



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

XYPRO Education



XYGATE User Authentication



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

Copyright & Trademark

XYGATE User Authentication®

Copyright © 2013 XYPRO Technology Corporation. All rights reserved.

This course, as well as the software described in it, is furnished under a License Agreement or Non-disclosure Agreement. The course may be used or copied only in accordance with the terms of the Agreement. Use of this course constitutes acceptance of the terms of the Agreement. No part of this course may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, and translation to another medium, for any purpose without the written permission of XYPRO Technology Corporation.

Trademarks

XYGATE and XYPRO are registered trademarks of XYPRO Technology Corporation. All other brand or product names, trademarks or registered trademarks are acknowledged as the property of their respective owners.

XYPRO Technology Corporation

4100 Guardian Street, Suite 100 Simi Valley, California 93063 USA




How This Course Is Organized

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

This course consists of the topics listed at the left side of this screen. The topics are presented in the order listed. Most sections have multiple slides.

If accessing the course electronically, the sections can be accessed directly by clicking on a topic and/or accessed in sequence using the Page Up and Page Down keys or the < > links.

Practice exercise opportunities are identified by the  image at the upper right of the screen. Exercises may be completed when encountered or together after the course is completed.

The Q & A and Glossary topics at the end of the course provide common questions and definitions of some of the terms used throughout this course.



Who Should Take This Course

This course is intended to provide a basic understanding of the XYGATE User Authentication (XYGATEUA) product.

Students who have no previous experience with the XYGATEUA product should take this course.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Course Objectives

The XYGATE User Authentication (XYGATEUA) course covers the topics listed at the left of the screen. This course is intended to introduce students to the XYGATEUA product.

Upon completion of this course, students will be able to:

- Discuss the purpose and advantages of XYGATEUA
- List and discuss the main components of XYGATEUA
- Describe the XYGATEUA architecture
- Use the XYGATEUA host macros
- Create UAACL user authentication rules
- Perform “what-if” tests to test UAGROUP rules prior to putting the rules into production.
- Generate audit reports

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UAACNF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Overview

The features of the Safeguard security-management software fall into four categories:

1. User Authentication
2. Object Access Authorization
3. Password Quality
4. Auditing

This course provides instruction on **User Authentication**.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



The Safeguard subsystem:

- authenticates users.
- ensures that only persons who enter a valid user name and associated password can access the system.
- controls both interactive and procedural logon attempts by verifying a user's user name and password.
- passes authentication requests to the Authentication Security Event Exit Process (SEEP) if configured and enabled.
- enforces user access and authentication controls such as user expiration date, password expiration date, and grace period during which an expired password can be changed.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Overview

XYGATEUA enhances Safeguard security by providing the ability to:

- **group users and aliases by function**, making the manipulation of a user in the security system a single operation, rather than the modification of multiple records.
- configure `PASSWORD_REQUIRED`, `PASSWORD_MAY_CHANGE`, `AUTHENTICATE_FAIL_FREEZE`, `AUTHENTICATE_FAIL_TIMEOUT`, and `AUTHENTICATE_MAXIMUM_ATTEMPTS` on a per user basis as well as globally.
- restrict logons based on the **ancestor of the process** that is requesting the logon.
- restrict logons to **specific ports**.
- restrict logons to **specific object files** of the processes requesting the logon.
- restrict logons to **specific days and time ranges**.
- **remove the need for users to share sensitive logon IDs** such as that of `SUPER.SUPER`.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Overview

XYGATEUA enhances Safeguard security by providing the ability to:

- map the NonStop user database to an **alternative authentication database** such as LDAP, RSA SecurID or RADIUS.
- divert user authentication to an **LDAP** database.
- require the **RSA SecurID®** authentication.
- work in conjunction with **RADIUS** authentication.
- **test logon rules** before putting them into production.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Overview

XYGATEUA software:

- is bundled with the latest NonStop Server platforms (i.e., NB56000c and NB56000c-cg).
- can be purchased as an upgrade to the Security Bundle on NonStop J-series systems.
- is available as an independent product that can be licensed from HP and XYPRO for H-series systems. If licensed by XYPRO, support will be provided by XYPRO.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Overview

This course is not intended to provide instruction on all features of XYGATEUA nor is it intended for use as documentation.

XYGATEUA is fully documented in the **XYGATE® User Authentication (XUA) Reference Manual**. Refer to this manual for documentation on:

- Installing and securing XYGATEUA
- Configuring XYGATEUA
- Configuring the XYGATEUA SEEP
- Configuring Control Logons Based on the Ancestor Program, Port, Requester, and Time
- Configuring Control Logons via Alternative Authentication Databases
- “What-If” Testing
- Audit Reports
- Host Macros

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Architecture

Safeguard can be configured to pass authorization, authentication, and password-change requests to a Security Event Exit Process (SEEP).

A SEEP is a user-written process that is allowed to participate in security policy enforcement. The Safeguard subsystem passes it requests for authorization, authentication, and password changes.

The SEEP rules on the request and returns the ruling to the Safeguard subsystem for interpretation and enforcement.

XYGATEUA is a SEEP designed to participate in and enhance Safeguard user authentication.

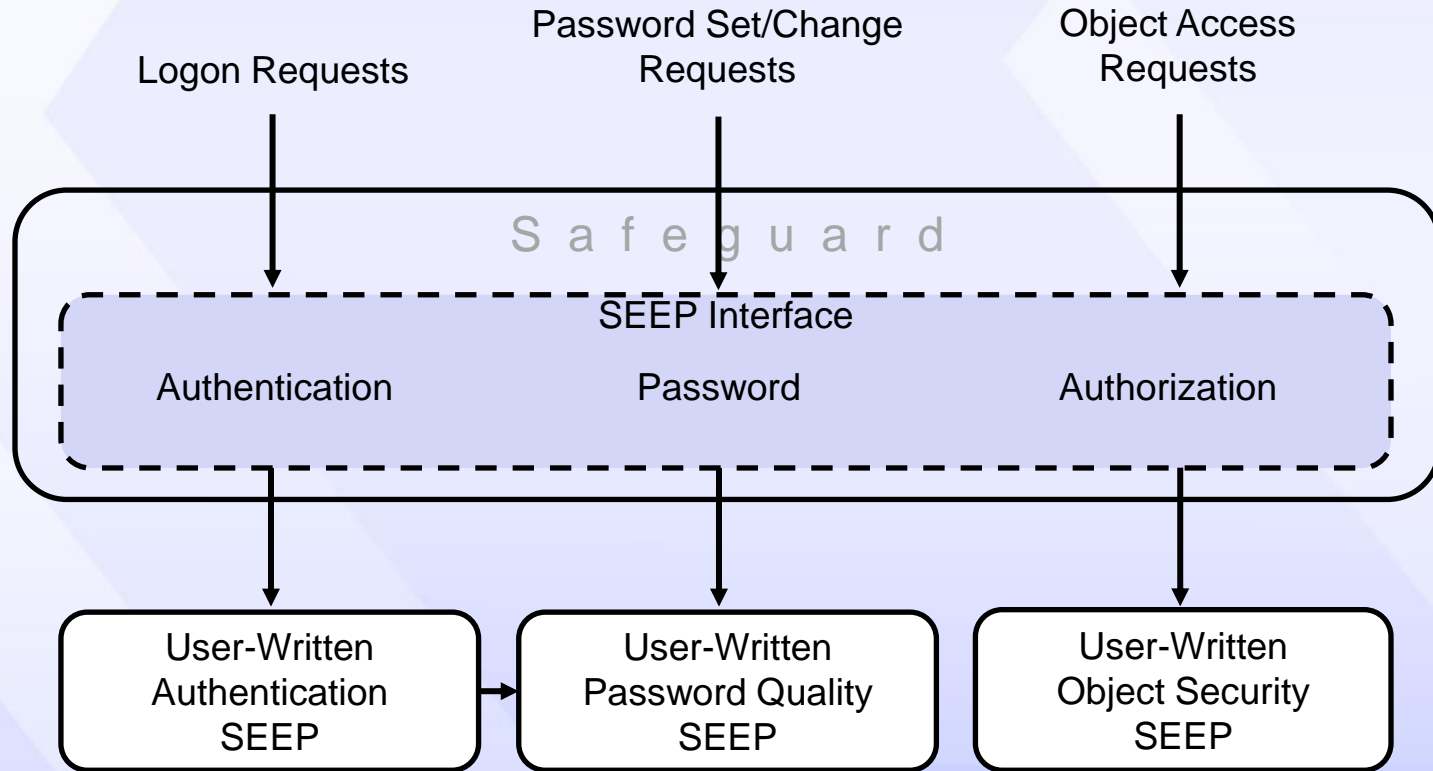
1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9. Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

Architecture

This illustration depicts the overall security event exit process (SEEP) architecture.

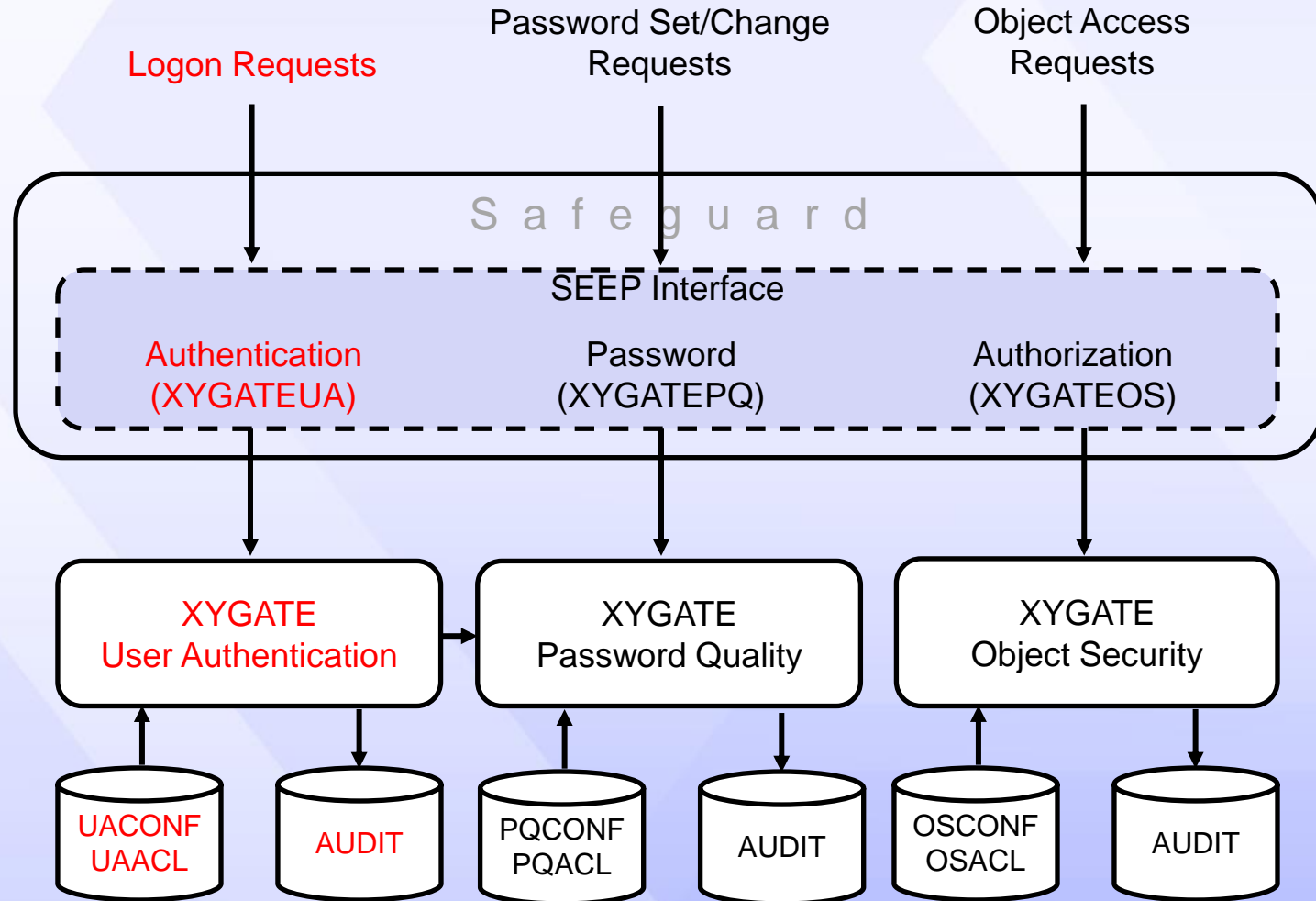




- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9. Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

Architecture

This illustration depicts the security event exit process (SEEP) architecture with emphasis on XYGATEUA.





