FUJ00088104

Document Title: Secure Support Role Definitions for SECURENT Build

Document Type: Requirement Definition

Release: BI3S55/S60 onward

Abstract: The ACP requires that access to POA 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 tool sets, they need in order to complete the tasks associated with that particular role. This document summarises the requirements and defines the roles specifically engaged in support activities, with associated objects, domains and access requirements.

Document Status: APPROVED

Originator & Dept: Mark Ascott, DU Secure Builds

Contributors: Simon Fawkes, Peter Robinson, Steve Parker, Alex Robinson

Internal Reviewers: See section 0.2

External Reviewers: None

Approval Authorities:

Name	Position	Signature	Date
Mik Peach	SSC Manager		
Steve Gardiner	Core Services Operational Manager		
Ian Cooley	SMC Manager		
Bill Mitchell	POA Security Manager		

© 2004 Fujitsu Services

FUJ00088104

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL No.
0.1	10/01/02	First draft	CP3283
0.2	19/10/02	Updated with comment received from PVCS review cycle.	CP3283
0.3	04/02/03	Updated to reflect minor implementation changes to the solution	CP3283
0.4	15/07/03	Updated with new Riposte tools for counters.	CP3482
1.0	08/08/03	Updated to APRROVED with appropriate comments from PVCS review cycle addressed. from	CP3482
1.1	31/12/03	Updated with new roles for ADSL CHAP Password Management. Added new SAPSUP role.	CP3584 CP3640
2.0	18/03/04	Updated to V2.0 APPROVED following PVCS Review cycle.	CP3584 CP3640

0.2 Review Details

Review Comments by:	
Review Comments to:	Mark.ascot GRO

Mandatory Review Authority	Name
APDU Delivery Unit Manager	Mark Taylor
IPDU PIT Manager	Jim Stanton
RASD POA Security TDA	Alex Robinson
CS POA Security Manager	Peter Sewell
CS Systems Support Centre Manager	Mik Peach
DU Design Authority Support	Simon Fawkes
ITU PIT	Asad Sheikh
ITU PIT	Brian Bradley
DU Secure Builds	Mia Brittain, Stephen Sloan
RASD Systems Management TDA	Glenn Stephens
Core Services Operational Management	Steve Gardiner
Core Services SMC	Ian Cooley

FUJ00088104

Core Services SMG	Mike Conneely
Core Services Operational Management	Warren Welsh
Optional Review/Issued for Information	
DU DCO	Suzanne Gordon
ITU Test	Debbie Richardson
ITU LST	Pete Dreweatt
CS POA Security	Chris Billings
CS Migration Implementation Manager	Sheila Bamber
RASD	Nial Finnegan
ITU LST	Graham Jennings
SMG	John Bradley

0.3 Associated Documents

Reference	Tag	Version	Date	Title	Source
PA/TEM/001	[1]			This document is created from this version of PA/TEM/001	PVCS
RS/POL/003	[2]			Access Control Policy	PVCS
RS/FSP/001	[3]			Security Functional Specification	PVCS
DE/HLD/002	[4]			OpenSSH Auditing and Logging Server	PVCS
TD/ION/029	[6]			FTMS Configurations for AP Clients at CSR+	PVCS
RS/REQ/020	[7]			Implementation of Anti-Virus Requirements	PVCS
RS/DES/075	[8]			Communication Monitoring System DMZ Security Overview	PVCS
RS/DES/080	[9]			BI3 NT Domain Design	PVCS
RS/DES/081	[10]			BI3 Implementation Guide for NT Platforms	PVCS
RS/DES/082	[11]			BI3 NT Server and Workstation Names	PVCS
RS/REQ/022	[12]			BI3 Secure Role Definitions for SECURENT Build	PVCS
SMG/DES/017	[13]	0.1		Terminal Server Document	SMG
RS/DES/093	[14]	0.3		HLD for CHAP Password Handling	PVCS

Unless a specific version is referred to above, reference is made to the current versions of the documents.

0.4 Abbreviations/Definitions

Abbreviation	Definition

FUJ00088104

BDC	Windows NT Backup Domain Controller Server
BI3	Release Banking Increment 3
CP	Change Proposal
CSR+	Core Services Release +
DCS	Debit Card Services
DRS	Data Reconciliation Services
ISD	Abbreviation associated with Core Services staff
Local	Access via the console attached directly to an NT platform
NWB	Network Banking
PDC	Windows NT Primary Domain Controller Server
SAS	Secure Access Server
SSE	Secure Support Environment
SSH	Secure Shell
SSHC	Secure Shell Client
SSHD / SSH Server	Secure Shell Server
TS	Terminal Server

0.5 Changes in this Version

Version	Changes
1.0	Updated to APPROVED
1.1	New PWYLoad role added. References to Pathway have been changed to POA. New SAPSUP role added for Fujitsu Consulting SAP Support.
2.0	Updated to APPROVED

0.6 Changes Expected

Changes
For BI3S60 no further changes are expected prior to this document being set to APPROVED status. For BI3S70, CP3652 and CP3653 which cover enhancents to the Cygwin Toolset and Riposte installation on SAS servers will result in new drafts of this document being produced.

