

Your Ultimate Source for E-Tool Management and Security

User Manual

E-Tool 10-Drawer CAC Mobile Manager

With Optional 6-Drawer Add-On



Introduction	3
PART NUMBERS	4
Gen 2	4
	4
AC Power	5
Network Connection	5
Included Materials	5
Cabinet Overview (Layout)	6
Cabinet Installation	7
Sidecar Assembly	8
A/C & LAN Connection	13
INSTALLING DEVICES IN THE DRAWER	15
Location and Orientation	16
	17
	10
Operation	48
Software	49
Velocity	49
Event Viewer	50
Microsoft SOL	53
SECURE LAPTOP CLIENT	54
A1-SLSS STARTUP PROCEDURE CHECKLIST	58
A2-Logic Overview	65
Trouble Shooting	68
DRAWERS	70
REPLACEMENT PART NUMBERS	71
Maintenance	73
AIR FILTERS	74
FANS	75
DRAWER	73
DRAWER MODULE	79
DRAWER EMITTER	82
ELECTRONICS BAY	84
ELECTRONICS ASSEMBLIES	88
KEYPAD	89
SNIB2	91
INTERFACE BOARD	93
POWER SUPPLY	96





PART NUMBERS

This manual describes multiple cabinets, with part numbers listed below. Not all sections or images apply to every cabinet type.

<u>Gen 2</u> 510-1230-F50-00 510-1233-F00-00 563-0111-F00-00

<u>Gen 2.5</u> 563-0104-F21-00 563-0104-F23-00 563-0104-F25-00

563-5001-F00-00 563-5001-F20-00 563-5001-F25-00

REQUIRED FACILITIES

AC Power

Every Mobile Manager cabinet and sidecar requires a dedicated AC power circuit with a 15A or 20A circuit breaker. For a 16-drawer installation, each of the two cabinets (10-drawer main cabinet and 6-drawer sidecar) must have an independent AC power source. Under some conditions, the combined 16-drawer power requirement can exceed the capability of a single 20A service.

Network Connection

Each Mobile Manager cabinet or combination requires a single Local Area Network connection. The cabinet can accommodate a network switch in a 1U 19" rack-mount chassis. For a 16-drawer installation, a 24-port network switch in the 10-drawer main cabinet services the 6-drawer sidecar through internal wiring.

Included Materials

Each cabinet has a box in the bottom drawer, and includes:

- AC Line Cord (depending on model)
- 2' Ethernet Cable, 1 per drawer
- Drawer Key
- Network Switch Compartment Key
- Hardware for Lower Brackets
- Hardware for Upper Bracket
- Straps
- Fan Filters

Front View



Rear View







SIDECAR ASSEMBLY

If the cabinet is a stand-alone model, skip this step and proceed to AC Power Connection.

The Tracewell Systems 16-drawer E-Tool Mobile Manager arrives as two separate cabinets that must be joined together for operation. Joining the main cabinet and sidecar requires #1 and #2 Phillips screwdrivers. (figure 1)





With a #2 Phillips screwdriver, remove four mounting screws from the left side of the sidecar top cover. Use these screws to mount the Upper Bracket to the sidecar. (figure 2)



With a #1 Phillips screwdriver, remove the access covers from the right side of the main cabinet and left side of the sidecar. Pull six LAN cables and 2 control cables out of the pocket in the main cabinet. (figure 3)



Position the 6-drawer sidecar to the right of the 10-drawer main cabinet. The front corners of the cabinets should be touching and the rear corners should be 6" apart. (figure 4)



Connect the 6 Ethernet cables and 2 control cables as indicated on the label. Each cable is identified with a wire marker. After the cables are connected, push the two cabinets together while tucking any excess cable inside the pocket in the main cabinet. Do not attach the Upper Bracket to the main cabinet at this time. (figure 5)



Two identical Lower Brackets are supplied to join the cabinets. Remove two screws from the bottom front of each cabinet. These are in the lower front corners. Position a Lower Bracket across the front of the two cabinets and adjust the cabinet positions so that the holes in the bracket align with holes in the cabinets. Attach the bracket with 8 pieces (4 per cabinet) of Base Bracket Screws: 010-5063-000-OH. Base Brackets (front & back): 163-0058-099-01. (figure 6)



Repeat the procedure to install a Lower Bracket across the rear of the cabinets. Note that four screws are removed from each cabinet for the rear bracket. (figure 7)



Attach the Upper Bracket to the right side of the large cabinet. Use two pieces of Top Mounting Brackets: 163-0057-156-03 hardware set. Note: Use existing screws from Figure 2. (figure 8)



AC Power Connection

With a #1 Phillips screwdriver, remove the Lower Access Cover, Connect external AC power to the terminal block. (figure 9)



LAN Connection

Connect the external network cable to the connector marked "PORT SWITCH CAT-6". Replace the Lower Access Cover. (figure 10)



Network Connection (not visible)



Network Switch

For some models, the network switch is provided and installed by the user. To install a network switch, turn the Switch Key counterclockwise. Turn the clasp 1/2 turn counterclockwise and release. Lift up and remove the switch cover. Position the switch as shown and secure it to the mounting brackets with screws. Attach all Ethernet cables. Each cable has a wire marker with the assigned port number. Attach the AC power line cord. Replace the switch cover, turn the clasp 1/2 turn clockwise to secure the cover, and turn the key clockwise to remove it and lock the cover in place. (figure 11)











INSTALLING DEVICES IN THE DRAWER

Location and Orientation

Each drawer can hold one device such as a laptop computer. The device should be placed in the drawer with the open side to the front. There is room in the back of the drawer for the AC power adapter. The floor of the drawer has labels showing the correct locations for the device and its AC power adapter.

Connect the AC power adapter line cord to the AC power outlet on the rear wall of the drawer. (figure 12)



Keep the power adapter and its wires behind the line indicated by the labels. (figure 13)



Connect the 2-foot Ethernet cable to the RJ-45 connector.

Position the device in the drawer in the area marked by labels.

Note:

Placing the asset in the drawer correctly assures that it will be detected by the cabinet. This is important for logging its check-in. It also helps maintain the correct airflow around the device for cooler operation.

Correct (figure 14)





Wrong (figure 15)





Check Out Asset / Check In Asset

To Check Out an Asset:

- 1. Insert your Common Access Card (CAC) into the card reader as shown. The gold contact area goes into the reader first.
- 2. Wait until the keypad icon lights.
- 3. Enter your Personal Identification Number (PIN), then press Ent. Remove your card.
- 4. Notice which drawer LED is flashing green. Open the drawer, remove the power and Ethernet cables, remove the device, make syre the AC power adapter and Ethernet cable are behind the line as indicated, and close the drawer.

Check In An Asset:

- 1. Insert your CAC into the card reader.
- 2. Wait until the keypad icon lights.
- 3. Enter your PIN, then press Ent. Remove your card.
- 4. Notice which drawer LED is flashing red. Open the drawer, replace the device in the are marked by the labels, connect the power and Ethernet cables, and close the drawer.

Velocity v3.1 Secure Laptop Installation Procedure

4/11/2011 Software version 3.1.9.4

Overview

These procedures are for installing Velocity v3.1 using SQL Server 2005 Express with the Secure Laptop Extension on a standalone single user system. The Velocity documentation at <u>http://www.hirschelectronics.com/products-services/physical-security/access-control-software</u> contains essential information for the installation and configuration of Velocity. Velocity is the management software for access control and security operations.

Below is an overview of the Velocity components that are applicable to the Velocity Secure Laptop Solution.



The physical components are the Velocity workstation and the Tracewell E-Tool CAC enabled cabinet. The workstation and the cabinet communicate over an Ethernet network. All communication between the workstation and the controller uses AES (Rijndael) encryption. The cabinet manages laptops that contain the Electronics Technical Interactive Manuals (ETIM). The data flow process to successfully checkout a laptop is as follows.

- 1. Prior to accessing the E-Tool cabinet, each Common Access Card (CAC) must be registered into the Velocity access control system. The EDIPI on the CAC is used to generate a code that is sent to the controller board located inside the cabinet. The EDIPI number and other CAC information is never to the controller.
- 2. A technician with a CAC inserts their card to the reader on the E-Tool cabinet.
- 3. The technical enters their PIN for authentication.
- 4. The EDIPI number is read from the card, converted to a code and sent to the controller inside the cabinet. No other information other than the EDIPI number is read from the card by the reader on the cabinet.

- 5. The cabinet controller sends an event message to the Velocity workstation with the successfully read information. The DIGI*TRAC service component of Velocity communicates with the cabinet controller.
- 6. Velocity receives the event and displays it on the Velocity Event Viewer and the Message Queue Writer component writes the event to a MS Message Queue.
- 7. The Secure Laptop Extension reads the event from the MS Message Queue.
- 8. The Secure Laptop Extension decides which cabinet drawer to unlock and sends XML to the XML-RPC Web Server.
- 9. The web server sends a command to the cabinet to unlock the specific drawer again via the DIGI*TRAC service. The drawer LED blinks indicating which drawer is unlocked.
- 10. The CAC technician opens the drawer, removes the laptop and closes the drawer.
- 11. Another event is sent back to Velocity, via the DIGI*TRAC service. Velocity again writes it to the queue and the Secure Laptop service consumes it and records the checkout.

The laptop return process is similar.

- 1. The CAC is already registered into the Velocity.
- 2. A technician with a CAC inserts their card to the reader on the E-Tool cabinet.
- 3. The technical enters their PIN for authentication.
- 4. The EDIPI number is read from the card, converted to a code and sent to the controller inside the cabinet. No other information other than the EDIPI number is read from the card by the reader on the cabinet.
- 5. The cabinet controller sends an event message to the Velocity workstation with the successfully read information. The DIGI*TRAC service component of Velocity communicates with the cabinet controller.
- 6. Velocity receives the event and displays it on the Velocity Event Viewer and the Message Queue Writer component writes the event to a MS Message Queue.
- 7. The Secure Laptop Extension reads the event from the MS Message Queue.
- 8. The Secure Laptop Extension has previously recorded a checkout and therefore this is a check-in. The checkout information recorded the cabinet and drawer from which the laptop was checked out. The Secure Laptop Extension sends XML to the XML-RPC Web Server to unlock the same drawer.
- 9. The web server sends a command to the cabinet to unlock the specific drawer again via the DIGI*TRAC service. The drawer LED blinks indicating which drawer is unlocked.
- 10. The CAC technician opens the drawer, inserts the laptop and closes the drawer.
- 11. Another event is sent back to Velocity, via the DIGI*TRAC service. Velocity again writes it to the queue and the Secure Laptop service consumes it and records the check-in. The CAC holder is disassociated with the laptop.

Requirements

- Verify the minimum hardware and software requirements are fulfilled.
- Velocity 3.1 Secure Laptop Extension Setup.exe containing the configuration files.
- A Tracewell E-Tool CAC enabled cabinet.
- A network and patch or crossover cable to provide communication between Velocity and the cabinet.

Tasks

- Install Windows XP Professional or Windows Vista.
- Logon the workstation with the user Administrator or another that is in the local Administrator group.
- If using Vista, attempt turn off the User Access Control for the current logon.
- Obtain the password complexity rules from sites IT group.
- If desired, install SQL Server 2005.
- Install Velocity 3.1.

- Create the Velocity product activation key request file.
- Create and email the Velocity Message Queue Writer feature activation key request.
- Run the Velocity 3.1 Secure Laptop Extension setup.
- Create and email the activation.act file to license the Velocity 3.1 Secure Laptop Extension from Hirsch Professional Services Group.
- Backup the Velocity database.
- Turn off the firewall.
- Verify the IP address of the Velocity server is appropriate for the network and the SNIB2.
- Setup the Message Queue.
- Import the predefined controller to Velocity.
- Establish communication between the cabinet controller and the Velocity server.
- Download the configuration to the controller.
- Verify the SNIB2 firmware (Xbox properties) is the current revision.
- Create the Velocity Command Sets.
- Change the Velocity Service Settings using the Velocity Service Control Manager. o Enable the Velocity Web Server.
- Activate the Secure Laptop license.
- Connect and configure the enrollment reader.
- Create a Velocity Credential Template.
- Configure Velocity 3.1 Secure Laptop Extension.
- Verify the functionality of the solution.
- Add the Secure Laptop Reports to Velocity

Task Details and Notes

- Install Windows XP Professional or Windows Vista.
- Logon the workstation with the user Administrator or another that is a local Administrators group.
- If using Vista, turn off the User Access Control for the current logon. If this cannot be done, run the install processes as Administrator.
- Get the password complexity rules from IT.
- If desired, install SQL Server 2005.
 - o Refer to the Velocity Installation Guide for the appropriate version and edition of SQL Server.
- Install Velocity 3.1.
 - o Run Setup.exe from the installation CD.
 - o Enter passwords, do not accept the default. Note the passwords; they need to be entered later in the Secure Laptop configuration.
 - o For Vista, add the local administrator as a SQL Server administrator per http://msdn.microsoft.com/en-us/library/bb326612.aspx
 - o Stop the Velocity services. With Vista, the Velocity Service Control Manager may be unable to control the services for administrator rights reasons and therefore Windows Computer Management must be used to manage the Velocity services.
 - o The Velocity CCTV can be disabled because no CCTV cameras are present. Although minimal, this will reduce the load on the system by not running unnecessary processes.

- o Apply Velocity 3.1 updates on the Velocity installation CD or from the Hirsch Electronics Technical Support web site. The format of the update name is Velocity_3-1_Update_KB???.exe.
- Create the Velocity product activation key request file.
 - o Using the Velocity menu option Help About, click the Registry button.
 - o Fill out the information and click Next.
 - o Save the information to a file. Later in the installation process, the file will be emailed to request a product activation key along with a feature activation key.
 - Create and email the Velocity Message Queue Writer feature activation key request.
 - o In Velocity Administration, expand Interfaces Configuration.
 - o Select Message Queue Writer.
 - o Double click on "Add New Message Queue Writer".
 - o The following windows will appear. Click the Copy button to copy the System Identity to the Windows Clipboard.

Feature Activation
This feature is enabled with a Feature Key. The Feature Key is obtained from the Hirsch Sales Department via e-mail at info@hirschelectronics.com or telephone toll free at 1-888 -809-8880 x124. You will need to provide the System Identity displayed below when contacting Hirsch Sales. Hirsch Sales when then provide you with a five-part Feature Key that will need to be entered below.
Feature: Message Queue Writer
System Identity:
E78F86125A788F17FC56CF26A64B6D87 Copy
Feature Key:
Register
Cancel

- o Paste the System Identity in the product activation key request file.
- o Email the product activation key request file to the address provided requesting a product activation key and a Message Queue Writer feature key.
- Run the Velocity 3.1 Secure Laptop Extension setup.
 - o Execute the Setup.exe to install the configuration files on the Velocity server in the folder "Program Files\Hirsch Electronics\Velocity 3.1 SecureLaptop Extension".
- Create and email the activation.act file to license the Velocity 3.1 Secure Laptop Extension from Hirsch Professional Services Group.
 - o Copy the product.info file to the Program Files\Hirsch Electronics\Velocity 3.1 SecureLaptop Extension Service\Installation Files folder.

Run PSGLicensing.exe in Program Files\Hirsch Electronics\Velocity 3.1 SecureLaptop Extension Service\Installation Files.

💾 Hirsch Electronics PSG Licensing
Activation To activate your application license, please enter your Software and Product ID click the generate button. If this is your first time activating your application, an .act file will be generated in the application directory.
Software ID: 10015 Product ID: 0WEAD 0KCV1 L3KH5 H2SLB Generate
If you have obtained an activation.lic file, please browse to the activation.lic file and click the Activate button to complete the application activation process.
License File: Browse
Deactivation To remove your application License, please provide the Software and Product ID to deactivate and click on the deactivate button.
Software ID: 10015 Product ID: 0WEAD 0XCV1 L3KH5 H2SLB Deactivate Wipe

o Click Generate to generate an activation file for Software ID 10015.

o Email the activation file to Hirsch Professional Services Group (PSG).

o Hirsch PSG will create and return a license file.

Backup the Velocity database. MS SQL Server Management Studio can be used to create a backup of the database.

- Turn off the firewall.
- Determine the IP addresses of the Velocity stand alone workstation (server) and the SNIB2.
- Setup the Message Queue.
 - o If not present, add the Windows component MS Message Queue. Use the "Control Panel" "Programs and Features" "turn Windows features on or off" option to add the MSMQ. This actually may take several minutes as stated and require restarting Windows.

💽 Windows Features	- • •
Turn Windows features on or off	0
To turn a feature on, select its check box. To turn a feature check box. A filled box means that only part of the feature	off, clear its is turned on.
Indexing Service	A
🕀 🔳 📗 Internet Information Services	
🕀 🔳 🐌 Microsoft .NET Framework 3.0	
😑 🔲 🐌 Microsoft Message Queue (MSMQ) Server	=
😑 🔽 📙 Microsoft Message Queue (MSMQ) Server C	ore
MSMQ Active Directory Domain Services	Integration 🛄
🛛 📕 MSMQ HTTP Support	
🔽 📙 MSMQ Triggers	
🔽 🚺 Multicasting Support	
MSMQ DCOM Proxy	
🕀 🔳 📔 Print Services	
Remote Differential Compression	-
ОК	Cancel

- o Create a MS Message Queue
 - Use "Computer Management" "Services and Application" "Message Queueing" to create a new queue.
 - Create a private queue for standalone installation and a public queue when using domain accounts. Name it "SecureLaptop".
 - ⁿ Modify the security for the queue.
 - After creating the queue, select the queue, right click and select properties.

Assign the appropriate privileges to a User or Group. Full Control to Everyone works fine.

o Enable/Install the Velocity MS Message Queue Writer

- ⁿ Add-Ins Server Extensions.
- ⁿ Enable the Message Queue Writer and click OK. The Message Queue Writer should be installed but not enabled. There should be no need to click the Install button.
- ⁿ Restart the Extension Service as instructed.
- o Add a Velocity MSMQ Writer
 - ⁿ Administration Interfaces Message Queue Writer.
 - ⁿ Double click on "Add New Message Queue Writer".
 - ⁿ On the first use, enter the feature activation key returned from the registering with Hirsch Electronics.
 - ⁿ Enter the name "SecureLaptop".

🔢 Message Queue Writer - Untitled Propertie	s	
Settings		
Name: SecureLaptop		
Queue: psg-vista\private\$\securelaptop		
Format: Velocity XML 1.0		•
Active during time zone: <a>Always>		-
 Alarms Transactions {Granted/Denied} Internal Events ✓ External Events Miscellaneous Events Communication Events ✓ Software Events Integrated Events 	Selec	it E <u>v</u> ents
✓ Enabled		
Help	ОК	Cancel

 The Queue name is the full name of the "SecureLaptop" MS Message Queue added in the prior step. The format of the queue name for a private queue is machine_name/private\$/SecureLaptop. The full name can be found in the Windows Computer Management – Message Queues. Note the full queue name; it will be entered later in the Velocity 3.2 Secure laptop Extension configuration.

securelaptop Pro	perties	? <mark>×</mark>
General Multica	ast Security	
psg-v	ista\private\$\securelaptop	
Label:	private\$\SecureLaptop	
<u>T</u> ype ID:	{0000000-0000-0000-0000-000000000000}	
	Limit message storage to (KB):	
	Authenticated	
	Nontransactional queue	
Privacy level:	Optional 🔹	
Journal		
<u>E</u> nabled		
Limit jour	nal <u>s</u> torage to (KB):	
	OK Cancel	Apply



- Select the time zone "Always".
- Save the Writer by clicking on OK.
- Reopen the Writer to select the events.
- Click on the checkboxes for Transaction, External and Software.
- Click on the Select Events button.
- Select the events listed below. The events are listed in numerical order.
- Software 1151 Logged on to controller address.
- Transaction 2034 Control Trigger Granted.
- External 4024 Input State Change at Expansion Input.