How It Works

Before XYGATEUA can make user authentication rulings, Safeguard must be configured to send user authentication requests to XYGATEUA.

```
$VCLASS SUPER 4> safecom info event-exit-process xua
```

```
EVENT-EXIT-PROCESS XUA
```

```
ENABLED = ON  
RESPONSE-TIMEOUT = 60 SECONDS  
TIMEOUT-ALL-AUTHZREQ = OFF  
ENABLE-AUTHENTICATION-EVENT = ON  
ENABLE-AUTHORIZATION-EVENT = OFF  
ENABLE-PASSWORD-EVENT = OFF  
PROG = $SYSTEM.XYGATEUA.XYGATEUA  
LIB = * NONE *  
PNAME = $XUA  
SWAP = * NONE *  
CPU = ANY  
PRI = 198  
PARAM-TEXT = SERVER
```

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

How It Works

When enabled, the authentication SEEP (XYGATEUA) rules on the user authentication request and returns the ruling to the Safeguard subsystem for interpretation and enforcement.

Both interactive and programmatic logon authentication requests are sent to the XYGATEUA.

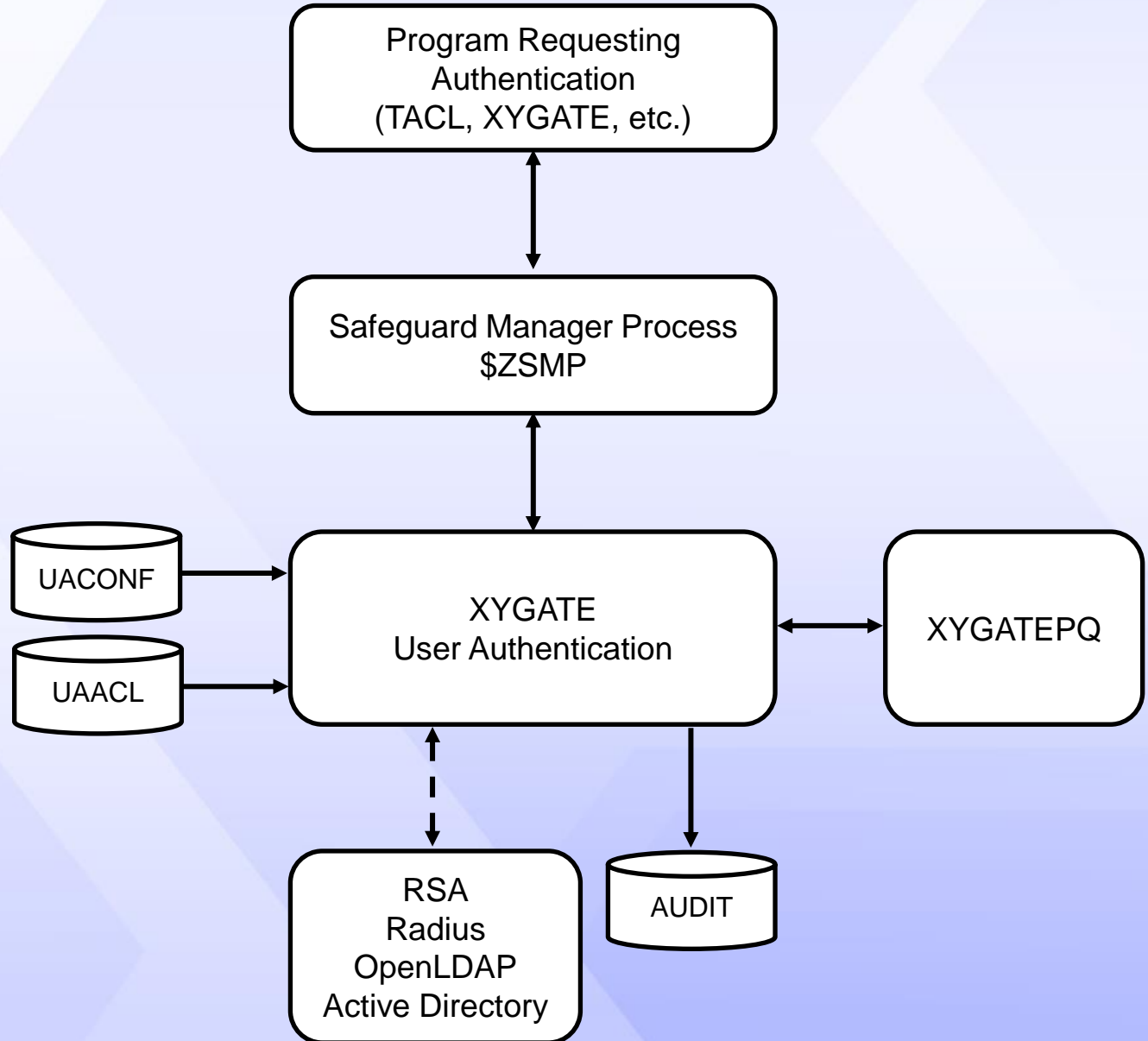
Unlike authorization events, the rulings on these events are the sole responsibility of XYGATEUA. The Safeguard software does not participate in authentication rulings.



- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9. Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

How It Works

This illustration depicts the XYGATEUA environment.





1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

How It Works

1. TACL requests user authentication.
2. The authentication request is sent to the Safeguard Manager Process (\$ZSMP).
3. Since the Authentication SEEP is enabled, the Safeguard Manager Process sends the authentication request to XYGATEUA.
4. XYGATEUA applies its authentication rules and makes an authentication ruling.

If the password is being changed during logon and the PQ_SEEP_OBJECT keyword is present in the UACONF, XYGATEUA sends the password change request to XYGATEPQ so XYGATEPQ's password quality rules can be applied to the new password. If the PQ_SEEP_OBJECT keyword is omitted from the UACONF, XYGATEUA changes the password and applies Safeguard's password quality rules (if any are set).

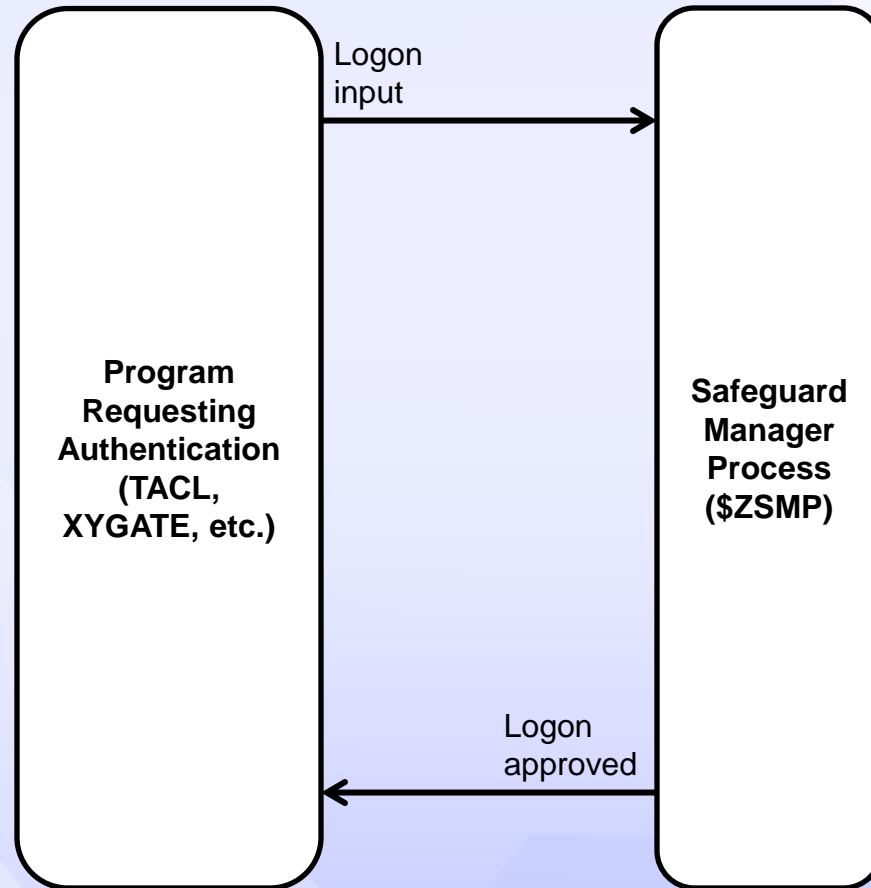
5. XYGATEUA responds to the Safeguard Manager Process with the authentication ruling.
6. The Safeguard Manager Process responds to TACL with the authentication ruling (approved or denied).



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

How It Works

Safeguard Approved Logon - Without XUA



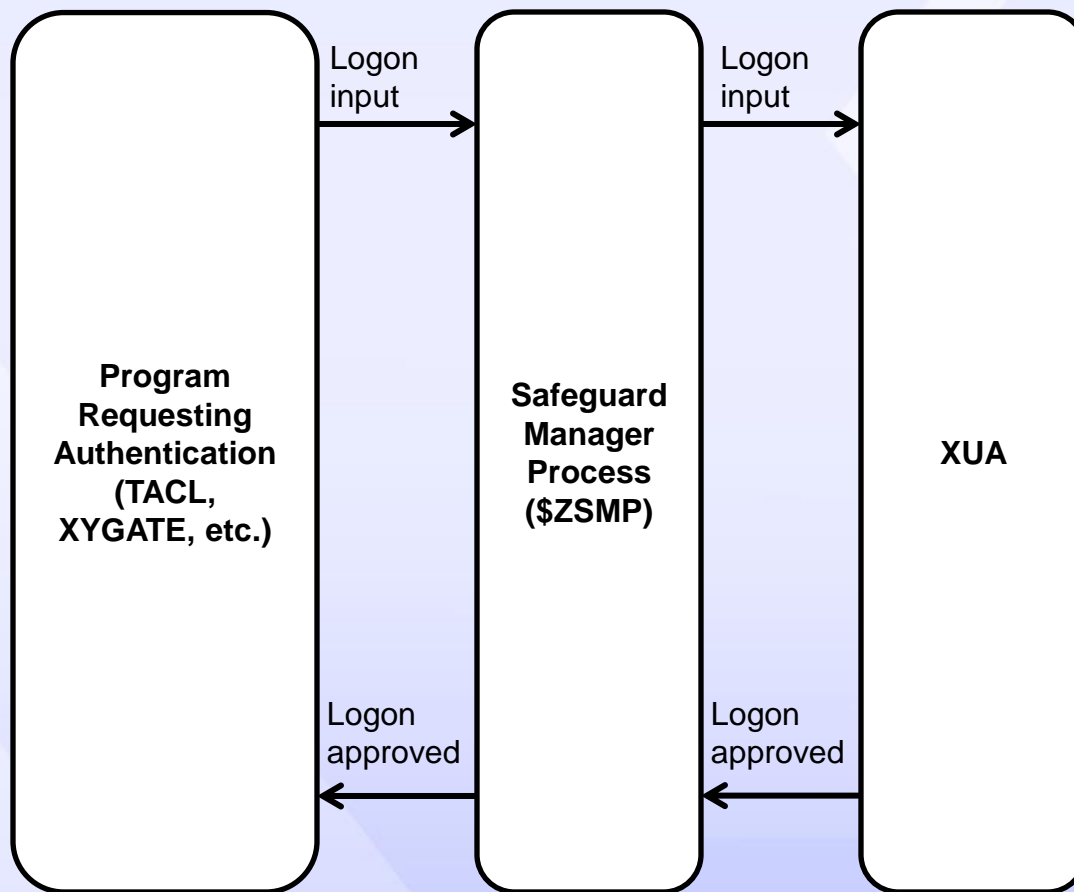
When **ENABLE-AUTHENTICATION-EVENT** is **OFF**, authentication requests are ruled on by Safeguard alone.



- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9. Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

How It Works

Safeguard Approved Logon - With XUA



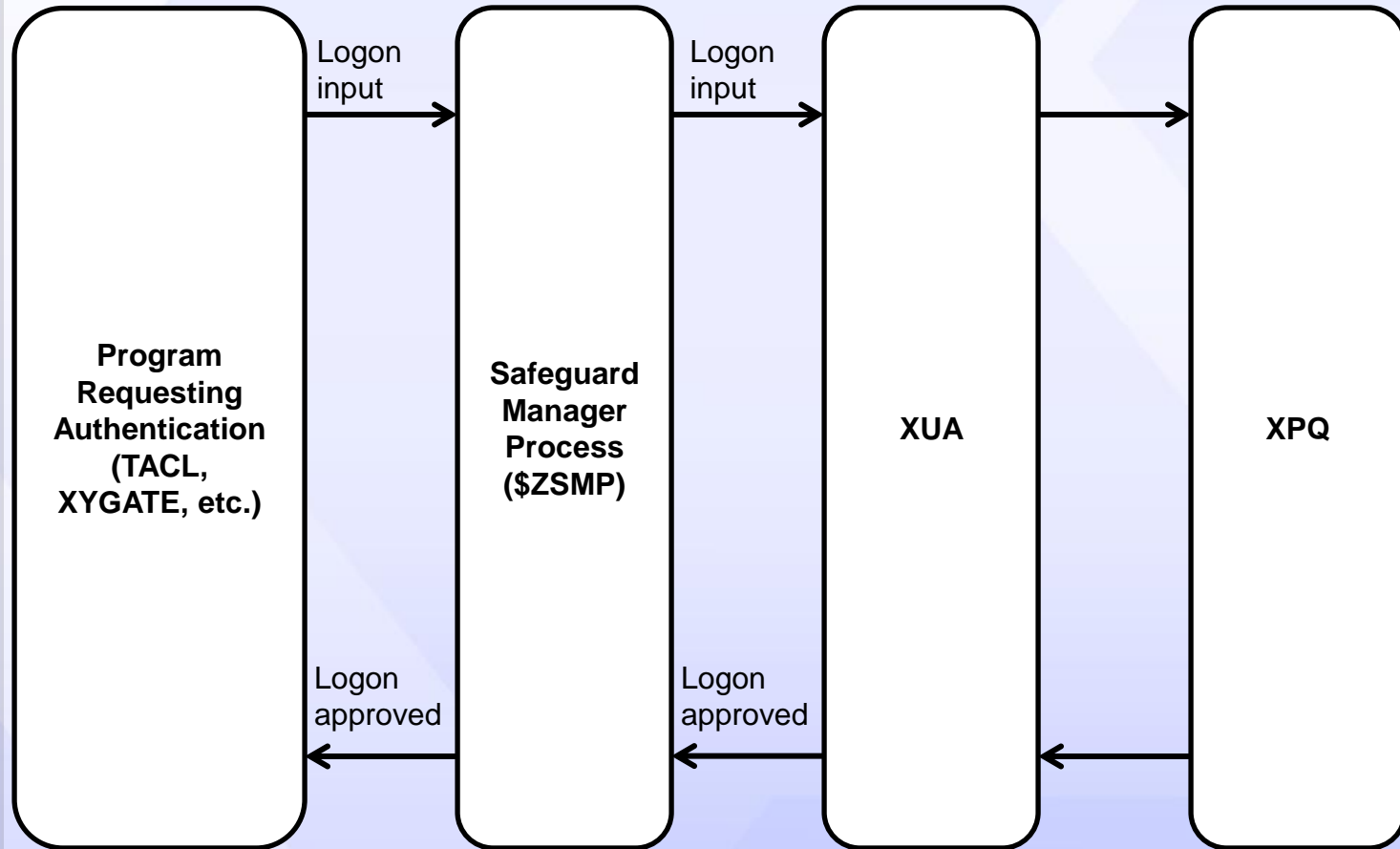
When **ENABLE-AUTHENTICATION-EVENT** is **ON**, Safeguard routes authentication requests to the event-exit process (e.g., XUA) and XUA rules on the authentication request.



How It Works

Safeguard Approved Logon and Password Change - With XUA

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9. Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary



When **ENABLE-AUTHENTICATION-EVENT** is **ON**, Safeguard routes authentication requests to the event-exit process (e.g., XUA) and XUA rules on the authentication request. If the password is changed during logon, XUA sends the password change request to XPQ.



Components

The main components of XYGATEUA include:

XYGATEUA – The Authentication SEEP that processes authentication requests from Safeguard.

UACONF – The file that defines the XYGATEUA global processing values.

UAACL – The file that defines the XYGATEUA ACL groups and the XYGATEUA rules.

Audit – The file to which XYGATEUA audit entries are made. Additional audit destinations can be configured.

Host Macros – Host macros are TACL macros that are used to perform various common XYGATEUA tasks on the NonStop server.

TACLSEG – A file accessible by TACL that contains the XUA TACL macro and other host macros.

P25F001 – The XYGATEUA license file.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Components

The main components of XYGATEUA include:

Audit Server – A copy of the XYGATEUA process that performs auditing. The original XYGATEUA process sends all generated audits to the audit server, reducing the main server's processing time. The audit server is given a system-generated process name and will be terminated whenever the main server goes away.

Refer to the documentation for a complete list of components.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Installation

There are three methods to install XYGATEUA.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

1. XYGATE Master Installer (XMI)

XMI provides helpful GUI controls to install multiple software modules in a single session. It automatically performs all the necessary system checks & validations, and pre- & post-install commands required to complete the installation process.

This method is recommended.

2. Host Install Macro

This method involves individually downloading XYGATE product BIN files from the XYPRO website and uploading them to your NonStop server. They then have to be unpacked and installed.



Installation

There are three methods to install XYGATEUA.

3. Automated Install Script

This method is used when you installing XYGATEUA from a CD or DVD. The AutoInstall script is designed for an easy installation of the XUA server pieces by providing default run-time parameters which can be changed later.

The next few slides show a manual XYGATEUA installation with the host install macro.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Installation

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

```
Which volume do you want XYGATEUA installed on <$VCLASS>?
Which subvolume do you want XYGATEUA installed on <XYGATEUA>?
What do you want to name the macro to run XYGATEUA <XUA>?xua
What do you want to name the CXUA HELP macro <CXUAHELP>?
What do you want to call the XYGATE audit file <AUDIT>?
What priority should XYGATEUA run at <198>?
What do you want the Home Terminal of XYGATEUA to be <$VHS>?
Do you want to audit successful accesses <No>?
Do you want to audit failed accesses <Yes>?
Does SUPER.SUPER pass all ACL checks <Y>?
Can Group Managers log down <Y>?
Peruse object <$SYSTEM.XYGATESP.PERUSE>?
Spool Collector <$S>
Company Name <XYPRO Support>?XYPRO Technology
```

```
XYGATEUA volume           : $VCLASS
XYGATEUA subvolume        : XYGATEUA
Security server name      : $XUA
Macro to run XYGATEUA     : XUA
Macro to get Command Help : XUAHELP
```

UACONF file contents :

```
MACRO_NAME           XUA
AUDIT                 $VCLASS.XYGATEUA.AUDIT
AUDIT_SERVER         OFF
PRIORITY             198
HOMETERM             $VHS
AUDIT_ACCESS_PASS    OFF
AUDIT_ACCESS_FAIL    ON
SUPERSUPEROK        ON
GROUPMANAGER_OK     ON
PHANDLE_MISMATCH_CHECK OFF
```



Installation

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

```
PERUSE_OBJECT          $SYSTEM.XYGATESP.PERUSE
COLLECTOR              $$
COMPANY_NAME           "XYPRO Technology"
PQ_SEEP_OBJECT         $SYSTEM.XYGATEPQ.XYGATEPQ $XPQ
AUTHENTICATE_FAIL_FREEZE  OFF
AUTHENTICATE_FAIL_STOP  OFF
FROZEN_OK              OFF
EXPLICIT_NODES         OFF
PASSWORD_REQUIRED      ON
!IGNORE_LEADING_SPACES  OFF
!SUBJECT_LOOKUP        OFF
!IPMAP                 SUBVOL $SYSTEM.XYGATEHE
!IMPERSONATION_CHARACTERS  "//"
!PASSWORD_EXPIRES_MESSAGE  OFF

!PASSWORD_MAY_CHANGE    0
!EMS_CRITICAL_IF_DENIED  OFF
!AUTHENTICATE_FAIL_TIMEOUT  60
!AUTHENTICATE_MAXIMUM_ATTEMPTS  3
!AUTHENTICATE_FREEZE_PERIOD  900
!AUTHENTICATE_FAIL_FREEZE_MSG  OFF

!MONITOR                $$.#XUA.MONITOR
!MONITORAUDIT           OFF
!MONITOR_AUDIT_SERVER   $$.#XUA.MONAUD
!MONITOR_ACCESS_CHECK   $$.#XUA.MONITORA
!EXPLAIN_LOG            $VCLASS.XYGATEUA.ZZEXP
```

```
Creating new UAACL file
Creating new HELP file
```

```
•
•
•
```



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

```
Creating new XUAUPDT file  
Creating new XUAEDIT file  
Creating new DDL Dictionary
```

```
Do you want the installation performed <Y>?
```

```
Doing install, please wait
```

```
Installing UALIB object file  
Installing XYGATEUA object file  
Installing UACONF file  
Installing UAACL file  
Installing UAACLSAM file  
Installing UAHELP file  
TEXT EDITOR - T9601H01 - (01MAY05)  
CURRENT FILE IS $VCLASS.XYGATEUA.UAHELP  
Installing UAACHLP file  
Installing LICENSE file  
Installing LICCHK object file  
Installing REGTEST object file  
Installing SEND object file  
Installing SERVICE object file  
Installing REPSAMP file  
Installing REPMAC file  
Installing XRMMETA file  
Installing XRMT0001 file  
Installing XRMT0002 file  
.  
.  
.
```



Installation

You may purge the following installation files if you wish.
(All files that start with the letter I)

IEMSBUIL	IEMSDDL	IEMSTEMP	IG2OSS	ILDAPINS	ILDAPPAS	ILDAPSRI	ILDAPSRV
ILDSRCH	ILDSRCHI	ILICCHK	ILOGDDL	INSLIB	INSMACS	INSRUN	INSTALL
IOSHCOLL	IOSSDIRC	IOSSFE	IP25F001	IPRNCONF	IPRNGDCN	IPRNGDN3	IPRNGDN4
IPRNGIN	IRADSRV	IRADSRVI	IREGTEST	IREPMAC	IREPSAMP	IRMT0001	IRMT0002
IRMT0003	IRMT0004	IRMT0005	IRND	IRSACHEC	IRSACLI	IRSAINIT	IRSAINST
IRSA LIST	IRSAOSS	IRSASRV	IRSASRVI	ISEND	ISERVICE	ISOFTDOC	ITACLSRC
ITASKACL	ITCPUPRO	ITEMPNAM	ITESTLDA	ITESTRAD	ITESTRSA	IUAACHLP	IUAACL
IUAACLSA	IUAHELP	IUALIBN3	IUALIBN4	IUAOBJN3	IUAOBJN4	IUAQDDL	IUAQFUP
IVER182	IWARNING	IXCFLANG	IXRMMETA	IXUA	IXUAEDIT	IXUAUPDT	IXYBIN

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary



Installation

At this point, all of the XYGATEUA files have been installed. The XUA_FINISH_INSTALL macro must be executed to finish the install, however.

You must logon as 255,255 and do the following commands to complete the installation:

```
RUN $VCLASS.XYGATEUA.XUA INSTALL
XUA_FINISH_INSTALL
```

NOTE: The file \$VCLASS.XYGATEUA.SOFTDOC contains the SOFTDOC file for XYGATEUA. Please, read it for information not contained in the Users Manual and information about known problems.

following command, You might want to put it in your \$SYSTEM.SYSTEM.TACLLOCL file

```
run $VCLASS.XYGATEUA.XUA INSTALL
```

```
$VCLASS.P25DSDST (30,255) 23>
```

Normally, logging on as 255,255 is required to complete the installation. Here, XYGATEAC was used to start a TACL owned by 255,255.

```
$VCLASS.P25DSDST (30,255) 23> xac tacl-255
```

```
XAC - \GUARD.CLASS.SUPER Password:
```

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary



Installation

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

XYGATEAC 5.70 XYPRO Support \GUARD 20991231 (see <<CONFIG for Copyright)

Loaded from \$VCLASS.XYGATEAC.LOADXOA:

OSH

```
(255,255)$VCLASS P25DSDST 1> RUN $vol.XYGATEUA.XUA INSTALL
```

```
(255,255)$VCLASS P25DSDST 2> XUA_FINISH_INSTALL
```

Licensing \$VCLASS.XYGATEUA.UALIB

PROGIDing \$VCLASS.XYGATEUA.XYGATEUA

```
(255,255)$VCLASS P25DSDST 3>
```

At this point, XYGATEUA host installation is complete.



Host Macros

Host macros are TACL macros that perform various common XYGATEUA tasks on the NonStop server. Some of these are:

- XUA
- XUA_AUDIT_REPORT
- XUA_DATE_TIME_MAKE
- XUA_EDIT_ACL
- XUA_FINISH_INSTALL
- XUA_INSTALL_LICENSE
- XUA_REPORT
- XUA_SYNTAX_CHECK
- XUA_VERSION
- XUA_VOLUME

Use the XUAHELP host macro to get the complete list of XYGATEUA host macros.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Host Macros

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

Before XYGATEUA host macros can be invoked, XYGATEUA's TACLSEG file must be attached to the TACL session. A TACL macro is supplied with XYGATEUA that performs this task.

