Veritas™ Appliance AutoSupport Reference Guide

VERITAS™

Veritas™ Appliance AutoSupport Reference Guide

Last updated: 2023-03-06

Legal Notice

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

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 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 5240 Appliance

- NetBackup 5250 Appliance
- NetBackup 5330 Appliance
- NetBackup 5340 Appliance
- NetBackup 5350 Appliance
- Veritas 5150 Appliance
- Veritas 5250 Appliance
- Veritas 5340 Appliance
- Veritas 5350 Appliance
- Access 3340 Appliance
- Access 3350 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	When a failure occurs, the following sequence of alerts occur:
	■ The appliance uploads all the monitored hardware and software information to a Veritas server.
	■ The appliance generates the following three 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.
	■ 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.
	■ The appliance also generates an SNMP trap.

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:

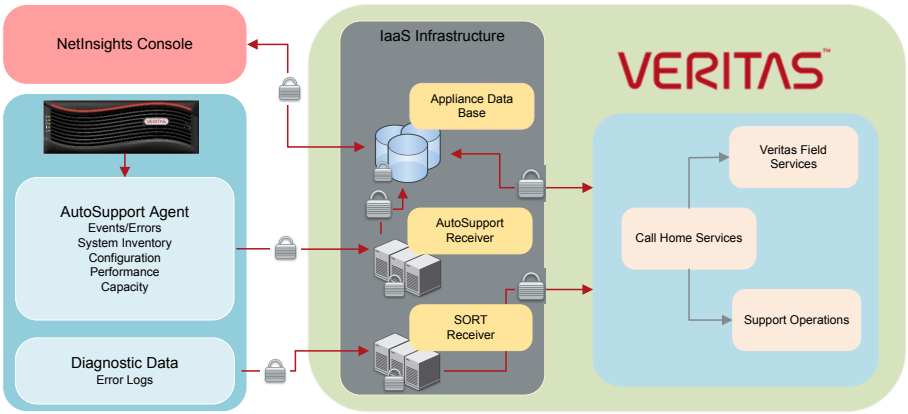
Introduction to AutoSupport architecture

With Appliance Release 2.7.1, a new architecture for both client and server is implemented in 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 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) team is located in Pune, India 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.

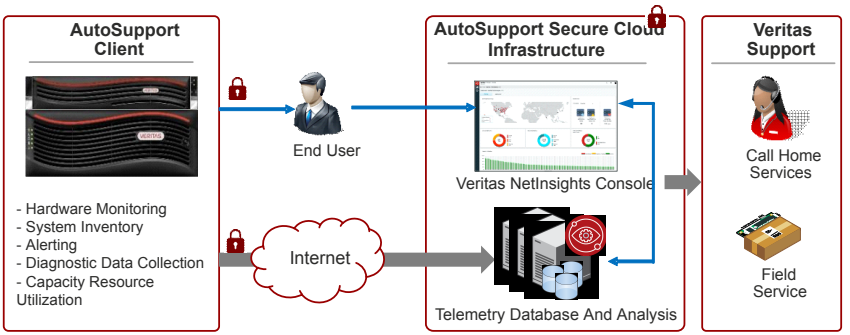
When an appliance transmits event data to Veritas, it is sent to the Veritas Appliance Monitoring infrastructure servers. The appliance also transmits a `DataCollect` package to the API endpoint, and an incident ticket is opened to track the status. A CHS engineer triages the incident and determines 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 NetInsights Console

The Veritas NetInsights Console is SaaS-based platform that allows users to manage Veritas usage and license entitlements. NetInsights uses product diagnostic and support data to offer insights about the operational health of Veritas systems in a single interface.

The NetInsights Console uses the AutoSupport architecture and requires Call Home to be configured and enabled on your appliance. For more information about NetInsights, see the *Veritas Usage Insights for NetBackup Getting Started Guide*.

Figure 2-2 AutoSupport architecture and NetInsights Console



About System Health Insights portal

Veritas System Health Insights, a part of Veritas NetInsights Console, enables you to monitor the health and operational state of your appliances and receive targeted recommendations to maintain maximum reliability and uptime. It uses artificial intelligence and machine learning to analyze the Call Home data and suggest improvements. You can register your appliances and access the System Health Insights portal at https://netinsights.veritas.com.

