HP NonStop Education Talk
XYGATE User Authentication
XYGATE Access Control
Sept 27th, 2011

Karen Copeland
NED Product Management

Barry Forbes
Vice President, XYPRO Sales & Marketing
Agenda

• Managing Security Risks
• NonStop Security Products
• New products now available from NonStop:
  • XYGATE User Authentication
  • XYGATE Access Control
Security breaches are expensive

<table>
<thead>
<tr>
<th>Security Breach</th>
<th>User records Impacted</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heartland Payment Systems (2009)</td>
<td>100,000,000+</td>
<td>$12.6M</td>
</tr>
<tr>
<td>Sony Corporation Playstation3 (2011)</td>
<td>77,000,000</td>
<td>Millions and growing</td>
</tr>
<tr>
<td>TJ Maxx retail stores (2007)</td>
<td>45,700,000</td>
<td>$4.5B</td>
</tr>
<tr>
<td>Deutsche Telecom (2008)</td>
<td>17,000,000</td>
<td>estimated at $1B</td>
</tr>
<tr>
<td>Dai Nippon Printing (2007)</td>
<td>9,000,000</td>
<td>$8.6M</td>
</tr>
</tbody>
</table>

- A security breach in the U.S. today costs a company around $214 per record.*
- Breach costs have risen to $7.2M per incident.***
- Median cost of cyber crime is now $5.9 million per year, a 56% increase from the median cost in last year’s study.**

Sources include:
http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP
* 2010 Annual Study: U.S. Cost of a Data Breach, March 2011, Poneman Institute, LLC, Symantec
** 2nd Annual Cost of Cyber Crime Study, an HP-sponsored survey by Poneman Institute, LLC, Symantec
How companies lose money

- Information loss
- Business disruption
- Revenue loss
- Equipment damages
- Other costs

Additionally there can be:
- Fines
- Stock price loss

Source: 2nd Annual Cost of Cyber Crime Study, an HP-sponsored survey by Poneman Institute, LLC, Symantec – August 2011
What type of cybercrime occurred

Companies have to control:

- Insider access to data
- Who has a userid
- Where they can logon
- What they can do on the system
- When they can do it
- How they monitor what people are doing on the system

Source: 2nd Annual Cost of Cyber Crime Study, an HP-sponsored survey by Poneman Institute, LLC, Symantec – August 2011
Compliance is no longer optional

- Security compliance affects businesses worldwide
- Today compliance regulations exist for nearly all industries
  - Financial, Retail, Telco, Healthcare
- Regulations get stricter each year with stronger penalties for failure
  - PCI/DSS, HIPAA, Sarbanes-Oxley, etc
- Laws continue to emerge that govern what actions a company must take when a breach occurs
  - 45 states, Washington D.C., Puerto Rico and the Virgin Islands all have legislation in this area.
HP NonStop Server
More secure than ever before

On Platform Security
- Virus free environment
- Modern password & userid controls
- Event logging
- LDAP integration
- Access control, including key stroke logging

Data in Motion Security
- Encryption of data traffic
- Modern and standard security products
- Protects both Guardian and OSS

Data at Rest Security
- Integrated low latency data encryption
- State of the art enterprise key management

Auditing and Compliance
- Automated event collection and reporting
- Event alarms
- System and File Integrity Monitoring
- Evaluation for security compliance
- SIEM (Security Information and Event Manager) device integration

|= New Offerings
Security Areas

1. **On Platform**
   - Only authorized users can access the system. Access to data and other resources are controlled.

2. **Data In Motion**
   - Network and sensitive data moving between systems or workstations cannot be deciphered if intercepted.

3. **Data At Rest**
   - Stored data and sensitive customer information is protected on disk or tape.

