How to Scan a Site - The New Scan/Configuration Page

https://campus.barracuda.com/doc/97520312/

The **New Scan**/**Configuration** page makes it easy for you to scan sites so you can help your customers understand their security vulnerabilities and how to improve them. On this page, you:

- enter your scan credentials
- choose the network IP range to scan
- choose devices to scan
- understand which devices cannot be scanned
- start the scan

The Barracuda Site Security Scanner scans Windows sites only. Linux and Apple devices are not scanned.

Barracuda Site Security Scanner

![Barracuda logo] Barracuda.
Your journey, secured.

(1) ⚙ Configuration **(2)** Security Professional 👤

⚙
CONFIGURATION

📊
RESULTS

(3) Scan Credentials

ACCOUNT TYPE ⓘ   USER NAME *

DOMAIN NAME ⓘ   PASSWORD *
                                                            👁

VALIDATE

(4) Scan Details   **(5)**   **(6)**

DETECTED NETWORKS ⓘ   RESET   ADD IP RANGE

1:   IP   2:   IP

3:   IP   4:   IP

(7)   GET DEVICES LIST   CANCEL

(8) Devices To Scan (5) ⓘ   **(9)** Unknown Devices (19) ⚠   **(10)** SCAN NOW

(11)

Unknown devices can potentially be identified and scanned by first running a preparation tool on the device itself. This tool ensures that all of the necessary firewall and registry settings are configured to identify the device so that it can be scanned. It will then revert those changes once the tool is uninstalled, which can be done anytime after the scan completes.

☁ DEVICE PREP TOOL

| IP ADDRESS	DEVICE NAME ↑	OS	REASON
10.65.2.24	AZURE-INT02	Unknown	Access Denied
10.65.2.23	AZURE-INTEGRATI	Unknown	Access Denied
10.65.2.37	BNSEC-DSS	Unknown	Access Denied
10.65.2.15	DEMOSC2019	Unknown	Access Denied
10.65.2.14	HYDRA-SERVER201	Unknown	Access Denied
10.65.2.35	HYDRA-SRV2008R2	Unknown	Access Denied
10.65.2.34	Hydra-Srv2012r2.Mw.Cudaops.Com	Unknown	Access Denied
10.65.2.38	HYDRA-SRV2016-1	Unknown	Access Denied
10.65.2.36	Hydra-Ubuntu-20.Internal.Cloudapp.Net	Unknown	WMI Ports Are Closed
10.65.2.27	HYDRA-WIN10	Unknown	Access Denied

(12)

You have 30 days left in the 30-day product period

|< < **1** 2 > >| Items per page 10 ▾   1-10 of 19

To navigate to the **New Scan/Configuration** page after you have completed a scan, click **New**
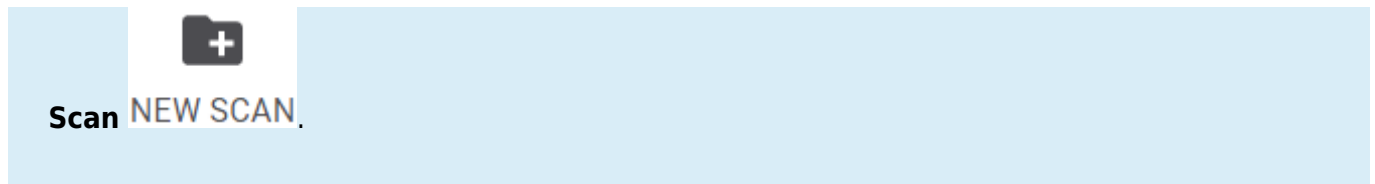
Scan NEW SCAN.

1. The **New Scan**/**Configuration** page is where you set up and run scans.

2. The Profile area lets you edit your profile. Click the icon.

3. The **Scan Credentials** area is where you identify your account type (**Domain Account** or **Local Admin Account on Target Device**), the name of the domain you want to scan, and the credentials of a domain admin with rights to access the domain.

4. The **Scan Details** area is where you choose the range of IP addresses to scan. One or more IP ranges is automatically detected when you validate your credentials for your site. Click **Get Devices List** when you want to get a list of devices in that range.

5. **Reset** clears any IP ranges you have added and shows only the detected range or ranges.

6. **Add IP Range** lets you add another range of IPs to scan.

7. Click **Get Devices List** to get the devices in the range.

8. Once you click **Get Devices List**, the **Devices** area is populated with two lists of devices. **Devices to Scan** shows the devices that are available to scan.
   - You can clear the check boxes of any device you want to exclude from the scan.

9. Click the **Unknown Devices** tab to show the devices that can't be scanned. See the **Reason** column for the reason the device can't be scanned.

10. Click **Scan Now** to start the scan.

11. Click to download the Device Prep Tool. See What To Do About Unknown Devices and Unassessed Assets.

12. This area displays the number of days you have left before your product expires.

Figures

1. Config_page_numbers.png
2. New Scan Button.png
3. profile.png