

G06.31 Release Version Update Compendium

Abstract

This compendium provides a summary for the products that have major changes in the G06.31 release version update (RVU), including the products' new features, migration issues, and fallback considerations. The compendium is written for system managers or anyone who needs to understand how migrating to G06.31 affects installation, configuration, operations, system management, maintenance, applications, networks, and databases.

Product Version

N.A.

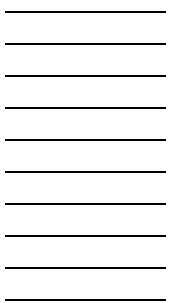
Supported Release Version Updates (RVUs)

This publication supports the G06.31 RVU only.

Part Number	Published
544625-001	July 2007

Document History

Part Number	Product Version	Published
544625-001	N.A.	July 2007



G06.31 Release Version Update Compendium

Tables

- [What's New in This Manual](#) iii
- [Manual Information](#) iii
- [New and Changed Information](#) iii
- [About This Manual](#) v
- [Who Should Use This Guide?](#) v
- [Organization](#) v
- [Related RVU Manuals](#) v

1. G06.31 Overview

- [Major New Features](#) 1-1
- [Products Removed From the Site Update Tape \(SUT\)](#) 1-2

2. Operating System

- [New Parameter for osh Command in OSS](#) 2-1

3. Application Development Products

- [Visual Inspect Server Enhancements](#) 3-1
- [Migration](#) 3-2
- [Fallback](#) 3-2

4. Database and Transaction Processing Products

5. Installation and Configuration Products

6. Manageability Products

- [Safeguard Password Enhancements](#) 6-1
- [Maximum Password Length Increased](#) 6-1
- [Password Quality Enhancements](#) 6-3
- [Migration](#) 6-3
- [Fallback](#) 6-4

7. Hardware Products

- [Generation 3 SCSI Tape Drives](#) 7-1

8. Networking Products

A. Sources for Migration Assistance and Information

[ExpressNotice](#) A-1

[Information on the Site Update Tape \(SUT\)](#) A-2

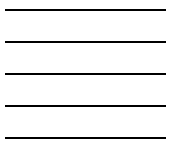
[Scout for NonStop Servers](#) A-2

[Global Mission Critical Solution Center \(GM CSC\)](#) A-2

[NonStop Technical Library \(NTL\)](#) A-3

Tables

[Table 1-1.](#) [Summary of the G06.31 RVU](#) 1-1



What's New in This Manual

Manual Information

Abstract

This compendium provides a summary for the products that have major changes in the G06.31 release version update (RVU), including the products' new features, migration issues, and fallback considerations. The compendium is written for system managers or anyone who needs to understand how migrating to G06.31 affects installation, configuration, operations, system management, maintenance, applications, networks, and databases.

Product Version

N.A.

Supported Release Version Updates (RVUs)

This publication supports the G06.31 RVU only.

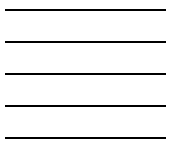
Part Number	Published
544625-001	July 2007

Document History

Part Number	Product Version	Published
544625-001	N.A.	July 2007

New and Changed Information

This is a new manual.



About This Manual

This compendium provides categorized information for new features, migration issues, and fallback considerations for G06.31. It also includes references and sources for migration planning.

Who Should Use This Guide?

This compendium is written for system managers or anyone who needs to understand how migrating to G06.31 affects installation, configuration, operations, system management, maintenance, applications, networks, and databases.

Organization

Section	Description
Section 1, G06.31 Overview	An overview listing the products that have major changes
Section 2, Operating System Section 3, Application Development Products Section 4, Database and Transaction Processing Products Section 5, Installation and Configuration Products Section 6, Manageability Products Section 7, Hardware Products Section 8, Networking Products	Categorized product information that summarizes: <ul style="list-style-type: none">● New features● Migration issues (if available)● Fallback considerations (if available)
Appendix A, Sources for Migration Assistance and Information	References and sources for migration planning

Related RVU Manuals

For a list of RVU and migration manuals, see [NonStop Technical Library \(NTL\)](#) on page A-3.

