Veritas NetBackup Appliance AutoSupport 2.0 Reference Guide

Release 3.0

Document Revision 2

VERITAS™

Veritas NetBackup Appliance AutoSupport 2.0 Reference Guide

Release 3.0

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

APPL.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

Introduction

This chapter includes the following topics:

Overview of AutoSupport

Veritas AutoSupport is a set of infrastructures, processes, and systems that enhance the support experience through proactive monitoring of Veritas Appliance hardware and software. AutoSupport also provides automated error reporting and support case creation.

Through automation, Internet access, and case management integration, Veritas can improve the support process and give our support engineers the tools to solve problems faster. The AutoSupport infrastructure within Veritas analyzes the Call Home data from each appliance to provide proactive customer support and incident response for hardware failures. This feature reduces the need for an administrator to initiate support cases. It also enables Veritas to better understand how customers configure and use appliances, and where improvements would be most beneficial. AutoSupport can also correlate the Call Home data with other site configuration data held by Veritas, for technical support and error analysis. With AutoSupport, Veritas greatly improves the customer support experience.

This document discusses many aspects of AutoSupport, including architecture (how it works), operation (how to configure it), security and data privacy, and technical detail (the data). It primarily focuses on the NetBackup 52xx, 5330 Appliances.

AutoSupport 2.0 supported platforms

AutoSupport 2.0 supports the following NetBackup Appliance platforms:

- NetBackup 5220 Appliance (software version 2.7.1 and above)

- NetBackup 5230 Appliance (software version 2.7.1 and above)
- NetBackup 5240 Appliance (software version 2.7.3 and above)
- NetBackup 5330 Appliance (software version 2.7.1 and above)

Additional information

For more information and additional documentation on Veritas Appliances, please visit the following Information Stores available on the Veritas website:

- NetBackup Appliance Home Page
- Veritas Technical Support Page
- Veritas Appliance Services Page

About Call Home

Your appliance can connect with a Veritas AutoSupport server and upload hardware and software information. Veritas support uses this information to resolve any issues that you might report. The appliance uses the HTTPS protocol and uses port 443 to connect to the Veritas AutoSupport server. This feature of the appliance is referred to as Call Home. It is enabled by default.

Call Home is not required, but it serves as a critical step to proactive customer support and incident response for failures.

The following table provides more details to what happens when Call Home is disabled.

Table 1-1 What happens when Call Home is disabled

Monitoring status	Failure routine

Call Home enabled	When a failure occurs, the following sequence of alerts occur:
	■ The appliance uploads all the monitored hardware and software information to a Veritas AutoSupport server.
	■ The appliance generates 3 kinds of email alerts to the configured email address.
	  ■ An error message by email to notify you of the failure once an error is detected.
	  ■ A resolved message by email to inform you of any failure once an error is resolved.
	  ■ A 24-hour summary by email to summarize all of the currently unresolved errors in the recent 24 hours.
	■ The appliance also generates an SNMP trap.

Table 1-1 What happens when Call Home is disabled *(continued)*

Monitoring status	Failure routine
Call Home disabled	No data is sent to the Veritas AutoSupport server. Your system does not report errors to Veritas to enable faster problem resolution.

Chapter 2

Architecture

This chapter includes the following topics:

Introduction to AutoSupport 2.0 architecture

With Appliance Release 2.7.1, a new architecture for both client and server is implemented to expand AutoSupport's ability to improve the customer's support experience. We have created a new client framework that provides modularity in alert management, component monitoring, and software monitoring. It also enables future advanced diagnostics capabilities.

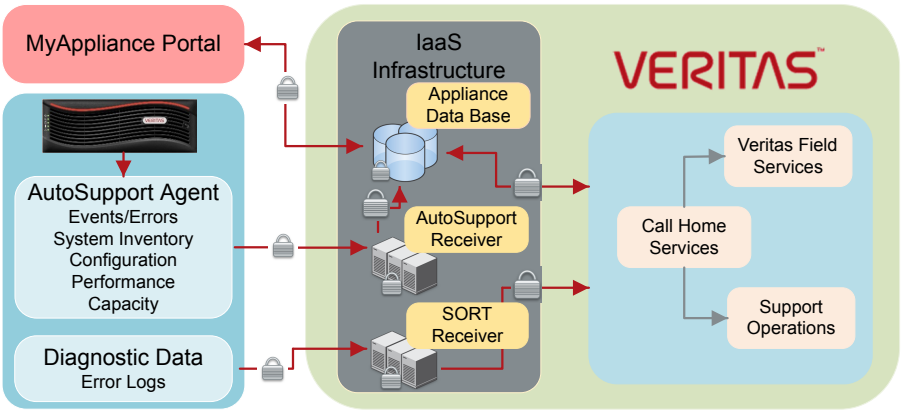
The AutoSupport 2.0 architecture for both client and server is implemented to expand AutoSupport's ability to improve the customer's support experience. Veritas AutoSupport introduces a framework that provides modularity in alert management, component monitoring, software monitoring. It also enables future advanced diagnostics capabilities.

AutoSupport components

The AutoSupport technology contains three major components: the AutoSupport client agent, the AutoSupport receiver, and the MyAppliance Portal.

The diagram below outlines the basic AutoSupport architecture.

Figure 2-1 AutoSupport 2.0 architecture



About the AutoSupport client agent

The AutoSupport client agent constantly monitors the appliance hardware and software components. It responds to critical events by collecting problem diagnostics data, system health data, and inventory data and transmitting it securely to Veritas via the CallHome infrastructure. Veritas Support uses the data to aid in diagnostics and troubleshooting.