4. **Compliance**
   - Security policies can be verified to be working and compliance regulations can be proven to be in place.
### Security Products by Platform at a glance

<table>
<thead>
<tr>
<th>J Series</th>
<th>H Series</th>
<th>G Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-Core &amp; BladeSystems</td>
<td>NonStop Integrity</td>
<td>S-series Platforms</td>
</tr>
<tr>
<td><strong>Included with the system out of the box</strong></td>
<td><strong>Included with the system out of the box</strong></td>
<td><strong>Included with the system out of the box</strong></td>
</tr>
<tr>
<td>Safeguard &amp; SafeArt</td>
<td>Safeguard &amp; SafeArt</td>
<td>Safeguard &amp; SafeArt</td>
</tr>
<tr>
<td>Data Sanitization (OSM)</td>
<td>Data Sanitization (OSM)</td>
<td>NonStop SSH – full license</td>
</tr>
<tr>
<td>iTP Secure WebServer</td>
<td>iTP Secure WebServer</td>
<td>NonStop SSH – FTP license only</td>
</tr>
<tr>
<td>NonStop Security Update Bundle</td>
<td>NonStop Security Update Bundle</td>
<td>Secure Virtual Tape Subsystem (VTS)</td>
</tr>
<tr>
<td>Includes:</td>
<td>Includes:</td>
<td>Data Sanitization (in OSM)</td>
</tr>
<tr>
<td>NonStop SSH</td>
<td>NonStop SSH</td>
<td>XYGATE Merged Audit (XMA)</td>
</tr>
<tr>
<td>NonStop SSL</td>
<td>NonStop SSL</td>
<td>SFTP API Plug-in</td>
</tr>
<tr>
<td>XYGATE Merged Audit</td>
<td>XYGATE Merged Audit</td>
<td>XMA Plug-in for ACI Base24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Purchased separately</strong></th>
<th><strong>Purchased separately</strong></th>
<th><strong>Purchased separately</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Level Encryption (VLE)</td>
<td>Volume Level Encryption (VLE)</td>
<td>Safeguard &amp; SafeArt</td>
</tr>
<tr>
<td>Enterprise Secure Key Manager (ESKM)</td>
<td>Enterprise Secure Key Manager (ESKM)</td>
<td>NonStop SSH – full license</td>
</tr>
<tr>
<td>Secure Virtual Tape Subsystem (VTS)</td>
<td>Secure Virtual Tape Subsystem (VTS)</td>
<td>NonStop SSH – FTP license only</td>
</tr>
<tr>
<td>IPSec (with purchase of IP CLIM)</td>
<td>IPSec (with purchase of IP CLIM)</td>
<td>Secure Virtual Tape Subsystem (VTS)</td>
</tr>
<tr>
<td>NonStop Security Update Bundle</td>
<td>NonStop Security Update Bundle</td>
<td>Data Sanitization (in OSM)</td>
</tr>
<tr>
<td>{For servers purchased before Sept 2010}</td>
<td>{For servers purchased before Sept 2010}</td>
<td>XYGATE Merged Audit (XMA)</td>
</tr>
<tr>
<td>SFTP API Plug-in</td>
<td>SFTP API Plug-in</td>
<td>SFTP API Plug-in</td>
</tr>
<tr>
<td>XMA Plug-in for ACI Base24</td>
<td>XMA Plug-in for ACI Base24</td>
<td>XMA Plug-in for ACI Base24</td>
</tr>
<tr>
<td>XMA Plug-in for HP HLR</td>
<td>XMA Plug-in for HP HLR</td>
<td>XMA Plug-in for HP HLR</td>
</tr>
<tr>
<td>XYGATE Compliance PRO</td>
<td>XYGATE Compliance PRO</td>
<td>XYGATE Compliance PRO</td>
</tr>
<tr>
<td>XYGATE Access Control</td>
<td>XYGATE Access Control</td>
<td>XYGATE Access Control</td>
</tr>
<tr>
<td>XYGATE User Authentication</td>
<td>XYGATE User Authentication</td>
<td>XYGATE User Authentication</td>
</tr>
<tr>
<td>ArcSight Integration</td>
<td>ArcSight Integration</td>
<td>ArcSight Integration</td>
</tr>
</tbody>
</table>
XYGATE User Authentication
XYGATE Access Control

Now available from HP
• 28 years serving the HP NonStop™ community
• Specialists in security, compliance & encryption
• Sales & Support offices around the world
  – North America, Latin America, UK & Europe, APJ, Middle East & Africa
• Sales numbers reflect increased spending on security products within the NonStop user base
  – 2010 sales up 60% over 2009
  – Growth continuing in 2011
Security needs

- Compliance
- Authentication
- Audit
- Access Control
Can I pass a compliance audit? Does my system meet all internal security policies and rules?