1 G06.31 Overview

This section lists the major new features for the G06.31 RVU.

Major New Features

For descriptions of new features, see the appropriate sections in [Table 1-1](#).

Table 1-1. Summary of the G06.31 RVU

Sections and Categories	Major New Features	Migration Alerts	Fallback Alerts
Section 2, Operating System	<ul style="list-style-type: none">New Parameter for osh Command in OSS		
Section 3, Application Development Products	<ul style="list-style-type: none">Visual Inspect Server Enhancements	X	X
Section 4, Database and Transaction Processing Products	<ul style="list-style-type: none">No new features in the G06.31 RVU		
Section 5, Installation and Configuration Products	<ul style="list-style-type: none">No new features in the G06.31 RVU		
Section 6, Manageability Products	<ul style="list-style-type: none">Safeguard Password Enhancements	X	X
Section 7, Hardware Products	<ul style="list-style-type: none">Generation 3 SCSI Tape Drives		
Section 8, Networking Products	<ul style="list-style-type: none">No new features in the G06.31 RVU		

Products Removed From the Site Update Tape (SUT)

No products were removed from the Site Update Tape (SUT) in the G06.31 RVU.

For recent product removal information, see the Discontinuation Notices at
<http://h20223.www2.hp.com/NonStopComputing/cache/77208-0-0-225-121.aspx>.

2 Operating System

New Parameter for osh Command in OSS

The `-phd` option is added to the `osh` command.

The `-phd` option specifies that the child process uses the the initial logon directory of the current effective Process Access ID (PAID) of the parent process as configured on the HP node that runs the child process. If the `-phd` option is not specified to `osh`, the child process uses the initial logon directory of the parent process as configured on the HP node that runs the child process.

The `-phd` option can affect the value of OSS environment variable HOME or PWD for a child process when the Guardian HOME PARAM or Guardian PWD PARAM variable is not defined.

See "Process Environment" in the `osh(1)` reference page for more detailed information.

Application Development Products

Visual Inspect Server Enhancements

Visual Inspect supports these new features for the G06.31 RVU:

- iCode support. This feature enables you to view instructions interleaved with source code in source views.
- Maximum C String Length and Format C String Length are now supported as a preference and a command, respectively.
- You can more easily configure Visual Inspect in a firewall situation by specifying a range of TCP port numbers for the client and the server.
- New features for viewing instructions:
 - You can use the new **View>Instructions** command to toggle the display of machine instructions interleaved with source code on Program Control and Scope Source views.
 - The new instruction movement indicator in the source pane indicates instructions that the compiler moved during optimization.
 - You can use the new **View>Instruction Annotations** command to toggle the display of instruction annotations for the current scope in the Program Control and Scope Source views.
- Load levels are now assigned to all loadfiles associated with the current program. The three load levels (Symbols, Scope Names Only, and No Symbols) determine whether a loadfile is fully loaded for debugging.
- Privileged debugging enhancements. The super ID can explicitly enable privileged access using two new options:
 - **Allow Hold in Priv Code** on the Open Program dialog
 - **Enable access to privileged code and data** on the Program Properties: Options tab
- New toolbar buttons are added for the **Step Instruction** and **Step In Instruction** commands.
- Breakpoint persistence is enhanced: Visual Inspect now preserves how a breakpoint was originally set. When a breakpoint is restored from persistence data, the same method used originally to set the breakpoint will be used.
- Multibyte characters are now supported in breakpoint condition text. This makes it possible to specify certain non-English characters such as Japanese or Chinese.