🔢 Ad	Advanced Event Selection					
Gen	eral					
	Туре	Event No.	Description	^	Select All	
	Software	1148	Import complete. % Person(s) were imported by %			
	Software	1149	Execution failed. Dialup location % is disabled		<u>D</u> eselect All	
	Software	1150	Connecting to controller address %			
	Software	1151	Logged on to controller address %			
	Software	1152	No download required for credential %			
	Software	1153	Alarm viewer preference changed by %			
	Software	1154	Credential %1 assigned to person %2 by %3			
	Software	1155	Credential %1 unassigned from person %2 by %3			
	Software	1156	Modem disconnected. Controller is expected to call Velocit			
	Software	1157	CCTV port % was added by %			
	Software	1158	CCTV port % was deleted by %			
	Software	1159	CCTV port % was changed by %			
	Software	1160	Task schedule % was added by %			
	Software	1161	Task schedule % was deleted by %			
	Software	1162	Task schedule % was changed by %			
	Software	1164	Application defined integration event	Ŧ		
F	lelp		(ок	Cancel	

- Verify the MSMQ Writer is functioning correctly by reviewing the "Velocity MSMQ Writer Extension-Technical Support File.Txt" in "Program Files\Hirsch Electronics\Velocity".
- Add the predefined controller to Velocity.
- The M16 and M2 controllers must be powered and connected to the same network as the Velocity server.
- Add a XNET Port.
- Administration DIGI*TRAC Configuration.
- Select XNET in the left pane and Add Port in the right pane. Name it "Secure Laptop Port". Select XNET and TCP/IP. Run ipconfig from a command window to get the local ID address.
- Select XNET and add a Port. Name it Secure Laptop Port.
- Select the Search button to find the controller. Once found, double click on the SNIB2 to change the SNIB2 settings.
- If not detected, used the snib2config.exe tool in Program Files\Hirsch Electronics\Velocity\Unsupported to
 configure the SNIB2. The IP address and subnet mask should be set to allow the Velocity DIGI*TRAC service
 to communicate with the SNIB2.
- Add an Xbox.
- Select Secure Laptop Port in the left pane and Add XBox in the right pane. Name it "Secure Laptop Xbox". The defaults are fine.
- Add the controller.
- Select Secure Laptop XBox in the left pane and Import Controller in the right pane.

- A wizard will guide you through the import process. Browse and select the xml file from the folder Program Files\Hirsch Electronics\Velocity 3.1 SecureLaptop Extension\Installation Files.
- For the M16 version of the cabinet, use the M16_Velocity 3.1 Secure Laptop Controller Export.xml file for the import.
- For the M2 version of the cabinet, use the M2_Velocity 3.1 Secure Laptop Controller Export.xml file for the import.
- If needed, modify the controller name and description.
- Establish communication between the cabinet controller and the Velocity server.
- Refer to "E-Tool Power up Procedure" section if needed.
- Turn of the power to the cabinet.
- With the power turned off, rotate the cabinet key to turn off the SNIB2 default encryption key.
- Repower the controller. The controller should come online.
- Download the configuration to the controller.
- Verify the SNIB2 firmware (Xbox properties) is the current revision (5.98 as of 4/15/2011).
- Download to Velocity Firmware folder.
- Import latest binary file into Velocity.
- Download latest firmware to each controller as needed.
- After setting up all controllers for new cabinets, disable, then re-enable the port for each controller. This is to verify that the Expansion Input status shows up correctly in Velocity's Status Viewer. The expansion input state is how the Secure Laptop service determines whether or not laptops exist in each drawer. You can verify this is working correctly by selecting Console -> Status Viewer from the Velocity menu:

File Console Wini	dow Add-Ins Help	
Alarma III Gunnte I	Envollment III Gran	hirr Offician Suplayer (Blanestr III Status) 🔐 🗺 🗺 🖄 🔘 🚥 🚇
Alams in events 1	Z emonimente Dig orap	
Masked 🔊 Status Gr	oup 👻 Status Group:	None 🗾 🖬 🕄
[1	
Host Time	Controller Lime	Description Status Group All Legisland de Tababall
4/14/2011 1:44:36 PM		Status choop withinputs added by Tebonom
4/14/2011 1.20.22 PM		Controller Secure Laptop M16-2 was deleted by Tebonory

When you first open this screen, no status groups will be selected. Click on the icon immediately to the right of the status group combo box, (when you hover the mouse over it, "Configure Status Groups" is the tooltip message that pops up). This brings up the Status Viewer properties screen that will be blank. Select the "XInputs" radio button at the top right of the form, and that will cause all Expansion Input entries that are on

your system to appear in the left hand, "Available" window. Select all the addresses that correspond to the controllers you just added. For example, if you added a new controller with address \\XNET.001.0001.001.01, then all its laptop expansion inputs will have that address as their prefix: typically \\ XNET.001.0001.001.01.XI01 to \\XNET.001.0001.001.01.XI16.

Select all the expansion input addresses and click the single ">" arrow button to select them. Enter a name for your new status group:

tatus	Groups Column Headers						
Status	Group: Controller 1		JX	View as: C Doors C Inputs C Relays	ccc	Readers Controllers Xboxes	 C Ports ✓ XInputs ✓ XRelays
Availat	ble			Selected	- 1	4.11	
115	Address	- ^		Name Name		Address	0001.001
414	VVNET.001.0003.001.01.XI13			Xinput 01 D	ſ	WWNET.001	.0001.001
413	VYNET 001 0003 001 01 VI13			Minput 02 D		WWNET 001	.0001.001
+12	VYNET.001.0003.001.01.2112		>>	Minput 03 D	·	WWNET 001	.0001.001
a 11	VYNET 001 0003 001 01 VI11		[amounted]	Minput 04 D	I	WANET OUT	0001.001
e 10	VXNET.001.0003.001.01.X110		>	Xinput 05 D		WWNET 001	0001.001
09	VXNET 001 0003 001 01 X109		(Annual annual a	Xinput 07 D		WET 001	0001.001
1 08	WNET 001 0003 001 01 ×108			Xinput 08 D	,	AVXNET 001	0001.001
t 07	WNET.001.0003.001.01.×107			Xinput 09 D	1	WNET 001	0001.001
t 06	\XXNET.001.0003.001.01.XI06		<<	XInput 10 D	ſ	WNET.001	.0001.001
t 05	\XXNET.001.0003.001.01.XI05			XInput 11 S	D	WNET.001	.0001.001
it 04	\XXNET.001.0003.001.01.XI04			Xinput 12 S	p	WNET.001	.0001.001
it 03	\XXNET.001.0003.001.01.XI03			XInput 13 S	p	WNET.001	.0001.001
it 02	\WNET.001.0003.001.01.XI02			Xinput 14 S	p	WXNET.001	.0001.001
t 01	\VXNET.001.0003.001.01.XI01	+		Xinput 15 S	p	WNET.001	.0001.001
4	m	•		XInput 16 S	p	WNET.001	.0001.001

Click the OK button, and this returns you to the Status Viewer screen where you can see the status of your expansion inputs. If everything is set up correctly and Velocity is communicating with the controllers, then you'll see info under the Status, 1ALRM, and 2RQE fields for each address:

Masked 🚯 Status Group 💌	Status Group: Controller 1	- 20					
XInput Name	Address	Status	Alarm	Masked	Enabled	1ALRM	-
🛞 Xinput 01 Drawer Input 1	WANET.001.0001.001.01.301	OPEN		3.4	Yes	11	
🔌 Xinput 02 Drawer Input 2	\W/NET.001.0001.001.01.302	Secure		3	Yes	×	
🔌 Xinput 03 Drawer Input 3	\W/NET.001.0001.001.01.2003	Secure			Yes	×	
🔌 Xinput 04 Drawer Input 4	\V-NET.001.0001.001.01.2004	Secure	2	10	Yes	×	
Alinput 05 Drawer Input 5	\VvNET.001.0001.001.01.XI05	Secure		1	No	×	
🔌 Xinput 06 Drawer Input 6	\W/NET.001.0001.001.01.X106	Secure	+	84	Yes	×	
Anput 07 Drawer Input 7	WONET.001.0001.001.01.007	Open Circuit	÷.	2	Yes	Open Circuit	
Minput 08 Drawer Input 8	\\v0NET.001.0001.001.01.X108	Open Circuit	10		Yes	Open Circuit	
Kinput 09 Drawer Input 9	WONET.001.0001.001.01.0109	Open Circuit	10	38	Yes	Open Circuit	
Kinput 10 Drawer Input 10	\WNET.001.0001.001.01.210	Open Circuit	10	12	Yes	Open Circuit	
Minput 11 Spare	WKNET.001.0001.001.01.X11	Open Circuit			Yes	Open Circuit	
Anput 12 Spare	WANET.001.0001.001.01.X12	Open Circuit		1.	Yes	Open Circuit	
Minput 13 Spare	\WNET.001.0001.001.01.313	Open Circuit	40	25	Yes	Open Circuit	
Xinput 14 Spare	\VXNET.001.0001.001.01.X114	Open Circuit	98	3	Yes	Open Circuit	
	natio'						-

If Velocity and the controller are not communicating, then all those field values will be blank since Velocity can't tell their status:

Alarms III Events 🚯	Enrollment T Graphics	/ideo Explorer 🚜 Ri	ports 🕅 Status	DI PAT (07 °G @		1-1-
Masked 🚯 Status Grou	up 👻 Status Group: Controller 1		-60		-		_
XInput Name	Address	Status	Alarm	Masked	Enabled	1ALRM	2
Anput 01 Drawer Inp	VXNET.001.0001.001.01.XI01			24.	Yes		
Alinput 02 Drawer Inp	\VXNET.001.0001.001.01.XI02	12	2.5		Yes	123	14
剩 XInput 03 Drawer Inp	VVNET.001.0001.001.01.X03	549 C			Yes	4.5	
- XInput 04 Drawer Inp	\VXNET.001.0001.001.01.XI04	100	1.00	÷.	Yes	8	
🔫 XInput 05 Drawer Inp	WWNET.001.0001.001.01.XI05			4	Yes	, 1 5	.+
🔫 Xinput 06 Drawer Inp	WONET.001.0001.001.01.005			(4)	Yes	1	÷
-) XInput 07 Drawer Inp	\WNET.001.0001.001.01.XI07	1011		18	Yes	×.	
- Xinput 08 Drawer Inp	\VXNET.001.0001.001.01.X108	881	100	850	Yes	* S	
🔫 XInput 09 Drawer Inp	\VXNET.001.0001.001.01.XI09	8	100	150	Yes	50	1
Anput 10 Drawer Inp	WWNET.001.0001.001.01.XI10	-			Yes		
-) Xinput 11 Spare	WWNET.001.0001.001.01.XI11				Yes	*	
- Xinput 12 Spare	\VXNET.001.0001.001.01.XI12		0.20	2	Yes	20.	
- Xinput 13 Spare	\VXNET.001.0001.001.01.XI13		1.	+	Yes	¥3	
-) Xinput 14 Spare	WNET.001.0001.001.01.X114	14	5/251		Yes	4	
-) Xinput 15 Spare	WANET.001.0001.001.01.X115	940		(2 1) = 1	Yes	¥0	+
W W 10 P							_
Host Time	Controller Time De	scription					
4/14/2011 1:56:02 PM	Stat	tus Group Controller 1 a	dded by TebohoN				
4/14/2011 1:44:56 PM	Stal	tus Group All Inputs ad	ded by TebohoN				

- Create the Velocity Command Sets. This step is only required for M16 version controller cabinets. The command sets are executed by the service each time it receives the controller logged on even for the M16, to turn on the LEDs.
 - o The Command Sets are used when the controller logs onto Velocity with event number 1151. This occurs when powering up or when the controller is enabled.

- o Modify controller name and execute the SQL script Program Files\Hirsch Electronics\Velocity 3.1 SecureLaptop Extension\Installation Files\Create Command Sets.sql.
 - ⁿ Modify the controller name in the script to match the controller name defined in Velocity.
- Change the Velocity Service Settings using the Velocity Service Control Manager in the System Tray.

Velocity Settings	
System CCTV Database Network Diagnostics Advanced Web Server	These settings are used to re-configure factory defaults for database connectivity and CCTV and to assist in troubleshooting Velocity.
Help	OK Cancel

- o Diagnostics
 - n Within the Velocity Settings, select the Diagnostics. Check the "Enable line voltage updates on input state changes".
- o Web Server.
 - ⁿ Enable the Web Server.
 - ⁿ Change the port to 8080.
- o Restart the Velocity services as instructed.
- o Verify the Velocity Web Server is serving by starting Internet Explorer and entering the url http://localhost:8080. The web server should return a page noting it from the Velocity Web Server.
- o A XML RPC test tool is included to test the functionality of the Velocity Web Server. This is only needed if the Secure Laptop Extension service is not connecting to the Velocity HTTP Server.
- Activate the Secure Laptop license.
 - o Copy the returned .lic file from Hirsch in the Program Files\Hirsch Electronics\Velocity 3.1 SecureLaptop Extension Service\Installation Files folder.
 - o Run PSGLicensing.exe in Program Files\Hirsch Electronics\Velocity 3.1 SecureLaptop Extension Service\Installation Files.

o Browse to license file folder and select the .lic file.

- o Click Activate. A confirmation message will be displayed.
- Connect and configure the enrollment reader.
 - o Insert the SCR3311 reader into USB slot on the enrollment workstation. No special drivers are needed. Windows should detect it and make it ready for use.
 - o Enrollment Manager Tools User Defined Fields
 - Pick a User Defined Field (UDF) and change the caption to DoD EDIPI and change the type from Text to Number.
 - o Enrollment Manager Tools Device Configuration
 - ⁿ Select the PIV Readers tab.
 - ⁿ Check Enable
 - ⁿ Select the CAC Reader from the reader drop down list
 - ⁿ MAP the UDFs. Drag CAC source fields to Velocity fields.
 - Map the name fields.
 - Map the DODEDIPersonalIdenity to the DoD EDIPI UDF field.
 - o Enrollment Manager Tools Preferences.
 - ⁿ Select a UDF other than EDIPI as the UDF to parse the name.
- Create a Velocity Credential Template.
 - o Administrator Velocity Configuration Credential Templates.
 - o Add a template named "Secure Laptop" with the following on the General tab.
 - n IDF 2 Card.
 - ⁿ Card Type Octal Passthru.
 - ⁿ Card Data Select the UDF button.

- Check the checkbox for DoD EDIPI.
- o Select the Credential Functions tab.
 - ⁿ Add a function for Relay Trigger.
 - Select the controller.
 - Select SCZ62.
 - Click Add.
- o Click OK and OK to save the template.
- Configure Velocity 3.1 Secure Laptop Extension.
 - o Do not use: Start All Programs Velocity 3.1 Secure Laptop Configuration because it cannot be ran as Administrator. In Windows Explorer, run the configuration program as Administrator.
 o Refer to the "Velocity 3.1 Secure Laptop Extension" section.

The SQL Server Name includes the instance name if not the default instance. The format is machine_name\instance_name. Use the regedit command to view the value in *HKEY_LOCAL_MACHINE\SOFTWARE\HirschElectronics\Velocity\Database\ServerName.*

- o The database name is Velocity.
- o The App. Role is Velocity Users.
- o Enter the same password that was noted when installing Velocity. The "Velocity Users" App Role password can be reset using the Microsoft SQL Server Management Studio under Velocity Security Roles Application Roles. Right click on Velocity Users, select Properties and reset the password. The next time the Velocity client is opened, the same password must reentered for the client software.
- o The Queue name is the full name of the "SecureLaptop" queue. The name format for a private queue is machine_name/private\$/SecureLaptop. In Windows Computer Management, the name is found in the Properties of the SecureLaptop private queue.
- o XML RPC Connection.
 - Operators can be found in Velocity Administration Velocity Configuration Operators. The Domain value precedes the Operator Name.
 - Set the Port to 8080.
 - Use the XML RPC Test Tool included on the installation CD to confirm the XML RPC functionality and compare the Test Tool values to the Secure Laptop Configuration settings.
- o Click on the "Database Tables" button to create and set the permissions on the tables used by the Secure Laptop Extension.
- Verify the functionality of the solution.
 - o In Window Computer Management, expand the Service and find Velocity 3.1 Secure Laptop.
 - o Select the service and right click to modify the Properties.
 - o Change the logon to an appropriate Velocity Operator.
 - o Start the Velocity Secure Laptop service.
 - o Review the log file in Program Files\Hirsch Electronics\Velocity 3.1 SecureLaptop Extension Service.
 - o Enroll a person by scanning their CAC card and create a credential from the credential template. Verify the credential was downloaded successfully to the controller.
 - o Have card holder use their card at the cabinet.

In Windows Computer Management – MSMQ – Private Queues – SecureLaptop, verify the messages are being written to the queue.

- o If necessary, use the XML RPC Test Tool to confirm the XML RPC functionality and compare the Test Tool values to the Secure Laptop Configuration settings.
- o From Start All Programs Velocity 3.1 Secure Laptop, select the Monitor application.
- o Refer to the "Velocity 3.1 Secure Laptop Extension" section.
- Add the Secure Laptop Extension Reports to Velocity.
 - o Add a printer to the Velocity server.
 - In Velocity, select the menu option Console Preferences and then the Printers tab. Select a printer as the Report printer. "Microsoft XPS Document Writer" is acceptable.
 - o Create the views and function.
 - The SQL is in zip file in "C:\Program Files\Hirsch Electronics\Velocity 3.1 SecureLaptop Extension Service\InstallationFiles\ViewsAndReports.zip". The file name is: "Create PSGSecureLaptop Function and Views.sql".
 - o Check the permissions on views.
 - Select each view, right click and select Properties. Modify the permission for "Velocity Users" app role to match the other views.
 - o Add reports.
 - ⁿ Copy the .rpt files to Program Files\Hirsch Electronics\Velocity\Reports.
 - ⁿ In Velocity Report Manager, create a new report group.
 - Select an existing group and click on the "Add Group" toolbar icon.
 - Name the new group "Secure Laptop".
 - ⁿ Select the "Secure Laptop" group.
 - ⁿ Select the "Add Report" toolbar icon and select one of the Secure Laptop reports.
 - ⁿ Select the added report and import the report definition file.
 - ⁿ Repeat for all Secure Laptop reports.
 - o Test the reports.
- Optionally configure the Velocity Status Viewer.
 - o The Status Viewer enables you to quickly review all the current hardware component settings.
 - o Select Status on the Velocity tool bar.
 - o Select the Configure Status Groups icon on the Status Viewer tool bar.
 - o Enter the name of a new Status Group.
 - o Select XInputs, XRelays, Controllers, etc.
 - o Use the buttons to make the Available XInputs, XRelays, Controllers, etc. Selected.
 - o Click OK when all components are selected.
 - o Refer to Velocity help for further assistance.