FUJ00088104

0.7 Table of Contents

FUJ00088104

FUJ00088104

1 Introduction

The nature of the POA Horizon system requires that access to the counters and core systems should be strictly controlled. [ACP] states that effective control depends on having a clear definition of the roles and the 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 POA implementing the principles of least privilege as described in [SFS]. POA will translate the human roles detailed in [ACP] into securely configured roles, known as secure roles.

RS/REQ/022 defines the requirements for all POA human secure roles (except for Support Roles) that access the POA data centre systems via an access point, which is usually an NT workstation. These requirements are translated by IPDU Secure Builds and IPDU PIT in order to generate a secure desktop for each role.

RS/REQ/023, this document defines the requirements of the human secure roles involved with providing support of the POA Horizon solution. It describes for each of the POA support groups the menus and tool sets required and the secure support environment desktop access method used to connect to remote counters and data centre systems.

2 Scope

This document only addresses the human user roles defined for use by the support groups involved with supporting the POA Horizon solution systems. These support roles are to be implemented as part of the POA central NT systems and access rights assigned to each role. Each support role specified within this document access counters and the data centre NT systems through the POA NT Domain Structure referenced in [9] and in accordance with the security configuration referenced in [10]. SMC and SMG support roles that authenticate in the SYSMAN domain are not described in terms of their Secure Desktops. For these roles it is assumed that their desktops include Terminal Server Client and that Terminal Server Client provides these roles with access to the Secure Support Environment implemented within the POA NT Domain Structure. Document reference [13] describes the configuration for SYSMAN secure roles.

Non support roles used by SMC, SMG and Girobank are specifically excluded from this document as they are authenticated on separate NT systems which form part of a third party managed service. These roles are excluded from accessing the Secure Support Environment.

This document does not describe the implementation or configuration of OpenSSH components on the NT data centre systems or counters. This information is described fully in reference [4].

FUJ00088104

3 Requirements

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

Release BI3 Network Banking and release BI3S30 Debit Card System introduced more stringent requirements regarding support access to counters and the data centre NT systems. To satisfy these new requirements, a Secure Support Environment is being introduced and as a result new user desktops and access mechanism are required for the support groups. This document defines the new authentication processes, desktops, and tool sets available to the support groups.

3.1 Affected Support Roles

The POA support roles affected by CP3283 are:

- PWYDCS\SSC Apps SUP
- PWYDCS\SSC Apps MAN
- PWYDCS\Operational MAN
- PWYDCS\Application SUP

In addition to the above two roles that authenticate in the SYSMAN third party supplier domain are also affected. These two roles are:

- SYSMAN\SMC
- SYSMAN\MSS

3.2 New Support Roles

At Release BI3S55 a new privileged role is introduced for ADSL CHAP Password Handling. See RS/DES/093 for more details concerning the use and procedures associated with this new role. The role is named:

- PWYDCS\PWYLoad

At Release BI3S60 a new support role is introduced for Fujitsu Consulting staff who will provide support for the new SAP financial system being introduced to the Horizon data centres at BI3S60. This new will provide this group of support staff access to the SAP Host via the SAS servers and SSH. The role is named:

- PWYDCS\SAPSUP

3.3 Redundant Support Roles

None of the existing support roles are made redundant.

FUJ00088104

FUJ00088104

4 Implementation

For the four POA support roles, each support role will be set up as a Secure Role. Secure Roles will be mapped very tightly on to the Group concept within NT. Individual users will be assigned to these Groups in which access to objects, domains, servers and associated privileges will be controlled. Reference [10] describes in more detail the rules and methods for applying Secure Roles onto the NT Group concept. These Secure Roles are defined in Section 7.

Secure Roles use defined access points that have an accompanying Physical Platform Design Specification (PPDS) document. Access to objects will be made available to each role at the relevant access point. This document specifically covers the Secure Support Roles accessing the data centres and counters.

The definition of the Secure Support Roles is maintained in a spreadsheet by IPDU Secure Builds, this spreadsheet is converted to produce automated NT command files. These command files will be made available to ITU PIT. The command scripts will be incorporated into the POA SECURENT build process and into the specific platform configuration builds by ITU PIT for deployment into test and live estate environments.

Secure Support Roles, as defined in this document, will be implemented using automated command scripts. By doing this, it will simplify the implementation and maintenance of the roles.

Human user accounts created from the defined roles may only be members of one Role/Group definition. This is required to ensure the user is only provided with one appropriate tool set. Implementation of the menu structure for each Group will ensure that users assigned to that Group will be able to access the application set necessary for them to fulfil their duties.

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. POA 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 POA solution.

To address this issue, POA 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 POA 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 'POA Code of Practice', PA/STD/010.