- You can switch to the system debugger by using the new command **Program>Switch to System Debugger** on the Program Control and Application Control views.
- Support for register watch items:
 - You can monitor registers by selecting **Create watch item** from the context menu in the Program Properties and Stack Frame Properties dialogs when at the top of a stack.
 - For a Register Watch Item, you can modify register values and view registers in different style formats.
- You can now display SPI and EMS buffers.
- Conditional data breakpoints are now supported by the Add Data Breakpoint dialog.
- Scope Browser is enhanced to include:
 - COBOL paragraphs and sections
 - TAL subprocedures and labels
 - pTAL labels
 - C/C++ labels
- You can now use Visual Inspect to read TNS/E snapshot files on a TNS/R system.
- Performance is improved for:
 - Conditional data breakpoints
 - Array operations
 - Expanding a large struct

Migration

Upgrading Visual Inspect client is optional. However, to get the full benefit of the features and performance of the G06.31 Visual Inspect server and client, you must upgrade to Visual Inspect client version 3.3

Fallback

Problems can occur when reverting to a previous version of the Visual Inspect client after upgrading to the new client along with the new server. In some cases, new persistent information is not handled properly by older versions of the client. If this is a concern, you should save a copy of the original VISINSP.INI file, located in the c:\Windows directory. You can use this copy to ensure a smooth fallback, if fallback becomes necessary.

4

Database and Transaction Processing Products

The G06.31 RVU contains no new features for the database and transaction processing products.

5

Installation and Configuration Products

The G06.31 RVU contains no new features for the installation and configuration products.

6

Manageability Products

Safeguard Password Enhancements

Safeguard supports these new features in the G06.31 RVU:

- Maximum password length is increased
- Passwords can contain embedded spaces
- Password quality enhancements

Maximum Password Length Increased

The maximum password length is increased from 8 characters to 64 characters. These new attributes are introduced to facilitate the longer password feature:

Attribute Name	Default Value
PASSWORD-COMPATIBILITY-MODE	ON
PASSWORD-MAXIMUM-LENGTH	8

This existing attribute is modified:

Attribute Name	Previous Maximum Value	New Maximum Value
PASSWORD-MINIMUM-LENGTH	8	64

PASSWORD-COMPATIBILITY-MODE

The new password configuration attribute PASSWORD-COMPATIBILITY-MODE is used to determine whether a given user or alias is allowed to set passwords longer than eight characters. This attribute is set to ON by default. When you migrate to the G06.31 RVU, the longer password feature is not automatically enabled, and therefore the user or alias is not able to set passwords longer than eight characters. This attribute must be set to OFF to enable the longer password feature. This attribute takes effect only during password change and does not impact authentication. When the user or alias has set the password to more than eight characters, the user or alias is authenticated against the longer password regardless of the PASSWORD-COMPATIBILITY-MODE setting.

When the user or alias supplies more than eight characters for the new password string and PASSWORD-COMPATIBILITY-MODE is ON during password change, only the first eight characters of the supplied password are effective and the rest of the password input string is discarded. A warning message is displayed stating that only the first eight characters of the supplied password are accepted. Authentication requests sent after this change consider only this eight character password.

When PASSWORD-COMPATIBILITY-MODE is OFF during password change, the full password string (up to 64 characters) is effective and is considered for subsequent user authentication.

PASSWORD-MAXIMUM-LENGTH

The other new password configuration attribute, PASSWORD-MAXIMUM-LENGTH, specifies the maximum length allowed for the passwords being set or changed. This attribute can be modified only when the PASSWORD-ENCRYPT attribute is set to ON and the PASSWORD-ALGORITHM attribute is set to HMAC256. When PASSWORD-ENCRYPT is set to ON and PASSWORD-ALGORITHM is set to HMAC256, accepted values of PASSWORD-MAXIMUM-LENGTH are between 8 and 64 inclusive. The default value is 8.

There are special considerations. PASSWORD-MAXIMUM-LENGTH is reset to 8 when PASSWORD-MAXIMUM-LENGTH is greater than 8 and one of these situations is true:

- PASSWORD-ENCRYPT is changed from ON to OFF.
- PASSWORD-ALGORITHM is changed from HMAC256 to DES.

PASSWORD-MINIMUM-LENGTH

The maximum value of PASSWORD-MINIMUM-LENGTH is increased from eight to 64 characters.