Security needs

- Compliance
- Authentication
- Audit
- Access Control
Can I pass a compliance audit?  Does my system meet all internal security policies and rules?

Who is allowed onto my system?  When can they logon on?
Can I pass a compliance audit?
Does my system meet all internal security policies and rules?

Who is allowed onto my system?
When can they logon on?

Who can do what on my system?
What commands can they execute?
Can I pass a compliance audit? Does my system meet all internal security policies and rules?

Who is allowed onto my system? When can they logon on?

What’s been happening on my system?

Who can do what on my system? What commands can they execute?
Can I pass a compliance audit? Does my system meet all internal security policies and rules?

Who is allowed onto my system? When can they logon on?

What’s been happening on my system?

Who can do what on my system? What commands can they execute?
Security needs

Can I pass a compliance audit? Does my system meet all internal security policies and rules?
- Analyze current relevant security settings
- Flag settings that may cause compliance issues

What’s been happening on my system?

Who is allowed onto my system? When can they logon on?

Who can do what on my system? What commands can they execute?
Security needs

Can I pass a compliance audit? Does my system meet all internal security policies and rules?

- Analyze current relevant security settings
- Flag settings that may cause compliance issues

What’s been happening on my system?

XYGATE Compliance PRO

Who is allowed onto my system? When can they logon on?

- Authenticate against LDAP, RSA SecurID and RADIUS
- Provide granular logon controls

XYGATE User Authentication

XYGATE Merged Audit

Who can do what on my system? What commands can they execute?

XYGATE Access Control
Can I pass a compliance audit? Does my system meet all internal security policies and rules?
- Analyze current relevant security settings
- Flag settings that may cause compliance issues

What's been happening on my system?

Who is allowed onto my system? When can they logon on?
- Authenticate against LDAP, RSA SecurID and RADIUS
- Provide granular logon controls

Who can do what on my system? What commands can they execute?
- Eliminate Shared USERIDs
- Control who can issue individual commands and subcommands in all system utilities
- Log activity at the keystroke level
Can I pass a compliance audit? Does my system meet all internal security policies and rules?
- Analyze current relevant security settings
- Flag settings that may cause compliance issues

What’s been happening on my system?
- Capture all NonStop security events
- Filter to only show events of interest
- Feed data to off board SIEM devices

Who is allowed onto my system? When can they logon on?
- Authenticate against LDAP, RSA SecurID and RADIUS
- Provide granular logon controls

Who can do what on my system? What commands can they execute?
- Eliminate Shared USERIDs
- Control who can issue individual commands and subcommands in all system utilities
- Log activity at the keystroke level

XYGATE Compliance PRO
XYGATE User Authentication
XYGATE Merged Audit
XYGATE Access Control
Security needs

Offered by HP as an independent product in May 2011

Bundled by HP with the NonStop OS in fall of 2010.
Today's talk focuses on these new products!
XYGATE
User Authentication
XYGATE User Authentication

Features

XYGATE User Authentication, available this month from HP, allows customers to implement logon controls at a granular level and integrate their NonStop server into larger LDAP environments

• Logon Controls at a granular level, including time based.
• Rules for User group logons and controls for group manager capabilities
• Audit reporting on logon events
• IP, Requestor and Ancestor controls
• LDAP interface for NonStop
• Support for RSA SecurID tokens and RADIUS authentication
• Offered as an independent product shipped on a DVD for J Series, H Series and G Series.
SEEP Evaluation

