Customizing Service Center

https://campus.barracuda.com/doc/88114116/

Setting Refresh Options for the Central Dashboard and Alert Lists

You can set the auto-refresh times for the Central Dashboard and for Alert lists.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **General** tab.
3. To set the auto-refresh time for the Central Dashboard, enter a value in minutes on the **Central Dashboard Refresh Rate** box.
4. To set the auto-refresh time for the Alerts listing, enter a value in minutes in the **Alerts Refresh Rate** box.
   Note: The **Alerts Viewer** is a live view that displays alerts as they are received by Service Center. The auto-refresh settings have no effect on its operations.
5. Click **Save**.

Enabling or Disabling Website Usage Tracking

To help track which pages are most used in Service Center and in the online help, website tracking usage is automatically enabled. Web tracking usage is powered by Google Analytics, and all statistics gathered are private and not used for any other purpose. However, you can disable web tracking usage if preferred.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **General** tab.
3. To prevent Google Analytics from tracking the pages clicked in Service Center, clear the **Enable website tracking usage** check box.

Setting Regional Preferences

You can set the default languages for Service Center and reports. You can also set a default font for reports, and create font exceptions for additional report languages, if desired. For example, you can set your default report language to English, and assign Verdana as the default font. Then, you can create font exceptions by applying different fonts to other report languages. For example, you can specify that Japanese reports use Gothic, or German reports use Arial.

Changing the font for reports does not change the font for existing reports; the selected font will only be applied to new reports going forward.

To set default locales for Service Center and reports

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **General** tab.
3. In the **Regional Preferences** section, click **Modify**.
4. From the **Default locale for UI** list, select a language for the Service Center UI.
5. From the **Default locale for reports** list, select a default language for reports.
6. Click **Save**.

To set the default font for reports

1. In Service **Center**, click **Configuration** > **System Settings**.
2. Click the **General** tab.
3. In the **Regional Preferences** section, click **Modify**.
4. In the **Default Report Fonts** area, from the **Default font** list, select a default font that will be applied to all reports.
5. Click **Save**.

To create font exceptions for report languages

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **General** tab.
3. In the **Regional Preferences** section, click **Modify**.
4. Click **Add**.
5. From the **Language** list, select a language.
6. From the **Font** list, select a font.
7. Click **Save**.
8. # In Service Center, click **Configuration** > **System Settings**.
9. Click the **General** tab.
10. In the **Regional Preferences** section, click **Modify**.
11. Select the check box beside the report language you want to edit.
12. Click **Edit**.
13. Make any changes as required.
14. Click **Save**.

To delete font exceptions for report languages

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **General** tab.
3. In the **Regional Preferences** section, click **Modify**.
4. Select the check box beside the report language you want to delete.
5. Click **Delete**.

When you delete a font exception for a report language, any future reports created in that language will use the default font for reports. Existing reports in that language will continue to use the font that had been selected as the exception.

Setting Onsite Manager Installer Preferences

You can set the default installation configuration settings for Onsite Manager, including whether to install optional components such as SQL Server Management Studio Express. During the installation, these settings can be overridden by choosing to perform an advanced installation.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **General** tab.
3. In the Onsite Manager Installer Settings area, click **Modify**.
4. To change the default Onsite Manager installation path, select the **Custom Location** check box, and in the **Full installation path** box, type a new path.
5. To prevent Onsite Manager from automatically scanning the local subnet, clear the **Auto Scan** check box.
6. To change the root path for the Microsoft SQL Server Express instance, in the Microsoft SQL Server Express area, select the **Custom Location** check box, and in the **Full installation path** box, type a new path.
7. In the Microsoft SQL Server Management Studio Express area, select the **Install Component** check box to install SQL Server 2008 R2 Management Studio Express.
8. Click **Save**.

Adding or Deleting Performance Counters

The **Network Objects** tab provides a list of all Performance Counters that are available for monitoring. Additional Performance Counters can be added here, or any that are not in use can be removed.

To add a Performance Counter to the Service Center database manually

The **WMI Class Name** and **WMI Property Name** boxes are used for non- English monitoring with Barracuda Managed Workplace. A Barracuda Managed Workplace script called Get Performance Counter Class can be used to determine the WMI class and properties if you do not know these.

1. In Service Center, click **Configuration** > **System Settings**.

2. Click the **Network Objects** tab.
3. In the **Performance Counters** section, click **Add**.
4. Do one of the following:
   - Select the Performance Object from the **Performance Object** list.
   - If the Performance Object does not exist, select the **Other** check box, and enter the Performance Object in the box that appears.
5. Do one of the following:
   - Select the Object Instance from the **Object Instance** list.
   - If the Object Instance does not exist, select the **Other** check box, and enter the Object Instance in the box that appears.
6. Do one of the following:
   - Select the WMI Class Name from the **WMI Class Name** list.
   - If the WMI Class Name does not exist, select the **Other** check box, and enter the WMI Class Name in the box that appears.
7. Do one of the following:
   - Select the WMI Property Name from the **WMI Property Name** list.
   - If the WMI Property Name does not exist, select the **Other** check box, and enter the WMI Property Name in the box that appears.
8. Click **Save**.