FUJ00088104

4.2 TSadmin Role

CP3283 introduces a new administrator role known as TSadmin. This new role will be responsible for day to day operations and administration of the PWYSAS domain and the Secure Access Servers. The security configuration will be setup to prevent PWYDCS roles from administering PWYSAS. Likewise, PWYSAS\Admininistrator whilst not being prevented from its administration capability by security configuration changes, sufficient monitoring capability will be added to the Security Event Auditor and POA Security Manager roles to 'watch' the use of this user.

The TSadmin role will be allocated to senior Core Services NT staff and will be limited to no more than three individuals at any one point in time. It is this role that will create and manage the terminal server user accounts. These individual accounts will be created from the pre-defined TS user templates. Each individual user will be mapped to a TS profile and will have a defined user home directory. Customer Services Security will be responsible for TSAdmin user accounts are allocated, created and managed.

4.3 SSHadmin Role

This new role is introduced for the purpose of managing the configuration of the SSH Client and SSH Server components. Like the TSadmin role, this new role will be limited for use by senior Core Services NT staff and will be limited to no more than three individuals at any one point in time. This role will only be able to administer the Secure Shell configuration files. Only this human role will be granted access control permissions greater than Read and Execute. Customer Services Security will be responsible for SSHAdmin user accounts are allocated, created and managed.

4.4 PWYLoad Role

This is a special role introduced for use by the Customer Services Security Management team. The purpose of the role is to load obfuscated passwords into the CHAP Password database. The role accesses the CHAP Password database by logon at Release BI3S55 at the BootLoader Server console. Once logged on, an executable is called to provide a GUI interface that enables passwords to be loaded into the database. At Release BI3S60 the role will also be able to logon at the ADSL Radius Servers and FRIACO/Dialled Radius Servers console.

© 2004 Fujitsu Services

FUJ00088104

5 Support Role Users

5.1 PWYDCS Users

SSC support staff and Core Services operational management staff who access the POA Horizon systems must have an individual user account registered in the PWYDCS domain. Each user account is created from a pre-defined user template which is described in Section 7 of this document. Associated with each NT user account registered in PWYDCS is a SecurID Token and four digit PIN.

Existing support user accounts remain unchanged within the SSE. New support user accounts will be created using the existing and current processes.

User templates exist for the following support roles:

- Users assigned to SSC Apps SUP role have user accounts created from user template ‘zzSSC Apps Sup’
- Users assigned to SSC Apps MAN role have user accounts created from user template ‘zzSSC Apps MAN’
- Users assigned to Operational MAN role have user accounts created from user template ‘zzOPSMAN’
- Users assigned to Application SUP role have user accounts created from user template ‘zzAPPSUP’

5.2 HUTHTIP, PDRTIP Users

Both HUTHTIP and PDRTIP domains which contain the Remote TIP Gateway systems at Post Office sites are authentication domains. Both are configured with identical support roles to those described for PWYDCS Users above. Access to these remote domains/systems using SSHD will require support staff to login and authenticate using user accounts created in the HUTHTIP and PDRTIP domains.

5.3 PWYKMS Users

TBA following input from Graham Hooper and Geoffrey Vane.

5.4 PWYCSM Users

TBA

FUJ00088104

5.5 SYSMAN Users

User accounts registered in this third party supplier managed domain must comply with the security policies defined in [ACP].

From the requirements specified in CP3283 the following support roles from this domain are relevant to the SSE:

- SMC
- MSS

5.6 Secure Access Server Users

Changes to the solution implementation mean that user templates and user accounts are no longer required within the PWYSAS domain and Secure Access Servers.

5.7 Counter Access Users

CP3283 specifies that only the SSC support group will be granted access to counters using SSE.

At the counter only a common/shared user account is required. SSH Client will capture the logon username from the Terminal Server Client session and will record this user name in the command log files that SSH Client generates. The user account defined for the SSC support group is:

- sussc

5.8 NT Data Centre System Access Users

Access to Data Centre NT systems will in the main be achieved by support staff logging on via SSHD using their PWYDCS user account. Exceptions to this will be HUTHTIP and PDRTIP remote TIP FTMS Gateway domains, PWYKMS and PWYCSM domains. Access to these four domains will be achieved by using equivalent user accounts created in these domains.

6 Support Authentication Process

6.1 Logon at Desktop

All support users that logon with a PWYDCS user account will specify their unique username and associated password. The system will then prompt for SECURID logon using their assigned PIN with the token value displayed at the time of logon.

The same logon and authentication process should be followed for all support users who authenticate in the SYSMAN domain.

FUJ00088104

Once the identification and authentication process has completed the user is presented with their usual desktop with an array of tools as specified in Section 7. One of the tools available from this desktop is the Terminal Server Client. Executing the Terminal Server Client tool will result in the system opening a new window at the workstation that results from a connection to a Secure Access Server located in PWYSAS domain. This new Terminal server window will display a prompt for a user name and password. At Release BI3S30, Support Users can still access counters and NT data centre systems using their pre BI3S30 desktops and tools. However from BI3S30 the only approved and authorised support access method to counters and NT systems in the PWYPUB and DCSSERV resource domains is via the Terminal Server/Secure Shell access route.