To access the System Health Insights portal perform the following steps:

1. Open https://netinsights.veritas.com/ in a browser.
2. Sign in using your Veritas Account Manager credentials.
3. Click **System Health Insights**.

All appliances must be registered to the System Health Insights portal. For more information, see the *Veritas System Health Insights User Guide*.

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 (primary 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 */log/data-collect/sosreport-<serial number>-<creation timestamp>-*-*.tar.xz*.
  For example:
  /log/data-collect/sosreport-VTAS9002275-20220117225904-periodic-ihirgyq.tar.xz
- 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

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:

- 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

Enabling Call Home provides a one-way communication that only transmits data and does not allow the appliance to receive any incoming data or notifications. All data that is transmitted to Veritas from an appliance is done with TLS-encrypted transmission by HTTPS PUT over port 443/tcp.

Data transmissions for the following services are sent to https://api.appliance.veritas.com.

- Appliance Call Home Provisioning
- Data Collect packages
- Virtual Appliance Serialization data

Note: If you configure a proxy server on the appliance, the proxy must allow connections to the above URLs to ensure that the AutoSupport feature can transmit data to Veritas.

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 the 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 that you enable the proxy and/or the firewall to outbound 443/TCP TLS socket connections to the following site: https://api.appliance.veritas.com.

For more information about the Call Home data transmission infrastructure, see the following technical article:

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/.

Chapter 4

Configuring client settings on NetBackup and Access appliances

This chapter includes the following topics:

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. The MyAppliance portal is no longer supported with the release of the Veritas NetInsights Console and will be decommissioned. Appliance registration should be done by signing in to the NetInsights portal (https://netInsights.veritas.com) with your Veritas Account Manager credentials. For more information, see the *Veritas Appliance AutoSupport Reference Guide* and the *Veritas NetInsights Console User Guide*.

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 31.

See "Deleting and disabling Call Home settings" on page 34.

Enabling and disabling Call Home from the NetBackup Appliance Web Console

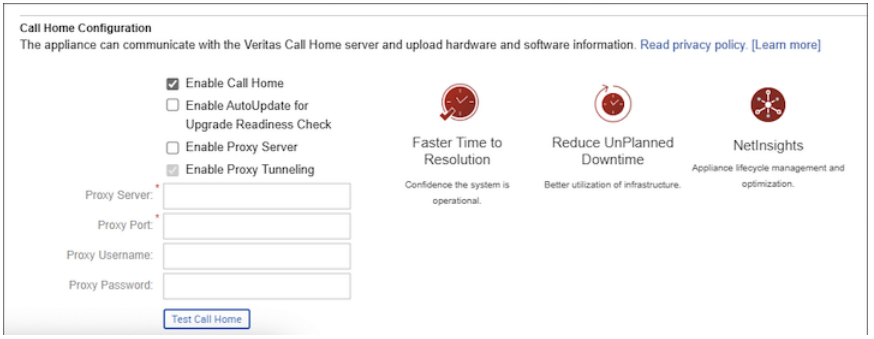
The following procedures describe how to use the NetBackup Appliance Web Console to enable and disable Call Home on a NetBackup appliance.

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.

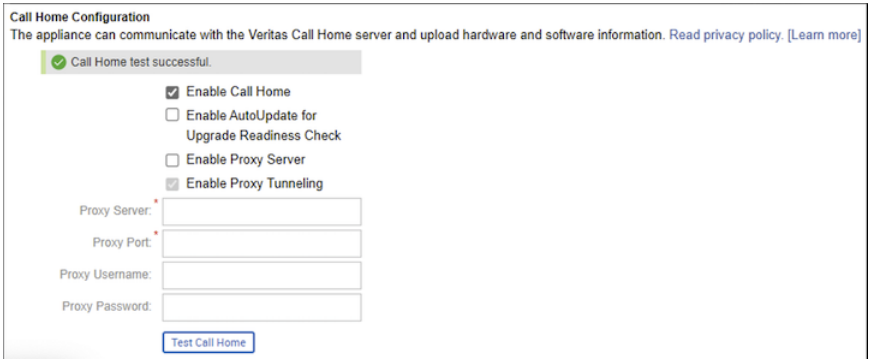
See "Enabling and disabling Call Home from the appliance shell menu" on page 19.