- XYGATE XUA is a Safeguard authentication Security Event Exit process (SEEP)
- SEEPs are configured using SAFECOM (or SPI)
- SEEPs are exits where Safeguard will check to see if an external product is defined and active, and if so, will pass a request evaluation message to the product before evaluating the request under Safeguard's own rules.
  - If the SEEP returns NO, the request is denied
  - If the SEEP returns YES, Safeguard then evaluates the request itself and abides by the decision made based on Safeguard's rules
  - If the SEEP returns NO DECISION, Safeguard then evaluates the request itself and abides by the decision made based on Safeguard's rules
Logon Controls

• Safeguard:
  – Userid or alias
  – 64-character password or pass-phrase
  – Basic password quality options
  – Global setting of maximum bad attempts
  – Global setting of either fail-freeze or timeout when maximum bad attempts is reached

• XYGATE UA extensions:
  – Individual settings of maximum bad attempts
  – Individual choice of fail-freeze, timeout, or process-stop when maximum bad attempts is reached
User Authentication Features

• Control logons based on:
  • Ancestor program
  • Requestor program
  • Port/IP Address
  • Time of day/day of week
  • Current logged-on user

• Supports user impersonation – logon using SUPER.SUPER but your own password.

• Apply global-level authentication controls to the user/group-level (e.g. Apply Authenticate_Fail_Freeze to a user or group, not global)
User Authentication Features

- Includes EXPLAIN/WHATIF functionality for testing of rules
- Authentication decisions are audited, and audit data can be integrated/sent to a SIEM device with Merged Audit
- NonStop userids can be frozen/have passwords expired – all authentication must come from LDAP/AD/RSA
- Allows customers to meet corporate standards for authentication
XYGATE User Authentication (XUA) Architecture

XUA provides an extension to Safeguard to authenticate users based on pre-set rules that are applied on top of NonStop security settings.
XYGATE User Authentication (XUA) Architecture

XUA provides an extension to Safeguard to authenticate users based on pre-set rules that are applied on top of NonStop security settings.

Users can now access NonStop servers through an industry SSO solution. The Authentication layer will trace the user to the associated NonStop userid for authentication.

100% of NonStop's Authentication Requests are handled through the User Authentication layer.
XYGATE User Authentication (XUA) Architecture

XUA provides an extension to Safeguard to authenticate users based on pre-set rules that are applied on top of NonStop security settings.

Users can now access NonStop servers through an industry SSO solution. The Authentication layer will trace the user to the associated NonStop userid for authentication.

User activities can be monitored and audited.

Audit Data
(Audits can be captured in up to 9 locations simultaneously)
Sample XUA Rules – Freeze Policy

UAGROUP FAIL_FREEZE_NOT_PRIV
DESCRIPTION "Freeze Permanently on max attempts"
FROM_USER $EVERYONE
TO_USER $EVERYONE NOT $PRIVIDS
AUTHENTICATE_MAXIMUM_ATTEMPTS 3
AUTHENTICATE_FAIL_FREEZE ON
Sample XUA Rules – Freeze Policy

UAGROUP FAIL_FREEZE_NOT_PRIV
DESCRIPTION "Freeze Permanently on max attempts"
FROM_USER $EVERYONE
TO_USER $EVERYONE NOT $PRIVIDS
AUTHENTICATE_MAXIMUM_ATTEMPTS 3
AUTHENTICATE_FAIL_FREEZE ON
Sample XUA Rules – Freeze Policy

UAGROUP FAIL_FREEZE_NOT_PRIV
DESCRIPTION "Freeze Permanently on max attempts"
FROM_USER $EVERYONE
TO_USER $EVERYONE NOT $PRIVIDS
AUTHENTICATE_MAXIMUM_ATTEMPTS 3
AUTHENTICATE_FAIL_FREEZE ON

XYGATE ACL Group

$EVERYONE \*.\*. *
ALIAS:”\*.\*.”