6.2 Logon at SAS Terminal Server

At the Terminal Server window login prompt the support user should re-enter their individual terminal server user account created in PWYDCS domain and its associated password.

Successful logon will result in the SAS desktop being made available to the user. From this desktop the Secure Shell Client (SSHC) will be available.

6.3 Logon to SSH Server

The user can invoke the SSHC by typing:

ssh –l <user name> <target-address>

where:

<user name> will equate to the support group users individual user account name created in PWYDCS domain or the other authentication domains referred to in section 5 for NT data centre systems or user account sussc for counters.

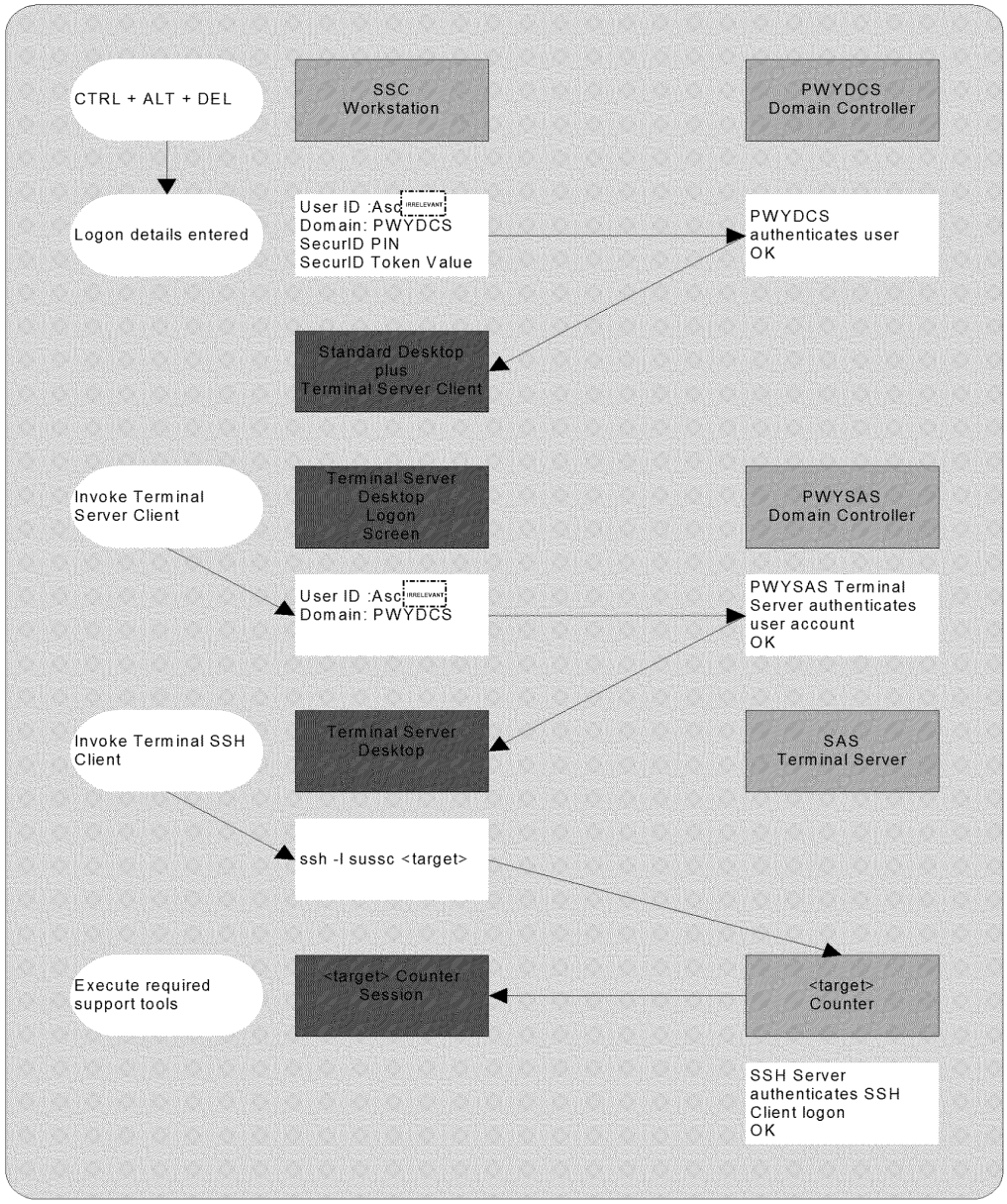
<target-address> will equate to the IP address of the target counter or NT system.

Execution of the above causes the SSHC to make a connection with the SSH server running on the target system. The user account specified will be authenticated at the target-system and if successful a SSH session will be initiated. The SSHC will log each command executed during the session recording the PWYDCS domain (or other domain) logon user account name that has initiated the SSH session.

FUJ00088104

6.4 Process Summary

See diagram below.



