

Veritas™ Appliance AutoSupport Reference Guide

Veritas™ Appliance AutoSupport Reference Guide

Last updated: 2019-12-03

Legal Notice

Copyright © 2019 Veritas Technologies LLC. All rights reserved.

Veritas, the Veritas Logo, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This product may contain third-party software for which Veritas is required to provide attribution to the third party ("Third-party Programs"). Some of the Third-party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Refer to the Third-party Legal Notices document accompanying this Veritas product or available at:

<https://www.veritas.com/about/legal/license-agreements>

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Veritas Technologies LLC and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Veritas as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<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

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://www.veritas.com/content/support/en_US/dpp.Appliances.html

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	Product overview	6
	Overview of AutoSupport	6
	About Call Home	7
Chapter 2	Architecture	9
	Introduction to AutoSupport architecture	9
	AutoSupport components	9
	About the client agent	10
	About the Veritas Appliance monitoring infrastructure	11
	About the MyAppliance portal	12
	Call Home data transmission	12
Chapter 3	Call Home security	15
	Data security standards	15
	How the Call Home data is transmitted	15
	How the Call Home data is received and stored	16
	How long the Call Home data is maintained	16
	Data privacy	17
Chapter 4	Configuring client settings on NetBackup and Access appliances	18
	Enabling and disabling Call Home from the appliance shell menu	18
	Enabling and disabling Call Home from the NetBackup Appliance Web Console	19
	Settings > Notifications > Alert Configuration	20
	Configuring alert settings	25
Chapter 5	Configuring client settings on a Flex appliance	26
	Viewing Call Home information	26
	Configuring Call Home settings	27
	Deleting and disabling Call Home settings	29

Chapter 6	Using the MyAppliance portal	31
	Configuring the MyAppliance portal	31
	Registering an appliance	32
	Obtaining a copy of your Heartbeat packages	35
	Unregistering an appliance	35
Chapter 7	NetBackup Product Improvement Program	36
	About the NetBackup Product Improvement Program	36
	How Veritas uses NetBackup Product Improvement Program data	37
	How NetBackup Product Improvement Program data is transmitted	38
	Data privacy	38
	Enabling or disabling the NetBackup Product Improvement Program	39
	NetBackup Product Improvement Program proxy configurations	39
Appendix A	Frequently Asked Questions	41
	Frequently asked questions	41

Product overview

This chapter includes the following topics:

- [Overview of AutoSupport](#)
- [About Call Home](#)

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 correlates 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).

AutoSupport supported platforms

AutoSupport supports the following appliance platforms:

- NetBackup 5230 Appliance (software version 2.7.1 and above)

- NetBackup 5330 Appliance (software version 2.7.1 and above)
- NetBackup 5240 Appliance
- NetBackup 5340 Appliance
- Veritas 5150 Appliance
- Veritas 5340 Appliance
- Access 3340 Appliance

Additional information

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

- [Veritas Appliance Home Page](#)
- [Veritas Technical Support Page](#)
- [Veritas Appliance Services Page](#)

About Call Home

Your appliance can connect with a Veritas server and upload hardware and software information. Veritas Technical 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 server. This feature of the appliance is referred to as Call Home. It is enabled by default.

Note: 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 about what happens when Call Home is enabled or disabled.

Table 1-1 What happens when Call Home is enabled or disabled

Monitoring status	Failure routine
Call Home enabled	<p data-bbox="639 322 1213 348">When a failure occurs, the following sequence of alerts occur:</p> <ul data-bbox="639 366 1213 791" style="list-style-type: none"><li data-bbox="639 366 1213 418">■ The appliance uploads all the monitored hardware and software information to a Veritas server.<li data-bbox="639 427 1213 479">■ The appliance generates the following three kinds of email alerts to the configured email address:<ul data-bbox="666 487 1213 670" style="list-style-type: none"><li data-bbox="666 487 1213 539">■ An error message by email to notify you of the failure once an error is detected.<li data-bbox="666 548 1213 600">■ A resolved message by email to inform you of any failure once an error is resolved.<li data-bbox="666 609 1213 661">■ A 24-hour summary by email to summarize all of the currently unresolved errors in the recent 24 hours.<li data-bbox="639 670 1213 756">■ Starting from software release 2.7.1, Veritas an email alert is sent if Veritas servers do not receive any Call Home data from your appliance for over 28 hours.<li data-bbox="639 765 1213 791">■ The appliance also generates an SNMP trap.
Call Home disabled	<p data-bbox="639 822 1213 900">No data is sent to the Veritas AutoSupport server. Your system does not report errors to Veritas to enable faster problem resolution.</p>