Troubleshooting

The scope of troubleshooting Velocity can be extensive but this section will focus on the areas most relative to the Secure Laptop Extension. Generally troubleshooting will be needed to resolve a problem where a card holder is unable to check-in or check-out a laptop. The basic troubleshooting procedure will be to follow the flow of data, determine the point in the flow that failed and then take the necessary action to resolve the cause. The data flow process described in the overview will be followed to diagnose and correct the problem. Each step in the flow starting from beginning must be verified that it is working properly until the step that failed is encountered.

- 1. There are several logs that can be reviewed to determine the cause.
 - a. Windows Event Log. The Windows Event Viewer can be used to review the Windows Logs. These logs usually contain information at a high level such as services starting, security failures, etc.
 - b. Velocity log files. Several log files in "C:\Program Files\Hirsch Electronics\Velocity" can be reviewed. The files are named: "Velocity ...-Technical Support File.txt".
 - c. Velocity SecureLaptop Extension log files. 2 log files in "C:\Program Files\Hirsch Electronics\Velocity 3.1 SecureLaptop Extension Service" have information specifically for the Secure Laptop Extension. The file names are: "SecureLaptop TransactionLog.txt" and 'Velocity 3.1 SecureLaptop Extension Service-PSG Support Log.txt".
- 2. Verify the cabinet is properly communicating with Velocity.
 - a. The Velocity Event Viewer and the Status Viewer show the activity and the status of the hardware. Use Velocity Administration – DIGI*TRAC Configuration to manage the DIGI*TRAC hardware. In the DIGI*TRAC Configuration, expand the Port, Xbox and Controller and attempt to trigger an expansion relay. The cause may be the network, bad patch cable, unplugged patch cable, broken encryption, one or more of the Velocity services are stopped especially the DIGI*TRAC service, etc. Minimally, the Velocity workstation should be able to ping the IP address of the cabinet.
- 3. The CAC is not read successfully.
 - a. The card may be damaged. The card holder may have entered the incorrect PIN. The issue might be with the cabinet.
 - b. The cardholder may be entering their PIN before the reader is ready. After inserting the CAC, wait for the keypad indicator to light up before entering their PIN.
- 4. The CAC read results in Control Denied.

The person and card might not be enrolled in Velocity. A credential may exist for the card but the credential function might not exist. The function may exist but the trigger relay may not exist for the particular controller. The EDIPI number could also be incorrect.

- 5. The card read results in Control Granted but a drawer is not unlocked.
 - a. Review the SecureLaptop log files. These files will be have detailed processing information when Velocity and the Velocity SecureLaptop Extension are running properly.
 - b. Since the event successfully reached Velocity, the subsequent step is for Velocity to write the event to the MS Message Queue. Stop the Velocity SercureLaptop Service while keeping the other Velocity services running. The events should be written to the MS Message Queue. Check the queue to see if they were written to the queue. If that is successful, restart the SecureLaptop service. Starting the service purges the queue. Retry the card and review the Securelaptop logs.
 - c. Review the log files to determine if the service attempted to unlock a drawer.
 - d. If a drawer with a laptop was available, then XML should have been sent to the Velocity web server to unlock the drawer. The XML RPC Test Tool can be used to verify the XML-RPC Web Server is working properly. The Secure Laptop Monitoring application show the availability of the laptops.

Velocity 3.1 Secure Laptop Extension

The Velocity 3.1 Secure Laptop Extension is made up of three components: 1) The "Hirsch SecureLaptop Service" 2) the "SecureLaptopConfig" used to configure the settings for the service, and 3) the "SecureLaptopClient" displays information about the transactions and users that are managed by the service.

Configuration:

• Run the SecureLaptop setup file. This installs all three components

- Review the "Log On" properties for the "Velocity 3.1 SecureLaptop Extension Service".
- Verify the Velocity XML RPC web service is up and running.
- Define a Velocity Message Queue Writer that the service will connect to, and make sure it is up and running. When selecting the events to be written to the MS Message Queue Writer, select all "Transaction" and all "External Events". (The service listens only for 2034 Control Trigger Granted transaction events, and 4024 Input State Change at Expansion Input external events. Here's a sample screenshot of a Velocity Message Queue Writer that's setup of the Secure Laptop Extension:

Image: SecureLaptop Image: SecureLaptop			
 Alarms IIII Events S Enrollment IIII Graphics IIII Video Explorer IIIII Reports IIII Status IIIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIII			
 Configuration Velocity Configuration Add New Message Add New Message Add New Message Add New Message Message Queue Writer - SecureLaptop Properties SecureLaptop SecureLaptop SecureLaptop Queue: VelocityWS\SecureLaptop VelocityWS\SecureLaptop Format: VelocityXML 1.0 Active during time zone: <always></always> 			
Alarms ☐ Transactions (Granted/Denied) ☐ Internal Events ☐ External Events ☐ Communication Events ☐ Software Events ☐ Integrated Events ☐ Integrated Events ☐ Enabled <u>Help</u> OK Cancel			
PETEH O Active Alarms: 3 O Ack. Alarms: 0 O Off Normal: 0 Download Monitor Threat Level: Level 00 4/29/2010 //			

Initial Configuration:

- Open the services control panel applet and configure the "Hirsch SecureLaptop" service so it logs in using a windows account that has the necessary permissions to connect to the Velocity SQL Server database
- Run the SecureLaptop Service Configuration utility that should now appear in your programs menu. This is the screen you use to configure how the service connects to the Velocity database, and Message Queue Writer. This is a sample screenshot of the screen with all required info on a test machine:

🖶 Secure	Laptop Config	- • •	
SQL	Server Connection		
SQL	. Server Name:	seclaptop-vista\hirsch	
Data	abase Name:	Velocity	
Арр	Role:	Velocity Users	
Арр	Role Password:	*****	
Rep	eat Password:	******	
MSM	MSMQ Connection		
MSN	4Q Name:	seclaptop-vista\securela	
XML	XML RPC Connection		
Velo	city Server Name:	seclaptop-vista	
Velo	city Operator Name:	tebohon	
Оре	rator Password:	*****	
Rep	eat Password:	*****	
Velo	city Domain:	Hirsch	
Port:		8080	
Other Configuration			
Rela	ay Timeout (secs):	60	
Lap	top Return Timer (secs):	60	
Rec	harge Time (mins):	0	
Мах	: Log File Size (MB):	1	
Max Backup Log Files to Keep: 1			
Database Tables			

The configuration fields are:

- SQL Server Name: The name of Velocity's SQL Server instance.
- Database Name: The name of the Velocity database.
- App Role: The name of the Velocity application role "Velocity Users".
- App Role Password: The application role password entered during Velocity installation.
- MSMQ Name: The name of the defined MS Message queue.
- Velocity Server Name: The Windows machine name for the server that has Velocity installed.
- Velocity Message Queue Writer Connection Port: The port that the Velocity Message Queue Writer is configured to listen on.
- Velocity Operator Name: The name of a valid operator in Velocity.
- Operator Password: The velocity operator's password.
- Velocity Domain: The domain Velocity is installed in.
- XML RPC Port: The port that the XML RPC web service is listening on.
- Relay Timeout: The period of time in seconds that the service waits after firing a relay for the corresponding input state change event, (which gets sent when a user adds or removes a laptop). Make sure this timeout is at least as long as all the relay timeouts that are set in Velocity for the SecureLaptop cabinet.

- Laptop Return Timeout: The period of time in seconds that the service waits after firing a relay to check if the laptop has been returned. The service saves the corresponding input state change events, (which gets sent when a user adds or removes a laptop) and waits until the timeout is reached or another card is swiped. After the wait, the service will check the status of the returned laptop. If the laptop is present, the transaction is closed disassociating the card holder from that laptop. If the laptop is not present, the transaction will remain open and laptop will remain checked out to the card holder. Make sure this timeout is at least as long as all the relay timeouts that are set in Velocity for the SecureLaptop cabinet.
- Recharge Time: The period of time in minutes that must elapse after a laptop gets returned before the service will make it available to be removed by the next user.
- Max Log File Size: The service logs all activity it performs to a text log file in the same path as the service's executable file. Set this value to 0 to have the service append to the log file indefinitely. If this value is greater than 0, as soon as the log file size is greater than this value, the service will start a new log file, backing up the current file if configured, or deleting it if not.
- Max Backup Log Files to Keep: If the Max Log File Size is set, when a new file gets created, the previous files get saved up to the number indicated by this value.
- Click on the "Database Tables" button to create the tables used by the Secure Laptop Extension.

Running SecureLaptop:

After entering the configuration information for your system, you should be able to run the service from the services control panel applet.

When the service runs, it waits indefinitely for messages to come in from the Velocity Message Queue Writer. The service defines a new "laptop transaction" each time it receives a 2034 Control Trigger Granted event. There are currently two types of transactions that are supported: "Get Laptop" and "Return Laptop" transactions.

When a Velocity user is granted access, if they already have a laptop assigned to them, (which happens when a record for their user exists in the PSGSecureLaptopUsers table), then the service starts a new Return Laptop transaction. If not, then a new Get Laptop transaction is started.

After the current transaction type is determined, the service will fire the relay for the transaction so the user can either return or remove their laptop. When a laptop is added or removed, the service receives the corresponding state change event from the Velocity Message Queue Writer, after which it completes the transaction.

Use the SecureLaptop Service Monitor client program to see status and transaction info for the service. This client program is installed in the same folder as the service, (and must be run from that location because it loads the service's configuration information from that location).

There are three main screens to the client program. The first shows information about the laptop expansion inputs as the service sees them in Velocity, and the current SecureLaptop users that are being managed by the service:


Controllers: Secure Laptop Case M16								
Controllers:	Secure Laptop Case M16							
Kinput Id	Address		Laptop Status		Last Returned D	ate	Next Laptop Index	
31	\\01.01.01.001.01.X01		LAPTOP NOT AVAILABLE		10/12/2009 4:55	5.06 PM		
2	\\01.01.01.001.01.X02		Laptop is present		10/19/2009 11:1	13.22 AM	1	
3	\\01.01.01.001.01.X03		Laptop is present		10/19/2009 11:51:34 AM 2 10/12/2009 4:59:22 EM 2			
4	\\01.01.01.001.01.004		Laptop is present		10/12/2009 4:58	8.22 PM	3	
5	\\01.01.01.001.01.005		Laptop is present	10/16/2009 12:25:51 PM 4 10/16/2009 12:43:55 PM 5				
6	V01.01.01.001.01.X06	J1.01.001.01.2006 Laptop is present					0.00	
a c	VUD.01.00.001.01.X007		[Xinput for this laptop is DISA	BLED J				
8	\\01.01.01.001.01.X08		Xinput for this laptop is DISA	BLED J				
A 10	VUD.01.01.00.001.01.2009		20 August for this laptop is DISA	BLED				
A 11	V01.01.01.001.01.2010		[Xinput for this laptop is DISA	BLED J				
A 12	V01.01.01.001.01.01.011		[Ainput for this laptop is DISA [Manual for this laptop is DISA	BLED I				
A 12	V01.01.01.001.01.2012		[Minput for this taptop is DISA [Minput for this taptop is DISA	BLED J				
A 14	VID1.01.01.001.01.2113		[Vinput for this laptop is DISA [Vinput for this laptop is DISA	RIEDI				
A 15	V01.01.01.001.01.01.014		Example for the laptop is bras-	GLED J				
	STATE AND AND ADDRESS AND ADDRESS ADDRESS		1 X IPPE & DOI 1000 Landon PLAS 345	OPEN CIRCUIT 1				
16	\\01.01.01.01.001.01>016		[Xinput for this laptop has an [Xinput for this laptop has an	OPEN CIRCUIT] OPEN CIRCUIT]				
15 16 urrent User	V.01.01.01.001.01.216		[Xinput for this laptop has an	OPEN CIRCUIT] OPEN CIRCUIT]				
Add User	V01.01.01.00.01.01.2016 s with Laptops Delete User Name	Condential Id	[Anput for this laptop has an [Minput for this laptop has an	DPEN CIRCUIT] OPEN CIRCUIT]	Transaction Date	Lanton Terr	•	
Add User	Vx01.01.01.001.01.2016 s with Laptops Delete User Name Billy Bob	Credential Id	[Anput for this laptop has an [Anput for this laptop has an Laptop Address (V01.01.01.001.01.3001	OPEN CIRCUIT] OPEN CIRCUIT] Transaction Id 56	Transaction Date 10/16/2009 10:44-41	Laptop Tim 4 days, 5 h	e	
Add User User Id 3	V.01.01.01.00.01.01.216 s with Laptops Detete User Name Billy Bob	Credential Id 4	Laptop Address	OPEN CIRCUIT] OPEN CIRCUIT] Transaction Id 56	Transaction Date 10/16/2009 10:44:41	Laptop Tim 4 days, 5 h	e ours, 40	
Add User User Id 3	V.01.01.01.00.01.012016 s with Laptops Delete User Name Billy Bob	Credential Id 4	Laptop Address	OPEN CIRCUIT] OPEN CIRCUIT] Transaction Id 56	Transaction Date 10/16/2009 10:44:41	Laptop Tim 4 days, 5 h	e ours, 40	
Add User Add User User Id 3	W01.01.01.001.01.2016 s with Laptops Detete User Name Bity Bob	Credential Id 4	Laptop Address	OPEN CIRCUIT] OPEN CIRCUIT] Transaction Id 56	Transaction Date 10/16/2009 10:44:41	Laptop Tim 4 days, 5 h	e ourt, 40	
And User Add User User Id 3	VX01.01.01.001.01.2016 s with Laptops Detete User Name Billy Bob	Credential Id 4	Laptop Address	OPEN CIRCUIT] OPEN CIRCUIT] Transaction Id 56	Transaction Date 10/16/2009 10:44:41	Laptop Tim 4 days, 5 h	e	
And User Add User User Id 3	Vx01.01.01.001.01.2016 s with Laptops Delete User Name Billy Bob	Credential Id 4	Laptop Address	OPEN CIRCUIT] OPEN CIRCUIT] Transaction Id 56	Transaction Date 10/16/2009 10:44:41	Laptop Tim 4 days, 5 h	e	
And User Add User User Id 3	V.01.01.01.00.01.2116 s with Laptops Delete User Name Billy Bob	Credential Id 4	Laptop Address	OPEN CIRCUIT] OPEN CIRCUIT] Transaction Id 56	Transaction Date 10/16/2009 10:44:41	Laptop Tim 4 days, 5 h	e	
And User Add User User Id 3	V.01.01.01.00.01.2016 s with Laptops Delete User Name Billy Bob	Credential Id 4	Laptop Address V01.01.00.001.01.2001	OPEN CIRCUIT] OPEN CIRCUIT]	Transaction Date 10/16/2009 10:44:41	Laptop Tim 4 days, 5 h	e ours, 40	
Add User Add User User Id 3	Vx01.01.01.001.01.2016 s with Laptops Delete User Name Billy Bob	Credential Id 4	Laptop Address	OPEN CIRCUIT] OPEN CIRCUIT] Transaction Id 56	Transaction Date 10/16/2009 10:44:41	Laptop Tim 4 days, 5 h	e ours, 40	

At the top is the "Laptop Status in Velocity" data. This shows the hardware status of the expansion inputs as obtained from Velocity. This data should always match what you see if you open up the Status Viewer screen in the Velocity client application. The service will ignore expansion input address that are disabled or are otherwise not configured.

At the bottom is data for the current users who have laptops as managed by the service.

The second tab on the SecureLaptop Service Monitor client program shows user history for all users who have successfully retrieved, and returned a laptop using the service. This data comes from the PSGSecureLaptopUserHistory table in the Velocity database:

5 Judy 6 6 Tamm 7 Jeenn 1 Frank 4 John 5 Judy 6 7 Tamm 3 Billy 8 1 Frank 1 Frank 1 Frank	ly Bloom nnny Aames mry Cunningham nk Smith n Doe ly Bloom nnny Aames r Bob	Vi01 01 01 001 01 01 005 Vi01 01 01 001 01 005 Vi01 01 01 001 01 005 Vi01 01 01 001 01 0100 Vi01 01 01 001 01 000 Vi01 01 01 001 01 000 Vi01 01 01 001 01 000 Vi01 01 01 000 001 01 000	4 minutes 16 minutes 6 minutes 3 days, 30 minutes 3 days, 1 hour, 6 min. 1 hour, 59 minutes	10/19/2009 11:11:55 AM 10/19/2009 10:59 48 AM 10/16/2009 343:14 PM 10/16/2009 343:14 PM 10/16/2009 10:45:45 AM 10/16/2009 10:45:15 AM 10/16/2009 10:44:11 AM	10/19/2009 11:16:34 AM 10/19/2009 11:16:30 AM 10/16/2009 3:49 48 PM 10/19/2009 11:16:40 AM 10/19/2009 11:51:34 AM	6 7 8 2	0 0 0 0 0 0
6 Tamm 7 Jerem 1 Ftank 4 John 5 Judy 6 Tamm 3 Billy B 1 Ftank 1 Ftank 1 Ftank	nny Aames my Cunningham nk Smith n Doe ly Bloom nny Aames I Bob	V(01,01,01,001,01,2405 V(01,01,01,001,01,2405 V(01,01,01,001,01,2405 V(01,01,01,001,01,2404 V(01,01,01,001,01,2405 V(01,01,01,001,01,2405	16 minutes 6 minutes 3 days, 30 minutes 3 days, 1 hour, 6 min. 1 hour, 59 minutes	10/19/2009 10:59 48 AM 10/16/2009 3:43:14 PM 10/16/2009 10:45:45 AM 10/16/2009 10:45:15 AM 10/16/2009 10:45:15 AM	10/19/2009 11:16:30 AM 10/16/2009 3:49:48 PM 10/19/2009 11:16:40 AM 10/19/2009 11:51:34 AM	7 8 2	0
7 Jerem 1 Frank 4 John 5 Judy 6 Tame 3 Biby 8 1 Frank 1 Frank 1 Frank	en y Cunningham nk Smith n Doe ly Bloom nny Aames I Bob	V(01.01.01.001.01.2005 V(01.01.01.001.01.2004 V(01.01.01.001.01.2004 V(01.01.01.001.01.2003 V(01.01.01.001.01.2005	6 minutes 3 days, 30 minutes 3 days, 1 hour, 6 min. 1 hour, 59 minutes	10/16/2009 3:43:14 PM 10/16/2009 10:45:45 AM 10/16/2009 10:45:15 AM 10/16/2009 10:44:11 AM	10/16/2009 3:49 48 PM 10/19/2009 11:16:40 AM 10/19/2009 11:51:34 AM	8	0
1 Frank 4 John 1 5 Judy 8 6 Tamm 3 Billy 8 1 Frank 1 Frank	nk Smith in Doe ly Bloom nmy Aames i Bob	V01.01.01.001.01.003 V01.01.01.001.01.003 V01.01.01.001.01.006 V01.01.01.001.01.006	3 days, 30 minutes 3 days, 1 hour, 6 min. 1 hour, 59 minutes	10/16/2009 10:45:45 AM 10/16/2009 10:45:15 AM 10/16/2009 10:44:11 AM	10/19/2009 11:16:40 AM 10/19/2009 11:51:34 AM	2	0
4 John 1 5 Judy 8 6 Tamm 3 Billy B 1 Frank 1 Frank 1 Frank	n Doe ly Bloom nny Aames y Bob	V.01.01.01.001.01.003 V.01.01.01.001.01.006 V.01.01.01.001.01.005	3 days, 1 hour, 6 min. 1 hour, 59 minutes	10/16/2009 10:45:15 AM 10/16/2009 10:44:11 AM	10/19/2009 11:51:34 AM		
5 Judy 5 6 Tamm 3 Billy B 1 Frank 1 Frank 1 Frank	ly Bloom nny Aames 9 Bob	V01.01.01.001.01.208 V01.01.01.001.01.205	1 hour, 59 minutes	10/16/2009 10:44:11 AM	and the shares and the state and the s	5	0
6 Tanun 3 Billy B 1 Frank 1 Frank 1 Frank	nny Aanes Bob	Vi01.01.01.001.01.3405	Sharp distant		10/16/2009 12 43:55 PM	6	6
3 Billy B 1 Frank 1 Frank 1 Frank	Bob	and the she when the hard a sector	1 nour, 42 minutes	10/16/2009 10:43:44 AM	10/16/2009 12:25:51 PM	7	7
1 Frank 1 Frank 1 Frank	A	1002 101.01.001.01.001	0 minutes	10/13/2009 3 38:04 PM	10/13/2009 3:38:40 PM	7	7
1 Frank 1 Frank	nk Smith	\\01.01.01.001.01.>004	0 minutes	10/12/2009 4:57:28 PM	10/12/2009 4:58:22 PM	2	2
1 Frank	nk Smith	\\01.01.01.001.01.003	0 minutes	10/12/2009 4 55:48 PM	10/12/2009 4:56:33 PM	2	2
	nk Smith	\\01.01.01.001.01.3001	0 minutes	10/12/2009 4:54:42 PM	10/12/2009 4:55:06 PM	2	2
1 Frank	nk Smith	\\01.01.01.001.01.201	3 minutes	10/12/2009 4:44:49 PM	10/12/2009 4:47:55 PM	2	2
3 Billy B	Bob	\\01.01.01.001.01.001	1 day, 2 hours, 1 min	10/12/2009 1:24:08 PM	10/13/2009 3:25:11 PM	4	2
2 TomJ	n Jones	VV01.01.01.001.01.X002	6 days, 21 hours, 50	10/12/2009 1:22:55 PM	10/19/2009 11:13:22 AM	3	3
1 Frank	nk Smith	\\01.01.01.001.01.201	1 minute	10/12/2009 1:22:31 PM	10/12/2009 1:23:38 PM	2	2
1 Frank	nk Smith	\\01.01.01.001.01.2001	0 minutes	10/8/2009 4:06:52 PM	10/8/2009 4:07:47 PM	2	2
1 Frank	nk Smith	VV01.01.01.001.01.2001	5 minutes	10/8/2009 11:41:01 AM	10/8/2009 11:46:59 AM	2	2
1 Frank	nk Smith	\\01.01.01.001.01.201	0 minutes	10/8/2009 11:02:17 AM	10/8/2009 11:02:47 AM	2	2
1 Frank	nk Smith	VV01.01.01.001.01.2001	10 minutes	10/7/2009 12:38:43 PM	10/7/2009 12:49:12 PM	2	2
1 Frank	nk Smith	\\01.01.01.001.01.3001	10 minutes	10/7/2009 12:38:43 PM	10/7/2009 12:49:12 PM	2	2

