

**PROTECT-X**  
**AUTOMATED EXPERT SECURITY**  
**HARDENING**  
**FOR SAFEGUARD AND OSS**

*Callum Barclay*  
*CTO and Founder*  
*Computer Security Products, Inc.*



# Agenda

- Brief review of CSP and current offerings
- CSP-Wiki – Expert NonStop Security Knowledge at Your Fingertips
- Introduction to Protect-X

# CSP Product Portfolio

**Protect-XP – GUI interface to manage Safeguard**

**CSP-PassPort – User access control and command management**

**CRM/FIC – PCI Compliance reporting and File Integrity Monitoring**

**NIMS – LDAP based Safeguard User management support for  
Oracle IDM**

**Alert-Plus – Rules-based SG event alerts plus real-time merged audit**

**Auditview – Report writer for Safeguard and CSP Product Audit**

**CSP Authenticator – RSA two-factor authentication support**

**CSP NetPass – Change user passwords on multiple systems at once**

**Spoolview – GUI interface for Peruse**



# CSP-Wiki®

**CSP-Wiki contains best practices for securing Safeguard, OSS and UNIX**

**Data compiled from many sources**

**Free access to any NonStop customer**






















[Random page](#)

#### Tools

[What links here](#)  
[Related changes](#)  
[Special pages](#)  
[Printable version](#)  
[Permanent link](#)  
[Page information](#)  
[Cite this page](#)

## Security Hardening Rules

-   Security Hardening Rules
  -   Initial System Hardening
    -   Safeguard Configuration and Management
      -  Audit
      -  Safeguard Configuration Files
      -  Passwords
      -  Users and Aliases
      -  Security Groups
      -  Administrative Groups
      -  Authentication
      -  Access Control
      -  Default Passwords
    -  Software Installation Using DSM/SCM and Software Essentials
  -   User Management
  -   Guardian File Security
  -   OSS File Security
    -  SQL/MP Object Security
  -   SQL/MX Object Security
  -   NonStop Server for Java (NSJ)

# 0013 - Optimize Audit Trail Record Writing for Performance

[<Prev](#) [Next>](#)

Rule Number	0013
Rule Name	Optimize Audit Trail Record Writing for Performance
Verifiable	Yes
Category Level 1	Initial System Hardening
Category Level 2	Safeguard Configuration and Management
Category Level 3	Audit
Description/Reason	Audit trail record writing must be optimized for performance. You can configure Safeguard to either write audit records to disk individually (CACHE ON) or to cache the records in memory and write multiple records at a time (WRITE-THROUGH CACHE OFF).
Recommendation	For performance reasons, HP recommends setting WRITE-THROUGH CACHE to OFF (the default). Note: You run a small risk of losing THROUGH CACHE set to OFF.
Technical Notes	<p><b>WRITE-THROUGH CACHE { ON   OFF }</b></p> <p>ON specifies that after each audit record is written, the block in which it resides is written to disk. OFF specifies that a block modified as a cache in memory and not written to disk immediately. The initial setting of WRITE-THROUGH CACHE is OFF.</p> <pre>Protect XP GUI &gt; Safeguard&gt; Audit Service   Write Through Cache ON OFF</pre> <pre>TACL&gt; SAFECOM INFO AUDIT SERVICE CURRENT AUDIT POOL  \$AUDIT.SAFE CURRENT AUDIT FILE  \$AUDIT.SAFE.A0759814 NEXT AUDIT POOL RECOVERY            RECYCLE FILES CURRENT STATE       RECYCLING FILES WRITE-THROUGH CACHE OFF EOF REFRESH         ON</pre>



# Protect-X

Automated Security Hardening

Multi-Platform Support

Browser-Based Interface

Driven by CSP-Wiki ®



# Introducing ... Protect-X !

Click below to watch the video:

<https://www.youtube.com/watch?v=CEuVqcmoJcw>





# Introducing ... Protect-X !

**New NonStop security hardening solution**

**Self-Hosted Web Application using HTML5**

**Automated Hardening Rules Compliance**

**Change Control using Workflows**

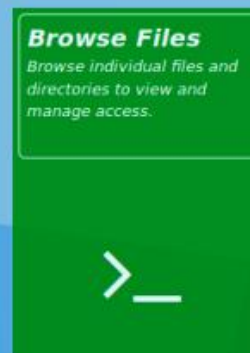
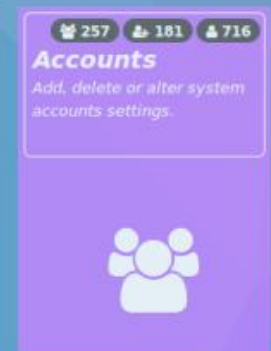
**Task Approval and Scheduling**