Use the SEGINFO command to see that the TACLSEG file was attached.

```
$VCLASS.XYGATEUA (30,255) 24> run xygateua.xua install  
$VCLASS.XYGATEUA (30,255) 25> seginfo
```

Segment	File	Access	Pgs		Bytes		% UC	Directory
			Now	Max	Now	Max		
\$VCLASS.XYGATEPQ.TACLSEG		SH	70	1036	139696	2121728	6 1	:CXPQ_SEG.1

The name of the TACL macro that attaches the XUA_SEG TACL segment file may be different at your installation. Check the value of the MACRO_NAME parameter in the UACONF file for the correct TACL macro name.



This command should be placed in the security administrator's TACLCSTM file.



Host Macros

To view a full list of XYGATEUA host macros, enter XUAHELP at the TACL prompt.

```
$VCLASS.XYGATEUA (30,255) 25> xuahelp
```

```
XUA_AUDIT_REPORT           Allows a user to generate a report from an obey
                             file or TACL macro.
```

```
XUA_DISPLAY_RADLOG        Displays Radius proxy log contents.
```

```
XUA_DISPLAY_RSALOG        Displays RSA proxy log contents.
```

```
XUA_DISPLAY_LDAPLOG        Displays LDAP proxy log contents.
```

```
XUA_DATETIME_MAKE          Calculates a date in the past equal to the days
                             entered. This macro can be used to calculate
                             dates and establish date ranges to include in a
                             customized XYGATEUA report.
```

```
XUA_EDIT_ACL                Provides version control and non-realtime
                             editing of the UAACL file. It first creates a
                             copy of the file called NEWUAACL, which you can
                             edit as usual. When you finish, you will choose
                             whether or not to put the new changes into
                             effect by loading the new file. If you don't
                             want to load the file now, you can load it later
                             using the CXUA_UPDATE_ACL macro.
```

```
XUA_EXECUTE_LDAP_PROXY      Helps troubleshoot the XUA and LDAP server's
                             communication.
```

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

Host Macros

XUAHELP

XUA_EXECUTE_RADIUS_PROXY	Helps troubleshoot the XUA and RADIUS server's communication.
XUA_EXECUTE_RSA_PROXY	Helps troubleshoot the XUA and RSA server's communication.
XUA_EXPLAIN	Puts XYGATEUA Access into EXPLAIN mode, which generates information about its rulings on access requests including a list of the UAGroups that were considered
XUA_FINISH_INSTALL	Finishes the XYGATEUA installation. It must be executed as SUPER.SUPER. This macro licenses the UALIB file.
XUA_INSTALL_LICENSE	Does a license check on the file selected and asks yes/no to proceed. Renames the current license and installs the new license.
XUA_LDAP_INSTALL	Assists in configuring XUA interface to an LDAP server.
XUA_NETWORK_CHECK	Used for HP NonStop system configuration readiness for LDAP or RSA authentication.



- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

Host Macros

XUAHELP

XUA_RADIUS_INSTALL	Assists in configuring XUA interface to an RADIUS server.
XUA_REPORT	Used to generate XYGATEUA audit reports.
XUA_RSA_INSTALL	Assists in configuring XUA interface to an RSA server.
XUA_SAFECOM_BOUNCE	Disables and then enables XYGATEUA in Safeguard. You must be logged on as a member of the SECURITY-ADMINISTRATOR group or if not using the SECURITY-ADMINISTRATOR group as a member of the SUPER group to run this macro.
XUA_SAFECOM_DISABLE	Disables, but does not remove, XYGATEUA in Safeguard. You must be logged on as a member of the SECURITY-ADMINISTRATOR group or, if not in use, as a member of the SUPER group to run this macro.
XUA_SAFECOM_ENABLE	Enables a previously installed XYGATEUA in Safeguard. You must be logged on as a member of the SECURITY-ADMINISTRATOR group or, if not in use, as a member of the SUPER group to run this macro.



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

Host Macros

XUAHELP

XUA_SAFECOM_INSTALL

Installs XYGATEUA as a SEEP in Safeguard. This macro does not enable the software. CXUA_SAFECOM_ENABLE must be used to start XYGATEUA. You must be logged on as a member of the SECURITY-ADMINISTRATOR group or, if not in use, as a member of the SUPER group to run this macro.

XUA_SAFECOM_UNINSTALL

Removes XYGATEUA from Safeguard.

XUA_START

Enables a previously installed XYGATEUA in Safeguard. You must be logged on as a member of the SECURITY-ADMINISTRATOR group or, if not in use, as a member of the SUPER group to run this macro.

XUA_STATUS

Displays the status of the XYGATEUA server.

XUA_STOP

Disables, but does not remove, XYGATEUA in Safeguard. You must be logged on as a member of the SECURITY-ADMINISTRATOR group or, if not in use, as a member of the SUPER group to run this macro.

XUA_SYNTAX_CHECK

Reads the specified UAACL file to ensure that the entries are syntactically correct.



- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

Host Macros

XUAHELP

XUA_UPDATE_ACL

This macro will load a NEWUAACL file that was created earlier but not put into use. This macro does not give you an opportunity to view or change the contents of the file. If you want to make further changes before loading the file, you must use the CXUA_EDIT_ACL macro instead.

XUA_VERSION

Displays information about the XYGATEUA installation.

XUA_VOLUME

Changes the user's volume and subvolume to the volume and subvolume where XYGATEUA is installed.

XUAHELP

Displays this help message.

XUA_UNINSTALL

This macro will remove all files in your XYGATEUA installation. The uninstall macro must be run by the installation owner.



Host Macros

Here is an example of using the XUA_EDIT_ACL macro.

```
$VCLASS.XYGATEUA (30,255) 36> xua_edit_acl
```

This file edits the current XYGATE-USER-AUTHENTICATION list. It will create a file named \$VCLASS.XYGATEUA.NEWUAACL from the current \$VCLASS.XYGATEUA.UAACL file.

These are your old \$VCLASS.XYGATEUA.UAACL files:

```
No files match \GUARD.$VCLASS.XYGATEUA.OLDACL*
```

```
FILES DUPLICATED: 1  
TEXT EDITOR - T9601H01 - (01MAY05)  
CURRENT FILE IS $VCLASS.XYGATEUA.NEWUAACL  
*e
```

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



XUA_EDIT_ACL macro.

Checking for SYNTAX errors in the NEWUAACL

```
XYGATEUA 1.82 (c) 1999-2013 XYPRO Technology Corporation XYPRO  
Support \GUARD  
20991231  
LDAPPASS CHECKSUM 1013581070 ($VCLASS.XYGATEUA.LDAPPASS)  
UACONF CHECKSUM 794378584 ($VCLASS.XYGATEUA.UACONF)  
UAACL CHECKSUM 1835367705 ($VCLASS.XYGATEUA.NEWUAACL)  
No syntax errors found
```

```
Do you want to install the new ACL (Y/N) <N>?n
```

```
Do you wish to have the NEWUAACL file purged (Y/N) <N>?y
```

```
$VCLASS.XYGATEUA.NEWUAACL Purged
```

```
$VCLASS.XYGATEUA (30,255) 37>
```

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary



Host Macros

Here is an example of using the XUA_VERSION macro.

```
$VCLASS.XYGATEUA (30,255) 38> xua_version
```

```
This is version 1.82 of XYGATEUA
```

```
XYPRO license check XYPRO Support \GUARD 20991231  
XYPRO Support P25-0999 20991231 \EST1983(047) \GUARD(100)  
                                \X(007) \XYS7000(253)
```

```
--BEGIN XYPRO SIGNATURE
```

```
PUBLIC-KEY:
```

```
LICENSE-CREATE: 20130116-103720
```

```
CUSTOMER-NAME: XYPRO Support
```

```
CUSTOMER-NUMBER: 0999
```

```
PRODUCT: XYGATE-UA 20991231 20130115
```

```
  NODE: \EST1983 0047 77247 00/0 *           00
```

```
  NODE: \GUARD 0100 77248 00/0 *           00
```

```
  NODE: \X 0007 58060 00/0 *             00
```

```
  NODE: \XYS7000 0253 43421 00/0 *           00
```

```
License good
```

```
.  
. .  
. .
```

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Host Macros

XUA_VERSION macro.

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

VPROC - T9617H01 - (01 FEB 2009) SYSTEM \GUARD Date 10 JUL
2013, 12:55:50
Copyright 2004 Hewlett-Packard Development Company, L.P.

```
$VCLASS.XYGATEUA.XYGATEUA
    Binder timestamp: 29MAY2013 08:26:22
    Version procedure: T9999D30^P25^XUA^182
    Version procedure: T9999D30_P16_ESDKLIB_332
    Version procedure: T1325V01_03JUL2013
    Version procedure: T8432H04_04JAN2013_CCPLMAIN
    Version procedure: T9999D30_P16_XEL_510
    TNS/E Native Mode: runnable file
.
.
.
```



XUA_VERSION macro.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

```
EVENT-EXIT-PROCESS XUA

ENABLED = ON
RESPONSE-TIMEOUT = 60 SECONDS
TIMEOUT-ALL-AUTHZREQ = OFF
ENABLE-AUTHENTICATION-EVENT = ON
ENABLE-AUTHORIZATION-EVENT = OFF
ENABLE-PASSWORD-EVENT = OFF
PROG = $SYSTEM.XYGATEUA.XYGATEUA
LIB = * NONE *
PNAME = $XUA
SWAP = * NONE *
CPU = ANY
PRI = 198
PARAM-TEXT = SERVER
```



Host Macros

Here is an example of using the XUA_INSTALL_LICENSE

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

```
$VCLASS.XYGATEUA (30,255) 39> xua_install_license p99f001
XYPRO license check XYPRO Support \GUARD 20991231
XYPRO Support P25-0999 20991231 \EST1983(047)
\GUARD(100) \X(007) \XYS7000(253)
--BEGIN XYPRO SIGNATURE
PUBLIC-KEY:
LICENSE-CREATE: 20130116-103720
CUSTOMER-NAME: XYPRO Support
CUSTOMER-NUMBER: 0999
PRODUCT: XYGATE-UA 20991231 20130115
  NODE: \EST1983 0047 77247 00/0 * 00
  NODE: \GUARD 0100 77248 00/0 * 00
  NODE: \X 0007 58060 00/0 * 00
  NODE: \XYS7000 0253 43421 00/0 * 00
License good

Do you want to install this license file <YES>?

FILES DUPLICATED: 1
New license installed, old license in $VCLASS.XYGATEUA.XUA49454
$VCLASS.XYGATEUA (30,255) 40>
```



UACONF File

The UACONF (User Authentication Configuration) file on the NonStop server configures the default processing characteristics of the XYGATEUA software. Some can also be set on individual XYGATEUA UAGROUPS

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

```
MACRO_NAME          XUA
AUDIT                $VCLASS.XYGATEUA.AUDIT
AUDIT_SERVER        OFF
PRIORITY            198
HOMETERM            $VHS
AUDIT_ACCESS_PASS   OFF
AUDIT_ACCESS_FAIL   ON
SUPERSUPEROK        ON
GROUPMANAGER_OK     ON
PHANDLE_MISMATCH_CHECK OFF
PERUSE_OBJECT        $SYSTEM.XYGATESP.PERUSE
COLLECTOR            $$
COMPANY_NAME         "XYPRO Technology"
PQ_SEEP_OBJECT       $SYSTEM.XYGATEPQ.XYGATEPQ $XPQ
AUTHENTICATE_FAIL_FREEZE OFF
AUTHENTICATE_FAIL_STOP OFF
FROZEN_OK            OFF
EXPLICIT_NODES       OFF
PASSWORD_REQUIRED    ON
```



UACONF

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

```
!IGNORE_LEADING_SPACES      OFF
!SUBJECT_LOOKUP              OFF
!IPMAP                        SUBVOL $SYSTEM.XYGATEHE
                              "//"
!IMPERSONATION_CHARACTERS    " //"
!PASSWORD_EXPIRES_MESSAGE    OFF
!PASSWORD_MAY_CHANGE         0
!EMS_CRITICAL_IF_DENIED      OFF
!AUTHENTICATE_FAIL_TIMEOUT   60
!AUTHENTICATE_MAXIMUM_ATTEMPTS 3
!AUTHENTICATE_FREEZE_PERIOD  900
!AUTHENTICATE_FAIL_FREEZE_MSG OFF

!MONITOR                      $$.#XUA.MONITOR
!MONITORAUDIT                  OFF
!MONITOR_AUDIT_SERVER          $$.#XUA.MONAUD
!MONITOR_ACCESS_CHECK          $$.#XUA.MONITORA
!EXPLAIN_LOG                    $VCLASS.XYGATEUA.ZZEXP
```




