



Citigroup Technology Infrastructure
Global Engineering

Third Party Remote Access

**Solution Design
7.0**

1. Version Control

Version	Date	Author	Reviewed	Comments
3.0	18-Nov-04	Bromin Menezes, Parul Jain	Project team	2 nd draft
4.0	6-Dec-04	Bromin Menezes, Parul Jain	-	3 rd draft
5.0	9-Dec-04	Bromin Menezes, Parul Jain	-	Release
6.0	12-April-04	Parul Jain	-	Added design for Connectrix Manager application
6.1	27-April-05	Michael Baccala	-	WWDS wishes to use this access for all vendors
7.0	19-May-05	Parul Jain		Made architecture generic. Moved device specific material to appendix.

2. Legal Notice

Information contained herein is for Internal Use and may be used only for business purposes authorized by Citigroup.

CITI, CITIBANK, CITICORP, CITIGROUP and the Umbrella Device are trademarks and service marks of Citicorp and are used and registered throughout the world. Citibank, Citicorp, Citigroup and their subsidiaries also claim rights in certain other trademarks and service marks contained in these pages.

3. Contact

Please address any comments or questions regarding the information contained in this document via email to the “*GT US Sztabnik Group” distribution list.

4. Latest Versions

It is recommended that the latest version of the document be used from the TBD website. Newer versions may include expanded scope, or comments on issues discovered after deployment.

5. Table Of Contents

1. VERSION CONTROL	2
2. LEGAL NOTICE.....	3
3. CONTACT.....	3
4. LATEST VERSIONS	3
5. TABLE OF CONTENTS	4
6. APPROVALS	5
7. EXECUTIVE SUMMARY	6
8. AUDIENCE	6
9. SCOPE	7
10. CERTIFICATION PROCESS	7
11. CURRENTLY CERTIFIED DEVICES	8
12. REMOTE ACCESS ARCHITECTURE	8
12.1. ACCESS 1: REMOTE ACCESS	8
12.2. ACCESS 2: ACCESS FROM CORPORATE NETWORK	9
12.3. ACCESS 3: DIAL-OUT	9
13. APPENDIX A: IMPLEMENTATION CHECKLIST.....	10
14. APPENDIX B: SUGGESTED AUTHORIZATION AND RECORDING PROCEDURE	11
15. APPENDIX C: DIAL-IN INSTRUCTIONS	12
16. APPENDIX D: EMC SYMMETRIX DEVICE	13
16.1. OVERVIEW	13
16.2. FIREWALL REQUIREMENTS	13
16.2.1. ACCESS 1: REMOTE ACCESS	13
16.2.2. ACCESS 2: ACCESS FROM CORPORATE NETWORK	13
17. APPENDIX E: EMC CONNECTRIX SWITCH DEVICE	14
17.1. OVERVIEW	14
17.2. FIREWALL REQUIREMENTS	14
17.2.1. ACCESS 1: REMOTE ACCESS	14
17.2.2. ACCESS 2: ACCESS FROM CORPORATE NETWORK	15

6. Approvals

Department	Name	Approved (Y/N)	Approval Date	Remarks
Global Engineering/ External Networks	Peter Callahan	YES	11/18/04	
Global Engineering/ Remote Access	Kambiz Mofrad	YES	11/18/04	
Global Engineering/ B2B	Rob Centra			
Global Engineering/ Storage	Bob Small			

7. Executive Summary

Several hardware devices within Citigroup datacenters require remote access by third party. Such access is used for the following purposes:

1. Alerting of system faults such as power supply failure, disk failure etc. to the third party customer support center.
2. Remote diagnostics and periodic maintenance by third party personnel.

This type of access is industry standard for certain pieces of equipment that require very high availability. Examples of such equipment within the Citigroup IT environment are EMC and IBM Storage Arrays, Storage Area Network Switches, PABX, and certain high-end servers. This arrangement ensures that any component failures are caught and addressed before they can cause an application outage. Often, the remote support is inseparable from the product; the manufacturer assigns reliability and availability specifications based on the remote support capability.

The alerting and remote access is usually enabled through a modem attached to the equipment. The modem connects to the third party support center over the public telephone network. The following issues have been identified with this approach:

- Citigroup has no control over the remote access; the access is always on
- Citigroup is not notified of the event
- Citigroup cannot determine whether such access is for authorized use by authorized parties

Although business data cannot be accessed through such access, the remote access permits re-configuration of the equipment that can lead to an outage.

The proposal from Security Engineering, Remote Access Engineering, B2B Engineering, and Global Distributed Storage Engineering is to leverage the Citigroup standard remote access infrastructure, called “WWDS”, for enabling third party remote access for fault management applications.

