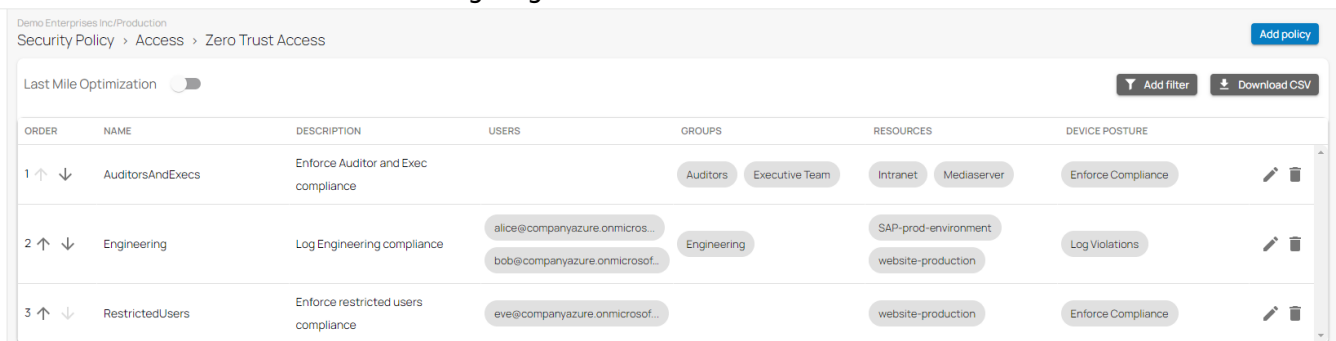


## Zero Trust Access Policies

<https://campus.barracuda.com/doc/98223646/>

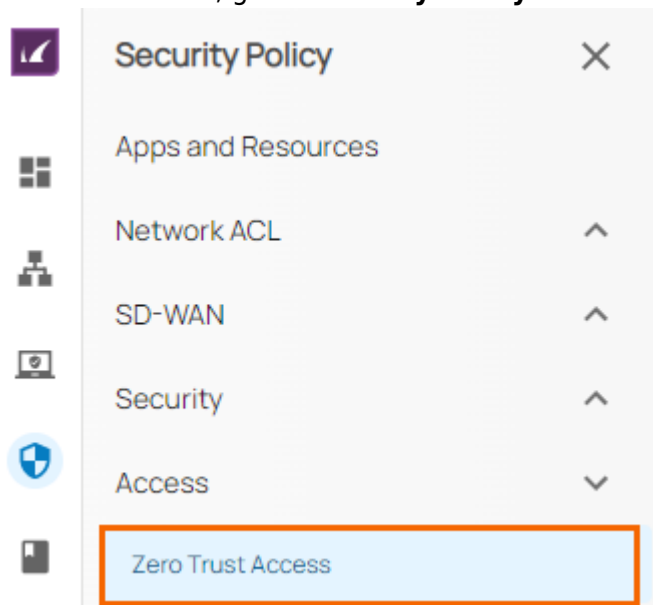
Barracuda SecureEdge allows administrators to define a number of policies that specify the access requirements associated with the various resources that the Barracuda SecureEdge Agent can connect to. As with SD-WAN and security policies, there is a zero trust access policy per workspace or tenant. The Barracuda SecureEdge Agent allows users or groups of users to connect to different resource types like custom apps or public endpoints such as SaaS services. The policies also define the security attributes, such as the security inspection and device posture of the device itself, that must be in place to grant access. A zero trust access policy defines the resources made available to end users of the Barracuda SecureEdge Agent and the associated access restrictions.



ORDER	NAME	DESCRIPTION	USERS	GROUPS	RESOURCES	DEVICE POSTURE
1	AuditorsAndExecs	Enforce Auditor and Exec compliance		Auditors, Executive Team	Intranet, Mediaserver	Enforce Compliance
2	Engineering	Log Engineering compliance	alice@companyazure.onmicrosof..., bob@companyazure.onmicrosof...	Engineering	SAP-prod-environment, website-production	Log Violations
3	RestrictedUsers	Enforce restricted users compliance	eve@companyazure.onmicrosof...		website-production	Enforce Compliance

## Create a Zero Trust Access Policy

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, go to **Security Policy > Access** and click **Zero Trust Access**.