When either PASSWORD-ENCRYPT is set to OFF or PASSWORD-ENCRYPT is set to ON and PASSWORD-ALGORITHM is set to DES, PASSWORD-MINIMUM-LENGTH must have a value between 0 and 8 inclusive. When PASSWORD-ENCRYPT is set to ON and PASSWORD-ALGORITHM is set to HMAC256, then PASSWORD-MINIMUM-LENGTH can have a value between 0 and 64 inclusive, or between 0 and PASSWORD-MAXIMUM-LENGTH inclusive, whichever is smaller.

There are special considerations. PASSWORD-MINIMUM-LENGTH is reset to 6 when PASSWORD-MINIMUM-LENGTH is greater than 8 and one of these situations is true:

- PASSWORD-ENCRYPT is changed from ON to OFF.
- PASSWORD-ALGORITHM is changed from HMAC256 to DES.

Enabling the Longer Password Feature

By default, the longer password feature is disabled. After migrating to the G06.31 RVU, the following Safeguard configuration attributes must be changed using SAFECOM (if Safeguard is running) or PWCONFIG (if Safeguard is not running):

1. Change PASSWORD-COMPATIBILITY-MODE to OFF.
2. Change PASSWORD-MAXIMUM-LENGTH to a value greater than 8 characters.

Password Quality Enhancements

The versions of Standard Security and Safeguard released with the G06.31 RVU provide these password enhancements:

- Support for new password quality attributes
- Support for embedded spaces in user or alias passwords

The following new password quality attributes are introduced:

Attribute	Description
PASSWORD-UPPERCASE-REQUIRED	When set to ON, passwords must contain at least one uppercase character.
PASSWORD-LOWERCASE-REQUIRED	When set to ON, passwords must contain at least one lowercase character.
PASSWORD-NUMERIC-REQUIRED	When set to ON, passwords must contain at least one numeric character.
PASSWORD-SPECIALCHAR-REQUIRED	When set to ON, passwords must contain at least one special character (any nonalphanumeric character except for commas, double quotes, or semicolons).

In addition, the following attributes are introduced:

Attribute	Description
PASSWORD-MIN-QUALITY-REQUIRED	Specifies the minimum number of quality criteria that must be met when a password is set or changed. Valid values are 0 through 4.
PASSWORD-SPACES-ALLOWED	When set to ON, passwords may optionally contain embedded spaces.

The password quality attributes are disabled by default; they must be explicitly enabled through Safeguard (if Safeguard is running) or by using the PWCONFIG command. The password quality attributes can be modified only if the PASSWORD-ENCRYPT attribute is set to ON and the PASSWORD-ALGORITHM attribute is set to HMAC256. In addition, for PASSWORD-SPACES-ALLOWED to be altered, PASSWORD-COMPATIBILITY-MODE must be set to OFF.

Migration

There are no special considerations for migrating to the G06.31 RVU. However, a mitigation procedure is available for handling any unexpected failures that might occur during migration. This procedure preserves the user or password database that is necessary to restore the original system user or alias database.

Once the new version is installed, use the new PWCONFIG utility to modify the appropriate attributes if you do not want to accept the new default values.

The mitigation procedure is:

1. Use VPROC to determine the current versions of:
 - OSMP
 - OSMON
 - SAFEART
 - SAFECOM
2. Back up current Safeguard files (\$*.SAFE.*, \$SYSTEM.SYSTEM.USERID, and \$SYSTEM.SYSTEM.USERAX).
3. Use SAFECOM to build an Obey file to save the current policy:

```
TACL> safecom/out $system.safe.safevalu/
=display as commands on
=info safeguard, detail
```

The output from these commands is retained in the SAFEVALU file located at \$SYSTEM.SAFE.

Once the new version of Safeguard is installed and you want to retain your original Safeguard values, run the SAFEVALU Obey file created in Step 3 in SAFECOM to restore the original Safeguard values.

You can restore the files backed up in the previous steps if any unexpected failures occur during migration.

If you do not follow these steps and you wish to restore the original default values, then, once the new version of Safeguard is installed, use SAFECOM to modify the appropriate attributes.