Appliance hardware monitoring

Call Home monitors the following hardware components:

- CPU
- Disk
- Fan
- Power supplies
- Environmental telemetry data
  - System temperatures
  - System voltages
  - Fan speeds
  - BBU charge status
- RAID controllers

- RAID volume groups
- System temperature
- System board components by the Integrated Platform Management Interface (IPMI) and the Baseboard Management Controller (BMC) chip
- Storage subsystems (shelves and interconnects)

Appliance software monitoring

Software monitoring is based on the appliance model the monitoring agent is running on.

The AutoSupport client agent monitors the following data specific to application configuration and performance .

- Capacity utilization
- Firmware
- MSDP performance
- Application versions
- Operating system packages
- Patches and Engineering binaries and engineering bundles (EEBs)

About the Veritas Appliance monitoring infrastructure

The Veritas Appliance monitoring infrastructure comprises two independent recipient servers: the AutoSupport receiver and the SORT data receiver.

Veritas utilizes managed infrastructure as a service (IaaS) facility located within the continental United States to host this infrastructure and is highly redundant.

Veritas CallHome Services (CHS) teams are located in three geographically suited locations: the United States, Ireland, and Singapore to provide first-line global incident response and 24-hour monitoring.

Veritas Support includes Veritas CallHome Services, Veritas Enterprise Support Operations and Veritas Field Services, all of which are globally staffed for “Follow-the-Sun” support.

When an appliance transmits event data to Veritas, it is sent to the Veritas Appliance Monitoring infrastructure servers. In the event of a heartbeat failure, the CHS team is alerted. The appliance also transmits a `DataCollect` package to the SORT receiver, and an incident ticket is opened to track the status. A CHS engineer triages the incident and determines the course of action. The CHS engineer then escalates the issue to Support Operations or dispatches a hardware repair order to Veritas Field Services.

About the MyAppliance portal

The MyAppliance web portal provides a centralized registration and support experience as well as an Information Store for Veritas appliances. Within the portal, you can view support cases and additional information about their appliance(s). They can also access best practices and additional knowledge base articles, as well as register and maintain administrative contact and location information for appliances.

Note: Registering appliances on the MyAppliance portal is not required, but it serves as a critical step in the support process. Registration ensures Veritas's ability to contact the right person in the event of an identified appliance failure, and to dispatch field services to the correct location for repairs.

Call Home data transmission

The AutoSupport Client Agent transmits data on a routine basis to provide proactive monitoring and advanced diagnostics for support purposes. These data collections and transmissions are classified into 4 primary categories:

- Event data
- Configuration and Inventory data
- Telemetry and Performance data
- Diagnostic data

The following section describes each category, their transmission interval, and basic properties:

Event data condition

Interval:

- Immediately upon an event detection, such as a hardware or software fault or failure

Basic properties:

- Appliance mode (master or media server)
- Appliance state (healthy or not healthy)
- Serial number
- Time of failure
- Firmware versions

Extended attributes of only the failed components:

- Battery voltage level, charge state, etc.

System Inventory & Configuration Data

Interval:

- Once per 24 hours

Basic properties:

- Inventory of all hardware components including:
  - Manufacturer
  - Model
  - Serial Number
  - Type
  - Location
  - Firmware
  - Other component-specific metadata or attributes provided by the component vendor
- Configuration data including user-defined configuration states:
  - storage configuration
  - network information
  - feature enable/disable flags
- Telemetry and performance data:
  - Storage utilization
  - Extended attributes of certain components, for example, battery voltage, charge state, thermal sensor data, fan speeds, and power supply voltages.

DataCollect package

Interval:

- Every three days
- If a failure state is detected in the interim time, within 30 minutes, the `DataCollect` package is assembled, and the three-day transmission cadence resets.

Full diagnostic and hardware configuration inventory:

- Operating system diagnostics:
  - System message log (`/var/log/messages`)

- `dmesg` log
- Boot log
- Disk partition usage (`df -h` output)
- Memory state information
- `iostat` disk performance logs
- `vmstat` volume performance logs
- `vxfsstat` file system performance logs

- IPMI and chassis hardware:
  - IPMI alarm state log
  - IPMI sensor data
  - CPU diagnostic data
  - Field Replaceable Unit (FRU) chassis log
- RAID controllers:
  - RAID adapter logs
  - RAID Battery Backup Unit state log
  - LUN configuration data
- Storage subsystem:
  - Disk group information
  - Expansion shelf diagnostics
  - Enclosure diagnostics
  - Physical disk logs
  - SMART disk diagnostics
- Patch management:
  - Patch install logs

Chapter 3

Call Home security

This chapter includes the following topics:

Data security standards

All data that is transmitted to Veritas from an appliance is done with industry standard high encryption methods. The following data security standards are applied to all AutoSupport data sent between the client and server, and the data communication between the different components inside the client:

- AES-128/256/384 encryption
- RSA-1024/2048 encryption
- SHA-256/384 certification authentication
- TLS-encrypted transmission by HTTPS PUT over port 443/tcp

Note: The NetBackup Appliance 2.6.1.x only supports the SHA-1 certification authentication. Technical article 000108230 recorded this issue. Follow the instructions on the document to upgrade your appliance to enable CallHome support for SHA-256 certification authentication.

How the Call Home data is transmitted

All data that is transmitted to Veritas from an appliance is done with TLS-encrypted transmission by HTTPS PUT over port 443/tcp.

Registration data is sent to https://api.appliance.veritas.com

Call Home data is sent to https://receiver.appliance.veritas.com.

`DataCollect` packages are sent to https://sort.veritas.com.

Note: If you configure a proxy server on the appliance, the proxy must accept connections from the above mentioned URLs in order for the AutoSupport platform to work.

