MyFloridaNet-2 (MFN-2)
Remote Access VPN Reference Guide

15 November 2018

Document Control Number: 7055011
Contract Number: DMS-13/14-024

Prepared for:

Florida Department of Management Services
Division of Departmental Purchasing
4050 Esplanade Way, Suite 355.F
Tallahassee, FL 32399-0950

Prepared by:

HARRIS CORPORATION

Government Communications Systems
P.O. Box 37
Melbourne, FL USA 32902-0037

REVISION RECORDS

REVISION	DATE	DESCRIPTION
0	22 January 2018	Initial Submittal.
1	31 January 2018	Addressed comments from DMS.
–	07 February 2018	All DMS Comments incorporated and accepted. Initial Formal Release.
A	15 November 2018	Addition of CSAB ordering details per Derek Howard at DMS, modification of Client-to-LAN client installation instructions to reflect a more streamlined process, and the option of ordering additional tokens.

TABLE OF CONTENTS

Paragraph	Title	Page
1	INTRODUCTION	1
2	REMOTE ACCESS VPN	2
2.1	Ordering a Remote Access VPN	2
2.2	Downloading and Installing the RSA SecurID Token Application	2
2.3	Import the Token	6
2.4	Register the Token and Create a PIN	9
3	ACCESSING THE VIRTUAL PRIVATE NETWORK (VPN)	12
3.1	Clientless VPN	12
3.2	Client-to-LAN	13
3.2.1	Cisco AnyConnect Secure Mobility Client Installation	14
3.2.2	Cisco AnyConnect Manual Installation	19
3.2.3	Cisco AnyConnect ISE Compliance Installation	22
4	ORDERING NEW CLIENTLESS AND CLIENT-TO-LAN VPNS IN THE CSAB	25
4.1	Clientless	25
4.2	Client-to-LAN	32
4.3	Creating a VPN Profile	33
5	MIGRATING VPNS IN THE CSAB	38

LIST OF ILLUSTRATIONS

Figure **Title** **Page**

Figure 2.2-1. Downloaded RSA SecurID Software Token 3
Figure 2.2-2. Extracted RSA Token File 3
Figure 2.2-3. Run the Installer File 4
Figure 2.2-4. RSA SecurID Software Token Setup Wizard 4
Figure 2.2-5. Accept License Agreement 5
Figure 2.2-6. Typical Setup 5
Figure 2.2-7. Click to Install 6
Figure 2.3-1. Emailed Token Zip File 6
Figure 2.3-2. Extracted Token Zip File on Desktop 7
Figure 2.3-3. Open RSA SecurID Token Application 7
Figure 2.3-4. Import from File 7
Figure 2.3-5. Navigate to Folder on Desktop 8
Figure 2.3-6. OK to Import 8
Figure 2.3-7. Enter Token Password 8
Figure 2.3-8. Leave the Token Name As Is 9
Figure 2.3-9. Token Display 9
Figure 2.4-1. Register Token Link 9
Figure 2.4-2. RSA Self-Service Console 10
Figure 2.4-3. Passcode Text Box 10
Figure 2.4-4. PIN Creation 11
Figure 2.4-5. RSA My Account Page 11
Figure 3.1-1. VPN Login Page 12
Figure 3.1-2. Custom VPN Links Example 13
Figure 3.1-3. VPN Logout Page 13
Figure 3.2.1-1. Cisco AnyConnect Secure Mobility Client Download 14
Figure 3.2.1-2. Internet Explorer Prompt for Add-On 14
Figure 3.2.1-3. Downloader 15
Figure 3.2.1-4. Download Error 15
Figure 3.2.1-5. Internet Explorer Internet Options 15
Figure 3.2.1-6. Trusted Sites 16
Figure 3.2.1-7. Add Trusted Site 16
Figure 3.2.1-8. Update Java 17
Figure 3.2.1-9. Run Java Installation File 17
Figure 3.2.1-10. Cisco AnyConnect Installation 17
Figure 3.2.1-11. Connection Established 18
Figure 3.2.1-12. VPN Connect 18
Figure 3.2.1-13. Entering Credentials 19
Figure 3.2.1-14. VPN Connected 19
Figure 3.2.2-1. Unsuccessful Web-Based Installation 19
Figure 3.2.2-2. Run Installer File 20
Figure 3.2.2-3. Cisco AnyConnect Secure Mobility Client Wizard 20
Figure 3.2.2-4. Finish the Installation 21

LIST OF ILLUSTRATIONS

Figure **Title** **Page**

Figure 3.2.2-5. Connect to VPN 21
Figure 3.2.2-6. Enter Credentials 22
Figure 3.2.2-7. Successful VPN Connection 22
Figure 3.2.3-1. System Scanning 23
Figure 3.2.3-2. Compliant System 23
Figure 3.2.3-3. Non-Compliant System 24
Figure 3.2.3-4. Windows Update Needed Example 24
Figure 4.1-1. CSAB Ordering 25
Figure 4.1-2. Remote Access VPN 26
Figure 4.1-3. Billing Information 26
Figure 4.1-4. Ordering Proxied Clientless (SSL) 27
Figure 4.1-5. Contact and User Information 29
Figure 4.1-6. Verify and Add to Cart 30
Figure 4.1-7. Checkout or Save, Delete, Reconfigure 31
Figure 4.1-8. Preferred Delivery Date 31
Figure 4.2-1. Ordering Client-to-LAN with Split Tunneling and Extra Tokens 32
Figure 4.2-2. Verify and Add to Cart 33
Figure 4.2-3. Checkout or Save, Delete, Reconfigure 33
Figure 4.3-1. VPN Profile 34
Figure 4.3-2. Billing Information 35
Figure 4.3-3. New VPN Profile and VRF 35
Figure 4.3-4. VPN Profile Configuration 36
Figure 4.3-5. Attach File If Necessary 37
Figure 4.3-6. Verify and Add to Cart 37
Figure 4.3-7. Checkout or Save, Delete, Reconfigure 38
Figure 4.3-8. Preferred Delivery Date 38
Figure 5-1. CSAB Inventory 39
Figure 5-2. VPN By Service 39
Figure 5-3. Start Provider Migration 40
Figure 5-4. Execute Action 40
Figure 5-5. Go to Ordering 41
Figure 5-6. Edit Configuration 41
Figure 5-7. Enter Contact Information 42
Figure 5-8. Add to Cart 43
Figure 5-9. Check Out 44
Figure 5-10. Submit Order 45

1 INTRODUCTION

The purpose of this guide is to provide the MFN-2 customer end user with instructions on remote VPN access. The two options of remote access VPN for customers is the Clientless version, which allows the user to access preconfigured web resources via a web browser, and the Client-to-LAN version, which requires the Cisco AnyConnect Secure Mobility Client application. Both options require multifactor authentication and must be approved by the Department of Management Services (DMS).

The VPN account creation process includes the download and installation of a software token, which is used with a PIN and the user's username to provide multifactor authentication protection. Once a user has VPN access, they can reach resources on their agency network remotely.

The credentials generated during the VPN account creation process are the same as used for Customer Portal access, however, a Customer Portal account is not necessary for VPN access. Remote VPN access is ordered via the Communication Services Authorization and Billing (CSAB) system, while a Customer Portal account, typically used only by agency networking staff, is obtained via a Customer Portal request form submitted by the agency's Security Administrator.

In addition to the software token, Client-to-LAN VPN access requires the Cisco AnyConnect Secure Mobility Client be downloaded and installed on the VPN client device. The Clientless method of VPN connectivity uses the Internet to connect and does not require the download of a client application.

Users should contact the MFN-2 NOC/SOC at +1 (844) 548-MFN2 (6362) if they have any difficulty with these instructions. Once connected, press 2 to reach the Security Operations Center (SOC).

NOTE:

The RSA soft token installation and the Cisco AnyConnect Secure Mobility Client installation both require administrator rights on the device on which they are being installed. If the user does not have administrator rights on the device, assistance from their Information Technology department will likely be necessary.

2 REMOTE ACCESS VPN

Remote access VPNs connect a remote user's device, via an encrypted tunnel to a VPN gateway (firewall) at the Internet Access Gateways (IAGs) at the Miami or Tallahassee2 core nodes. The tunnel is decrypted on the gateway, and the traffic is then mapped to the appropriate VRF and sent to the agency's Customer Edge (CE) router. This access requires a VPN order as well as the download and install of a software token as outlined in this section.

2.1 Ordering a Remote Access VPN

The remote VPN access process begins when an MFN-2 agency representative orders VPN access for an authorized VPN user in the CSAB. VPN accounts must be associated with a VPN Profile, which lists the IP addresses the user will have access to once connected to the VPN, and the VRF to which the profile is associated. VPN Profiles are also ordered in the CSAB and must be approved by DMS before the remote access VPN order can be completed. Details on the VPN order process and VPN Profile creation are covered in Section 4 of this document.

Once the remote access VPN order is complete, the MFN-2 NOC/SOC creates the user's account and emails the user with:

- A username
- A link to the RSA SecurID Token application
- A token.zip file
- A password to unlock the token.zip file

The soft tokens are available for Apple, Android, or Windows computer. Administrative permissions are required on whichever platform is selected.

NOTE:

An RSA token is associated with the device on which it is installed and cannot be used on additional devices. If a user will be connecting via VPN from multiple different devices, it is best to order the soft token for a mobile device, such as a cell phone. If desired, the user has the option of ordering up to two additional tokens.

2.2 Downloading and Installing the RSA SecurID Token Application

NOTE:

DMS users with hard tokens should skip to Section 2.4 of this document and register the token and create a PIN as described there.

NOTE:

The following instructions in this Section 2 are for downloading and installing the token on a Windows computer. The steps will be slightly different on an Apple or Android device.

To download the RSA SecurID soft token, open the **Internet Explorer** browser, navigate to the following URL and click **Save** when prompted to save the zip file.

https://community.rsa.com/docs/DOC-73395.

By default, the file will save to the **Downloads** folder, as shown in Figure 2.2-1.

Figure 2.2-1. Downloaded RSA SecurID Software Token

When the download is complete, navigate to the **Downloads** folder, and right click the **.zip** file and click **Extract All**. Click **Extract** to extract the file in the destination location listed, which should be an RSASecurIDSoftwareToken folder in the Downloads folder.

Double-click the extracted **RSASecurIDSoftwareToken** folder, then double-click the **RSASecurIDToken** folder inside, and then double click the **RSASecurIDToken** folder inside that. There should be two .msi files, as shown in Figure 2.2-2. Double-click the **RSASecurIDToken502.msi** file and click **Run** as shown in Figure 2.2-3.

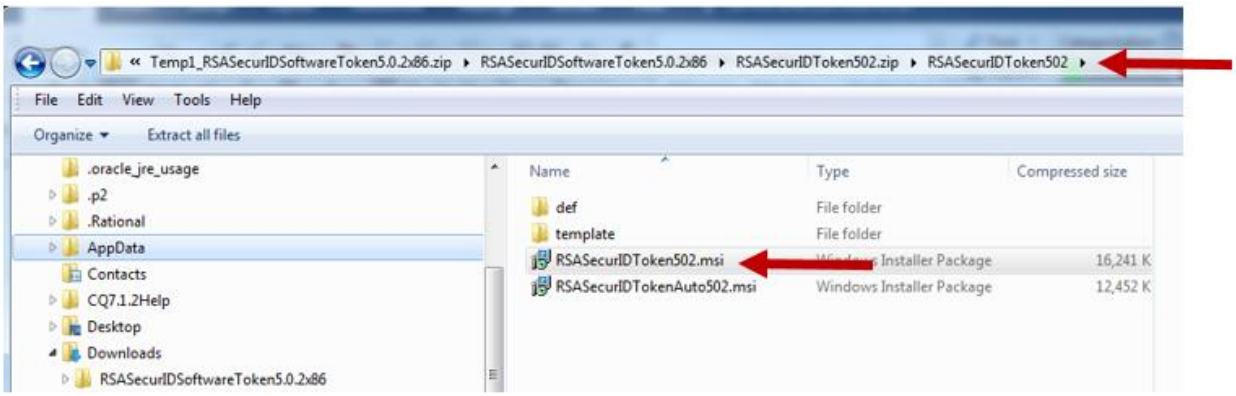

Figure 2.2-2. Extracted RSA Token File

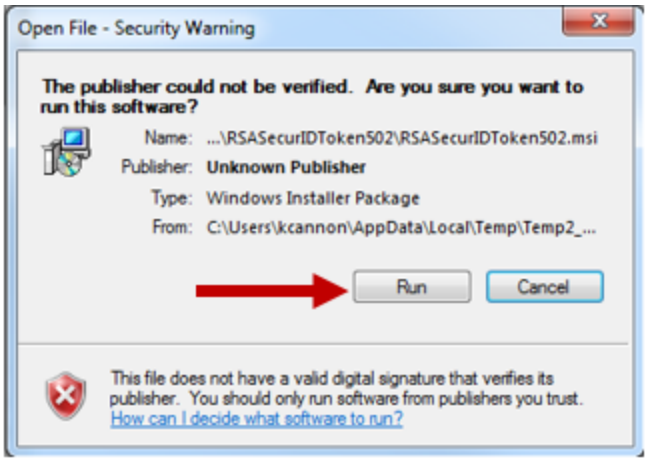

Figure 2.2-3. Run the Installer File

Follow the wizard to install the token as shown in Figure 2.2-4, Figure 2.2-5, Figure 2.2-6, and Figure 2.2-7. Choose **Typical** when prompted for Setup Type. You may be asked to enter administrator credentials on the client device. Administrator access is required. Click **Finish** when the setup wizard has completed the install.

Figure 2.2-4. RSA SecurID Software Token Setup Wizard

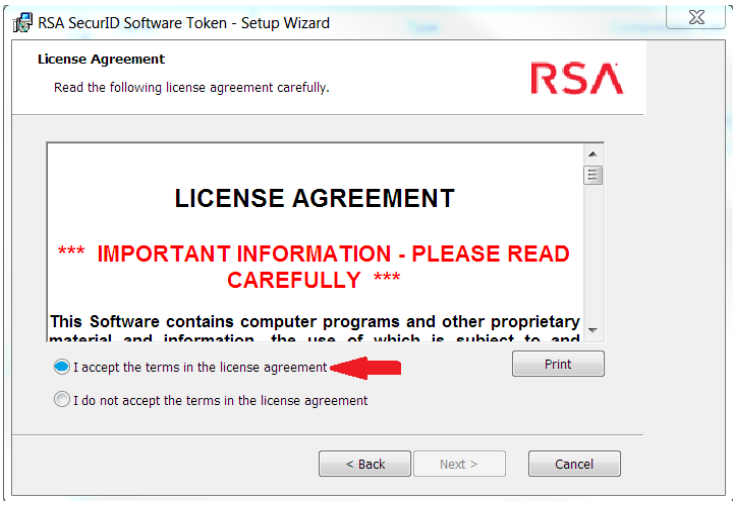

Figure 2.2-5. Accept License Agreement

Figure 2.2-6. Typical Setup

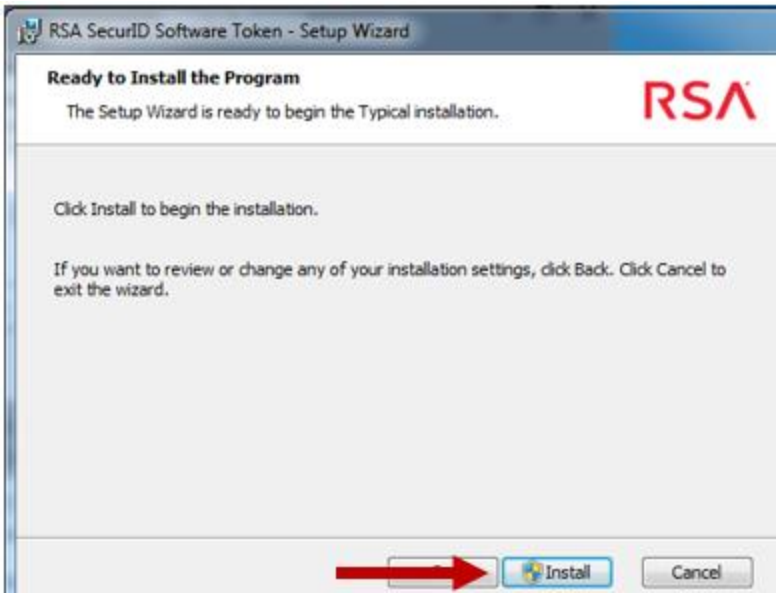

Figure 2.2-7. Click to Install

2.3 Import the Token

Once the application has been installed, the user's token file must be imported into it. Locate the **software_token.zip** file received via email as shown in the redacted version in Figure 2.3-1, and click the dropdown arrow beside it, and then click **Save As** and save it to the **Desktop**. Right-click the **software_token.zip** file just saved and click **Extract All**. Click **Extract** to extract the file to the Desktop, as shown in Figure 2.3-2.