$PRIVIDS \*.SUPER.*
NETUNDERLYING \*.255,*
*,255
ALIAS:”\*.APPOWNER”
Sample XUA Rules – Remote Access

UAGROUP Users-From-Outside-DMZ

DESCRIPTION "Remote users must use VPN and log via XYGATE AC"
FROM_USER 0,0
TO_USER $EVERYONE
PORT 207.124.10.23*
REQUESTOR $SEC.XYGATEAC.XYGATEAC
AUTHENTICATE_MAXIMUM_ATTEMPTS 5
AUTHENTICATE_FAIL_FREEZE ON
Access Control Features

• Granular control of access to resources
  – Eliminate shared ID use
    • All user job functions can be performed from a single user ID
    • Supports role based access control (RBAC)
  – Command and Sub-Command level control
    • Control commands within utilities
  – Audit to the keystroke level
    • Audit only what is needed – specific users or functions
    • Complete and accurate user accountability
    • Audit the commands entered from OBEY files
Access controls are set up and stored on the system
Access controls are set up and stored on the system.

As users attempt to access system resources, their rights are queried and allowed or denied by the Access Control layer.

PC/Terminal

Configuration Settings and Access Rules

ACCESS CONTROL

NonStop Utility Programs
- TACL
- OSS Shell
- FUP
- All Others
Access controls are set up and stored on the system.

As users attempt to access system resources, their rights are queried and allowed or denied by the Access Control layer.

User activities are monitored and audited including key strokes as desired.
XYGATE Access Control – Shared IDs

• Each user only requires one ID
  – Can be a Guardian User or Alias
  – No need for Super group level (255, *)
  – No need for Manager user level (*, 255)

• Grant privileges based on need

• Passwords to sensitive IDs are not required
XYGATE Access Control – Shared IDs

• Example – SUPER.SUPER Access to SCF via Guardian

$VDBF USER1 4> logon super.super
Password: *******

Welcome to the XYPRO Technology Production Computing Facility \XYS7000.

Last Logon:  12 APR 2010, 22:17
Last Unsuccessful Attempt: 12 APR 2010, 22:11  Total Failures: 3361
$SYSTEM SYSTEM 5> scf
SCF - T9082G02 - (06JAN06) (31OCT05) - 04/13/2010 06:57:11 System \XYS7000
(C) 1986 Tandem (C) 2006 Hewlett Packard Development Company, L.P.
(Invoking \XYS7000.$SYSTEM.SYSTEM.SCFCSTM)
1->
XYGATE Access Control – Shared IDs

• Example – SUPER.SUPER Access to SCF via XYGATE Access Control

$VDBF USER1 5> xac scf-255

XAC - \XYS7000.XYPRO.USER1 Password: ********
XYGATEAC 5.52 XYPRO Eastern North America \XYS7000 20110630 (see >CONFIG for Copyright)
SCF - T9082G02 - (06JAN06) (31OCT05) - 04/13/2010 07:06:19 System \
XYS7000
(C) 1986 Tandem (C) 2006 Hewlett Packard Development Company, L.P.
(Invoking \XYS7000.$SYSTEM.SYSTEM.SCFCSTM)
1->

SCF Running as SUPER.SUPER
XYGATE Access Control – Shared IDs

- Example – SUPER.SUPER Access to SCF via XYGATE Access Control
  - Basic Configuration

```
COMMAND SCF-255
  DESCRIPTION "SCF as SUPER.SUPER"
  USER 255,255
  OBJECT $SYSTEM.SYSTEM.SCF
  ACL $SUPER
  VERIFYUSER $EVERYONE
  TIMEOUT 900
  PASSWORDTIMEOUT 600

! Command executes SCF as SUPER.SUPER
! Executes as SUPER.SUPER
! Executes SCF
! Only privileged users can execute this
! Validate user executing the command
! Stop after 15 minutes of inactivity
! Ask for password again after 10
! minutes of inactivity
```
XYGATE Access Control – Shared IDs

- Example – SUPER.SUPER Access to SCF via XYGATE Access Control
- – Deny Commands Configuration