UACONF File

Some important UACONF keywords include:

Keyword	Meaning
AUDIT	Controls the type and location of the XUA audit trails.
AUDIT_SERVER	When this keyword is set to ON, it causes the XYGATEUA object file to start a copy of itself to use as an audit server. The original server sends all generated audits to the audit server, reducing the main server's processing time. The audit server will be given a system-generated process name, and will be terminated whenever the main server goes away.
SUPERSUPEROK	If SUPERSUPEROK is set to ON, then SUPER.SUPER is capable of logging on to any userid or Safeguard alias in the group. If SUPERSUPEROK is OFF, SUPER.SUPER will be evaluated as any other userid. SUPER.SUPER can be explicitly denied access in any UAGROUP for a particular set of users if desired. The defaults value is OFF.
MACRO_NAME	Specifies the name of the TACL macro that is used to attach the XYGATEUA TACLSEG file.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



UACONF File

Some important UACONF keywords include:

Keyword	Meaning
IMPERSONATION _CHARACTERS	Allows logon by impersonation and sets the two impersonation characters. The default impersonation characters are //.
PASSWORD_REQ UIRED	Controls whether or not a userid logging on is required to provide a password. This keyword can be used in the UAACL.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



UAACL File

The UAACL (User Authentication Access Control List) file consists of three main types of configuration components:

1. ACLGROUPs (optional)
2. TIMEGROUPs (optional)
3. UAGROUPs

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



UAACL File

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UAACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

ACLGROUPs assist in grouping like users into more manageable user-sets to facilitate easier security administration. ACLGROUPS can be used as arguments to the MEMBERS, FROM_USER, TO_USER, and IMPERSONATION_FROM_USER keywords. ACLGROUPs are optional.

Syntax:

```
ACLGROUP $<user-defined-name> <aclgroup> <userid-list>
```

Example Usage:

```
ACLGROUP $EVERYONE \*.*.* ALIAS:"\*.*"
```

```
ACLGROUP $GRPMGR *,255
```

```
ACLGROUP $SUPER 255,255 30,255 100,255
```

```
ACLGROUP $SECURITY 255,255 30,255 NETUNDERLYING:30,255
```

ACLGROUP definitions can also contain previously defined ACLGROUPs. For example:

```
ACLGROUP $GRPMGR *,255
```

```
ACLGROUP $SUPER 255,255 $GRPMGR
```



UAACL File

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

TIMEGROUPs define a set of users that are allowed to logon only during a specific time. TIMEGROUPs are optional. The TIME keyword specifies the allowed logon day(s) and logon time range.

Syntax:

```
TIMEGROUP $<user-defined-name>  
    MEMBERS <aclgroup> <userid-list>  
    TIME { <day(s) of the week> | <military time range>
```

Example:

```
ACLGROUP $students 30,* NOT 30,255
```

```
TIMEGROUP $xygate-class-8am-5pm  
    MEMBERS $students  
    TIME MON-FRI 08:00-17:00
```

After authenticating the userid and password, XYGATEUA checks for a TIMEGROUP that includes the userid being logged-on to. If found, the TIMEGROUP rule is applied.

Alternatively, the TIME keyword can be used in UAGROUPs.



UAACL File

The UAGROUP entity defines the logon rules to be applied to various sets of users.

Syntax:

```
UAGROUP <user-defined-name>  
    FROM_USER <aclgroup> <userid-list>  
    TO_USER <aclgroup> <userid-list>
```

Example:

```
ACLGROUP $EVERYONE *.* ALIAS:"*"
```

```
UAGROUP STANDARD-LOGON  
    DESCRIPTION "Allows everyone to logon as themselves"  
    !Selection Criteria:  
    FROM_USER $EVERYONE  
    TO_USER $EVERYONE
```

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



UAGROUPs have three parts:

1. UAGROUP Name
2. Selection Criteria
3. Control Keywords

XYGATEUA reads the UAACL from the top to bottom. UAGROUPs are processed in the order in which they are encountered in the UAACL file.

Once XYGATEUA finds an entry that matches all of the selection criteria for the current logon request, XYGATEUA makes a ruling and stops searching.

The most specific UAGROUPs should be before the least specific UAGROUPs.

If XYGATEUA doesn't find an entry that matches all of the selection criteria, authentication is performed using the credentials provided.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



UAACL File

The following keywords are required in a UAGROUP.

Keyword	Meaning
UAGROUP <name>	<name> is 31 alphanumeric characters and may include "\$", "-", ".", and "_".
FROM_USER <aclgroup> <user list>	The selection criteria matches when the userid who is trying to logon matches a userid in the aclgroup and/or user list.
TO_USER <aclgroup> <user list>	The selection criteria matches when the userid being logged on to matches a userid in the aclgroup and/or user list.

A UAGROUP may have additional selection criteria and control keywords.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



UAACL File

Additional selection criteria keywords may be included to further control logon. These are:

Keyword	Meaning
ANCESTOR	The selection criteria matches when the specified ANCESTOR object is the same as the ancestor of the requestor to which the user is logging on. ANCESTOR can be specified using a wild-carded object file name.
PORT	The selection criteria matches when the specified PORT is the same as the logging on user's terminal and incoming IP address.
REQUESTOR	The selection criteria matches when the specified REQUESTOR object is the same as requester to which the user is logging on. REQUESTOR can be specified using a wild-carded object file name.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



UAACL File

Control keywords may be included to further control authentication. Some of these are:

Keyword	Meaning
FROZEN_OK	Controls whether or not a userid logging on can logon to to a frozen userid.
IMPERSONATION	Controls whether or not a userid can logon as a another user (e.g., super.super) with the user's own password.
IMPERSONATION_FROM_USER	Specifies the userid(s) who may impersonate.
OMIT_PASSWORD_USERS	Specifies the userid(s) who do not have to supply a password while logging on.
PASSWORD_REQUIRED	Controls whether or not a userid logging on is required to provide a password. If this keyword is omitted, the value in the UACONF file is used.
RESULT_DENIED	Denies logon even with the correct password.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



UAACL File

Control keywords may be included to further control authentication. Some of these are:

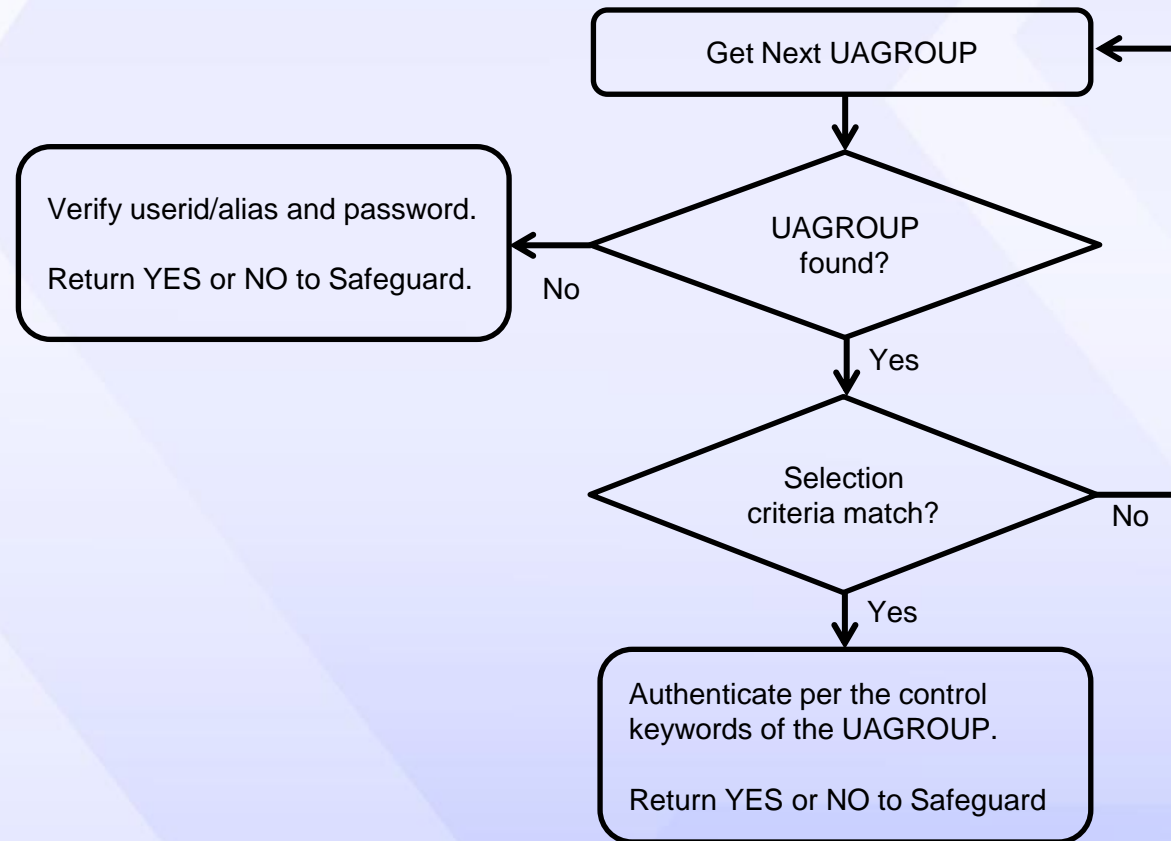
- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

Keyword	Meaning
SUPERSUPEROK	Controls whether SUPER.SUPER is capable of logging on to any user id or Safeguard alias in the group. If set to OFF, SUPER.SUPER will be evaluated as any other userid.
GROUPMANAGER_OK	Controls whether or not a group manager (group,255) is capable of logging on to any user id or Safeguard alias in the group. If set to OFF, the group manager will be evaluated as any other user id.



UAACL File

A user authentication request is processed by XYGATEUA as follows:



If a matching UAGROUP cannot be found, authentication is performed by validating the userid/alias and password. If no matching UAGROUPS are found, a UAGROUP called INTERNAL-FINAL-GROUP-XYZ is assigned and YES or NO is returned.



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

UAACL File

A user authentication request is processed by XYGATEUA as follows:

1. Check for the next UAGROUP.
2. If a UAGROUP isn't found or there are no more UAGROUPs, XYGATEUA authenticates using the userid/alias and password provided and exits UAACL processing. YES or NO is returned to Safeguard.
3. If a UAGROUP is found, the selection criteria are checked.
4. If the selection criteria are satisfied, XYGATEUA authenticates per the control keywords of the UAGROUP. YES or NO is returned to Safeguard.

XYGATEUA repeats this process until a UAGROUP whose selection criteria are met is found or the end of the UAACL is reached without finding a matching UAGROUP.

Step 4 has many possibilities that affect the outcome of the authentication request.



There are limits to the number of ACL groups and object groups that can be defined in the UAACL. To determine the limits and current counts, run the XYGATEUA program with the STATS parameter. For example:

```
(030,255)$VCLASS.XYGATEUA (30,255) 13> run xygateua stats
XYGATEUA 1.82 (c) 1999-2013 XYPRO Technology Corporation XYPRO Support
\GUARD
20991231
LDAPPASS CHECKSUM 1013581070 ($VCLASS.XYGATEUA.LDAPPASS)
UACONF CHECKSUM 794378584 ($VCLASS.XYGATEUA.UACONF)
UAACL CHECKSUM 1631659097 ($VCLASS.XYGATEUA.UAACL)
No syntax errors found
```

Table	Current	Limit	Entry-size	Space-used	Mem-used/Available
ACL Groups	6	100	38	228	
ACL IDs	21	20000	54	1134	
Ports	0	1000	116	0	
Maps	0	3002	208	0	0 / 10001000
Requestors	0	1000	100	0	
Ancestors	0	1000	100	0	
UA Groups	4	1000	944	3776	
Time Groups	1	100	110	110	
Times	5	500	6	30	
Phandles	0	2000	82	0	
LDAPPASS	0	20	310	0	
Audits	1	9	288	288	

```
(030,255)$VCLASS.XYGATEUA (30,255) 14>
```

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary



UAACL File

Example 1 – Everyone can logon as themselves.

```
ACLGROUP $EVERYONE *.* ALIAS:"*"
```

```
UAGROUP ANYTHING-GOES
```

```
DESCRIPTION "Everyone can logon as themselves"
```

```
!Selection Criteria:
```

```
FROM_USER $EVERYONE
```

```
TO_USER $EVERYONE
```

```
RESULT_GRANTED
```

Explanation:

1. The \$EVERYONE ACLGROUP contains all userids and all aliases.
2. The ANYTHING-GOES UAGROUP has selection criteria that are satisfied when the subject userid/alias is any userid/alias and the target user is any userid/alias. If the provided userid/alias and password are correct, the logon is approved. It is not necessary to include RESULT_GRANTED. It is good practice, however.