Any existing third party remote access used for fault management purposes should be converted to the proposed architecture.

8. Audience

This document is intended to be read by Engineering and Operational product owners who either have products that are supported by third parties, or who are planning to outsource the fault management of existing products to a third party.

The document is also intended for regional Applied-Engineering as well as Integration teams, who would create site-specific layouts and bill of materials to prepare for implementation.

9. Scope

The architecture proposed in this document is suitable for the purpose of remote fault management of equipment installed within the data center, when the device permits remote access over TCP/IP. The design does not cater to other types of remote access, such as employee or partner access. Such access is detailed in separate documents.

The design can be implemented globally in any data center.

10. Certification Process

Before a new type of device can be serviced by this architecture, Global Engineering must establish the technical feasibility of the solution. Product owners should engage Global Engineering with a Project Initiation Form (“PIF”). Global Engineering will work with the product owner and the third party to establish the suitability of the architecture for that device. Results of the test will be appended to this document, and the device would be deemed certified for this architecture. Once certified, another PIF should be used to engage the applied engineering and integration teams for implementation.

It may not be technically feasible to use the proposed architecture for all types of devices. Even before approaching Global Engineering for certification, the product owner should do the following tests:

1. The device should be capable of being connected to an Ethernet/IP network and accept a Citigroup provided IP address, netmask and gateway.
2. The application software on the device should have a fixed list of TCP and/or UDP ports that it uses for communication to the remote third party workstation. It should be possible to run the communication through one or more firewalls, with or without network address translation (“NAT”).
3. The third party workstation should be capable of dialing up using MS-Windows dial-up networking.
4. If Citigroup personnel manage the device as well, the device management applications should be of client-server architecture. The client portion of the applications should be capable of being installed on a SOE server. The client portion should also be capable of talking to the server portion running on the device through a firewall.

11. Currently Certified Devices

The following devices are currently certified to work with the recommended architecture:

Infrastructure Component	Unit that will host remote access	Remote Access Application	See Appendix
EMC Symmetrix Storage Array	Service Processor	EMC SymmRemote	Appendix D
EMC Connectrix Fibre Channel Switch	Connectrix Service Processor	EMC SymmRemote	Appendix E
IBM Shark Storage Array	TBD	TBD	TBD

12. Remote Access Architecture

Three types of access would be provided to the device. Please refer to figure 1.

12.1. Access 1: Remote Access

The third party will use this access to remotely connect to the device to carry out diagnostics and maintenance tasks. Third party support person K will initiate a call using his or her modem to the Citigroup remote access server G, also known as "WWDS". WWDS authenticates callers with dynamic passwords that are generated by hardware tokens such as Safeword. Person K will make a voice call to the Citigroup control desk who have access to the hardware token. The control desk will identify the caller, make an entry in the log, open a trouble ticket and will issue the password to person K. The caller will use the password to get connected to WWDS. The caller will be assigned an IP address from a pool of IP addresses. There will be several pools, and the pool will be selected based on the hardware token serial number used to generate the password.

The remote access firewall F protects Citigroup resources B,C,D from person K. Once person K has full control over device H, the B2B firewall E protects Citigroup resources B,C,D from person K.