The third tab on the SecureLaptop Service Monitor client program shows transaction history for all transactions that have occurred in the service. SecureLaptop transactions always start when a 2034 Control Trigger Granted event arrives from the Velocity Message Queue Writer:

See Env									
Successful	Transaction Id	Credential Id	UserId	Name	Transaction Type	Laptop Address	Enor	Time	
True	78	0	4	John Doe	MANUAL RETURN Lapt			10/19/2009 11:51:34	
True	77	0	1	Frank Smith	MANUAL RETURN Lapl			10/19/2009 11:16:40	
O True	76	0	5	Judy Bloom	MANUAL RETURN Lapt			10/19/2009 11:16:34	
O True	75	0	6	Tammy Aames	MANUAL RETURN Lapt			10/19/2009 11:16:30	
Falce	74	8	7	Jeremy Cunningham	GET Laptop		ProcessControlGrant faile.	10/19/2009 11:14:08	
O True	73	3	2	Tom Jones	RETURN Laptop	\\01.01.01.001.01.002		10/19/2009 11:13:19	
A False	72	8	7	Jeremy Cunningham	GET Laptop		ProcessControlGrant faile	10/19/2009 11:12:28	
O True	71	6	5	Judy Bloom	GET Laptop	\\01.01.01.001.01.005		10/19/2009 11:11:52	
A False	70	6	5	Judy Bloom	GET Laptop		ProcessInputStateChang	10/19/2009 11:10:15	
A False	69	6	5	Judy Bloom	GET Laptop		TIMEOUT ERROR for L	10/19/2009 11:09:36	
O True	68	7	6	Tammy Aames	GET Laptop	\\01.01.01.001.01.205		10/19/2009 10:59 45	
O True	67	7	7	Jeremy Cunningham	MANUAL RETURN Lapl			10/16/2009 3 49 48 8	
O True	66	8	7	Jeremy Cunningham	GET Laptop	\\01.01.01.001.01.205		10/16/2009 3 43 10 8	
A Faine	65	8	7	Jeremy Cunningham	GET Lanton		ProcessControlScant faile	10/16/2009 1:37:44	
A False	64	8	7	Jeremy Curningham	GET Lanton		ProcessControllisant faile	10/16/2009 12:44:20	
() Inst	63	6	5	Jude Bloom	RETURN Lactor	V01.01.01.001.01.2006		10/16/2009 12:43:52	
A False	62	8	7	Jeremy Curningham	GET Laotoo	100000000000000000000000000000000000000	ProcessControlEsant taile	10/16/2009 12 41 27	
A False	61	8	7	Jeremu Cuppingham	GET Lastro		TIMEOUT FRROR IN L	10/16/2009 12 26 18	
() Tare	60	7	6	Tammu dames	BETLIBN Lanton	V01.01.01.001.01.205	The sect stringer to se	10/16/2009 12:25:45	
A False	59	8	7	Jeremy Cunningham	GET Lanton	10010010010010000	ProcessControlScant Iale	10/16/2009 12:24:27	
() Ine	58	2	1	Frank Smith	GET Lanton	5501-01-01-001-015004		10/16/2009 10:45:42	
True	57	5	4	John Doe	GET Lanton	V01.01.01.001.01.003		10/16/2009 10:45:12	
C Tax	55	4	3	RauRob	GET Laster	V01.01.01.001.01 V00		10/16/2009 10:44:38	
Co Taxe	65	6	6	Judi Bloom	GET Lasten	M01.01.01.001.01 M06		10/16/2009 10 44 09	
QTare	54	2	6	Tammu Aamer	GET Lanton	V01.01.01.001.01.205		10/16/2009 10:42:00	
A Ealer	53	7	6	Tammy Asses	GET Laston	101.01.01.001.01.000	TIMEOUT EPROP (m)	10/16/2009 10:41-29	
A False	52	7	6	Tammy Asses	GET Laster		TIMEOUT ERBOR for I	10/16/2009 10:40:16	
C Tout	51	7	3	Rilly Rob	MANUAL RETURN Land		THEOUT ENHOLINE.	10/13/2009 3 38 40 8	
C Taur	50	7	2	Pay Dob	MANUAL CET Lanton I			10/12/2009 2 20:04 0	
() Taup	49	7	2	Dily Dob	MANUAL DETUDNU and			10/13/2009 3:36:047	
O Tool	40	2		Faral Carib	OFTUDALI ALLA			10/13/2009 3/23/11 4	

Manually Adding/Removing Laptop Users

It's possible for the laptop user data in the database to get out of sync with the users who really have laptops. This can happen if laptops are added/removed outside of the service because the service isn't running, (or if there is an issue with velocity events not arriving correctly from the Velocity Message Queue Writer).

When that happens, you can manually change the current laptop users by clicking the Add User and Delete User buttons on the first screen:

lser Id	Name	Credential Id	Laptop Address	Transaction Id	Transaction Date	Laptop Time
	Billy Bob	4	\\01.01.01.001.01.X101	56	10/16/2009 10:44:41	4 days, 5 hours, 40

You can delete any user by clicking the delete button after it becomes enabled after selecting the user you want to delete in the grid.

Clicking add brings up a dialog screen that displays all the laptop expansion input states, along with all the users in Velocity that do not currently have a laptop assigned to them. On this screen you can select the laptop address, and the user to add -- be sure to only select laptop addresses where the laptop is present:



Lontrollers:	Secure Lap	otop Case M16	<u> </u>			
Kinput Id	Address		Laptop Status			Last Returned I 🔺
a 1	\\01.01.01.	001.01.XI01	LAPTOP NOT A	VAILABLE		10/12/2009 4:1
2	\\01.01.01.	001.01.XI02	Laptop is preser	yt.		10/19/2009 11
🖓 3	\\01.01.01.	001.01.×103	Laptop is preser	nt .		10/19/2009 11
4	\\01.01.01.	001.01.×104	Laptop is preser	t.		10/12/2009 4:
6 5	\\01.01.01.001.01.×105		Laptop is preser	Laptop is present		
96	\\01 01 01	001 01 ×106	Lanton is nreser	4		10/16/2009 12
Last Name		First Name	Mi	ddle Name	Host User Id	
Last Name		First Name	Mi	ddle Name	Host User Id	
Last Name Aames Blume		First Name Tammy Judy	Mi 6 5	ddle Name	Host User Id 6 5	
Last Name Aames Blume Cunningha	am	First Name Tammy Judy Jeremy	6 5 7	ddle Name	6 5 7	
Last Name Aames Blume Cunningha Doe	am	First Name Tammy Judy Jeremy John	Mi 6 5 7 4	ddle Name	Host User Id 6 5 7 4	
Last Name Aames Blume Cunningha Doe Jones	am	First Name Tammy Judy Jeremy John Tom	Mi 6 5 7 4 2	ddle Name	Host User Id 6 5 7 4 2	-
Last Name Aames Blume Cunningha Doe Jones Smith	am	First Name Tammy Judy Jeremy John Tom Frank	Mi 6 5 7 4 2 1	ddle Name	Host User Id 6 5 7 4 2 1	-
Last Name Aames Blume Cunningha Doe Jones Smith	e em	First Name Tammy Judy Jeremy John Tom Frank	Мі 6 5 7 4 2 1	ddle Name	Host User Id 6 5 7 4 2 1	
Last Name Aames Blume Cunningha Doe Jones Smith) am	First Name Tammy Judy Jeremy John Tom Frank	Мі 6 5 7 4 2 1	ddle Name	Host User Id 6 5 7 4 2 1	
Last Name Aames Blume Cunningha Doe Jones Smith) am	First Name Tammy Judy Jeremy John Tom Frank	Mi 6 5 7 4 2 1	ddle Name	Host User Id 6 5 7 4 2 1	-

E-Tool Power up Procedure

These are the steps that need to be performed when an e-Tool cabinet is powered up. These steps reestablish communication between the Hirsch controller in the Tracewell cabinet and the Velocity server. There are 2 main procedures that are required to reestablish communications. The first is restoring the TCP/IP connection and followed by resetting the encryption keys. These procedures are performed on a Velocity client or the Velocity server.

Restoring and resetting the encryption keys can be performed at the same time. When re-enabling the port, the encryption keys can be reset at the same time. The Port, XBox and Controller will come online in one step.

Restoring the TCP/IP connection

The Velocity server manages the TCP/IP connections to one or more Velocity controllers. The controller loses power when the cabinet loses power, because the cabinet powers the Hirsch controller which is located inside th cabinet. The DIGI*TRAC (DT) Network service is a windows service program running on the Velocity server and it manages the TCP/IP connections. When a controller is disconnected, the DT service attempts to reconnect to it for a configured number of retries. If the DT service exhausts the retries without connecting, the DT service stops trying. Then, a Velocity operator must perform these steps to restore the connection.

In addition to the card swiping not unlocking a cabinet drawer, the Velocity Event Viewer has "Port Socket Error" messages indicating the server in not communicating

with the cabinet. The DT service attempts to reconnect every 23 seconds for the set number of attempts configured in the port properties window. The default attempts are set to 50 equating to approximately 20 minutes or retrying. A value of 0 for infinite retries causes the DT service to attempt 500 times (approximately 3 hrs).

ile <u>⊂</u> onsole <u>W</u> indow <u>A</u> c	id-Ins <u>H</u> elp							
乡 Alarms 🛛 🔝 Browser 💵	Events 🧕 Enrolmer	nt 📆 Graphics 🗔 V	ideo Explorer 🤞	📑 Reports 🛛 🕅 St	atus 😻 My Velocity	📴 🎫 🔝 🚡	🙆 📖	
4	1					1		
Host Time	Description					Address	Event Type	Event ID
Host Time 01/22/2010 11:32:17 AM	Description Port Socket Error					Address	Event Type Port	Event ID
Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM	Description Port Socket Error Port Socket Error					Address \\01.01.01 \\01.01.01	Event Type Port Port	Event ID 8504 8504
Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM	Description Port Socket Error Port Socket Error Port Socket Error					Address \\01.01.01 \\01.01.01 \\01.01.01	Event Type Port Port Port	Event ID 8504 8504 8504
Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:31:08 AM	Description Port Socket Error Port Socket Error Port Socket Error Port Socket Error					Address \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01	Event Type Port Port Port Port	Event ID 8504 8504 8504 8504 8504
Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:31:08 AM 01/22/2010 11:30:45 AM	Description Port Socket Error Port Socket Error Port Socket Error Port Socket Error Port Socket Error					Address \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01	Event Type Port Port Port Port Port	E vent ID 8504 8504 8504 8504 8504 8504
Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:31:38 AM 01/22/2010 11:30:45 AM 01/22/2010 11:30:22 AM	Description Port Socket Error Port Socket Error Port Socket Error Port Socket Error Port Socket Error Port Socket Error					Address \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01	Event Type Port Port Port Port Port Port	Event ID 8504 8504 8504 8504 8504 8504 8504
Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:31:38 AM 01/22/2010 11:30:45 AM 01/22/2010 11:30:22 AM 01/22/2010 11:32:59 AM	Description Port Socket Error Port Socket Error Port Socket Error Port Socket Error Port Socket Error Port Socket Error					Address \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01	Event Type Port Port Port Port Port Port	Event ID 8504 8504 8504 8504 8504 8504 8504
Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:31:08 AM 01/22/2010 11:30:55 AM 01/22/2010 11:29:59 AM 01/22/2010 11:29:59 AM	Description Port Socket Error Port Socket Error					Address \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01 \\01.01 \\01.01 \\01.01 \\01.01	Event Type Port Port Port Port Port Port Port Port	Event ID 8504 8504 8504 8504 8504 8504 8504 8504
Host Time 01/22/2010 11:32:17:AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:31:36 AM 01/22/2010 11:30:45 AM 01/22/2010 11:30:45 AM 01/22/2010 11:30:36 AM 01/22/2010 11:23:36 AM	Description Port Socket Error Port Socket Error					Address V(01.01.01 V(01.01.01 V(01.01.01 V(01.01.01 V(01.01.01 V(01.01.01 V(01.01.01 V(01.01.01	Event Type Port Port Port Port Port Port Port Port	Event ID 8504 8504 8504 8504 8504 8504 8504 8504

The PING line command can be used to verify the controller is available on the network. The IP address is found in the port properties using the Velocity Status Viewer. A successful ping indicates the controller is powered up and available. If pinging is unsuccessful, refer to section "Resetting the SNIB2 IP Address".

III.	Valacity								
-g-	a Copcole Window Ad	d-Inc Help							
C.	e Console <u>wi</u> ndow <u>A</u> u	id-tris Eleip			_				
•	Alarms 🔝 Browser 🛄	Events 🕵 Enrollment	Graphics	Video Explorer	🚑 Reports	🔠 Status 💔 My Velocity	🖻 🎦 🎦 🎁 🎯 🗆	<u>Da</u>	
×	Hast Time	Description		_			Address	Eugent Turce	Europet ID
×	Host Time	Description					Address	Event Type	Event ID 8504
×	Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM	Description Port Socket Error Port Socket Error					Address \\01.01.01 \\01.01.01	Event Type Port Port	Event ID 8504
×	Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM	Description Port Socket Error Port Socket Error Port Socket Error	_				Address (V01.01.01 (V01.01.01 (V01.01.01	Event Type Port Port Port	Event ID 8504 8504
×	Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:31:39 AM	Description Port Socket Error Port Socket Error Port Socket Error Port Socket Error					Address \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01	Event Type Port Port Port Port	Event ID 8504 8504 8504 8504
×	Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:31:08 AM	Description Port Socket Error Port Socket Error Port Socket Error Port Socket Error Port Socket Error					Address \\\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01	Event Type Port Port Port Port Port	Event ID 8504 8504 8504 8504 8504
×	Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:30:45 AM 01/22/2010 11:30:45 AM	Description Port Socket Error Port Socket Error Port Socket Error Port Socket Error Port Socket Error Port Socket Error			ī	-	Address \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01 \\01.01.01	Event Type Port Port Port Port Port Port	Event ID 8504 8504 8504 8504 8504 8504
×	Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:32:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:31:08 AM 01/22/2010 11:30:45 AM 01/22/2010 11:30:22 AM 01/22/2010 11:30:22 AM	Description Port Socket Error Port Socket Error Port Socket Error Port Socket Error Port Socket Error Port Socket Error					Address V01.01.01 V01.01.01 V01.01.01 V01.01.01 V01.01.01 V01.01.01 V01.01.01	Event Type Port Port Port Port Port Port Port Port	Event ID 5004 5504 5504 5504 5504 5504 5504 5504
×	Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:31 AM 01/22/2010 11:30:45 AM 01/22/2010 11:30:45 AM 01/22/2010 11:30:25 AM 01/22/2010 11:28:35 AM	Description Part Socket Error Part Socket Error Part Socket Error Part Socket Error Part Socket Error Part Socket Error Part Socket Error					Address \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	Event Type Port Port Port Port Port Port Port Port	Event ID 5004 8504 8504 8504 8504 8504 8504 8504
×	Host Time 01/22/2010 11:32:17 AM 01/22/2010 11:31:54 AM 01/22/2010 11:31:51 AM 01/22/2010 11:30:43 AM 01/22/2010 11:30:22 AM 01/22/2010 11:32:45 AM 01/22/2010 11:22:453 AM	Description Part Socket Error Part Socket Error					Addiess \\\\01.01.01 \\\\01.01.01 \\\\01.01.01 \\\\01.01.01 \\\\01.01.01 \\\\01.01.01 \\\\01.01.01 \\\\01.01.01	Event Type Port Port Port Port Port Port Port Port	Event ID

After verifying the controller is available, open the Velocity Status Viewer by selecting the Status icon on the Toolbar.



III File Console Window Add Inc. Holp	
Bi Die Cousole Willion Wooth's Deb	
🔶 Alarms 🔚 Browser 🔳 Events 🧕 Enrollment 📆 Graphics 🗔 Video Explorer 🚑 Reports 🗐 Status 💖 Ny Ve	locit
Status Group: None 🔽 🚰	

Select the Status Group named "Reset Port" from the drop down list.