Architecture

This chapter includes the following topics:

- [Introduction to AutoSupport architecture](#)
- [AutoSupport components](#)

Introduction to AutoSupport architecture

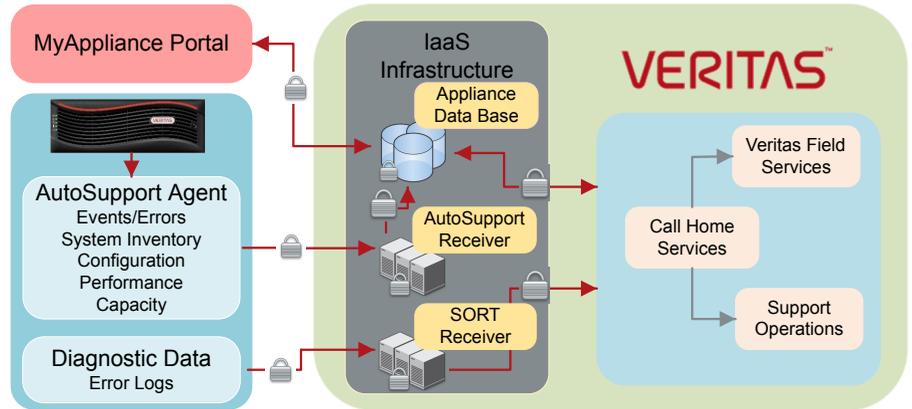
With Appliance Release 2.7.1, a new architecture for both client and server is implemented AutoSupport to expand Veritas's ability to improve customer support. We have created a new client framework that provides modularity in alert management, component monitoring, and software monitoring. It also enables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

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 architecture



About the client agent

The 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 Call Home infrastructure. Veritas Support uses the data to aid in diagnostics and troubleshooting.

Appliance hardware monitoring

Call Home monitors the following hardware components as they apply to your specific appliance model:

- 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 of the monitoring agent.

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

- Capacity utilization
- Firmware
- MSDP performance
- Application versions
- Operating system packages
- Patches, updates, and Emergency Engineering Binaries (EEBs)

About the Veritas Appliance monitoring infrastructure

The Veritas Appliance monitoring infrastructure comprises two independent recipient servers: the receiver and the API endpoint.

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

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

Veritas Support includes Veritas Call Home 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 API endpoint, 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. You 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 helps Veritas 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 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 during this time the `DataCollect` package is assembled within 30 minutes. The three-day transmission cadence resets.

File locations

- NetBackup files are located at `/log/DataCollect.zip`

- Flex files are located at `/log/autosupport/DataCollect.zip`

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

Call Home security

This chapter includes the following topics:

- [Data security standards](#)
- [How the Call Home data is transmitted](#)
- [How the Call Home data is received and stored](#)
- [How long the Call Home data is maintained](#)
- [Data privacy](#)

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:

- RSA 2048 bit keys for server authentication
- AES 128/256 bit keys for data encryption
- SHA1, SHA2 (256/384 bit) hashes for message 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.

Beginning with NetBackup Appliance release 3.1 transmissions for the following services are sent to <https://api.appliance.veritas.com>.

- Appliance CallHome Provisioning

- DataCollect packages
- Virtual Appliance Serialization data

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 static IP address pools for data transmission.

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.

If your firewalls can only register entities by IP addresses the static endpoints retain their respective dedicated IP address pools.

On the appliance make sure you enable the proxy and/or the firewall to outbound 443/TCP TLS socket connections to the following site.

<https://api.appliance.veritas.com>.

Prior to release 3.1 the datacollect packages were sent to <https://sort.veritas.com>.

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

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 practices to secure it. Veritas AutoSupport adheres to the European GDPR rules and regulations.

For more information about how Veritas manages customer privacy and our commitment to GDPR refer to the following site.

<https://www.veritas.com/about/privacy/>.

Configuring client settings on NetBackup and Access appliances

This chapter includes the following topics:

- [Enabling and disabling Call Home from the appliance shell menu](#)
- [Enabling and disabling Call Home from the NetBackup Appliance Web Console](#)
- [Settings > Notifications > Alert Configuration](#)
- [Configuring alert settings](#)

Enabling and disabling Call Home from the appliance shell menu

You can enable or disable Call Home from the appliance shell menu. Call Home is enabled by default.

