Configuring Service Center - Hosted

https://campus.barracuda.com/doc/86544921/

After logging in to Service Center, there are several operation settings that you must configure.

Configuring the Alert Settings

Service Center is able to use any email address and mail server you provide to issue email alerts and system notifications. The address you provide will also be used as the reply-to address for report delivery schedules, so it is a good idea to have someone watch the address for responses from customers.

You can also use the Alerts Setting to have the system check for any possible monitoring failures (such as which monitor is not collecting data). If enabled, Administrators will receive email reports regarding failures on the selected interval (hourly, daily or weekly). Regularly reviewing these reports with your team will help you streamline your monitoring strategy.

Configuring the Monitoring Failure Settings

Barracuda Managed Workplace can track the status of monitor failures and send email reports to administrators. Monitor failures are when data being requested cannot be collected from a managed device. This can occur when there are environmental problems or configuration issues.

Examples of environmental problems are firewalls blocking access to WMI ports or corrupt WMI repositories.

Configuration issues are when users have applied monitoring policies or device level monitors to devices that cannot respond. Examples of this would be applying the Apple OS X or Cisco Firewall monitoring policies to Windows devices.

1. In the **Monitoring Settings** section, select the **Enable Log Monitoring** check box.
2. Select how frequently the system will run an audit (hourly, daily or weekly).
3. Click **Save**.

Scanning for Devices

You can define which device IP addresses you want the Onsite Manager to manage. Configuring the network scans and running the initial scan is done in the Site Management dialog box of Service Center. The initial network scan

must run manually after you have configured it, but will run automatically thereafter.

Configuring Scan Intervals

There are two intervals used to determine how frequently Onsite Manager and Device Managers update information:

Device Discovery The Device Discovery interval is how long an Onsite Manager will wait following a network scan before initiating another. By default, 5 minutes will elapse between the end of a scan and the beginning of the next one.

Important: Device availability alerts rely on the amount of time that has gone by since the last time Onsite Manager received a response during a network scan. If you extend this interval, you are also increasing how long it takes to determine a device is down for the purposes of alerting.

Asset Discovery The Asset Discovery interval is the time frame within which all known devices must have asset data collected. Data collection for all devices is distributed through the entire period. By default, each device will have its assets collected once every four hours.

You can configure these scan intervals in Service Center, by clicking Configuration, and then clicking Site Management. Click the site name, and then click the Network Discovery tab.

Running an Initial Scan

When first configuring the Onsite Manager scan options, the initial scan must be run manually and it may take some time before the results appear, depending on the number of devices being scanned.

When the scan completes, check to make sure that each discovered device has at least one management protocol (WMI or SNMP) enabled. This allows Onsite Manager to accurately identify a device.

To avoid any issues with discovery, you must do one of the following:

- Enable WMI or SNMP on each managed 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.

Any or all the above actions will help Onsite Manager intelligently classify unique devices.

To run a network scan manually

1. In Service Center, click **Configuration** > **Site Management**.
2. In the **Site Name** column, click the site for which you want to perform a network scan.
3. Click the **Network Discovery** tab.
4. In the **Network Scan (Local Network)** section, click **Scan Now.**

Limiting the IP Addresses to Scan

You can configure the network scan to skip individual or ranges of IP addresses. Wherever possible, you should scan the smallest number of IP addresses which will ensure you still discover all required devices.

Best Practice: Using static IP addresses for devices, and controlling DHCP scopes and subnets are valuable tools to ensure you do not pick up devices you are not obligated to monitor for your clients. For example, you may have clients which allow their employees or customers to use wifi at their location. Configuring a separate subnet or private network range for the router is an easy way to ensure you are not discovering transient consumer grade devices such as iPads or Android phones.

1. In Service Center, click **Configuration** > **Site Management**.
2. Click the site for which you want to edit the scan settings.
3. Click the **Network Discovery** tab.
4. In the **Network Scan (Local Network)** section, click **Modify**.
5. In the **Scan Settings** section, click **Add**.
6. Do one of the following:
    - To ignore a single IP address, select the **Single** option button and type the device IP address in the **IP Address** box.
    - To ignore a range of IP addresses, select the **Range** option button and type the **Start IP Address** and **End IP Address** in the boxes. Type a description, if desired.
7. Select the **Skip** check box.
8. Click **Save**.

Scanning Intel® vPro™ Devices

To prepare Intel® vPro™ devices for discovery, you must provide the Global Intel® AMT credentials in Service Center. Global site credentials will be used

where valid unless you specify an exception with explicit device credentials. Once the Intel® AMT Administrator account credentials are successfully configured, Barracuda Managed Workplace can remotely power up and power down the device, monitor events, generate alerts, and collect asset information.

1. In Service Center, click **Configuration** > **Site Management**.
2. Click the name of the site for which you want to run the scan.
3. Click the **Network Discovery** tab.
4. Under **Network Scan**, click **Modify**.