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**.

Note: If you click **Save** and the **Enable AutoUpdate for Upgrade Readiness Check** option is not checked, an alert message appears. Click **Yes** to enable the option and save the settings. Click **No** to leave the option disabled and save the settings without disabling the automatic update for the upgrade readiness check collector.

Settings > Notifications > Alert Configuration

The **Settings > Notifications > Alert Configuration** page on the NetBackup Appliance Web Console 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 NetBackup Appliance Web Console.

Table 4-1 SNMP Server Configuration settings

Fields	Description
Notification Interval	Enter the interval for the server to upload alerts to the Veritas Call Home server. Entries must be in increments of 15 minutes.
SNMP Server Configuration	Select one of the following options: ■ **SNMP V2** ■ **SNMP V3** ■ **None** (default)
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 the 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. The default port is 162. **Note:** Your firewall must allow access from the appliance to the SNMP server through this port.

Table 4-1 SNMP Server Configuration settings *(continued)*

Fields	Description
SNMP Community	This field is required for SNMP V2 and is optional for SNMP V3. 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, your company name. If you do not expect to disclose your company name, Veritas provides the system-defined values including: `admin_group`, `public`, and `private`. The default is `public`.
SNMP Username (SNMP V3 only)	Enter an SNMP user name as follows: ■ Enter up to 32 characters maximum. ■ May include uppercase letters, lowercase letters, numbers, and the following punctuation marks: period, hyphen/dash, underscore. ■ Spaces, commas, and special characters are not allowed.
Authentication Protocol (SNMP V3 only)	Configure as follows to set the security level: ■ **None** (default) Sets the security level to no authentication and no privileges (authentication is disabled). Password and encryption fields are greyed out and not required. ■ **SHA256** or **SHA512** Sets the security level for authentication. An SNMP password is required.
SNMP Password/**Confirm SNMP Password** (SNMP V3 only)	Enter a password for the SNMP user as follows: ■ Must have 8 or more characters. ■ May include uppercase letters, lowercase letters, numbers, and the following punctuation marks: period, hyphen/dash, underscore. ■ Spaces, commas, and special characters are not allowed. Enter the same password in the **Confirm SNMP Password** field.

Table 4-1 SNMP Server Configuration settings *(continued)*

Fields	Description
Encryption Protocol (SNMP V3 only)	Configure as follows to set the encryption policy: ■ **None** (default) Encryption policy is not used or enforced. Passphrase fields are greyed out and not required. ■ **AES128 AES192 AES256 AES512** Select one of these options to enforce the associated encryption policy. An **Encryption Passphrase** is required.
Encryption Passphrase/**Confirm Encryption Passphrase** (SNMP V3 only)	If you set the **Encryption Protocol** to use an encryption policy, enter a passphrase for the SNMP user as follows: ■ Must have 8 or more characters. ■ May include uppercase letters, lowercase letters, numbers, and the following punctuation marks: period, hyphen/dash, underscore. ■ Spaces, commas, and special characters are not allowed. Enter the same passphrase in the **Confirm Encryption Passphrase** field.

The following describes summaries of the required fields for specific SNMP configuration scenarios:

- **SNMP V2**
  SNMP Server
  SNMP Port
  SNMP Community
  All other fields are not required.
- **SNMP V3** - no authentication/no privileges
  SNMP Server
  SNMP Port
  SNMP Community (optional)
  Authentication Protocol - None
  All other fields are not required.
- **SNMP V3** - authentication/no privileges
  SNMP Server
  SNMP Port
  SNMP Community (optional)
  Authentication Protocol (SHA256, SHA512)
  SNMP Password/Confirm SNMP Password

All other fields are not required.

- **SNMP v3** - authentication/privileges
  SNMP Server
  SNMP Port
  SNMP Community (optional)
  Authentication Protocol (SHA256, SHA512)
  SNMP Password/Confirm SNMP Password
  Encryption Protocol (AES128, AES192, AES256, AES512)
  Encryption Passphrase/Confirm Encryption Passphrase

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.