Note: For Call Home to work properly, you need to register your appliance. You can register your appliance from the **Appliances > My Appliances** page of the [MyAppliance portal](#).

To enable or disable Call Home from the shell menu

- 1 Log on to the 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 the NetBackup appliance `Main > Settings > Alerts > CallHome` commands, refer to the *NetBackup Appliance Commands Reference Guide*.

For more information on the Access Appliance `Main > Settings > Alerts > CallHome` commands, refer to the *Access 3340 Appliance Initial Configuration and Administration Guide*.

For information about Call Home settings for the Flex 5340 Appliance refer to the following sections.

See [“Configuring Call Home settings”](#) on page 27.

See [“Deleting and disabling Call Home settings”](#) on page 29.

Enabling and disabling Call Home from the NetBackup Appliance Web Console

The following procedures describe how to use the NetBackup Appliance Web Console to enable and disable Call Home on a NetBackup appliance.

Note: The Veritas Access 3340 Appliance does not support configuring AutoSupport 2.0 through a web console. Refer to the following for instructions regarding configuring AutoSupport from the Access Appliance Shell menu.

See [“Enabling and disabling Call Home from the appliance shell menu”](#) on page 18.

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.

Call Home Configuration

The appliance can communicate with the Veritas Call Home server and upload hardware and software information. [Read privacy policy.](#)

Enable Call Home
 Enable Proxy Server
 Enable Proxy Tunneling

Proxy Server:
Proxy Port:
Proxy Username:
Proxy Password:

- 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:

Call Home Configuration

The appliance can communicate with the Veritas Call Home server and upload hardware and software information.

Call Home test successful.

Enable Call Home
 Enable Proxy Server
 Enable Proxy Tunneling

- 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 section is dedicated to provide details for **SNMP**, **SMTP**, and **Call Home** alert notifications.

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 of the page.

Table 4-1 SNMP Server Configuration settings

Fields	Description
Enable SNMP Alert	Select this check box to enable SNMP alert configuration.
SNMP Server	<p>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.</p> <p>Notification of the alerts or traps that are generated in the appliance are sent to this SNMP manager.</p> <p>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.</p>
SNMP Port	<p>Enter the SNMP Server port number. If you do not enter anything for this variable, then the default port is 162.</p> <p>Note: Your firewall must allow access from the appliance to the SNMP server through this port.</p>
SNMP Community	<p>Enter the community to which the alerts or traps are sent. For example, Backup Reporting Department.</p> <p>You can enter a value that you configured on your SNMP server. For example, your company name. If you do not expect to disclose your company name, Veritas provides the system-defined values including: <code>admin_group</code>, <code>public</code>, and <code>private</code>. If you do not enter anything, then the default value is <code>public</code>.</p>

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 view the details of the MIB file from the SNMP Server Configuration pane. To view 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 Appliance Shell Menu 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 documentation of your appliance.

Starting with NetBackup Appliance version 3.1.2 you can configure the SMTP port and set encryption.

You can use the following commands in the Appliance Shell Menu to configure encrypted communication with the SMTP server:

- Main_Menu > Settings > Alerts > Email SMTP ConfigurePort [25] [465] [587] [custom]
- Main_Menu > Settings > Alerts > Email SMTP Encryption [Disable] [Enable]

You can use the following command to view the SMTP port number and encryption configuration details.

```
Main_Menu > Settings > Alerts > Email Show
```

[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
SMTP port	<p>You can select one of the following options:</p> <ul style="list-style-type: none"> ■ Port 25 to use Plain Text ■ Port 465 to use the SMTPS protocol ■ Port 587 to use the STARTTLS protocol ■ Custom port within the range of 1 to 65,535 <p>The default SMTP port number is 25. Encryption is disabled by default.</p>
Encryption	<p>Select Enable Encryption to use a secure connection.</p>
Software Administrator Email	<p>Enter the email ID of the software administrator, to receive software alerts that are specific to the Veritas NetBackup Appliance software. The email ID that you designate receives alerts for the following software conditions:</p> <ul style="list-style-type: none"> ■ Host information such as: <ul style="list-style-type: none"> ■ 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	<p>Enter the email ID of the hardware administrator, to receive hardware alerts that are specific to the Veritas NetBackup Hardware Appliance. For example, enter hardwareadmin@usergroup.com.</p>
Sender Email	<p>Enter the email ID to receive any replies to the alerts or the reports that the appliance sends.</p>
SMTP Account	<p>Enter the user name to access the SMTP account.</p>
Password	<p>Enter the password for the above mentioned SMTP user account.</p>

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 if Call Home functions 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 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.