This is the most general rule. If used, it should be the last rule in the UAACL file.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Example 2 – Special auditing for SUPER group.

```
ACLGROUP $EVERYONE *.* ALIAS:"*"
ACLGROUP $SUPER 255,* UNDERLYING:255,*
```

```
UAGROUP NO-AUDIT-SUPER-TO-EVERYONE-LOGON
DESCRIPTION "Don't audit $SUPER logon as $EVERYONE"
FROM_USER $SUPER
TO_USER $EVERYONE NOT 253,1
AUDIT_ACCESS_PASS OFF
AUDIT_ACCESS_FAIL OFF
```

Explanation:

1. The \$EVERYONE ACLGROUP contains all userids and all aliases. The \$SUPER group contains and super group members.
2. The No-AUDIT-SUPER-TO-EVERYONE-LOGON UAGROUP has selection criteria that are satisfied when the subject userid is 255,* and the target userid/alias is any userid/alias other than 253,1. Logon is allowed without auditing.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Example 3 – Logon without a password.

```
ACLGROUP $EVERYONE *.* ALIAS:"*"
```

```
UAGROUP SUPER-LOGON-NO-PASSWORD
```

```
DESCRIPTION "SUPER can logon as any userid w/o a pw"
```

```
!Selection Criteria:
```

```
FROM_USER 255,255
```

```
TO_USER $EVERYONE NOT 253,1
```

```
PASSWORD_REQUIRED OFF
```

Explanation:

1. The \$EVERYONE ACLGROUP contains all userids and all aliases.
2. The SUPER-LOGON-NO-PASSWORD UAGROUP has selection criteria that are satisfied when the subject userid is 255,255 and the target userid/alias is any userid/alias other than 253,1. Logon is allowed without a password.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Example 4 – Controlling logon based on time.

```
ACLGROUP $EVERYONE *.* ALIAS:"*"  
ACLGROUP $STUDENTS 30.* NOT 30,255
```

```
TIMEGROUP $XYGATE-CLASS  
MEMBERS $STUDENTS  
TIME MON-FRI 08:00-17:00
```

```
UAGROUP ANYTHING-GOES  
DESCRIPTION "Everyone can logon as themselves"  
!Selection Criteria:  
FROM_USER $EVERYONE  
TO_USER $EVERYONE
```

Explanation:

1. The \$XYGATE-CLASS TIMEGROUP has members of the \$STUDENTS ACLGROUP. If the target userid/alias is a userid that is a member of the timegroup, logon is denied outside the hours of 8:00 to 17:00.
2. The ANYTHING-GOES UAGROUP is processed the same as in Example 1 except that XYGATEUA always checks for a timegroup that contains the target userid/alias.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Example 5 – Controlling logon based on time.

```
ACLGROUP $EVERYONE *.* ALIAS:"*"  
ACLGROUP $STUDENTS 30.* NOT 30,255
```

```
UAGROUP STUDENTS-8-5
```

```
DESCRIPTION "Students can logon Mon-FRI 8 to 5"  
!Selection Criteria:  
FROM_USER $EVERYONE  
TO_USER $STUDENTS  
TIME MON-FRI 08:00-17:00
```

Explanation:

1. The \$EVERYONE ACLGROUP contains all userids and all aliases. The \$STUDENTS ACLGROUP contains userids 30,* except 30,255.
2. The UAGROUP named STUDENTS-8-5 has selection criteria that are satisfied when the subject userid/alias is any userid/alias and the target user is a student userid. If the provided userid and password are correct and the logon time is within the times specified, the logon is allowed.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Example 6 – Impersonating a userid.

```
ACLGROUP $EVERYONE *.* ALIAS:"*"
```

```
ACLGROUP $PRO 37,* ALIAS:"PRO.*"
```

```
UAGROUP PRO-CAN-IMPERSONATE-CLASS-SUPER
```

```
DESCRIPTION "PRO userids can impersonate CLASS.SUPER"
```

```
!Selection Criteria:
```

```
FROM_USER $PRO
```

```
TO_USER CLASS.SUPER
```

```
IMPERSONATION_FROM_USER $PRO
```

```
IMPERSONATION OPTIONAL
```

Explanation:

1. The \$EVERYONE ACLGROUP contains all userids and all aliases. The \$PRO ACLGROUP contains userids 37,*.
2. The PRO-CAN-IMPERSONATE-CLASS-SUPER UAGROUP has selection criteria that are satisfied when the subject user is any userid/alias and the target userid is \$CLASS.SUPER. Impersonation is optionally allowed to members of the \$PRO ACLGROUP only. If the userid/alias specified in the password field does not match the IMPERSONATION_FROM_USER list, XYGATEUA will continue to search for the UAGROUP that matches.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Example 7 – Temporarily freezing userids

```
ACLGROUP $EVERYONE *.* ALIAS:"*"
```

```
UAGROUP ANYTHING-GOES
```

```
FROM_USER $EVERYONE
```

```
TO_USER $EVERYONE
```

```
AUTHENTICATE_MAXIMUM_ATTEMPTS 3
```

```
AUTHENTICATE_FAIL_FREEZE ON
```

```
AUTHENTICATE_FREEZE_PERIOD 120 !Seconds
```

Explanation:

1. The \$EVERYONE ACLGROUP contains all userids and all aliases.
2. The ANYTHING-GOES UAGROUP has selection criteria that are satisfied when the subject userid/alias is any userid/alias and the target user is any userid/alias. If the provided userid/alias and password are correct, the logon is allowed.
3. If the provided userid/alias and password are incorrect, the logon is denied. If this happens three times in succession, XYGATEUA freezes the target userid for a period of 2 minutes.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Example 8 – Controlling logon based on port.

```
UAGROUP NO-LOGON-TO-SUPER-FROM-0-0
DESCRIPTION "SUPER cannot logon from 0,0 on any PORT"
!Selection Criteria:
FROM_USER 0,0
TO_USER SUPER.SUPER
PORT $*.*#* +*
!Result
RESULT_DENIED
```

Explanation:

1. The NO-LOGON-TO-SUPER-FROM-0-0 UAGROUP has selection criteria that are satisfied when the subject userid is 0,0, target userid is SUPER.SUPER, and port is any terminal & IP address starting with a number.
2. RESULT_DENIED is required to explicitly deny the logon attempt when the selection criteria are met.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

Example 9 – Use node-conditional keywords to cause UAACL entries to apply to a specific node only.

```
#IF @NODE = "\GUARD"  
  UAGROUP NO-LOGON-TO-SUPER-FROM-0-0  
    DESCRIPTION "Must logon as yourself before SUPER"  
    !Selection Criteria:  
    FROM_USER 0,0  
    TO_USER SUPER.SUPER  
    RESULT_DENIED  
#ENDIF
```

Explanation:

1. The NO-LOGON-TO-SUPER-FROM-0-0 UAGROUP applies only to the \GUARD node.

The #IF @NODE keyword can include the =, <>, LIKE, and NOTLIKE conditional operators. LIKE and NOTLIKE require regular expression style wildcarding (e.g., #IF @NODE LIKE "\X.*").

Use the node-conditional keywords to create a "master" UAACL file that can be duplicated across NonStop servers, but provides specific UAACL processing for any given NonStop server. Node conditional operators can be used anywhere in the UAACL.



Example 10 – Controlling logon based on requestor.

```
UAGROUP XYGATE-ACCESS-CONTROL
DESCRIPTION "XAC can logon as anyone"
FROM_USER $EVERYONE
TO_USER $EVERYONE
REQUESTOR $SYSTEM.XYGATEAC.XYGATEAC
SAFEGUARD_PRIVLOGON ON
DIALOG_MODE OFF
PASSWORD_REQUIRED OFF
```

Explanation:

1. The XYGATE-ACCESS-CONTROL UAGROUP has selection criteria that are satisfied when the subject userid/alias is any userid/alias, the target user is any userid/alias, and requestor is XYGATEAC.
2. The SAFEGUARD_PRIVLOGON keyword allows a program to set a special flag when calling USER_AUTHENTICATE_. If the program also has a Safeguard diskfile ACL that has the PRIV-LOGON flag set, then logons are allowed without a password regardless of the Safeguard PASSWORD-REQUIRED setting.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Example 11 – RSA authentication.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

UAGROUP RSA-AUTHENTICATE

```
FROM_USER $EVERYONE  
TO_USER PRO.*
```

```
RSA_AUTHENTICATE ON  
RSA_REQUIRE_PASSWORD OFF
```

!Strips GROUP name and replaces USER name with RSA
!ID. Replaces alias with RSA ID.

```
MAP RE:"^.*\." DELETE  
MAP RE:"DAVID" REPLACE "david"  
MAP RE:"ROB" REPLACE "rob"  
MAP RE:"PRO_DAVID" REPLACE "david" EXIT  
MAP RE:"PRO_ROB" REPLACE "rob" EXIT  
MAP RE:"^.*$" APPEND "@xypro.com" EXIT
```

Explanation:

1. The RSA-AUTHENTICATE UAGROUP has selection criteria that are satisfied when the subject userid/alias is any userid/alias and the target user is any PRO.*
2. The RSA_AUTHENTICATE keyword causes XYGATEUA to send the userid and password to the RSA authentication server. The MAP keywords replace the user name or alias with the RSA ID.



Example 12 – LDAP authentication.

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9. Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

UAGROUP LDAP-AUTHENTICATE

```
FROM_USER $EVERYONE
```

```
TO_USER PRO.*
```

```
LDAP_AUTHENTICATE ON
```

```
!Strips GROUP name and replaces USER name with LDAP  
!network ID. Replaces alias with LDAP network ID.
```

```
MAP RE:"^.*\." DELETE
```

```
MAP RE:"DAVID" REPLACE "N3442041" EXIT
```

```
MAP RE:"ROB" REPLACE "N3442063" EXIT
```

```
MAP RE:"PRO_DAVID" REPLACE "N3442041" EXIT
```

```
MAP RE:"PRO_ROB" REPLACE "N3442063" EXIT
```

Explanation:

1. The LDAP-AUTHENTICATE UAGROUP has selection criteria that are satisfied when the subject userid/alias is any userid/alias and the target user is any PRO.*
2. The LDAP_AUTHENTICATE keyword causes XYGATEUA to send the userid and password to the LDAP authentication server. The MAP keywords replace the user name or alias with the LDAP network ID.



Example 13 – SUPER.SUPER undeniable for a particular UAGROUP.

```
ACLGROUP $EVERYONE *.* ALIAS:"*"
```

```
UAGROUP SUPER-SUPER  
DESCRIPTION "SUPER.SUPER Undeniable"  
!Selection Criteria:  
FROM_USER SUPER.SUPER  
TO_USER $EVERYONE  
SUPERSUPEROK ON
```

Explanation:

1. The \$EVERYONE ACLGROUP contains all userids and all aliases.
2. The SUPER-SUPER UAGROUP has selection criteria that are satisfied when the subject userid is SUPER.SUPER and the target userid/alias is any userid/alias.
3. SUPERSUPEROK ON allows SUPER.SUPER to logon to any userid or Safeguard alias in the group. SUPERSUPEROK OFF means the SUPER.SUPER userid is treated like any other userid and must adhere to the access rules as defined in the UAACL.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Example 14 – Group managers can logon to group members.

UAGROUP GROUP-MANAGERS

DESCRIPTION "Group Managers Can Logon To Group Mmbrs"

!Selection Criteria:

FROM_USER *,255

TO_USER GROUP,* UNDERLYING:GROUP,*

GROUPMANAGER_OK ON

Explanation:

1. The GROUP-MANAGERS UAGROUP has selection criteria that are satisfied when the subject userid is any group manager (*,255) userid and the target userid/alias is any userid/alias in the same group as the group manager.
2. GROUPMANAGER_OK ON allows a group manager to logon to any userid or Safeguard alias in the same group as the logged-on group manager. GROUPMANAGER OFF means group manager userids are treated like any other userid and must adhere to the access rules as defined in the UAACL.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

“What-If” Testing

Unlike XOS, **XUA does not run in warning mode**. The initial configuration must be tested before the software is enabled as the authentication SEEP in Safeguard.

XYGATEUA rules can be tested:

1. before enabling it as the Authentication SEEP.

This is harmless since XYGATEUA is not participating in the object access request.

