Wholesale Partner Technical Guide

6/10/2025

Wholesale Customer Connectivity

Initiating Contact

The first step in initiating the process for establishing a connection with your company and Fidium in order to receive Daily Usage Files (DUF) is to contact your Fidium Account Manager. He/She will contact the IT Production Control Department at Fidium, who will send an Accessible Letter. The Accessible Letter requests information for contacts from your company who will be working with the Fidium's IT Network team to establish connectivity between your company and Fidium that will be used for file transfers. Once you have completed the Accessible Letter, email it to carrierbilling@fidium.com.

Connectivity

Depending on the connectivity option you chose on the Accessible Letter, Fidium's IT Billing Production will send either a Connectivity/Dedicated Circuit Access Request Form or a connectivity/VPN Access Request Form for you to complete. To begin, development connectivity will be established for all wholesale partners for testing purposes. Fidium will send test data via email during the period that connectivity is being established. Once testing is successful, a production connection will then be established.

Fidium offers the following connectivity/file transfer options:

Dedicated Circuit using NDM – The current turnaround time for this option is 6-8 weeks. Once you've selected the option to utilize a Dedicated Circuit using NDM for file transfers, Fidium IT Production Control will send a Connectivity/Dedicated Access Request form for you to complete. Once complete, the form should be sent to carrierbilling@fidium.com. The completed form will be sent to Fidium IT Security for approval. Once the Connectivity/Dedicated Access Request form has been approved by Fidium IT Security, a conference call will be scheduled to complete the Dedicated Circuit. Technical contacts from Fidium and your company should be included on this call.

VPN Tunnel using NDM -This process can be completed within a few days of receiving your completed Connectivity/VPN Access Request Form. Once you've selected the option to utilize a VPN Tunnel using NDM, Fidium IT Production Control will send a Connectivity/VPN Access Request form for you to complete. Once complete, the form should be sent to carrierbilling@fidium.com. The completed form will be sent to Fidium IT Security for approval. During the time the form is out for approval, the technical contact from your company can begin setting up your company's end of the VPN tunnel. The VPN tunnel is a Business to Business VPN connection for all wholesale partners. Configurations can be found on page two of the Connectivity/VPN Access Request Form. Once the Connectivity/VPN Access Request form has been approved by Fidium IT Security, a conference call will be scheduled to complete the VPN tunnel. Technical contacts from Fidium and your company should be included on this call. Once the call takes place, the tunnel has been established and the call has ended, the Fidium IT Network team member will contact the technical member from your company to exchange a Pre-Shared Key. The information will be stored on both ends of the tunnel. At this point, the VPN tunnel will be complete and ready to test sample files using NDM.

Pre-Shared Key Exchange

If your company will be using a VPN tunnel for file transfers, a member of the Fidium Network IT team will contact the technical contact from your company to exchange a Pre-Shared key. This should be done with only the two technical contacts over the telephone.

VPN Tunnel using SFTP – This process can be completed within a few days of receiving your completed Connectivity/VPN Access Request Form.

If your file transfer option includes sftp you will need to generate a pair of Secure Keys. This process will generate both a public and private key. The public key should be emailed to carrierbilling@fidium.com.

Generating Secure Keys - When the user tries to authenticate him/herself, the server checks for matching public keys and sends a challenge to the user end. The user is authenticated by signing the challenge using her private key.

Remember that your private key file is used to authenticate you. Never expose your private keys. If anyone else can access your private key file, they can attempt to login to the remote host computer as you, and claim to be you. Therefore it is extremely important that you keep your private key file in a secure place and make sure that no one else has access to it.

Once you've selected the option to utilize a VPN Tunnel using SFTP, Fidium IT Production Control will send a Connectivity/VPN Access Request form for you to complete. Once complete, the form should be sent to carrierbilling@fidium.com. The completed form will be sent to Fidium IT Security for approval. During the time the form is out for approval, the technical contact from your company can begin setting up your company's end of the VPN tunnel. The VPN tunnel is a Business to Business VPN connection for all wholesale partners. Configurations can be found on page two of the Connectivity/VPN Access Request Form. Once the Connectivity/VPN Access Request form has been approved by Fidium IT Security, a conference call will be scheduled to complete the VPN tunnel. Technical contacts from Fidium and your company should be included on this call. Once the call takes place, the tunnel has been established and the call has ended, the Fidium IT Network team member will contact the technical member from your company to exchange a Pre-Shared Key. The information will be stored on both ends of the tunnel. At this point, the VPN tunnel will be complete and ready to test sample files using SFTP.

Pre-Shared Key Exchange

If your company will be using a VPN tunnel for file transfers, a member of the Fidium Network IT team will contact the technical contact from your company to exchange a Pre-Shared key. This should be done with only the two technical contacts over the telephone.