The infrastructure consists of a set of endpoints with a mix of static and dynamic IP pools for load balancing and high availability. Registration and Call Home data have static IP pools, whereas the `DataCollect` package transmission endpoint has a dynamic IP pool. Veritas highly recommends using DNS or fully qualified hostname resolution provisioning at the proxy and/or firewall level to reduce the chance of possible service interruptions.

Make sure you enable on the appliance, the proxy, and/or the firewall to outbound 443/TCP TLS socket connections to the URL's above.

For more information regarding the Call Home data transmission infrastructure, see the following technical article on Veritas Support website:

https://www.veritas.com/support/en_US/article.000126756

How the Call Home data is received and stored

All data transmitted to Veritas is held within a managed IaaS infrastructure within the continental United States.

Only specific authorized Support and Engineering personnel have access to the data through authenticated, audited and controlled access.

How long the Call Home data is maintained and held

Veritas maintains the data collected for the maintenance life-cycle of each machine, which is typically 5-7 years. Data may be aggregated and anonymized for further use internally for research and development purposes beyond these timelines.

Data privacy

Veritas AutoSupport collects limited configuration data that some customers may deem sensitive, such as the appliance hostname and IP addresses. This data is collected for the sole purpose of providing Veritas Technical Support with additional context for troubleshooting purposes. Veritas recognizes the sensitivity of this data in the eyes of the customer and upholds stringent security practices to secure it.

For more information on how Veritas manages customer privacy, visit https://www.veritas.com/about/privacy/.

Chapter 4

Configuring AutoSupport client settings

This chapter includes the following topics:

Enabling and disabling Call Home from the NetBackup Appliance Shell Menu

You can enable or disable Call Home from both, the NetBackup Appliance Web Console and the NetBackup Appliance Shell Menu. Call Home is enabled by default.

To enable or disable Call Home from the NetBackup Appliance Shell Menu

1. Log on to the NetBackup Appliance Shell Menu.
2. To enable Call Home, run the `Main > Settings > Alerts > CallHome Enable` command.
3. To disable Call Home, run the `Main > Settings > Alerts > CallHome Disable` command.

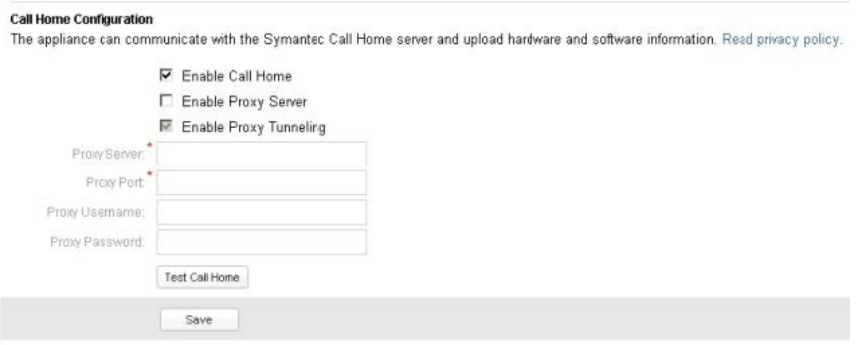
For more information on `Main > Settings > Alerts > CallHome` commands, refer to the *NetBackup Appliance Command Reference Guide*.

Configuring Call Home from the NetBackup Appliance Web Console

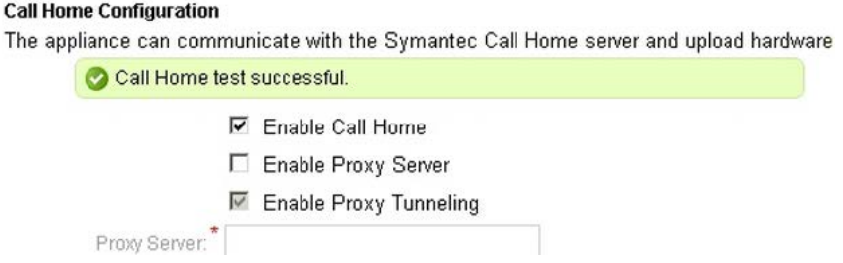
The following procedures describe how to use the NetBackup Appliance Web Console to configure Call Home on a NetBackup Appliance.

To configure Call Home on a 52xx appliance from the NetBackup Appliance Web Console

1. Log on to the NetBackup Appliance Web Console and navigate to the **Settings**> **Notification** > **Alert Configuration** page.
2. Select the **Enable Call Home** check box.



3. To test the Call Home functionality, click on Test Call Home at the bottom of the screen. The system attempts to push a heartbeat package to Veritas. Upon success, the following message appears:



4. Click **Save**.

Settings > Notifications > Alert Configuration

The **Settings > Notifications > Alert Configuration** page provides you with one location from where you can enable SNMP, SMTP, and Call Home alert notifications. The page is divided into three sections each dedicated to enable and provide details for **SNMP**, **SMTP**, and **Call Home**.

Under **Alert Configuration** is the **Notification Interval** field. You must enter the time interval in minutes between two subsequent notifications for the SNMP and the SMTP configurations. The time interval should be in multiples of 15 and it should not be zero.

Configuring SNMP

Table 4-1 lists the fields from the **SNMP** (Simple Network Management Protocol) section.

Table 4-1 SNMP Server Configuration settings

Fields	Description
Enable SNMP Alert	Select this check box to enable SNMP alert configuration.
SNMP Server	Enter the SNMP Server host name. You can enter a host name or an IP address to define this computer. The IP address can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed. Notification of the alerts or traps that are generated in Appliance are sent to this SNMP manager. **Note:** The NetBackup Appliance supports all the SNMP servers in the market. However, the ManageEngine™ SNMP server and the HP OpenView SNMP server are tested and certified for version 2.6.
SNMP Port	Enter the SNMP Server port number. If you do not enter anything for this variable, then the default port is 162. **Note:** Your firewall must allow access from the appliance to the SNMP server through this port.
SNMP Community	Enter the community to which the alerts or traps are sent. For example, Backup Reporting Department. You can enter a value that you configured on your SNMP server. For example, you can enter a company name or a name like, `admin_group`, `public`, or `private`. If you do not enter anything, then the default value is `public`.

