

Configuring the Alert Settings - On Premise

<https://campus.barracuda.com/doc/98220485/>

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 - On Premise

Barracuda RMM 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 macOS 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**.

© Barracuda Networks Inc., 2024 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.