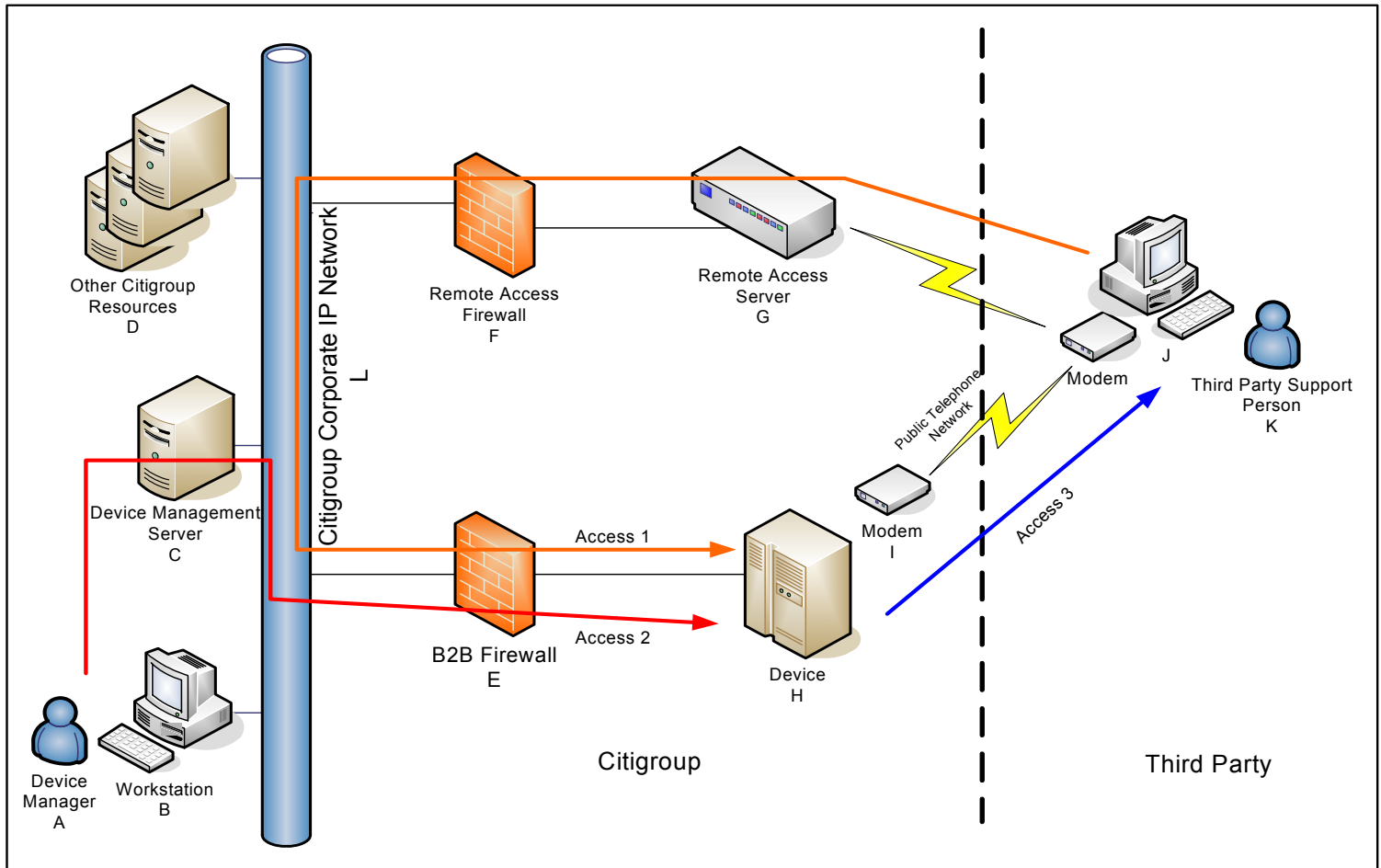


Figure 1 Types of Access

12.2. Access 2: Access from Corporate Network

This optional access is provided for devices that need to be managed by Citigroup personnel in addition to third party personnel. Citigroup device manager A would use his or her SOE workstation B to connect to device management server C. Server C would be a SOE server that hosts applications that are required to manage device H. The B2B firewall E will allow these applications from server C to talk to the device H.

12.3. Access 3: Dial-out

This optional access is provided so that the device can report faults to the third party support center. A modem connected to the public telephone network is used by application software running on the device to dial-out and connect to the server at the support center. **The telephone line connected to the modem at Citigroup end must be configured to allow outgoing calls only; incoming calls should not be allowed.**

13. Appendix A: Implementation Checklist

The following is the sequence of events to migrate a device to the new remote access architecture:

- Get device certified from Global Engineering.
- Develop authorization and recording procedures.
- Obtain approval from third party that is supporting the device. It may be required to revise the support contracts.
- Build and configure the environment.
- Train Citigroup and third party personnel that will be involved in the process.
- Test new access method with third party.
- Switch over to the new access.

14. Appendix B: Suggested Authorization and Recording Procedure

Operational product owners should develop their own procedures for authorizing and recording of third party access as a part of the implementation project. The following is a high level template that may be used for such development:

1. A 24x7 “control desk” should be setup within Citigroup. This control desk will be equipped with hardware tokens.
2. When the third party requires access to the device, they will call the control desk to request access.
3. The control desk will record the request into a system such as a trouble ticket system.
4. The control desk will call back the third party at a pre-defined telephone number to give out the password generated by the hardware token.
5. The third party will proceed to connect to the device and carry out diagnostic or maintenance activities on the device.
6. Once the work is completed and remote access session is terminated, the third party will call the control desk with a status update. The control desk will record the status.

15. Appendix C: Dial-in Instructions

Using “Dial-Up networking”, select “bring up terminal window after connecting”.

