ICL Pathway	Group Definitions for the Secure NT Build Release 2	Ref:RS/REQ/012 Version:3.0 Date:21/10/98

Document Title: Group Definitions for the Secure NT Build

Document Type: Requirement Definition

Abstract: The ACP requires that access to Pathway systems be controlled by the use of pre defined roles to which users can be assigned. Such roles will allow users to access only those parts of the system, with associated objects, they need in order to complete the tasks associated with that particular role. This document summarises this requirement and defines the roles, with associated objects, domains and access requirements.

Status: Approved

Distribution   Barry Procter, Mark Ascott, Chris Sundt, Joe Brown, Ian Morrison, John Allen, Belinda Fairthorne, Gerry Boyce, Mik Peach, Graham Chatten, Stephen Doyle, Alan Ward, Chris Humphries, Library

Author: Alan D'Alvarez

0. Document control

0.1 Document history

Version	Date	Reason
0.1	2/9/98	Initial draft with limited circulation for comment.
0.2	3/9/98	Incorporates comments from Chris Sundt and Barry Procter
1.0	8/9/98	Baselined version
1.1	9/9/98	CP1523 - MIS component breakdown
2.0	18/9/98	Baseline with amended set of tools for support roles
2.1	8/10/98	CP 1583 - Incorporates changes identified as a result of test and meetings
2.2	9/10/98	Incorporates changes identified as a result of document review
3.0	21/10/98	Approved for NR2 MOT build

0.2 Approval authorities

Name	Position	Signature	Date
Stephen Doyle	Design Manager		

Associated documents

	Reference	Vers	Date	Title
ACP	RS/POL/0003	2.0	24/2/98	Access Control Policy
SFS	RS/FSP/0001	3.0	3/12/97	Security Functional Specification

0.3 Abbreviations and definitions

Local   Access via the console attached directly to an NT platform

0.4 Changes in this version

[Changes since V2.1] Use of Exceed for the SSC. Amendments to ICL Outsourcing roles including creation of additional users and revisions to toolsets. Additional tools for Pathway FRM Manager. Change of name for FCMS user to Pathway FRM User. Ad hoc changes identified after review of previous version. Revisions to Authentication/Resource Domain access.

ICL Pathway **Group Definitions for the Secure NT Build Release 2**

Ref:RS/REQ/012
Version:3.0
Date:21/10/98

0.5 Changes Forecast

Identify further tools for the SSC to replace the use of the POSIX subsystem for the filtering of Riposte scans.

ICL Pathway   **Group Definitions for the Secure NT Build**   Ref:RS/REQ/012
                    Release 2   Version:3.0
                                                                           Date:21/10/98

0.6 Table of content

Appendices
    A. Table of roles and associated access requirements

1. Introduction

The nature of the Pathway system requires that access to the core systems should be strictly controlled. [ACP] states that effective control depends on having a clear definition of the roles and responsibilities of all personnel who need some form of access to the system. Users will gain access by being assigned to these roles. This will be core to Pathway implementing the principles of least privilege.

This document summarises the requirement and defines the human roles that will be implemented for NT platforms; which objects will be used by each role; the domains each role will function within; access point for the role; and associated privileges.

2. Scope

This document addresses the roles to be implemented as part of the Pathway central NT systems and access rights assigned to each role.

3. Requirements

The requirement to implement a role based access control system emanates from [ACP]. [ACP] further defines the roles that are required for access to the Pathway Systems and the responsibilities of these roles.

It should be noted that the Pathway solution has moved on since Version 2 of the ACP was issued and, as such, the Groups defined at Appendix A do not always correlate with the roles defined in [ACP]. This will be addressed by feeding these role definitions into the current review of the ACP which will be subject to a CP once all necessary changes have been agreed.

4. Implementation

Each role will be set up as a Group within NT. Individual users will be assigned to these Groups in which access to objects, domains, servers and associated privileges will be controlled. These Groups are defined in Appendix A.

Roles will have defined access points which will have an accompanying Platform Design Document. Access to objects will be made available to each role at the relevant access point.

4.1 NT Administrator User

The Windows NT operating system is provided with a super user known as the 'Administrator'. This user has full administration and configuration privileges which is exercised at both system/server and domain level. This capability cannot be removed from Windows NT. Pathway recognises the power that this user has and the ability that a human user, using the administrator user, has to interfere with the day to day operation of the Pathway solution.