**Audit**

**Mobile Friendly**

# Protect-X Dashboard

Node selected: TITANIUM Logged in as: admin Logout






# Protect-X Users Screen



Node selected:  TITANIUM ▾ Logged in as: admin  7 [Logout](#)

## Protect-X Users

### Add users




 No roles will be applied 

[Add user](#)

### Available users

 admin

 DB administrator

 John Doe

### User profile

[User details](#) [Roles](#) [Change Password](#)

#### Profile

First name

Last name

Job title


E-mail

Work phone

Phone

Office number



[Upload picture](#) 

#### User details

|

[Apply](#) [Cancel](#)

## Protect-X Users

## Add users

Add user

## Available users

## User profile

 Copy Create profile

## Hardening

## Vulnerability

☒ Can view effective access page

## Approvals

☒ Can access approvals page☒ Can manage Approval cases

## File control - Browse files

☒ Can browse remote systems


## File control - Change Control


# Protect-X - Safeguard User Management


User Management

Node selected


Add user

 Please enter group name


 Please enter user name


 Please enter password

Here you can specify SafeGuard User ID for the user.

 Please enter user ID

Please select user you want to clone from.





 Clone user

Expert mode ^

Add user

Available users

 ABCTEST.A [155,0]

 ABCTEST.ARTEM123 [155,88]

User profile

Actions

General

Password

Def. Prot.

Def. Prot. ACL

Aliases

Groups

Comint

OSS

Owner Lis

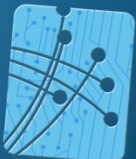
Thaw

Freeze

Delete

Cleanup

Alias

**CSP**   
COMPUTER SECURITY PRODUCTS, INC.

# OSS File Browser

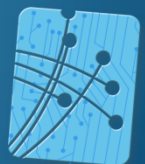
Logged in as: admin 42 Logout

File browser / (0 items in file basket) Show Node selected: aproskurin-pc

	<input type="checkbox"/> Name	Size	Permissions	Owner	Group	Modified
Change control	<input type="checkbox"/> bin	4K	drwxr-xr-x	root	root	8/17/2015, 6:42:06 AM
	<input type="checkbox"/> boot	4K	drwxr-xr-x	root	root	9/9/2015, 9:27:43 AM
	<input type="checkbox"/> cdrom	4K	drwxrwxr-x	root	root	7/30/2015, 7:00:02 AM
Vulnerability Management	<input type="checkbox"/> dev	5K	drwxr-xr-x	root	root	10/19/2015, 12:49:24 PM
	<input type="checkbox"/> etc	12K	drwxr-xr-x	root	root	10/19/2015, 8:53:21 AM
	<input type="checkbox"/> home	4K	drwxr-xr-x	root	root	8/28/2015, 10:18:31 AM
Command Control	<input type="checkbox"/> lib	4K	drwxr-xr-x	root	root	7/30/2015, 7:38:52 AM
	<input type="checkbox"/> lib64	4K	drwxr-xr-x	root	root	4/22/2015, 8:01:55 AM
	<input type="checkbox"/> lost+found	16K	drwx-----	root	root	7/30/2015, 6:55:34 AM
	<input type="checkbox"/> media	4K	drwxr-xr-x	root	root	7/30/2015, 7:17:03 AM
	<input type="checkbox"/> mnt	4K	drwxr-xr-x	root	root	4/17/2015, 5:34:41 PM
	<input type="checkbox"/> opt	4K	drwxr-xr-x	root	root	9/14/2015, 12:23:11 PM
	<input type="checkbox"/> proc	0b	dr-xr-xr-x	root	root	10/16/2015, 11:20:39 AM
	<input type="checkbox"/> root	4K	drwx-----	root	root	8/31/2015, 5:31:35 PM
	<input type="checkbox"/> run	820b	drwxr-xr-x	root	root	10/17/2015, 7:51:29 AM
	<input type="checkbox"/> sbin	12K	drwxr-xr-x	root	root	8/17/2015, 6:42:06 AM
	<input type="checkbox"/> srv	4K	drwxr-xr-x	root	root	4/22/2015, 8:01:51 AM
	<input type="checkbox"/> sys	0b	dr-xr-xr-x	root	root	10/16/2015, 11:20:40 AM
	<input type="checkbox"/> tmp	4K	drwxrwxrwt	root	root	10/20/2015, 12:21:15 PM
	<input type="checkbox"/> usr	4K	drwxr-xr-x	root	root	4/22/2015, 8:01:51 AM
	<input type="checkbox"/> var	4K	drwxr-xr-x	root	root	8/5/2015, 1:47:27 PM
	<input type="checkbox"/> initrd.img	33b	lrwxrwxrwx	root	root	9/9/2015, 9:27:07 AM
	<input type="checkbox"/> initrd.img.old	33b	lrwxrwxrwx	root	root	8/19/2015, 6:51:31 AM
	<input type="checkbox"/> vmlinuz	30b	lrwxrwxrwx	root	root	9/9/2015, 9:27:07 AM
	<input type="checkbox"/> vmlinuz.old	30b	lrwxrwxrwx	root	root	8/19/2015, 6:51:31 AM

