

Creating Policies for Security and Compliance

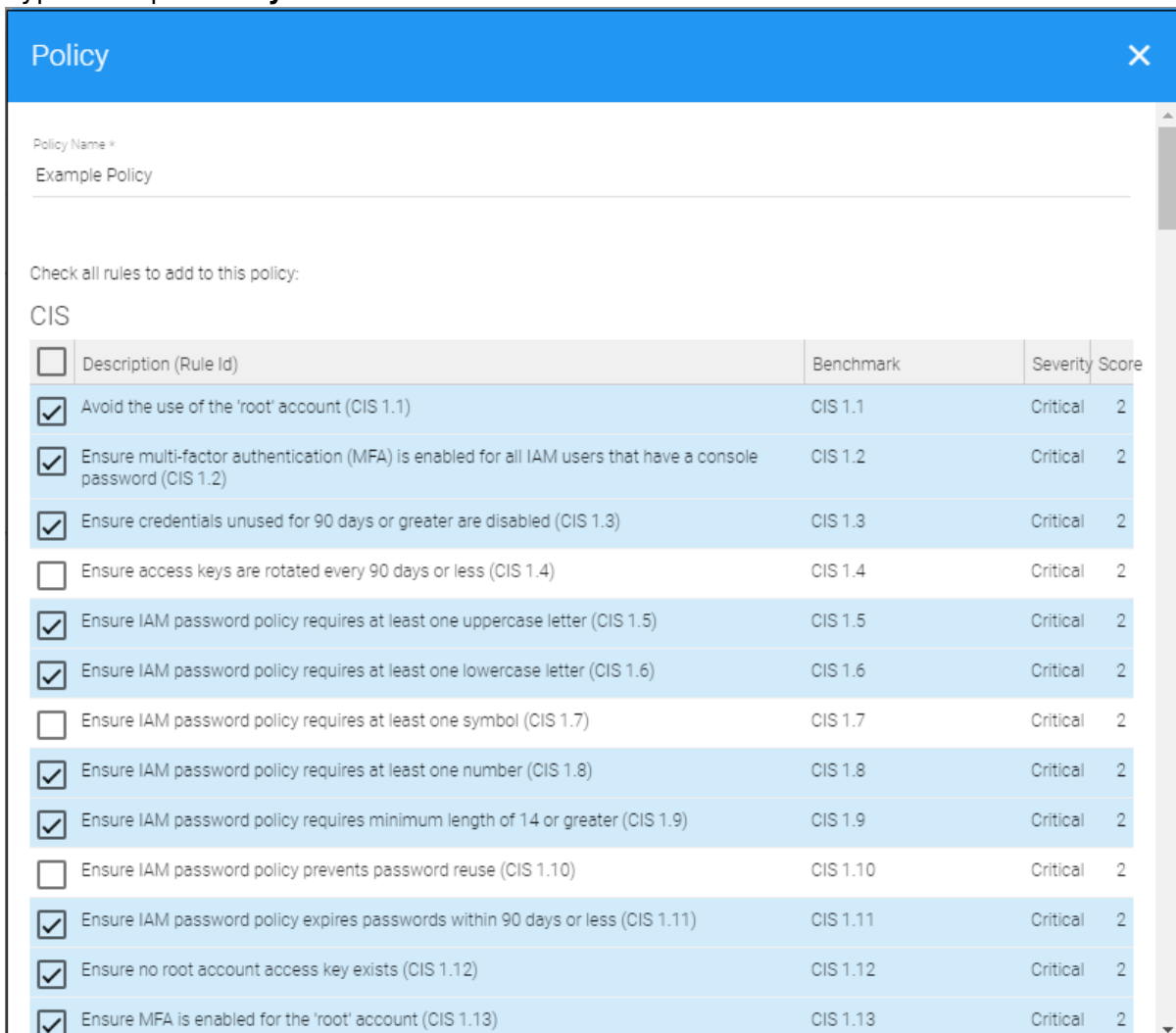
<https://campus.barracuda.com/doc/78808286/>

To create a new policy in Barracuda Cloud Security Guardian:

1. Navigate to **Policy Management > Security & Compliance**.
2. In the section of the page corresponding to the cloud provider you want to work with, click **New Policy**.



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



<input type="checkbox"/>	Description (Rule Id)	Benchmark	Severity	Score
<input checked="" type="checkbox"/>	Avoid the use of the 'root' account (CIS 1.1)	CIS 1.1	Critical	2
<input checked="" type="checkbox"/>	Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (CIS 1.2)	CIS 1.2	Critical	2
<input checked="" type="checkbox"/>	Ensure credentials unused for 90 days or greater are disabled (CIS 1.3)	CIS 1.3	Critical	2
<input type="checkbox"/>	Ensure access keys are rotated every 90 days or less (CIS 1.4)	CIS 1.4	Critical	2
<input checked="" type="checkbox"/>	Ensure IAM password policy requires at least one uppercase letter (CIS 1.5)	CIS 1.5	Critical	2
<input checked="" type="checkbox"/>	Ensure IAM password policy requires at least one lowercase letter (CIS 1.6)	CIS 1.6	Critical	2
<input type="checkbox"/>	Ensure IAM password policy requires at least one symbol (CIS 1.7)	CIS 1.7	Critical	2
<input checked="" type="checkbox"/>	Ensure IAM password policy requires at least one number (CIS 1.8)	CIS 1.8	Critical	2
<input checked="" type="checkbox"/>	Ensure IAM password policy requires minimum length of 14 or greater (CIS 1.9)	CIS 1.9	Critical	2
<input type="checkbox"/>	Ensure IAM password policy prevents password reuse (CIS 1.10)	CIS 1.10	Critical	2
<input checked="" type="checkbox"/>	Ensure IAM password policy expires passwords within 90 days or less (CIS 1.11)	CIS 1.11	Critical	2
<input checked="" type="checkbox"/>	Ensure no root account access key exists (CIS 1.12)	CIS 1.12	Critical	2
<input checked="" type="checkbox"/>	Ensure MFA is enabled for the 'root' account (CIS 1.13)	CIS 1.13	Critical	2

4. Select the benchmarks you want to use for this new policy.

- Select the checkbox in the top line of CIS, PCI DSS, HIPAA, NIST, and/or Custom policies to select all of the policies under that heading.
 - If you choose, clear any checkboxes for policies you don't 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 either AWS or Azure.

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

After you create policies, enable them in regions. Refer to [Enabling Policies in a Region](#) for details.

Figures

1. policies.png
2. examplePolicy.png

© Barracuda Networks Inc., 2020 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.