2. after enabling it as the Authentication SEEP.

If XYGATEUA is enabled as the Authentication SEEP, it participates in the object access request.



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

“What-If” Testing

XYGATEUA can be asked to rule on a “what-if” object access request.

What-If testing allows user authentication to be tested without XYGATEUA making a ruling to Safeguard.

What-If testing can be performed before and after enabling XYGATEUA as the Authentication SEEP.

The idea being what if <userid> attempted to logon as <userid>?

Examples:

- What if user 0,0 attempted to logon as SUPER.SUPER?
- What if user class.user1 attempted to logon before 8:00 am or after 5:00 pm?
- What if user PRO.DAVID attempted to impersonate CLASS.SUPER by logging on to CLASS.SUPER using with the PRO.DAVID password?



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

“What-If” Testing

XYGATEUA performs interactive “what-if” testing when in “access” and “explain” modes.

When run in access mode, XUA issues one of two results, YES or NO, and the UAGROUP that was used.

When in explain mode, a list of the UAGROUPs that were considered is displayed as well.

Access mode can be entered by running the XYGATEUA program from TACL with the ACCESS parameter.

Explain mode can be entered three ways by:

1. running the XYGATEUA program from TACL with the EXPLAIN option.
2. running the XUA_EXPLAIN host macro.
3. entering EXPLAIN ON while in ACCESS mode.



“What-If” Testing

Running XYGATEUA in access mode:

```
$VCLASS.XYGATEUA (30,255) 15> run xygateua access
XYGATEUA 1.82 (c) 1999-2013 XYPRO Technology Corporation XYPRO
SALES DEMO ENVIRONMENT \GUARD 20140630
LDAPPASS CHECKSUM 1013581070 ($VCLASS.XYGATEUA.LDAPPASS)
UACONF CHECKSUM 1046104162 ($VCLASS.XYGATEUA.UACONF)
UAACL CHECKSUM 74722652 ($VCLASS.XYGATEUA.UAACL)
```

```
Access check: exit
```

```
$VCLASS.XYGATEUA (30,255) 16>
```

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



“What-If” Testing

Running XYGATEUA in explain mode:

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. “What-If” Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

```
$VCLASS.XYGATEUA (30,255) 16> run xygateua explain
XYGATEUA 1.82 (c) 1999-2013 XYPRO Technology Corporation XYPRO
SALES DEMO ENVIRONMENT \GUARD 20140630
LDAPPASS CHECKSUM 1013581070 ($VCLASS.XYGATEUA.LDAPPASS)
UACONF CHECKSUM 1046104162 ($VCLASS.XYGATEUA.UACONF)
UAACL CHECKSUM 74722652 ($VCLASS.XYGATEUA.UAACL)
Explain mode on
```

```
Safeguard Password May Change : 10 days before
                                expiration
Safeguard Password History      : 0
Safeguard Minimum Password Length : 2
Safeguard Maximum Password Length : 64
Safeguard Password Spaces Allowed : Off
Safeguard Password Required     : Off
Safeguard Authenticate Maximum Attempts : 3
Safeguard Authenticate Fail Timeout : 60 seconds
Safeguard Authenticate Fail Freeze : Off
Safeguard Namelogon             : On
Safeguard Blindlogon            : On
Safeguard Password Expiry Grace : 15 days
```

```
Access check: exit
$VCLASS.XYGATEUA (30,255) 17>
```



“What-If” Testing

Running the XUA_EXPLAIN host macro:

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. “What-If” Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

```
$VCLASS.XYGATEUA (30,255) 14> xua_explain
XYGATEUA 1.82 (c) 1999-2013 XYPRO Technology Corporation XYPRO
SALES DEMO ENVIRONMENT \GUARD 20140630
LDAPPASS CHECKSUM 1013581070 ($VCLASS.XYGATEUA.LDAPPASS)
UACONF CHECKSUM 1046104162 ($VCLASS.XYGATEUA.UACONF)
UAACL CHECKSUM 74722652 ($VCLASS.XYGATEUA.UAACL)
Explain mode on
```

```
Safeguard Password May Change : 10 days before
                                expiration
Safeguard Password History      : 0
Safeguard Minimum Password Length : 2
Safeguard Maximum Password Length : 64
Safeguard Password Spaces Allowed : Off
Safeguard Password Required     : Off
Safeguard Authenticate Maximum Attempts : 3
Safeguard Authenticate Fail Timeout : 60 seconds
Safeguard Authenticate Fail Freeze : Off
Safeguard Namelogon             : On
Safeguard Blindlogon            : On
Safeguard Password Expiry Grace : 15 days
```

Access check:



“What-If” Testing

Running the XUA_EXPLAIN host macro:

Access check: `help`

Valid commands are one of:

ABORT <dialogid> Aborts the logon session specified by <dialogid>. (Only valid in server mode).

AUDIT {on|off|test} Toggles auditing or does an audit test

COMMENT
== Can be used to insert comments
Alternate method of doing comments, leading
==

EXIT Exits from program.

·
·
·

Access check: `exit`

`$VCLASS.XYGATEUA (30,255) 15>`

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



“What-If” Testing

Example 1:

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

```
$VCLASS.XYGATEUA (30,255) 18> run xygateua access
XYGATEUA 1.82 (c) 1999-2013 XYPRO Technology Corporation XYPRO
SALES DEMO ENVIRONMENT \GUARD 20140630
LDAPPASS CHECKSUM 1013581070 ($VCLASS.XYGATEUA.LDAPPASS)
UACONF CHECKSUM 1046104162 ($VCLASS.XYGATEUA.UACONF)
UAACL CHECKSUM 74722652 ($VCLASS.XYGATEUA.UAACL)
```

```
Access check: logon class.super * 0,0
SEEP msg: Password:
SEEP return 00000,00070,00004
SEEP dialog ID 1 (dialog will continue)
ECHO would be turned off
Response? <to-user-pw>
SEEP return 00000,00000,00000
Access result - YES using GROUP DEFAULT
```

```
Access check: explain on
```

Explain mode can be entered from access mode by entering the EXPLAIN ON command.



“What-If” Testing

Example 2:

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9. Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. “What-If” Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

```
$VCLASS.XYGATEUA (30,255) 19> run xygateua explain
XYGATEUA 1.82 (c) 1999-2013 XYPRO Technology Corporation XYPRO
SALES DEMO ENVIRONMENT \GUARD 20140630
LDAPPASS CHECKSUM 1013581070 ($VCLASS.XYGATEUA.LDAPPASS)
UACONF CHECKSUM 1046104162 ($VCLASS.XYGATEUA.UACONF)
UAACL CHECKSUM 74722652 ($VCLASS.XYGATEUA.UAACL)
Explain mode on
```

```
Safeguard Password May Change : 10 days before
                                expiration
Safeguard Password History      : 0
Safeguard Minimum Password Length : 2
Safeguard Maximum Password Length : 64
Safeguard Password Spaces Allowed : Off
Safeguard Password Required     : Off
Safeguard Authenticate Maximum Attempts : 3
Safeguard Authenticate Fail Timeout : 60 seconds
Safeguard Authenticate Fail Freeze : Off
Safeguard Namelogon             : On
Safeguard Blindlogon            : On
Safeguard Password Expiry Grace : 15 days
```

Access check:



“What-If” Testing

Example 2:

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

```
Access check: logon class.super * 0,0
User          : CLASS.SUPER (030,255) on 2013-09-16
               13:19:26.755945
User Expires  : * None *
Password Expires : 2013-09-29 00:00:00.000000
Password May Change : 2013-09-19 00:00:00.000000 (change not
               allowed)
Password Must Change : Every 180 days
Password Expiry Grace : 30 days (grace time left)
Last Logon      : 2013-09-16 12:13:41.969340
Last Unsuccessful Lgn : 2013-09-16 06:58:45.417425
Fail count      : * None *
Static fail count : 69
Frozen/Thawed   : Thawed
Last Modification Time: 2013-09-16 12:13:41.964991
From User      : 000,000 NULL.NULL
Requestor      : $NONE $NONE.NONE.NONE
Ancestor       : $NONE $NONE.NONE.NONE
To User        : 030,255 CLASS.SUPER
Port           : $NONE $NONE.NONE.NONE
Dialog ID      : 001 Tag=0 Dialog=On
.
.
.
```



“What-If” Testing

Example 2:

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. “What-If” Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

```
State      : 01 Initial
Options    : 0000000000000001
           Option 15: Logon
UAGROUP PRO-CAN-IMPERSONATE-CLASS-SUPER Target in TO_USER list
UAGROUP PRO-CAN-IMPERSONATE-CLASS-SUPER Subject in FROM_USER
list
UAGROUP PRO-CAN-IMPERSONATE-CLASS-SUPER Selection criteria
satisfied
UAGROUP PRO-CAN-IMPERSONATE-CLASS-SUPER Description: PRO
userid's can impersonate CLASS.SUPER
subproc check_for_impersonation:begin
Impersonation chars not in password field
UAGROUP PRO-CAN-IMPERSONATE-CLASS-SUPER
AUTHENTICATE_MAXIMUM_ATTEMPTS 0
UAGROUP PRO-CAN-IMPERSONATE-CLASS-SUPER
AUTHENTICATE_FAIL_FREEZE OFF
UAGROUP PRO-CAN-IMPERSONATE-CLASS-SUPER AUTHENTICATE_FAIL_STOP
OFF
Password required on - acl password_required
Process state 01
Begin State_Initial
Setting dialog state to 00002 Need first password
.
.
.
```



“What-If” Testing

Example 2:

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. “What-If” Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

```
Assigning error,status,outcome of 00070,00004,00001
Setting msg: Password:
UAGROUP PRO-CAN-IMPERSONATE-CLASS-SUPER Replying with access
CONTINUE
UAGROUP PRO-CAN-IMPERSONATE-CLASS-SUPER Outcome is NEED-FIRST
SEEP msg: Password:
SEEP return 00000,00070,00004
SEEP dialog ID 1 (dialog will continue)
ECHO would be turned off
Response? <to-user-pw>
User                : CLASS.SUPER (030,255) on 2013-09-16
                    : 13:19:32.261030
User Expires        : * None *
Password Expires    : 2013-09-29 00:00:00.000000
Password May Change : 2013-09-19 00:00:00.000000 (change not
                    : allowed)
Password Must Change : Every 180 days
Password Expiry Grace : 30 days (grace time left)
Last Logon          : 2013-09-16 12:13:41.969340
Last Unsuccessful Lgn : 2013-09-16 06:58:45.417425
Fail count          : * None *
Static fail count   : 69
Frozen/Thawed      : Thawed
.
.
.
```




“What-If” Testing

Example 2:

Last Modification Time: 2013-09-16 12:13:41.964991

UAGROUP DEFAULT Replying with access YES

UAGROUP DEFAULT Outcome is LOGON

SEEP return 00000,00000,00000

Access result - YES using GROUP DEFAULT

Access check:

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

Auditing

XYGATEUA can be configured with up to nine audit locations of the following types:

1. Disk files
2. Processes
3. IP addresses

Audit locations are configured in the UACONF file.

The default configuration includes disk file auditing only.



Auditing

Here is an example of disk file audit configuration:

```
AUDIT                               $VCLASS.XYGATEUA.AUDIT
```

where:

AUDIT is the auditing keyword that enables disk file auditing.

\$VCLASS.XYGATEUA.AUDIT is the name of the audit disk file.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Audit Reports

Audit reports can be obtained in four ways:

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

1. XYGATE Report Manager (XRM) GUI

- a. PC-based querying and reporting (available only with the Audit PRO product installed).
- b. Host-based reporting using the RM TACL macro.

2. XUA_REPORT Host Macro

- a. XUA_REPORT is host macro that provides a menu to the user for report criteria selection and run options.

3. REPMAC TACL Macro

- a. REPMAC is a TACL macro that can be modified for the required report criteria. It can be run from a TACL prompt or scheduled to run using a utility such as NetBatch. REPMAC runs the XUA_DATETIME_MAKE and XUA_AUDIT_REPORT host macros.

4. RM TACL Macro

- a. Same as 1b above except without the GUI.



Auditing

XYGATEUA audit records include such data as:

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

- 1. System
- 2. Date & Time
- 3. From User
- 4. SessionIP
- 5. Target Group
- 6. Target User
- 7. Result
- 8. Operation
- 9. Object Type
- 10. Others

To User/	SbjSystem	DateTime	From User	SessionIP	Terminal	IgtG	IgtU	Result
To User: CLASS.SUPER	F\GUARD	2013-09-16:14:57:18.27	NULL.NULL	10.1.1.179	\GUARD.\$X7Q2.#IN	030	255	UAGROUP PR

Displayed with XYGATE Event Monitor (XEM)



Audit Reports

XYGATE Report Manager (XRM) GUI: Report Criteria

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

The screenshot shows the 'All Activity' report configuration window in the XYGATE Report Manager. The window has a title bar with 'All Activity' and standard window controls. Below the title bar are three tabs: 'Report Criteria' (selected), 'Layout', and 'View Reports'. The main area is divided into two sections: 'Report Attributes' and 'Data Selection Criteria'.

