Configuring Service Center - On Premise

https://campus.barracuda.com/doc/85493139/

Some information required for operation is not collected during Service Center setup, so you must make some choices and complete the configuration once the application is up and running.

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 Your Email Settings

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Alert Configuration** tab.
3. In the **Message Settings** section, type an email address in the box.
   Depending on the configuration of the SMTP server, this may need to be a valid email address.
4. In the **SMTP Settings** section, do the following:
   1. Type the IP address or FQDN for the SMTP Server in the **Server Name** box.
   2. Enter the **Server Port.** The default SMTP port is 25.
   3. Check **Requires TLS** if your mail server requires transport layer security.
   4. Choose either **Anonymous** or **Basic Authentication**. Basic Authentication requires you to also enter a username and password.
5. Click **Save**.

Testing Your Email Settings

1. In the **Send Test Email** section, enter the address to which the test email is sent.
2. Enter a subject line for the email.
3. Click **Send**.
   A window appears with either a success message or details regarding any errors.
4. Click **Close**.

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**.

Configuring a Modem

If a modem is installed on the application server and you want alert notifications to be sent to alphanumeric pagers, follow the procedure below to provide Service Center with the information it needs to use the modem.

Note: Modems are not supported for Barracuda Managed Workplace 2013 R1 and later.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Modem** tab.
3. In the **Modem Configuration** section, select the appropriate values for each box.
   COM Port The communications port to which the internal or external modem is connected.
   Baud Rate The communication speed the Pager Service supports.
   Parity Depending on the pager protocol used by the Pager Service, None, Odd, Even, and Mark will be set. (Contact the pager service for details if this information is not known.)
   Data Bits Depending on the pager protocol used by the Pager Service, this will be set to 7 or 8 Data Bits. (Contact the pager service for details if this information is not known.)
   Stop Bits The number of bits indicating the end of a byte. Typically this setting should be 1.
4. Click **Save**.

Testing the Modem

You can send a test message for confirmation that the modem is functional with Service Center.

1. Enter the paging service modem number. If you are using a phone system that requires a prefix to call out, include it. If a pause is required, use a comma for each second.
   PIN Pagers require an ID number.
2. Enter the ID number if required. (Contact the pager Service for details if this information is not

known.)
3. Enter the callback number.
   The callback number is a numeric string sent to a pager indicating a problem has been detected.
4. Enter the value to wait (seconds).
   Some pager services have a default message that is played each time your pager number is dialed. To pause the Alert until the message has completed, specify the number seconds required.
5. Click **Send**.

Configuring Data Retention

Your data retention settings define how much history you retain in Service Center. Keeping a long history is beneficial to establish trends, but the more history retained, the larger the database footprint on disk.

On a weekly basis, Service Center reviews timestamps of data and purges any data older than the value you define. The default setting is to retain 400 days of data.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Data Retention** tab.
3. Enter the number of days of data to keep.
4. 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. 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.

1In Service Center, click Configuration > Site Management.

2Click the name of the site for which you want to run the scan.

3Click the Network Discovery tab.

4Under Network Scan, click Modify.