To delete a Performance Counter from the Service Center database manually

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Network Objects** tab.
3. Select the check box beside the performance counter you want to delete.
4. In the **Performance Counters** section, click **Delete**.

This Performance Counter will no longer be available for monitoring. Any monitors or monitoring policies currently using this counter will no longer be able to capture this data, but the historical information will still be available for reporting.

See Also

Adding a Monitor for Performance Counters

Adding or Deleting SNMP OIDs

The **Network Objects** tab provides a list of all SNMP OIDs that are available for monitoring. Additional SNMP OIDs can be added here, or any that are not in use can be removed.

There are two types of MIBs: scalar and tabular. Scalar objects define a single object instance whereas tabular objects define multiple related object instances grouped in MIB tables. You can choose to collect tabular OIDs.

You can create a tabular monitor for a known base OID, and Barracuda Managed Workplace will automatically create monitors for all elements within that table.

> Onsite Manager pulls a maximum 1,024 scalar monitors from each tabular monitor definition.

To add an SNMP OID to the Service Center database manually

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Network Objects** tab.
3. In the **SNMP OIDs** section, click Add.
4. Type the Object Name.
5. Type the OID.
6. From the **Object Type** list, select either **Numeric** or **Text**.
7. To collect tabular OIDs, select the **Tabular** check box.
8. If desired, in the **Description** box, type a description of the OID.
9. Click **OK**.

To remove an SNMP OID from the Service Center database manually

> An SNMP OID cannot be removed if it is used by any monitoring rule.

An SNMP OID cannot be removed if it is used by any monitoring rule.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Network Objects** tab.
3. Select the check box beside the SNMP OID you want to delete.
4. In the **SNMP OIDs** section, click **Delete**.

This SNMP OID will no longer be available for monitoring, but the historical information will still be available for reporting.

See Also

Adding a monitor for SNMP Object Identifiers (OIDs)

Adding or Deleting a Custom Network Service

The Network Objects tab provides a list of all Network Services that are available for monitoring.

Additional Network Services can be added here, or any that are not in use can be removed.

When you add a custom network service, it becomes available when configuring monitors, but it will not be automatically detected by the network scan.

To add a network service to the Service Center database manually

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Network Objects** tab.
3. In the **Network Services** section, click **Add**.
4. Type the name of the Network Service in the **Name** box.
5. Type the port number in the **Port** box.
6. Type the protocol in the **Transport Protocol** box.
   Only TCP is currently supported.
7. Type the timeout in milliseconds in the **Timeout** box.
8. Click **OK**.

To remove a network service to the Service Center database manually

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Network Objects** tab.
3. Select the check box beside the network service you want to delete.
4. In the **Network Services** section, click **Delete**.

See Also

Adding a Monitor for Network Services

Setting How Long to Keep the Data

You can modify the data retention values on a global level, which allows you to keep only the data that is required. This helps to manage the disk footprint of the database.

This value is set to ensure that while users are on vacation and their system is off, it does not get deleted as a stale device.

For hosted versions of Service Center, the data retention time is limited by the value set by the host. The host can set a limit for each VAR.

When a device is not responding to the Onsite Manager discovery scan, Service Center retains full asset, description and addressing information for the device, unless another device picks up the same IP address, at which point the IP is marked as stale on the original device. When a workstation picks up a new IP address, the old address is discarded and only the current address is displayed.

Workstation class computers have only a single IP address tracked by Barracuda Managed Workplace, even when multiple interfaces are being scanned with separate addressing, and all other IP addresses are removed by the stale IP process.
Unlike Workstations, there is no stale IP address cleanup routine run against any server-class Windows device or SNMP device.

In some cases, devices that have been removed may continue to be referenced in Service Center as unavailable devices until the specified interval specified triggers the next clean-up. As a remedy, you can specify a shorter interval for cleaning up stale IP addresses, or you can remove devices with stale IP addresses manually.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Data Retention** tab.
3. Type a value in days in the **Number of Days of Data to Keep** box.
4. Click **Save**.

See Also

About Deleting Devices

Viewing or Changing the Communication Settings

The **Communication Settings** tab allows you to

- view or modify the information provided to Onsite Managers and Device Managers to enable communications with Service Center
- view or modify the information provided to Onsite Managers and Device Managers to enable the remote control capabilities available in Service Center

In hosted Service Centers, you can view the communications settings. In on-premise Service Centers, you can change the communications settings.

To view the Service Center website communication settings

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Communication Settings** tab.

To change the Service Center website communication settings

Changing the Service Center website communication settings is only available for on-premise Service Centers.

