

Working with VSC Blueprints

<https://campus.barracuda.com/doc/84967487/>

Working with VSC Blueprints

The Virtual Service Center (VSC) blueprint feature allows you to create one or more pre-configured VSC definitions that are used during the creation of new VARs. As well a default blueprint may be set so new VAR creation will default to use a blueprint.

You can use VSC blueprints to pre-configure VSCs for MSPs, for example. You

can define the blueprint by

- [importing policy modules](#)
- [creating service groups](#)
- [adding additional scripts](#)
- [creating report categories](#)
- [importing reports](#)
- [creating new user roles](#)
- [modifying user permissions on existing roles](#)
- [assigning policy modules to service groups](#)

You can

- create new VSC blueprints (see [Creating VSC Blueprints](#))
- modify a VSC blueprint name and description (see [Modifying a VSC Blueprint Name or Description](#))
- remove VSC blueprints (see [Deleting VSC Blueprints](#))
- define the VSC blueprint details (see [Defining VSC Blueprints](#))
- create a new VSC and associate it with a VSC blueprint (see [Creating a New VSC and Associating it with a VSC Blueprint](#))
- associate an existing VSC with a VSC blueprint (see [Working with Existing VSCs](#))
- see a list of VSC blueprints and their associated VSCs (see [Viewing VSC Blueprints and their Associated VSCs](#))
- see how a VSC blueprint is defined (see [Viewing VSC Blueprint Definition Details](#))
- modify existing blueprints (see [Modifying a VSC Blueprint Name or Description](#))

Note: VARs can only inherit a blueprint's properties at the time the VAR is created and will use the current definition of the blueprint at that point in time. Subsequent changes to a blueprint will not automatically propagate to its applied VARs, but only to the new VARs created after those changes have been made. The Applied VARs section can be used to add scripts, policy

modules and reports to the VARs that may have been created with an older version of the blueprint. This will help them remain in sync with the current blueprint definition should it change over time.

Creating VSC Blueprints

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the VSC Blueprints window, click **Create**.
3. Type a **Name** and **Description** in the boxes.
4. If SQL credentials are required, enter the user name and password.
5. Click **Create**.

Setting a VSC Blueprint as the Default

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. Select the corresponding check box for the blueprint you want to set as the default.
3. From the **More Actions** list, select **Set as Default Blueprint**.

Creating a New VSC and Associating it with a VSC Blueprint

When creating a new Virtual Service Center (VSC), you can select which VSC blueprint to use to create the new VSC.

1. In the Hosted Console website, click **Status > VAR Dashboard**.
2. In the **VAR Dashboard** window, click **Add New VAR**.
3. In the **Add VAR** dialog box, enter the **VAR Company Name**.
This is how the VAR is labeled in the Hosted Console Dashboard.
4. Enter the **VAR Domain**.
This is used to distinguish between each VAR on the login page and database, and it must be provided to the VAR in order for them to access their Service Center.
5. Enter the **VAR Code**.
This is used to track VAR licensing.
6. Enter identifying information for the VAR in the **First Name, Last Name, Phone Number, Email Address** boxes.
7. Enter address information for the VAR in the **Street, P.O. Box** (if required), **City, State/Province, Country, Postal/ZIP Code** boxes.
8. Enter the **User Name** and initial **Password** for the Admin user that is created with the Virtual Service Center.
9. In the **VAR Settings** section, select the **VSC Blueprint for the VAR**.
The Host name or IP of the database server is pre-populated based on the database server specified during installation. By default, the **SQL Authentication User Name** and **Password** boxes are populated with the credentials that were used during installation. Different credentials can be specified by entering the information into the **SQL User Name** and **Password** boxes.
10. Select the server where the Virtual Service Center will be created from the **Application Server**

list.

11. Select the process where the Virtual Service Center will be created from the **Worker Process** list and click **Save**.

You can add a new worker process to host the VAR by selecting **Add New Process**.

Note: The Add New VAR UI's Application Server and Worker Process list will automatically have Application Server and Worker Process selected that has the lightest load, but you can override this by making another selection.

To edit the details of an existing VAR, see VAR Configuration.

Viewing VSC Blueprints and their Associated VSCs

You can see a list of the VSC blueprints that have been created and their associated VSCs.

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
The VSC Blueprints window opens and all the blueprints that have been created appear in the table.
2. Click a blueprint name.
The VSC Blueprints Editor window opens and in the Applied VARs section, you can see the VSCs that are associated with the blueprint.

Note: VSC blueprints display in the language of the default admin user. If this is not the language you prefer, you can change the language in **User Management**. You must then save the blueprint for this change to take effect.

Viewing VSC Blueprint Definition Details

You can see how a VSC blueprint is defined by clicking a VSC blueprint in the VSC Blueprints window. This will open the VSC Blueprint Editor window where you can click a tab at the top of the window (Policies, Groups, Scripts, Report Categories, Reports, Roles, or Users) to see the definition details for the item.

Modifying a VSC Blueprint Name or Description

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the blueprint list, click the VSC blueprint for which you want to modify the name or description.
3. In the **Summary** section, click **Modify**.
4. Type a new Name or Description in the boxes.
5. Click **Save**.

Deleting VSC Blueprints

You can only delete a VSC blueprint if no VSCs are associated with it.

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. Select the check box that corresponds with the VSC blueprint you want to delete.
3. Click **Delete**.
4. Click **OK**.

Defining VSC Blueprints

You can use Virtual Service Center (VSC) blueprints to pre-configure VSC definition for MSPs. For example, you can define the blueprint by defining policy modules, groups, scripts, report categories, reports, user roles and users.

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the blueprint list, click the VSC blueprint you want to define.
3. Depending on what you want to define, click one of the tabs at the top of the window (**Policies, Groups, Scripts, Report Categories, Reports, Roles, or Users**) and see one of the topics listed below for detailed information.

[Defining Policy Modules for a VSC Blueprint](#)

[Defining Groups for a VSC Blueprint](#)

[Defining Scripts for a VSC Blueprint](#)

[Defining Report Categories for a VSC Blueprint](#)

[Defining Reports for a VSC Blueprint](#)

[Defining Roles for a VSC Blueprint](#)

[Defining Users for a VSC Blueprint](#)

Defining Policy Modules for a VSC Blueprint

For information about defining policy modules, see the following topics:

[About Working with Policy Modules](#)[Creating Policy Modules](#)[About Importing Policy Modules](#)[Importing Policy Modules from the Library](#)[Importing Policy Modules from Files](#)[Exporting Policy Modules](#)[Deleting Policy Modules](#)[Overriding Alert Actions in Policy Modules](#)[Overriding Send Email Alert Notifications in Policy Modules](#)[Overriding Send Alert Notification Escalations in Policy Modules](#)[Overriding Create Trouble Tickets Alert Action in Policy Modules](#)

About Working with Policy Modules

The Policy Modules window lists the policy modules that have been added or imported into VSC Blueprint, and it allows for new policy modules to be

created or imported. For more information, see [Creating Policy Modules and About Importing Policy Modules](#).

To access the Policy Modules window

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. Click an existing Blueprint name
3. Click the **Policy Modules** tab.

The Policy Modules window provides the following information:

Column Header	Description
Module Name	The name of the policy module.
Devices	Note: Devices are not applicable to VSC Blueprints.

Groups	The number of groups to which the policy module is applied.
Collecting	The number of enabled monitors collecting data in the policy module.

The policy module list can be sorted in ascending or descending order by clicking a column header.

Tip: Policy modules allow sets of monitor and alert rules to be quickly applied to groups or devices to make it easier to implement effective monitoring.

A policy module is not a container for groups or devices, but a means of applying monitor and alert rules to groups or devices. Removing policy modules removes all monitor and alert rules from the groups or devices to which the policy module was applied. For more information, see [Deleting Policy Modules](#).

You can export a policy module to an XML file for backup purposes. For instructions, see [Exporting Policy Modules](#).

Creating Policy Modules

You can create policy modules to monitor devices or applications. When creating a new policy module, some research will be required to identify how the device or application reports its status or events. See [Configuring Individual Monitor Types](#) for a list of the monitors that you can add to policy modules, and how they are configured.

To create a policy module

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click a blueprint name.
3. Click the **Policies** tab.
4. Click **New**.
5. In the **New Policy Module Name** box, type a name for the new policy module.
6. If desired, in the **Description** box, type a description for the policy module.
7. Click **Create**.

To add a monitor to the policy module

1. Click the **Monitors** tab.
2. Click **Add Monitor**.
3. From the **Choose Monitor Type** box, select the type of monitor you want to add to the policy module.
4. Click **OK**.
If the monitor type doesn't have monitor rules applied to it, you will have to add them now. For detailed instructions about adding a specific monitor type, see [Configuring Individual Monitor Types](#).
5. Click the **Overview** tab.

To apply the policy module to one or more groups

1. In the Applied Groups section, click **Add Groups**.
2. In the **Group Type** list, select the type of group (All, Service Groups or Site Groups) to which you want to apply the policy module.
You can filter the groups list by selecting items from the lists located under each column header.
3. Do one of the following:
 - Select the check box that corresponds with each group to which you want to apply the policy module.
 - Select the check box in the column header to select all groups.
4. Click **Add** to apply the policy module to the selected groups.

The groups to which the policy module is applied appear in the **Applied Groups** section of the **Policy Module** window.