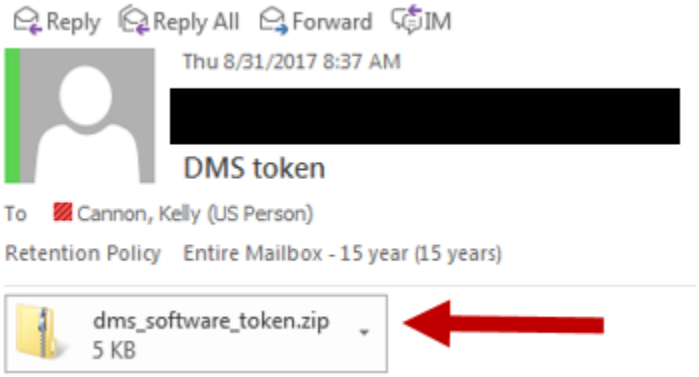

Figure 2.3-1. Emailed Token Zip File

Figure 2.3-2. Extracted Token Zip File on Desktop

Click the Windows **Start** button, and click the **RSA SecurID Token** application to run it, as shown in Figure 2.3-3.

Figure 2.3-3. Open RSA SecurID Token Application

Click **Import from File** as shown in Figure 2.3-4. Next, click **Browse** and navigate to the **Desktop.** Locate the **dms_software_token** folder, and double-click it as shown in Figure 2.3-5. Then click the **.sdtid** file inside of that folder and click **Open**. Click **OK** as shown in Figure 2.3-6. A password prompt displays.

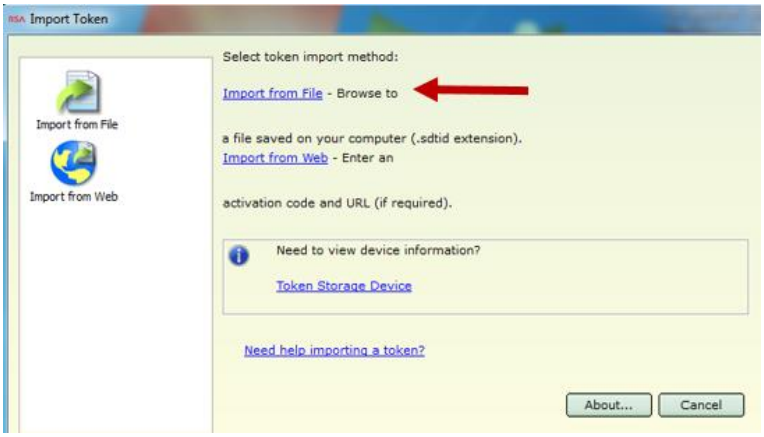

Figure 2.3-4. Import from File

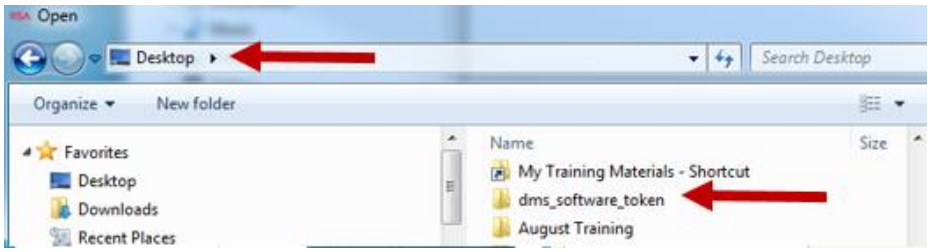

Figure 2.3-5. Navigate to Folder on Desktop

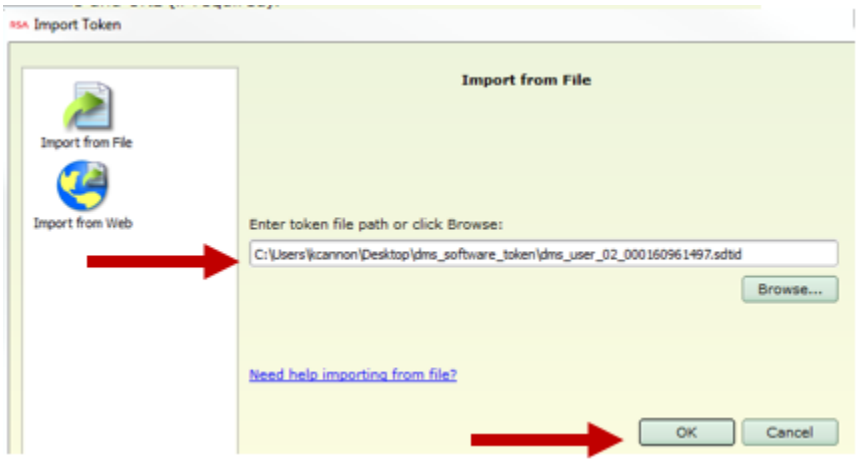

Figure 2.3-6. OK to Import

Navigate to the **email** that contains the password for the RSA SecurID token – this is a different password than the user's password. Enter the emailed **password**, as shown in Figure 2.3-7, and then click **OK**. Once the token has successfully imported, the user is prompted to change the name of the token, as shown in Figure 2.3-8. Click **OK** to leave the name unchanged. Figure 2.3-9 displays a successfully imported token.

Figure 2.3-7. Enter Token Password

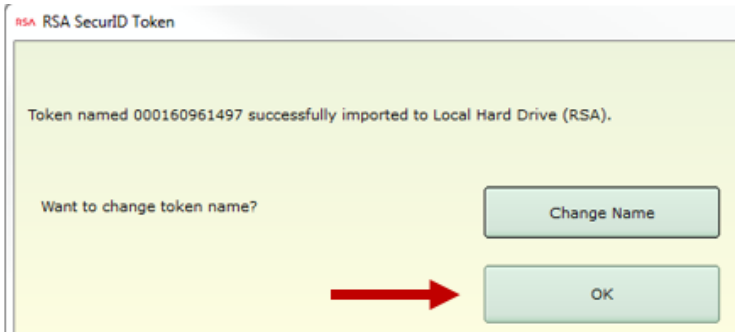

Figure 2.3-8. Leave the Token Name As Is

Figure 2.3-9. Token Display

2.4 Register the Token and Create a PIN

Once the RSA SecurID software token has been successfully installed, a PIN that is known only to the user must be created.

Open **Internet Explorer** and navigate to https://portal.mfn2.myflorida.com. Click **Register Token**, as shown in Figure 2.4-1. RSA Self-Service Console as shown in Figure 2.4-2.

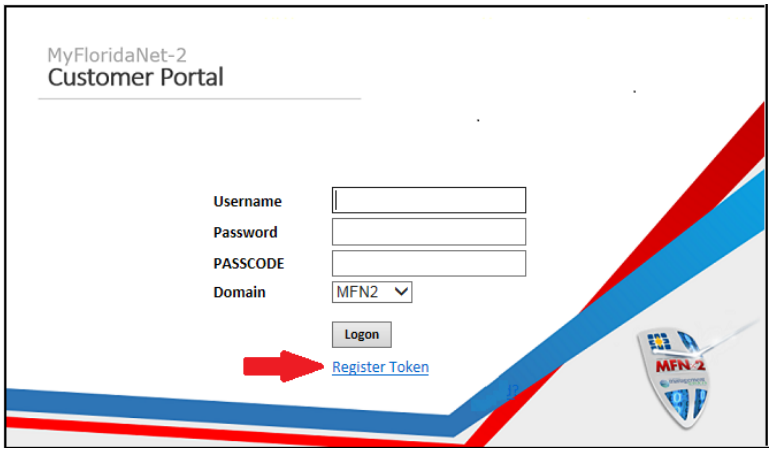

Figure 2.4-1. Register Token Link

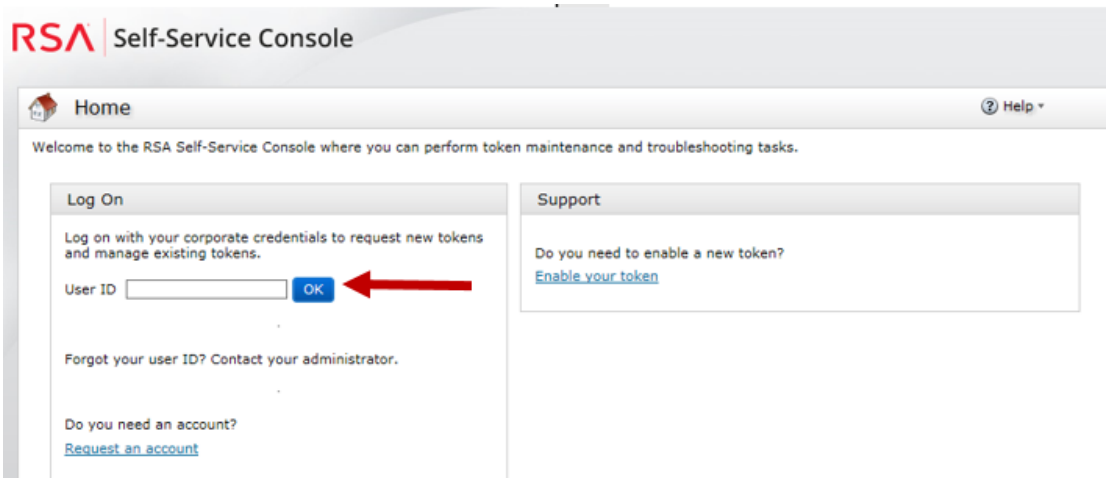

Figure 2.4-2. RSA Self-Service Console

Enter the **User ID** (username) and click **OK**, and a Passcode text box appears as shown in Figure 2.4-3. Enter the **six digits** currently displayed in the **RSA SecurID Token** application into the **Passcode** text box and click **Log On**.

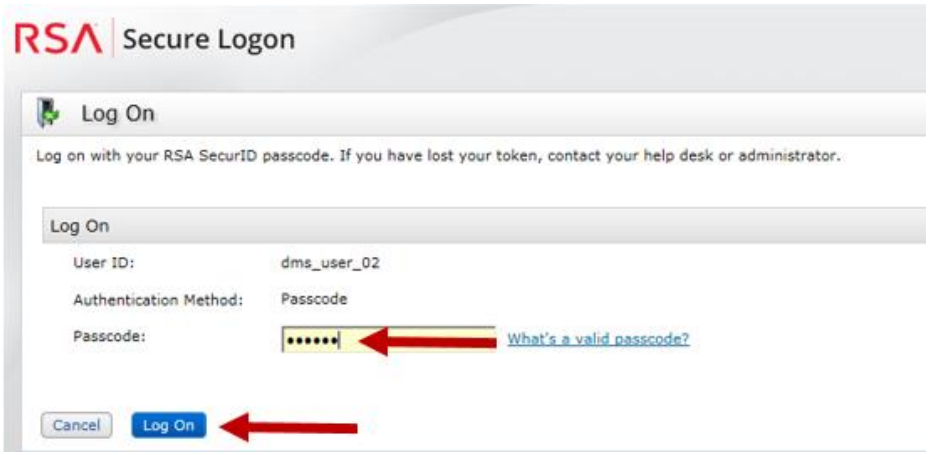

Figure 2.4-3. Passcode Text Box

Figure 2.4-4 displays the next screen which prompts for a **PIN**. While the system supports several characters, we recommend setting a four-digit PIN not related to any personally identifiable information. Enter the **PIN** into the **New PIN** and the **Confirm New PIN** text boxes. Finally, wait **60 seconds** or until the tokencode changes on the RSA SecurID token, and enter the new code into the **Next Tokencode** text box. Click **OK** to complete the token and PIN creation process.

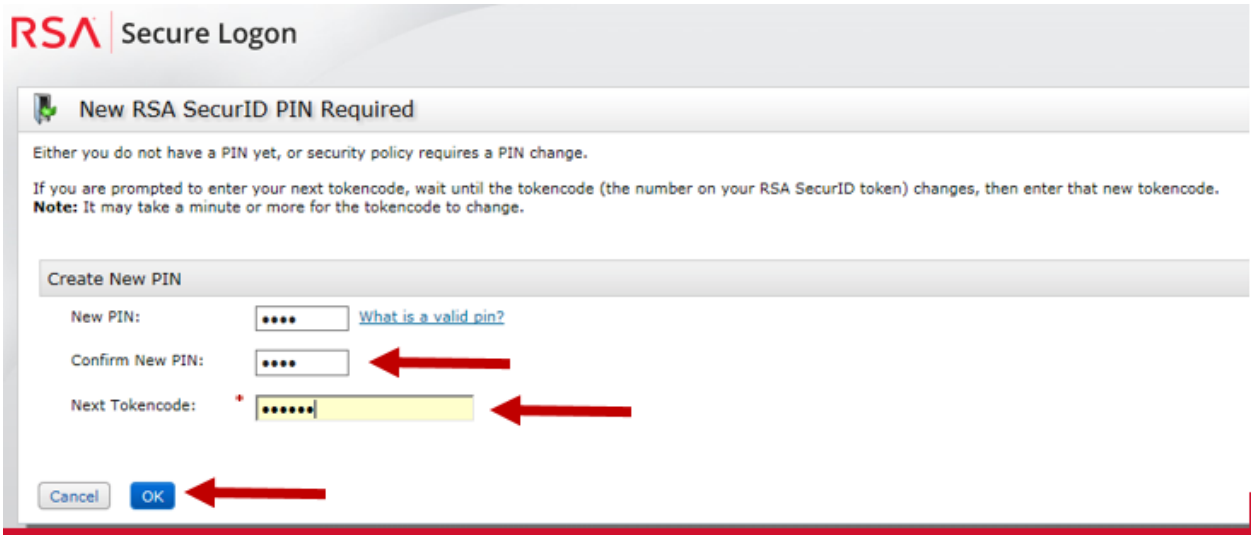

Figure 2.4-4. PIN Creation

Figure 2.4-5 displays an example of the My Account page resulting from the token registration process. There may be a yellow **Notes** area on the page that suggests the user should set up emergency authentication questions. At this time, these questions are not being used. The user can ignore this.

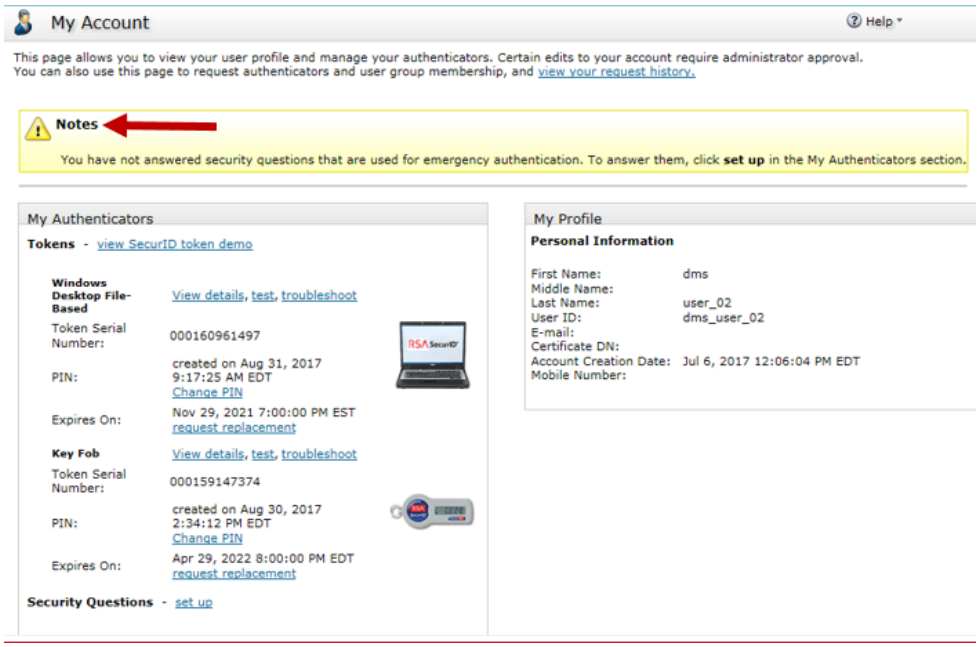

Figure 2.4-5. RSA My Account Page

3 ACCESSING THE VIRTUAL PRIVATE NETWORK (VPN)

Customers who have ordered a Clientless VPN should follow instructions in Section 3.1 to connect to the VPN. Customers who have ordered a Client-to-LAN VPN connection should follow instructions in Section 3.2.

3.1 Clientless VPN

No client software installation is necessary for MFN-2 network access when using the Clientless VPN option. To access the VPN using the Clientless option, customers navigate to the VPN login page at https://vpn.mfn2.myflorida.com using the **Internet Explorer** (preferred) web browser. To login, enter a **username** (lowercase) and **password**, and click **Login**. Figure 3.1-1 displays an example for a DMS test account. Note that in this context, PASSWORD refers to the user's **PIN plus token** code.

If Internet Explorer does not trust the VPN concentrator website, the user will see an **IN CASE OF A SECURITY ERROR** dialog box. If this happens, click **Internet Explorer's Tools** menu and then click **Internet Options** as shown in Figure 3.2.1-5. Click the **Security** tab and then click **Trusted Sites** and then the **Sites** button as shown in Figure 3.2.1-6. Click **Add** to add the https://vpn.mfn2.myflorida.com site as shown in Figure 3.2.1-7 and click **Close**, and then click **OK**. Refresh the screen and start the process again.