For more details, see Section 10 of the *Safeguard Administrator's Manual*.

Fallback

Longer passwords and embedded spaces in passwords are not supported in pre-G06.31 RVUs. Any user with a password that exceeds 8 characters or contains embedded spaces will be unable to login after fallback.

From the G06.31 RVU, you can fall back to the G06.29 or G06.30 RVU.

Considerations for falling back to a previous RVU in a Safeguard or Standard Security environment are:

- The super ID password must not exceed 8 characters and must not contain embedded blanks. If these conditions are not met, The super ID password must be changed accordingly; otherwise, the super ID will be unable to logon after falling back.
- If the PASSWORD-MINIMUM-LENGTH attribute value exceeds 8, the system administrator must change it to a value less than 8 using SAFECOM in a Safeguard environment or PWCONFIG in a Standard Security environment.

- Users whose password exceeds 8 characters in length or contains embedded spaces must request the system administrator to change their password to a length less than or equal to 8 characters and to remove embedded spaces before fallback.

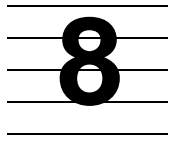
Users whose password does not exceed 8 characters in length and does not contain embedded spaces will be able to successfully logon after fallback.

7 Hardware Products

Generation 3 SCSI Tape Drives

The HP N1528A and N1529A ACL LTO generation 3 tape drives replace the N1526A and N1527A ACL LTO generation 2 tape drives, respectively. These auto cartridge loader (ACL) SCSI tape drives are available in rackmount (N1528A) or tabletop (N1529A) configurations. For more information, see the *N1528A and N1529A ACL Tape Drive Installation and User's Guide*.

The HP N1523A LTO generation 3 SCSI add-on tape drive for the Midrange Tape Library replaces the N1522A LTO generation 2 tape drive. For more information, see the *SL500 (M852x) Tape Library Installation and User's Guide* and the *Mid-Range Silo Media Manager Installation and User's Guide*.



Networking Products

The G06.31 RVU contains no new features for the networking products.

A

Sources for Migration Assistance and Information

This appendix describes the assistance HP provides when problems arise during the migration and testing process. HP also provides services that can help you develop a migration plan and implement migration tasks. Most migration and release documentation is available through the HP NonStop Technical Library (NTL).

This appendix includes information about these sources for migration assistance and information:

- [ExpressNotice](#)
- [Information on the Site Update Tape \(SUT\)](#)
- [Scout for NonStop Servers](#)
- [Global Mission Critical Solution Center \(GMCSC\)](#)
- [NonStop Technical Library \(NTL\)](#)

ExpressNotice

ExpressNotice is an automated information delivery system that proactively sends information pertinent to your installed products and software release whenever there are any issues or changes. (ExpressNotice generates notices only for supported RVUs.) Use ExpressNotice to customize your information notification needs interactively online. You can access ExpressNotice through the HP NonStop eServices Portal at <https://onepoint.nonstop.compaq.com/buildpage.asp>.

ExpressNotice message types include:

- Software Revision Notifications summarize the content and impact of newly released, generally available time-critical fix software product revisions (SPRs).
- Hotstuff messages alert you to product problems that might have particularly serious consequences. The three types of Hotstuff messages are general, Outage Prevention Notifications (OPNs), and Software Recall/Withdrawal.
- Support Notes (SUPNOTES) provide information of a more routine nature than that provided in Hotstuff messages.

ExpressNotice messages are also available through Scout for NonStop Servers (see page [A-2](#)).

You can ask the Global Mission Critical Solution Center (GMCSC) for the *ExpressNotice User's Guide*. You can also contact the ExpressNotice Help Desk by e-mail at express.notice@hp.com.

Information on the Site Update Tape (SUT)

These documents are available on the Y9230G_{nn} release subvolume located on the SUT for each G-series RVU:

- Content file
Contains a list of the product versions and software product revisions (SPRs) that are included on the site update tape (SUT).
- README
This file contains information that was not yet available when the manuals or softdocs were published.

You can access all other RVU information through NTL.