1. Using the Safeword Card Serial number as the “userID” call the Citi entity, which holds the vendor card for the dynamic password (“token”).
2. Enter card number as username and password in the password field of Dial Up Networking (DUN).
3. Dial a local MCI number (local numbers supplied from Remote Access).
4. In Post Terminal Window once connection is made you will need hit “enter” then “Shift plus +” this sets MCI parity to 8N1 so you can read “Enter Host name” in clear text.
5. You will then be prompted to enter “Host Name”, which is PPPVEN.
6. Next you will be prompted for “UIC” which is the serial number of your Safeword card.
7. Once you see the router prompt you will enter “PPP”
8. You should then see what looks like garbage in the window. At that point you should click the “Done” button at the bottom of the screen.
9. You will then see a box that says it is registering you on the network.

16. Appendix D: EMC Symmetrix Device

16.1. Overview

The fault management of EMC Symmetrix storage arrays has been outsourced to the vendor. A modem connected to the Symmetrix Service Processor dials out to vendor support center to alert faults. The vendor can then dial-in through the same modem for troubleshooting. This type of remote access allows the vendor to maintain a tight service level agreement.

The Symmetrix Service Processor exists solely for vendor purposes. Citigroup storage management team does not use the Symmetrix Service Processor for storage management tasks.

The EMC SymmRemote application provides keyboard, video and mouse ("KVM") access to the Symmetrix Service Processor over modem or TCP/IP network. The application is similar to commercially available software for the Wintel platform such as VNC or PCAnywhere etc.

The SymmRemote application can be configured to either wait for incoming calls on the modem or the TCP/IP network. When configured to work on the TCP/IP network, SymmRemote listens on a configurable TCP port for incoming connections from the SymmRemote client. The default port is TCP/5414.

The SymmRemote client software, which is only available to EMC support staff, connects to the SymmRemote server listening on TCP/5414 on the service processor. Once the connection is established, the remote user has full KVM control of the service processor.

16.2. Firewall Requirements

16.2.1. Access 1: Remote Access

Traffic Origination	Source Address	IP	Destination Address	IP	Protocol	Destination Port(s)	Traffic Description
Third party workstation	WWDS Pool		IP address assigned to the Symmetrix Service Processor		TCP	5414	SymmRemote client-server

16.2.2. Access 2: Access from Corporate Network

No access required.

17. Appendix E: EMC Connectrix Switch Device

17.1. Overview

McData switches and directors, also called EMC Connectrix switches and directors, are managed by using the Connectrix Manager, also known as "EFCM", application software. The server portion of this software is installed on a dedicated Wintel laptop or 1U server, called the Connectrix Service Processor ("CSP"), and is located within the Connectrix cabinet with the switches and directors. The client portion of the Connectrix Manager application is loaded on a SOE Solaris or Wintel server with IP connectivity to the CSP. Storage management personnel log onto this SOE server to use the Connectrix Manager client application.

The CSP is also accessed from the public telephone network with over a modem. The EMC SymmRemote application provides keyboard, video and mouse ("KVM") access to the Connectrix Service Processor over modem or TCP/IP network. The application is similar to commercially available software for the Wintel platform such as VNC or PCAnywhere etc.

The SymmRemote application can be configured to either wait for incoming calls on the modem or the TCP/IP network. When configured to work on the TCP/IP network, SymmRemote listens on a configurable TCP port for incoming connections from the SymmRemote client. The default port is TCP/5414.

The SymmRemote client software, which is only available to EMC support staff, connects to the SymmRemote server listening on TCP/5414 on the service processor. Once the connection is established, the remote user has full KVM control of the service processor.

17.2. Firewall Requirements

17.2.1. Access 1: Remote Access

Traffic Origination	Source Address	IP	Destination Address	IP	Protocol	Destination Port(s)	Traffic Description
Third party workstation	WWDS Pool		IP address assigned to the Symmetrix Service Processor		TCP	5414	SymmRemote client-server

17.2.2. Access 2: Access from Corporate Network

Traffic Origination	Source Address IP	Destination Address IP	Protocol	Destination Port(s)	Traffic Description
Corporate IP Network	One or more IP addresses of SOE servers on the Corporate IP Network that will be used to manage the McData fibre channel switches	IP Address of the public network interface of the Connectrix Service Processor	TCP	All high ports (1024 – 65535), and port 80	Connectrix Manager proprietary
Connectrix Service Processor	IP Address of the public network interface of the Connectrix Service Processor	One or more IP addresses of SOE servers on the Corporate IP Network that will be used to manage the McData fibre channel switches	TCP	All high ports (1024 – 65535)	Connectrix Manager proprietary