5 Enter the SMTP settings in the provided fields.

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.

7 Click **Save**, to save the SNMP, SMTP, and Call Home settings.

Configuring client settings on a Flex appliance

This chapter includes the following topics:

- [Viewing Call Home information](#)
- [Configuring Call Home settings](#)
- [Deleting and disabling Call Home settings](#)

Viewing Call Home information

An appliance has the ability to send an email to a local administrator when a hardware failure is detected. You can configure the email address that you want to use for hardware failure notifications from the Flex Appliance Shell. The contents of the email identifies the type of hardware failure that occurred and the status of the failure.

This section provides the information that is specific to the settings and configuration for the Call Home feature.

The available information is provided in the following table.

Table 5-1 Call Home information

Command	Description
<code>callhome</code>	Shows the current Call Home settings
<code>callhome-registration</code> <code>node-name=<node_name></code>	Shows Call Home registration information based on the node hostname

Table 5-1 Call Home information (*continued*)

Command	Description
<code>callhome-test</code>	Sends a test to verify that Call Home is functional
<code>email</code>	Shows the email and the SMTP settings
<code>email-test</code>	Tests SMTP and sends an email about hardware data

To view information about Call Home

- 1 Log in to the Flex Appliance Shell, and type any of the following as needed.

```
show alerts callhome

show alerts callhome-registration node-name=<node_name>

show alerts callhome-test

show alerts email

show alerts email-test
```

- 2 Press **Enter** after each string to display the information.

Configuring Call Home settings

Call Home is enabled by default. This section provides the specific information for the settings and configuration for the Call Home feature.

The available options are provided in the following table.

Table 5-2 Call Home options

Command	Description
<code>callhome</code>	Enable the Call Home feature
<code>callhome-proxy</code>	Enable the Call Home proxy server
<code>callhome-proxy-server</code>	Enter the Call Home proxy server settings
<code>callhome-proxy-tunnel</code>	Enable the Call Home proxy tunneling
<code>email-smtp</code> <code>smtp_account=<smtp_account></code>	(Optional) Enter the name of the account that is used for authentication to the SMTP server

Table 5-2 Call Home options (*continued*)

Command	Description
email-smtp smtp_password=<smtp_password>	(Optional) Enter the password for authentication to the SMTP server
email-smtp smtp_server=<smtp_server>	Enter the SMTP server that is used to send email
email-notification-interval interval=<interval>	Enter the time (in minutes from 1 to 44640) between alert emails that are sent to the administrator. The default value is 1440 minutes.
email-sender-id email_address=<email_address>	Enter an email ID or account for emails that are received from the appliance
email-hardware email_address=<email_address>	Add hardware administrator email accounts

To configure Call Home settings

- 1 Log in to the Flex Appliance Shell, and type the following as needed. Press **Enter** after each string to display the information.
- 2 Enable Call Home.


```
set alerts callhome
```
- 3 Set the Call Home proxy, proxy server, and proxy tunnel.


```
set alerts callhome-proxy
set alerts callhome-proxy-server
set alerts callhome-proxy-tunnel
```
- 4 Set the SMTP server.


```
set alerts email-smtp smtp_server=<smtp_server>
```
- 5 (Optional) Set the SMTP account and password.


```
set alerts email-smtp smtp_account=<smtp_account>
set alerts email-smtp smtp_password=<smtp_password>
```

- 6 Set the interval in minutes between email notifications.

```
set alerts email-notification-interval interval=<interval>
```

- 7 Set the sender and hardware administrator email addresses.

```
set alerts email-sender-id email_address=<email_address>
```

```
set alerts email-hardware email_address=<email_address>
```

Deleting and disabling Call Home settings

Call Home is enabled by default. You can delete or disable Call Home settings as needed. Call Home is not required, but it serves as a critical step to proactive customer support and incident response for failures.

This section provides the information that is specific to the settings and configuration for the Call Home feature.

The available options are provided in the following table.