Scout for NonStop Servers

Scout for NonStop Servers is a Web-based SPR analysis and delivery tool available through Electronic Support Services. You can access Scout through the HP NonStop eServices Portal at <https://onepoint.nonstop.compaq.com/buildpage.asp>. Online help for using Scout is available at the Scout Web site.

By providing access to a data warehouse with SPR information for many different RVUs, Scout makes SPR analysis fast, easy, and accurate. Through the Scout main menu, you can display detailed information about:

- Release version updates (RVUs)
- Product versions (PVs) and software product revisions (SPRs)
- Outage Prevention Notifications, Hotstuff messages, and Support Notes
- Prerequisites for an SPR
- Available SUTs and Independent Products

After researching available SPRs, you can download those you consider appropriate for your systems directly to your workstation, or you can request tape delivery.

Global Mission Critical Solution Center (GMCSC)

If you have questions or problems while implementing your migration plan or testing a new system, contact the Global Mission Critical Solution Center (GMCSC) at 1-800-255-5010.

You can also access information on products and services at <http://support.nonstop.compaq.com/>.

NonStop Technical Library (NTL)

In addition to this compendium, RVU and migration information is available in several other documents and manuals that you can access through NTL. Information is provided about planning your site for a new NonStop server, product installation and configuration, product availability in a particular RVU, and performance information for a specific RVU.

- *G06.31 Software Installation and Upgrade Guide*

Provides procedures for upgrading to the G06.31 RVU. Instructions include installing the G06.31 SUT and other related installation tasks.

- *NonStop S-Series Hardware Installation and FastPath Guide*

Written for anyone qualified to install a NonStop S-series server. Describes how to install and start a NonStop S-series server for the first time. It includes information about installing server hardware, cabling system enclosures, installing and starting system consoles, installing external system devices, starting the server, and configuring the server after startup. This guide also includes a case study of installing a sample system and a quick reference to installing and configuring a two-processor or four-processor NonStop S-series server in the Tetra 8 topology.

- *NonStop S-Series Planning and Configuration Guide*

Describes the ServerNet system area network (ServerNet SAN), the available hardware and software configurations for NonStop S-series servers, site planning and preparation, creating the operational environment, and making hardware and software configuration changes to an existing server. This guide describes how to plan and configure a NonStop S-series server and provides a case study documenting a sample system. This guide is written for those who are responsible for planning the installation, configuration, and maintenance of the server and the software environment at a particular site.

- *Hotstuff Messages*

If you do not enroll to receive ExpressNotice messages, you can view Hotstuff messages, SPR Notes, or other ExpressNotice messages in the NTL Support and Service library. For more information, see [ExpressNotice](#) on page A-1.

Note. SPR Notes are discontinued as of June 2006. Previously published SPR Notes continue to be available in NTL.

- *The Interactive Upgrade Guide and the Interactive Upgrade Guide 2*

Browser-based tools that are accessed through NTL, these guides provide customized migration planning information and highlight new features. The Interactive Upgrade Guide supports D-series through G06.24 RVUs. The Interactive Upgrade Guide 2 supports G06.16 and later RVUs and H-series RVUs.

- *Managing Software Changes*

Serves as an introduction and reference to the TRM2000, the system migration and installation process, SPR analysis, and HP resources for evaluating new RVUs and SPRs.

- *NonStop S-Series Operations Guide*

Written for system operators, this guide describes how to perform routine system hardware operations for NonStop S-series servers. These tasks include starting and stopping the system, monitoring the system, operating disk and tape subsystems, performing routine hardware maintenance, and performing recovery operations.

- *NonStop S-Series Service Provider Supplement*

Written for system support planners responsible for the correct operation of system hardware, this guide describes how to replace system hardware components defined as field-replaceable units (FRUs) on a NonStop S-series server. You can find this document in the Hardware Service and Maintenance Publications category of the NTL Support and Service library.

- *The NonStop System Console Installer Guide*

Provides information about upgrading a system console to the latest versions of the applications delivered on the NonStop System Console Installer DVD.