About Scan Configuration

https://campus.barracuda.com/doc/90440433/

This page provides the following topics:

Scan Configuration

After you install Onsite Manager, the first scan runs automatically, without the need to manually configure the settings. However, you may want to change the scan range and frequency values set for device and asset discovery. See Setting the Device Discovery Defaults.

Onsite Manager is installed from Service Center. For information on setting Onsite Manager installation defaults, see Setting Onsite Manager Installer Preferences. For information on installing Onsite Manager, see the *Setup Guide.*

Configuring the Scan

You can configure the scan by:

- adding individual IP addresses, ranges of IP addresses, IP subnets or any combination of these
- skipping individual IP addresses or ranges of IP addresses
- excluding devices from the scan
- deleting individual IP addresses, ranges of IP addresses, IP subnets or any combination of these that have been previously configured

Notes

- When configuring the Onsite Manager scan, add only the addresses for the devices that should be monitored. Having extra devices can lead to unwanted database growth and licensing issues.
- Do not include addresses that end in .255 or .0, as these are not valid IP addresses.

- The scan automatically attempts to scan up to 65540 IPs based on the subnet mask information collected from Onsite Manager, if the network is configured as **Class B**. The purpose of this is to isolate any devices that could be present in the network and bring that information back into the Service Center so you can gain insight to what is within the network and what should be managed. In some **Class B** networks, the scan interval can take up to 15 minutes to complete this configuration. If this is a concern and you wish to decrease the interval, it is recommended that you either alter the scan settings after the automatic scan has occurred, or not use automatic scan in these networks and instead manually configure the scan range.

Process for Network Discovery

Onsite Manager queries each IP address defined in the network scan using an **ICMP ECHO** request. An **ARP** cache retrieval is also performed to detect IP addresses on the local subnet that may not respond to the **ICMP ECHO** request. Each IP address that responds is further scanned to determine its identity.

To identify...	Onsite Manager...
A-name	Queries the reverse lookup zone in DNS and then validates with the forward lookup zone.
Machine name	Uses WMI calls.
sysName	Uses SNMP calls.
MAC addresses	Uses WMI or SNMP calls.

Onsite Manager uses a combination of device protocols to identify devices, including:

- **SSH**
- **Zeroconf**
- **NetBIOS**

All the collected identifying factors are used to create discovery variables, which are then compared against each known device to see if a match can be found. If a match is found, the IP address is associated with the known device. If no match is found, a new device is created.

- Onsite Manager always discovers itself regardless of whether it is in the scan range.
- Device Managers do not have scan settings for device discovery because it is only responsible for discovering the device on which it is installed.

Avoiding Issues with Network Discovery

Any or all the following actions help Onsite Manager classify unique devices and avoid issues with network discovery:

- Enable a management protocol (such as **WMI**, **SNMP**, or **SSH**) on each device.
- Assign static IP addresses to devices that do not have a management protocol enabled.
- Assign unambiguous DNS names to the device so that it is uniquely reverse resolvable.

© Barracuda Networks Inc., 2021 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.