To address this issue, Pathway will limit and restrict the use of the NT Administrator User. This will be achieved by:

➢ Renaming the Administrator User on all NT Servers so that it is hidden from the system. The account name and password will be specified by the Pathway Security Manager, which will be strictly controlled and stored in a secure safe.

➢ Restrict full administrator privileges to the 'Operational Management' role. Use of this role will be subject to the management and procedural controls set out in the 'Pathway Code of Practice', PA/STD/010.

ICL Pathway   **Group Definitions for the Secure NT Build**   Ref:RS/REQ/012
Release 2   Version:3.0
Date:21/10/98

APPENDIX A

Group Name to be implemented	Tools	NT Servers	Access Rights	Authentication Domain	Resource Domain access	Access Point	ACP Equivalent
ICL Outsourcing							
Application SUP	➢ Discoverer 2000 ➢ PC Xware ➢ Microsoft Office ➢ PC Anywhere ➢ Onnnet (telnet/ftp) ➢ Patrol v3.2.05 ➢ Legato Adimistrator ➢ IE4.0 ➢ SQL Server Admin	B/W SLAM Domain User Access to Sequent	Read / Write / Execute	PWYDCS	B/WSLAM	CFM NT Client PC	Application Support (CFM)
Base Installation & Configuration **(not an account template - no system policy)**	NT Administrator	All Servers	Administrative Full	Local	Server Console	Server Console	Base Installation & Configuration (CFM)
Engineer	PW Event viewer System Shut Down	All Servers Engineers require an account that has log on locally rights and is a member of the local Power Users group.	Read / Execute	PWYDCS SEQSUP ORASUP PWYHQ TEWKDLR SITTDLR DUNSDLR WYCODLR	B/WSLAM B/WPOCL B/WRELS B/WOPSS B/WSECS B/WDLR PWYMAS BRASUP FELURS	Server Console	Engineers (NT Data Centres)
Security Management	➢ PW User Admin ➢ PW Event Viewer ➢ SQL Server Admin ➢ SQL Server SecurityManager	All Servers	Read/Write	PWYDCS	All	CFM NT Client PC	Security Management
Operational Management	➢ Compaq systems reference library	All Servers	Administrative Full	PWYDCS	All	CFM NT Client PC	Operational Management

ICL Pathway **Group Definitions for the Secure NT Build Release 2** Ref:RS/REQ/012
Version:3.0
Date:21/10/98

	➢ Insight Manager ➢ SQL Server Admin ➢ Technet ➢ Microsoft Office ➢ NT Resource Kit ➢ Onnnet (telnet/ftp) ➢ Patrol v3.2.05 ➢ Legato Administrator ➢ nt srvtools ➢ Tivoli desktop ➢ IE4.0 for access to Tivoli web ➢ NT resource kit remote console server ➢ PC Xware	Access to Sequent					(CFM) Riposte Management
Network Management	➢ Telnet ➢ Router Configuration Software ➢ Network Diagnostic software			P/WDCS	N/A	Network Client PC	Network Management Configurer
Sequent Support	➢ PC Anywhere ➢ Hyper Terminal	Access to Sequent	Read	SEQSUP	N/A	Sequent Client PC	Sequent Support
Oracle Support	➢ Telnet	Access to Sequent	Read	ORASUP	N/A	Oracle Client PC	Oracle Support
EMC Support	➢ EMC proprietary Client software	Access to Sequent	Read	P/WDCS	N/A	EMC Client PC	None

ICL Pathway   **Group Definitions for the Secure NT Build**   Ref:RS/REQ/012
                              Release 2   Version:3.0
                                                                   Date:21/10/98