The SNMP MIB file serves as a data dictionary that is used to assemble and interpret SNMP messages. If you configure SNMP, you must import the MIB file into the monitoring software so that the software can interpret the SNMP traps. You can check the details of the MIB file from the SNMP Server Configuration pane. To check details about the SNMP MIB file, click **View SNMP MIB file**. An SNMP MIB file opens.

For information on how to send a test SNMP trap after configuration, see the following technical article on the Veritas Support website:

www.veritas.com/docs/TECH208354

Configuring SMTP

The SMTP mail server protocol is used for outgoing email. You can configure SMTP from the NetBackup Appliance Web Console (**Settings > Alert Configuration > SMTP Server Configuration**).

You can also use the following command in the Shell Menu of your appliance to configure the SMTP server and add a new email account:

`Main_Menu > Settings > Alerts > Email SMTP Add` *`Server`* `[Account] [Password]`, where *`Server`* is the host name of the target SMTP server that is used to send emails. `[Account]` and `[Password]` are optional parameters to identify the name of the account and the account password if authentication is required.

For more information, see the related customer documentation of your appliance.

Table 4-2 lists the fields from the **SMTP** section of the NetBackup Appliance Web Console.

Table 4-2 SMTP Server Configuration settings

Fields	Description
SMTP Server	Enter the SMTP (Simple Mail Transfer Protocol) Server host name. Notifications of the alerts that are generated in Appliance are sent using this SMTP server. The IP address can be an IPv4 or IPv6 address. Only global-scope and unique-local IPv6 addresses are allowed.

Table 4-2 SMTP Server Configuration settings *(continued)*

Fields	Description

Software Administrator Email	Enter the email ID of the software administrator, to receive software alerts that are specific to the Veritas NetBackup Appliance software. This email ID that you designate receives alerts for the following software conditions:
	■ Host information such as:
	  ■ Disk information.
	  ■ Overall backup status.
	  ■ Results of last seven backups for each client.
	■ An email of your catalog backup disaster recovery file.
	■ A patch installation success report.

Hardware Administrator Email	Enter the email ID of the hardware administrator, to receive hardware alerts that are specific to the Veritas NetBackup Hardware Appliance. For example, hardwareadmin@usergroup.com for more information about potential hardware alerts.
Sender Email	Enter the email ID to receive any replies to the alerts or the reports that are sent by the Appliance.
SMTP Account	Enter the user name to access the SMTP account. **Note:** You maybe asked to enter a user name as some SMTP servers may require user name and password credentials to send an email.
Password	Enter the password for the above mentioned SMTP user account. **Note:** You maybe asked to enter a password as some SMTP servers may require user name and password credentials to send an email.

You can configure this server to send email reports to a proxy server or to the Veritas Call Home server.

The following describes the supported proxy servers:

- Squid
- Apache
- TMG

Note: NTLM authentication in the proxy configuration is also supported.

Starting with NetBackup Appliance 2.6.1.1, all email notifications that get generated by the appliance use the same SMTP settings. These emails include hardware monitoring notifications and NetBackup job notifications. The configuration settings are located under **Settings > Notification > Alert Configuration** in the NetBackup Appliance Web Console or `Main_Menu > Settings > Alerts` in the NetBackup Appliance Shell Menu. These settings override any previous SMTP setup you may have previously used to send NetBackup job notifications.

Note: If you had already configured the appliance SMTP settings before you upgraded to NetBackup Appliance 2.6.1.1, you may need to re-save the configuration in order for NetBackup to use it. In the NetBackup Appliance Web Console, go to **Settings > Notification > Alert Configuration** and click **Save**. Or in the NetBackup Appliance Shell Menu, go to `Main_Menu > Settings > Alerts` and resubmit the `SMTP` and `SenderID` settings.

Configuring Call Home

Table 4-3 lists the fields from the **Call Home Configuration** section.

Table 4-3 Call Home Configuration settings

Fields	Description
Enable Call Home	Select this check box to enable Call Home alert configuration.
Enable Proxy Server	Select this check box to enable proxy.
Enable Proxy Tunneling	Select this check box if your proxy server supports SSL tunneling.
Proxy Server	Enter the name of the proxy server.
Proxy Port	Enter the port number of the proxy server.
Proxy Username	Enter the user name to log into the proxy server.
Proxy Password	Enter the password for the user name to log into the proxy server.

When Call Home is enabled, you can test whether or not Call Home is working correctly by clicking the **Test Call Home** option that is available below the Call Home configuration settings.

Note: The **Test Call Home** option is active on the NetBackup Appliance Web Console only when Call Home is enabled.

The following describes the supported proxy servers:

- Squid
- Apache
- TMG

NTLM is the supported authentication method for Call Home proxy settings.

Configuring Alert Configuration settings

This section provides the procedure to configure the SNMP, SMTP, and Call Home server settings using the **Settings > Notification > Alert Configuration** page.

To configure the SNMP, SMTP, and Call Home server settings

1. Log on to the NetBackup Appliance Web Console.
2. Click **Settings > Notification > Alert Configuration**.

   The system displays the **Alert Configuration** page.

   The **Alert Configuration** page is divided into three sections to enable and provide details for **SNMP**, **SMTP**, and **Call Home**.
3. In the **Notification Interval** field enter the time interval in minutes between two subsequent notifications, for **SNMP**, **SMTP**, and **Call Home** alert configurations.
4. Enter the SNMP settings in the provided fields. A description of the SNMP parameters is available in Table 4-1.
5. Enter the SMTP settings in the provided fields. A description of the SMTP parameters is available in Table 4-2.