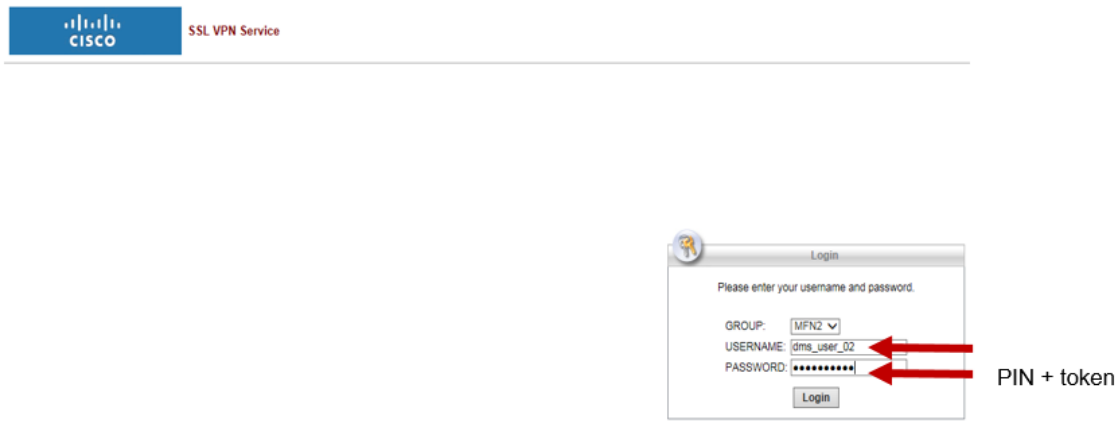

Figure 3.1-1. VPN Login Page

A successful login will land the user at a webpage hosting custom links to the agency's resources, as provided by the agency. An example is shown in Figure 3.1-2. The user should click **Logout** when the VPN session is no longer in use.

Clicking **Logout** navigates the user to the page displayed in Figure 3.1-3. If the user clicks **Logon**, they will return to the VPN login page as shown in Figure 3.1-1.

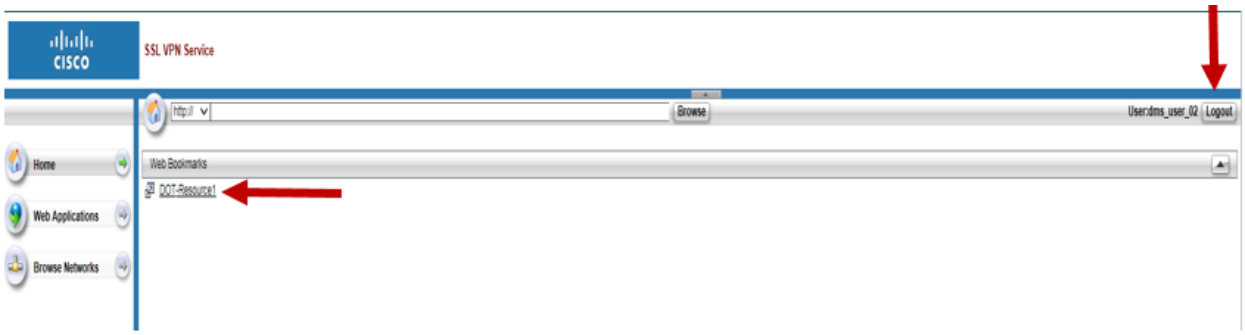

Figure 3.1-2. Custom VPN Links Example

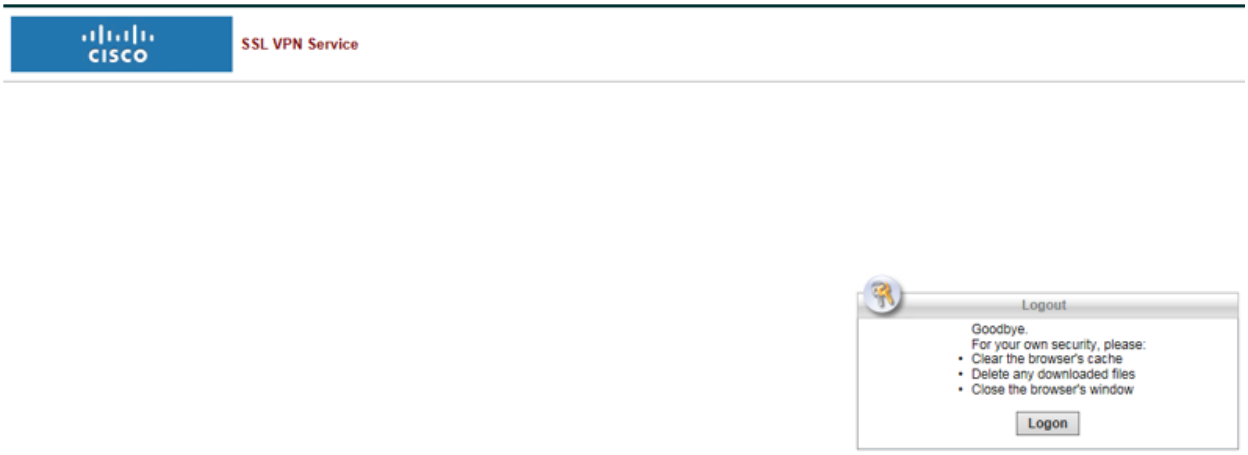

Figure 3.1-3. VPN Logout Page

3.2 Client-to-LAN

The Client-to-LAN option of remote access involves a download and installation of both the Cisco AnyConnect Secure Mobility Client, and the Cisco AnyConnect ISE Compliance software. The first application is the VPN connection component. The second is the application that scans the client device to assure its operating system and antivirus are up-to-date.

NOTE:

These installs are only necessary once per device.

NOTE:

Client devices under the control of their agency may have difficulty installing and using the Cisco AnyConnect Security Mobility Client due to agency policies and settings that reflect device location.

3.2.1 Cisco AnyConnect Secure Mobility Client Installation

The VPN login page is accessed in the same manner for both the Clientless and Client-to-LAN options, by navigating in **Internet Explorer** to https://vpn.mfn2.myflorida.com as shown in Figure 3.1-1. If, instead of Clientless, an MFN-2 customer has ordered the Client-to-LAN option in CSAB, the MFN-2 VPN concentrator will, upon successful login, attempt to automatically download the Cisco AnyConnect Secure Mobility Client, Cisco AnyConnect ISE Posture Module, Cisco AnyConnect ISE Compliance Module, and Cisco AnyConnect Diagnostics and Reporting Tool. Initially, the system detects the client platform and begins analyzing the client device, as shown in Figure 3.2.1-1. In the next few minutes ActiveX and Java are detected.

At this point, the user may be prompted to install an add-on as displayed in Figure 3.2.1-2. Click **Install** to accept the add-on installation. The user may be asked for permission and possibly administrator level credentials for the client device, which the user should supply. If the process is successful, the Cisco AnyConnect Secure Mobility Client application will begin downloading as shown in Figure 3.2.1-3.

Figure 3.2.1-1. Cisco AnyConnect Secure Mobility Client Download

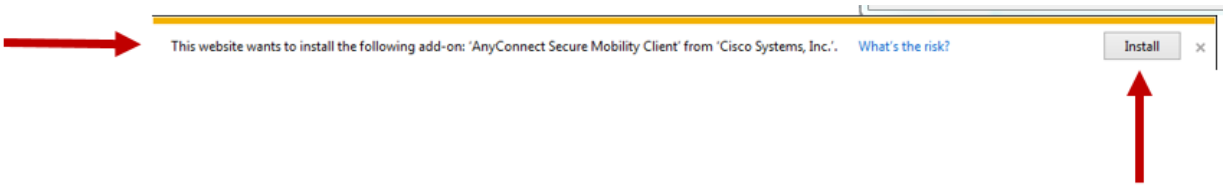

Figure 3.2.1-2. Internet Explorer Prompt for Add-On

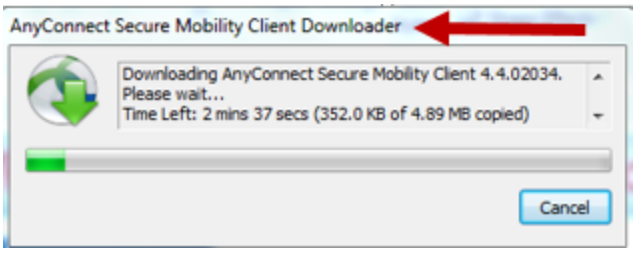

Figure 3.2.1-3. Downloader

In the event the user encounters a problem during the download, it is most likely due to Internet Explorer not trusting the VPN concentrator website. If this happens, the user will see the message shown in Figure 3.2.1-4. If there is no issue and the process is successful, the user will see a successful connection as shown in Figure 3.2.1-11.

If Internet Explorer does not trust the VPN concentrator website, the user will see an **IN CASE OF A SECURITY ERROR** dialog box. Click **OK** to close the dialog. Next, click the **Tools** menu and then click **Internet Options** as shown in Figure 3.2.1-5. Click the **Security** tab and then click **Trusted Sites** and then the **Sites** button as shown in Figure 3.2.1-6. Click **Add** to add the https://vpn.mfn2.myflorida.com site as shown in Figure 3.2.1-7 and click **Close**, and then click **OK**. Refresh the screen and start the process again.

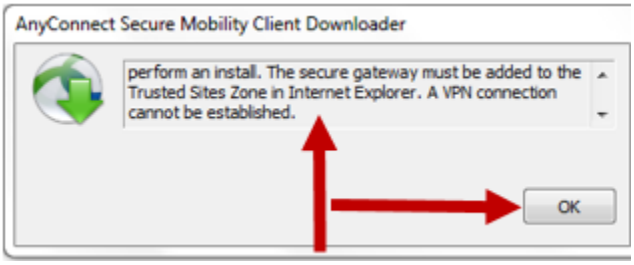

Figure 3.2.1-4. Download Error

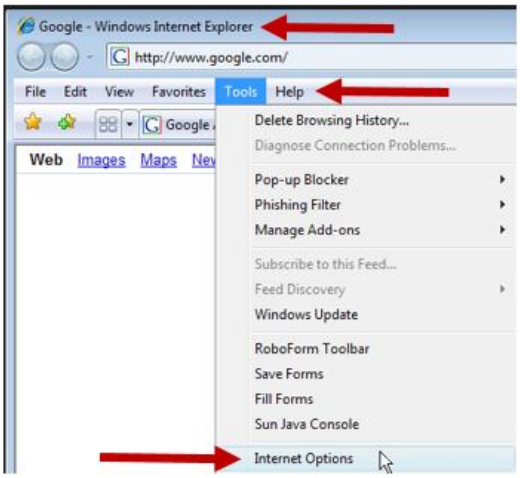

Figure 3.2.1-5. Internet Explorer Internet Options

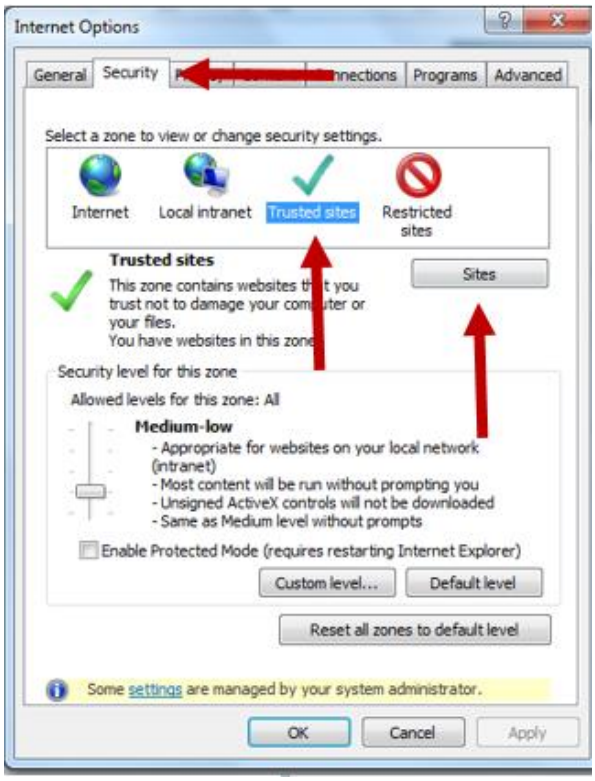

Figure 3.2.1-6. Trusted Sites

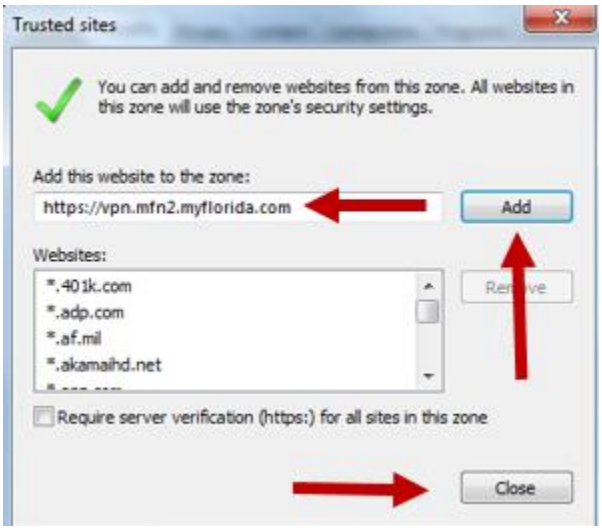

Figure 3.2.1-7. Add Trusted Site

Another issue that may arise during the automatic download and install process is an outdated version of Java, as shown in Figure 3.2.1-8. If this occurs, click **Update** to update the Java application, entering administrative credentials if prompted.

Figure 3.2.1-8. Update Java

Click **Agree and Start Free Download** when prompted, and then click **Run** to install Java, as shown in Figure 3.2.1-9.

Figure 3.2.1-9. Run Java Installation File

Eventually, the Cisco AnyConnect Secure Mobility Client Downloader will begin installing the application as shown in Figure 3.2.1-10. Successful connectivity will be indicated as shown in Figure 3.2.1-11.

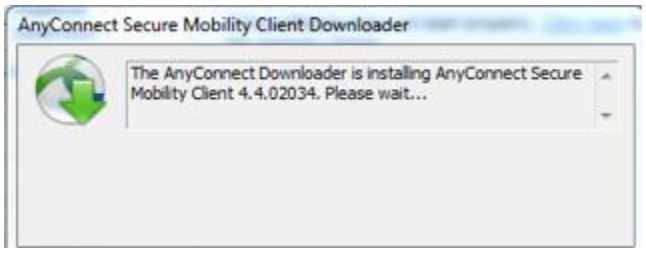

Figure 3.2.1-10. Cisco AnyConnect Installation

Figure 3.2.1-11. Connection Established

If the VPN doesn't connect automatically, click the Windows **Start** button and type **Cisco**. The Cisco AnyConnect Secure Mobility Client should appear in the Start menu. Click it to open the program and click **Connect** to connect to **vpn.mfn2.myflorida.com** as shown in Figure 3.2.1-12. Enter the **Username** and **PIN + token** code when prompted as shown in Figure 3.2.1-13 and click **OK**. If the connection is successful, the Cisco AnyConnect Secure Mobility Client icon will display in the Windows Tray with a lock on it as shown in Figure 3.2.1-14.

If the automatic web-based download and installation of the Cisco AnyConnect Secure Mobility Client was not successful, navigate to Section 3.2.2 and follow the instructions to download and install the application manually.

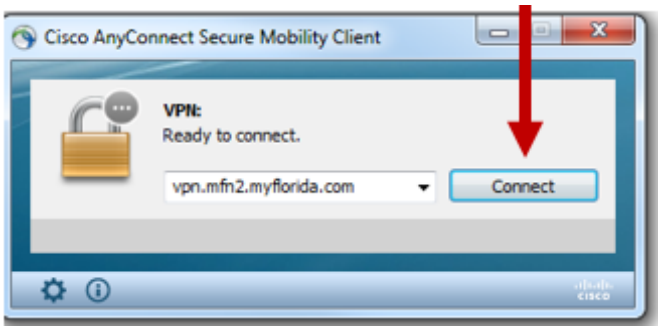

Figure 3.2.1-12. VPN Connect

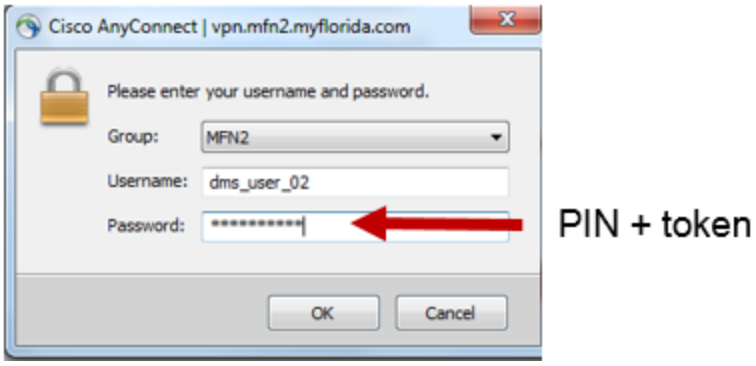

Figure 3.2.1-13. Entering Credentials

Figure 3.2.1-14. VPN Connected

3.2.2 Cisco AnyConnect Manual Installation

In many cases, the Cisco AnyConnect Secure Mobility Client will fail the automatic web-based installation and the user will see the dialog shown in Figure 3.2.2-1. The dialog prompts the user to download the installer and install the application manually. Click the **AnyConnect VPN** link if this is necessary.