The information in the Service Center Website Communication Settings section is automatically populated with the following URLs:

- Public Service Center URL
- Public SCMessaging URL
- Internal SCMessaging URL
- Update Service Public URL
- Update Service Internal URL
- Update Service DSS Sync Public URL

The public URLs are the Internet-facing addresses to which Onsite Managers and Device Managers will report. The internal addresses perform the same function, but work on the same network as the Service Center application server, where a different address may be required due to networking concerns.

These URLs are provided during the installation of Service Center, and may be required for Device Managers and Onsite Managers to access Service Center from both within and outside of a firewall. This information can be modified, if required. The information is provided to Device Managers and Onsite Manager to enable communications with Service Center.

The Public SCMessaging URL must point to the scwebservices.asmx file, which is used to provide the communications.

- The web page that appears when you browse this URL only provides a mechanism for receiving data and does not confirm that there are no communications issues between Onsite Manager and Service Center.
- Not all features are available if you are accessing the Service Center using a URL that is something other than what appears as the public SCMessaging URL.
- If you change any communication settings, you must restart the Service Center Monitor Windows service on the application server before the changes will take effect.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Communication Settings** tab.
3. In the **Service Center Website Communication Settings** section, click **Modify** .
4. Modify the **Public Service Center URL** and the **Public SCMessaging URL** boxes as required.
5. Click **Save**.

Setting Default Email Options

You can use the **Alert Configuration** tab to configure the From email address and the SMTP server address so that Service Center can send email alerts and system notifications.

To set the default email address

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Alert Configuration** tab.
3. In the **Email Settings** section, type an email address in the **Message Settings** box.

Depending on the configuration of the SMTP server, this may or may not need to be a valid email address. Most mail servers now verify that a real email address is used. They will bounce or capture messages with a fictive address in mail filters. The mail server doing the screening is linked to the email address of the recipient. If a fictive address is used in the **From** box, the message may not reach the destination if the recipient's mail server is screening messages, which is a common practice.

For alert notifications, this email address is used as the From address. For report delivery s, this email address is used as the Reply To address.

To set the SMTP options

The SMTP options are only available for on-premise Service Centers with a modem installed on the application server.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Alert Configuration** tab.
3. In the **Server Name** box, type the IP address or FQDN for the SMTP server.
4. Type the port in the **Server Port** box.
5. If Transport Layer Security (TLS) is used by the mail server to which you will be connecting, select the **Requires TLS** check box.
6. Select one of the following option buttons:
   Anonymous Allows anonymous logins.
   Basic Uses the username and password you specify for the mail server.
7. Click **Save**.

To test the email

The test email feature is only available for on-premise Service Centers.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Alert Configuration** tab.
3. In the **To** box, type a valid email address.
4. Enter a subject in the **Subject** box.
5. Click **Send**.

Turning Log Monitoring On or Off

You can have the system check for any possible monitoring failures (such as which monitor is not collecting data). If enabled, you can define the interval that you want the system to check for possible failures (hourly, daily or weekly). The Administrator can be notified when failures occur via a log in the System Viewer and a subsequent email. Email notifications can be set up to be delivered on a selected interval.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Alert Configuration** tab.
3. In the **Monitor Failure Settings** section, select the **Enable Log Monitoring** check box.
4. From the **Polling Interval** list, select the interval that you want the system to check for monitoring failures.
5. Click **Save**.

Setting System-Wide Alerting Actions for Site Communication Failures

You can set alert actions for a site not communicating at both the system level and at a site level. It is recommended that you first set your system-level defaults, and then override these defaults as needed on the site level. For more information about setting site level alert actions for site not communicating, see Setting Alerting Actions for Site Communication Failures .

Barracuda Managed Workplace includes three alerts that notify you of site communication failures:

- **Service Center Receive**—triggers when Service Center has not received information from an Onsite Manager for 65 minutes.
- **Onsite Manager Processing**—triggers when 12 hours has passed since an Onsite Manager has retrieved information, such as configuration changes, from Service Center.
- **Site Not Communicating**—status and asset information is sent to Service Center every two minutes. When two updates have been missed, and the alert conditions for both Service Center Receive and Onsite Manager Processing are met, this alert is triggered.

These three alerts form a hierarchy in which the Service Center Receive and Onsite Manager Processing alerts are subsets of the Site Not Communicating alert. The two lower-level alerts can exist simultaneously. However, if two updates have been missed in addition to the conditions required to trigger the lower-level alerts, then the Site Not Communicating alert triggers. The lower- level alerts self-heal, as they are subsumed by the Site Not Communicating alert.