   The appliance uses the global server settings to send email notifications to the SMTP server that you specify.
6. Enter the Call Home settings in the provided fields. A description of the Call Home parameters is available in Table 4-3.
7. Click **Save**, to save the SNMP, SMTP, and Call Home settings.

Chapter 5

Configuring the MyAppliance portal

This chapter includes the following topics:

Configuring the MyAppliance portal

The MyAppliance portal is integrated with the MyVeritas portal and can be accessed directly at https://my.appliance.veritas.com or https://my.veritas.com. In either case, if you do not have a user account, you can click **REGISTER NOW** to register for a new Veritas Account Manager (VAM) user account at the portal. The VAM credentials also give you access to MyVeritas, MySupport, Customer Care, and other Veritas web portals.

Once the VAM credentials are validated, navigate to the **Appliances** tab to visit the MyAppliance web portal. From there, you can register appliances, view and edit existing registered appliances, view support cases, and inspect heartbeat data.

For more information on the MyAppliance portal, visit https://my.appliance.veritas.com.

See “Managing Veritas Support cases” on page 28.

Registering an appliance

The appliance registration is centralized to the MyAppliance portal.

Registering your appliance is a vital step in allowing Veritas the ability to help maximize availability of your appliance, and provide proactive monitoring support. Registration provides Veritas with accurate contact details and site-specific information, which aids in expediting support, field services, and customer notification of failures.

Registering also provides access to additional reporting capabilities for your appliances, such as:

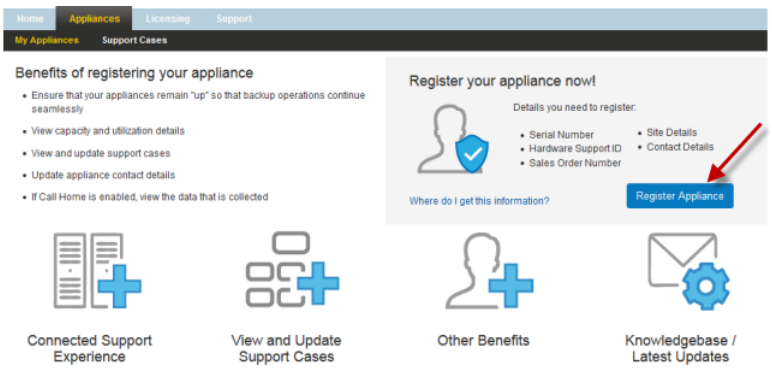
- An overview of all registered appliances
- Capacity and utilization details
- The ability to view and update support cases
- The ability to update contact and site information

Registration also ensures that you are alerted to product updates and other important information about your appliance.

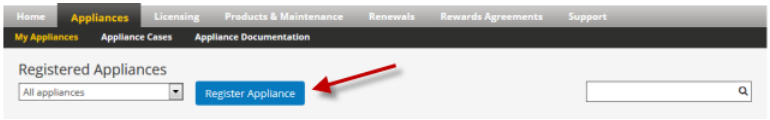
If your appliance has access either directly or through a proxy to the Internet, the registration details populate automatically. If the appliance is not provisioned, the message to verify and update the appliance registration information is displayed.

To register an appliance from the MyAppliance portal

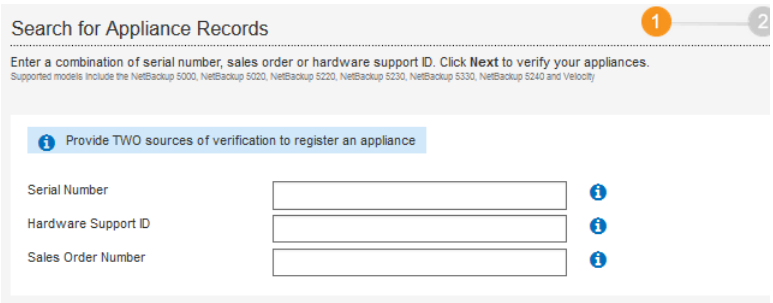
1. Log on to the MyAppliance portal and start the registration process with one of the following methods:
   - If it is your first visit to the portal, an information page appears. Click on **Register Appliance**.



- If you have previously registered appliances on your account, navigate to **Appliances > My Appliances** page and click on **Register Appliance**.

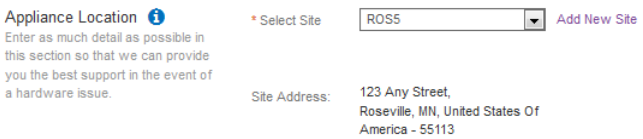


2 Input the sources of verification.

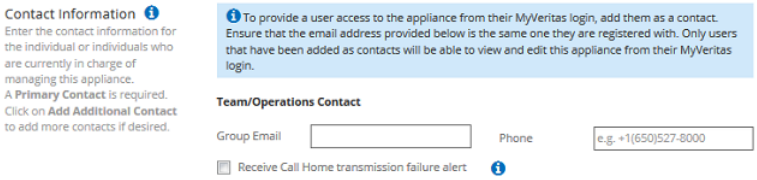


3 Verify your appliance status in the **Appliance Search Result** textbox.

4 Input the specific appliance details including the site of the appliance.



5 Add the contact information.



Note: Check the **Receive Call Home transmission failure alert** option if you want the MyAppliance portal to send you an email alert in the event that Veritas has not received a valid Call Home data transmission for over 28 hours. The alert will repeat every 24 hours until a valid data transmission is received.

6 Verify the information and click **Submit**.

Notification pops up to inform that your appliance is registered successfully.