Velocity - [Status Viewer]
Eile Console Window Add-Ins Help
🔶 Alarms 🔚 Browser 💵 Events 🚯 Enrollment 📆 Graphics 💷 Video Explorer 🏭 Reports 🟢 Status 😵 My V
Status Gradp: None 🔄 🖆
None Reset Port

Expand the Reset Port group by clicking on the "+" sign.

	/elocity - [Status Viewer]	
]	ijle <u>C</u> onsole <u>W</u> indow <u>A</u> dd-Ins <u>H</u> elp	
	Alarms 🔚 Browser 🎟 Events 🧕 Enrollment 📅 Graphics 💷 Video Explorer 🚑 Reports 🏢 Status 🕯	ø
Ş	s Group: Reset Port	
P	vits 🥠	

Right click on "Secure Laptop Port" and select "Configure Device" to open the properties window.

🔢 Velocity - [Status Viewe	ar]		
<u>File C</u> onsole <u>W</u> indow <u>A</u> d	d-Ins <u>H</u> elp		
🤞 Alarms 🔝 Browser 💵 Eve	ents 👷 Enrollment 📆 🤆	Graphics 🗔 Video Explorer	🏭 Reports 🔳 Status 💖 N
Status Group: Reset Port	_ 🚰		
Bert Name	Address	Status	Enabled
Secure Laptop Port	01.01.01	Offline	Yes

Disable the port. Uncheck the "Enable this Port" option and click OK.



🔢 Port - Secure Laptop Port \\01.01.01 Properties	X
General	
Name: Secure LT	
Network Type:	
C Serial Port © TCP/IP 🗹 XNET 2 protocol	
E Reset encryption	
IP address: 192 . 168 . 241 . 241 Search	
IP Port: 10001	
Max retry attempts: 0 + { 0 = infinite retries }	
Advanced	
Enable this Port	_
Help OK Cano	el

Enable the port. Open the properties window by reselecting the "Configure Device" option. Check the "Enable this Port" option and click OK.

Port - Secure LT \\01.01.01 Properties	×
General	
Name: Secure LT Network Type: C Serial Port ICP/IP IV XNET 2 protocol I Reset encryption	
IP address: 192 , 168 , 241 , 241 Search IP Port: 10001 Max retry attempts: 0 ÷ {0 = infinite retries }	1
]
Help OK Cance	el

DT service will begin attempting to connect to the port. A Port Online and XBox Online message will appear in the Velocity Event Viewer. Although Velocity is communicating to the Port and Xbox, the encryption keys are broken and the DT service is not communicating with the controller. The encryption keys must be reset for controller to communicate with the DT service. The DT service will attempt every 23 seconds to reconnect to the port for the number of retries set in the port properties. If no connection is made to the controller within the retry limit, this process must be repeated.



Alarma Contractor III	Carto & Combant	The country Parister Carbons (The second				
Adres Debuser	Evens L Enoment	25 ordanics mendeo criteria. Mustori	2 1 Starte A M March 23 23 21			
Disklass		a la	Fachlad	Instant		
Hok reared	Val. 01.01	Doine Y	enableo	01/25/2010 3:25 2	21 PM	
	1			L	1	
Hast Time	Description		Addenz	Event Type	Event ID	
Hast Tiree 01/25/2010 3 (502) FW	Description Encryption Broken Pol	ling Kalas	Addens With 01 Ch List 40 For 000	Event Type	Event D	
Hast Time In ASYANTON (SIGT FM DI ASYANTON (SIGT FM DI ASYANTON (SIGT FM	Description Encryption Broken, Pet XBac Online	ting Halad	Address Victorial on Victorial produt	Event Type Part MB pe	Event D (511 4047	
Hoad Time (17/25/2010.3.252) FM (17/25/2010.3.252) FM (17/25/2010.3.252) FM (17/25/2010.3.252) FM	Description Encryption Broken, Pol XBox Online Post Online Box Enclose Encryption	ding Halled	Addwara Man an Kan Man an Kan Jaght Man an Len Man an Len	Event Type Part VB ce Computed for	Event ID 6511 4047 4049	
Host Time (17/25/2010.3.15.2) FM (17/25/2010.3.25.2) FM (17/25/2010.3.25.2) FM (17/25/2010.3.25.2) FM (17/25/2010.3.25.2) FM	Description Encryption Excitons, Pol XBox Online Post Online Post Social Econocide Commission Post S	fing Halled d	Address Vari in tri Vari at de det Vari at de Vari at de Vari at de	Event Type Fast XBox Companies from Fast Fast	Event ID (511 4047 4048 1500	
Hast Tree 01/25/2010 3 2521 Per 01/25/2010 3 2521 Per 01/25/2010 3 2521 Per 01/25/2010 3 2521 Per 01/25/2010 3 2520 Per	Description Encryption Broten: Pol NBox Online Pol Social Connecter Commission: Pol S Pol Stations Dorol	forg Halled d reces LT was charged by pitch	Address Warring an Warring and Warring and Warring an Warring an Warring an	Event Type Past X8 be Communication Post Software Post	Event D ES11 4047 4048 ES00 1009 ES00	
Hast Time 11/25/2010 3 (5:21 PM 10/25/2010 3 (5:21 PM 10/25/2010 3 (5:21 PM 10/25/2010 3 (5:21 PM 10/25/2010 3 (5:20 PM 10/25/2010 3 (2:21 PM 10/25/2010 3 (2:21 PM	Description Encoption Rotars Pol XBox Online Pol Social Connection Connection Fort Pol Social Connection Pol Studione Compto Controllo Langer (Chi	lerg Halled d decas LT was charged by pileh deal	Address Visit for 161 Visit for 161 Not 0001 Visit for 161 Not 0001 Visit for 161 Not 0001 Visit for 0001 Not 0001 Visit for 0001 Not 0001	Event Type Part XBos Comparing dison Part Software Part	Event D (51) 4047 4046 5500 1009 6500	
Hast Time (n/25/2010 3 (52) PM (n/25/2010 3 (52) PM	Description Encoption Rotans, Pat Silos Ordina Pat Social Connectes Connected Connectes Connectes Encoption Controlling Languages	ling Huled d lenae L1 vez shargedbypeteh enae L1 vez shargedbyneteh	Address Vicin at an Vicin at an Vicin at an Vicin at a Vicin at a Vicin at an Vicin at an Vicin at an Vicin at an	Event Type Part Sitte Comparied for Part Saftware Part Comparied ann Saftware Saftware	Evert D ES11 4047 4048 6500 7000 1079 1079	
Hast Time Int25/2010 3 (52) FM Int25/2010 3 (42) FM Int25/2010 3 (42) FM Int25/2010 3 (42) FM Int25/2010 3 (42) FM	Description Encoption Existens Pat Nex Orders Port Societ Connector Connectors Port S Connectors Port S Connectors Excels Contactions Ports Contactions Ports	long Holad di ecca LT was sharged by petch deal Secar LT was sharged by petch Secar LT was sharged by petch	Addware Visio di Un Visio di Un José Visio di Un José Visio di Un José Visio di Un Visio di Visio di Un Visio di Visio di Di On Visio di Visio di V	Event Type Pat XB os Comunication Pat SafAas Pat Comunication SafAas Dist Tope	Event D (511 404) 6500 1009 6500 7000 1009 6500 7000 9005	
Hast Tree (n/25/2010.3.15.2) Per (n/25/2010.3.15.2) Per (n/25/2010.3.5.2) Per (n/25/2010.3.5.2) Per (n/25/2010.3.5.2) Per (n/25/2010.3.5.2) Per (n/25/2010.3.2) Per (n/25/2010.3.2) Per (n/25/2010.3.2) Per (n/25/2010.3.2) Per	Description Encryptern Parken, Pel Misso Online Pel Oschat Connectes Connected Connectes Pel Statutione Complet Connected Integrat Of Connected Integration Connected Integratio	ing Halad i ing Halad ing	Addares Statistics With the form With the form form form	Event Type Fait 2016 Fait SetVeen Pait Connected and SetVeen Dig Tracinitien Dig Tracinitien Dig Tracinitien	Evert D EX1 4047 4048 550 7000 7000 8005 8005	
Hart Tere International Scale Re- InterSchernola Scale Re-	Description Encryption Robers, Pai Stace Online Part Stack Connected Connected and Connected Connected and Connected Connected and Connected Connected and Connected Theast Level race at 0 ACB 115 Tragment	long Halad di secure L3 rous sharges(loypeteh secul 13 rous sharges(loypeteh m) Cantades Social Lights M1 Gal controller Si	Address Vice at the of edge Vice at the of edge Vice at the Vice at the Ord At the Vice at the Vice at the Ord At the Vice at the Vice at the Ord At the Vice at the Vice at the Ord At the Vice at the Ord At the Vice at the	Evert Isse Pat 2010 Connected for Pat Schwar Pat Connected for Schwar Dig*Trac Internal Dig*Trac Internal Dig*Trac Internal	Ever D (51) (447) (449) (447) (449) (447) (449) (447) (449) (447) (4	
Hast Time (n252/n1013/521 FM (n252/n1013/521 FM	Description Encription Devices Pell Selectrine Pell Ontrine Perl Scholl Connectes Connectedations Cample Contacts Legard 01 Connectedations Perl Mail 115 Triggend Controls Road Add 115 Triggend Contacts Road	forg Halad d anaa Anaa LT nea chargadiyyateh Anaa LT nea chargadiyyateh n Caritades Sacara Lagrap HTB at correlar St	Address Vicinities Vicinities Vicinities	Event Type Fait 2019 Fait Saftware Pait Communication Saftware Dig Trace Internal Dig Trace Internal Dig Trace Internal Dig Trace Internal	Exert D EST1 4047 4048 ESD 8500 7000 8004 8004 8004 8004 8004	
Had Tow mr252000 3 521 Hi mr252000 3 521 Hi mr252000 3 523 Hi mr252000 3 243 Hi mr252000 3 244 Hi	Description Encogister Texture Part Nets Orbine Part Gente Connected and Connecter Connected and Connecter Connected and Connecter Connected and Connecter Theast Level rays at 0 A CB 115 Triggend A CB 115 Triggend A CB 115 Triggend A CB 115 Triggend A CB 112 Triggend A CB 112 Triggend	fog tielog d erzer LT mer chergedbypetek erze ierze LT mer chergedbypetek in Caritable Sezue Laftep MTG at controller St	Addem Oct it in Verifield to rodat Verifield to rodat Verifield to Verifield to	Event Tops Part 28 to Software Part Software DepTract Internal DepTract Internal DepTract Internal DepTract Internal DepTract Internal	Ever D (51) (447) (447) (448) (52) (52) (53) (53) (53) (54) (55) (54) (55) (54) (55) (54) (55) (54) (55) (54) (55) (54) (

Resetting the Encryption Keys

After the Port and Xbox are online, the encryption keys must be reset. Again select the "Configure Device" option to display the port properties. Check the "Reset Encryption" option and click on OK.

🖩 Port - Secure Laptop Port \\01.01.01 Properties 🛛 🔀
General
Name: Secure LT
Network Type:
C Serial Port
E Reset encryption
IP address: 192, 168, 241, 241 Search
Max retry attempts: 0 = infinite retries)
Help OK Cancel

A port was changed event message will appear in the Event Viewer. Then the "Controller Online" event will appear.

The America literature	ewer]			
Elle Console Window	Bog-jue Rab			
Alerns The Browser	i Events 🧕 Envolment 🖽 Graphics 💷 Wideo Explorer 🔐 Reports 🔝 Status 💖 My Velocity	C C C C C C C C C C C C C C C C C C C	2	
us Group: Reset Port	<u>二</u> 留			
Hast Time	Decorption	Addeers	Event Type	Event ID
01/25/2010 3:26:42 PM	Input State Diange at Expansion Input Kinput 07 Drawer Input 7 to Door XI RDE // I Tanger X Circ.	. VID1.01.01.001.01.2007	Digi Trao External	4024
01/25/2010 3.26.42 PM	Input State Divange at Expansion Input Kinput 05 Draver Input 5 to Door XI RDE // I Tanper X Curr.	V01.01.01.001.01.000	Digi"Trac External	4024
01/25/2010 3 26:42 PM	Input State Divinge at Expansion Input Kinput 05 Draver Input 5 to Door XI ROE // I Tamper X Curr.	. \\01.01.01.001.01.205	DigiTrac External	
01/25/2010 3 26:42 PM	Input State Divange at Expension Input Xinput 04 Draver Input 4 to Door X1RDE //11 anper X1Curr	W01.01.01.001.01.2004	DigiTrac External	
01/25/2010 3 26:42 PM	Input State Diverge at Expension Input XInput 03 Drawer Input 3 to Door XI RDE // Tanger X Crar.	. W01.01.01.001.01.203	Digi"Trac External	4024
01/25/2010 3 26:42 PM	Input State Diange at Expansion Input Kinput 02 Draver Input 2 to Door XI RDE // I Tanger X Curr	VD1.01.01.001.012002	Diol [®] Trac External	
01/25/2010 3 26 42 PM	Input State Divange at Expension Input Xinput 01 Draves Input 1 to Door XTRDE // Tanper X Curr	. V.01.01.01.001.01.2001	DigiTrac External	4024
01/25/2010 3 26:42 PM	Network Offine Friori-alam Fat controller Secure Laptop N16	V01.01.01.001.01	DigiTrac External	4027
01/25/2010 3 26:41 PM 01/25/2010 3 26:41 PM	Controller Unline at controller	50,100,10,00,001	Communication	4049
01/25/2010 3 26:41 PM 01/25/2010 3 26:41 PM 01/25/2010 3 26:41 PM	Controlles Online at controller Controlles Online at controller Controlles Online Reposiding	50,100,101,01,001,02	Connunication Connunication	4049 7007
01/25/2010 3 26:41 PM 01/25/2010 3 26:41 PM 01/25/2010 3 26:41 PM 01/25/2010 3 26:41 PM	Volume Consider Papering & addets: Vol Or of the Later Sognation from Controller United to antifuler Controllers Online/Reporting	9001.01.01.001.02 9001.01.01.001 9001.01.01.001	Communication Communication XB os	4049 7907 4047
01/25/2010 3.26:41 PM 01/25/2010 3.26:41 PM 01/25/2010 3.26:41 PM 01/25/2010 3.26:41 PM 01/25/2010 3.26:41 PM	Controller Charlow Proceeding & address from on the first servicing sectory most Controller Charlow Temporating 28th Charlow Providers	VVD1.01.01.001.02 VVD1.01.01 001 VVD1.01.01.001 VVD1.01.01	Communication Communication XB or Communication	4049 7007 4047 4048
01/25/2010 3 26:41 PM 01/25/2010 3 26:41 PM	Volmeng Control Proceeding & address Volt of 101 101 102 Lineage address Volt of 102 L	W01.01.01.001.02 W01.01.01.00 W01.01.01.00 W01.01.01 W01.01.01	Connunication Communication X8 or Connunication Part	4043 7007 4047 4048 8503
01/25/2010 2 20:41 PH 01/25/2010 2 26:41 PH 01/25/2010 2 26:35 PH	Controller Officer Terroristication and address international to the fact service approximation of the Control of Control	Vion of .01.001.02 Vion of .01.001 Vion of .01.001 Vion of .01 Vion of .01 Vion of .01	Connunication Communication NB or Connunication Part Part	4049 7007 4047 4048 8059 8050

The "Controller Online" event will be followed by several other controller events. The "Logged on to Controller" event indicates the controller is ready for use.

felocity - [Status Vi	iewer]				
ile <u>C</u> ansole <u>W</u> indow	êdd-3ns ₩elp				-
uarns The Browser	Events 🤨 Enrolment 🕮 Graphics 🖽 Wideo Explorer 🕮 Reports 🔟 Status 😁 Wiv Velocity	1 PT 17 10 PM 0	0		
Group Read Post	- R				
Contrade (The Rest for				+	
last Time	Description	Addees	Event Type	Event ID	
/25/2010 3 26:43 PM	ADB 120 Triggered	V01.01.01.001.01	Dig/Trac Internal	9004	
/25/2010 3 26:43 PM	ACB 76 Triggered	V01.01.01.001.01	Digi [®] TracInternal	5024-	
1/25/2010 3 26:43 PM	Operator System Account Sat DigiTrac Date & Time		Software		
/25/2010 3 28:43 PM	Logged on to Controller: Secure Laptop M16 at address VU1.01.01.001.01	Valiat	Software	1151	
/25/2010 3 26:43 PM	Network Active at controller Secure Laptop M16	V/01.01.01.001.01	Digi [*] Trac Estatual	4015	
/25/2010 3 26:43 PM	Kapped CAC Eticol 001 Drifte	V01.01.01.001.01.SM01	Digit Trac External	4004	
/25/2010 3 26:43 PM	NATEH Address 1 CAC Excel 001 Online	V.D1.01.01.001.001	Digi [*] Trac Estavual		
/25/2010 3 26:43 PM	Input State Change at Expansion Input Xinput 16 Space to Open Circuit Danest Macking D(alare pill.	V01.01.01.001.01.5016	DigitTrac Estand		
/25/2010 3 26:43 PM	Input State Change at Expansion Input Xinput 15 Spare to Open Circuit Current Masking Difetence pt.	V01.01.01.001.012015	Digit Trac External	4024	
/25/2010 3 26:43 PM /25/2010 3 26:43 PM /25/2010 3 26:43 PM	Input State Change at Expansion Input Vinput 15 Space to Open Circuit Datent Macking Dijalana pit . Engl Input Manual 15 Space Open	V.01.01.01.001.01.X015	DigitTrac Esternal DigitTrac Alarm	4024	
/25/2010 3 26:43 PM /25/2010 3 26:43 PM /25/2010 3 26:43 PM /25/2010 3 26:43 PM	Input State Change al Expansion Input Niput 15 Space to Open Discut Quent Marking Oplaam pi . Engl Input Nimut 15 SpaceOpen Input State Change al Expansion Input Niput 14 Space to Open Discut Quent Marking Oplaters pi .	V.01.01.01.001.01.5015 V.01.01.01.001.01.5015 V.01.01.01.001.01.5014	DigitTrac External DigitTrac Abers DigitTrac External	4004 E000 4004	
1/25/2010 3 26:43 PM 1/25/2010 3 26:43 PM 1/25/2010 3 26:43 PM 1/25/2010 3 26:43 PM 1/25/2010 3 26:43 PM	Input State Change at Expansion logal Neput 15 Space to Open Circuit Carsert Hashing Of alare pit. Spip Input Neput 15 SpaceOpen Input State Change at Expansion logal Neput 14 Space to Open Circuit Carsert Hashing Of alare pit. Spip Input Neput 15 SpaceOpen	Vidi 01.01.001.01.3015 Vidi 01.00.01.01.3015 Vidi 01.01.001.01.3014 Vidi 01.001.01.3014	DigitTrac Esternal DigitTrac Alarn DigitTrac Esternal DigitTrac Esternal	4004 5000 4004 5000	
/25/2010 3 25:43 PM /25/2010 3 26:43 PM	Input State Change at Expansion logid Neput 15 Space to Open Direct Darset Hashing D'(alam pit. <u>Exp. Input State Change at Expansion logid Neput 14 Space to Open Direct Darset Hashing D'(alam pit.</u> <u>Exp. Input Neput 14 Space Chan</u> <u>Input State Change at Expansion logid Neput 13 Space to Open Direct Darset Hashing D'(alam pit.</u>	V0101.01.01.01.01.515 V0101.01.01.01.01.515 V0101.01.00.01.01.514 V0101.01.00.01.01.514 V0101.01.00.01.01.514	DigitTrac External DigitTrac Alarn DigitTrac External DigitTrac Alarn DigitTrac External	4004 5000 4004 50507 4004	
(25/2010 1 28:43 PM (25/2010 1 28:43 PM)	Inged State Change at Expersion legal Mappel 15 Space to Open Direct Darreet Hashing Difalore pit. Engl Ingel Maha Darreet 15 Space Open Ingel Maha Darreet at Expersion legal Mappel 14 Space to Open Direct Darreet Hashing Difalore pit. Engl Ingel Maha Change at Expersion legal Mappel 13 Space to Open Direct Darreet Hashing Difalore pit. Top Ingel Maha Change at Expersion legal Mappel 13 Space to Open Direct Darreet Hashing Difalore pit.	V01.01.01.00.01.01.5015 V01.01.01.00.01.01.5015 V01.01.01.01.01.5014 V01.01.01.00.01.01.5014 V01.01.01.00.01.01.5013 V01.01.01.00.01.01.5013	DigitTrac Esternal DigitTrac Alarn DigitTrac Esternal DigitTrac Alarn DigitTrac Esternal DigitTrac Esternal	4004 5000 4004 5000 4004 5000	

Resetting the SNIB2 IP Address

The IP address of the SNIB2 device resets to a default value when the cabinet is powered off for an extended number of days. The IP address will also reset if the SNIB2 is disconnected from the controller board for more than 5 minutes.