File Retrieval – Username & Password

Once all required forms/public key information has been received by Fidium and connectivity has been established, you will be issued a username and password that will be used to log into a directory that has been created for your company by Fidium IT in order to retrieve your files.

Please email carrierbilling@fidium.com with any questions you may have regarding this process.

AccessibleLetterExample

Name of your Company: XYZ Company

ACNA: Access Carrier (or Customer) Abbreviation

CIC: Carrier Identification Code

List of OCNs: Operating Company Number

Type of Business: Independent Tel. Co/UNE-P/ Reseller/CLEC/Other (please specify)

Is there a specific file-naming convention you need Fidium to follow, when the files are sent to you? Please provide the details. Also, please specify the file-naming convention, if any, that you use for sending files to Fidium.

Example

State	File Name Requested
ME	DUF.101708.ME
NH	DUF.101708.NH
VT	DUF.101708.VT

Via what method are you expecting to send/receive these files?
If the method is FTP/SFTP, please provide the IP address of the machine/server.

What method of transmission are you planning to use in order to retrieve your files from Fidium?

- NDM – Network Data Mover (Known at Fidium as Connect: Direct)
- SFTP – Secure (SSL) File Transfer Protocol

If you are using an outside vendor to send/receive your data files please provide the following:

Vendor Name:
Vendor Data Center Address:
Vendor Email:
Vendor Telephone Number

If you currently use a vendor to process your files, please provide their contact information above. Please note: If you do not use a vendor for all of your files, please note which files your vendor processes for you in this section.

Contact with Your Company that will be implementing a connection between your company and Fidium.

Name:
Address:
Telephone Number:
Email:

Please provide the contact information for the technical support person from your company who will be establishing either a Dedicated Circuit or a VPN Tunnel with Fidium.

Please provide a general contact for your company who is responsible for retrieving files from Fidium:

Name:
TelephoneNumber:
Email:

Please list a contact for your company for after-hours emergencies below:

<u>After Hours Contact</u>
Name:
TelephoneNumber:
Email:

Are you connected through a Mainframe or a PC type of system?

Please list what type of equipment will you be using to retrieve files from Fidium.

If your platform is a PC or Unix System please provide the directory where you would like to have the files sent

Directory:
Sub-directories:

List a directory/sub-directory where you would like Fidium to send your files.

SAMPLE

Connectivity / VPN Access Request Form

Please complete all required information

Type of VPN Access Requested:

x Business-to-Business VPN: Used for Wholesale Customer Connections

- For more than 5 concurrent users
- Application-to-application connections available
- VPN Tunnel

☐ Client / SSL VPN

- Appropriate for 5 or less concurrent users
- Application-to-application connections available
- Local area network (LAN) printing may be allowed

☐ Other _____

If this is a B2B VPN Request:

- Review Fidium standards for B2B VPN connections in **Addendum A**.
- Complete the information requested in **Addendum B**.

If this is a Client / SSL VPN Request:

- Complete the information requested in **Addendum C**.

This area contains necessary information required to establish your end of the VPN tunnel

ADDENDUM A – Fidium Standards for B2B VPN

IKE Policies (**DO NOT MODIFY**)	PHASE 1	
Parameter		**Value**
Message encryption algorithm		**Triple-DES**
Message integrity (hash) algorithm		**SHA**
Peer authentication method		**Preshared key**
Key exchange parameters (Diffie-Hellman group identifier and Perfect Forward Secrecy Group)		**Group 2 (1024-bit)**

NOTE:

Fidium will provide the pre-shared key to be used with each Supplier.

Fidium reserves the right to change this key and/or the method for obtaining this key at its discretion.

IPSec Parameters (**DO NOT MODIFY**)	PHASE 2	
Parameter		**Value**
Security-association (SA) establishment		**Ipsec-isakmp (IKE)**
IPSec Mode		**Tunnel**
Mechanism for payload		**ESP**
ESP transform		**ESP-3DES**
Hashed Message Authentication Code		**ESP-SHA-HMAC**