About Importing Policy Modules

Barracuda Managed Workplace ships with a library of policy modules that let you implement remote monitoring and management quickly. The policy modules have been created with the monitors and alerts that are most useful, but may not be appropriate for every environment.

Policy modules can be added manually by creating a new policy module (see Creating Policy Modules). Or you can import a policy module from the library or from a file. For more information, see Importing Policy Modules from the Library and Importing Policy Modules from Files.

Importing Policy Modules from the Library

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint into which you want to import the policy modules.
3. Click the **Policies** tab.
4. Click **Import From Library**.
5. Do one of the following:
 - Select the check box that corresponds with policy modules you want to import.
 - Select the check box in the column header to select all policy modules.
6. Click **Import**.

Importing Policy Modules from Files

To import a policy module from a file

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint into which you want to import the policy modules.
3. Click the **Policies** tab.
4. Click **More Actions** to display a list.
5. Click **Import Policy Module**.
6. In the **Policy Module** file name box, click **Browse** to search for the file.
7. Select the file you want to import and then click **Open**.
8. Click **Import**.

Exporting Policy Modules

You can export a policy module to an XML file for backup purposes.

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the policy module you want to export.
3. Click the **Policies** tab.
4. Do one of the following:
 - Select the check box that corresponds with the policy module you want to export.
 - Select the check box in the column header to select all policy modules.

Note: Only one policy module can be exported at a time.

5. Click **More Actions** to display a list.
6. Click **Export Policy Module**.
7. Click **Save**.
8. Browse to the location where you want to save the file.
9. Type a file name and click **Save**.

Deleting Policy Modules

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the policy modules you want to delete.
3. Click the **Policies** tab.
4. In the list of policy modules, select the check box that corresponds with the policy module you want to delete.
5. Click **Delete**.
6. Click **OK**.

Caution: Deleting policy modules removes all monitor and alert rules from the groups to which the policy module was applied.

Overriding Alert Actions in Policy Modules

If required, you can override the following alert actions that are part of a policy module:

- send email alert notification, see [Overriding Send Email Alert Notifications in Policy Modules](#)
- escalate alert notifications, see [Overriding Send Alert Notification Escalations in Policy Modules](#)
- create trouble ticket, see [Overriding Create Trouble Tickets Alert Action in Policy Modules](#)

For information about alert actions, see [Setting Up Alert Actions](#).

For information about overriding alert actions in monitors, see [Overriding Alert Actions in Policy Modules](#).

Overriding Send Email Alert Notifications in Policy Modules

To override the send email alert notification alert action in a policy module

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the policy module for which you want to override the Send Email Alert notification.
3. Click the **Policies** tab.
4. Do one of the following:
 - Select the check box that corresponds with the policy module for which you want to override the alert action.
 - Select the check box in the column header to select all policy modules.
5. Click **More Actions** to display a list.
6. Click **Override Send Email Alert Notifications**.
7. Depending on if you want to send an email alert notification, select or clear the **Send Email** check box.
8. If you chose to enable the alert action, depending on to whom you want to send the email, select either the **To Authorized Users** or the **To the Following Email Addresses** option button.
9. If you selected the **To the Following Email Addresses** option button, then: do the following:
 - If you need to add a new email address, click **Add New**. In the **Add New Email Address** dialog box type the new Email Address in the box and click OK.
 - If you want to use an email address from an existing user defined in the VSC Blueprint, click **Add From Users**. In the **Add Email Addresses from Users** dialog box, select the check boxes that correspond with the users to whom you want to send the email alert notification. Or, select the check box at the top of the check box column to select all check boxes. Click **OK**.

To modify an email address

1. In the email address list, select the check box that corresponds with the email address you want to change.
2. Click **Modify**.
3. Make the required changes in the Email Address box.
4. Click **OK**.

To remove an email address

1. In the email address list, select the check box that corresponds with the email address you want to remove.
2. Click **Delete**.
3. Click **OK**.

Overriding Send Alert Notification Escalations in Policy Modules

To override the 'escalation alert notification' alert action in a policy module:

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the policy modules for which you want to override the **Send Alert Notification Escalation**.
3. Click the **Policies** tab.
4. Do one of the following:
 - Select the check box that corresponds with the policy module for which you want to override the alert action.
 - Select the check box in the column header to select all policy modules.
5. Click **More Actions** to display a list.
6. Click **Override Escalate Alert Escalation Notifications**.
7. Depending on if you want to send an escalation alert notification, select or clear the Escalate Alert check box.
8. If you chose to enable the alert action, choose the Hours and Minutes in which the alert escalation notification should be sent via email.
9. Depending on to whom you want to send the escalation alert notification, select either the **To Authorized Users** or the **To the Following Email Addresses** option button.
10. If you selected the To the Following Email Addresses option button, then do the following:
 - If you need to add a new email address, click **Add New**. In the **Add New Email Address** dialog box, type the new Email Address in the box and click **OK**.
 - If you want to use an email address from an existing user defined in the VSC Blueprint, click **Add From Users**. In the **Add Email Addresses from Users** dialog box, select the check boxes that correspond with the users to whom you want to send the alert notification. Or, select the check box at the top of the check box column to select all check boxes. Click **OK**.

To modify an email address

1. In the email address list, select the check box that corresponds with the email address you want to change.
2. Click **Modify**.
3. Make the required changes in the **Email Address** box.
4. Click **OK**.

To remove an email address

1. In the email address list, select the check box that corresponds with the email address you want to remove.
2. Click **Delete**.
3. Click **OK**.

Overriding Create Trouble Tickets Alert Action in Policy Modules

To override the 'create trouble ticket' alert action in a policy module

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the policy modules for which you want to override the Create Trouble Ticket alert action.
3. Click the **Policies** tab.
4. Do one of the following:
 - Select the check box that corresponds with the policy module for which you want to override the alert action.
 - Select the check box in the column header to select all policy modules.
5. Click **More Actions** to display a list.
6. Click **Override Create Trouble Ticket Action**.
7. Depending on if you want to create a trouble ticket, select or clear the **Create Trouble Ticket** check box.
8. Click **OK**.

Modifying Policy Modules

On the Overview tabbed page of the Policy Module window, you can

- modify a policy module, see [Modifying a Policy Module Name or Description](#)
- add policy modules to groups, see [Applying Policy Modules to Groups](#)
- remove policy modules from groups, see [Removing Policy Modules from Groups](#)

Modifying a Policy Module Name or Description

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the policy modules you want to modify.
3. Click the **Policies** tab.
4. In the list of policy modules, click the name of the module you want to modify.
5. In the **Summary** section, click **Modify**.
6. Make the required changes in the **Policy Module Name** and **Description** boxes.
7. Click **Save**.

Applying Policy Modules to Groups

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.

2. In the **Blueprints** list, click the blueprint that has the policy modules you want to add to groups.
3. Click the **Policies** tab.
4. In the list of policy modules, click the name of the policy module you want to add to groups.
5. To add the policy module to one or more groups:
 1. a Click **Add Groups**.
 2. b In the **Select Groups** dialog box, select the check boxes that correspond with the groups to which you want to add the policy module. To select all check boxes at once, select the check box at the top of the check box column.
6. Click **Add**.

The groups to which the policy module is applied appear in the **Applied Groups** section of the **Policy Module** window.

Removing Policy Modules from Groups

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the policy modules you want to remove.
3. Click the **Policies** tab.
4. In the list of policy modules, click a **Module Name**.
5. To remove the policy module from a group, in the **Applied Groups** section, select the check boxes that correspond with the groups from which you want to remove the policy module. To select all check boxes at one time, select the check box at the top of the check box column.
6. Click **Remove**.

Working with Policy Module Monitors

On the Monitors tabbed page of the **Policy Module** window, you can:

- add monitors to policy modules, see [Adding Monitors to Policy Modules](#)
- edit existing policy modules, see [Modifying Policy Modules](#)
- turn on or off monitors, see [Turning On or Off Monitors in Policy Modules](#)
- remove monitors, see [Deleting Monitors from Policy Modules](#)
- override alert actions, see [Overriding Alert Actions in Policy Modules](#)

Adding Monitors to Policy Modules

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the policy module to which you want to add a monitor.
3. Click the **Policies** tab.
4. In the list of policy modules, click a **Module Name**.
5. Click the **Monitors** tab.
6. Click **Add Monitor**.
7. From the **Choose Monitor Type** list, select the type of monitor you want to add to the policy

module.

8. Click **OK**.
9. Click the **Monitor** tab.
10. Configure the monitoring and alerting rules for the monitor type.
For specific instructions for each type of monitor, see [Configuring Individual Monitor Types](#).
11. Click **Save**.

Turning On or Off Monitors in Policy Modules

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the policy modules you want to modify.
3. Click the **Policies** tab.
4. In the list of policy modules, click a **Module Name**.
5. Click the **Monitors** tab.
6. In the list of monitors, select the check boxes that correspond with the monitors you want to turn on or off. Or, select the check box in the check box column header to select all check boxes.
7. Depending on what you want to do, select either **Turn On** or **Turn Off**.
In the list of monitors, the **State** column indicates whether the monitor is on or off.

Deleting Monitors from Policy Modules

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the policy module that includes the monitor you want to delete.
3. Click the **Policies** tab.
4. In the list of policy modules, click a **Module Name**.
5. Click the **Monitors** tab.
6. In the list of monitors, select the check boxes that correspond with the monitors you want to delete. Or, select the check box in the check box column header to select all check boxes.
7. Click **More Actions > Delete Monitor**.
8. Click **OK**.