FUJ00088104

7 Support Role Desktops

7.1 Standard Secure Role Desktop

This section describes the desktop menu and tool set provided to the four POA Support Roles as a result of logging on with their PWYDCS, PWYKMS, (HUTHTIP, PDRTIP) user account, password and Securid Token. This logon will be conducted at their normal access point workstation or server.

FUJ00088104

7.1.1 SSC Apps MAN

Group Name to be Implemented	SSC Apps MAN
Last Updated	
Secure Role Type	Privileged Full Administrator capable
Desk Top Type	Restricted Desktop Menu
NT Servers	All NT Servers, also needs access to Post Office Outlet Counters and access to Sequent UNIX Servers
Access Rights	Read, Write, Execute
Requires SecurID Authentication	Yes
Authentication Domain	PWYDCS, PWYHQ, PWYFTMS, HUTHTIP, PDRTIP
Resource Domain Access	All resource domains and NT data centre systems via SSH Client access method
Access Point	SSC NT Client PC SD/DES/172
ACP Equivalent	Application Support (SSC)
Change Triggers	
Menus and Tools	➢ Tivoli Remote Console
	➢ Rclient
	➢ Rconsole
	➢ Terminal Server Client
	➢ RiposteGetMessage.exe
	➢ RiposteIndex.exe
	➢ RiposteNode.exe
	➢ RiposteObjectSecurity. Exe
	➢ RiposteObject.exe
	➢ RipostePing.exe
	➢ RipostePriorityMessage.exe
	➢ RiposteQueryUK.exe
	➢ RiposteNextMessage.exe
	➢ RipostePutMessage.exe
	➢ RiposteScanMessage
	➢ RiposteStatus.exe
	➢ RODBClient.exe
	CMD prompt
	➢ ExCeed for Windows NT (V 6.1)
	➢ Visual Basic I.D.E

FUJ00088104

	➢ Telnet
	➢ FTP (To Host Sequent, and other POL Services)
	Microsoft Diagnostics
	NT Event Viewer
	WinZip/Pkzip
	CD Rom writing software
	Textpad
	Microsoft Word
	Microsoft Excel
	Microsoft Access
	Microsoft Explorer
	Internet Explorer (c/w SSC default links page)
	Full NT Control Panel
	Performance Monitor
	Registry editor
	TIP Repair
In-house Utilities	➢ Archive Viewer
	➢ Expiry Reporter
	➢ Stops Reporter
	➢ Formatted File Utility
	➢ MessageStore Utility
	➢ EndOfDay Reporter
	➢ MessageStore Sort Utility
VPN Utilities	➢ VPNDiagClient.exe
	➢ SVPNTSTN.exe
Athene Utilities	Athene Analyst Analyst ViewDB Storage
	Athene Automatic Reporting Define A Report Schedule Editor View Processed Reports
	Athene Client-Server Client-Server
	Athene CustomDB CustomDB Schedule Editor Web Log Parser
	Athene Explorer Define A Report Explore Reports

FUJ00088104

	Athene Planner Build Baseline Model Calibrate Baseline Model Delete Models Edit Baseline Model Edit Reference Tables Edit Thresholds Evaluate Model Modify Model View Results
	Athene Sentinel Alert Summary Sentinel
Requires Access to	All systems

User Template	Is a member of	Global Group	Is a member of	Local Group
ZzSSCAPP_MAN				
	Yes	SSC Apps MAN		
	Yes	Domain Admins	Yes	Administrators
	Yes	Domain Users	Yes	LSSC Apps MAN
			Yes	LconfineLogin

FUJ00088104

7.1.2 SSC Apps SUP

Group Name to be Implemented	SSC Apps SUP
Last Updated	
Secure Role Type	Privileged Full Administrator capable
Desk Top Type	Restricted Desktop Menu
NT Servers	All NT Servers, also needs access to Sequent UNIX servers
Access Rights	Read, Execute
Requires SecurID Authentication	Yes
Authentication Domain	PWYDCS, PWYHQ, PWYFTMS, HUTHTIP, PDRTIP
Resource Domain Access	All resource domains and NT data centre systems via SSH Client access method
Access Point	SSC NT Client PC SD/DES/172
ACP Equivalent	Application Support (SSC)
Change Triggers	
Menus and Tools	➢ Tivoli Remote Console
	➢ Rclient
	➢ Rconsole
	➢ Terminal Server Client
	➢ RiposteGetMessage.exe
	➢ RiposteIndex.exe
	➢ RiposteNode.exe
	➢ RiposteObject.exe
	➢ RipostePing.exe
	➢ RipostePriorityMessage.exe
	➢ RiposteNextMessage.exe
	➢ RiposteQueryUK.exe
	➢ RiposteScanMessage.exe
	➢ RiposteStatus.exe
	➢ RODBClient.exe
	CMD prompt
	➢ ExCeed for Windows NT (V 6.1)
	➢ Visual Basic I.D.E.
	➢ Telnet