Table 5-3 Call Home disable and delete options

Command	Description
callhome	Disable the Call Home feature
callhome-proxy	Disable the Call Home proxy server
callhome-proxy-tunnel	Disable Call Home proxy tunneling
email-sender-id	Delete the email ID for emails that are received from the appliance
email-smtp	Delete the SMTP server that is used by the appliance
email-hardware email_address=<email_address>	Delete hardware administrator email accounts

To delete Call Home settings

- 1 Log in to the Flex shell, and type any of the following as needed. Press **Enter** after each string to display the information.
- 2 Disable the Call Home feature.

```
delete alerts callhome
```

3 Disable the Call Home proxy settings.

```
delete alerts callhome-proxy
```

```
delete alerts callhome-proxy-tunnel
```

4 Delete the appliance sender ID and the SMTP settings.

```
delete alerts email-sender-id
```

```
delete alerts email-smtp
```

5 Delete the hardware administrator email address.

```
delete alerts email-hardware email_address=<email-hardware>
```

Using the MyAppliance portal

This chapter includes the following topics:

- [Configuring the MyAppliance portal](#)
- [Registering an appliance](#)
- [Obtaining a copy of your Heartbeat packages](#)
- [Unregistering an appliance](#)

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>. After Call Home is enabled you can use the MyAppliance portal.

You must register your appliance to enter the portal. If you do not have a user account, 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, and inspect heartbeat data.

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

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.

Registration 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 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**.

Benefits of registering your appliance

- Ensure that your appliances remain "up" so that backup operations continue seamlessly
- View capacity and utilization details
- View and update support cases
- Update appliance contact details
- If Call Home is enabled, view the data that is collected

Register your appliance now!

Details you need to register:

- Serial Number
- Hardware Support ID
- Sales Order Number
- Site Details
- Contact Details

Where do I get this information?

Register Appliance

Connected Support Experience

View and Update Support Cases

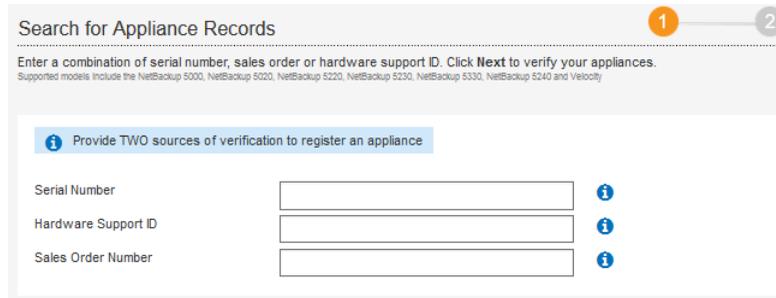
Other Benefits

Knowledgebase / Latest Updates

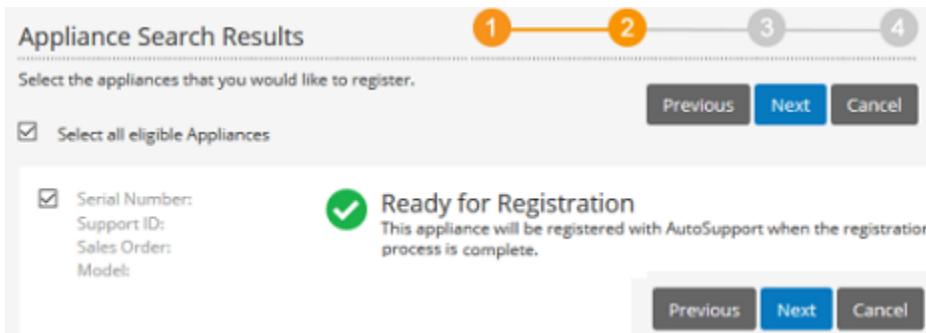
- If you have previously registered appliances on your account, navigate to **Appliances > My Appliances** page and click on **Register Appliance**.



- 2 Input the sources of verification. Only two sources are required to register an appliance.



- 3 Click **Next** to initiate a search.
- 4 Choose the appliance you want to register.



- 5 Click **Next** to enter the **Register a New Appliance** page.

Note: Any field highlighted with an asterisk is compulsory for registration. Move to the next step only after you have entered the required information.

- 6 In the basic information column, input your company name.
- 7 In the **Appliance Location** column, click the **Add New Site** button to create a new site.
- 8 In the pop-up dialog box, input the site name, site address and other information.