Configuring Individual Monitor Types

Each type of monitor that can be added to a policy module is configured differently depending on the type of monitor. After you have added the monitor to a policy module (see [Adding Monitors to Policy Modules](#)), you can configure the monitor type. For specific instructions about configuring each type of monitor, see:

[Configuring AMT Event Monitors](#)

[Configuring Device Availability Monitors](#)

[Configuring MBSA Reports Monitors](#)

[Configuring Network Services Monitors](#)

[Configuring Patch Status Monitors](#)

[Configuring Performance Counter Monitors](#)

[Configuring SCE Monitors](#)

[Configuring SNMP Monitors](#)

[Configuring SNMP from MIB Monitors](#)

[Configuring SNMP Traps Monitors](#)

[Configuring Syslog Messages Monitors](#)

[Configuring Windows Events Monitors](#)

[Configuring Windows Services Monitors](#)

Configuring AMT Event Monitors

AMT Event monitors will only function correctly if the devices being monitored have successfully been added to the Intel® AMT device list.

To configure an AMT event monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select **AMT Events**.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes.
6. In the **AMT Event Rule** section, do the following:
 1. Select the **All** check box to collect events from all sources, or deselect it and specify a source by the source in the **Source** box.
 2. Select a severity level from the **Severity list**.
 3. Type any text string to search for in the **Details Search Text** box (maximum 255 characters).
7. In the **Event Collection** section, select the **Collect Events** check box to activate this monitor, or deselect it to deactivate this monitor (useful when creating exceptions for monitors).
8. If you want to configure the alert rules at this time, then continue with the next step or click

Save to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**.
5. In the **AMT Events Rule Parameters** section, do the following:
 1. Select a source from the **Event Source list**. If you selected either **Equal** or **Not Equal**, type a value in the corresponding box.
 2. Select a severity from the **Event Severity list**. If you selected either **Equal** or **Not Equal**, then select a value from the list that appears.
 3. Type any text string to search for in the **Details Search Text** box (maximum 255 characters).
 4. Click **Save**.
 5. Repeat this step until all required alert rules have been defined.
6. If more than one alert rule has been defined, select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
7. In the Alert Categories, Actions and Notifications section, do the following:
 1. Click **Add/Remove Category**.
 2. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 3. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 4. Click **OK**.
8. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
Note: Self-Heal is not an available option.
9. Click **Save**.
10. Click **Save**.

Configuring Device Availability Monitors

Device Availability monitors will function for all discovered devices.

To configure a device availability monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select **Device Availability**.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes.
6. If you want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**, and do the following:
 1. Select a period of time from the **Trigger alert when Device is Down** for list.
 2. Click **Save**.
 3. Repeat step a to b until all required alert rules have been defined.
5. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
6. In the **Alert Categories, Actions and Notifications** section, do the following:
 1. Click **Add/Remove** Category.
 2. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 3. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 4. Click **OK**.
7. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
8. Click **Save**.
9. Click **Save**.

Configuring Device Warranty Monitors

You can add a monitor that notifies you when a warranty is about to expire.

Tip: You can import the Warranty Expiration policy module and apply it to monitored devices. Then Barracuda Managed Workplace will alert and send an email when either a vendor or a custom warranty is going to expire in 60 days. If you clear the alert for vendor warranty expiration, for example, you will still be alerted about the custom warranty expiration.

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. Type a title for the alert.
4. Optionally, type a description for the alert.
5. Click **Add Alert Rule**.
6. From the **Trigger Type** section, do the following:
 - To create an alert that notifies you when the vendor warranty expires, select the **Vendor Warranty** check box.
 - To create an alert that notifies you when the custom warranty expires, select the **Vendor Warranty** check box.
 - To create an alert when either warranty expires, select both check boxes.
7. In the **Alert (days)** box, type the number of days before or after the expiry that you want to be

alerted.

8. Click **Save**.
9. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
10. Click **Save**.
11. Click **Save**.

Configuring MBSA Reports Monitors

MBSA Report monitors will only function correctly if the devices being monitored have WMI enabled.

To configure a MBSA report monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select **MBSA Reports**.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes. If you want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**.
5. In the **MBSA Category** section, select either the **All MBSA Categories** or **Choose MBSA Category** option button.
 - If you selected **All MBSA Categories**, then select a score from the **Score list**.
 - If you selected **Choose MBSA Category**, then select the category from the **MBSA Category list**, and then select the score from the **Score list**.
 1. If you selected **Choose MBSA Category**, the **MBSA Check** section appears.
 2. Select either the **All MBSA Checks from list** or the **Selected MBSA Checks from list** option button.

Tip: Use the CTRL key on the keyboard to select multiple checks.

1. Click **Save**.
6. Repeat steps 4 and 5 until you have defined all the alert rules.
7. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
8. In the **Alert Categories, Actions and Notifications** section, do the following:
 1. Click **Add/Remove Category**.
 2. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 3. If you want to remove any existing alert categories, in the panel on the right side of the

dialog box, select the alert categories and click **Remove**.

4. Click **OK**.

9. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.

For more information, see [Setting Up Alert Actions](#).

Note: Self-Heal is not an available option.

10. Click **Save**.

11. Click **Save**.

Configuring Network Services Monitors

Network Services monitors will function for all discovered devices.

Caution: Monitoring more than 100 network services at a single site may result in degraded performance of the Onsite Manager. This should not be an issue for most sites; however, if more monitoring is required, a second Onsite Manager should be used.

To configure a network services monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select **Network Services**.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes.
6. In the **Network Service Rule** section, do the following:
 1. Select the service to monitor from the **Network Services** list.
 2. The only option available from the **IP Address list** is **ALL** because there are no sites for the blueprint.
 3. Type the port used by the service in the **Port** box.
 4. Select a timeout value for the service from the **Timeout list**.
7. In the Scheduling section, do the following:
 1. Select how often the monitor is run by selecting a value from the **Polling Interval list**.
 2. In the **Schedule** box, by default, the monitor is set to **Run Always**. If you want to change the default, click **Run Always** to open the **Select Interval** dialog box.
 3. In the **Select Interval** dialog box, select either the **Daily Interval** or **Specific Interval** option button and use the corresponding lists to define the monitoring schedule.
 4. Click **OK**.
8. If you want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.

3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**.
 1. Select a value from the **Time Down before alerting** list.
 2. Click **Save**.
 3. If required, repeat this step until all required alert rules have been defined.
5. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
6. In the **Alert Categories, Actions and Notifications** section, click **Add/Remove Category**.
 1. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 2. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 3. Click **OK**.
7. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
8. Click **Save**.
9. Click **Save**.

Configuring Patch Status Monitors

Patch Status monitors will only function correctly if the devices being monitored have had a Windows Update Agent Policy defined, and the devices are reporting into patch management successfully.

To configure a patch status monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select **Patch Status**.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes.
6. If you want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**.
 1. In the **Patch Status** section, select a patch status from the **An alert will be triggered when any patch has a status of list**.
 2. Click **Save**.
 3. If required, repeat this step until you have defined all the alert rules.
5. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.

6. In the **Alert Categories, Actions and Notifications** section, click **Add/Remove Category**. The **Add/Remove Alert Categories** dialog box appears.
 1. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 2. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 3. Click **OK**.
7. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
8. Click **Save**.
9. Click **Save**.

Configuring Performance Counter Monitors

Performance Counter monitors will only function correctly if the devices being monitored have WMI enabled.

To configure a performance counter monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select **Performance Counters**.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes.
6. In the **Counter Selection** section, do the following:
 1. Select the performance object to monitor from the **Performance Object** list.
 2. Select the instance from the **Object Instance** list.
 3. Select the counter from the **Counter** list. If available, the **Counter Help** will appear, which provides description of the counter.
7. In the **Scheduling** section, do the following:
 1. Select how often the monitor is run by selecting a value from the **Polling Interval** list.
 2. In the **Schedule** box, by default, the monitor is set to **Run Always**. If you want to change the default, click Run Always to open the **Select Interval** dialog box.
 3. In the **Select Interval** dialog box, select either the **Daily Interval** or **Specific Interval** button and use the corresponding lists to define the monitoring schedule.
 4. Click **OK**.
8. If you want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**. The **Performance Counter Alert Rule**

dialog box appears.

5. In the **Trigger alert when performance counter is** section:
 1. Select either less than or greater than from the list.
 2. Type a value in the **threshold** box.
 3. Type a value in the **data points** box.
 4. Click **Save**.
 5. If required, repeat this step until you have defined all the alert rules.
6. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
7. In the **Alert Categories, Actions, and Notifications** section, click **Add/Remove Category**. The **Add/Remove Alert Categories** dialog box appears.
 1. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 2. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 3. Click **OK**.
8. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
9. Click **Save**.
10. Click **Save**.

Configuring SCE Monitors

SCE monitors will only function correctly if the devices being monitored have SCE (System Center Essentials) installed.

To configure an SCE monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select **SCE**.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes.
6. In the **Scheduling** section:
 1. Select how often the monitor is run by selecting a value from the **Polling Interval** list.
 2. Select the **Monitoring** check box to activate this monitor, or deselect it to deactivate it (useful when creating exceptions for monitors).
7. If you want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.