FUJ00088104

	➢ FTP (To Host Sequent, and other POL Services)
NT utilities	Microsoft Diagnostics
	Event Viewer
	WinZip/Pkzip
	CD Rom writing software
	Textpad
	Microsoft Word
	Microsoft Excel
	Microsoft Access
	Microsoft Explorer
	Internet Explorer (c/w SSC default links page)
	Full NT Control Panel
	Performance Monitor
	Registry editor
	TIP Repair
In-house Utilities	➢ Archve Viewer
	➢ Expiry Reporter
	➢ Stops Reporter
	➢ Formatted File Utility
	➢ MessageStore Utility
	➢ EndOfDay Reporter
	➢ MessageStore Sort Utility
VPN Utilities	VPNDiagClient.exe
Athene Utilities	Athene Analyst Analyst ViewDB Storage
	Athene Automatic Reporting Define A Report Schedule Editor View Processed Reports
	Athene Client-Server Client-Server
	Athene CustomDB CustomDB Schedule Editor Web Log Parser
	Athene Explorer Define A Report Explore Reports

FUJ00088104

	Athene Planner Build Baseline Model Calibrate Baseline Model Delete Models Edit Baseline Model Edit Reference Tables Edit Thresholds Evaluate Model Modify Model View Results
	Athene Sentinel Alert Summary Sentinel
Requires Access to	All systems

User Template	Is a member of	Global Group	Is a member of	Local Group
ZzSSCAPP_SUP				
	Yes	SSC App SUP		
	Yes	Domain Admins	Yes	Adminstrators
	Yes	Domain Users	Yes	LSSC Apps SUP
			Yes	LconfineLogin

FUJ00088104

7.1.3 Operational MAN

Group Name to be Implemented	Operational MAN
Last Updated	
Secure Role Type	Privileged
Desk Top Type	Restricted Desktop Menu
NT Servers	All NT Servers Access to Sequent UNIX Servers
Access Rights	Full Administrator
Requires SecurID Authentication	Yes
Authentication Domain	PWYDCS, PWYHQ, PWYFTMS, HUTHTIP, PDRTIP
Resource Domain Access	All resource domains and NT data centre systems
Access Point	Core Service NT Client PC Third Party Supplier PC NT server console
ACP Equivalent	Operational Management Core Services Role
Change Triggers	
Menus and Tools	➢ Compaq systems reference library
	➢ Insight Manager
	➢ Terminal Server Client
	➢ SQL Server Admin
	➢ Technet
	➢ Microsoft Office
	➢ NT Resource Kit
	➢ Onnnet (telnet/ftp)
	➢ Patrol v3.2.05
	➢ Legato Administrator
	➢ nt srvtools
	➢ Tivoli desktop
	➢ IE5.5 for access to Tivoli web
	➢ NT resource kit remote console server
	➢ PC Xware
	CMD prompt
	➢ VPNDiagClient.exe

FUJ00088104

	➢ Notepad
	➢ SVPNTSTN.exe (Utimaco API Function Tool)
Athene Utilities	Athene Analyst Analyst ViewDB Storage
	Athene Automatic Reporting Define A Report Schedule Editor View Processed Reports
	Athene Client-Server Client-Server
	Athene CustomDB CustomDB Schedule Editor Web Log Parser
	Athene Explorer Define A Report Explore Reports
	Athene Planner Build Baseline Model Calibrate Baseline Model Delete Models Edit baseline Model Edit Reference Tables Edit Thresholds Evaluate Model Modify Model View Results
	Athene Sentinel Alert Summary Sentinel
Requires Access to	Floppy disc drive Locally connected printer

FUJ00088104

User Template	Is a member of	Global Group	Is a member of	Local Group
zzOPS_MAN				
	Yes	Operational MAN		
	Yes	Domain Users	Yes	Loperational MAN
			Yes	LconfineLogin

FUJ00088104

7.1.4 Application SUP

Group Name to be Implemented	Application Sup
Last Updated	
Secure Role Type	Privileged
Desk Top Type	Restricted Desktop Menu
NT Servers	Access to Sequent UNIX Servers
Access Rights	Read, Write, Execute
Requires SecurID Authentication	Yes
Authentication Domain	PWYDCS, PWYHQ, HUTHTIP, PDRTIP
Resource Domain Access	PERFMAN
Access Point	Core Services NT Client PC Third Party Supplier PC
ACP Equivalent	Application Support Core Services Role
Change Triggers	
Menus and Tools	➢ Discoverer 2000
	➢ PC Xware
	➢ Microsoft Office
	➢ Onnnet (telnet/ftp)
	➢ Patrol v3.2.05
	➢ Legato Administrator
	➢ IE5.5
	➢ SQL Server Admin
	➢ Terminal Server Client
	CMD prompt
Athene Utilities	Athene Analyst Analyst ViewDB Storage
	Athene Automatic Reporting Define A Report Schedule Editor View Processed Reports
	Athene Client-Server Client-Server

FUJ00088104

	Athene CustomDB CustomDB Schedule Editor Web Log Parser
	Athene Explorer Define A Report Explore Reports
	Athene Planner Build Baseline Model Calibrate Baseline Model Delete Models Edit baseline Model Edit Reference Tables Edit Thresholds Evaluate Model Modify Model View Results
	Athene Sentinel Alert Summary Sentinel
Requires Access to	Floppy disc drive Locally connected printer