Please complete all highlighted areas on this page

ADDENDUM B – Business-to-Business VPN Connection

Addendum B	**Date Requested:**
Company :	**Communication**
Contact Name	**John Doe**
Contact Email:	**John.Doe@Communication.com**
Contact Phone:	**123-456-7890**
How many users will be using the B2B VPN connection?	**1**
What is your external, Internet-facing IP address(s)?	**1.2.3.4 (Public IP Address)**
Peer Address:	**1.2.3.4 (VPN or Firewall External Address)**
Peer Network:	**5.6.7.8 (NATed or public IP)**
Technical Contact Name:	**John Doe**
Technical Contact Email:	**John.Doe@Communication.com**
Technical Contact Phone:	**123-456-7890**
Technical Contact Cell Phone:	**123-456-7890**
What type of device (make/model) do you plan to terminate your VPN connection on?	**Cisco ASA 5520**
What type of connection do you have to the Internet? (e.g. leased line, DSL, dial-up)	**I Gig**
Do you have an existing connection (private line circuit, VPN, etc.) between your company and Fidium or it's affiliates? If yes, what networks' IP addresses of yours do we route to via that connection? Will this new VPN be replacing this connectivity, or are we introducing a new route to you via the tunnel?	**No**
What are the Fidium network addresses you will you need to access? **Note:** **This should be a summary of the Fidium Networks identified by the System/Application/ or Business owner** ***** If unsure, please ask your Fidium Sponsor as you will need this information to configure your end of the VPN Tunnel.**	9.10.11.12/32

	Addendum B to be completed by Fidium personnel	

ADDENDUM B – Business-to-Business VPN Connection (cont.)

Fidium Supervisor or Above:	**Date:**
Title:	**Department:**
Email:	**Phone:**
Business Purpose of Access:	
Duration of Access: from (Date): **To (Date):** **Note: Needs to be re-verified every 6 months**	
Fidium Employee Contact Name:	
Site Location:	**Title**
Email:	**Telephone:**
Has the Fidium Mutual Confidentiality and Non-Disclosure Agreement been signed by this vendor? (Required): ☐ **Yes** ☐ **No**	
Please provide VPN access for the above. I understand that I will be held responsible for all actions of the group/individual in accessing the Fidium Network. **All signatures (on the Signature Page Only, page 6 of 6) are required for approval. Please print, sign and return completed form via fax to Fidium IT Security Director**	

No information needed from wholesale customers on this page

ADDENDUM C – Client / SSL VPN Request: Access

Company :			Client		SSL VPN Request Type
Date of Request:					
Individuals Name:		**Individuals Title:**			
Individuals Email:		**Individual Phone:**			
Individual Signature:					
Host IP(s) / System/ or Application on Fidium side (s): *****If unsure, please ask your Fidium Sponsor as you will need this information to complete the request**					
Supervisor's Name:		**Supervisor's Title:**			
Supervisor's Email:		**Supervisor's Phone:**			
Supervisor Signature:					
Business Purpose of Access:					
Duration of Access: from (Date): **To (Date):** **Note: Needs to be re-verified every 6 months**					
Fidium Employee Contact Name:					
Site Location:		**Title**			
Email:		**Telephone:**			
Has the Fidium Mutual Confidentiality and Non-Disclosure Agreement been signed by this vendor? (Required): ☐ **Yes** ☐ **No**					
Please provide group/individual VPN access for the above. I understand that I will be held responsible for all actions of the group/individual in accessing the CCI Network.					

Please print and sign your name in the Employee Vendor area on this page.

SIGNATURE PAGE ONLY

Fidium Supervisor:

Print:_____**Signature:** _____

System / Application owner:

Print:_____**Signature:** _____

Employee/Vendor:

Print:_____**Signature:** _____

Director IT Network:

Print:_____**Signature:** _____

Director of Information Security:

Print:
_____**Signature:**_____

Network Administrator who Completed Request:

Print:
_____**Signature:**_____

If needed - RSA Token Issued -

_____

IS Security Team Member who issued token:

Print:
_____**Signature:**_____

SAMPLE

CONNECTIVITY / DEDICATED ACCESS REQUEST FORM

Please complete all required information

Type of Access Requested:

☐ **Point-to-Point T1**:

ADDENDUM A – Dedicated Access Request Connection

Addendum A	
REQUESTING COMPANY INFORMAITON	
Company Name:	**Communication**
Contact Name:	**John Doe**
Contact E-mail:	**John.Doe@communication.com**
Contact Number:	**123-456-7890**
TECHNICAL CONTACT SECTION:	
Technical Contact Name:	**John Doe**
Technical Contact E-mail:	**John.Doe@communication.com**
Technical Contact Phone:	**123-456-7890**
Technical Contact Cell Phone:	**123-456-7890**
CONFIGURATION SECTION:	
Your Router Gateway Ethernet Port:	**G0/0**
IP Address on you LAN Segment	**192.x.x.x**
Your Router Serial Interface (s0/0 or s1/0):	**S1/0**
IP Address assigned to your Serial Interface	**194.165.x.x**
DNS CONFIGURATION (if required)	
Primary DNS Resolver:	**4.2.x.x**
Secondary DNS Resolver:	**4.1.x.x**
Your Circuit ID:	**DHEC-123456 xxxx**
Cisco Router Configuration:	
Encapsulation (HDLC):	**PPP**
IP Classless (in the global configuration):	**Yes**
Default Route: (0.0.0.0 0.0.0.0 Serial 1 or whatever interface is connected to your CSU/DSU or MUX.	
CIRCUIT CONFIGURATION:	
Net Signal: (ESF Extended Super Frame)	**Yes**
Line Coding: (B8ZS Bipoler 8 zeros substitution)	**Yes**
Timing: (Net from the Network)	**Serial**
Port Base Rate: (64K – 1 ch = 56k, 2 or more 64k each channel)	**N/A**
Port Speed: (1.5 mb/s Total Bandwidth Speed)	**1.54**
Channel Allocations: (Assign # 1 to 24)	**1-24**
LBO (0.0db – If cat 5 or 6 < 50ft default in most units, if > next setting 7.5db	