Report Attributes (\GUARD.\$VCLASS.XYGATEOS.XRMD0001)

Title: All Activity

From: Today (dropdown), 2013-03-25 (calendar), 00:00 (time)

To: Today (dropdown), 2013-03-25 (calendar), 23:59 (time)

Audit Pool: <DEFAULT-AUDIT> (dropdown) Spooler: <DEFAULT-LOCATION> (dropdown)

Buttons: Run, Save, Save As, Delete, Run with Dehun (checkbox)

Data Selection Criteria

Name	Expression
Subject UserId	*.*
Subject Login Name	* ...
Subject System	*
Subject Terminal	*
Object Group	* ...
Object Name	* ...
Result	ALL
Production/Test	BOTH
Warning	BOTH
Comment	*
Suppress Comment	NO
Operation	*



Audit Reports

XYGATE Report Manager (XRM) GUI: Layout

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

The screenshot shows the 'All Activity' window in the XYGATE Report Manager (XRM) GUI. The window has three tabs: 'Report Criteria', 'Layout', and 'View Reports'. The 'Layout' tab is active. The interface is divided into several sections:

- Layout Options:** Contains two radio buttons: 'Predefined Layout:' (unselected) and 'Custom Layout' (selected). To the right are three buttons: 'Run', 'Save', and 'Save As'.
- Custom Report Columns:** This section is split into two columns:
 - Available Columns:** A list of columns including Comment, Elapsed Seconds, Modifier, Object Type, Process Descriptor, Request Type, Requestor Name, Requestor Object, Subject Group Number, Subject System, Subject User Number, Test, and Warning Mode. Below this list are four buttons: '- >>', 'Add ->', '<- Remove', and '<< -'.
 - Selected Columns:** A list of columns including Date, Time, Subject Login Name, Operation, Result, Object Name, <Line-Break>, Object Group, and Terminal. To the right of this list are four buttons: 'Move Up', 'Move Down', 'Line Break', and 'Space'.
- Sorting:** Contains three dropdown menus. The first is labeled 'Sort by:' and has 'Date' selected. The other two are labeled 'Then by:'.
- Page Size:** Contains three radio buttons: 'Portrait' (selected), 'Landscape', and 'Custom'. To the right are two spinners: 'Width: 80 Characters' and 'Height: 60 Lines'.



Audit Reports

XYGATE Report Manager (XRM) GUI: View Reports

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

Report Criteria | Layout | View Reports

Spooler Job Filter

Node: \GUARD Product: Object Security

Owner: Both Report Definition: All Activity

List Jobs

Spooler Job List

Drag a column header here to group by that column

System	Supervisor	Job	Date	Time	State	Hold	Location	Pages	Copies
\GUARD	\$SPLS	510	2013-03-22	13:47:27	READY		#XRMXOS.XRMD0001	2	1

Open Save As Delete Refresh



Audit Reports

The report can be retrieved (from the NonStop spooler) and viewed using the XRM GUI.

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

XYPRO Technology \GUARD All Activity
 Date produced: 22-MAR-2013 13:47 Page: 1
 Criteria:2013-03-22 00:00 to 2013-03-22 23:59 File:\$VCLASS.XYGATEOS.AUDIT

YYYY-MM-DD/ HH:MM:SS	Login Name/ Object Group	Operation	R	Object Name/ Terminal
2013-03-22 13:39:22	SUPER.SUPER EXCEPTIONS-TO-CURRENT-SYSNN		312 S	\$SYSTEM.SYSTEM.USERID \$X4K1.#IN
2013-03-22 13:39:22	CLASS.SUPER EXCEPTIONS-TO-CURRENT-SYSNN		312 F	\$SYSTEM.SYSTEM.USERID \$X4K1.#IN
2013-03-22 13:41:45	SUPER.SUPER EXCEPTIONS-TO-CURRENT-SYSNN		312 S	\$SYSTEM.SYSTEM.USERID \$X4K1.#IN
.				
.				
.				



Audit Reports

The report can also be viewed using the PERUSE spooler utility.

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

```
$VCLASS XYGATEOS 30> peruse
PERUSE - T9101H02 - (18OCT2012)      SYSTEM  \GUARD
(C)Copyright 2012 Hewlett-PackardDevelopment Company, L.P.
```

```
      JOB  BATCH STATE PAGES COPIES PRI HOLD LOCATION          REPORT
      510  123  READY  2      1      4      #XRMXOS XRMD0001 CLASS    SUPER
```

XYPRO Technology \GUARD All Activity

Date produced: 22-MAR-2013 13:47

Page: 1

Criteria:2013-03-22 00:00 to 2013-03-22 23:59 File:\$VCLASS.XYGATEOS.AUDIT

YYYY-MM-DD/

HH:MM:SS	Login Name/ Object Group	Operation	R	Object Name/ Terminal
2013-03-22 13:39:22	SUPER.SUPER EXCEPTIONS-TO-CURRENT-SYSNN	312 S		\$SYSTEM.SYSTEM.USERID \$X4K1.#IN
2013-03-22 13:39:22	CLASS.SUPER EXCEPTIONS-TO-CURRENT-SYSNN	312 F		\$SYSTEM.SYSTEM.USERID \$X4K1.#IN
2013-03-22 13:41:45	SUPER.SUPER EXCEPTIONS-TO-CURRENT-SYSNN	312 S		\$SYSTEM.SYSTEM.USERID \$X4K1.#IN
_exit				



XUA_REPORT Host Macro:

- 1. How This Course Is Organized
- 2. Who Should Take This Course
- 3. Course Objectives
- 4. Overview
- 5. Architecture
- 6. How It Works
- 7. Components
- 8. Installation
- 9 Host Macros
- 10. UACONF File
- 11. UAACL File
- 12. "What-If" Testing
- 13. Auditing
- 14. Audit Reports
- 15. Exercises
- 16. Q & A
- 17. Glossary

```
$VCLASS XYGATEOS 33> xos_report
```

Choose an option:

```
A:  Audit File                :$VCLASS.XYGATEOS.AUDIT
B:  Report date range         :2013-03-25 00:00 to 2013-03-25 23:59
C:  Subject userid            :*. *
D:  Subject Login name        :*
E:  Subject System            :*
F:  Subject Terminal          :*
G:  OS Group                  :*
H:  Object Name               :*
I:  Result (All,S,F,N)        :ALL
J:  Production/Test results   :Both
K:  Warning/Non-warning results:Both
L:  Comment contains          :*
M:  Suppress comments         :No
N:  Output file               :$S.#XYGATE.OBJSEC
O:  Sort order                :OBJECT
P:  Operation                 :*
Q:  User specified title      :*
X:  Exit the report macro
Z:  Run the audit report
ZP: Run the audit report and go into PERUSE and return here
    Hit Break or Control-Y to terminate
```



XUA_REPORT Host Macro:

Selection?zp

FILE NAME	LEVEL READ	RECORDS READ	POSITIONS
\$VCLASS.XYGATEOS.AUDIT	1	15	1
100,01,00606 BEGIN(03/25/13 - 11:54:05:48) END(03/25/13 - 11:54:05:93)			
STRATEGY COST = 2			

** END-OF-ENFORM-RUN **

XYGATESP 3.16 (c) 1994-2013 XYPRO XYPRO Support \GUARD 20991231

Job	Batch	State	Pages	Copies	Pri	Hold	Location	Report
579		Ready	2	1	4		#XYGATE OBJSEC	CLASS SUPER

—

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Exercises

Exercise 1 – Attaching the XYGATEUA TACLSEG to TACL

Steps:

1. Logon to the HP NonStop server using your *class.user#* user ID and *pasusr#* password where # is the number assigned to you.
2. Run your XUA TACL macro with the INSTALL parameter.

```
TACL> run $vcl##.xygateua.xua install
```

3. Verify your TACLSEG is attached to TACL. If attached, you will see your TACLSEG file listed.

```
$VCLASS.SUPER (30,255) 3> seginfo
```

Segment File	Access	Now	Max	Bytes	Bytes	%	UC	Directory
\$VCLASS.XYGATEUA.TACLSEG	SH	126	1036	243332	2121728	11	1	:XUA_SEG.1

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Exercises

Exercise 2 – XUAHELP Host Macro

Steps:

1. Logon to the HP NonStop server using your *class.user#* user ID and *pasusr#* password where # is the number assigned to you.
2. Enter your XUA instance name with the HELP parameter.

```
TACL> xua#help
```

3. Familiarize yourself with the output.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Exercise 3 – XUA_VERSION Host Macro

Steps:

1. Logon to the HP NonStop server using your *class.user#* user ID and *pasusr#* password where # is the number assigned to you.

2. Enter your XUA version macro name.

```
TACL> xua#_version
```

3. Familiarize yourself with the output.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Exercises

Exercise 4 – Viewing the UACONF and UAACL Files

Steps:

1. Using the XYGATE Configuration File Manager (XCF) GUI, open and view your UACONF and UAACL files.
2. Familiarize yourself with the contents.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Exercise 5 – UAACL

Steps:

1. Access the XYGATE Configuration (XCF) GUI.
2. Open your UAACL file.
3. Add the following ACLGROUP:

```
ACLGROUP $STUDENT 30, #
```

where # is the number assigned to you.

4. Add a TIMEGROUP

```
TIMEGROUP $logon-8am-5pm  
MEMBERS $STUDENT  
TIME MON-FRI 08:00-17:00
```

5. Check the syntax and apply changes.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Exercises

Exercise 5 – “What-If” Testing in Access mode

Steps:

1. Logon to the HP NonStop server using your *class.user#* user ID and *pasusr#* password where # is the number assigned to you.
2. Run your XYGATEUA in access mode and give the following commands:
 - a. `logon class.user# * 0,0`
 - b. `exit`
3. What was the result of “a” above?

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Exercise 6 – “What-If” Testing in Explain mode

Steps:

1. Logon to the HP NonStop server using your *class.user#* user ID and *pasusr#* password where # is the number assigned to you.
2. Run your XYGATEUA in explain mode and give the following commands:
 - a. `logon class.user# * 0,0`
 - b. `exit`
3. What was the result of “a” above?

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. “What-If” Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Exercise 8 – Audit Reporting Using XRM

Steps:

1. Access the XYGATE Report Manager (XRM) GUI.
2. Right click on Audit PRO Reports and select Add a New Report Definition. Scroll down and select XUA – All Activity.
3. Configure the report to run for today's audit entries only.
4. Run the report.
5. View the report.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



Exercises

Exercise 9 – Audit Reporting Using the XUA_REPORT Host Macro

Steps:

1. Logon to the HP NonStop server using your *class.user#* user ID and *pasusr#* password where # is the number assigned to you.
2. Run your XUA#_REPORT host macro.
3. Configure the report to run for today's audit entries only.
4. Run the report.
5. View the report.

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
- 9 Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

Q & A

1. Does XYGATEUA require a separate user database?

No. All XYGATE modules use standard Guardian userids and Safeguard aliases.

2. Does the order of commands in the UAACL matter?

Yes. UAGROUPs are processed in the order in which they are encountered. UAGROUPs selected most often should be placed before UAGROUPs selected least often.

3. Is there a rule of thumb for creating UAGROUPs?

Yes. Always put the most specific UAGROUPs before the least specific.

4. What is the maximum length of an UAGROUP name?

Up to 32 characters are allowed.



Q & A

1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

5. What characters are allowed in an XYGATEUA UAGROUP name?

Allowed characters include alphanumeric characters, dash, underscore, period, and dollar sign.

6. Does XYPRO provide sample XYGATEUA UAGROUPs?

Yes. The XYGATEUA documentation contains sample UAGROUPs.



1. How This Course Is Organized
2. Who Should Take This Course
3. Course Objectives
4. Overview
5. Architecture
6. How It Works
7. Components
8. Installation
9. Host Macros
10. UACONF File
11. UAACL File
12. "What-If" Testing
13. Auditing
14. Audit Reports
15. Exercises
16. Q & A
17. Glossary

Glossary

Open LDAP – Open LDAP software is a free, open source implementation of the Lightweight Directory Access Protocol (LDAP). With LDAP, users' passwords are maintained only within the LDAP database and can be used for NonStop authentication via XYGATEUA.