The following table outlines which alerts are triggered for various combinations of site communication failure conditions:

What if...	**Then...**
Service Center has not received information from Onsite Manager for 65 minutes	the Service Center Receive alert is triggered.
12 hours has passed since an Onsite Manager has retrieved information from Service Center	the Onsite Manager Processing alert is triggered.
Service Center has not received information from Onsite Manager for 65 minutes and 12 hours has passed since an Onsite Manager has retrieved information from Service Center	both the Service Center Receive and Onsite Manager Processing alerts are triggered.
Service Center has not received information from Onsite Manager for 6 minutes and two updates have been missed.	the Site Not Communicating alert is triggered. Any existing Service Center Receive and Onsite Manager Processing alerts will self-heal, as the Site Not Communicating alert takes precedence.
12 hours has passed since an Onsite Manager has retrieved information from Service Center and two updates have been missed.	the Site Not Communicating alert is triggered. Any existing Service Center Receive and Onsite Manager Processing alerts will self-heal, as the Site Not Communicating alert takes precedence.
Service Center has not received information from Onsite Manager for 65 minutes and 12 hours has passed since an Onsite Manager has retrieved information from Service Center and two updates have been missed.	the Site Not Communicating alert is triggered. Any existing Service Center Receive and Onsite Manager Processing alerts will self-heal, as the Site Not Communicating alert takes precedence.

Default Settings

When a site is not communicating, Barracuda Managed Workplace creates a trouble ticket and sends an email to all users for the site whose role is set to receive alert notifications. It is also set to self-heal, by default.

This option is not available for a site based on Device Managers.

1. In Service Center, click **Configuration** > **System Settings**.

2. Click the **Alert Configuration** tab.
3. Click **Modify**.
4. Do the following to change the default alert configuration:
    - To add an alert category when a site is not communicating so that it appears on the Central Dashboard, click **Categorize Alert** and add a category from the list. To set up a new alert category, see Creating an Alert Category. Click **Save**.
    - To create a trouble ticket when a site is not communicating, select the **Create Trouble Ticket** check box.
    - To send an email when a site is not communicating, select the **Send Email** check box and configure the settings.
    - To escalate an alert if an alert has not been resolved in a set amount of time, select the **Escalate Alert** check box and select a time after which the Alert Escalation will take effect.
5. Repeat steps 1 to 5 as needed to configure the alert actions for the Service Center Receive and Onsite Manager Processing alerts.
6. Click **Save**.

See Also

Setting Alert Actions

Creating Alert Categories

Setting System-Wide Alerting Actions for New Devices

By default, Service Center performs a device discovery network scan on sites every 5 minutes. You can configure an alerting action to notify you when new devices are discovered as the result of the network scan.

Best Practice

It is recommended that you first set the system-wide alert actions for new devices, and then override the system defaults on a per-site basis, as required. See also Setting Alerting Actions for New Devices for a Site.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Alert Configuration** tab.
3. In the **New Device Alert Configuration** area, click **Modify**.
4. Ensure that the **Enable New Device Alert** check box is selected.
5. Do the following to change the alert configuration:
    - To add an alert category when a new device is discovered so that it appears on the Central Dashboard, click **Categorize Alert** and add a category from the list. To set up a

new alert category, see Creating Alert Categories. Click **Save**.
- To create a trouble ticket when a new device is discovered, select the **Create Trouble Ticket** check box.
- To send an email when a new device is discovered, select the **Send Email** check box and configure the settings. If multiple devices are discovered from the same scan, they will be included in the same email.
- time, select the **Escalate Alert** check box and select a time after which the Alert Escalation will take effect.

6. Click **Save**.

See Also

Setting Alert Actions

Creating Alert Categories

Setting the Device Discovery Defaults

Setting System-Wide Alerting Actions for Loss of Monitoring Protocol

You can set system-wide alert actions that are triggered when WMI or SNMP ceases to work on a device. This alert determines that monitoring has stopped on a device, and that the monitoring protocol has failed. You can then investigate the root cause of the failure and resolve the problem.

You can set the system-wide alert actions for loss of monitoring protocol, and then override these actions at the site level, if required. See Setting Alert Actions for Loss of Monitoring Protocol at a Site.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Alert Configuration** tab.
3. In the **Loss of Monitoring Protocol Alert Configuration** section, click **Modify** .
4. Do the following to change the alert configuration:
   - To add an alert category when the monitoring protocol drops on a device so that it appears on the Central Dashboard, click **Categorize Alert** and add a category from the list. To set up a new alert category, see Creating Alert Categories. Click **Save**.
   - To create a trouble ticket when a monitoring protocol is dropped, select the **Create Trouble Ticket** check box.
   - To send an email when a monitoring protocol is dropped, select the **Send Email** check box and configure the settings. If multiple devices are discovered from the same scan, they will be included in the same email.

Modifying the Alert Configurations

You can modify the alert configuration for system-wide alerts.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Alert Configuration** tab.
3. Under the title of the alert you want to configure, click **Modify**.
4. Make changes to the alert configuration.
5. Click **Save**.