4. In the **Alert Rules** section, click **Add Alert Rule**.
5. In the **Severity**, **Priority** and **Category** boxes, do the following:
 1. Select either **All**, **Equal**, or **Not Equal** from the list.
 2. If you selected **Equal** or **Not Equal**, select a corresponding item from the list.
6. In the **Name**, **Description**, **Source**, and **Management Group Search String** boxes, do the following:
 1. Select either **All**, **Equal**, or **Not Equal** from the list.
 2. If you selected **Equal** or **Not Equal**, type a value in the corresponding box.
7. Click **Save**.
8. Repeat steps 4 to 7 until all the required alert rules have been defined.
9. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
10. In the **Alert Categories, Actions and Notifications** section, do the following:
11. Click **Add/Remove Category**. The **Add/Remove Alert Categories** dialog box appears.
 1. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 2. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 3. Click **OK**.
12. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
13. Click **Save**.
14. Click **Save**.

Configuring SNMP Monitors

SNMP monitors will only function correctly if the devices being monitored have SNMP enabled.

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

To configure an SNMP monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select **SNMP**.
3. Click **Add Monitor**.
4. In the **Monitor** tab, type a title for the monitor.
5. Optionally, type a description for the monitor.
6. Ensure the **Enabled** check box is selected.
7. Select the **New SNMP OID** option button.
8. In the **Object Name** box, type the OID text identifier.

9. In the **OID** box, type the OID numeric value.
10. From the **Object Type** list, select either Numeric or Text.
11. To collect tabular OIDs, select the **Tabular** check box.
12. In the **Description** box, type a description for the OID.
13. If you selected the **Tabular** check box, select an appropriate time to set how frequently tabular children scalar OIDs are captured.
14. From the **Polling Interval** list, select an appropriate time to set how frequently the data is captured.
15. Do one of the following to set when the monitor runs:
 - To set the monitor to run all the time, do nothing.
 - To change when the monitor runs, click **Run Always** to open the **Select Interval** dialog box and select either the **Daily Interval** or **Specific Interval** option button and use the corresponding lists to define the monitoring schedule. Click **OK**.
16. If you want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**.
5. In the **Trigger alert when SNMP counter is** section, select either **less than** or **greater than** from the list.
 1. Type a value in the **threshold** box.
 2. Type a value in the **data points** box.
 3. Click **Save**.
 4. Repeat until all required alert rules have been defined.
6. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
7. In the **Alert Categories, Actions and Notifications** section, click **Add/Remove Category**. The **Add/Remove Alert Categories** dialog box appears.
 1. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 2. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 3. Click **OK**.
8. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
9. Click **Save**.
10. Click **Save**.

Configuring SNMP from MIB Monitors

SNMP from MIB monitors will only function correctly if the devices being monitored have SNMP

enabled. To create the monitors using a file, it must have the .MIB extension. These files may be provided by the vendor, or you can click [here](#).

The MIBs that appear in the MIB Library and the objects identifiers (OIDs) that are loaded into the MIB Browser are remembered on a per user basis.

To configure an SNMP from MIB monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select SNMP from MIB and click **OK**.
3. Select the MIB file from the **Browse Library** list. If the MIB file has not been previously imported into VSC Blueprint, then you have to upload the file. To upload the file:
 1. Click **Upload MIBs to Library**.
 2. Click **Browse**.
 3. Select the file and click **Open**.
 4. Click **Upload**. The Results section confirms the upload was successful, listing number of files added.
 5. Click **Finished**.
 6. From the **Browse Library** list, select the MIB file that you just added and click **Load MIB**.
(You can also delete a MIB from the library by clicking **Delete from Library**.)
4. In the **Loaded MIBs** pane, select the check box of each MIB for which you want to see the OIDs.
The OIDs appear in the **MIB Browser** pane. If available, a description of the OID will appear in the **Selected Object Description** pane. If there are dependencies or errors related to a MIB, the information appears in the message box below the viewer area.
5. In the **MIB Browser** pane, select the check box of each OID you want to add as a monitors in the policy module.
6. In the **Scheduling** section, select how often the monitor is run by selecting a value from the **Polling Interval** list.
 1. In the **Schedule** box, by default, the monitor is set to **Run Always**. If you want to change the default, click **Run Always** to open the **Select Interval** dialog box.
 2. In the **Select Interval** dialog box, select either the Daily Interval or Specific Interval option button and use the corresponding lists to define the monitoring schedule.
 3. Click OK.
7. Click **Add Selected Objects**.
8. If you want to configure the alert rules at this time, then in the **Monitors** list, click the monitor for which you want to configure the alert rules and continue with the next step.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**.
5. In the **Trigger alert when SNMP** counter is section, select either less than or greater than

from the list.

1. a Type a value in the **threshold** box.
2. b Type a value in the **data points** box.
3. c Click **Save**.
4. d Repeat until all required alert rules have been defined.
6. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
7. In the **Alert Categories, Actions and Notifications** section, click **Add/Remove Category**.
 1. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click Add.
 2. b If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click Remove.
 3. c Click **OK**.
8. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
9. Click **Save**.
10. Click **Save**.

Configuring SNMP Traps Monitors

The Onsite Manager has to be defined as an SNMP Trap receiver on the devices being monitored.

To configure an SNMP Traps monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select SNMP Traps.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes.
6. In the **SNMP Trap Rule** section, if you want to monitor for a specific aspect of SNMP Traps, then select an item from **Generic Type** list.
7. If you selected Enterprise Specific in the previous step, then the Enterprise OID box becomes available so you can enter your Enterprise OID.
8. If you want to enable SNMP Trap Collection, then select the check box.
9. If you want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**.
5. In the **SNMP Trap Parameters** section, select an item from the **Generic Type** list.
6. If you selected Enterprise Specific in the previous step, then the **Enterprise OID** box becomes available so you can enter your Enterprise OID.
7. In the **Variable Binding Parameters** section, select **Any**, **Contains**, or **Does Not Contain** from the Variable Binding list. If you selected Contains or Does Not Contain, type the value in the box.
8. Click **Save**.
9. Repeat until all required alert rules have been defined.
10. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
11. In the **Alert Categories, Actions and Notifications** section, click **Add/Remove Category**.
 1. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 2. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 3. Click **OK**.
12. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
- Note:** Self-Heal is not an available option.
13. Click **Save**. The **Alert Configuration** dialog box closes.
14. Click **Save**. The **Monitor** dialog box closes.

Configuring Syslog Messages Monitors

Syslog Messages monitors will only function correctly if the Onsite Manager has been defined as a Syslog Message receiver on the devices being monitored.

To configure a Syslog Message monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select Syslog Messages.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes.
6. In the **Syslog Rule** section, if you want to monitor for specific aspects of syslog messages, then perform any combination of the following:
 1. Select a Facility from the list.
 2. Select a Severity from the list.
 3. Type part of a syslog message in the **Message Search** box.

7. If you want to enable **Syslog Collection**, then select the check box.
8. If want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**.
 1. In the **Syslog Rule Parameters** section, select **All**, **Equal**, or **Not Equal** from the **Syslog Category** list. If you selected **Equal** or **Not Equal**, select the syslog category from the corresponding list.
 2. Select **All**, **Equal**, or **Not Equal** from the **Severity** list. If you selected **Equal** or **Not Equal**, then select the severity level from the corresponding list.
 3. Select **All**, **Equal**, or **Not Equal** from the **Message Substring** list. If you selected **Equal** or **Not Equal**, then type the text string in the corresponding box.
 4. Click **Save**.
 5. Repeat this step until all required alert rules have been defined.
5. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
6. In the Alert Categories, Actions and Notifications section, click Add/Remove Category.
 1. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 2. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 3. Click **OK**.
7. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
- Note:** Self-Heal is not an available option.
8. Click **Save**.
9. Click **Save**.

Configuring Windows Events Monitors

Windows Event monitors will only function correctly if the devices being monitored have WMI enabled.

To configure Windows event monitors

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select **Windows Events**.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes.
6. In the **Windows Event Rule** section, select the Windows event log to monitor from the Log list.

7. To define a new Windows event log, select the **Other** check box, and type the name of the log in the corresponding box.
 1. Select the **All** check box to collect events from all sources, or deselect the **All** check box and type the source in the **Source** box.
 2. Select the **All** check box to collect events with all event IDs, or deselect the **All** check box and type the event ID in the **Event ID** box.
 3. Select a severity level for the event from the **Severity** list.
 4. Type a text string to find in the **Details Search Text** box, if required.
8. In the **Event Collection** section, select the **Collect Events** check box to activate this monitor, or deselect it to deactivate it (useful when creating exceptions for monitors).
9. If you want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**.
5. Select the Windows event log to monitor from the **Event Log** list.
6. To define a new Windows event log, select the **Other** check box, and type the name of the log in the corresponding box.
 1. Select the **All** check box to collect events from all sources, or deselect the All check box and type the source in the **Event Source** box.
 2. Select the **All** check box to collect events with all event IDs, or deselect the All check box and type the event ID in the **Event ID** box.
 3. Select a severity level for the event form the **Event Severity** list.
 4. Type a text string to find in the **Details Search Text** box, if required.
 5. Repeat this step until all required alert rules have been defined.
7. If more than one alert rule has been defined, then select either the **Alert When Any Rule Conditions are Met** or the **Alert When All Rule Conditions are Met** option button.
8. In the **Alert Categories, Actions and Notifications** section, click **Add/Remove Category**.
 1. a In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 2. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 3. Click **OK**.
9. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
10. Click **Save**.
11. Click **Save**.