Click **Run** to run the installation file as shown in Figure 3.2.2-2 and the Cisco AnyConnect Secure Mobility Client Setup Wizard will display as shown in Figure 3.2.2-3.

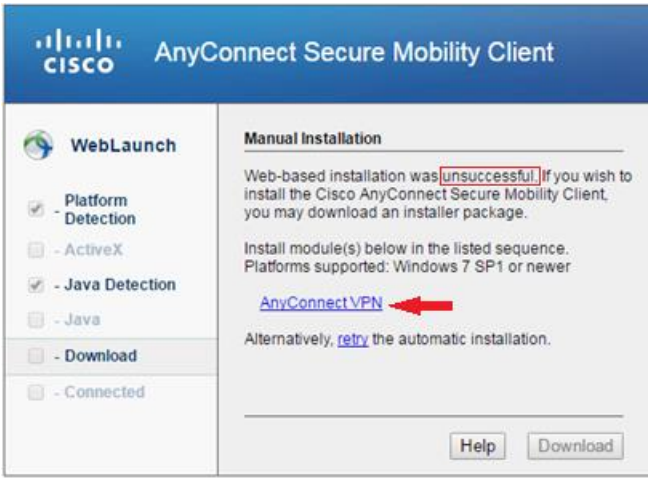

Figure 3.2.2-1. Unsuccessful Web-Based Installation

Figure 3.2.2-2. Run Installer File

Figure 3.2.2-3. Cisco AnyConnect Secure Mobility Client Wizard

Click **Next**, click to **accept** the agreement, click **Install**, and then enter administrative credentials, if prompted. Click **Finish** to exit the Setup Wizard as shown in Figure 3.2.2-4.

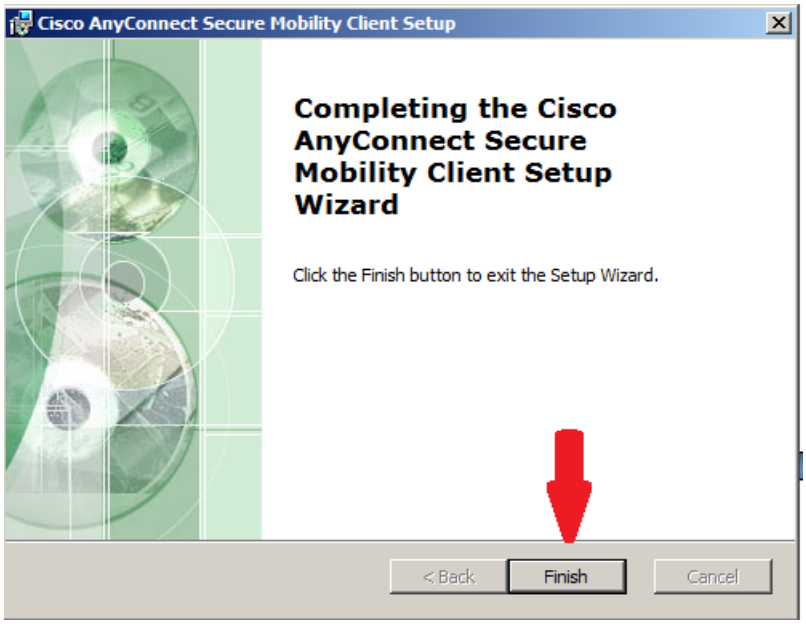

Figure 3.2.2-4. Finish the Installation

Click the Windows **Start** button and then type **Cisco**, and the **Cisco AnyConnect Secure Mobility Client** should display in the Start menu. Click to open the application. Click **Connect** to connect to **vpn.mfn2.myflorida.com** as shown in Figure 3.2.2-5, then enter **username** and **PIN+token** when prompted, as shown in Figure 3.2.2-6. If the connection is successful, the Cisco AnyConnect Secure Mobility Client icon will display in the Windows Tray with a lock on it as shown in Figure 3.2.2-7.

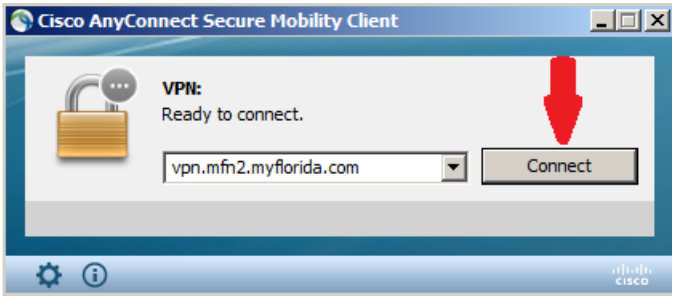

Figure 3.2.2-5. Connect to VPN

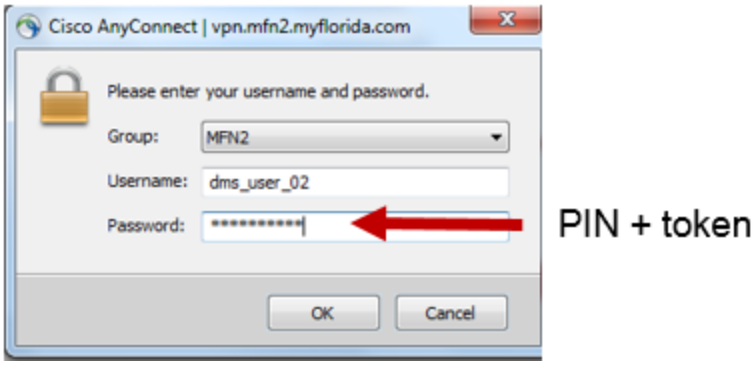

Figure 3.2.2-6. Enter Credentials

Figure 3.2.2-7. Successful VPN Connection

3.2.3 Cisco AnyConnect ISE Compliance Installation

At this point, the Client-to-LAN VPN software is installed and the user is connected to the VPN, however, the Cisco AnyConnect ISE Posture Module, Cisco AnyConnect ISE Compliance Module, and Cisco AnyConnect Diagnostics and Reporting Tool must be downloaded and installed to scan the client device and assure the operating system and antivirus are up-to-date, and a client firewall is active.

NOTE:

User must be connected to the VPN for the above steps to work.

Once the Cisco AnyConnect ISE Compliance Posture Agent is installed, it will begin scanning the client device as shown in Figure 3.2.3-1. If the client device is operating system and antivirus compliant, network access is allowed as shown in Figure 3.2.3-2. With the Client-to-LAN option, the user is not directed to any particular website as with the Clientless option. Instead, users navigate to their resources on their own. To disconnect from the VPN, click the **Disconnect** button.

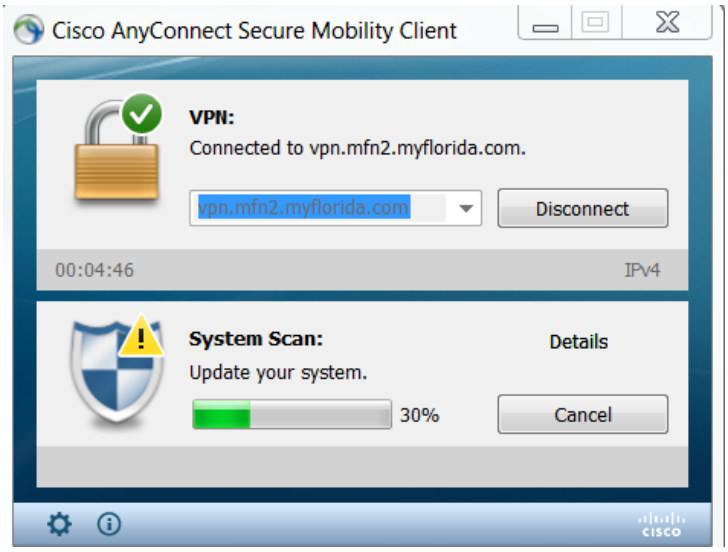

Figure 3.2.3-1. System Scanning

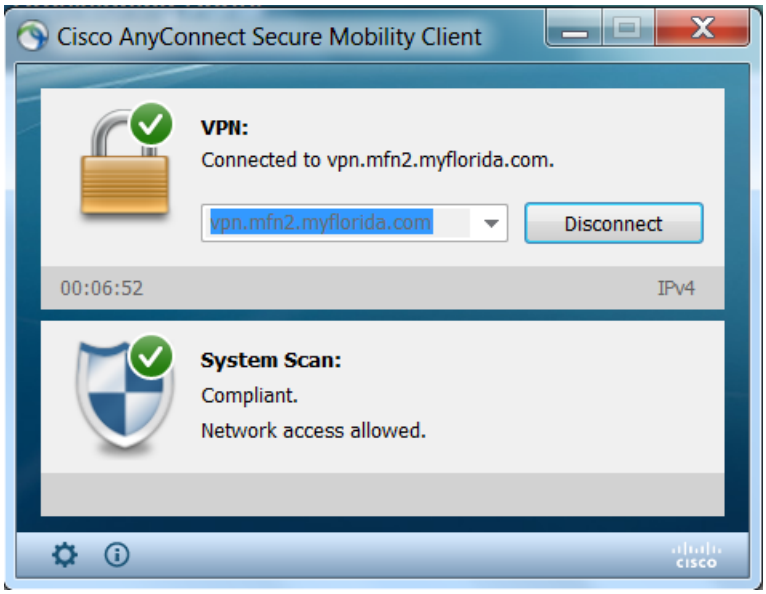

Figure 3.2.3-2. Compliant System

In the event Cisco AnyConnect determines the client device to be non-compliant with respect to the operating system, firewall, or antivirus, the user will see the dialog shown in Figure 3.2.3-3 and possibly the reason for the non-compliance, an example of which is shown in Figure 3.2.3-4.

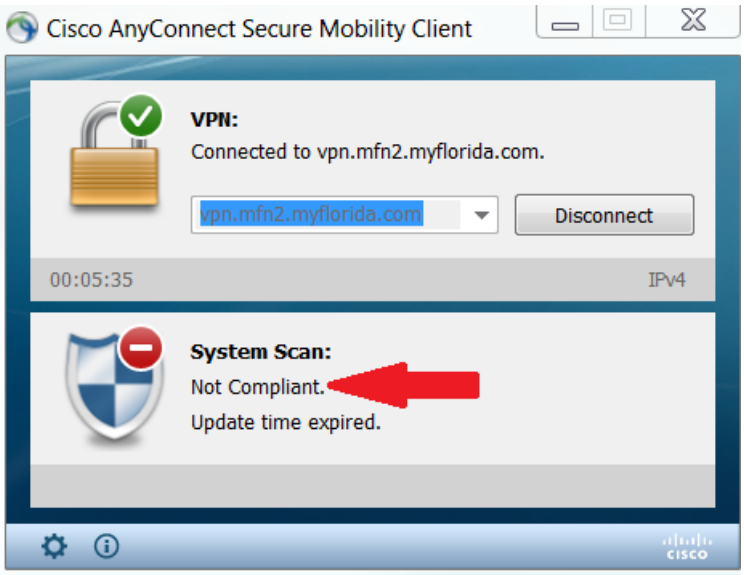

Figure 3.2.3-3. Non-Compliant System

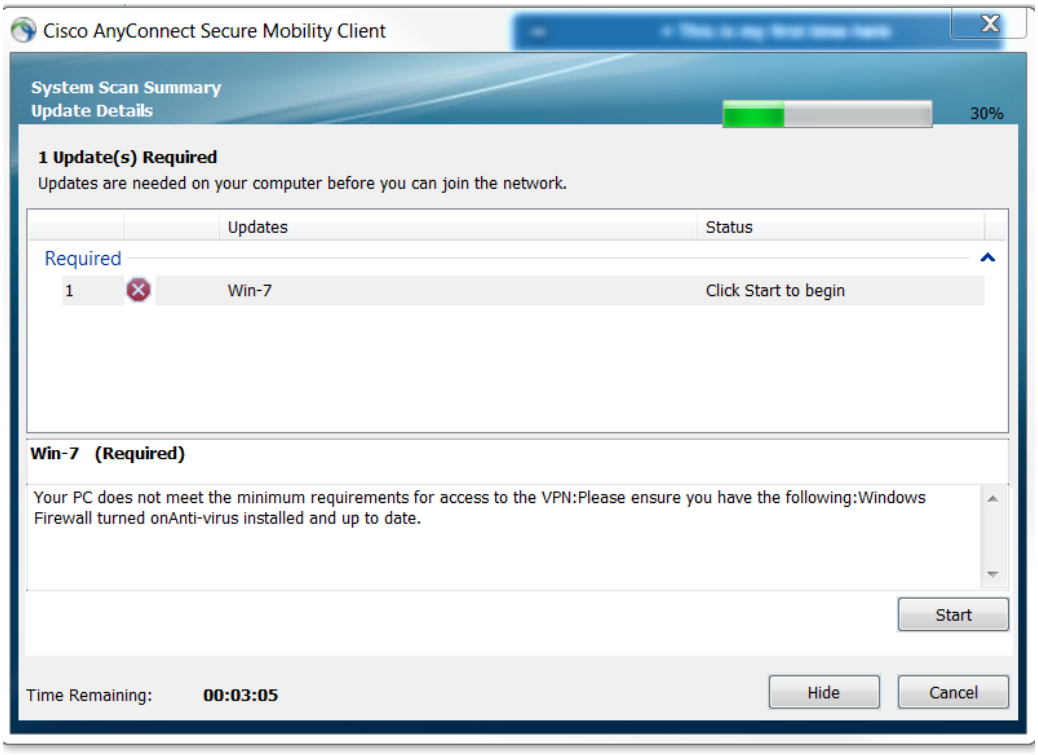

Figure 3.2.3-4. Windows Update Needed Example

Figure 3.2.3-4 implies the user can click the dialog Start button to resolve the issue, but this functionality is not in place. The user should close the **System Scan Summary Update Details** dialog, disconnect from the VPN, and remediate the issues manually. Once the issues are fixed, reconnect to the VPN and the Posture Agent will scan the system again for compliance.

NOTE:

Users should contact the MFN-2 SOC if they are unable to resolve issues preventing them from successfully accessing their resources via the VPN.

4 ORDERING NEW CLIENTLESS AND CLIENT-TO-LAN VPNS IN THE CSAB

Subsections 4.1 and 4.2 instruct on the ordering aspect of Clientless and Client-to-LAN remote access in the CSAB. Except for one step in the process, the ordering is essentially the same.

4.1 Clientless

To begin the Clientless VPN ordering process, log in to the CSAB website at: https://portal.suncom.myflorida.com, then click **Ordering** as shown in Figure 4.1-1. If the options shown in the figure do not display, click the **apps** menu and select **Ordering** from the dropdown list box.

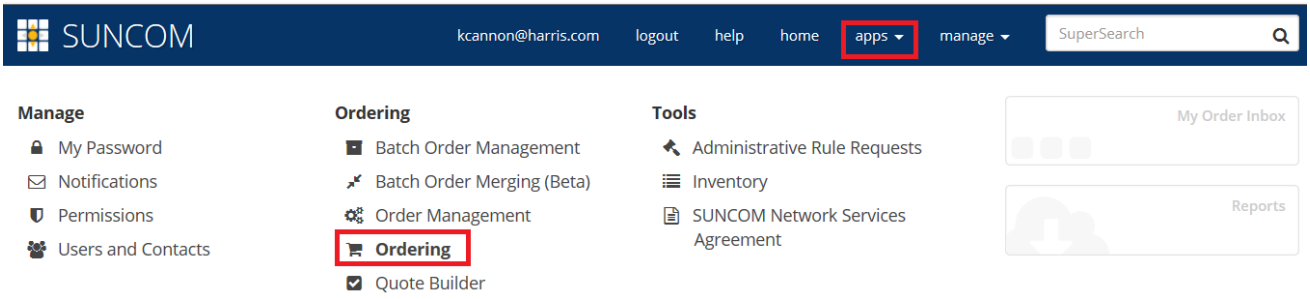

Figure 4.1-1. CSAB Ordering

Once on the **Ordering** page, expand **Remote Access**, and then click **VPN**. Under **VPN Client to LAN** on the right, click **Configure**, as shown in Figure 4.1-2.