Creating Custom Ticket Statuses

You can create custom ticket statuses in Barracuda Managed Workplace for more comprehensive ticket status mapping with your Connectwise, Salesforce, or Remedy PSA configuration, or simply to create more descriptive ticket statuses for use within Service Center.

If your PSA configuration includes additional ticket statuses that do not easily match up with the four ticket statuses available with Barracuda Managed Workplace, you can create custom statuses in Service Center, and then map these custom statuses to the appropriate ticket status in your PSA. For more information, see the *Barracuda Managed Workplace Integration Guide - Service Desks*.

When you create a custom ticket status, you can optionally designate it as a closed status. A closed status indicates that the ticket is not active and no further action is required. For example, you can create an on-hold or resolved ticket status and designate it as closed. You can create multiple closed statuses as required.

> If you have a Autotask, Tigerpaw, Fieldpoint, Solutions 360, or a custom PSA integration installed, you can create custom ticket statuses, but the only attribute that will be passed to the PSA is whether the ticket is a closed status. For this reason, it is only recommended to create custom ticket statuses if you also have a Connectwise or Salesforce PSA installed.

To create a custom ticket status

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Ticketing** tab.
3. Click **New**.
4. Type a name in the **Ticket Status Name** box.
5. If the custom status is a closed ticket status, select the **Closed Status** check box.

6. Click **OK**.

To edit a custom ticket status

> You cannot edit the Barracuda Managed Workplace system ticket statuses.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Ticketing** tab.
3. Click **Edit** in the row for the custom ticket status you want to edit.
4. Select or clear the **Closed Status** check box.
5. Click **OK**.

To delete a custom ticket status

You can delete a custom ticket status if it is not currently mapped to a PSA or service desk ticket status. If it is mapped, a notification message appears, and you must unmap the custom status before deleting it.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Ticketing** tab.
3. Select the check box beside the status you want to delete.
4. Click **Delete**.

Working with Printer Transforms

A printer transform is a collection of information about a printer. It is only required if a printer doesn't adhere to the standard printer MIB (which defines the SNMP locations to find print information). Normally, printers will adhere to this standard, but occasionally some data is not in the standard location. In those cases a printer transform can be used that tells the system the custom location of the data. Once applied, Barracuda Managed Workplace uses the transform to determine the custom location whenever it discovers a printer of that make or model.

Printer transforms are available to install from the Update Center Components page. There are printer transforms available for Hewlett Packard, Lexmark and OKI Data, and new ones will be added in the future. You may want to install all printer transforms for the printers you manage and monitor.

What You Can Do

When you install a printer transform, it is applied to each site registered with the Service Center regardless of whether you are managing that type of printer at the site or not. After installing, Barracuda Managed Workplace automatically collects information about that type of printer

according to the transform.

When an upgrade for a printer transform is available, a green icon appears beside Update Center > Components in the navigation pane to indicate that there is a new component available for upgrade. You can update printer transforms via the Update Center.

You can export a printer transform and save it as an .XML file.

If you no longer want to use a printer transform, you can delete it.

Details about Printer Transforms

Here is a list of the additional data that is collected by some of the printer transforms currently available:

- Total Color Page Count for Hewlett Packard, Lexmark and OKI Data
- Total Mono Page Count for Hewlett Packard, Lexmark and OKI Data
- Printer Serial Number for Lexmark and OKI Data

To install a printer transform

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Printer Transforms** tab.
3. Click **Get More**.
   The **Components** page opens with a list of printer transforms available for installation.
4. Select the check box beside each printer transform you would like to install.
5. Click **Install**.

See Also

Updating and Installing Service Center Components

To import a printer transform

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Printer Transforms** tab.
3. Click **Import**.
4. Click **Browse** and locate the file, and then click **Open**.

To export a printer transform

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Printer Transforms** tab.
3. Select the check box beside the name of the printer transform.
4. Click **Export**.

To update a printer transform

1. In Service Center, click **Update Center** > **Components**.
2. Click **Updates**.
3. In the **Type** column, select **Printer Transforms** from the list.
4. Select the check box beside the name of each printer transform you want to update.
5. Click **Install**.

See Also

Updating and Installing Service Center Components

To delete a printer transform

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Printer Transforms** tab.
3. Select the check box beside the name of the printer transform.
4. Click **Delete**.

Setting Remote Control Options

You can use the Remote Control tab to configure system-wide settings for remote control tools. These include Premium Remote Control, specific custom integrations such as TeamViewer, LogMeIn Pro, or ScreenConnect, as well as a more general "other" configuration.

Custom Third Party Integration versus "Other" Option The custom third party integration provides a direct connection with TeamViewer, LogMeIn Pro, or ScreenConnect. You can set up all three integrations, however only the tool that is selected in System Settings will be available when launching a remote session on a device. The "other" option is a more generic configuration. It can be used with any remote access tool that meets the requirements, and has been tested on GoToAssist, LogMeIn Rescue, LogMeIn Pro, DameWare, and Bomgar.