Configuring Windows Services Monitors

Windows Services monitors will only function correctly if the devices being monitored have WMI

enabled.

To configure a Windows services monitor

1. Click **Add Monitor**.
2. From the **Choose Monitor Type** list, select **Windows Services**.
3. Click **OK**.
4. Click the **Monitor** tab.
5. In the **Monitoring Rule** section, type a monitor Title and Description in the boxes.
6. In the **Service Selection** section, select the Windows service you want to monitor from the **Service** list.
7. Select the type of monitoring from the Monitoring Type list:
 - **Off - No Monitoring**
 - **Low - Do not restart but send event to Service Center** will not attempt to restart the Windows Service, but will send an alert to Service Center.
 - **Medium - Restart and send event to Service Center if restart fails** will attempt to restart the Windows service, and send an alert to Service Center if the restart of the service fails.
 - **High - Restart and send event to Service Center** will attempt to restart the Windows service, and send an alert to Service Center whether or not the restart of the service fails.
8. In the **Enable/Disable Rule** section, select the **Enable this Rule** check box to activate this monitor, or deselect it to deactivate it (useful when creating exceptions for monitors).
9. If you want to configure the alert rules at this time, then continue with the next step or click **Save** to close the dialog box.

To configure the alert rules

1. Click the **Alerts** tab.
2. Click **Add Alert Configuration**.
3. In the **Alert** section, type an alert Title and Description in the boxes.
4. In the **Alert Rules** section, click **Add Alert Rule**.
5. The alert rules have already been defined in the previous steps. Click **Save**.
Note: It is not necessary to add an additional alert rule.
6. In the **Alert Categories, Actions and Notifications** section, click **Add/Remove Category**.
 1. In the panel on the left side of the dialog box, select all the alert categories under which you want this alert to appear (in the Central Dashboard) and click **Add**.
 2. If you want to remove any existing alert categories, in the panel on the right side of the dialog box, select the alert categories and click **Remove**.
 3. Click **OK**.
7. Select the check boxes that correspond with any Alert Actions, Alert Notifications, or Escalation Notification you want to enable.
For more information, see [Setting Up Alert Actions](#).
Note: Self-Heal is not an available option.
8. Click **Save**.
9. Click **Save**.

Setting Up Alert Actions

When adding Monitors and Alert Rules as part of a policy module, alert actions can be configured to determine what should occur when the alert condition, which is defined by the alert rules, has been discovered by the Onsite

Manager. For more information about the various alert actions, see one of the following topics:

[Creating Trouble Tickets from Alerts Automatically](#)

[Self-Healing Alerts](#)

[Running Scripts](#)

[Receiving Alert Notifications via Email](#)

[Escalating Alert Notifications](#)

For information about configuring monitors, see [Configuring Individual Monitor Types](#).

Creating Trouble Tickets from Alerts Automatically

The Create Trouble Ticket Alert Action causes a trouble ticket to be automatically generated when the alert is triggered. The trouble ticket will be populated with the Alert Details, as well as the following information:

Item	Description
Ticket ID	A unique ID number that is assigned when the ticket is created.
Site	The site for which the alert was generated.
Ticket	For tickets created by an alert action, this box displays the Alert Configuration title.
Status	For tickets created by an alert action, the initial status is set to New.
Assigned To	Tickets created by an alert action are assigned to the first Technician assigned to the site.
Priority	For tickets created by an alert action, the initial priority is set to High.

Self-Healing Alerts

The Self-Heal Alert Action is available so that alerts can automatically be removed from the Central Dashboard if the condition triggering the alert no longer exists. This is not an available alert action for

all monitor types, as some Monitors scan for single events (such as AMT Events, MBSA Reports, SNMP Traps, Syslog Messages and Windows Events) and can therefore not self-correct.

To self-heal alerts

1. Select the **Self-Heal** check box.
2. Select the **Clear Trouble Ticket** check box to have any trouble tickets created as part of this alert configuration cleared when the alert self-heals.
Note: The **Clear Trouble Ticket** check box is only available if the **Create Trouble Ticket** check box was enabled for the alert.
3. Select the **Enable Self-Heal Notification** check box to receive notification through Email when the alert self-heals.
4. Choose time range from the **Notify if alert is cleared within** list.
5. Click **Save**.

Running Scripts

Note: Running a script is not applicable in blueprints.

Receiving Alert Notifications via Email

The Send Email Alert Action causes an email to be automatically generated when the alert is triggered. Users set to receive the email alerts must have that right defined in a role assigned to the user.

To receive alert notifications via email

1. Select the **Send Email** check box.
2. Choose either the **All users for the site whose role is configured to receive Alert Notifications** or the **Specify emails (separate emails by semicolon)** option button.
 - If **All users for the site whose role is configured to receive Alert Notifications** is selected, all users with the appropriate role for the site will receive the email.
 - If **Specify emails (separate emails by semicolon)** is selected, highlight any desired addresses in the **Choose from a list of notifiable users across all sites** list, and click the Add to notification list button, or manually enter the email addresses separated by a semicolon in the Email notifications to be sent to the following addresses box.
3. If required, change the **Alert Emailed From** address (set by default to the value configured on the **Configuration > Master Settings > From Email** box) to the address that should send the alert.
Note: Depending on the SMTP server being used, this may or may not have to be an actual email address.
4. Click **Save**.

Escalating Alert Notifications

The Escalate Alert Action is available so a second tier of notification can be implemented when a

condition that triggered an alert has not been resolved in a set amount of time.

To escalate alert notifications

1. Select the **Escalate Alert** check box.
2. Select a time after which the Alert Escalation will take effect.
3. Select the **Send Email** check box.
4. Click **Save**.

Overriding Alert Actions in Monitors

If required, you can override the following alert actions that are part of a monitor:

- send email alert notification, see [Overriding Send Email Alert Notifications in Policy Modules](#)
- escalate alert notifications, see [Overriding Send Alert Notification Escalations in Policy Modules](#)
- create trouble ticket, see [Overriding Create Trouble Tickets Alert Action in Policy Modules](#)

For information about alert actions, see [Setting Up Alert Actions](#).

For information about overriding alert actions in policy modules, see [Overriding Alert Actions in Policy Modules](#).

Overriding Send Email Alert Notifications in Monitors

To override the send email alert notification alert action in a monitor

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the monitoring rules for which you want to override the **Send Email Alert** notification.
3. Click the **Policies** tab.
4. In the list of policy modules, click a **Module Name**.
5. Click the **Monitors** tab.
6. In the list of monitors, select the check box that corresponds with the monitoring rules for which you want to override the alert action. Or, select the check box in the check box column header to select all check boxes.
7. Click **More Actions** to display a list.
8. Click **Override Send Email Alert Notifications**.
9. Depending on if you want to send an email alert notification, select or clear the **Send Email** check box.
10. If you chose to enable the alert action, choose the Hours and Minutes in which the alert escalation notification should be sent via email.
11. If you chose to enable the alert action, depending on to whom you want to send the email, select either the **To Authorized Users** or the **To the Following Email Addresses** option

button.

12. If you selected the **To the Following Email Addresses** option button, then do the following:
 - If you need to add a new email address, click **Add New**. In the **Add New Email Address** dialog box type the new Email Address in the box and click **OK**.
 - If you want to use an email address from an existing user defined in the VSC Blueprint, click **Add From Users**. In the **Add Email Addresses From Users** dialog box, select the check boxes that correspond with the users to whom you want to send the email alert notification. Or, select the check box at the top of the check box column to select all check boxes. Click **OK**. The email addresses are added to the list.

To modify an email address

1. In the email address list, select the check box that corresponds with the email address you want to change.
2. Click **Modify**.
3. Make the required changes in the **Email Address** box.
4. Click **OK**.

To remove an email address

1. In the email address list, select the check box that corresponds with the email address you want to remove.
2. Click **Delete**.
3. Click **OK**.

Overriding Send Alert Notification Escalations in Monitors

To override the 'escalation alert notification' alert action in a monitor

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the monitoring rules for which you want to override the **Send Alert Notification Escalation**.
3. Click the **Policies** tab.
4. In the list of policy modules, click a Module Name.
5. Click the **Monitors** tab.
6. In the list of monitors, select the check box that corresponds with the monitoring rules for which you want to override the alert action. Or, select the check box in the check box column header to select all check boxes.
7. Click **More Actions** to display a list.
8. Click **Override Escalation Alert Escalation Notifications**.
9. Depending on if you want to send an escalation alert notification, select or clear the **Escalate Alert** check box.
10. If you chose to enable the alert action, choose the Hours and Minutes in which the alert escalation notification should be sent via email.
11. Depending on to whom you want to send the escalation alert notification, select either the **To Authorized Users** or the **To the Following Email Addresses** option button.
12. If you selected the **To the Following Email Addresses** option button, then do the following:

- If you need to add a new email address, click **Add New**. In the **Add New Email Address** dialog box type the new **Email Address** in the box and click **OK**.
- If you want to use an email address from an existing user defined in the VSC blueprint, click **Add From Users**. In the **Add Email Addresses from Users** dialog box, select the check boxes that correspond with the users to whom you want to send the alert notification. Or, select the check box at the top of the check box column to select all check boxes. Click **OK**. The email addresses are added to the list.

To modify an email address

1. In the email address list, select the check box that corresponds with the email address you want to change.
2. Click **Modify**.
3. Make the required changes in the **Email Address** box.
4. Click **OK**.