Managing Veritas Support cases

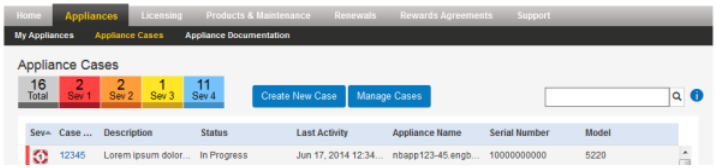
You can view, manage, and open Veritas Support cases from the **Appliances > Support Cases** page of the MyAppliance web portal.

See the section called “Viewing and managing Veritas Support cases” on page 28.

See the section called “Opening a Veritas Support case” on page 29.

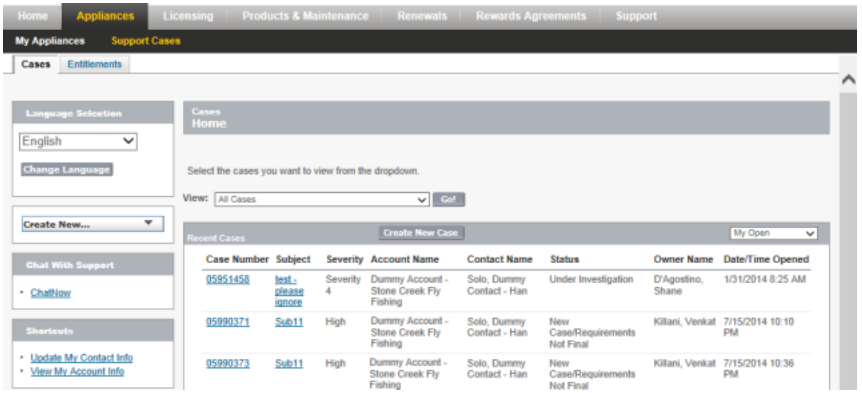
Viewing and managing Veritas Support cases

Log on to the MyAppliance web portal and navigate to the **Appliances > Support Cases** page to view and manage support cases. The page displays a list of your current appliance support cases.



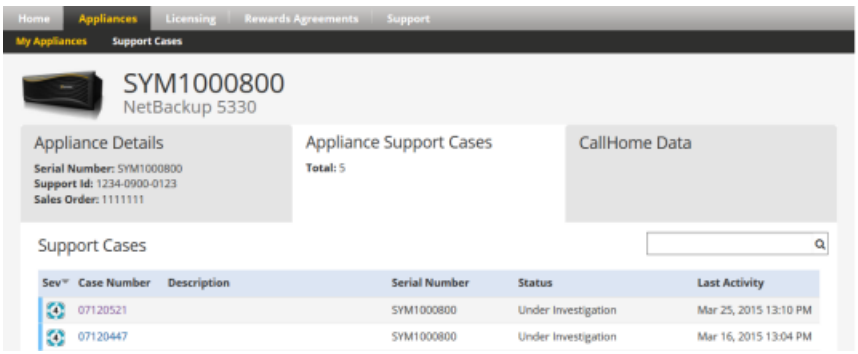
Click on any of the case numbers for further information.

You can also see a list of all of your open support cases, including the non-appliance cases, by clicking on **Manage Cases**. The following page appears:



Click on any of the case numbers for further information.

Specific details on appliance support cases are also available from the **Appliance > My Appliances** page of the MyAppliance portal. From the **Appliance > My Appliances** page, click on the appliance name in the **Registered Appliances** list, and navigate to the **Appliance Support Cases** tab. All open support cases for that appliance display in the **Support Cases** list.

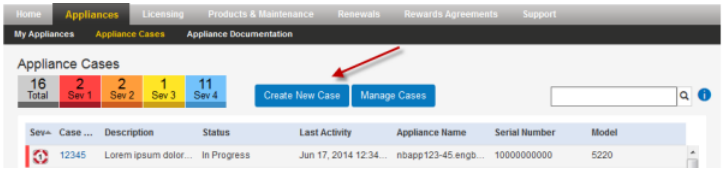


Opening a Veritas Support case

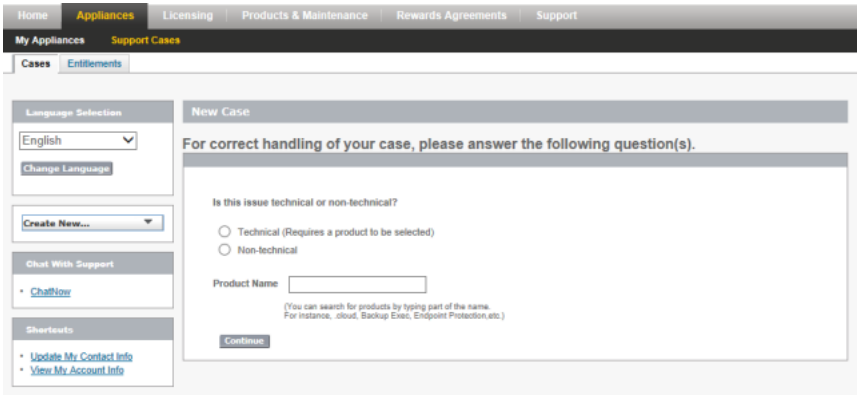
You can open a new support case from the **Appliances > Support Cases** page of the MyAppliance portal.

To open a new support case

1 Click on **Create New Case**.



2 The following page appears:

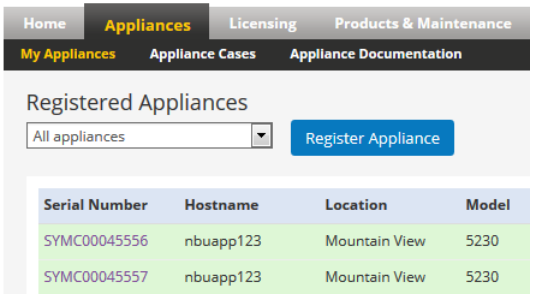


Input the appliance details and click **Continue** to open a new support case with Veritas Support.