Configuring Premium Remote Control Access

Premium Remote Control uses ISL Light technology to provide remote access to managed devices. Premium Remote Control consists of the following components:

- AlwaysOn - An agent that is automatically installed on all eligible managed devices.
- Business Premium Remote Control.exe - A client that you install on your computer. When you initiate a remote control session with Premium Remote Control, the client opens automatically for you to connect to the managed device.

When you enable Premium Remote Control, a remote control account is automatically set up, without

the need for configuration. The agent is then automatically installed on managed devices across all sites that meet the following criteria:

- A Windows device with the Admin share open;
- A Mac device with SSH enabled. The credentials for SSH must also be on the sudoer's list.

If you need to remove the Premium Remote Control agent from a device, Barracuda Managed Workplace includes scripts to uninstall Premium Remote Control. To run the script on a device, go to Automation > Library, and select one of the following scripts:

- Uninstall Business Premium Remote Control MAC
- Uninstall Business Premium Remote Control WIN

To set up a template Premium Remote Control invitation

Users are invited to Premium Remote Control sessions by email. You can customize the email template that is sent by default.
To restore the default email at any time, click Restore Default.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Remote Control** tab.
3. Type a title in the **Title** box.
   {{code}} represents the session code that Barracuda Managed Workplace inserts in the title.
4. Type an email in the **Body** box.
   {{url}} represents the link to the session that Barracuda Managed Workplace inserts in the body of the email.
5. Click **Save**.

Starting Premium Remote Control Sessions with Chat by Default

Premium Remote Control chat lets you communicate with the user whose device you are controlling through a chat window. Chat also gives you a higher screen resolution, but may slow down the connection.

To start Premium Remote Control sessions with chat by default

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Remote Control** tab.
3. Select the **Enable chat by default** check box.
4. To use chat by default on all devices, regardless of their settings, click **Clear Overrides**. Certain devices may have a setting that overrides the system setting that enables chat by default. Using Clear Overrides removes those settings and enables chat by default.
5. Click **Save**.

Configuring a Custom Third Party Integration

You can set up access credentials to TeamViewer, LogMeIn Pro, and ScreenConnect. The integration type that you select will appear as an option when launching a remote session on a device. You can select only one integration. By default, no custom third party integration is selected.

To configure TeamViewer access

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Remote Control** tab.
3. In the **Custom Third Party Integration** area, select the **TeamViewer** option button.
4. In the **Application Path** box, type the file location where TeamViewer is installed on the technician's computer.
5. In the **Global Password** box, type the TeamViewer password. This password will override the client password on the remote machine. Optionally, you can leave this box blank, and then provide a password when launching a TeamViewer session.
6. Click **Save**.

Click the **Clear Overrides** button to delete all device and user level overrides and to save changes. A dialog box will prompt you to confirm the action.

To configure LogMeIn Pro access

When configuring LogMeIn Pro, you must provide a Company ID and a PSK encryption key, which you must request from LogMeIn support.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Remote Control** tab.
3. In the **Custom Third Party Integration** area, select the **LogMeIn Pro** option button.
4. In the **Company ID** box, type your company ID.
5. In the **PSK** box, enter the PSK encryption key provided to you by LogMeIn.
6. Click **Save**.

Click the **Clear Overrides** button to delete all device and user level overrides and to save changes. A dialog box will prompt you to confirm the action.

To configure ScreenConnect access

ScreenConnect uses a web-based remote access mechanism, while the client PC must have the end-user software installed. When you configure system- wide ScreenConnect settings, you provide the base URL to your self-hosted ScreenConnect site. Optionally, you can also specify which folder to open by default, e.g. "/Host # All Machines".

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Remote Control** tab.
3. In the **Custom Third Party Integration** area, select the **ScreenConnect** option button.
4. In the **Base URL** box, enter the base ScreenConnect URL.
5. Optionally, in the **Folder** box, enter the name of the subsection of the ScreenConnect UI that you want to open when ScreenConnect is launched.
6. Click **Save**.

Click the **Clear Overrides** button to delete all device and user level overrides and to save changes. A dialog box will prompt you to confirm the action.

Configuring the "Other" Remote Control Application

If you are using third-party remote control tool to assist your customers, you can create a link to launch this application from within Barracuda Managed Workplace. You can do this by configuring an "other" option when initiating a remote control session, in one of the following:

- From a device page, by clicking **Remote Control** in the sidebar.
- In the **Remote Control** shortcut menu, which is available by clicking the shortcut icon beside a device name in a device list. The **Remote Control** shortcut menu displays the third-party tool specified as the "Other" option, and any remote control options available for the selected device.

You can create a shortcut link to any remote control tool that meets the following requirements:

- the tool is launched from a URL, either on the client computer or the technician's computer, or the tool is launched as an application on the technician's computer.
- preferably, the URL link or application executable contains all information required to fully establish remote connectivity.