User Template	Is a member of	Global Group	Is a member of	Local Group
ZzApplication_SUP				
	Yes	Application SUP		
	Yes	Domain Users	Yes	Lapplication SUP
			Yes	LconfineLogin

FUJ00088104

7.1.5 PWYLoad

Group Name to be Implemented	PWYLoadGroup
Last Updated	08/01/04
Secure Role Type	Privileged Administrator access capable
Desk Top Type	Restricted Desktop Menu
NT Servers	Access to BootLoader Server , ADSL Radius Servers and FRIACO/Dialled Radius Servers
Access Rights	Read, Write, Execute
Requires SecurID Authentication	Yes
Authentication Domain	PWYDCS
Resource Domain Access	BBOOT, WBOOT and PWYRAD systems via direct logon at server console
Access Point	Server Console for BootLoader Servers, ADSL Radius Servers and FRIACO/Dialled Radius Servers
ACP Equivalent	None
Change Triggers	CP3584
Menus and Tools	
	CMD prompt
	Microsoft Diagnostics
	NT Event Viewer
	WinZip/Pkzip
	Textpad
	Microsoft Word
	Microsoft Excel
	Microsoft Access
	Windows Explorer
	Full NT Control Panel
	Registry editor
In-house Utilities	➢ Password Loader executable (maps onto C:\RADIUS_CFG\Bin\RcapPwdLoader.exe on the Bootloader server)
Requires Access to	All systems in BBOOT, WBOOT and PWYRAD domains. Requires access to floppy disc drive.

FUJ00088104

User Template	Is a member of	Global Group	Is a member of	Local Group
ZzPWYLoad				
	Yes	GPWYLoadGroup		
	Yes	Domain Users	Yes	LPWYLoadGroup
			Yes	LconfineLogin

FUJ00088104

7.1.6 SAPSUP

Group Name to be Implemented	**GSAPSUP**
Last Updated	26/02/04
Secure Role Type	Privileged Administrator access capable
Desk Top Type	Restricted Desktop Menu
NT Servers	Access to SAP Host via dedicated SAS Servers MBOSAS03 or MWISAS03
Access Rights	Read, Write, Execute
Requires SecurID Authentication	Yes
Authentication Domain	PWYDCS
Resource Domain Access	PWYSAS
Access Point	Fujitsu Consulting Support Workstation + SecurID ACE Agent
ACP Equivalent	None
Change Triggers	CP3640
Menus and Tools	
	Terminal Server Client
	SAP GUI Interface (maps onto an executable that needs to be supplied by Fujitsu Consulting staff, may require FJC to complete an installation to obtain this piece of information.
	FTP Client. Notes: 1, the SAP Host will be configured with FTP Server Service and the FJC SAP Support user group on the Solaris SAP Hosts must be granted permissions to access and execute FTP. 2, the DMZ firewalls must be configured to allow inbound and outbound FTP traffic for this support group.
In-house Utilities	➢ None requirements specified.
Requires Access to	FTP capability between SAP Hosts and FJC SAP Support Workstations.

FUJ00088104

User Template	Is a member of	Global Group	Is a member of	Local Group
ZzSAPSUP				
	Yes	GSAPSUP		
	Yes	GSAPSUP	Yes	LPWYSUP
	Yes	Domain Users	Yes	LSAPSUP
			Yes	LconfineLogin

FUJ00088104

7.2 Terminal Server Client Desktop

This section describes the desktop available to each of the Support groups provided with Terminal Server access to the SSH Client.

7.2.1 SSC Support Group

Access provided to SSH Client. The SSH Client can be used to access counters and data centre NT systems.

7.2.2 SMC Support Group

No access to SSH Client provided.

7.2.3 MSS Support Group

No access to SSH Client provided.

7.2.4 Operational Management Support Group

Access provided to SSH Client. The SSH Client can only be used to access data centre NT systems.

7.2.5 Fujitsu Consulting SAP Support Group

Access provided to SSH Client. The SSH Client can only be used to access the SAP Host in the data centres.

FUJ00088104

8 Support Tools

8.1 Tool Set Location and Access

The support tool set will be installed at the same location on all NT platforms.

The 'root' directory is known as:

- C:\Support

Underneath this directory is the following structure:

- C:\Support\Tools\Generic
- C:\Support\Tools\Generic\Cygwin
- C:\Support\Tools\Generic\Ntreskit
- C:\Support\Tools\Admin (only on Secure Access Servers)

As the directory names imply, Generic means that the tools are common and available to all support groups. The Cygwin directory holds all the GNU tools generated and delivered into PVCS by IPDU Estate Management Development team. The Ntreskit directory holds all Windows NT resource kit utilities. These are made available to all support groups.