CSP

COMPUTER SECURITY PRODUCTS, INC.



# OSS File Security Management

Logged in as: admin 4 [Logout](#)

### Owner Information

**Existing owner**  

👤 aproskurin

**Existing group owner**  

👤 aproskurin

**New owner**  

Select user

**New group owner**  

Select group

**Recommended values**

Add

### Existing Permissions Information

**Existing permissions**

Owner

rW-

Group

rW-

Other

r--

Special modes

---

**New/recommended permissions**

Owner

???

Group

?wx

Other

? ??

Special modes

??? ???

Add

### Pending changes

Change file permissions  
=> rw???????


Change file permissions  
=> rwxrw????

Change file permissions  
=> ???wx???

Implement Now

Submit for approval

File basket						Clear selected		Clear all			
System Name	Name		Size	Permissions	Owner	Group	Modified				
aproskurin-pc	<input type="checkbox"/>	/home/aproskurin/test_files/file1	0b	-rw-rw-r--	👤 aproskurin	👤 aproskurin	11/3/2015, 11:14:04 AM				
aproskurin-pc	<input type="checkbox"/>	/home/aproskurin/test_files/file2	0b	-rw-rw-r--	👤 aproskurin	👤 aproskurin	11/3/2015, 11:14:05 AM				
aproskurin-pc	<input type="checkbox"/>	/home/aproskurin/test_files/file3	0b	-rw-rw-r--	👤 aproskurin	👤 aproskurin	11/3/2015, 11:14:07 AM				
aproskurin-pc	<input type="checkbox"/>	/home/aproskurin/test_files/file4	0b	-rw-rw-r--	👤 aproskurin	👤 aproskurin	11/3/2015, 11:14:07 AM				
aproskurin-pc	<input type="checkbox"/>	/home/aproskurin/test_files/file5	0b	-rw-rw-r--	👤 aproskurin	👤 aproskurin	11/3/2015, 11:14:08 AM				

**CSP**   
COMPUTER SECURITY PRODUCTS, INC.



# Protect-X - Safeguard Globals Management

Node selected: TITANIUM

Logged in as: admin

Logout

Safeguard Globals management

GeneralDevicesDisk filesProcessesTerminalsAuthenticationPasswordDisk file patternSearch

Search for...Search

AUDIT-CLIENT-SERVICE

AUDIT-CLIENT-GUARDIAN

Defines whether the Safeguard software accepts Guardian-related audit records from HP privileged subsystems. These

ON

AUDIT-CLIENT-OSS

ON specifies that the Safeguard software will accept OSS related audit records from privileged client subsystems and write

OFF

AUDIT-OSS-FILTER

ON

<

WARNING-MODE

SYSTEM-WARNING-MODE

When SYSTEM-WARNING-MODE is set to ON, Safeguard bases its access ruling on the global parameter

OFF

OBJECT-WARNING-MODE

This setting determines whether or not Safeguard will evaluate WARNING-MODE attribute in Individual Object Protection