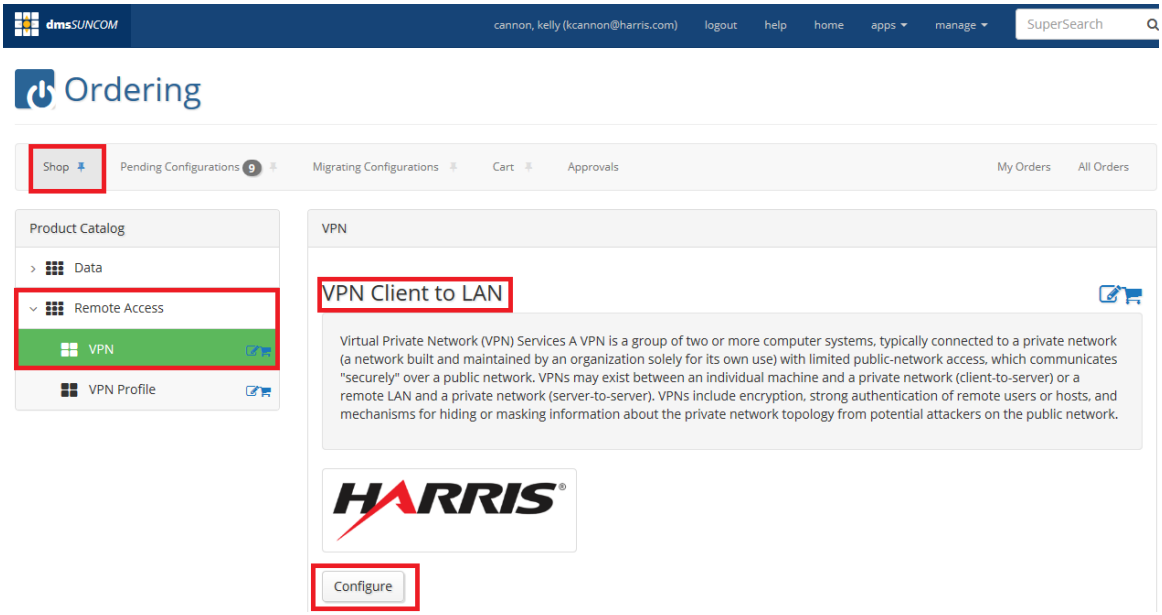

Figure 4.1-2. Remote Access VPN

On the **Bill to Account** page, locate the correct agency, expand it, and click the associated **account number** as shown in Figure 4.1-3. Click **Next** to continue.

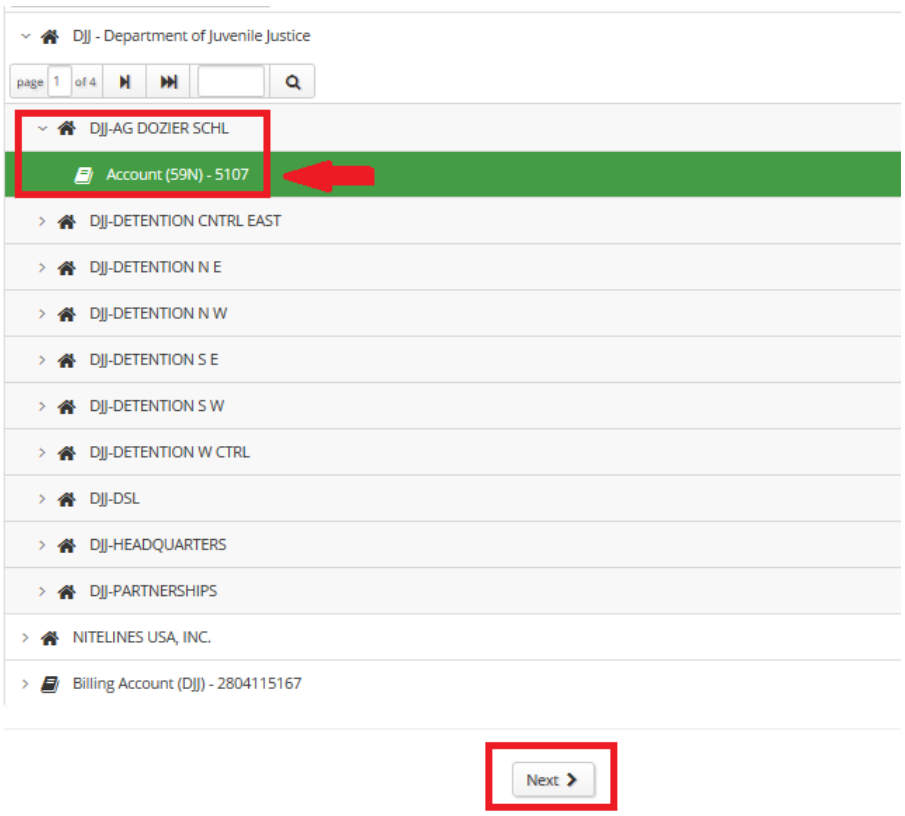

Figure 4.1-3. Billing Information

Figure 4.1-4 displays the Service Options. Expand **Client Type** and select **Proxied Clientless (SSL)**, then click to expand **Token Platform** and select the type of software token desired. One or two extra tokens may be ordered for an additional non-recurring cost.

NOTE:

If a prospective VPN user has a Customer Portal account, the user already has a soft token. The same token will be used for VPN remote access, so no additional token will be assigned, however the user should select the token platform already in use. As noted above, up to two extra tokens may be ordered.

In the example in Figure 4.1-4, a **Windows** token has been ordered as well as an additional token for an **Apple** cell phone. The figure displays the **Clientless** selection with the monthly recurring service charge and the non-recurring charge for the extra token, plus the installation charge for the VPN itself. Click **Next**.

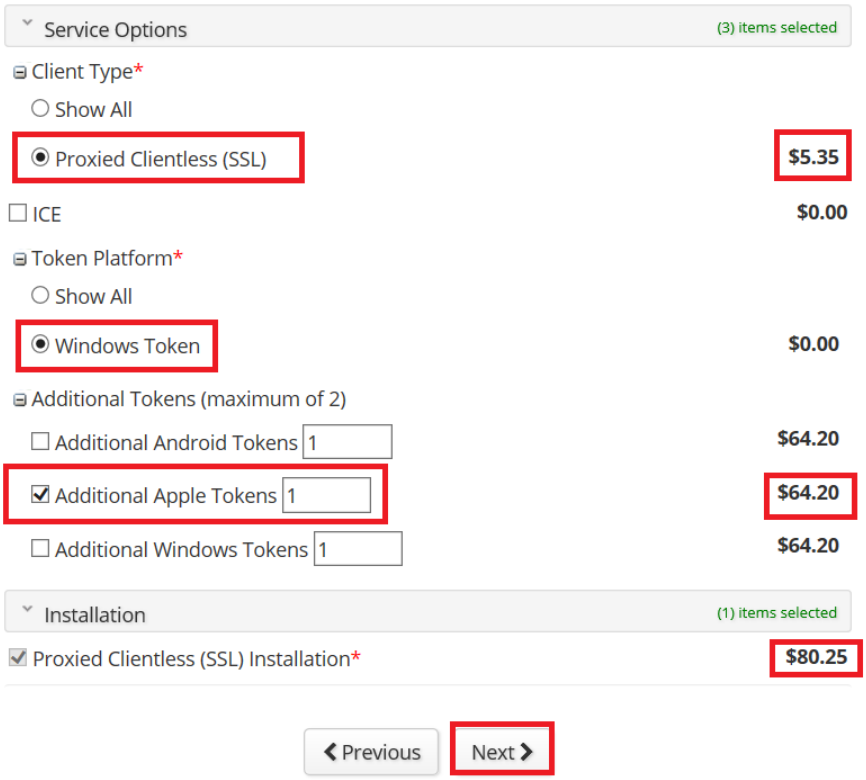

Figure 4.1-4. Ordering Proxied Clientless (SSL)

Figure 4.1-5 displays the information users will be prompted to enter next which includes: **Primary Contact** and **Technical Contact** information, as well as the **Physical Address** of the site.

Finally, a VPN profile is requested. If the agency or profile name does not appear in the **Agency or Profile** dropdown, a new profile needs to be created. The instructions for creating a new profile are covered in Section 4.3.

The **VPN User ID** is the user's **firstname** and **lastname**, all lowercase, with nothing in between as shown in the example for user Kelly Cannon, whose User ID is kellycannon. Click **Next**.

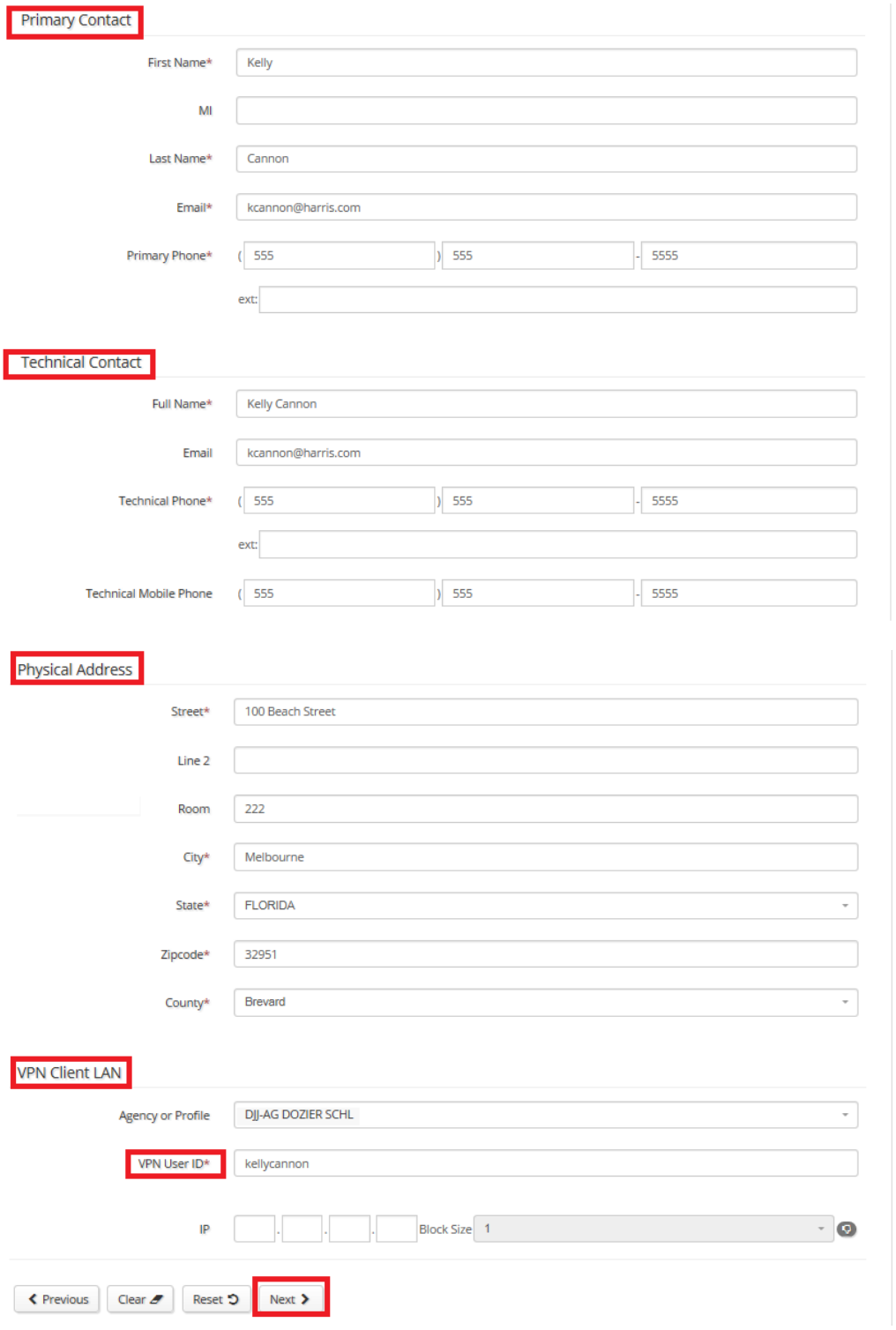

Figure 4.1-5. Contact and User Information

On the **Summary** page, the user should verify the options ordered and the monthly and non-recurring costs, and if correct, click **Add to Cart**, as shown in Figure 4.1-6. If the items are not correct, click **Previous**, and make the necessary changes.

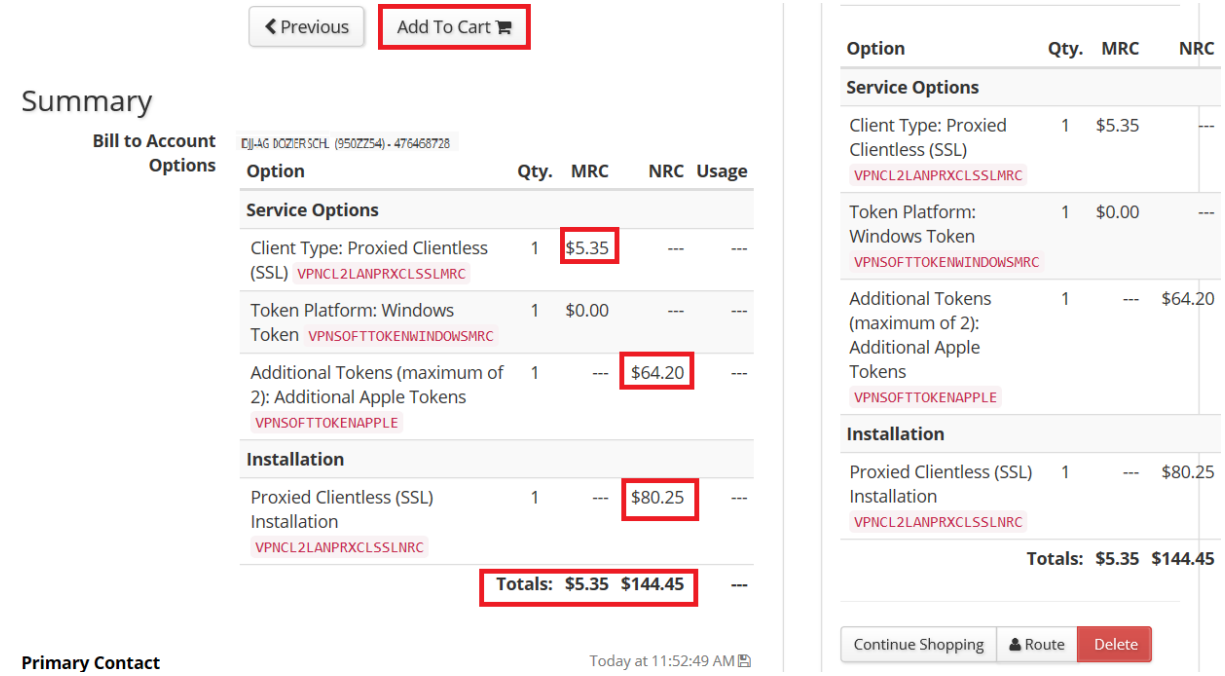

Figure 4.1-6. Verify and Add to Cart

The customer is taken to the checkout page and should once again verify the order. At this point the user can still make a change by selecting the checkbox next to the order and clicking **Save Items For Later**, or **Delete Items**, or **Reconfigure** as shown in Figure 4.1-7. If satisfied with the order, click **$Checkout**.

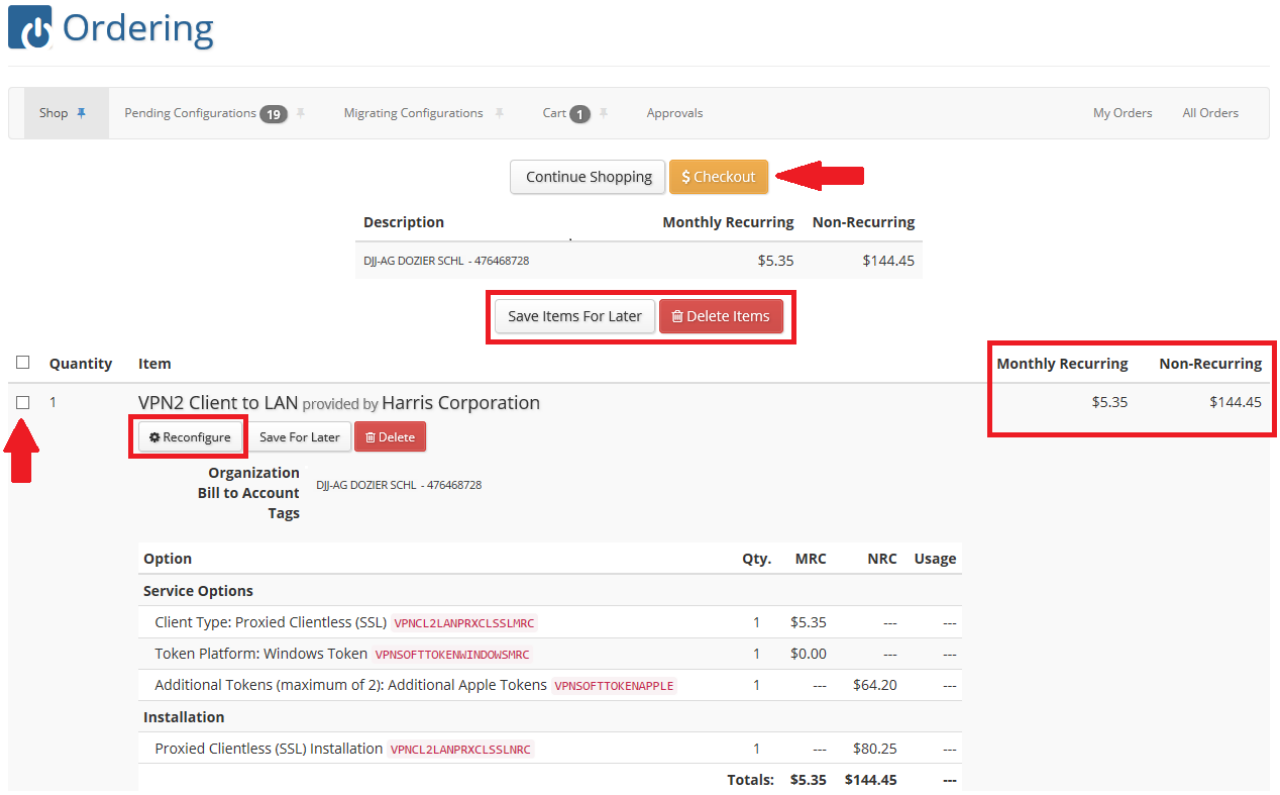

Figure 4.1-7. Checkout or Save, Delete, Reconfigure

Finally, select a **Preferred Delivery Date**, and then click **$Submit Order** as shown in Figure 4.1-8.