The following remote control applications have been tested for integration with Barracuda Managed Workplace:

Remote Control Tool	Launch Method
GoToAssist	Launch URL on client computer
LogMeIn Rescue	Launch URL on client computer
LogMeIn Pro	Launch URL on technician computer
DameWare	Launch application on technician computer
Bomgar	Launch URL on client computer

- You can create one shortcut link to a third-party remote control tool.
- When creating a shortcut link to Dameware, you must enter the application parameter

m:{ipaddress}, and this setting should not be altered at the device level. This parameter passes the IP address for the specific device to the DameWare application and will automatically create an entry or load an existing entry in DameWare for the IP address. Additionally, Dameware does not support connection through the Onsite Manager socket, so this option should not be selected when configuring the global settings. DameWare offers a proxy utility that can be installed on the client network, which can be used as an alternate method of connecting. To download this utility, go to http://www.dameware.com/downloads.aspx .

When setting up the third-party selection item, you provide the following information:

- The name of the third-party tool as it will appear in the Remote Control shortcut menu;
- whether to launch a URL on the technician's computer, launch the application on the technician's computer, or launch a URL on the client's computer;

if launching an application on the technician's computer, the application path and parameters. You must also specify whether a socket connection is required, including the port number.

The configuration that you provide can be overridden at the device level. For more information, see Initiating a Remote Control Sesson by Launching a Third-Party Remote Control Tool.

To add an "other" link to the Remote Control shortcut menu

Best Practice

For remote control applications that launch a URL on either the client computer or technician computer, it is recommended that you leave the URL box blank, as in most cases the technician will enter a session-specific URL when initiating the remote control session.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Remote Control** tab.
3. In the **Name** box, type the name of the third-party remote control tool.
4. Do one of the following:
   - Click the **Launch URL on Tech computer** option button, and optionally, type the global default URL for the remote control application in the **URL** box.
   - Click the **Launch Application on Tech computer** option button. In the **Application path** box, type the path to the folder where the application is installed. If required, in the **Application Parameters** box, provide any required application parameters. If the application require a socket connection to the Onsite Manager server, select the **Socket connection required** check box, and in the **Port** box, type the port number.
   - Click the **Launch URL on Client computer o**ption button, and optionally, type the global default URL for the remote control application in the URL **box**.

5. Click **Save**.

Configuring Centrify

Centrify has been rebranded as Idaptive. You cannot configure Centrify at this time. Changes are coming in Barracuda Managed Workplace 12 Service Pack 2.

Centrify is a stand-alone application that is included with your Barracuda Managed Workplace license. With Centrify, you log in to your computer using your Active Directory account, and from there you can access the Centrify User Portal to launch your most frequently used applications, including Barracuda Managed Workplace, CloudCare, your PSA solution, and many more.

Centrify includes the following components:

- **Business SSO User Portal** A web-based dashboard that displays the applications you can sign in to, including Barracuda Managed Workplace.
- **Business SSO Cloud Manager** The administrative interface of Business SSO, which you use to manage the User Portal by adding and removing users and applications.
- **Business SSO Cloud Connector** An on-premise component that you install in your Active Directory environment -or, if you are reselling, in your client's Active Directory environment - that acts as a source for user accounts for Business SSO.

To set up Centrify, you must perform the following steps:

1. Configure Service Center to use SSL, if you have not done so already. SSL is required for Centrify to be configured in Service Center.
   If you are using a hosted environment, your Service Center is already configured to use SSL and no action is required.
2. Register for Centrify by contacting your salesperson. You will receive an email with access to the Business SSO user portal.
3. Log in to your domain controller.
   Log in to the Business SSO user portal, switch to the Cloud Manager view, and download SSO Cloud Connector to the domain controller. See Downloading Cloud Connector to your Domain Environment.
4. Add the Barracuda Managed Workplace application to the Business SSO user portal, if it is not already there. See Adding the Barracuda Managed Workplace Applicaiton to the SSO Portal.
5. Configure SSO in Service Center. See Configuring SSO in Service Center.
6. Invite users to the User Portal from the Cloud Manager. See Inviting Users to the Business SSO Portal.

Downloading Cloud Connector to your Domain Environment

The Cloud Connector is a software package that you install on a Windows computer inside your firewall that lets you use your Active Directory accounts to authenticate users with Active Directory accounts for access to the administrator and user portals.

1. Log in to the SSO User Portal.
2. To access Cloud Manager, click your user name in the top right corner, and then click **Switch to Cloud Manager**.
3. Click the **Settings** tab.
4. In the left pane, click **Cloud Connectors**.
5. Click **Add Cloud Connector**.
6. Run through the guided steps to download Cloud Connector to your domain environment. Note that you must register the Cloud Connector by entering your admin user name and password. Now that Cloud Connector is installed in your domain environment, you are ready to add the Barracuda Managed Workplace application to the SSO portal.