OFF

Audit object access

AUDIT-OBJECT-ACCESS-PASS

Defines additional auditing for successful object accesses. This setting supplements the audit settings in all object

NONE

AUDIT-OBJECT-ACCESS-FAIL

Defines additional auditing for unsuccessful object accesses. This setting supplements the audit settings in all object

ALL

Audit object authorization record access

AUDIT-OBJECT-MANAGE-PASS

Defines additional auditing for successful object authorization record accesses. This setting supplements the audit settings in

ALL

AUDIT-OBJECT-MANAGE-FAIL

ALL

<

Misc

WARNING-FALLBACK-SECURITY

WARNING-FALLBACK-SECURITY controls SAFEGUARD results when WARNING-MODE is ON.

GRANT

ALLOW-NODE-ID-ACL

OFF

<

Submit for approval

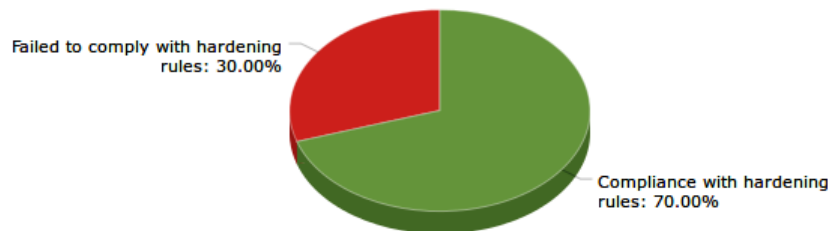
Implement Now

# Protect-X NonStop Security Hardening Engine







Node selected: ITANIUM  Logged in as: admin  0 [Logout](#)

## Hardening


### Overall system status



### Available nodes


Type	Version	Name	Status
 NonStop	123.22	ITANIUM	<div><div>70%</div><div>30%</div></div>
 UBUNTU	321.22	V-UBNTX64-SRV	<div><div>40%</div><div>60%</div></div>
 NonStop	123.222...	ITANIUM-1	<div><div>40%</div><div>60%</div></div>
 NonStop	123.222...	ITANIUM-2	<div><div>10%</div><div>90%</div></div>
 NonStop	123.222...	ITANIUM-3	<div><div>90%</div><div>10%</div></div>
 NonStop	123.222...	ITANIUM-4	<div><div>100%</div><div>0%</div></div>


### Selected Node Details

 NonStop	123.22	ITANIUM	<div><div>85%</div><div>15%</div></div>
<b>System details</b>			
System name:	ITANIUM		
System type:	NonStop		
System Version:	123.2366		
System address:	192.168.4.228(/24)		
Kernel version:	123.021Vddd		
CPU's	123.021Vddd		
Available disc space	123Tb		


### Profiles

Profile name	Created by	Status	
<input checked="" type="checkbox"/> Initial System Hardening	CSPsecurity	<div><div>25%</div><div>75%</div></div>	 
<input checked="" type="checkbox"/> User and Alias Security	CSPsecurity	<div><div>50%</div><div>50%</div></div>	 
<input checked="" type="checkbox"/> OSS Security Settings	CSPsecurity	<div><div>85%</div><div>15%</div></div>	 
<input type="checkbox"/> copy of OSS Security Set...	Artem Proskurin		  
<input type="checkbox"/> copy of User and Alias S...	Artem Proskurin		  

[Re-evaluate all](#) 

[Show Summary Report](#) 

# Protect-X Safeguard Hardening Screen

Node selected:  ITANIUM

Logged in as: **admin**

 0

Logout

Hardening

Show all

 NonStop ITANIUM - Details

ITANIUM hardening compliance

Initial System Hardening

2 / 5

## AUDIT-CLIENT-GUARDIAN

Defines whether the Safeguard software accepts Guardian-related audit records from HP privileged subsystems. These subsystems are known as clients. ON indicates that the Safeguard software accepts audit records from Guardian clients. OFF indicates that it does not accept the

Expected value:

LOCAL

Current value:

REMOTE

## AUDIT-CLIENT-GUARDIAN

Defines whether the Safeguard software accepts Guardian-related audit records from HP privileged subsystems. These subsystems are known as clients. ON indicates that the Safeguard software accepts audit records from Guardian clients. OFF indicates that it does not accept the