- 9 In the **Select Site** field, choose the site you created .
- 10 In the **Contact Information** column, click the **Add New Contact** button to create a new primary contact person.
- 11 In the pop-up dialog box, input contact name, email address, phone number and other information. You can add a total of twenty contacts per appliance.
- 12 In the **Select Contact** field, choose the contact person you created.

Note: The **Receive Call Home transmission failure alert** option is checked by default to enable alerts 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.

If you have spam filtering enabled, configure your filtering settings to allow emails from this sender ID: appliance.veritas.com.

Uncheck the option if you no longer want to receive an alert from Veritas for Call Home transmission failure.

- 13 Verify the information and click **Submit**.

A notification informs you that your appliance is registered successfully.

Upon registration, appliance information including hostname and version are expected to update to the portal. In the event that such appliance information is not displayed, you can try the following actions on NetBackup Appliance or Access Appliance to update it manually.

Note: These steps do not apply to Flex Appliance.

To update appliance information manually on NetBackup Appliance or Access Appliance

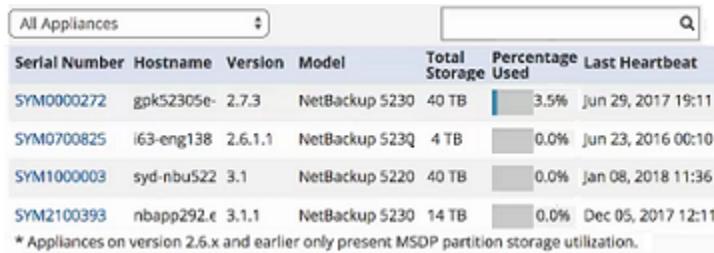
- 1 Verify that your appliance has access to Veritas servers either directly or through a proxy.
- 2 Verify that Call Home is enabled by using command `Settings > Alerts > CallHome Test` in the Appliance Shell Menu.
- 3 Update the appliance information manually using command `Support > Collect Inventory` in the Appliance Shell Menu.

Obtaining a copy of your Heartbeat packages

A heartbeat is a signal that is generated at regular intervals to indicate that systems are working correctly.

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.



Serial Number	Hostname	Version	Model	Total Storage	Percentage Used	Last Heartbeat
SYM0000272	gpk52305e-	2.7.3	NetBackup 5230	40 TB	3.5%	Jun 29, 2017 19:11
SYM0700825	i63-eng138	2.6.1.1	NetBackup 523Q	4 TB	0.0%	Jun 23, 2016 00:10
SYM1000003	syd-nbu522	3.1	NetBackup 5220	40 TB	0.0%	Jan 08, 2018 11:36
SYM2100393	nbapp292.e	3.1.1	NetBackup 5230	14 TB	0.0%	Dec 05, 2017 12:11

* Appliances on version 2.6.x and earlier only present MSDP partition storage utilization.

- 2 Click on the serial number to manage your appliance.
- 3 Click on the **CallHome Data** tab to view your heartbeat data. The **Last Refresh** field shows the timestamp for the last heartbeat data transmission.

You can also click **Save as CSV** to export a copy of the data as a comma-separated value list.

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**.

NetBackup Product Improvement Program

This chapter includes the following topics:

- [About the NetBackup Product Improvement Program](#)
- [How Veritas uses NetBackup Product Improvement Program data](#)
- [How NetBackup Product Improvement Program data is transmitted](#)
- [Data privacy](#)
- [Enabling or disabling the NetBackup Product Improvement Program](#)
- [NetBackup Product Improvement Program proxy configurations](#)

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 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 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 the [Veritas 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 packages”](#) on page 35.

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/opensv/netbackup/bin/bpsetconfig -set TELEMETRY_UPLOAD=NO
```

The attribute is stored in `/usr/opensv/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/opensv/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 URL.

<https://api.appliance.veritas.com>

Frequently Asked Questions

This appendix includes the following topics:

- [Frequently asked questions](#)

Frequently asked questions

Which Veritas appliances support Veritas AutoSupport

AutoSupport functionality is currently implemented in the appliance(s) listed at the following link.

See [the section called “AutoSupport supported platforms”](#) on page 6.

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 service?

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

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

Yes, server certificates are issued by a trusted authority.

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

No. Veritas appliance does not support any local certificate authority.

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 assurance that a file cannot be copied from 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?

Yes. Call Home is an outbound-only connection.