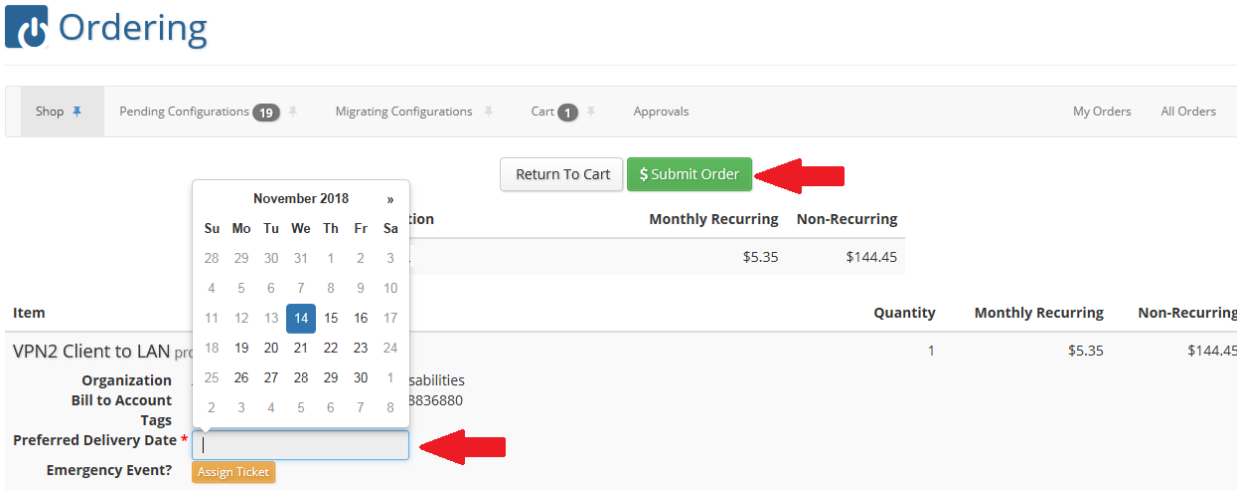

Figure 4.1-8. Preferred Delivery Date

4.2 Client-to-LAN

As previously mentioned, the process for ordering Client-to-LAN service is essentially the same as for Clientless, except for the consideration of the additional Split Tunnel order. Without split tunneling, the Client-to-LAN user will be unable to reach any other network, including the Internet, when attached to the MFN-2 network via VPN. In the example shown in Figure 4.2-1, the **Split Tunnel** checkbox has been selected, thereby adding that feature to the Client-to-LAN order. The customer has selected **Android Token** and 2 additional Android tokens. These additional tokens add a non-recurring cost of $64.20 each.

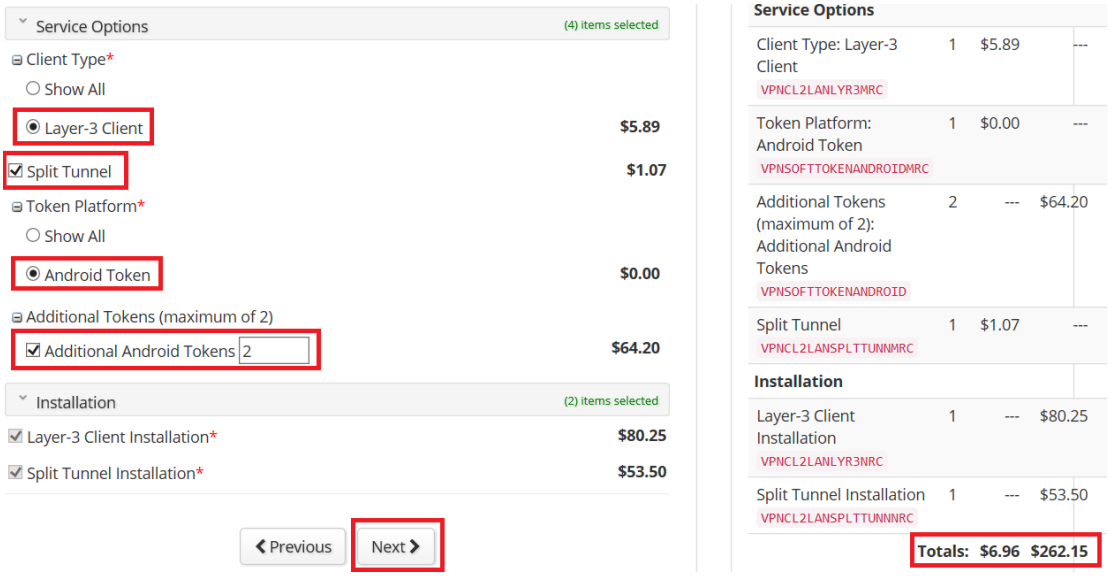

Figure 4.2-1. Ordering Client-to-LAN with Split Tunneling and Extra Tokens

As with Clientless, verify the service and installation before clicking **Add to Cart**, as shown in Figure 4.2-2.

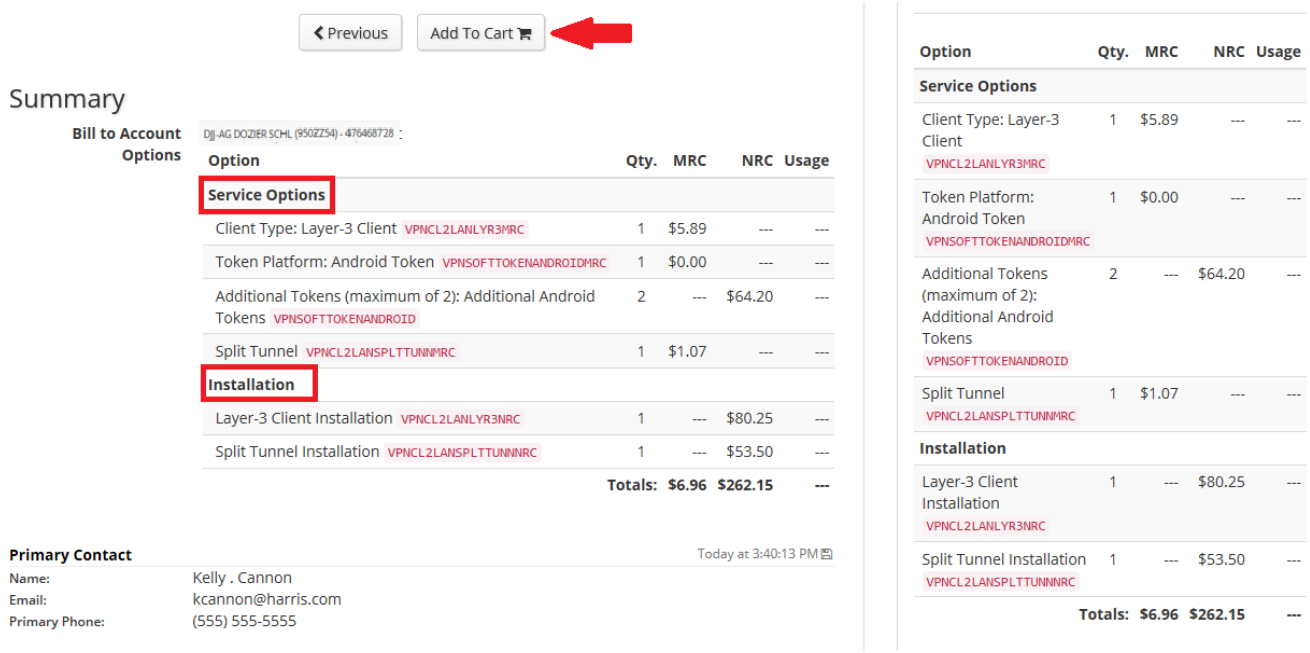

Figure 4.2-2. Verify and Add to Cart

Once reverified, click **$Checkout**. Alternatively, select the **checkbox** and **Save Items For Later**, or **Delete Items**, or **Reconfigure**, as shown in Figure 4.2-3.

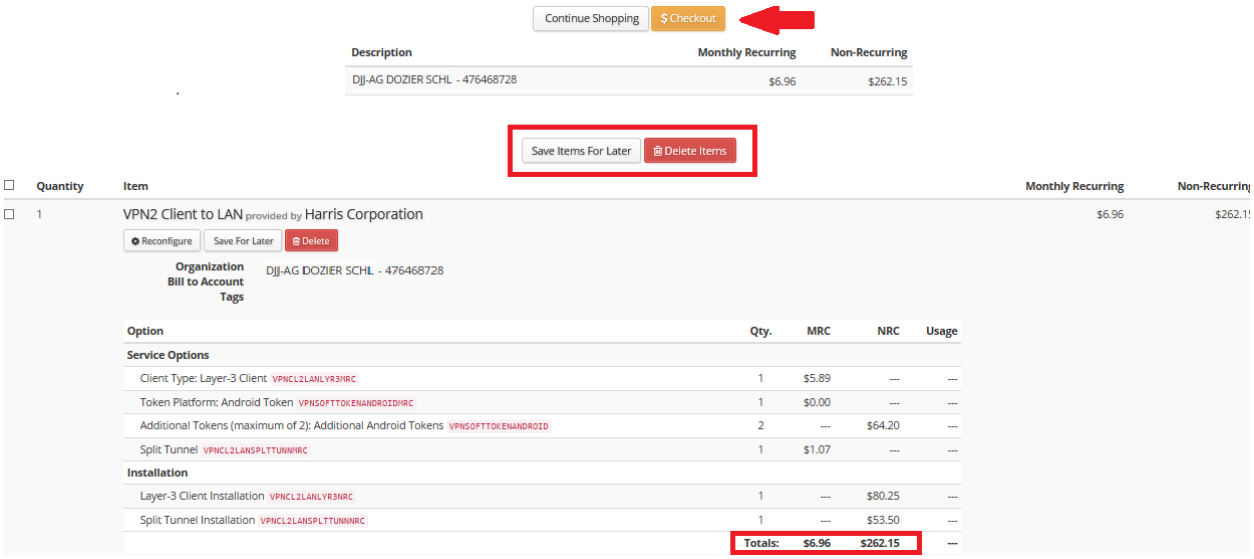

Figure 4.2-3. Checkout or Save, Delete, Reconfigure

4.3 Creating a VPN Profile

As previously mentioned, VPN accounts must be associated with a VPN Profile. The profile serves as an access list, providing the IP addresses the user will have access to once connected to

the VPN. Profile names are unique and so cannot be reused. VPN Profiles are ordered in the CSAB and must be approved by DMS before the remote access VPN order can be completed.

If an organization is accessing another network, authorization needs to be obtained via email or letter, and attached to the Configuration Summary area of the CSAB work order.

An associated VRF is also required. If no VRF is indicated, the Common Services VRF is assumed.

To create a new VPN Profile in CSAB, select the **Ordering** application and in the left pane, expand **Remote Access**, click **VPN Profile**, and then click **Configure** as shown in Figure 4.3-1.

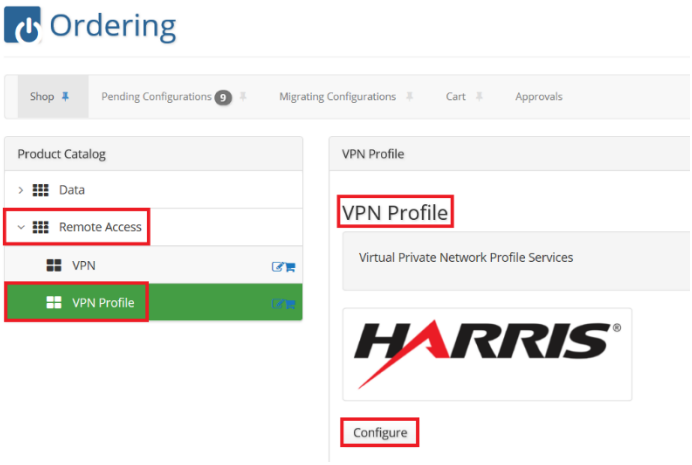

Figure 4.3-1. VPN Profile

Select the account to bill for the service and click **Next**, as shown in Figure 4.3-2.

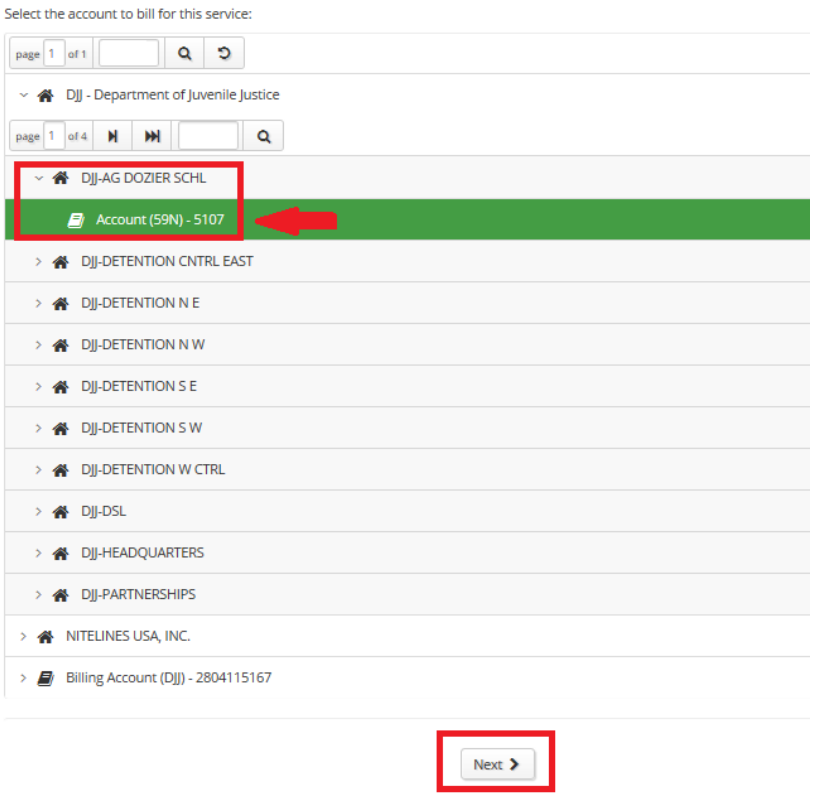

Figure 4.3-2. Billing Information

Check to select **New VPN Profile**. If the profile will be mapped to a VRF other than the Common Services VRF, check to select the **Mapping a VRF?** checkbox as shown in Figure 4.3-3. Click **Next**.

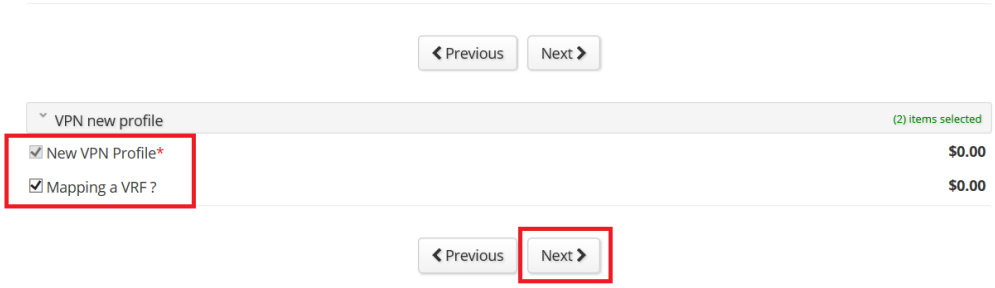

Figure 4.3-3. New VPN Profile and VRF

Enter the **Physical Address**, the **Technical Contact**, the **Profile** information, and the **VRF** if necessary. In Figure 4.3-4 the **Profile Name** entered is DJJ-BEACH. Profile names must be unique and cannot be reused. In the example, two **Profile IP** addresses have been configured. These permitted addresses serve as an access list. Also entered is a single **DNS** address. Note, the addresses in the figure have been redacted for security purposes. Finally, in the **VRF** section, the **VRF Name** BEACH has been added. This input is necessary because the user indicated they wanted to map a VRF to the profile. Click **Next** to navigate to the Summary page.