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCF-255-RESTRICTED</td>
<td>Command executes SCF as SUPER.SUPER</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>&quot;SCF as SUPER.SUPER&quot;</td>
</tr>
<tr>
<td>USER 255,255</td>
<td>!Executes as SUPER.SUPER</td>
</tr>
<tr>
<td>OBJECT $SYSTEM.SYSTEM.SCF</td>
<td>!Executes SCF</td>
</tr>
<tr>
<td>ACL $SUPER</td>
<td>!Only privileged users can execute this</td>
</tr>
<tr>
<td>VERIFYUSER $EVERYONE</td>
<td>!Validate user executing the command</td>
</tr>
<tr>
<td>TIMEOUT 900</td>
<td>!Stop after 15 minutes of inactivity</td>
</tr>
<tr>
<td>PASSWORDTIMEOUT 600</td>
<td>!Ask for password again after 10 minutes of inactivity</td>
</tr>
<tr>
<td>DENYCMD ALTER</td>
<td>!Prevent users from altering in SCF</td>
</tr>
<tr>
<td>DENYCMD DELETE</td>
<td>!Prevent users from deleting in SCF</td>
</tr>
</tbody>
</table>
XYGATE Access Control – Role Based

- XYGATE Access Control ACL Groups
  - Provides Role-Based Access Control
  - Allows for ease of administration

<table>
<thead>
<tr>
<th>ACLGROUP</th>
<th>ALIAS</th>
<th>NETUNDERLYING</th>
</tr>
</thead>
<tbody>
<tr>
<td>$EVERYONE</td>
<td>\.<em>.</em>.*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALIAS: &quot;\.<em>.</em>&quot;</td>
<td></td>
</tr>
<tr>
<td>$SUPER</td>
<td>255,255</td>
<td>222,11</td>
</tr>
<tr>
<td></td>
<td>\.*.222,11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>\.*.XYPRO.BARRY</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALIAS: &quot;\.*.barry&quot;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NETUNDERLYING: 222,11</td>
<td></td>
</tr>
</tbody>
</table>
XYGATE Access Control - Audit

- Auditing User and Alias activity is as flexible as you want it to be
  - Keystroke Audit, input and output, all activity for every user.
  - Keystroke Audit only the activity of specific users or functions.
  - Audit the commands entered from OBEY files.
XYGATE Access Control

- Auditing all user activity – Transparency

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>CONVERSATION</td>
</tr>
<tr>
<td>Subtype</td>
<td>DYNAMIC</td>
</tr>
<tr>
<td>Display</td>
<td>ON</td>
</tr>
<tr>
<td>Owner</td>
<td>N/A</td>
</tr>
<tr>
<td>CPU</td>
<td>N/A</td>
</tr>
<tr>
<td>Swap</td>
<td>N/A</td>
</tr>
<tr>
<td>Program</td>
<td>$SYSTEM.XYGATEAC.XYGATEAC</td>
</tr>
<tr>
<td>Lib</td>
<td>N/A</td>
</tr>
<tr>
<td>Resilient</td>
<td>OFF</td>
</tr>
<tr>
<td>Param</td>
<td>audited-tcpip-tacl</td>
</tr>
<tr>
<td>Assigned Window</td>
<td>OFF</td>
</tr>
<tr>
<td>Default Service</td>
<td>OFF</td>
</tr>
<tr>
<td>Autodelete</td>
<td>OFF</td>
</tr>
<tr>
<td>Access</td>
<td>ALL</td>
</tr>
<tr>
<td>Pri</td>
<td>N/A</td>
</tr>
<tr>
<td>Auditing TCP/IP</td>
<td>audited-tcpip-tacl</td>
</tr>
<tr>
<td>Default Service</td>
<td>OFF</td>
</tr>
</tbody>
</table>
XYGATE Audit Reporting
XYGATE Audit Reporting

[Image of XYGATE Report Manager interface]
XYGATE Audit Reporting
XYGATE Audit Reporting

[Image of XYGATE Audit Reporting interface]

All product views are illustrations and might not represent actual product screens.
XYGATE Audit Reporting
XYGATE Audit Reporting