You can also use the following command in the appliance shell menu to configure the SNMP server:

```
Main_Menu > Settings > Alerts > SNMP Set Server [Community] [Port]
```

For example: `Main_Menu > Settings > Alerts > SNMP Set Server 10.80.97.223`

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

https://www.veritas.com/content/support/en_US/article.100009877

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 release 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.
SMTP port	You can select one of the following options: ■ 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 The default SMTP port number is 25. Encryption is disabled by default.
Encryption	Select **Enable Encryption** to use a secure connection.

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. The 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 Appliance hardware. For example, enter hardwareadmin@usergroup.com.
Email Test	A test email is sent to the email address that was configured above. If the test email is not received, follow the error prompts to view the network connections, SMTP settings, and email settings. You can contact your system administrator for more assistance.
Sender Email	Enter the email ID to receive any replies to the alerts or the reports that the appliance sends.
SMTP Account	Enter the user name to access the SMTP account.
Password	Enter the password for the above mentioned SMTP user account.

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.

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.

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 AutoUpdate for Upgrade Readiness Check	Select this check box to enable automatic updates for the Appliance Upgrade Readiness Analyzer tool (analyzer tool) on the appliance. Enabling this feature lets you keep pre-upgrade checks up to date and receive accurate upgrade readiness status recommendations through System Health Insights on the NetInsights Console. You can download the latest version of the analyzer tool from the Veritas Download Center. Veritas recommends that you enable AutoUpdate.
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.

Starting with the 5.0 release, when you enable Call Home and click **Save**, a Call Home test is performed automatically.

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 15-minute increments 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.

Chapter 5

Configuring client settings on a Flex appliance

This chapter includes the following topics:

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
`callhome`	Shows the current Call Home settings
`callhome-registration node-name=<node_name>`	Shows Call Home registration information based on the node hostname

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

Command	Description
`callhome-test`	Sends a test to verify that Call Home is functional
`diskspace-threshold`	Shows the threshold for high disk usage alerts
`email`	Shows the email and the SMTP settings
`email-test`	Tests SMTP and sends an email about hardware data

To view information about Call Home

1 Log in to the , 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 diskspace-threshold

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
`callhome`	Enable the Call Home feature
`callhome-proxy`	Enable the Call Home proxy server
`callhome-proxy-server`	Enter the Call Home proxy server settings
`callhome-proxy-tunnel`	Enable the Call Home proxy tunneling

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

Command	Description
`diskspace-threshold`	Set the threshold for high disk usage alerts
`email-smtp smtp_account=<smtp_account>`	(Optional) Enter the name of the account that is used for authentication to the SMTP server
`email-smtp 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-software email_address=<email_address>`	Add software administrator email accounts
`email-hardware email_address=<email_address>`	Add hardware administrator email accounts

To configure Call Home settings

1. Log in to the , 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> smtp_password
```

You can also enter each separately, as follows:

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

```
set alerts email-smtp smtp_password
```

6 Set the interval in minutes between email notifications.

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

7 (Optional) Set the threshold for high disk usage alerts. The default threshold is 80%.

```
set alerts diskspace-threshold threshold=<value>
```

Where *<value>* is an integer between 1 and 93. If you enter 0, all disk usage alerts are disabled.

Note: Critical disk usage alerts are sent when disk usage exceeds 94%. This threshold cannot be changed.

---

8 Set the sender and the administrator email addresses.

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

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

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

You can enter multiple administrator email addresses using a comma-separated list or by running the command once for each email address.

Note: If you encounter the following message, the email address was added to the appliance successfully, but the test email did not go through:

```
[Error] The appliance was able to connect to your SMTP server,
but either we were not able to authenticate properly, or your
SMTP server is preventing us from sending emails through it.
Please check your SMTP server for details.
```

Verify the email address, sender ID, and SMTP password that you entered. If they are all correct, check the settings on your SMTP server.

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
`diskspace-threshold`	Disable high disk usage alerts
`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. Disable high disk usage alerts.

   ```
   set alerts diskspace-threshold threshold=0
   ```

5 Delete the appliance sender ID and the SMTP settings.

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

```
delete alerts email-smtp
```

6 Delete the hardware administrator email address.

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

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 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`

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 as follows:

- 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 ability of the appliance to report error conditions to Veritas, and can also delay the response time to repair failures.

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.

Appendix A

Frequently Asked Questions

This appendix includes the following topics:

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.