To remove an email address

1. In the email address list, select the check box that corresponds with the email address you want to remove.
2. Click **Delete**.
3. Click **OK**.

Overriding Create Trouble Tickets Alert Action in Monitors

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the monitoring rules for which you want to override the **Create Trouble Ticket** alert action.
3. Click the **Policies** tab.
4. In the list of policy modules, click a **Module Name**.
5. Click the **Monitors** tab.
6. In the list of monitors, select the check box that corresponds with the monitoring rules for which you want to override the alert action. Or, select the check box in the check box column header to select all check boxes.
7. Click **More Actions** to display a list.
8. Click **Override Create Trouble Ticket Action**.
9. Depending on if you want to create a trouble ticket, select or clear the **Create Trouble Ticket** check box.
10. Click **OK**.

Defining Groups for a VSC Blueprint

For more information about defining groups, see the following topics:

[Setting Up Groups](#)

[Creating Service Groups](#)

[Deleting Groups](#)

Setting Up Groups

You can use the Group Configuration window to create service groups.

To access the Group Configuration window

- In the main menu, click Configuration > Groups.

Service groups are used to organize devices by the function or role of the devices. Devices and sites cannot be added to service groups in a VSC Blueprint. Service groups will appear on the VAR's Central Dashboard under the group folder to which the service group belongs. Group folders can be used as logical containers for multiple service groups. For example, an Applications group folder can be created to contain IIS and Exchange service groups.

Groups allow VARs to easily manage a large number of devices by applying Policy Modules and Windows Update Agent Policies to multiple devices at one time. Applying Windows Update Agent Policies is not applicable to VSC Blueprints.

To create groups, see [Creating Service Groups](#). To remove a group, see [Deleting Groups](#).

Creating Service Groups

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint in which you want to create a service group.
3. Click the **Groups** tab.
4. In the **Browse By** box at the top of the window, select the Service Groups option button.
5. Depending on what type of group you are creating, click Add **Service Group**.
6. From the **Group Folder** list, select a group folder to contain the service group. If you want to create a new group folder, select the **Other** check box and in the box that appears, type a name for the new group folder.
7. In the **Group Name** box, type a name for the group and if desired, type a description of the group in the **Group Description** box.
8. Click **Add and Configure**.
9. Click the **Name** tab. The group name and description you just entered appear in the **Group Identification** section.
10. In the **Policy Modules Applied to Group** section, do the following:
 1. Click **Apply Policy Module**. The **Policy Module** list appears.
 2. From the **Policy Module** list, select a policy module to apply to the group.

3. Click **Apply**. The policy module now appears in the **Policy Modules Applied to Group** list.
 4. Repeat this step until all required policy modules are applied to the group.
11. Click **Add**.
- Notes:**
- Site groups are not applicable to VSC Blueprints because no sites are present in a blueprint.
 - The Group Configuration UI has a Devices tab; however, this is not applicable to VSC Blueprints.

Deleting Groups

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that has the service group you want to delete.
3. Click the **Groups** tab.
4. Select the **Service Groups** option button.
5. In the list, click the **Delete** button that corresponds with the group you want to delete. A confirmation dialog box will appear.
6. Click **OK**.

Defining Scripts for a VSC Blueprint

For information about defining scripts, see the following topics:

[Adding Scripts](#)

[Deleting a Script](#)

[Running Scripts](#)

The Scripts and Executables window displays the list of currently available scripts and executables that may be deployed. By default there are maintenance scripts automatically populated with Barracuda Managed Workplace. Note that for VSC Blueprints there will not be any devices on which to execute the scripts.

The Scripts and Executables window defaults to a Grouped View where the Scripts are organized by intended use. This can be changed to Single View, where the Scripts are displayed in a sortable listing.

To navigate to the Scripts and Executables view

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.

2. In the **Blueprints** list, click the blueprint you want to work with.
3. Click the **Scripts** tab.
4. To view a list of script, clear the **Group by Category** check box.

The following information is displayed for each script. The Category only appears when using Single View.

Adding Scripts

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint to which you want to add a script.
3. Click the **Scripts** tab.
4. Click **Add**.
5. In the **Name** box, type a name for the script.
6. Click **Browse** and locate the script file or .ZIP file, and then click **Open**.
7. If the script file you added was a compressed file (such as a .ZIP), then select the starting file from the Starting File list.

The starting file in the .ZIP file must be at the root level of the .ZIP file and have a file extension that is recognized by Barracuda Managed Workplace. This is done to protect against trying to run files with unknown file types that may cause the task to hang.
8. Select a category from the list or type a new one.

Script categories allow for easier organization of scripts. A category can be created by typing in a new name. If you type a new name, Barracuda Managed Workplace creates a new category.
9. In the **Version** box, type a number.

Versions for scripts must be in the form of <num>.<num>.<num>.<num>, though only a single number is required.
10. In the **Minimum MW Version** box, type the version of Barracuda Managed Workplace that this script supports.

By default, the Minimum MW Version is not automatically populated with the current version of Service Center, but this is usually the value you want to enter. If you need to specify that it only works with the current version, type 6.2. If this is done, the script will be sent to Onsite Managers that are not the specified version number but will stay in a state of "Pending Upgrade" until Onsite Manager is upgraded or the schedule expires. Note however, that they can be assigned to devices on older Onsite Managers. If this is done, the script will be run on the device when Onsite Manager is upgraded, unless the execution time is in the past and the retry period has expired.

You can locate Barracuda Managed Workplace build numbers in the correct format under **Help > About**.

When there is a new version of a script, Onsite Manager checks the file version and determines whether to download the file from Service Center.
11. In the **Author** box, type the author name.
12. In the **Description** box, type a description.

This description is shown to users when they create tasks for the script. It is a good idea to describe how to use any parameters for the script.
13. If you want the script to run on Onsite Manager, select the **Run on Onsite Manager** check box.

14. If the script must run without another restricted script running, select the **Restricted** check box.
 15. If the script requires parameters at run-time click **Add Parameter** and do the following:
 - To set a parameter for a script as optional, select the **Optional** check box.
 - To set a parameter for a script as required, ensure the **Optional** check box is cleared.
 - To identify this parameter as unique, in the **Key** box, type a unique identifier. This key is the key expected by the script.
 - To set a label for a script parameter, type a label in the **Label** box. You can prefix the parameter label with a number, for example, to display them in the desired order.
 - To set the type for a script parameter, select either **String**, **Integer**, or **File**.
 - If you selected **String**, to set the length for a script parameter, type a length in the **Length** box.
 - If you selected **Integer**, to set the minimum and maximum for a script parameter, type a minimum and maximum in the appropriate boxes.
 - If you selected **String** or **Integer**, to set a default for a script parameter, type a default in the **Default** box.
- Note:** To delete a parameter for a script, click the trash can beside the parameter you want to delete.
16. Click **Save**.
The script is now ready to be used in a task.
 17. In the Hosted Console website, click **Configuration > VSC Blueprints**.
 18. In the **Blueprints** list, click the blueprint from which you want to remove a script.
 19. Click the **Scripts** tab.

Importing a Script or Automation Package

You can import a Barracuda Managed Workplace Script (an .MWS) file into Barracuda Managed Workplace. When you import an .MWS file, it includes all the meta data for the script.

Note: The .MWS file is a .ZIP file with the extension changed.

When a script is imported, its category is added to the system, if it doesn't already exist.

Version checking is performed when importing a script that is already on the system. You are warned if you attempt to import an older version of the script than is present on the system.

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint to which you want to import a script.
3. Click the **Automation** tab.
4. Click **Import**.
5. Click **Browse** and locate the script to import, and then click **Open**.
6. Click **OK**.

Exporting a Script or Automation Package

When you export a script or automation package, information from the scripts are stored in an .MWS file along with all required script files. The file contains the original script file or files (or .ZIP file) along with an .XML file that contains the meta data for the script. By doing this, if the script is imported into another system, the meta data is preserved.

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint from which you want to remove a script.
3. Click the **Automation** tab.
4. Select the check box beside the name of the script or automation package that you want to export.
5. Click **Export**.
6. Click **Save** and specify a location.
7. Click **Save**.

Deleting a Script

Any tasks using the deleted script will be deleted, unless they are currently running. If Onsite Manager already has the file, then it will be able to run. If it doesn't, then the task fails.

Deleting a script has no impact on historical information.

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint from which you want to remove a script.
3. Click the **Automation** tab.
4. Select the check box beside the name of the script that you want to delete.
5. Click **Delete**.
6. Click **OK**.

For more information about creating script jobs, see [Running Scripts](#).

Note: Tasks cannot be created in the VSC Blueprint editor.

Running Scripts

Note: Running a script is not applicable in blueprints.

Defining Report Categories for a VSC Blueprint

For information about defining report categories, see the following topics:

[Managing Report Categories](#)

[Adding Report Categories](#)

[Deleting Report Categories](#)

Managing Report Categories

The Report Categories window allows you to add and remove report categories.


You may find that grouping reports based on your own categories helps to organize your operations more closely than using the predefined categories. If this is the case, you may create and remove report categories as required.

Each report that is created must have a category defined. Any reports that are created without specifically selecting a Report Category will be categorized under (Uncategorized).

Adding Report Categories

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint for which you want to add a report category.
3. Click the **Report Categories** tab.
4. Click **Create Category**.
5. Type a name for the Category in the **Name** box.
6. Type a description for the type of reports being categorized in the **Description** box, if desired.
7. Click Save.