When this occurs, the desired IP address must be set by an operator. The correct IP address must be set prior to restoring the TCP/IP connection and resetting the encryption keys.

Open the port properties window using the "Configure Device" option in the Velocity Status Viewer. Click on the "Search" button.

🔢 Port - Secure Laptop Port W01.01.01 Properties 💦 👂
General
Name: Secure LT
Network Type:
C Serial Port
🗍 Reset encryption
IP address: 192, 168, 241, 241 Search
IP Port: 10001
Max retry attempts: 0 + { 0 = infinite retries }
Advanced
Enable this Port
Help OK Cancel

Velocity searches for all SNIB2s that have currently unassigned IP addresses. All SNIB2s Velocity detects on its system are listed. Double click the proper controller to set the IP address in the SNIB configuration window. Selecting the controller and assigning the IP address in the port properties window will NOT change the IP address. Most likely there will be only one controller. The default IP address will be different than the desired address. At initial deployment, each cabinet controller must be assigned an IP address.

Searching			
IP Address	Port	Name	Version
10.1.30.10		Robert Loves D	5.98.00
198.168.30.92		Rick's Sooner E	5.95.00
192.168.241.241	10001	Secure LT	5.95.00
192.168.30.55	10001	Kurt	5.98.00
123.123.123.20		RMA_HUE STA	5.98.00
192.168.30.62	10001	Kim's screaming	5.98.00
192.168.30.75	10001	Joseph M8	5.98.00
192.168.50.19	10001	Pete Hoffman	5.98.00
<)	>
r(1	
Help		OK	Cancel
<mark>≮</mark> <u>H</u> elp		OK	Cancel



The SNIB2 configuration window will appear. Enter the desired IP address and click OK. Clicking OK changes the IP address of the port device in the controller.

SNIB Configuration	
Settings	
Name: Secure LT	
Network	
IP Address: 1	192 168 241 241
Port: 10	0001
<u>H</u> elp	OK Cancel

The new IP address will appear in the properties window. Click OK. Continue restoring the TCP/IP connection and resetting the encryption keys.

🔢 Port - Secure Laptop Port \\01.01.01 Properties	×
General	
Name: Secure LT	
Network Type:	
C Serial Port ICP/IP I XNET 2 protocol	
E Reset encryption	
IP address: 192 . 168 . 241 . 241 Search	
IP Port: 10001	
Max retry attempts: 0 🗧 🛃 { 0 = infinite retries }	
Advanced	
🔽 Enable this Port	
Help OK Cance	»





There are three pieces of software that combine to form the operational basis for E-Tool Mobile Manager system: Velocity (including the Secure Laptop Extension), Microsoft SQL Server and Secure Laptop Client.
In a local installation, all three pieces run on a single host computer system. In a typical networked environment, Velocity and Secure Laptop Client run on an administrator's computer system, while SQL Server is installed on a server farm.

SOFTWARE

Velocity and SQL Server are provided on the Velocity CD. This disc contains installation guides and user manuals in <CD-drive>:\Velocity\Documents\Velocity Guides. Secure Laptop Client, along with an installation guide, card reader drivers, and a firmware update application are provided on the Tracewell Systems, Inc. CD.

Hirsch Electronics, Inc. (www.hirschelectronics.com) offers training courses for the software, and we strongly recommend that persons responsible for the administration and support of the cabinets attend these classes. Tracewell Systems, Inc. offers on-site installation and configuration of all hardware and software components.

Velocity

Velocity is a database application program used to administer and control all E-Tool Mobile Manager cabinets. In a local installation, the host system running Velocity might control only one cabinet or a small number of cabinets. In a network environment, a single instance of Velocity can administer hundreds of cabinets and thousands of users from a single location. Velocity is a standard product of Hirsch Electronics, and is the premier access control software package. The Secure Laptop Extension adapts Velocity to the unique requirements of the E-Tool Mobile Manager.

Administrator and Operator Guides are on the Velocity CD, and should be consulted for detailed information about the program. This section describes the modules most often used in the day-to-day administration of the users and cabinets. Each module is accessible through the Console menu, or with Function keys. The four modules most commonly used are Event Viewer, Administration, Enrollment Manager, and Status Viewer.

Alarma III Events	Freedward 20 Grandvirs 120	Man Evolver / Denn	de Master 😪 🖂 🕅 🗠			
	No.	Ame				
Velocity Configuration	s 🐳	XR01 Drawer 1	01			
DIGI*TRAC Configura	sion (TSECURE1)	XR02 Drawer 2	02			
SNET	*	XR03 Drawer 3	03			
SAME CARLIENS		XR04 Drawer 4	04			
E @ Secure L	aptop Xbox	XR05 Drawer 5	05			
🖻 🕞 Secu	ire Laptop M2	XR07 Drawer 7	05			
	Doors	XR08 Drawer 8	08			
	Expansion Inputs	XR09 Drawer 9	09			
	nputs	×R10 Drawer 10	10			
	Readers	XR11 Drawer 11	11			
	Relayo	XR12 Drawer 12	12			
E Secure Lapto	۹ 🛛 🕰	VP14 Drawer 14	13			
Interfaces Configurati	ion (TSECURE1)		12			
Host Time	Description			Address	Event Type	Event ID
/8/2011 11:24:26 AM	Expansion relay XR02 Drawer	2 state change (0) none	2	\WNET.001.0001.001.01 XR02	DIGI*TRAC Internal	9034
	Input state change at expansi	on input XI02 Drawer 21	o Door // IRQE X Tamper X curre	VVXNET.001.0001.001.01.X102	DIGI*TRAC External	
/8/2011 11:24:22 AM	Input state change at expansi	on input X002 Drawer 2 t	o Door // I RQE // Temper X cur	\WWNET.001.0001.001.01.01.002	DIGI*TRAC External	
/8/2011 11:24-19 AM	Expansion relay XB02 Drawer	2 state change (1) cont	tol zone trigger	VWNET 001 0001 001 01 XR02	DIGI*TRAC Internal	9034
	Operator USER triggered rela-	xXR02 Drawer 2 from w	orkstation TSECURE1	WTSECURE1.001	Software	6060
/8/2011 11:24:18 AM				VVINET.001.0001.001.01.01.012	DIGI-TRAC Transaction	3000
2/8/2011 11:24:18 AM 2/8/2011 11:24:06 AM	MRQ granted: X012 Drawer 1					
2/8/2011 11:24:18 AM 5/8/2011 11:24:06 AM 5/8/2011 11:24:06 AM	MRQ granted: X012 Drawer 1 Input state change at expansi	on input XI12 Drawer 12	to Door // RQE X Tamper X cur.	VVINET 001 0001 001 01 2012	DIGI*TRAC External	4024
28/2011 11:24:06 AM 2/8/2011 11:24:06 AM 2/8/2011 11:24:06 AM 2/8/2011 11:24:00 AM	MRQ granted: XI12 Drawer 1 Input state change at expansi Expansion relay XR12 Drawer	ion input XI12 Drawer 12 (12 state change (0) nor	to Door // RQE X Tamper X curr	VVANET.001.0001.001.01.2012 VVANET.001.0001.001.01.2012	DIGI*TRAC External DIGI*TRAC Internal	4024
/8/2011 11:24:08 AM /8/2011 11:24:06 AM /8/2011 11:24:06 AM /8/2011 11:24:00 AM /0/2011 11:24:00 AM	MRQ granted: X112 Drawer 1 Input state change at expansi Expansion relay XR12 Drawer Input state change at expansi	ion input XI12 Drawer 12 (12 state change (U) nor on input XI12 Drawer 12	to Door // [RQE X Tamper X curr re to Door // [RQE //] Tamper X cur	VVINET.001.0001.001.01.012 VVINET.001.0001.001.012912 VVINET.001.0001.001.012012	DIGI*TRAC External DIGI*TRAC Internal DIGI*TRAC External	4024 9034 4024
28/2011 11:24:06 AM 2/8/2011 11:24:06 AM 2/8/2011 11:24:06 AM 2/8/2011 11:24:00 AM 2/0/2011 11:24:00 AM 2/0/2011 11:24:00 AM	MRQ granted: X012 Drawer 1 Input state change at expansi Expansion relayXR12 Drawer Input state change at expansi Input state change at expansi	ion input XI12 Drawer 12 12 state change (0) nor on input XI12 Drawer 12 on input XI02 Drawer 21	to Door // RQE X Tamper X curr re to Door // RQE // Tamper X curr to Door // RQE X Tamper X curr	VVANET.001.0001.001.01.01.2012 VVANET.001.0001.001.01.2012 VVANET.001.0001.001.01.2012 VVANET.001.0001.001.01.2012	DIGI*TRAC External DIGI*TRAC Internal DIGI*TRAC External DIGI*TRAC External	4024 9034 4024 4024
28/2011 11:24:18:AM 2/6/2011 11:24:06:AM 2/8/2011 11:24:06:AM 2/8/2011 11:24:00:AM 2/8/2011 11:24:00:AM 2/8/2011 11:24:00:AM 2/8/2011 11:23:56:AM	MRQ granted: X012 Drawer 1 Input state change at expansi Expansion relay XR12 Drawer Input state change at expansi Input state change at expansi Input state change at expansi	4 ion input X112 Drawer 12 r 12 state change (U) nor on input X112 Drawer 12 on input X102 Drawer 21 on input X102 Drawer 21	to Door // RQE X Tamper X cur re to Door // RQE // Tamper X cur to Door // RQE X Tamper X cur to Door // RQE // Tamper X cur	VONET 001 0001 001 01 2012 VONET.001.0001 001.0129812 VONET.001.0001 001 012012 VONET.001.0001 001 01202 VONET.001.0001.001.01202	DIGI*TRAC External DIGI*TRAC Internal DIGI*TRAC External DIGI*TRAC External DIGI*TRAC External	4024 9034 4024 4024 4024
28/2011 11:24:18 AM 2/6/2011 11:24:06 AM 2/6/2011 11:24:06 AM 2/8/2011 11:24:00 AM 2/8/2011 11:24:00 AM 2/8/2011 11:24:00 AM 2/8/2011 11:23:56 AM 2/8/2011 11:23:56 AM	MRQ granted: XI12 Drawer 1 Input state change at expansi Expansion telay XR12 Drawer Input state change at expansi Input state change at expansi Input state change at expansi Input state change at expansi Expansion telay XR12 Drawer	c ion input X112 Drawer 12 r12 state change (U) nor ion input X112 Drawer 12 on input X012 Drawer 12 ion input X002 Drawer 21 ion input X002 Drawer 21 r12 state change (1) con	to Door // IRQE X Tamper X cur re to Door // IRQE // ITamper X cur to Door // IRQE X Tamper X cur s Door // IRQE // ITamper X cur tol zone trigger	\v\$NET 001 0001 001 01 3012 \v\$NET 001 0001 001 01 3012 \v\$NET 001 0001 001 01 3012 \v\$NET 001 0001 001 01 3002 \v\$NET 001 0001 001 01 3002 \v\$NET 001 0001 001 01 3012	DIGI'TRAC External DIGI'TRAC internal DIGI'TRAC External DIGI'TRAC External DIGI'TRAC External DIGI'TRAC (riternal	4024 9034 4024 4024 4024 9034
28/2011 11:24:18 AM 28/2011 11:24:06 AM 28/2011 11:24:06 AM 28/2011 11:24:00 AM 28/2011 11:24:00 AM 28/2011 11:24:56 AM 28/2011 11:23:52 AM	MRQ granted: X112 Drawer 1 Input state change at expansi Expansion relay XR12 Drawer Input state change at expansi Input state change at expansi Expansion relay XR12 Drawer Operator USER triggered relag	con input X012 Drawer 12 (12 state change (U) nor ion input X012 Drawer 12 on input X002 Drawer 21 on input X002 Drawer 21 (12 state change (1) con (XR12 Drawer 12 from v)	to Door // IRQE X Tamper X cur. te to Door // IRQE // Tamper X cur 0 Door // IRQE X Tamper X cure 5 Door // IRQE X Tamper X cure tel cone trigger vel cone trigger	VVANET 001 0001,001 01 3012 VVANET.001.0001,001.01 3912 VVANET.001.0001,001 01 3912 VVANET.001.0001,001 01 3912 VVANET.001.0001,001 01 3912 VVANET.001.0001,001 01 3912 VVANET.001	DIGITRAC External DIGITRAC Internal DIGITRAC External DIGITRAC External DIGITRAC External DIGITRAC External DIGITRAC Internal Software	4024 9034 4024 4024 4024 9034 6060
28/2011 11:24:18 AM 2/8/2011 11:24:06 AM 2/8/2011 11:24:06 AM 2/8/2011 11:24:06 AM 2/8/2011 11:24:00 AM 2/8/2011 11:23:52 AM 2/8/2011 11:23:52 AM 2/8/2011 11:23:52 AM	MRQ granted: X112 Drawer 1 Ingut state change at exponsi Expansion relay XR12 Drawer Ingut state change at exponsi Ingut state change at exponsi Exponsion relay XR12 Drawer Operator USER triggered relations Ingut state change at exponsi	2 ion input XI12 Drawen 12 ir 12 state change (U) non input XI12 Drawen 12 ion input XI02 Drawen 2 ti ch 12 state change (1) con xXR12 Drawen 12 Iron x con input XI02 Drawen 2 ti	to Door // IRDE X Tamper X curr. He to Door // IRDE // Tamper X curr. to Door // IRDE // Tamper X curr. to Door // IRDE // Tamper X curr. thit one trigger workstation TSECURE1 0 cor // IRDE X Tamper X curr.	VV-04ET_011_0001_001_01_01_01_012 VV-04ET_001_0001_001_01_01_012 VV-04ET_001_0001_001_01_01_012 VV-04ET_001_0001_001_01_002 VV-04ET_001_0001_001_01_01_012 VV-04ET_001_0001_001_01_01_002	DIGI*TRAC External DIGI*TRAC Internal DIGI*TRAC External DIGI*TRAC External DIGI*TRAC External DIGI*TRAC External DIGI*TRAC External	4024 9034 4024 4024 9034 9034 6060 4024

Event Viewer and Administration

Event Viewer (F7)

The Event Viewer window shows all internal and external Velocity events. For example, when a new person is enrolled in system, the Event Viewer shows the credential downloads to the cabinets. When someone uses a CAC to access a drawer, the Event Viewer shows the card reader transaction, access granted or denied, which drawer is unlocked, etc. The Event Viewer window usually is positioned across the bottom of the screen.

Administration (F2)

The Administration window is used to create and configure new cabinets within Velocity as they are added to the network, re-establish communications after a network or power outage, and manually override certain drawer functions for special circumstances or during troubleshooting. In the left pane is a standard Windows tree. Each entry can be expanded to access detail items below it.

The first two items under Velocity Configuration are Person Templates and Credential Templates. Enrollment Manager is used to add, manage, and delete users. Once the user is created, the user must have one or more credentials to access the cabinets. Users and credentials can be created individually, but templates make enrollment easier and more reliable for groups of users with identical requirements. Because templates can affect many (or all) users, they are managed under Administration. There can be many credential templates (day shift, supervisor, specific groups of cabinets, etc.), and one of them can be set as the default for new enrollments.

The second main item in the left pane is DIGI*TRAC Configuration. Expand the XNET item to see the Ports. Each Port represents one cabinet. Note that while the 16-drawer cabinet looks like two cabinets bolted together, it has only one card reader and one set of system electronics, and appears as one port to Velocity. Expanding the Port, Xbox, and Controller beneath it reveals the Expansion Inputs and Expansion Relays. These are the components within each cabinet that control the drawer locks. Individual components can be enabled or disables, triggered, and forced on or off. Direct control of these components through the Administration module is reserved for troubleshooting the system, and should not be a part of normal operation.

Note: Each Port, Xbox, and Controller in Velocity have names. It is important that the names reflect the physical location of the controllers because these names appear in operation logs and status reports. For example, the controller name "117" has very little useful information. However, a controller named "H23SE2F15" or "H23-SE-02-F15" could mean "Hangar 23, Southeast corner, cabinet #2, F-15 aircraft". When an alarm appears in the Event Viewer, this name identifies the location and type of asset without requiring a chart or some other form of directory.

The Administrator's Guide has sections devoted to creating the three elements (Port, Xbox, and Controller) associated with each cabinet, and should be studied for detailed operation of this module. This is a summary of the steps to create a cabinet in Velocity.

In the left pane, Expand DIGI*TRAC Configuration click XNET In the right pane, click Add New Port Name the port, uncheck the Enable box, click Apply

In the left pane, right-click the Port, select properties

Enrollment Manager	- TSECURE1\ Everyo	ne					_ @ ×
Search Explore	Credentials						
TSECURE1	IDF		ID	Function		Description	Status Issu
Search Results	Add New Cred	Mar Add New Credential from Template					
	Personal Inform General TAB 1 Several TD:	ation TAB 2 TAB 3 T/ 1	4B 4 T.∕	xB 5 TAB 6 TAB 7 Record I	TAB 8 TAI Last Updated:	3 9 TAB 10 Group 2/8/2011	is Additional Images
	Name: (First, Last)	Alex		Ho	ward		123
Last Name First	LandLine Phone	(800) 555-1212		Expiration Date	12 Jun 201	2	E
Sector Addresson no Sector Credenti	Mobile Phone Nun Building Location	Building 102		User Defined 9 User Defined 10	open open		C C
Howard Alex Pabis Jareo	Position	Fabrication		User Defined 11	open		172
	Parse Field	THX-1138		User Defined 12	open		Double-click images
	Address	Base, USA		User Defined 14	open		to edit
	Add Ne	ew Credential	Ø	Assign Credential	©	Preview Badge	Print Badge
People: 3 Assign	, Scan ed Credentials: 3	Unassigned Crede	entials: O	Guest Crede	entials: 0		ndn Analu

Enrollment Manager

The Enrollment Manager is used to create and delete users, and to assign credentials to allow access to the EMM cabinets. Users can be created individually or imported from a database file of personnel information. The Professional Services Group at Hirsch Electronics can assist in converting a personnel database for import into the Velocity system. Once a user has been created, credentials must be assigned. The credential has information about the user's access to the cabinets, such as which cabinets, which times of day, weekend or holiday lockouts, etc.