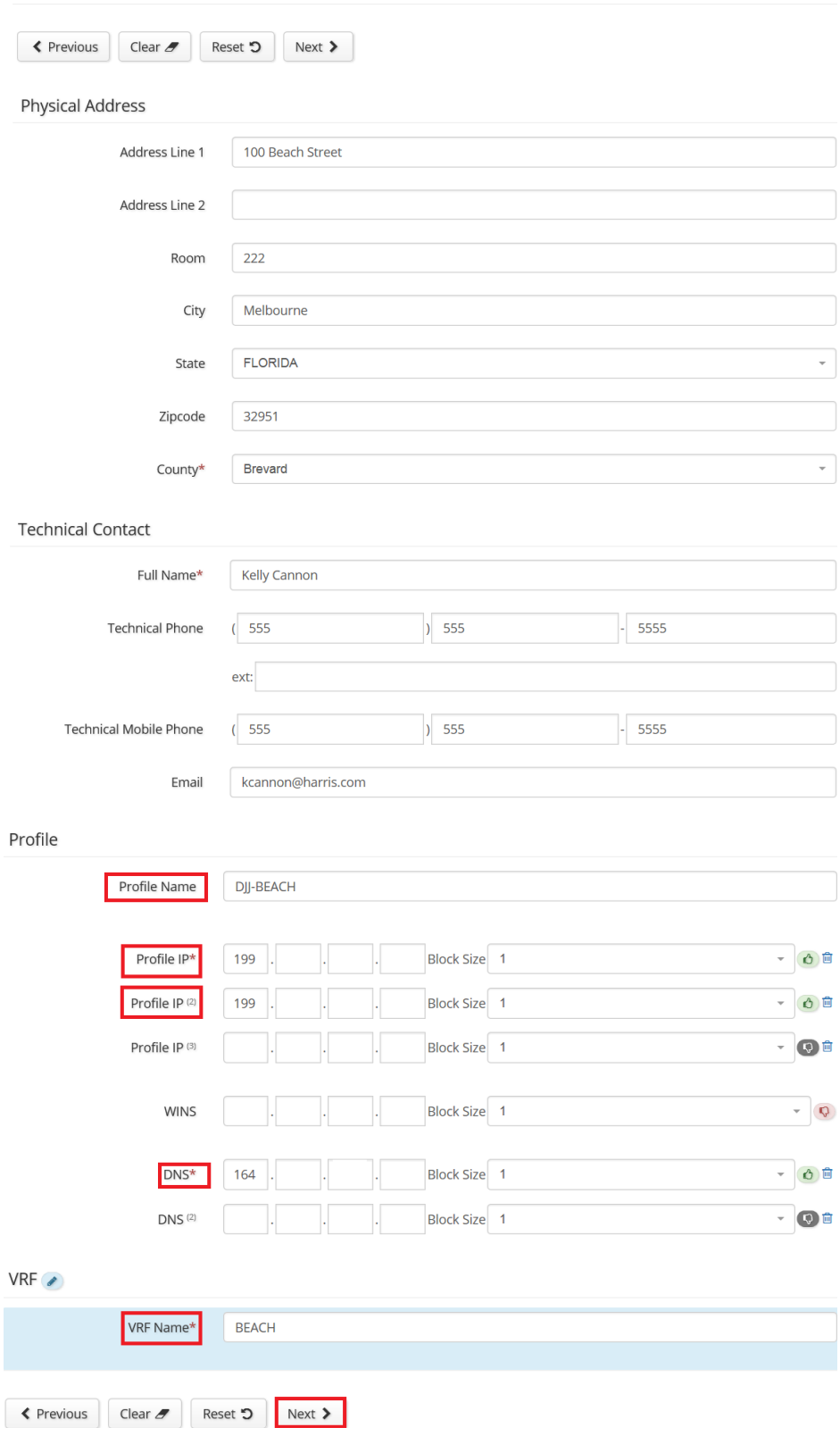

Figure 4.3-4. VPN Profile Configuration

If the VPN Profile includes a Profile IP address in a network not owned by the organization, written permission from the DMS is necessary. If this is the case, click the **Uploads** tab and then click **Attach File**, as shown in Figure 4.3-5. Browse to find the documentation requesting the access.

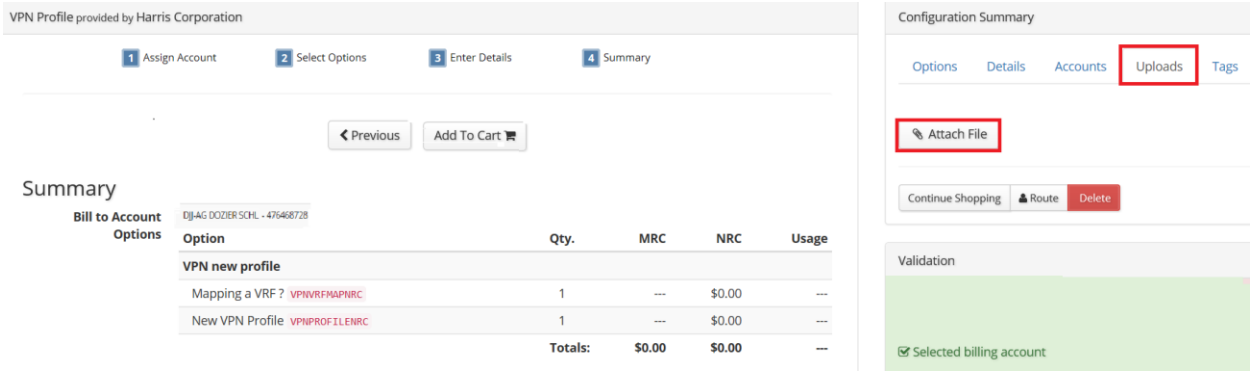

Figure 4.3-5. Attach File If Necessary

Review the order, and if correct, click **Add to Cart**, as shown in Figure 4.3-6. If the order is not correct, click Previous to return to the order particulars and make the necessary changes before proceeding.

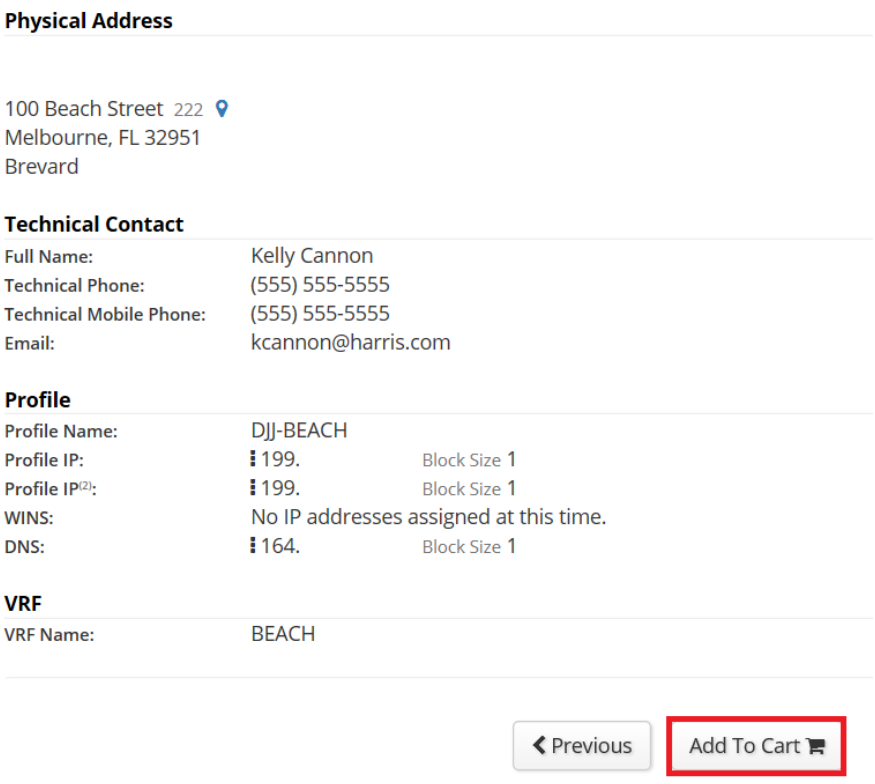

Figure 4.3-6. Verify and Add to Cart

Before checking out, verify the order one last time. If necessary, select the **checkbox** next to the order and click **Save Items For Later**, or **Delete Items**. If the order is correct and ready to be scheduled, click **$Checkout** as shown in Figure 4.3-7.

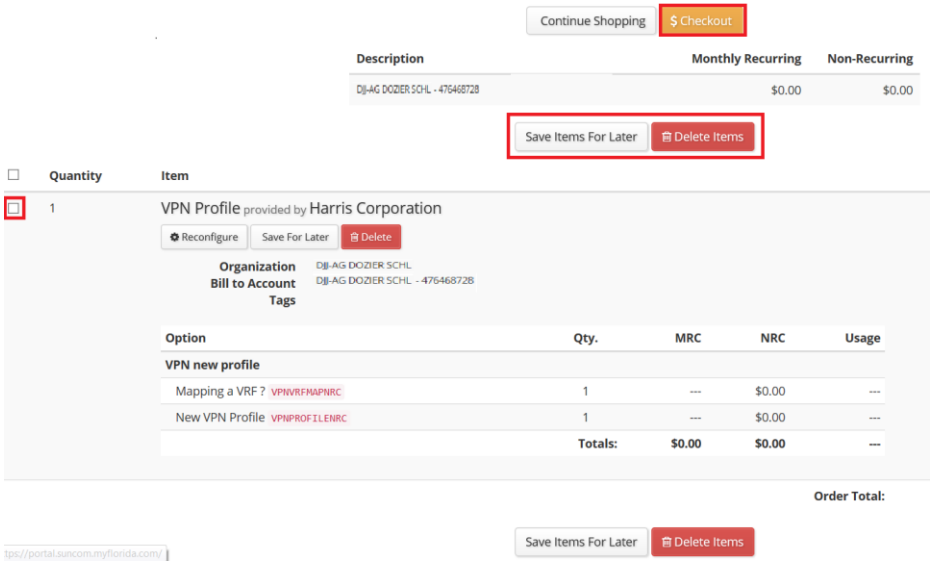

Figure 4.3-7. Checkout or Save, Delete, Reconfigure

Finally, click in the **Preferred Delivery Date** text box and select the desired delivery date using the pop-up calendar.

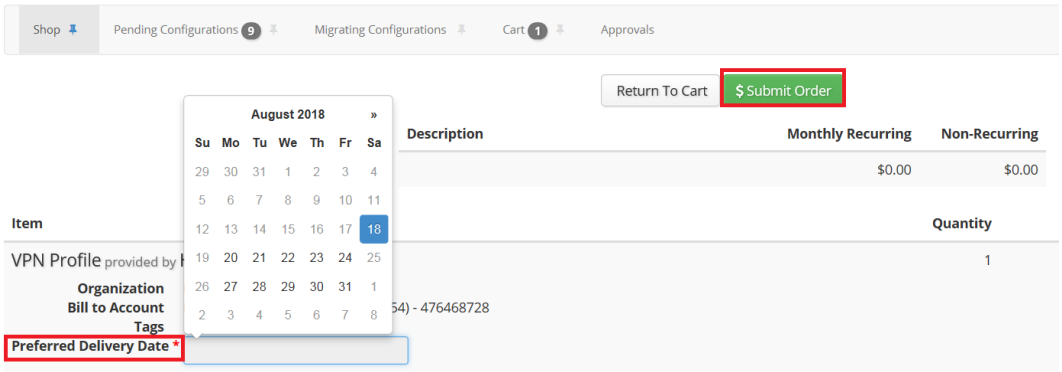

Figure 4.3-8. Preferred Delivery Date

Any problems with ordering or understanding VPN Profiles should be directed to the SUNCOM NOC.

5 MIGRATING VPNS IN THE CSAB

A customer site may already have a VPN service. In this case, a VPN service migration should be ordered in the CSAB. The VPN migration process is outlined in this section.

To begin the VPN migration, log in to the CSAB website at: https://portal.suncom.myflorida.com, then click **Inventory** as shown in Figure 5-1. If the options shown in the figure do not display, click the **apps** menu and select **Inventory** from the dropdown list box.

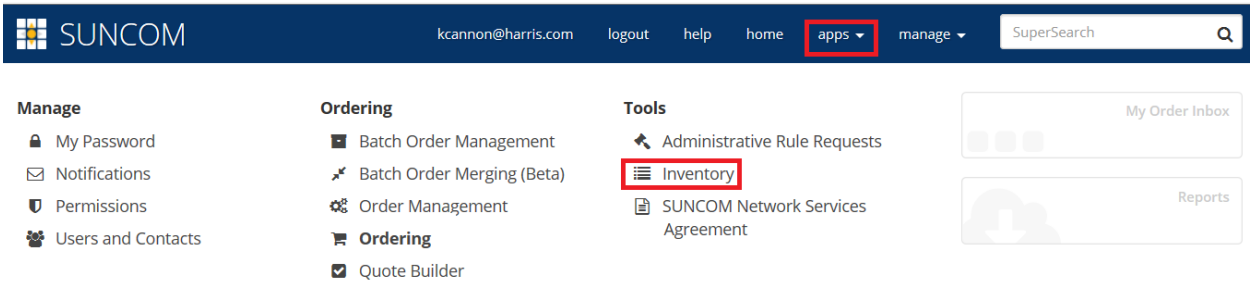

Figure 5-1. CSAB Inventory

Once on the **Inventory** page, click the **By Service** tab, and then expand **Remote Access**, and then **VPN**, then expand **VPN Client to LAN**, as shown in Figure 5-2.

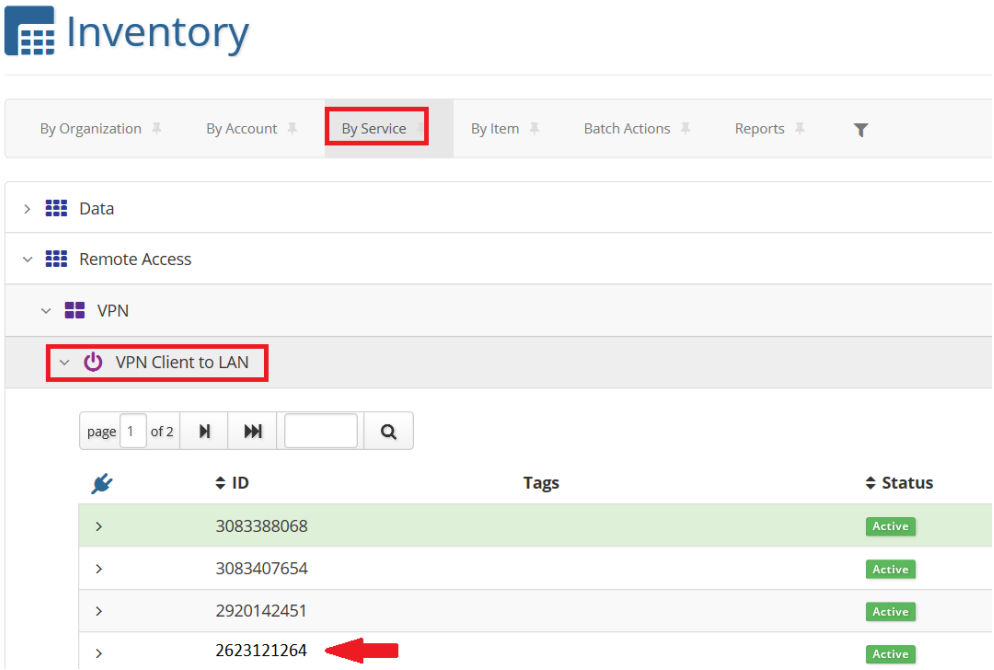

Figure 5-2. VPN By Service

Search for and select the inventory **ID** related to the current VPN service, and then click the **Actions** tab. Click **Start Provider Migration**, as shown in Figure 5-3.