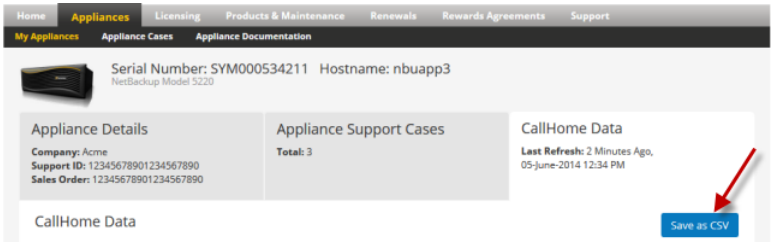
Obtaining a copy of your heartbeat and DataCollect packages

To obtain a copy of your heartbeat package

1 Log on to the MyAppliance portal, and select the desired appliance from the list of registered systems. Click on the desired appliance name from the first column.



2 Click the **CallHome Data** tab at the far right of the screen at the top of the appliance detail information. Note the last heartbeat timestamp, which indicates the transmission date and time. You can inspect the heartbeat data within the window, or you can click **Save as CSV** to export a copy of the data as a comma-separated value list.



To obtain a copy of your DataCollect package

1. Log on to the Appliance Shell Menu and run the `Support > DataCollect` command. The collection process takes several minutes and completes with the following message:

   ```
   All logs have been collected in /tmp/DataCollect.zip
   Log file can be collected from the appliance shared folder -
   \\<hostname>\logs\APPLIANCE
   Share can be opened using Main->Support->Logs->Share Open
   ```

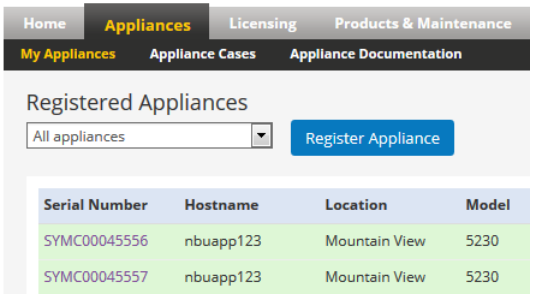
2. Retrieve the package file with the `Support > Logs > Share Open` command.

Unregistering an appliance

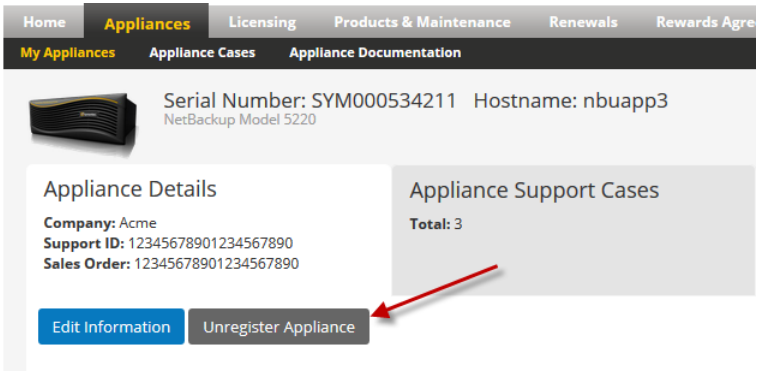
If an appliance is decommissioned or otherwise removed from your environment, you can unregister it from the **Appliances > My Appliances** page of the MyAppliance portal.

To unregister an appliance

1 From the **Appliances > My Appliances** page, click on the appliance that you want to unregister.



2 On the appliance **Details** page that appears, click **Unregister Appliance**.



3 A confirmation pop-up window appears. Click **Confirm Unregister**.

Chapter 6

NetBackup Product Improvement Program

This chapter includes the following topics:

About the NetBackup Product Improvement Program

The NetBackup Product Improvement Program is a feature that allows NetBackup to collect deployment and usage data periodically. The collected information helps identify how customers deploy and use NetBackup. For example, the collected data assists in identifying which features are used most often and what the usage patterns of those common features are. The aggregated data allows the NetBackup development and support teams to plan product improvements for ease of use, performance, installation, and many other product areas.

Participation in the Product Improvement Program is enabled by default on NetBackup appliances, with the default AutoSupport Call Home functionality. Disabling Call Home also disables the extended collection of product telemetry data.

The data that is collected and transmitted includes deployment and usage information, as follows:

Deployment information:

- Hardware and software configuration specifics of each server:
  - IP address, IP type
  - Fully qualified domain name (FQDN)
  - Alias, host name, host ID, platform, and architecture
- CPU name, type, clock speed, etc.
- Time zone
- Environmental language
- Operating system version level
- Memory size
- Licensed NetBackup software version
- Licensed NetBackup software features and installed packages
- Additional Veritas packages that are installed
- NetBackup Appliance deployment information

Usage information:

- Client counts by policy type and platform
- Media server counts by NetBackup version and platform
- Policy count by policy type
- Media counts by media on hold and retention level
- Storage Lifecycle Policy (SLP) counts by operation type

How Veritas uses the NetBackup Product Improvement Program data

The information that is collected through the Product Improvement Program is automatically and asynchronously transferred to Veritas periodically, through secure channels.

Veritas uses the collected information internally for statistical product deployment analytics to do the following:

- Identify and analyze trends and comparisons in the aggregated install base.

- Understand NetBackup licensed software product hardware and software deployment configurations.
- Improve Veritas products and services.
- Enhance technical support issue research.