SIGNATURE PAGE

Fidium Supervisor:

Print:_____**Signature:** _____

System / Application owner:

Print:_____**Signature:** _____

Employee/Vendor:

Print: **John Doe** **Signature:** *John Doe*

Director IT Network:

Print:_____**Signature:** _____

Director of Information Security:

Print:
_____**Signature:**_____

Network Administrator who Completed Request:

Print:
_____**Signature:**_____

Glossary of Terms

Accessible Letter – A form used to provide necessary information for a Wholesale Partner to select a preferred delivery method and begin the process of establishing connectivity to the Fidium billing systems and begin the migration process.

ACNA - Access Carrier (or Customer) Name Abbreviation
A three-character code assigned to each Interexchange Carrier; designates the customer to which circuits are billed.

CIC - Carrier Identification Code
A unique three- or four-digit access identification code that is assigned by Telcordia Technologies for use with certain switched access services. The CIC identifies the caller's long distance carrier.

CLEC - Competitive Local Exchange Carrier
Any company or person authorized to provide local exchange services in competition with an ILEC. A CLEC provides similar or identical telecommunications services to the ILEC.

Connect: Direct -
A direct electronic method of delivering CLEC and Reseller usage data files and Reseller bills, and transmitting CLEC ASRs. Available in several platforms including NDM-MVS for mainframe and NDM-PC for personal computers. Also known as Network Data Mover (NDM).

Dedicated Circuit -
A communications cable or other facility dedicated to a specific application.

Dedicated Circuit Access Request Form - A form that provides the necessary information for a company to begin the process of establishing connectivity to the Fidium billing systems and begin the migration process.

DUF – Daily Usage Files: Daily reports providing data enabling CLECs to bill end users for usage charges incurred.

Independent Telephone Co. - An independent company providing local exchange telecommunications service.

NDM - Network Data Mover
A direct electronic method of delivering CLEC and Reseller usage data files and Reseller bills, and transmitting CLEC Access Service Requests (ASR). Available in several platforms including NDM-MVS for mainframe and NDM-PC for personal computers. Also known as Connect: Direct.

OCN - Operating Company Number (OCN)
A four-character code assigned by the National Exchange Carrier Association (NECA) to a telecommunications provider. Specifically used to identify CLEC and Reseller usage data. Also known as Company Code.

Pre-Shared Key - Cryptography, a pre-shared key or PSK is a shared secret (a piece of data only known to the parties involved in a secure communication. The shared secret can be a password, a passphrase, a big number or an array of randomly chosen bytes. A Pre-Shared Key is only used for VPN connections.

Reseller - A business entity that purchases telecommunications services at wholesale and sells them to third parties; a service provider that does not own transmission facilities, but obtains communications services from a carrier for resale to the public for profit. Also known as a Resale Carrier.

Secure Key - Based on the use of digital signatures. Each user creates a pair of 'key' files. One of these key files is the user's public key, and the other is the user's private key. The server knows the user's public key, and only the user has the private key.

Glossary of Terms Continued

SFTP – A network protocol designed to provide secure file transfer and manipulation facilities over the secure shell (SSH) protocol.

UNE - Unbundled Network Element
Specific equipment and facilities that are "unbundled" from traditional end-to-end services (such as residential dial tone service) in order to allow other local exchange carriers to use components of another network. An example of a network element would be a loop connected to a competitor carrier's switch.

UNE-P - Unbundled Network Element-Platform
A service offering that combines elements that can be used to build a variety of platforms. UNE- P is also known as 'platform'.

VPN Access Request Form - A form that provides the necessary information for a company to begin the process of establishing connectivity to the Fidium billing systems and begin the migration process.

VPN Tunnel - A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The link-layer protocols of the virtual network are said to be tunneled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features.