Device Classification

https://campus.barracuda.com/doc/99616901/

This feature is used to classify end user devices as Personal, Managed, or Supervised. This powerful tool provides the following for the various roles in your organization:

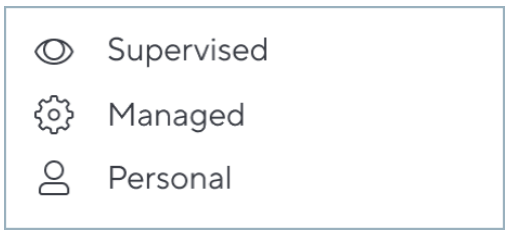
- IT administrators can classify devices as Personal, Managed, or Supervised in order to better manage and secure corporate devices.
- Users may want to know how their devices are classified so that they can understand how the device is being managed and secured.
- Security analysts can identify and report on the number of Personal, Managed, or Supervised devices in use, providing a better understanding of the organization's overall security posture.
- Compliance officers can ensure that all Personal devices are properly managed and secured, enabling the organization to meet regulatory requirements.
- Managers want to be able to monitor the usage of each classification of devices within their teams so that they can ensure that company resources are being used appropriately.

Configure Device Classification on the **Devices > Settings** page:

- *Supervised* – The Tamperproof feature is allowed and your organization's Web Security policies are enforced.
- *Managed* – The Tamperproof feature is disabled, and your organization's Web Security policies are enabled, but optional (user can opt-out).
- *Personal* – The Tamperproof feature and Web Security features are disabled. Your organization CANNOT see the web traffic on the device, even if the CloudGen Access app is installed and running.

When a device is enrolled in CloudGen Access, its device classification is determined by the Enrollment Slot (*Managed*, *Supervised*, or *Personal*) selected by the admin for that user. On the **Identity > Users** page, when creating an invitation for a new user, choose the device classification in the **New User** popup under **Enrollment Settings**.

You can also bulk edit the classification of devices. *Devices already enrolled* in CloudGen Access when the Device Classification feature was introduced were classified as *Supervised*. On the **Devices** page, the **Classification** column shows how each device is classified using the following icons:



Use the Filter on the **Devices** page to list all devices of a specific classification.

Device Invitations

On the **Identity > Users** page, when you click **+** to add a new user, a popup will prompt you with enrollment settings:

1. Enter the **User Name**, **Email**, and select the **Group**(**s**) the user belongs to.
2. Toggle **Send Email Invitation** to *ON* or *OFF*. If *ON*, an email invitation is sent to new users with enrollment instructions.
3. Select a Device Classification for the user: *Supervised, Managed,* or *Personal.*

Changes to Device Classification

To change the classification of a device, or a group of devices (bulk), see How to Change Device Classification. The user's consent is required to complete the update to the new classification in the following cases:

- From *Managed* to *Supervised*
- From *Personal* to *Supervised* or *Managed*

Important:

- The device user will be sent a notification email by the CloudGen Access agent stating the new classification and, if applicable per described above, requesting the consent of the user. If the device classification is changing from *Supervised* to *Managed*, or to *Personal*, the user is simply sent a notification email by the agent stating the new classification. See the Example Notification Email for Change in Device Classification.
- If the user does not respond to the email notification requesting their consent to the change in classification within 10 days, a red dot (badge) will appear on the icon for that device in the **Classification** column on the **Devices** page.

Upon change in classification:

- Personal – After assigning this classification, Tamperproof and Web Security are disabled.
- Managed – After assigning this classification, Tamperproof is disabled, and Web Security is enabled, but optional (user can opt-out).
- Supervised – Tamperproof is allowed and Web Security is enforced.

Figures