Expected value:

LOCAL

Current value:

LOCAL

## AUDIT-CLIENT-GUARDIAN

Defines whether the Safeguard software accepts Guardian-related audit records from HP privileged subsystems. These subsystems are known as clients. ON indicates that the Safeguard software accepts audit records from Guardian clients. OFF indicates that it does not accept the

Expected value:

LOCAL

Current value:

REMOTE

## AUDIT-CLIENT-GUARDIAN

Defines whether the Safeguard software accepts Guardian-related audit records from HP privileged subsystems. These subsystems are known as clients. ON indicates that the Safeguard software accepts audit records from Guardian clients. OFF indicates that it does not accept the

Expected value:

LOCAL

Current value:

LOCAL

## AUDIT-CLIENT-GUARDIAN

Defines whether the Safeguard software accepts Guardian-related audit records from HP privileged subsystems. These subsystems are known as clients. ON indicates that the Safeguard software accepts audit records from Guardian clients. OFF indicates that it does not accept the

Expected value:

LOCAL

Current value:

LOCAL

User and alias security

2 / 5



2 / 5

Unlock profile edit mode

Back

Apply

# Protect-X Actions Approval Screen

Node selected:  ITANIUM ▼ Logged in as: **admin**  **2** Logout

Approvals


Filter by a user ▼


Filter by category ▼

Filter by Node ▼

Case number: **#23**

- Status: **awaiting approval**
- Timestamp: at Thu Aug 11 2016 12:53:48 GMT-0400 (EDT)
- Affected items: 1 user

 admin, John Doe

 NonStop system user mana

ITANIUM

Change default protection ACL  
=> [ A.ASDFGR ]

Details ▲

Approve ▼

Decline ▼


Dismiss


userid: [ 16,0 ] grant: [ Grant ] permissions: [ R,,,, ] - added

userid: [ 155,11 ] grant: [ Grant ] permissions: [ R,W,,,, ] - added

Case number: **#22**

- Status: **awaiting approval**
- Timestamp: at Wed Aug 10 2016 16:54:10 GMT-0400 (EDT)
- Affected items: SafeGuard Globals profile

 admin, John Doe

 SafeGuard globals

ITANIUM

Update SafeGuard globals profile  
=> [ SafeGuard globals ]

Details ▲

Approve ▼

Decline ▼

Dismiss

[ field name:AUDIT-CLIENT-OSS value:OFF ]

# Protect-X Audit Log

Node selected:  VITANIUM Logged in as: admin  1 Logout

Audit

Filter by date



Filter by case number



Filter by a user



Filter by category



Filter by Node



08/11/2016

Apply

Clear filter

AM



11

:

59

PM

Sep 2016



Th	Fr	Sa	Su	Mo	Tu	We	Th	Fr	Sa
4	5	6	28	29	30	31	1	2	3
11	12	13	4	5	6	7	8	9	10
18	19	20	11	12	13	14	15	16	17
25	26	27	18	19	20	21	22	23	24
1	2	3	25	26	27	28	29	30	1
8	9	10	2	3	4	5	6	7	8

• Affected items: SafeGuard Globals profile

Audit record number: #59

- Text: #21 => Update SafeGuard globals profile , case has been implemented
- Timestamp: at Wed Aug 10 2016 16:28:43 GMT-0400 (EDT)
- Affected items: SafeGuard Globals profile

Audit record number: #58

admin, John Doe

SafeGuard globals

VITANIUM

Update SafeGuard globals profile  
=> [ SafeGuard globals ]

Details

admin, John Doe

SafeGuard globals

VITANIUM

Update SafeGuard globals profile  
=> [ SafeGuard globals ]

Details

admin, John Doe

SafeGuard globals

VITANIUM

Update SafeGuard globals profile  
=> [ SafeGuard globals ]

Details

admin, John Doe

SafeGuard globals

VITANIUM

Update SafeGuard olobals

# Protect-X Futures

## Planning on 3 releases for 2017

- Many new features to be announced at TBC
- Enhancements to CSP Wiki
- Cross Platform Support for other UNIX Servers

# THANK YOU!

Please visit our Website for  
more information

[www.CSPsecurity.com](http://www.CSPsecurity.com)