3. The **Zero Trust Access** page opens. To create a new zero trust access policy, click **Add**

## policy.

Demo Enterprises Inc/Production  
 Security Policy > Access > Zero Trust Access

Last Mile Optimization <input type="checkbox"/>		<a href="#">Add filter</a> <a href="#">Add policy</a> <a href="#">Download CSV</a>				
ORDER	NAME	DESCRIPTION	USERS	GROUPS	RESOURCES	DEVICE POSTURE
1	AuditorsAndExecs	Enforce Auditor and Exec compliance		Auditors Executive Team	Intranet Mediaserver	Enforce Compliance
2	Engineering	Log Engineering compliance	alice@companyazure.onmicrosof... bob@companyazure.onmicrosof...	Engineering	SAP-prod-environment website-production	Log Violations
3	RestrictedUsers	Enforce restricted users compliance	eve@companyazure.onmicrosof...		website-production	Enforce Compliance

4. The **Create Zero Trust Access Policy** window opens. In the **Policy** tab, specify values for the following:

- **Name** – Enter a unique name for the policy.
- **Description** – Enter a brief description.
- In the **RESOURCES** section, specify values for the following:
  - **Resources Type** – Select a resource type. You can choose between **Internal resources (custom apps)** and **Public endpoint (SaaS)**. Note: Select either **Internal resources** for resources that are accessible internally via a point of entry or **Public endpoints** for publicly accessible resources.
    - If you select the **Internal resources (custom apps)**, the **Security Inspection** field is disabled by default.
    - If you select the **Public Endpoint (SaaS)**, the **Security Inspection** field is optional.
  - **Resources** – Select a resource from the drop-down list, or type to search.
- In the **ACCESS CRITERIA** section, specify values for the following:
  - **Users** – Select a user from the drop-down list, or type to search. Note: if no users are selected, the selected apps are accessible to all.
  - **Groups** – Select a group from the drop-down list, or type to search. Note: if no groups are selected, the the selected apps are accessible to all.
  - **Device Posture** – Select a device posture from the drop-down list. You can choose between the following:
    - **Enforce Compliance** – Device attributes are evaluated and matched to the security compliance requirements defined in the **Device Posture** tab (Step 2) of the Zero Trust Access Policy. If the defined device attributes match, the user can access the resources. Otherwise, the user cannot access the resources.
    - **Log Violations** – Device attributes are evaluated and matched to the security compliance requirements defined in the **Device Posture** tab (Step 2) of the Zero Trust Access Policy. If the defined device attributes fail, the user can access the resource. However, there is a log entry showing this violation.
    - **Disable** – If you select **Disable**, the **Device Posture** tab (Step 2) is disabled in the Zero Trust Access Policy.
  - **Security Inspection** – Click to enable/disable.

Create Zero Trust Access Policy ×

1 Policy 2 Device Posture 3 Success

**Name \*** Campus

**Description** Zero Trust Policy for Campus

**RESOURCES**

**Resource Type \*** Public endpoint (SaaS)

**Resources \*** Salesforce BetaTesting-Cloud9  
Type to search

**ACCESS CRITERIA**

**Users** user@companyazure.onmicroso...  
Type to search

**Groups** Administrators  
Type to search

**Device Posture** Enforce Compliance

**Security Inspection** ☒

**Next**

5. Click **Next**.

6. In the **Device Posture** tab, specify values for the following:

- **Screen lock enabled** – Click to enable/disable. Supported platforms: **Android** and **iOS**.
- **Firewall enabled** – Click to enable/disable. Supported platforms: **MacOS** and **Windows**.
- **Antivirus enabled** – Click to enable/disable. Supported platform: **Windows**.
- **Block jailbroken devices** – Click to enable/disable. Supported platforms: **Android** and **iOS**.
- **Enforce disk encryption** – Click to enable/disable. Supported platforms: **Android**, **Windows**, **MacOS**, and **iOS**.
- **Barracuda SecureEdge Agent updates** – Click to enable/disable. When enabled,

specify **Minimum Version** of the Barracuda SecureEdge Agent. Supported platforms: **Android, Windows, MacOS, Linux, and iOS.**

- **OS updates** – Click to enable/disable. Click + to add more than one OS platform. When enabled, specify values for the following:
  - **Platform** – You can select from the drop-down list. You can choose among the following platforms: **Android, Windows, MacOS, and iOS.**
  - **Minimum Version** – Specify the minimum version of the operating system.