Each location that will enroll users should have a separate CAC reader. Tracewell supplies the SCM 3311 as the enrollment reader.

The Administrator's Guide and Operator's Guide have sections devoted to the Enrollment Manager, and should be studied for detailed operation of this module. This is a summary of the steps to create an individual user and assign a credential from a template.

Open the Enrollment Manager In the left pane, select Add Person Insert the person's CAC in the enrollment reader Click the Scan button In the Verify Scanner Data dialog box, click Read PIV Data Click Accept In the Add Person window, click Apply. It might take two clicks, now to select the window and one to apply.



Above the personal information, click Add Credential from Template Select template 2-Card

Masked Ro Stetu	s Group + Status Grou	n: DAC15		- P			. <u>m</u>						
Xinput Name	Address	Status	Alarm	Masked	Enabled	1A	2	3TMPR	LM	LM Volte	Updated		_
🗎 🖄 🕅 Drawer 1	WWNET.001.0001.001.	-		1.	Yes	-			3		02/01/2011	11:28:	
🔌 🖂 02 Drawer 2	WANET.001.0001.001.			14 - C	Yes		κ.	•	3		02/01/2011	11.28:	
🗎 XIII Diawer 3	WWNET.001.0001.001.		(2)		Yes	~			з		02/01/2011	11:28:	
🔌 🗵 04 Drawer 4	WANE T. 001.0001.001.		1.51		Yes				3		02/01/2011	11.28	
🛪 ×105 Drawer 5	WWNET.001.0001.001.	-		×	Yes	-	-	-	3	14	02/01/2011	11:28:	
🔌 🖄 D6 Drawer 6	WWNET.001.0001.001.		1.41	14	Yes	κ.	× .		3		02/01/2011	11.28:	
X D7 Drawer 7	WWNET.001.0001.001.		120		Yes	2			з	35	02/01/2011	11:29:	
🔌 🗵 D8 Drawer B	WANE T. OD1.0001.001.		1.0	12	Yes				3		02/01/2011	11:28:	
🔌 🛛 Diawer 9	WWNET.001.0001.001.		141	12	Yes	2		-	3	14	02/01/2011	11:28:	
🖠 🖂 10 Drawer 10	WANET.001.0001.001.	-		3	Yes		÷.		3		02/01/2011	11.28:	
🕯 🛛 11 Drawer 11	WWNET.001.0001.001.	ar - 1	100		Yes	2			3	15	02/01/2011	11:28:	
🖠 🖂 12 Drawer 12	WANET.001.0001.001.				Yes				3		02/01/2011	11.28:	
🕯 🛛 13 Diawer 13	WANE T.001.0001.001.		141		Yes	2		-	З	14	02/01/2011	11:29:	
🖠 🖂 14 Drawer 14	WANET.001.0001.001.		1.00	14	Yes				3		02/01/2011	11.28	
15 Diawer 15	WWNET.001.0001.001.	a a	175	12	Yes	<i></i>			3		02/01/2011	11:28:	
🕯 🖂 16 Drawer 16	WANE T. 001.0001.001.				Yes				3		02/01/2011	11:28:	
🕯 Xinput III Dra	WANE T.001.0002.001.		191		Yes	2	14	-	1	14	02/01/2011	11:29:	
🖠 🖄 nput 02 Dra	WANET.001.0002.001.			14	Yes	÷ .			1		02/01/2011	11.28	
🕯 Xinput 03 Dia	WWNE T.001.0002.001.		125		Yes	-		-	1	-	02/01/2011	11:29:	
🔌 🗵 nput D4 Dra	WANET.001.0002.001.				Yes				1		02/01/2011	11.28:	
Host Time	Description		an a	and the second se				Address			Event Type	EventID	_
2/1/2011 11:18:28	AM Communications	port CAC-16-M2 wa	s changed by U	SER				WITSECURE	1.001		Software	1079	
2/1/2011 11:17:56	AM Communications	port CAC-16-M2 wa	s changed by U	SER				WISECURE	1.001		Software	1079	
2/1/2011 11:17:35	AM Expansion relay	XR02 Drawer 2 state	e change (0) nor					WWNET.001	0001.001	.01×R02	DIGI*TRAC Internal	9034	
221/2011 11:17:29	AM Expansion relay	XR02 Drawer 2 state	e change (1) cor	nitol zone ling	ger			WANET.001	0001.001	01×802	DIGI*TRAC Internal	9034	

Status Viewer (F9)

The Status View displays information about the control electronics inputs and outputs in real time. For each controller on the network, you can create a group of inputs and/or outputs.

The Administrator's Guide and Operator's Guide have sections devoted to the Status Viewer, and should be studied for detailed operation of this module. Presented here is a brief listing of the steps to create status groups for the inputs and outputs of one controller.

Open the Status Viewer

Secure Laptop Client

learId	Name	Controller Mame	Lanton klama	Lanton Address	Lanton Time	Remove Date	Return Flate
3	Casen West	Serue Lanton M2	XI01 Draver 1	WANET OCT 0001 001 01 X01	0 minutes	12/8/2010 4:29:22 PM	12/8/2010 4:23 50 FM
2	Cases West	Serue Lanton M2	2001 Drawer 1	VSINET 001 0001 001 01 24 01	0 minutes	12/8/2010 11:18:17 AM	12/8/2010 11:18:33 AM
1	Casen West	Servie Lapton M2	XIII Drager 1	VSXNET OCT 0001 0CT 01 X101	1 day 1 bour 56 min	12/6/2010 11:43:02 4M	12/7/2010 1:39 43 EM
3	Casey West	Servie Lanton M2	2410 Drawer 10	WANET 001 0001 001 01 ×10	() minutes	12/3/2010 2:12:13 PM	12/3/2010 212 35 FM
í	Casen West	Servie Laptop M2	XIII Draver 1	VSXNET 001 0001 001 01 X101	1 den 4 hours 26 mi	12/2/2010 9-42-14 AM	12/3/2010 2:08 59 EM
3	Casey West	Servie Lanton M2	201 Drawer 1	VMNET 001 0001 001 01 ×101	10 minutes	12/2/2010.9:11:51 AM	12/2/2010 9:22 37 AM
1	Caseulidest	Service Lanton M2	M01 Drager 1	VSXNET 001 0001 001 01 X101	fi minutes	12/2/2010 9:09:23 AM	12/2/2010 9:09 51 AM
3	Casey West	Serue Lanton M2	2101 Draver 1	WANET ODI 0001 001 01 XIDI	() minutes	12/2/2010 8-54-33 AM	12/2/2010 R55 D4 AM
1	Casen West	Secure Laptop M2	XI01 Draver 1	VX/NET.001.0001.001.01 XI01	0 minutes	12/2/2010 8:46:57 AM	12/2/2010 B 47 19 AM
2	Casey West	Serue Lanton M2	2001 Draver 1	USENET OPLICED OPLICE ADD	1 minute	12/2/2010 9:38:50 AM	12/2/2010 R 40 D3 AM
1	Casen West	Secure Lapton M16.1	Monut01 Draver (cout 1	VSXNET.001.0002.001.01 X101	22 hours 51 minuter	12/1/2010 9:46:42 AM	12/2/2010 8:38:20 AM
3	Casey West	Servie Lanton M2	2001 Drawer 1	WANET OF LODI OF UT AT	() minutes	11/31/2010 # 36:25 PM	11/30/2010 4:36:42 PM
-	Casen West	Service Lapton M2	M02 Draver 2	V\$2NET 001 0001 001 01 X102	fl minutes	11/30/2010 & 16 & 4 PM	11/30/2010 4:17:06 PM
3	Casey West	Servie Lanton M2	2110 Drawer 10	WANET 001 0001 001 01 ×10	1 minute	11/31/2010 3 08:04 PM	11/30/2010 3:09:23 PM
2	Jared Pabis	Secure Laptop M2	XI01 Draver 1	WANE T. 001.0001.001.01 XID1	0 minutes	11/19/2010 2 58 21 PM	11/19/2010 2:58:38 PM
3	Casey West	Serure Lanton M2	2105 Drawer 5	WANET OF LODI OF UT MIS	1 minute	11/19/2010 9 21:13 AM	11/19/2010 9:22:28 AM
	Alex Howard	Secure Laptop M2	XI02 Draver 2	WANE T. 001.0001.001.01 XL02	1 minute	11/19/2010 9 20:22 AM	11/19/2010 9:22:03 AM
2	Jared Pabia	Secure Lapton M2	2403 Drawer 3	WANET OCT 0001 001 01 20 03	1 minute	11/19/2010 9 20:06 AM	11/19/2010 9:21:41 AM
3	Casey West	Secure Laptop M2	XI01 Drawer 1	WANE T. 001.0001.001.01 X D1	0 minutes	11/19/2010 9 19:47 AM	11/19/2010 9:20:45 AM
	Alex Howard	Secure Laptop M2	2116 Drawer 16	WANET.001.0001.001.012416	0 minutes	11/19/2010 9:18:35 AM	11/19/2010 9:19:14 AM
2	Jared Pabis	Secure Laptop M2	X15 Draver 15	WANET.001.0001.001.01.X15	1 minute	11/19/2010 9 18 16 AM	11/19/2010 9:19:27 AM
3	Case#West	Secure Laptop M2	2014 Drawer 14	WANET.001.0001.001.012414	0 minutes	11/19/2010 9 18:03 AM	11/19/2010 9:18:58 AM
1	Alex Howard	Secure Laptop M2	XI13 Draver 13	WANET.001.0001.001.01.X13	0 minutes	11/19/2010 9 16 52 AM	11/19/2010 9:17:44 AM
2	Jared Pabis	Secure Laptop M2	2112 Drawer 12	WANET.001.0001.001.01.212	0 minutes	11/19/2010 9.16:30 AM	11/15/2010 9:17:27 AM
3	Casep West	Secure Laptop M2	XIII Draver 11	WANET.001.0001.001.01.X11	0 minutes	11/19/2010 9 16:13 AM	11/19/2010 9:17:11 AM
	Alex Howard	Secure Laptop M2	>110 Drawer 10	WANET.001.0001.001.01.2110	0 minutes	11/19/2010 9:14:56 AM	11/19/2010 9:15:51 AM
2	Jared Pabis	Secure Laptop M2	×109 Drawer 9	WANE T. 001.0001.001.01 X109	0 minutes	11/19/2010 9 14:34 AM	11/19/2010 9:15:32 AM
3	Casey West	Secure Laptop M2	>108 Drawer 8	WANET.001.0001.001.01.2408	0 minutes	11/19/2010 9:14:18 AM	11/19/2010 9:15:15 AM
	Alex Howard	Secure Laptop M2	XI07 Drawer 7	WANET.001.0001.001.01.X07	1 minute	11/19/2010 9 12:55 AM	11/19/2010 9:13:58 AM
2	Jared Pabis	Secure Laptop M2	2406 Drawer 6	WANET.001.0001.001.01.206	1 minute	11/19/2010 9:12:25 AM	11/18/2010 9:13:36 AM
3	Casep West	Secure Laptop M2	XI04 Draver 4	WANET.001.0001.001.01.X04	1 minute	11/19/2010 9 11:30 AM	11/19/2010 9:13:17 AM
3	Casey West	Secure Laptop M2	×105 Drawer 5	WANET.001.0001.001.01.2405	1 day, 19 hours, 25	11/17/2010 1:20:41 PM	11/15/2010 8:46:33 AM
3	Casep West	Secure Laptop M161	Minput 01 Draver Input 1	WXNET.001.0002.001.01.X101	7 minutes	11/17/2010 1:12:40 PM	11/17/2010 1:20:10 PM
	Alex Howard	Secure Laptop M2	×103 Drawer 3	WANET.001.0001.001.01.2403	1 day, 19 hours, 43	11/17/2010 1:03:23 PM	11/19/2010 8:46:25 AM
2	Jared Pabis	Secure Laptop M2	XI02 Drawer 2	WANET.001.0001.001.01.X02	1 day, 19 hours, 43	11/17/2010 1:03:00 PM	11/19/2010 8:46:29 AM
2	Jared Pabis	Secure Laptop M2	×I01 Drawer 1	WANET.001.0001.001.01.2101	0 minutes	11/17/2010 1:00:00 PM	11/17/2010 1:00:40 PM

Secure Laptop Client

The Secure Laptop Client is a utility provided to monitor the cabinets and their assets. Through the Client you can see who has assets checked out, the status of any cabinet or drawer, and the history of any user or asset. If a problem occurred during checkout or checkin, the Client can reset the status of a user.

Note: the Secure Laptop Client does not update automatically after it is opened. To see the latest status for any cabinet, you must click Refresh.

Microsoft SQL Server

Velocity is a database application program that runs under Microsoft SQL Server. In a stand-alone installation, where the application and database engine are on the same computer, the standard Velocity installation includes Microsoft SQL Server Management Studio Express. This is a mini-version of SQL Server for a single instance of Velocity.

In a networked installation, SQL Server runs on a computer that is separate from the one running the Velocity application. Typically, SQL Server runs on a server farm under IT control, while the Velocity application runs on a desktop system conveniently located for managing the system, handling enrollments, and printing reports. In this case, several instances of Velocity can be running in different locations around the network.

SECURE LAPTOP CLIENT

High Level Description of SecureLaptop Logical Process, (v 3.1.9.6)

There are two types of events that occur in Velocity and are reported to the SecureLaptop service (through the MSMQ) that drive each laptop transaction. "Control Grant" events that start all new transactions, and "Input State Change" events that may end a previously started transaction. Transactions may also end at the end of one of two timeout intervals: 1) the "Relay Timeout" which is a limit on the length of a transaction from the time it first started, or 2) the "Laptop Return Timer" that can terminate a return event in lieu of a subsequent event. (These timer values are as they appear on the SecureLaptopConfig configuration program).

There is a third event type that is processed from Velocity, but is not part of any laptop transaction: the "Controller Logged On" event. When this event is received for an M16 controller, a sequence of command sets is executed to turn on the cabinet's LED lights.

The main flow of logic that occurs when the service is running is that it sits in a loop, waiting indefinitely for a new Velocity event to arrive, (Control Grant, Input State Change). When it does, each event gets processed sequentially. The first one must complete before the second one gets processed. This is true across all cabinets being managed.

When an event comes in, if that event is a Control Grant, then:

- Control Grant transaction for a specific credential is received for a controller being managed.
- Credential's user is determined.
- A check is made if there are any transactions still in process for the same controller that began less than 30 seconds ago. If any are found the current transaction ends.
- A check is made if there are any transactions still in process for the same controller (these are ones that began 30 seconds or more in the past). If any are found these transactions are ended. (These are transactions for users who presented their cards, but either did not complete their laptop transaction, or returned a laptop and the laptop return timer has not yet expired). If the previous transaction was a Laptop Return, then the "Finish Pending Laptop Return" process checks to make sure the laptop is present by querying Velocity for the laptop's Expansion Input state. If the laptop is present, the previous transaction gets saved as a successful laptop return. All other previous transaction end as failed laptop transactions.
- PSGSecureLaptopUsers table is queried for the user for the current Control Grant. If a user record is found this transaction is a "Return Laptop" transaction, otherwise it's a "Get Laptop" transaction.
- All current laptop Expansion Input states are retrieved from Velocity. For "Return Laptop" transactions, the Expansion Input for the laptop being returned is checked to make sure it's enabled, and the laptop is absent. For "Get Laptop" transactions the next available Expansion Input is determined based on date/time stamps from when they were last returned (and ignoring master laptops).
- The relay is determined for the drawer that needs to be opened, and sending the trigger relay command to Velocity fires the relay.
- Data is stored (in memory) to indicate that this laptop transaction is in process for the current controller and has not ended. This transaction will remain in process until it is ended by a subsequent Velocity event, or the transaction times out.

When the event that comes in is an Input State Change, then:

- Input State Change event for a laptop Expansion Input is received for a controller being managed.
- All laptop transactions still in process are checked to see if any are for the same laptop Expansion Input address as the address for which a state change event just occurred. If not, the event is logged as not corresponding to any current laptop transaction, and the event is finished being processed
- If the matching laptop transaction is a "Laptop Return", then appropriate info is logged, the transaction

remains open because the laptop return timer is used to determine the end of the transaction, and the event is finished being processed.

- If the current state change is for a "Get Laptop" transaction:
- If the laptop state as reported by the input state change event indicates that the laptop is not present, the laptop has been successfully removed. The laptop gets assigned to the current user in the PSG Secure Laptop Users table. Otherwise this transaction ends as a failed laptop transaction.

If the current state change is for a "Return Laptop" transaction:

• The event processing has already exited above.

At the same time the main flow of logic is occurring in the service, a secondary thread sits in a loop the entire time the service is running. It checks to see if there are any transactions that are still in process, (in memory), and if so, whether or not any of them have timed out.

After doing this check it sleeps for a full second, then checks again. Each time it finds a laptop transaction that's still in process, (and an Input State Change event has not already started working on it):

If the current laptop transaction is a "Return Laptop" transaction:

The date/time stamp when the transaction data was first created (at the time the relay was fired in the Control Grant event) is compared to the current date/time from the PC clock. If the interval in seconds is greater than the "Laptop Return Timer" value, then the laptop return timer has expired. The "Finish Pending Laptop Return" process checks to make sure the laptop is present by querying Velocity for the laptop's Expansion Input state. If the laptop is present, the transaction gets saved as a successful laptop return, the laptop user get saved to user history, and the laptop return date gets saved. Otherwise the transaction ends as a failed laptop transaction.

For all other transactions that are not "Return Laptop" transactions:

The date/time stamp when the transaction data was first created (at the time the relay was fired in the Control Grant event) is compared to the current date/time from the PC clock. If the interval in seconds is greater than the "Relay Timeout" value, then the transaction has timed out. The transaction ends as a failed laptop transaction.

Sample Use Cases

The following describes the sequence of events as they occur when a user who does not have a laptop assigned to them removes one from an ETool cabinet being managed by the SecureLaptop service.

Successful flow of events:

- 1. User presents their card at the reader and successfully authenticates. This triggers a control grant event in Velocity.
- 2. The service recognizes this as a user who does not have a laptop, and triggers the relay to open the drawer for the next available laptop.
- 3. User opens the drawer.
- 4. User removes the laptop from the drawer. At this point the service has not detected the laptop's removal because the open drawer is blocking the sensor.
- 5. User closes the drawer.
- 6. The service receives the state change event that indicates the laptop is no longer in the drawer since the sensor is no longer blocked by the drawer. The laptop is assigned to the user, and the user has successfully removed their laptop.

Alternative flow 3.1 – User never opens the drawer

- 1. No state change event is ever received for the relay that was triggered.
- 2. When the Relay Timeout period expires, or when another user successfully presents their card, this laptop transaction fails as an unsuccessful "Get Laptop" transaction and the user is not assigned the laptop.