Deleting Report Categories

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint for which you want to remove a report category.
3. Click the **Report Categories** tab.
4. Click the **Delete** icon that corresponds with the Category you want to delete.
 Delete icon
5. Click **OK**.

To delete a report category without deleting the reports, edit the reports prior to deleting the report category, assigning them a new category, using (Uncategorized) if required.

Defining Reports for a VSC Blueprint

For information about defining reports, see the following topic:

[Creating Reports](#)

[Importing Reports from a File](#)

[Importing Reports from the Library](#)

The Reports window lists all currently configured reports that are available and can be edited from this location. Additional reports can be created or imported and advanced reporting can be configured from this window as well.

The View list may be used to change how the reports are presented. Grouped View has reports with the same report category grouped, and Single View lists the reports individually.

The following information is presented in both views, with Single View offering the ability to sort the table in ascending or descending order by clicking a column header.

Item	Description
Report	The title of the report.
Category	The assigned report category.
Type	Site or Device (see Types of Reports).
Description	The defined description of the report.
Predefined?	Whether or not the report was predefined. Note: Predefined Reports cannot be edited.
Preview	The preview is not applicable to VSC Blueprints since there are no devices, sites or reportable data.

Types of Reports

There are two types of reports that are used in Barracuda Managed Workplace:

Site Reports Provides information about a site.

Device Reports Provides information about devices at various sites.

Creating Reports

New reports may be designed using the Report Creator. Each report will contain sections and section contents, which are determined when a report is created.

If you are familiar with SQL Reporting Services, you can use it to do custom reporting against the database, but any new reports that are created should not be imported to run or be viewed. It is possible to copy the .RDL files for the predefined reports to use these as a base, but it is vital that the reports not be imported back if you choose to do so.

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint for which you want to add a report.
3. Click the **Reports** tab.
4. Click **Add Report**.
5. Click the **Properties** tab.
6. Type a Name and Description for the report in the corresponding boxes.
7. Select a category for the report from the **Category** list.
8. Select either the **Site** or **Device** option button to define the type of
9. In the **Logo** section, select one of the following option buttons:
 - **No Image**
 - **Existing Image**
 - **New Image**
10. If you selected:
 - **Existing Image**, select the image from the list.
 - **New Image**, click **Browse**. In the **Choose File** dialog box that appears, locate the new image file and click Open.
11. Click the Content tab.
12. In the Report Sections area, select the check boxes that correspond with the sections you want to include in the report.
13. For each selected section, select the check boxes that correspond with the desired section content. (This is on the right side of the window.)

Remember that when creating reports you should only request the data that is relevant to the report's intended audience. The more items chosen from the report selectors for a report, the longer it will take to generate the report. This is especially true when reporting on Patch Management items, where there are a great number of filtering options and patches, performance can be less than optimal depending on how much data is being parsed.

Importing Reports from a File

1. Save the .ZIP file to an accessible location.
2. In the Hosted Console website, click **Configuration > VSC Blueprints**.
3. Click the **Reports** tab.
4. Click **Import From File**.
5. Click **Browse**.

6. Browse to the .ZIP file and select it.
7. Click **Open** to populate the path.
8. Click **Import**.
9. Click **Close**.

The report will now appear in the Report Categories section under the defined category or under (Uncategorized) if no category has been defined. The report is also added to the report library within Service Center.

Importing Reports from the Library

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint for which you want to import a report from the library.
3. Click the **Reports** tab.
4. Click **Import From Library**.
5. From the list, select the report you want to import.
6. Click **Import**.

The report will now appear in the Reports listing under the defined category or under (Uncategorized) if no category has been defined.

Defining Roles for a VSC Blueprint

For information about defining roles, see the following topics:

[Setting Up and Managing User Roles](#)

[Creating Roles](#)

[Information tab](#)

[Members tab](#)

[Permissions Tab](#)

[Applying Roles to Users](#)

[Modifying Roles](#)

[Deleting Roles](#)

Setting Up and Managing User Roles

The Roles window lists all roles that are available for use with Barracuda Managed Workplace.

The default roles that are provided with Barracuda Managed Workplace are listed in the table below.

Item	Description
Administrator	Members have Read and Modify access to all objects in Service Center. This role cannot be renamed or have its access permissions modified.
Technician	Members have Read access to all objects in Service Center, and modify access to all objects except Patch Management Initial Setup, Report Categories, User Management, System Settings and Service Desks. Members can initiate remote control sessions, receive email alerts, and have trouble tickets assigned to them. This role can be renamed or modified.
Customer	Members have Read access to all Status and Site Inventory objects, and modify access to Allow Trouble Ticket Assignment. Members can have trouble tickets assigned to them. This role can be renamed or modified.
Sales	Members have Read access to the Central Dashboard, Site Inventory, and Reporting. This role can be renamed or modified.
Guest	Members have Read access to all Status objects. This role can be renamed or modified.
Service Manager	Members have Read access to all objects in Service Center except Report Categories, User Management, System Settings and Service Desks, and Modify Access to Device Management, Alerts, Trouble Tickets, and Reporting. Members can initiate remote control sessions and have trouble tickets Assigned to them. This role can be renamed or modified.

If an attempt is made to access an area of Service Center that is not permitted by the roles of which a user is a member, a warning message appears notifying the user that they are not authorized to view that page.

Roles define the areas of Service Center that may be accessed by users who are members of the role. Additionally, the roles determine whether or not a user may initiate remote control sessions, receive email alerts, or have trouble tickets assigned to them.

Coupled with the Object Access security on the user level that defines which sites, groups, devices and websites a user may access, roles comprise the Barracuda Managed Workplace security model.

When a user is a member of more than one role with different access permissions, the least restrictive security settings will apply.

For more information, see the following topics:

[Creating Roles](#)

[Applying Roles to Users](#)

[Deleting Roles](#)

Creating Roles

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint for which you want to create a role.
3. Click the **Roles** tab.
4. Click **Create Role**.
5. Type a name to identify the role in the **Role Name** box.
6. Click **Create Role**.
A Windows Internet Explorer dialog prompts "Would you like to configure 'Role Name' now?"
7. Click **OK**.
8. Click the **Members** tab.
9. Click **Add User**.
10. Choose a user to add as a Role Member.
11. Click **OK**.
12. Repeat steps 9 to 11 until all desired users have been added.
13. Click the **Permissions** tab.
14. Configure the permissions for the role. See Permissions Tab.
15. Click **Save**.

Information tab

The **Role Information** tabbed page of the **Role Configuration** window displays the Role Name in the **Role Identification** section.

Members tab

The **Members** tabbed page of the **Role Configuration** window displays a listing of all Role Members.

Permissions Tab

The **Permissions** tabbed page of the **Role Configuration** window is where the accessible areas of Service Center are defined for members of the role. Additionally, whether or not a member may initiate remote control sessions, receive Email and Pager Alerts, or have trouble tickets assigned to them is defined using this tab.

A check mark in the **Read** column indicates that Role Members are able to access the corresponding

item in Service Center for viewing. A check mark in the Modify column indicates that Role Members are able to take actions and modify the contents of the corresponding item in Service Center.

Permission	Description
Device Management	Read and Modify Options <ul style="list-style-type: none"> • Device Management Other Options • Remote Control Access (when enabled, the role members will be able to initiate remote control sessions) • Onsite Manager Utilities (when enabled, the role members will be able to access the Onsite Manager Utilities)
Alerts	Read and Modify Options <ul style="list-style-type: none"> • Alerts Other Options <ul style="list-style-type: none"> • Receive Alert Notifications (when enabled, the role members will be able to be notified when alerts occur) • Receive Escalation Notifications
Status	Read and Modify Options <ul style="list-style-type: none"> • Central Dashboard • Devices • Device Search • Network Services • Websites
Site Inventory	Read and Modify Options <ul style="list-style-type: none"> • Windows Inventory • SNMP Inventory
Patch Management	Read and Modify Options <ul style="list-style-type: none"> • Overview • Patch Approval • Reports • Settings • Windows Update Agent Policies • Approval Groups

Applying Roles to Users

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that you want to work with.
3. Click the **Users** tab.
4. Click the name of the user in the **User** column.
5. Click the **Roles** tab.
6. Click **Add Role**.
7. From the list, select the role to you want to add.
8. Click **OK**.
9. Repeat steps 6 to 8 until all additional roles are added.
10. Click **Save**.

Modifying Roles

To modify a role

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint for which you want to modify a role.
3. Click the **Roles** tab.
4. Click a role name.
5. Click the **Role Information** tab.
6. If desired, enter a new value in the **Role Name** box.
7. Click the **Members** tab.


To add users

1. Click **Add User**.
2. A list of available users appears.
3. Choose a user to add as a Role Member.
4. Click **OK**.
5. Repeat the above steps until all desired users have been added.

To remove users

1. Click the **Remove** button that corresponds with the user you want to remove.
2. Click the **Permissions** tab.
3. Configure the permissions for the role. See [Permissions Tab](#).
4. Click **Save**.

Deleting Roles

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint for which you want to delete a role.
3. Click the **Roles** tab.
4. Click the **Delete** icon that corresponds with the role you want to delete.
 Delete icon
5. Click **OK**.

When a role is deleted, the users who were members of the role will no longer have the access provided by the removed role.