Create Zero Trust Access Policy ×

✓  
Policy

**2**  
Device Posture

3  
Success

i

Screen lock enabled

☒

i

Firewall enabled

☒

i

Antivirus enabled☒

i

Block jailbroken devices☒

i

Enforce disk encryption☒

i

Barracuda SecureEdge Access Agent updates☐

i

OS updates☐

Back

**Save**

7. Click **Save**.

8. In the **Create Zero Trust Access Policy** window, verify the status of newly created zero trust access policy.

Create Zero Trust Access Policy ×

New Zero Trust Access policy created successfully.

**Finish**

9. Click **Finish**.

After the configuration is completed, your zero trust access policy is created. On the **Zero Trust Access** page, you can see the new zero trust access policy.

Demo Enterprises Inc/Production  
Security Policy > Access > Zero Trust Access Add policy

Last Mile Optimization ☐ Add filter Download CSV

ORDER	NAME	DESCRIPTION	USERS	GROUPS	RESOURCES	DEVICE POSTURE	
1	AuditorsAndExecs	Enforce Auditor and Exec compliance		Auditors Executive Team	Intranet Mediaserver	Enforce Compliance	
2	Engineering	Log Engineering compliance	alice@companyazure.onmicrosof... bob@companyazure.onmicrosof...	Engineering	SAP-prod-environment website-production	Log Violations	
3	RestrictedUsers	Enforce restricted users compliance	eve@companyazure.onmicrosof...		website-production	Enforce Compliance	

## Edit an Existing Zero Trust Access Policy

1. Expand the **Access** menu on the left and select **Zero Trust Access**. The **Zero Trust Access** window opens.
2. Click on the pencil icon next to the policy you want to edit.

Demo Enterprises Inc/Production  
Security Policy > Access > Zero Trust Access Add policy

Last Mile Optimization ☐ Add filter Download CSV

ORDER	NAME	DESCRIPTION	USERS	GROUPS	RESOURCES	DEVICE POSTURE	
1	AuditorsAndExecs	Enforce Auditor and Exec compliance		Auditors Executive Team	Intranet Mediaserver	Enforce Compliance	
2	Engineering	Log Engineering compliance	alice@companyazure.onmicrosof... bob@companyazure.onmicrosof...	Engineering	SAP-prod-environment website-production	Log Violations	
3	RestrictedUsers	Enforce restricted users compliance	eve@companyazure.onmicrosof...		website-production	Enforce Compliance	

3. The **Edit Zero Trust Access Policy** window opens. Edit the value you are interested in.
4. Click **Save**.

## Remove an Existing Zero Trust Access Policy

1. Expand the **Access** menu on the left and select **Zero Trust Access**. The **Zero Trust Access** window opens.
2. Click on the trash can icon next to the policy you want to remove.

Demo Enterprises Inc/Production  
Security Policy > Access > Zero Trust Access Add policy

Last Mile Optimization ☐ Add filter Download CSV

ORDER	NAME	DESCRIPTION	USERS	GROUPS	RESOURCES	DEVICE POSTURE	
1	AuditorsAndExecs	Enforce Auditor and Exec compliance		Auditors Executive Team	Intranet Mediaserver	Enforce Compliance	
2	Engineering	Log Engineering compliance	alice@companyazure.onmicrosof... bob@companyazure.onmicrosof...	Engineering	SAP-prod-environment website-production	Log Violations	
3	RestrictedUsers	Enforce restricted users compliance	eve@companyazure.onmicrosof...		website-production	Enforce Compliance	

3. The **Delete Zero Trust Access Policy < Name of Zero Trust Access Policy >** window

opens.

4. Click **Ok** to confirm.

## Figures

1. ZTA page.png
2. goto-zero-trust-access.png
3. ZTA-AddPolicy.png
4. ZTA-Policy.png
5. ZTA\_AccessCriteria.png
6. ZTA-devPosture.png
7. ZTA-Finish.png
8. ZTA page.png
9. EditZTA.png
10. delZTA.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.