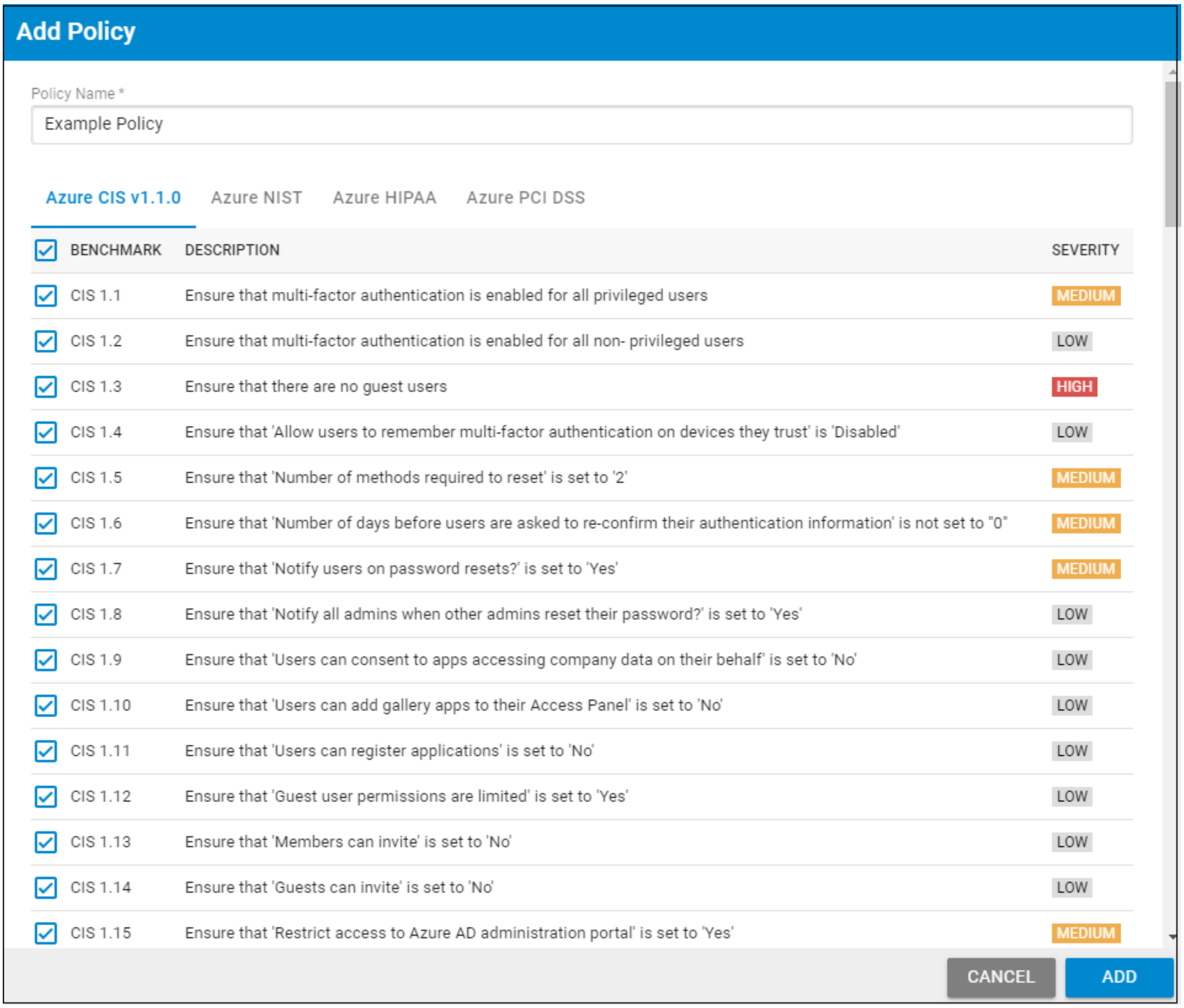


POLICY NAME	RULES					
Default	AWS CIS v1.2.0: **46** of 46	AWS NIST: **0** of 47	AWS HIPAA: **36** of 36	AWS PCI DSS: **11** of 11		EDIT
cuda	AWS CIS v1.2.0: **46** of 46	AWS NIST: **47** of 47	AWS HIPAA: **36** of 36	AWS PCI DSS: **11** of 11	DELETE	EDIT

Cloud Connections

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

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



Add Policy

Policy Name *

Example Policy

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

4. Select the standards and controls you want to use for this new policy.
    1. Specify the standard by selecting its tab in the top line, including CIS, NIST, HIPAA, and PCI DSS.
    2. 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.
5. At the bottom of the window, click **Add**.
6. 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