Defining Users for a VSC Blueprint


See the following topics for information about defining roles:

[Setting Up and Managing Users](#)

[Managing Users](#)[Creating User Accounts](#)[Removing User Accounts](#)[Modifying User Accounts](#)[User Configuration Window Profile Tab](#)[User Configuration Window Roles Tab](#)[User Configuration Window Object Access Tab](#)**Setting Up and Managing Users**

The **Users** window lists all users that are available for use with Barracuda Managed Workplace.

The following information is presented for each user:

Item		Description
User		The login name for the user.
First Name		The first name of the person assigned the user account.
Last Name		The last name of the person assigned the user account.
Role Assigned?		True = The user is a member of at least one role. False = The user is not a member of any roles.
Status		The user is enabled. The user is not enabled.
Delete		Click the Delete hyperlink to remove the user.

If an attempt is made to access an area of Service Center that is not permitted by the roles of which a user is a member, a warning message appears notifying the user that they are not authorized to view that page.

For more information about users in Barracuda Managed Workplace, see [Managing Users](#).

Managing Users

Users define the logon name and password for individuals requiring access to the Service Center website, and their personal information. Users are additionally provided with Object Access permissions to define which sites, groups, devices and websites may be accessed. Each user must

also be a member of at least one role.

Coupled with the Permissions security defined in the role, users comprise the Barracuda Managed Workplace security model.

When a user is a member of more than one role with different access permissions, the least restrictive security settings will apply.

For more information, see the following topics:

[Creating User Accounts](#)

[Removing User Accounts](#)

[Modifying User Accounts](#)

[Creating User Accounts](#)

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that you want to work with.
3. Click the **Users** tab.
4. Click **Create User Account**.
5. Type the logon name to be used in the **User Name** box.
6. Type the corresponding personal information in the **First Name** box.
7. Type the corresponding personal information in the **Last Name** box.
8. Type the account password in the **Password** box.
9. Type the account password in the **Confirm Password** box.
10. Type the corresponding personal information in the **Email** box.
This is the email address where email alerts will be sent, if applicable.
11. Choose whether the user is Active or Disabled using the **Account is Disabled** check box.
12. Click **Create User**.
13. Confirm all information is accurate on the **Profile** tab.
14. Click the **Roles** tab and see [User Configuration Window Roles Tab](#) for instructions about adding roles to the user.
15. Click the **Object Access** tab and see [User Configuration Window Object Access Tab](#) for instructions about configuring Object Access for the user.
16. Click **Save**.

Removing User Accounts

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that you want to work with.
3. Click the **Users** tab.
4. Click the **Delete** icon that corresponds with the user account you want to delete.

✖ Delete icon

5. Click **OK**.

Modifying User Accounts

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that you want to work with.
3. Click the **Users** tab.
4. Click the name of the user in the User column.
5. Make any required adjustments in the **Profile**, **Roles**, and **Object Access** tabs.

For more information, see the following topics:

[User Configuration Window Profile Tab](#)

[User Configuration Window Roles Tab](#)

[User Configuration Window Object Access Tab](#)

6. Click **Save**.

User Configuration Window Profile Tab

The Profile tabbed page of the User Configuration window displays the personal information for the user, including the email address that is used to send email alerts, the status of the user. Additionally, the user account may be locked out or disabled, or the password reset from this location.

The User Identification section presents the following information:

To reset a user password

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that you want to work with.
3. Click the **Users** tab.
4. Click the name of the user in the **User** column.
5. Click **Reset Password**.
6. Type a new password in the box.
7. Type the same password in the **Confirm New Password** box.
8. Click **Save**.

To lock out a user:

1. Launch and log into the Hosted Console website.
2. In the main menu, click **Configuration**.
3. In the **Configuration** menu, click **VSC Blueprints**.
4. In the **Blueprints** list, click the blueprint that you want to work with.
5. Click the **Users** tab.
6. Click the name of the user in the User column.
7. Select the Account is Locked Out check box.
8. Click **Save**.

A user whose account has been locked out may not login to the VSC website until the account has been unlocked by an Administrator. An account is locked out to prevent unauthorized access attempts, but does not affect any other aspect of the user account. The user will continue to receive notifications in the usual manner.

To disable a user

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that you want to work with.
3. Click the **Users** tab.
4. Click the name of the user in the **User** column.
5. Select the **Account is Disabled** check box.
6. Click **Save**.

A user whose account has been disabled may not login to the VSC website until the account has been enabled by an Administrator. A user with a disabled account will not receive notifications.

User Configuration Window Roles Tab

The Roles tabbed page of the User Configuration window displays a listing of all roles of which the user is a member.

To add a role for an existing user

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that you want to work with.
3. Click the **Users** tab.
4. Click the name of the user in the **User** column.
5. Click the **Roles** tab.
6. Click **Add Role**.
7. Choose the role to add from the list that appears.
8. Click **OK**.
9. Click **Save**.

To remove a role for an existing user

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that you want to work with.
3. Click the **Users** tab.
4. Click the name of the user in the **User** column.
5. Click the **Roles** tab.
6. Click the **Remove** button that corresponds with the role you want to remove.
7. Click **Save**.

User Configuration Window Object Access Tab

The Object Access tabbed page of the User Configuration window is where more granular security controls are defined on the user level. Access to each site, service or site group, device, and website may be allowed or restricted from this tab. However, site, site group, device and website are not available for configuration in the VSC Blueprint editor.

To allow a user access to an object, it must be listed in the Object Access tab.

Item	Description
Sites	When a user is allowed access to a site, that user may access all service groups, site groups and devices that belong to the site.
Service Groups	When a user is allowed access to a service group, that user may access all devices from all sites that belong to the service group.
Site Groups	When a user is allowed access to a site group, that user may access all devices that belong to the site group.
Devices	When a user is allowed access to a device, that user may access all controls for the device. If a user is not allowed access to a group that contains the device, the user will be able to access the group but will only see devices to which access has been granted.
Websites	When a user is allowed access to a website, that user may access all controls for the website.

When the Administrators Role has been assigned to a user, the Object Access tab will note "This user is part of the Administrator role. As such, the user automatically has access to all Objects."

To add Object Access for an existing user

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that you want to work with.
3. Click the **Users** tab.
4. Click the name of the user in the **User** column.
5. Click the **Object Access** tab.
6. Click **Add**.
7. Choose the Object Type (Device, Group, Site or Website) from the **Choose the type of Object to add** list.
Note: In the VSC Blueprint editor, only the Group object type can be configured.
8. Click **OK**.
9. Select all required items from the list.
10. Click **Save**.

To remove Object Access for an existing User

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **Blueprints** list, click the blueprint that you want to work with.

3. Click the **Users** tab.
4. Click the name of the user in the **User** column.
5. Click the **Object Access** tab.
6. Select the check boxes that correspond with the Object Access you want to remove.
7. Click **Remove Selected**.
8. Click **Save**.

Working with Existing VSCs

You can associate an existing VSC with a VSC blueprint. A VSC can only be associated with one blueprint.

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **VSC blueprint** list, click the VSC blueprint that you want to associate with an existing VSC.
3. In the **Applied VARs** section, click **Add VAR**.
4. Select the check box of the VSC you want to associate with the selected VSC blueprint.
5. Click **OK**.

The VAR appears in the Applied VARs section of the VSC Blueprints Editor window.

Modifying Existing VSC Blueprints and Applying them to Existing VSCs

You can modify existing blueprints; however, there are restrictions on what can be modified and then applied to the existing VSCs that are associated with the blueprint. Only additions can be performed to existing VARs which includes importing policy modules, reports and scripts and applying policy modules to groups; also when applying More Actions, such as importing policy modules, reports and scripts to existing VARs, there is an option to add the content being imported to the VSC Blueprint. If the additions are applied with the option to update the VSC Blueprint, any new VSCs you create will automatically use the modified version of the blueprint.

If you do make changes to policy modules, reports or scripts, you will have to import them into the existing VSCs. If you are importing policy modules, then you also have to apply the policy module to the group.

To modify an existing VSC blueprint and apply it to an existing VSC

1. In the Hosted Console website, click **Configuration > VSC Blueprints**.
2. In the **VSC blueprint** list, click the VSC blueprint that you want to work with.
3. In the **Applied VARs** section, select the check box of the VSC to which you want to make changes.
4. Click **More Actions**.
5. Depending on the type of change you want to make, do one of the following:

- Import Policy Module from File or Import Policy Module from Library
 - Import Report from File or Import Report from Library
 - Import Script from File
6. If you chose to import a policy module, report, or script from a file, then in the **File Name** box, click **Browse** to search for the file. Select the file you want to import and then click **Open**. Click **Import**. Select the **Apply to Blueprint** check box to have the modification added to the VSC Blueprint.
 7. If you chose to import a policy module from the library, then select the check boxes that correspond with the policy modules you want to import. Or, select the check box at the top of the check box column to select all the check boxes. Click **Import**. Select the **Apply to Blueprint** check box to have the modification added to the VSC Blueprint.
 8. If you chose to import a policy module from either a file or the library, you can also apply the policy module to a group.
 1. Click **More Actions** and then select **Apply Policy Module to Group**.
 2. Select the groups to which you want to apply the policy module by enabling the corresponding check box and then click **Apply Policy Module**.
 3. Select the check box that corresponds with the policy module you want to apply to the group and click **OK**.
 4. Select the **Apply to Blueprint** check box to have the modification added to the VSC Blueprint.

Figures

1. delete_var_admin.gif
2. delete_var_admin.gif
3. var_active.gif
4. var_disabled.gif
5. delete_var_admin.gif

© 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.