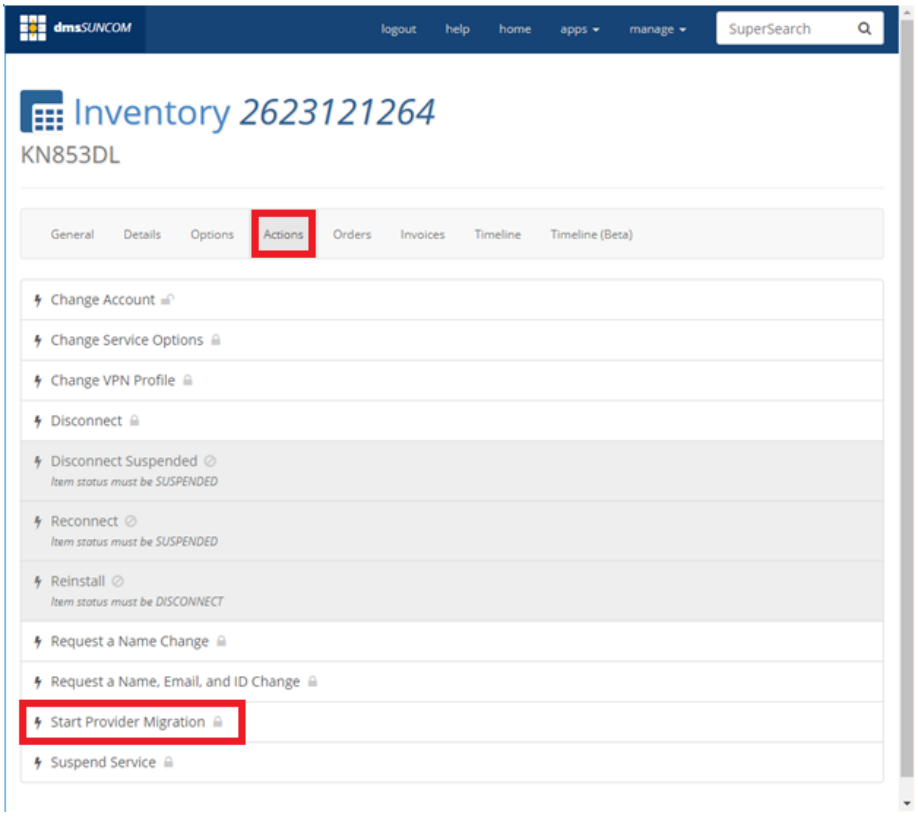

Figure 5-3. Start Provider Migration

Click **Add Attachments** to upload any related documentation, and then click **Execute Action** as shown in Figure 5-4.

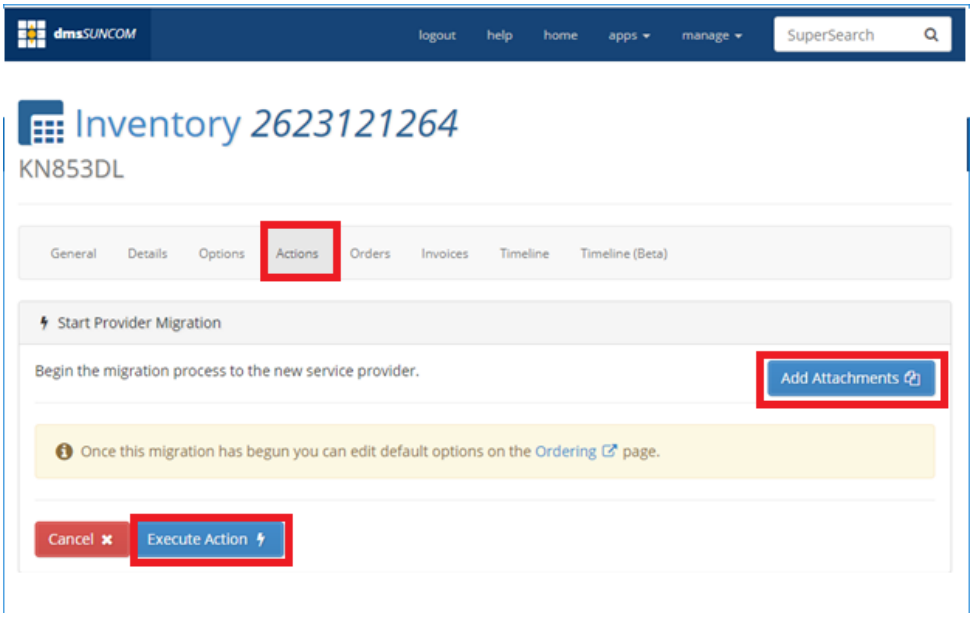

Figure 5-4. Execute Action

At this point the VPN migration has been executed but the process is not complete. The VPN itself still has to be ordered. Click the **Go to Ordering** link as shown in Figure 5-5 to start the ordering process.

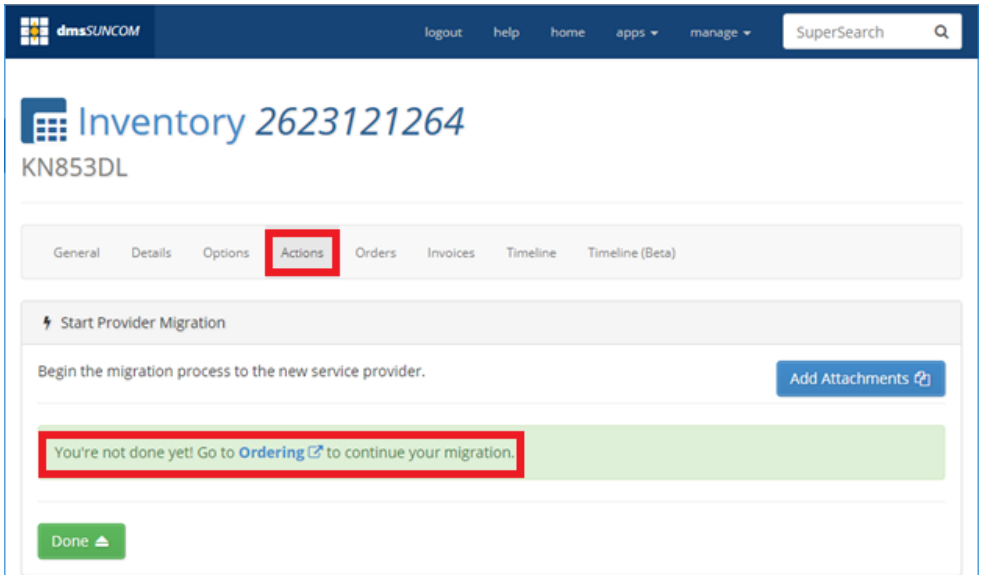

Figure 5-5. Go to Ordering

The **Migrating Configurations** tab should show that a migration has been executed. Click **Edit Configuration** to continue the ordering process, as shown in Figure 5-6. Alternatively, the migration could be cancelled by clicking Cancel Migration.

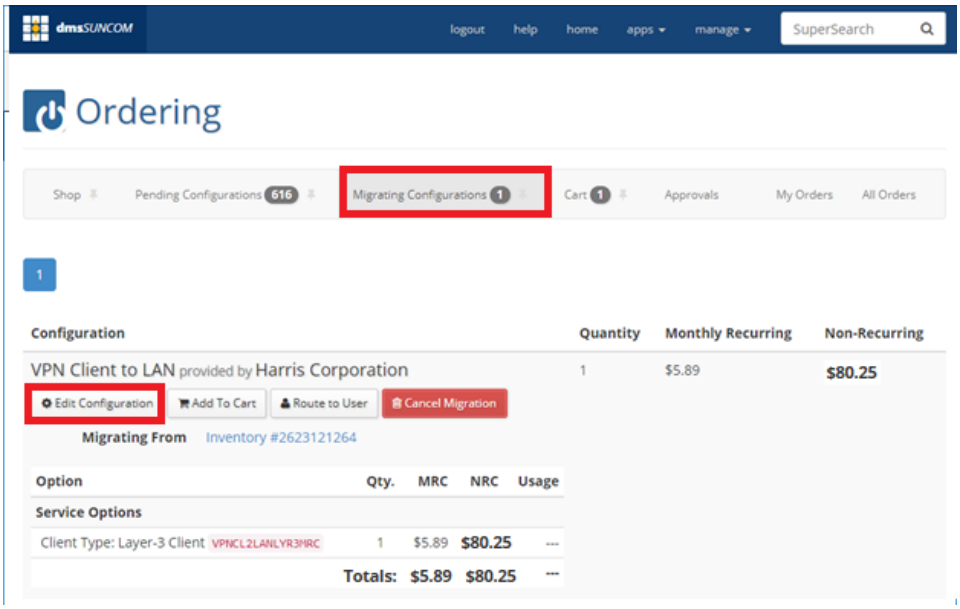

Figure 5-6. Edit Configuration

Enter the **contact information** related to the VPN service and then click **Next** as shown in Figure 5-7.

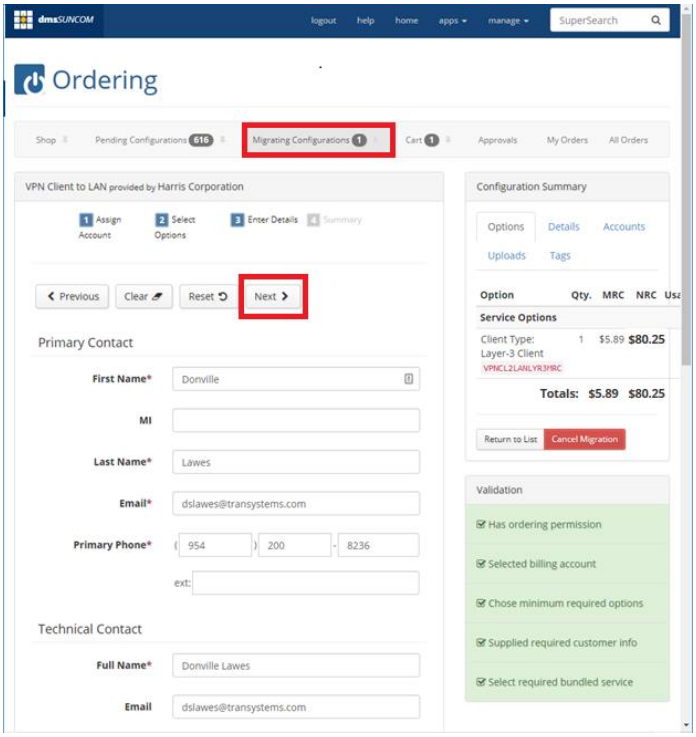

Figure 5-7. Enter Contact Information

Review the **Summary** of the order, and if correct, click **Add to Cart**, as shown in Figure 5-8.

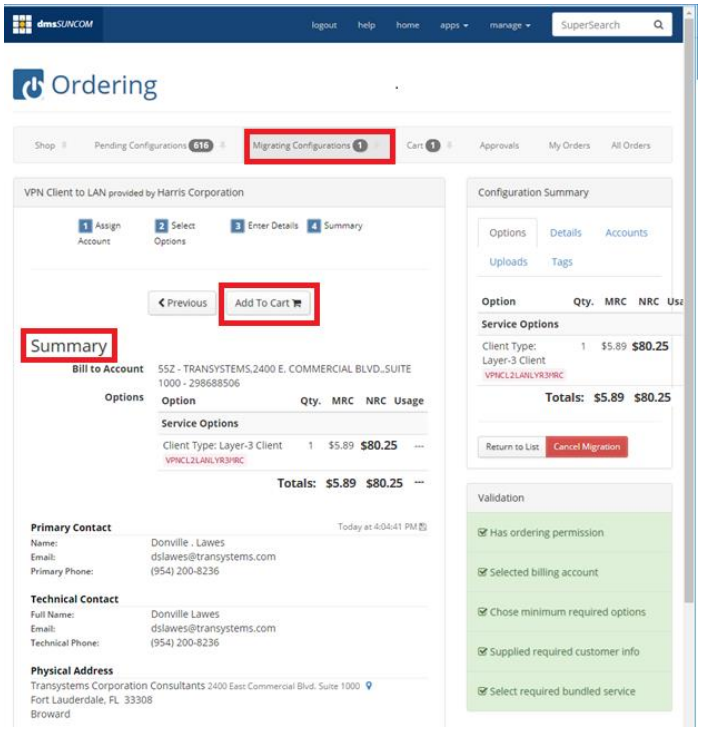

Figure 5-8. Add to Cart

At the checkout page, as shown in Figure 5-9, the customer has the option to Save Items For Later, Delete Items, Reconfigure the order, Wait to Migrate, or Cancel Migration. If the order is correct and should be ordered promptly, click **$Checkout**.

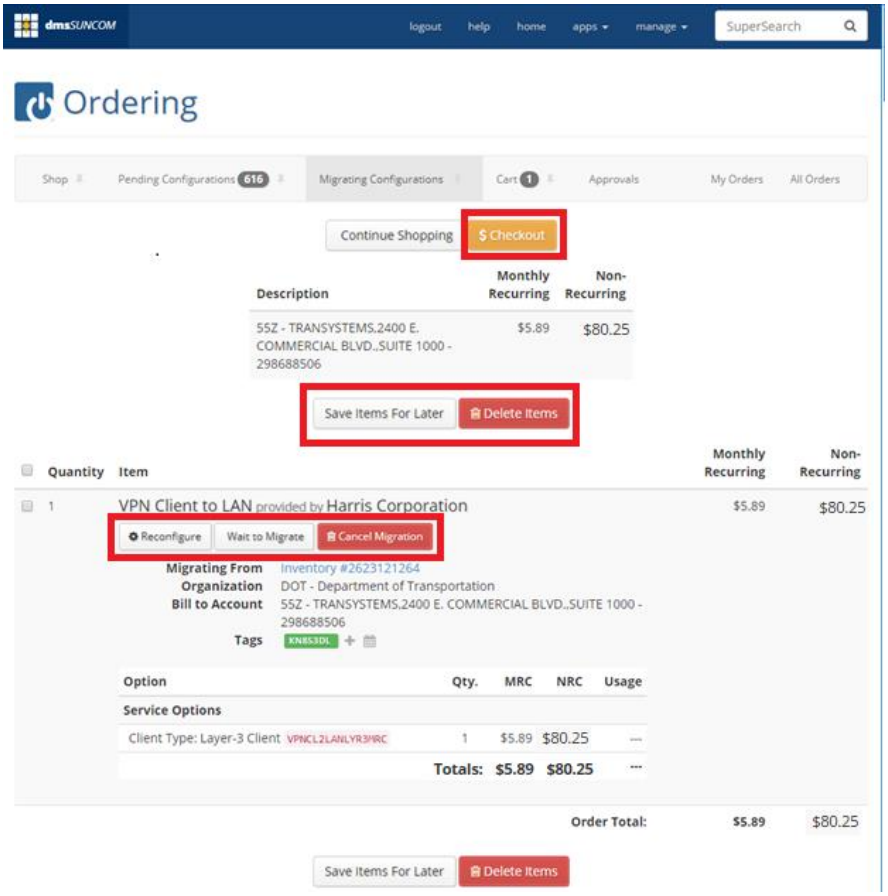

Figure 5-9. Check Out

Finally, select a **Preferred Delivery Date**, and then click **$Submit Order** as shown in Figure 5-10.

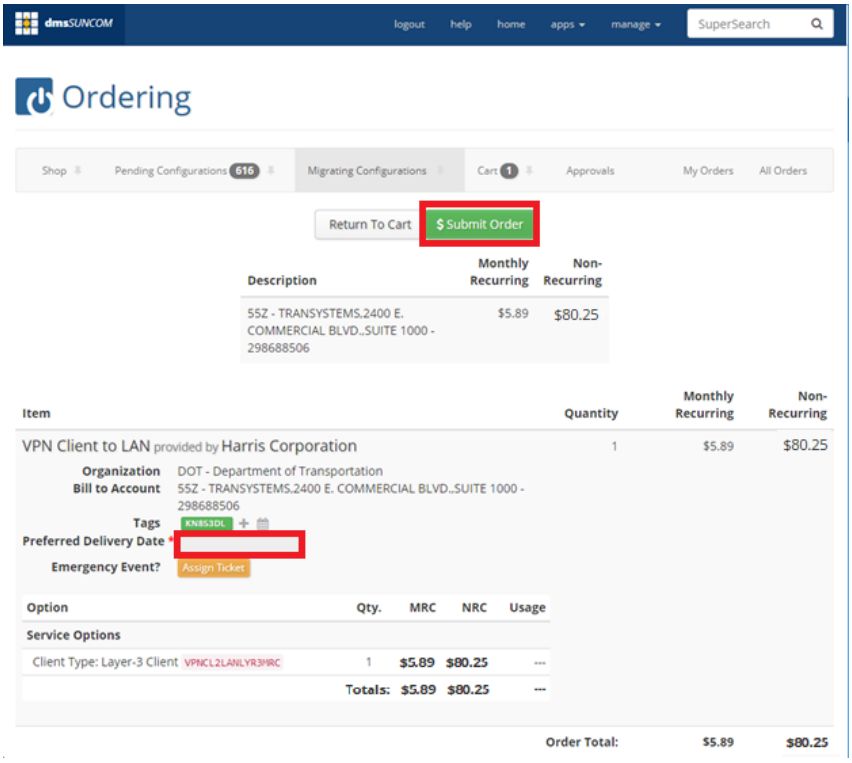

Figure 5-10. Submit Order

Any problems with ordering or understanding migrating VPN services should be directed to the SUNCOM NOC.

End of Remote Access VPN Reference Guide