Adding the Barracuda Managed Workplace Application to the SSO Portal

Centrify includes thousands of applications that you can add, including Barracuda Managed Workplace. When you register for the User Portal, the Barracuda Managed Workplace application is included by default. If the Barracuda Managed Workplace application is not included, you must add it to the user portal to enable Centrify.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Secure Sign On** tab.
3. In the **Service Provider Information** area, copy the Service URL. You will be pasting this URL into Cloud Manager in a few steps.
4. Log in to the SSO User Portal.
5. To access Cloud Manager, click your user name in the top right corner, and then click **Switch to Cloud Manager**.
6. Click the **Apps** tab.
7. Click **Add Web Apps**.
8. In the search box, type *Business Managed Workplace*.
9. Click the **Add** button beside *Business Managed Workplace* SAML.
10. Click **Yes** to add the application.
11. Click **Close**.
    Barracuda Managed Workplace now appears in the **Apps** list. Now you will download the signing certificate to be uploaded to Service Center.
12. In the **Service URL** box, paste the URL you copied in step 3.
13. Copy the URL from the **Identity Provider Sign-In URL** box. You will be pasting this URL in Service Center.
14. Scroll down and click the **Download Signing Certificate** link. You will be uploading this certificate to Service Center.

Now you are ready to complete the SSO configuration in Service Center.

Configuring SSO in Service Center

After adding the Barracuda Managed Workplace app to the Business SSO portal, you must upload the security certificate into Service Center, and paste the sign-in URL.

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Secure Sign On** tab.
3. In the **Identity Provider Information** section, click **Modify**.
4. Select the **Enable identity provider** check box.
5. Click **Upload** to upload the certificate you downloaded from Cloud Manager.
6. In the **Identity Provider Sign in URL** box, paste the URL you copied from Cloud Manager.
7. Click **Save**.

Inviting Users to the Business SSO Portal

If you have downloaded Cloud Connector to your domain environment, users are automatically added to the Business SSO user portal using their Active Directory accounts. As a final step, you must invite users to access the portal. When you invite a user, an email is automatically sent with their log in credentials to the user portal.

1. Log in to the SSO User Portal.
2. To access Cloud Manager, click your user name in the top right corner, and then click **Switch to Cloud Manager**.
3. Click the **Users** tab.
4. Select the check box beside each user you want to invite.
5. From the **Actions** list, select **Send email invite for user portal setup**.
6. Click **Yes** to proceed.

Collecting Diagnostics for Support Purposes

Barracuda Managed Workplace includes a diagnostics tool that you can run to collect information on your Service Center, Onsite Manager, and Device Manager installations to help support technicians determine whether your environments meet system requirements, and help them quickly determine the root issue. Support diagnostics can decrease time to resolution, and help technicians determine whether they need to escalate your issue for resolution.

The **Support Diagnostics** tab includes a history of the diagnostics that were run in the past 72 hours. After 72 hours, this data is purged. At any time you can download the diagnostic data displayed on the **Support Diagnostics** tab. The data is a collection of log files condensed in a zip file, for easy email delivery to the support team.

To collect Onsite Manager diagnostics for a site

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Support Diagnostics** tab.
3. Expand the **Add OMs to Diagnostics Query** section by clicking the expanding arrow.
4. In the **Add to Diagnostic Query** column, click the green arrow to select the OM site.
   The site is added to the **Diagnostics Query** section at the bottom of the screen.
5. Repeat steps 2 to 4 until you have added all of the Onsite Managers on which you want to run diagnostics.
6. Click **Run Diagnostics**.

To collect Device Manager diagnostics

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Support Diagnostics** tab.
3. Expand the **Add DMs to Diagnostics Query** section by clicking the expanding arrow.
4. In the **Add to Diagnostic Query** column, click the green arrow to select a Device Manager.
   The Device Manager is added to the **Diagnostics Query** section at the bottom of the screen.
5. Repeat steps 2 to 4 until you have added all of the Device Managers on which you want to run diagnostics.
6. Click **Run Diagnostics**.

To download diagnostic data

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Support Diagnostics** tab.
3. Do one of the following:
   - To download diagnostics that you have just selected, in the **Diagnostics Query** section, click **Download Diagnostics**.
   - To download diagnostics that were run in the past 72 hours, in the **Diagnostics Performed in last 72 hours** section, click **Download Diagnostics**.

The diagnostic data for all of the Onsite Manager sites and Device Managers that were added to the **Diagnostics Query** section is downloaded to a .zip file.

Configuring Modems

To set up a modem

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Modem** tab.
3. In the **Modem Configuration** section, select the correct options in the boxes.
4. Click **Save**.

To test a modem

1. In Service Center, click **Configuration** > **System Settings**.
2. Click the **Modem** tab.
3. In the **Test Modem Configuration** section, select the correct options in the boxes.
4. Click **Send**.