How the NetBackup Product Improvement Program data is transmitted

The NetBackup Product Improvement Program communicates using Secure Socket Layer (SSL) over port 443/tcp. The system needs to be able to access the host https://telemetry.veritas.com.

Example communication flow

1. Test access and open a port to https://telemetry.veritas.com
2. Perform a HEAD request on `/data/uploader/nbupload.conf`
3. Perform a GET request on `/data/uploader/nbupload.conf`
4. Perform a POST operation to `/uploader/submit/nb`

The client system initiates all communication. Some communications are bidirectional when the appliance requests data that is hosted on the telemetry system.

For example, the GET request provides an ability to dynamically update the collection parameters without installing or updating a normal patch or release. These dynamic updates are only collection updates, and the process does not deploy any additional code to the client. The most typical updates are changes in collection parameters, such as a command flag, or the addition of running a NetBackup command to collect additional configuration and run-time information.

Data privacy

The Veritas NetBackup Product Improvement Program does not track personally identifiable data, nor does it transfer information about the specific data that the software protects. To learn more on what information we collect or process about you and what we do with this information when you use Veritas NetBackup Appliance, see theVeritas NetBackup Appliance Privacy Notice.

If you want to inspect the data that is sent to Veritas, it is located in the root file system of the appliance:

`/var/symantec/telemetry/telemetry<timestamp><randomstring>/DATA/nb-install/1/telemetry_data.json`

For example,
`/var/symantec/telemetry/telemetry201402241031WdH/DATA/nb-install/1/telemetry_data.json`

You can also use the MyAppliance portal to check the Call Home data that is sent to Veritas.

See "Obtaining a copy of your heartbeat and DataCollect packages" on page 31.

Enabling or disabling the NetBackup Product Improvement Program

The NetBackup Product Improvement Program is automatically enabled by default upon installation of a NetBackup integrated appliance. You can disable the Product Improvement Program in two ways:

- By disabling Call Home
  By default, the NetBackup Product Improvement Program is tied to the Call Home enablement function. To enable or disable the Product Improvement Program, enable or disable Call Home.

  Note: Disabling Call Home is not recommended, as it affects the appliance's ability to report error conditions to Veritas, as well as delay the time to repair in failure situations.

- By editing the `bpsetconfig` file
  To edit the `bpsetconfig` file, log on to the NetBackup Appliance Shell Menu as a `NetBackupCLI` user and run the following command:
  `/usr/openv/netbackup/bin/bpsetconfig -set TELEMETRY_UPLOAD=NO`
  The attribute is stored in `/usr/openv/netbackup/bp.conf`

  Note: Since the NetBackup Product Improvement Program is also tied to the Call Home enablement function, disabling or enabling the Call Home functionality at any time resets the `TELEMETRY_UPLOAD` value back to a factory default state.

NetBackup Product Improvement Program proxy configurations

The NetBackup Product Improvement Program supports proxy configurations.

To configure a proxy for the Product Improvement Program on an appliance

1. Log on to the NetBackup Appliance Shell Menu as a `NetBackupCLI` user and run the following command:

   `/usr/openv/netbackup/bin/nbtelemetry`

2. Use the following commands to complete the configuration:

`--proxy-server=SERVER:PORT`	Specify the proxy server to be used during upload. For example, http://proxy.example.com:8080
`--proxy-username=USERNAME`	Specify the user name (if required) to be used with the proxy server during upload.
`--proxy-password=PASSWORD`	Specify the password (if required) to be used with the user name during upload.

3. When the proxy configuration is complete, make sure that the proxy server settings allow connections from the following URLs:

   - https://receiver.appliance.veritas.com (appliance registration data)
   - https://sort.veritas.com (`DataCollect` packages)

Appendix A

Frequently Asked Questions

This appendix includes the following topics:

Frequently asked questions

Which Veritas appliances support the Veritas AutoSupport functionality?

The Veritas AutoSupport functionality is currently implemented in the following appliances:

- The Veritas NetBackup 50xx De-duplication Appliance, software version D1.2 or later
- The Veritas NetBackup 52xx and 5330 Appliance, software version 2.7.1 or later
- The Veritas Backup Exec 3600 Appliance, software version 2.0.189 or later

---

Note: Appliances running on earlier versions of software can upgrade to the latest appliance-specific software release for proactive hardware monitoring capabilities.

Is Veritas AutoSupport a free service?

Yes, Veritas AutoSupport is included at no extra cost with the maintenance services purchased with the appliance. Veritas AutoSupport is aimed to improve the registration and support experience for appliance customers. The long term mission of AutoSupport is to provide high reliability, availability, and serviceability to the Veritas appliance.

Does AutoSupport allow remote changes or monitoring of any process, operation, or functionality on the device?

Current appliance releases do not provide any remote access or configuration change capability.

Does the appliance verify any certificate revocation lists (CRL) when it connects to the AutoSupport service?

Veritas does not validate client-side certificates, as they are self-signed.

Is the AutoSupport service certificate issued by a trusted certification authority?

Veritas VeriSign™ uses Symantec VeriSign™ Root Authority for the URLs that AutoSupport uses.

Does the appliance support local root certificate authorities so that it can be intercepted and scanned, and block content of the HTTPS flow?

No.

Can the Call Home process submit any data that is stored on the NetBackup target volumes?

No. The Call Home data collector only looks at volume performance metadata and does not inspect the content of the data that is stored on the volumes.

Can you provide an assurance that a file cannot be copied off of the appliance and transmitted?

The system is designed to sweep a designated directory structure for files to be packaged as part of the `DataCollect` process. A file can possibly be copied to that directory structure and subsequently transmitted to Veritas. However, the timing of such a process is precise, and the data is not held for any length of time before transmission.

Is Call Home an outbound connection only?

Call Home is an outbound-only connection.