In addition to the above 'common' directories, each support group will have a dedicated directory to hold bespoke developed tools. The directories are:

- C:\Support\Tools\SSCSUP
- C:\Support\Tools\SMCSUP
- C:\Support\Tools\SYSMANSUP
- C:\Support\Tools\OPSMANSUP
- C:\Support\Tools\SAPSUP

Each support group will be able to access tools located in their directory. They will not be able to access the directories of the other support groups. All support group access will be configured as Read and Execute. Only administrator privileged users will be able to update the above directories and add further tools to the tool set.

FUJ00088104

8.2 Riposte Tools on Counters (CP3482)

The following tools are added to all counters via the PIT build at Release BI3S40R as a result of CP3482. The tools are located in directory **C:\Counters\Bin**.

RiposteConfig.exe

RiposteGetMessage.exe

RiposteListen.exe

RiposteNextMessage.exe

RiposteNode.exe

RiposteObject.exe

RipostePutMessage.exe

RiposteScanMessage.exe

RiposteStatus.exe

8.3 Tools Available

A full list of the tools available is given in a table in Appendix A. This appendix will be kept update as further tools are added in the future.

8.4 Updating the Tool Set

There are two situations in which the support tool set can be updated. These are 'normal' and 'exceptional' circumstances.

8.4.1 Normal Circumstances

This section gives a brief overview of the process that should be followed in normal circumstances in order to add new tools to the tool set.

- The Support group identifies new tool(s).
- The Support group subject the tool(s) to local testing to ensure the tool(s) is/are fit for purpose.
- The Support group raise a CP to introduce the new tool(s), indicating whether it is/they are generic tool(s) or specific to the support group and identifying the target release.
- POA development impacts the CP. If the CP is approved
- IPDU Secure Build update this document [RS/REQ/023] and publish on PVCS review cycle.

FUJ00088104

- The Security TDA and POA Security Manager are both Approval Authorities. In addition each Support group will also have an Approval Authority for this document. The IPDU PIT Manager will also be an Approval Authority.
- Once this document has gained the necessary approval signatures, the IPDU PIT Manager will authorise IPDU PIT to progress the updates necessary to add the tool(s) to the tool set directories. IPDU Secure Build will adjust the security configuration as necessary.
- The work packages are subjected to testing by IPDU System Test and on completion of testing the new work packages are added to the SUPPORT TOOLS platform configuration build for release to the live estate systems.
- The new tools are delivered and installed onto the NT platforms using Tivoli.

8.1.2 Exceptional Circumstances

There will always be emergency situations that will require new tools to be made available urgently. At this point in time, no process for handling exceptional circumstances has been identified. Simon Fawkes is leading the investigation into how this situation will be dealt with and will identify the proposed solution once known.

9 Appendix A – Support Tool Set

This appendix lists the GNU tools available as part of the Support Tools platform Configuration SPBV.

The following detail is associated with the table on the next page.

The tools identified in the table are located in directory:

C:\Support\Tools\Generic\Cygwin (on all platforms)

A ‘Yes’ in the following column indicates that the program is to be executable by members of the support group, while ‘No’ indicates that permission to execute the commands is not to be granted.

The commands shown in the table do not have the ‘.exe’ suffix. The ‘.exe’ suffix will be present for all executables when delivered to PVCS and installed on the platform.

Selected and where required, security approved NT Resource kit utilities provided by Microsoft at Release Supplement 4 are made available in directory:

C:\Support\Tools\Generic\NTreskit (on all platforms)

FUJ00088104

FUJ00088104

Table 1

	Support groups at Data Centre					User groups at Counters				
Commands	**SSC**	**ISD**	**MSS**	**Tivoli**	**Maestro**	**SSC**	**ISD**	**MSS**	**Tivoli**	**Maestro**
basename	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
bash	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
cat	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
chgrp	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
chmod	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
chown	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
chroot	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
cmp	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
cp	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
cut	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
cygpath	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
date	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
dd	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
df	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
diff	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
dirname	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
du	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
echo	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
egrep	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
expr	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
false	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
find	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
fold	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
gunzip	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
gzip	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
head	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
hostname	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
kill	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
less	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
ln	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
login	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
ls	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
md5sum	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
mkdir	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
mount	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
mv	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
nawk	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
nice	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
nl	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
od	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
paste	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
printf	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
ps	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
pwd	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
regtool	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
rm	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
rmdir	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
sed	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
sleep	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
sort	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
tail	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
tar	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
tee	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
test	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
touch	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
tput	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
true	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
tset	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
umount	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
wc	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes

Table 2

FUJ00088104

	Support groups at Data Centre					User groups at Counters				
Commands	**SSC**	**ISD**	**MSS**	**Tivoli**	**Maestro**	**SSC**	**ISD**	**MSS**	**Tivoli**	**Maestro**
compreg	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
disksave	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
dumpel	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
getmac	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
getsid	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
kill	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
pulist	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
rkill	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
robocopy	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
sc	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
scanreg	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
sclist	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
scopy	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
showacls	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
showdisk	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
showgrps	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
showmbrs	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
shutdown	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
sleep	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
tlist	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes
xcopy	Yes	Yes	No	No	Yes	Yes	No	No	No	Yes