Group Name to be implemented	Tools	NT Servers	Access rights	Authentication Domain	Resource Domain access	Access Point	ACP Equivalent
SSC							
SSC Application Management	Tivoli Remote Console ExCeed for Windows NT (V 6.1) Rclient RiposteGetMessage.exe RiposteNode.exe RiposteObjectSecurity.exe RiposteObject.exe RipostePing.exe RipostePriorityMessage.exe RiposteQueryUK.exe RiposteNextMessage.exe RipostePutMessage.exe RiposteScanMessage.exe RiposteStatus.exe RODBClient.exe SQLServer V6.5 client NT utilities Microsoft Diagnostics Visual Basic I.D.E. PW Event Viewer WinZip/Pkzip CD Rom writing software Textpad Microsoft Word/ Excel/ Access/ Explorer Internet Explorer Services Manager CMD Prompt Performance Monitor Registry editor In-house Utilities Archve Viewer	All Servers Also; Access to Sequent	Read/Write/ Execute	PWYDCS	All	SSC NT Client PC	Application Support (SSC)

ICL Pathway   **Group Definitions for the Secure NT Build**   Ref:RS/REQ/012
                           Release 2   Version:3.0
                                                                                              Date:21/10/98

	Expiry Reporter Stops Reporter Formatted File Utility MessageStore Utility EndOfDay Reporter MessageStore Sort Utility						
SSC Application Support	Tivoli Remote Console ExCeed for Windows NT (V 6.1) Rclient RiposteGetMessage.exe RiposteNode.exe RiposteObject.exe RipostePing.exe RipostePriorityMessage.exe RiposteNextMessage.exe RiposteQueryUK.exe RiposteScanMessage.exe RiposteStatus.exe RODBClient.exe SQLServer V6.5 client NT utilities Microsoft Diagnostics Visual Basic I.D.E. W Event Viewer WinZip/Pkzip CD Rom writing software Textpad Microsoft Word/ Excel/ Access/ Explorer Internet Explorer Services Manager CMD Prompt Performance Monitor In-house Utilities Archve Viewer Expiry Reporter	All Servers Also; Access to Sequent	Read / Execute	PWYDCS	All	SSC NT Client PC	Application Support (SSC)

ICL Pathway **Group Definitions for the Secure NT Build** Ref:RS/REQ/012
Release 2 Version:3.0
Date:21/10/98

	Stops Reporter Formatted File Utility MessageStore Utility EndOfDay Reporter MessageStore Sort Utility						

ICL Pathway   **Group Definitions for the Secure NT Build**
                      Release 2

Ref:RS/REQ/012
Version:3.0
Date:21/10/98

Group Name to be implemented	Tools	NT Servers	Access rights	Authentication Domain	Resource Domain access	Access Point	ACP Equivalent
Pathway Roles							
Auditor	Legato client.exe RiposteRQueryUK	Audit Archive and Retrieval Server	Read/ Execute	PWYDCS	B/WOPSS	Audit PC SD/DES/077	NAO Auditor DSS Auditor POCL Auditor Pathway Business Functions Auditor
Auto-Configuration Administrator	ACDB Client.exe (assign member of ACDB Admin Group)	Auto-Configuration Server	Read/Write/Execute	PWYDCS	B/WRELS	Auto-Configuration Client PC SD/DES/026	None
Auto-Configuration User	ACDB Client.exe (assign member of ACDB User Group)	Auto-Configuration Server	Read/Write/Execute	PWYDCS	B/WRELS	Auto-Configuration Client PC SD/DES/026	None
Business Support	Discoverer Client RiposteQueryUK.exe	Access to PAS/CMS	Read / Execute	PWYHQ	B/WOPSS	Business Support Client PC SD/DES/092	Business Support Pathway Management
MIS BPS Users	MIS Client ➢ BPS_MIS Universe Windows Explorer MS Office WinZip v6..3 3.5 floppy CD ROM Printer CD Writer Software (Easy CD from adaptec)	B/W SLAM Also: Access to Data Warehouse	Read/Execute	PWYHQ	B/WSLAM	SLAM Client PC SD/DES/015	Implicit in text

COMMERCIAL IN CONFIDENCE   Page 12

ICL Pathway   **Group Definitions for the Secure NT Build**   Ref:RS/REQ/012
Release 2   Version:3.0
                                                                    Date:21/10/98