FTP Report To

FTP Server Settings
- Saved Settings: Test
- FTP Server: ftp.yourserver.com
- Port: 21
- User: ftpuser
- Password: **********

Directory: reports\secops\daily
File Name:

Leave blank to use default: AuditPRO_<XMA Installation>_<Report Title>

Append timestamp to file name

Format: TXT

Cancel  Test
XYGATE Audit Reporting

XAC Command Usage - Detail

| Subject Login: DEMO.MANAGER | Object Name: SCP-255 | Session ID: 000000000000000000000000000000000000000000000000
<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Terminal</th>
<th>SessionID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-09-21 09:33:37</td>
<td>\x. $e7n2. $e7t2</td>
<td>10.1.1.185</td>
</tr>
<tr>
<td>2011-09-21 09:43:41</td>
<td>\x. $e7n2. $e7t2</td>
<td>10.1.1.185</td>
</tr>
<tr>
<td>2011-09-21 09:44:40</td>
<td>\x. $e7n2. $e7t2</td>
<td>10.1.1.185</td>
</tr>
<tr>
<td>2011-09-21 09:44:41</td>
<td>\x. $e7n2. $e7t2</td>
<td>10.1.1.185</td>
</tr>
</tbody>
</table>

XAC-I
XAC-C who
XAC-C exit
XAC-C Program ending

Subject Login: DEMO.MANAGER | Object Name: TACL-255 | Session ID: 000000000000000000000000000000000000000000000000
<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Terminal</th>
<th>SessionID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-09-21 10:12:32</td>
<td>\x. $e7n2. $e7t2</td>
<td>10.1.1.185</td>
</tr>
<tr>
<td>2011-09-21 10:12:32</td>
<td>\x. $e7n2. $e7t2</td>
<td>10.1.1.185</td>
</tr>
<tr>
<td>2011-09-21 10:12:31</td>
<td>\x. $e7n2. $e7t2</td>
<td>10.1.1.185</td>
</tr>
<tr>
<td>2011-09-21 10:12:30</td>
<td>\x. $e7n2. $e7t2</td>
<td>10.1.1.185</td>
</tr>
<tr>
<td>2011-09-21 10:12:29</td>
<td>\x. $e7n2. $e7t2</td>
<td>10.1.1.185</td>
</tr>
<tr>
<td>2011-09-21 10:12:28</td>
<td>\x. $e7n2. $e7t2</td>
<td>10.1.1.185</td>
</tr>
</tbody>
</table>

XAC-I
XAC-C Good password at verifyuse
XAC-C LOAD/KEEP 1/$DEMO.XYGATE
XAC-C sink [#history/reset/]
XAC-C run \x.$DEMO.XYGATE .. REM
XAC-C Logoff
Support and Service
Support

XYGATE Access Control and XYGATE User Authentication are supported by the GCSC when purchased from HP.

HP will engage XYPRO if needed as our development resource behind the scenes if any serious issue is found by a customer.
Service

Customers can now purchase security services for these products from HP.
Services may include:

- Installation, configuration set-up and training
- System security evaluation for compliance and vulnerabilities
- Customized security service based on customer’s unique needs

Services can be performed on-site or remotely.
Summary

It’s now easier than ever for NonStop customers to gain access to these products to secure their systems.

• Talk to your HP NonStop Sale representative.

• No need to qualify a new vendor, just add-on to your existing HP P.O. and support contract.

• One place to go for round the clock support – HP

• Get product updates from one central place – HP through NonStop Scout
Questions?

Karen Copeland  Karen.Copeland@hp.com
Wendy Bartlett  Wendy.Bartlett@hp.com
Barry Forbes  Barry_f@xypro.com
Andrew Price  Andrew_p@xypro.com
For More Information

Useful Links:
http://www.hp.com/go/nonstop/security/compliance
  includes datasheets for Compliance PRO and Merged Audit

http://www.hp.com/go/nonstop/security/onplatformsecurity
  future location for datasheets on Access Control and User Authentication

http://www.xypro.com/
  XYPRO’s main website