Group Name to be implemented	Tools	NT Servers	Access rights	Authentication Domain	Resource Domain access	Access Point	ACP Equivalent
SLAM Users	MIS Client ➤ SLAM Users ➤ CON SQL* Forms ➤ Ad Hoc reporting ➤ BO_REP Universe ➤ CCS SQL* Forms ➤ Reference Data SQL*Forms app ➤ BO Designer ➤ Supervisor Windows Explorer MS Office Printer 3.5 floppy CD ROM	B/W SLAM	Read/Execute	PWYHQ	B/WSLAM	SLAM Client PC SD/DES/015	Implicit in text
MIS Business Development Users	MIS Client ➤ BPS _MIS Universe Windows Explorer MS Office Printer	B/WSLAM Access to Data Warehouse	Read/Execute	PWYHQ	B/WSLAM	SLAM Client PC SD/DES/015	Implicit in text
ECCO MIG users	As per SD/DES/016	Migration Agent Server	Read/Write/Execute	PWYMAS	PWYMAS B/WOPSS	ECCO Migration Laptop SD/DES/016	None

ICL Pathway **Group Definitions for the Secure NT Build Release 2**

Ref:RS/REQ/012
Version:3.0
Date:21/10/98

Pathway FRM Manager	MIS Client ➤ FCMS SQL*Forms App ➤ FRM Universe ➤ FCMS Audit ➤ Fraud Universe ➤ Designer ➤ Supervisor ➤ Ad hoc universe Windows Explorer MS Office Printer CD ROM 3.5 inch floppy CD Writer Software (Easy CD from adaptec)	Access to Sequent only	Read / Execute	PWYDCS	B/WSLAM	FRM Client PC SD/DES/091	Pathway FRM

Pathway FRM Analyst	MIS Client
	➤ FCMS
	   SQL*Forms App
	➤ FRM Universe
	➤ Fraud Universe
	➤ FraudAud
	   Universe
	➤ Ad hoc universe
	➤ Designer
	➤ Supervisor
	Windows Explorer
	MS Office
	Printer
	CD ROM
	3.5 inch floppy
	CD Writer Software
	(Easy CD from adaptec)
		Access to Sequent only	Read / Execute	PWYDCS	B/WSLAM	FRM Client PC
						
						SD/DES/091
							None

Pathway FRM User	MIS Client ➤ FCMS SQL*Forms App ➤ FRM Universe	Access to Sequent only	Read / Execute	PWYDCS	B/WSLAM	FRM Client PC SD/DES/091	Girobank FRM

ICL Pathway   **Group Definitions for the Secure NT Build**   Ref:RS/REQ/012
                                    Release 2   Version:3.0
                                                                   Date:21/10/98

	➢ Fraud Universe ➢ Ad hoc universe Windows Explorer MS Office Printer CD ROM 3.5 inch floppy CD Writer Software (Easy CD from adaptec)						
Roll Out Support Advisor	RODB Client	RODB Server	Read / Execute	PWYDCS	B/WRELS	RODB Client PC SD/DES/050	Roll Out Support Desk Advisors
Roll Out Administrator	RODB Client NT Shares to RODB and ACDB	RODB Server ACDB Server	Read/ Write/ Execute	PWYDCS	B/WRELS	RODB Client PC SD/DES/050	None
Security Event Auditor	SecurID admin.client PW Event Viewer Tivoli Web Browser	All	Read / Execute	PWYDCS	All	SecurID Admin W/S SD/DES/090	Pathway Security Event Auditor
Pathway Security Management	SecurID admin.client PW Event Viewer Tivoli Web Browser	All Access to Enterprise Server (SecurID)	Read /Execute	PWYDCS	All	SecurID Admin W/S SD/DES/090	Pathway Security Manager
Other Roles							
DSS FIT	MIS Client > FCDB SQL*Forms Application	Access to Sequent only	Read / Execute	PWYDCS	B/WSLAM	FRM Client PC SD/DES/091	DSS FIT
FTMS Remote User DLR	Windows Explorer	Local share	Read / Execute	TEWKDLR SITTDLR WYCODLR DUNSDLR	N/A	DLR Client PC [Server Console] SD/DES/060	None
RODB external	Windows Explorer	Roll out database	Read/Write/	*External supplier*	N/A	RODB Gateway Remote	Pathway External

ICL Pathway **Group Definitions for the Secure NT Build Release 2**

Ref:RS/REQ/012
Version:3.0
Date:21/10/98

supplier			Execute	*domain*		PC SD/DES/065	Suppliers