Alternative flow 4.1 – User opens and closes the drawer without removing the laptop.

- 1. No state change event is ever received for the relay that was triggered.
- 2. When the Relay Timeout period expires, or when another user successfully.
- 3. presents their card, this laptop transaction fails as an unsuccessful "Get Laptop" transaction and the user is not assigned the laptop.

Alternative flow 4.2 – User opens the drawer and keeps it open.

- 1. No state change event is ever received for the relay that was triggered.
- 2. When the Relay Timeout period expires, or when another user successfully presents their card, this laptop transaction fails as an unsuccessful "Get Laptop" transaction and the user is not assigned the laptop.

The following describes the sequence of events as they occur when a user who has a laptop assigned to them replaces it to an ETool cabinet being managed by the SecureLaptop service.

Successful flow of events:

- 1. User presents their card at the reader and successfully authenticates. This triggers a control grant event in Velocity.
- 2. The service recognizes this as a user who has a laptop, and triggers the relay to open the drawer for the same laptop.
- 3. User opens the drawer.
- 4. The open drawer blocks the laptop sensor, which triggers the laptop input state change event. This event is ignored by the service because it uses a Return Laptop Timer to determine when the laptop has been replaced.
- 5. User replaces the laptop in the drawer.
- 6. User closes the drawer. No more input state change events occur because the sensor was blocked as soon as the drawer was opened.
- 7. When the Return Laptop Timer expires, or when another user presents their card, the service does the "Finish Pending Laptop Return" process: it queries Velocity to get the laptop state. Since the laptop is present, this transaction completes as a successful laptop return, and the laptop is no longer assigned to the user.

Alternative flow 3.1 – User never opens the drawer

- 1. No state change event is ever received for the relay that was triggered.
- 2. When the Relay Timeout period expires, or when another user successfully presents their card, the service does the "Finish Pending Laptop Return" process: it queries Velocity to get the laptop state.

Since the laptop is not present the transaction fails as an unsuccessful laptop return, and the user is still as signed their laptop.

Alternative flow 3.2 – User opens and closes the drawer without removing the laptop.

- 1. The open drawer blocks the laptop sensor, which triggers the laptop input state change event. This event is ignored by the service because it uses a Return Laptop Timer to determine when the laptop has been replaced.
- 2. When the Relay Timeout period expires, or when another user successfully presents their card, the service does the "Finish Pending Laptop Return" process: it queries Velocity to get the laptop state. Since the laptop is not present the transaction fails as an unsuccessful laptop return, and the user is still assigned their laptop.

Alternative flow 3.3 – User opens the drawer and keeps it open.

- 1. The open drawer blocks the laptop sensor, which triggers the laptop input state change event. This event is ignored by the service because it uses a Return Laptop Timer to determine when the laptop has been replaced.
- 2. When the Relay Timeout period expires, or when another user successfully presents their card, the service does the "Finish Pending Laptop Return" process: it queries Velocity to get the laptop state. Since the laptop is not present the transaction fails as an unsuccessful laptop return, and the user is still assigned their laptop.

A1-SLSS Startup Procedure Checklist

Checklist of steps when restarting Velocity and the SecureLaptop service on a system where THE SYSTEM HAS ALREADY BEEN INSTALLED AND CONFIGURED CORRECTLY.

Make sure all services and applications are shut down:

START THE VELOCITY SERVICES

- From the Velocity Services icon running in the system tray: Start the Velocity Security Domain Service.
- Start the Velocity DIGI*TRAC Network Service.
- Start the Velocity Extension Service.
- Verify that all services are running using the icon in the system tray.
- Open Windows Explorer and navigate to the Velocity installation folder: this is typically in the c:\Program Files\Hirsch Electronics\Velocity Folder.
- Sort all files in that folder in Date Modified, descending order, (newest files at the top).
- Open the "Velocity MSMQ Writer Extension-Technical Support File.Txt" file that should now have a date/time stamp that matches the fact you just restarted the services. (You may need to wait several moments for this file to be updated if it takes a while for your Velocity services to start).
- Near or at the bottom of that file with a recent timestamp, you should see a logged message similar to: "MSMQ Writer is pushing to Queue: [SecureLaptop Queue Name]". If you cannot confirm that the MSMQ Writer is writing in this log file, then there is an issue with your system's installation of the MSMQ, and/or how it's configured in Velocity.

VERIFY THE MSMQ MESSAGES ARE BEING WRITTEN BY VELOCITY

- With the SecureLaptop service not running, open Windows Explorer. Right-click the Computer icon, and select "Manage". This opens the Computer Management window. Expand the "Services and Applications" entry at the bottom of the list in the left window. Expand "Message Queuing". Expand "Private Queues", (the MSMQ used by SecureLaptop is likely a private queue for stand-alone systems because Public Queues are only valid on a domain). Expand your secure laptop message queue. Click on Queue Messages. There should be no messages if you haven't run any transactions since the SecureLaptop service was last stopped. If there are some messages in there, that's okay.
- Authenticate a card at the reader on the E-Tool cabinet. This generates a Control Grant transaction in Velocity. Right-click "Queueu messages" and select refresh.

(while Queue messages is still selected in the window). You should now see a new message that has been written to the MSMQ for the most recent control grant. If you do not see a new message, then there is an issue with your MSMQ configuration. Note that if you verified that Velocity was writing to this queue in the step above, and you are still not seeing any messages, then the most likely reason is either permissions, (the account Velocity is running under may not have NTFS permissions to write to this queue), or the message numbers that are configured in Velocity to be written to this queue are not correct. Please refer to the installation documentation to verify the messages that need to be configured.

VERIFY THAT VELOCITY IS COMMUNICATING WITH ALL PORTS/CONTROLLERS

 Verify that the Velocity Status Viewer is displaying status info for all the laptop expansion input addresses for your controllers. This status data is how the SecureLaptop service determines the presence/absence of each laptop in the cabinet. To do this, open the Status Viewer by selecting Console -> Status Viewer from the Velocity menu:



When you first open this screen, no status groups will be selected. Select the status group that shows all your controller expansion inputs. If everything is set up correctly and Velocity is communicating with the controllers, then you'll see info under the Status, 1ALRM, and 2RQE fields for each address:

Masked 🚯 Status Group 👻 S	Status Group: Controller 1	- 60				
XInput Name	Address	Status	Alarm	Masked	Enabled	1ALRM
🔌 Xinput 01 Drawer Input 1	VXNET.001.0001.001.01.X001	OPEN	+		Yes	11
Ninput 02 Drawer Input 2	\VXNET.001.0001.001.01.202	Secure		1.0	Yes	×
Ninput 03 Drawer Input 3	\VXNET.001.0001.001.01.2003	Secure	*:	12	Yes	×
🜒 Xinput 04 Drawer Input 4	\VXNET.001.0001.001.01.2004	Secure	2	12	Yes	×
🙀 XInput 05 Drawer Input 5	\VXNET.001.0001.001.01.XI05	Secure		1	No	×
Minput 06 Drawer Input 6	\VXNET.001.0001.001.01.XI06	Secure	+	8	Yes	×
Ninput 07 Drawer Input 7	\WNET.001.0001.001.01.>007	Open Circuit	÷.	2	Yes	Open Circuit
Sinput 08 Drawer Input 8	\VXNET.001.0001.001.01.208	Open Circuit	10	1	Yes	Open Circuit
Xinput 09 Drawer Input 9	WWNET.001.0001.001.01.2009	Open Circuit	*:	38	Yes	Open Circuit
Xinput 10 Drawer Input 10	WWNET.001.0001.001.01.2010	Open Circuit	*2	12	Yes	Open Circuit
Input 11 Spare	\WNET.001.0001.001.01.311	Open Circuit	•		Yes	Open Circuit
Nnput 12 Spare	\WNET.001.0001.001.01.>012	Open Circuit		64 - C	Yes	Open Circuit
Anput 13 Spare	\WNET.001.0001.001.01.2013	Open Circuit	42	14	Yes	Open Circuit
🕺 Xinput 14 Spare	\WNET.001.0001.001.01.2014	Open Circuit	38	a -	Yes	Open Circuit
Host Time Descri	ption					
Host time Description	ption					

The 1ALRM values of "//" and "X" indicate whether or not the laptop sensor is open or closed.

If, on the other hand, Velocity and the controller are not communicating correctly, then all those field values will be blank:

Masked 🚯 Status Gro	oup 👻 Status Group: Controlle	r 1	- 6 0				
Xinput Name	Address	Status	Alarm	Masked	Enabled	1ALRM	7
🕅 XInput 01 Drawer Inp	\\XNET.001.0001.001.01.XI0	1 •		14	Yes		
Ninput 02 Drawer Inp	\WNET.001.0001.001.01.X00	2 -	250	4	Yes	12	14
Sinput 03 Drawer Inp	VVINET.001.0001.001.01.00	3 -		,	Yes	+ ::	
XInput 04 Drawer Inp	WONET.001.0001.001.01.X10	4 -	1963	*	Yes	£1	
XInput 05 Drawer Inp	VV/NET.001.0001.001.01.X10	5 -		14	Yes	45	
Anput 06 Drawer Inp	WONET.001.0001.001.01.00	6 -		ST.	Yes	•	+
Ninput 07 Drawer Inp	\WNET.001.0001.001.01.XI0	7 .	1.00	181	Yes	×.	
Sinput 08 Drawer Inp	\WNET.001.0001.001.01.X10	8 •		881	Yes	5 3	
Sinput 09 Drawer Inp	WXNET.001.0001.001.01.X0	9 -	8350	100	Yes	10	
Anput 10 Drawer Inp	WWNET.001.0001.001.01.X11	0 -			Yes		
Kinput 11 Spare	VVINET.001.0001.001.01.XI1	1 -			Yes		
Sinput 12 Spare	\WNET.001.0001.001.01.XI1	2 -		2	Yes	20	
Anput 13 Spare	WXNET.001.0001.001.01.X11	3 -		4	Yes	10	
Ninput 14 Spare	WWNET.001.0001.001.01.X11	4 -	52451	12	Yes	4.	4
Xinput 15 Spare	VV/NET.001.0001.001.01.X11	5 -		(2)	Yes	*	
W	NAMET ON DOOL OF OLVIN	n					_
Host Time	Controller Time	Description					
4/14/2011 1:56:02 PM	s	tatus Group Controlle	1 added by TebohoN				

If this is the case, then there is a problem with the port and/or controller and how they are configured in Velocity. (When Velocity is first coming online after a power outage, it may just be that you need to disable, and re-enable the port to get everything working again).

• Another way to check whether or not the SecureLaptop service can get the expansion input state information from Velocity is to run the SecureLaptopClient.exe monitoring program, and select all the controllers on your system to view their laptop status.

If everything is set up correctly, you will see all the current laptop status info:

Controllers	[M16] Secure Lap	top M16 1				
XInput Id	ETool Name	Address		Laptop Status		
65	XInput 01 Draw	\WNET.001.0001.0	001.01.×101	Laptop is present		
66	XInput 02 Draw	\XXNET.001.0001.0	01.01.XI02	Laptop is present		
67	XInput 03 Draw	WXNET.001.0001.0	01.01.×103	Laptop is present		
68	XInput 04 Draw	\WNET.001.0001.0	01.01.×104	Laptop is present		
<u>A</u> 69	XInput 05 Draw	\WNET.001.0001.0	001.01.×105	[XInput for this laptop is	DISABLED]	-
A 70	XInput 06 Draw	\WNET.001.0001.0	001.01.×106	Laptop is present		
<u>Å</u> 71	XInput 07 Draw	\WNET.001.0001.0	01.01.XI07	[XInput for this laptop ha	as an OPEN CIRCUIT]	
<u>A</u> 72	XInput 08 Draw	\WNET.001.0001.0	01.01.XI08	[XInput for this laptop ha	as an OPEN CIRCUIT]	
A 73	XInput 09 Draw	\XXNET.001.0001.0	01.01.XI09	[XInput for this laptop ha	as an OPEN CIRCUIT]	
4 74	Missout 10 Draw			[Vincut for this laston ha		
Current Use	rs with Laptops	Fredential Id	Ponding Pohrm	Controller Marrie	Laster Marie	
Useria	IName	Credential Id	Pending Return		Laptop Name	
3	Jane Smith	8	No	Secure Laptop M21	×I04 Drawer 4	
						,

If Velocity is not communicating, you will see no info when you select the controller for the port that is not configured correctly:

A					
Controllers	: [[M16] Tracewell	line and a second		Transment to guarante a	
XInput Id	ETool Name	Address		Laptop Status	
•					
Current Use	rs with Laptops	m			
Current Use	rs with Laptops				
Current Use Add Use User Id	rs with Laptops	III Credential Id	Pending Return	Controller Name	Laptop Name
Current Use	rs with Laptops	TTT Credential Id 8	Pending Return No	Controller Name Secure Laptop M2 1	Laptop Name XI04 Drawer 4

VERIFY THAT THE VELOCITY WEB SERVER IS UP AND RUNNING

 The Velocity web server is how the SecureLaptop service triggers the drawer relays: the service sends an XML RPC command to the web server, which then acts on it and triggers each drawer relay. To make sure it's back up and running, open up Internet Explorer and type in the URL for the web server. These settings are found by right-clicking on the Velocity services icon in your system tray, selecting Settings, then clicking the Web Server setting:

ystem 	Web Server Settings: Image: Default page: Number Number Port: 8080 Root directory: %ApplicationPath%\WebRoot Image: Enable RSS
Help	OK Canc

These settings should of course match what you have configured for the SecureLaptop service. In the screenshot above, the web server is running on port 8080, so in Internet Explorer the URL would be the computer name followed by the port:

http://mycomputer:8080

And if the web server is up and running, you will see the Velocity HTTP Server page get displayed in your browser:



START THE SECURELAPTOP SERVICE

 Once everything is up and running in Velocity, you should be able to run the SecureLaptop service using the services control manager window. This assumes everything was working correctly before the cabinet lost power and went offline. If the service fails to start, or starts, then shuts back down with an error, the log file (and or the log entries in the Windows Event Viewer) will tell you the reason for the error, and you should be able to troubleshoot from there.

A2-Logic Overview

High Level Description of SecureLaptop Logical Process, (v 3.1.9.4)

There are two types of events that occur in Velocity and are reported to the SecureLaptop service (through the MSMQ) that drive each laptop transaction. "Control Grant" events which start all new transactions, and "Input State Change" events which may end a previously started transaction. Transactions may also end at the end of one of two timeout intervals: 1) the "Relay Timeout" which is a limit on the length of a transaction from the time it first started, or 2) the "Laptop Return Timer" which is only used for M16 controllers when a laptop is being returned. (These timer values are as they appear on the SecureLaptopConfig configuration program).

There is a third event type that is processed from Velocity, but is not part of any laptop transaction: the "Controller Logged On" event. When this event is received for an M16 controller, a sequence of commandsets are executed to turn on the cabinet's LED lights.

The main flow of logic that occurs when the service is running is that it sits in a loop, waiting indefinitely for each new Velocity event to arrive, (Control Grant, Input State Change). When it does, each event gets processed sequentially. The first one must complete before the second one gets processed. This is true across all cabinets being managed.

When an event comes in, if that event is a Control Grant, then:

Control Grant transaction for a specific credential is received for a controller being managed.

Credential's user is determined.

M2 CONTROLLERS ONLY: If the current controller is an M2, a check is made for any open drawers. If any are found the current transaction ends.

A check is made if there are any transactions still in process for the same controller that began less than 30 seconds ago. If any are found the current transaction ends.

A check is made if there are any transactions still in process for the same controller (these are ones that began 30 seconds or more in the past). If any are found these transactions are ended. (These are transactions for users who presented their cards, but either did not complete their laptop transaction, or returned a laptop for an M16 where the laptop return timer has not yet expired). If the previous transaction was a Laptop Return for an M16 controller, then the "Finish Pending Laptop Return" process checks to make sure the laptop is present by querying Velocity for the laptop's Expansion Input state. If the laptop is present, the previous transaction gets saved as a successful laptop return. All other previous transaction end as failed laptop transactions.

PSGSecureLaptopUsers table is queried for the user for for the current Control Grant. If a user record is found this transaction is a "Return Laptop" transaction, otherwise it's a "Get Laptop" transaction.

All current laptop Expansion Input states are retrieved from Velocity. For "Return Laptop" transactions, the Expansion Input for the laptop being returned is checked to make sure it's enabled, and the laptop is absent. For "Get Laptop" transactions the next available Expansion Input is determined based on date/time stamps from when they were last returned (and ignoring master laptops).

The relay is determined for the drawer that needs to be opened, and the relay is fired by sending the trigger relay command to Velocity.

Data is stored (in memory) to indicate that this laptop transaction is in process for the current controller and has not ended. This transaction will remain in process until it gets ended by a subsequent Velocity event, or the transaction times out.

When the event that comes in is an Input State Change, then:

Input State Change event for a laptop Expansion Input is received for a controller being managed.

All laptop transactions still in process are checked to see if any are for the same laptop Expansion Input address as the address who's state change event just occurred. If not, the event is logged as not corresponding to any current laptop transaction, and the event is finished being processed.

If the matching laptop transaction is a "Laptop Return", if it's for an M16 controller, then appropriate info is logged, the transaction remains open because the laptop return timer is used to determine the end of the transaction, and the event is finished being processed.

If the current state change is for a "Get Laptop" transaction:

M16 CONTROLLERS: If the laptop state as reported by the input state change event indicates that the laptop is not present, the laptop has been successfully removed. The laptop gets assigned to the current user in the PSGSecure-LaptopUsers table. Otherwise this transaction ends as a failed laptop transaction.

M2 CONTROLLERS: The drawer and laptop states are retrieved from the input state change data. If the drawer is not closed as reported by the input state change event, then this transaction remains open. If the drawer is closed, the current laptop's expansion input state is retrieved from Velocity. If Velocity reports that the laptop is still present, this transaction ends as a failed Get Laptop transaction. (The user is not assigned this laptop). If Velocity reports that the laptop is absent, then the laptop has been successfully removed. The laptop gets assigned to the current user in the PSGSecureLaptopUsers table.

If the current state change is for a "Return Laptop" transaction:

M16 CONTROLLERS: The event processing has already exited above.

M2 CONTROLLERS: The drawer and laptop states are retrieved from the input state change data. If the drawer is not closed as reported by the input state change event, then this transaction remains open. If the drawer is closed, the current laptop's expansion input state is retrieved from Velocity. If Velocity reports that the laptop is absent, this transaction ends as a failed Return Laptop transaction. (The user is still assigned to this laptop). If Velocity reports that the laptop is present, then the laptop has successfully been returned. The laptop user record get saved to the PSGSecureLaptopUserHistory table, removed from the PSGSecureLaptopUsers table, and the laptop's return date gets saved.

At the same time the main flow of logic is occurring in the service, a secondary thread sits in a loop the entire time the service is running. It checks to see if there are any transactions that are still in process, (in memory), and if so, whether or not any of them have timed out. After doing this check it sleeps for a full second, then checks again. Each time it finds a laptop transaction that's still in process, (and an Input State Change event has not already started working on it):

If the current laptop transaction is a "Return Laptop" for an M16 controller:

The date/time stamp when the transaction data was first created (at the time the relay was fired in the Control Grant event) is compared to the current date/time from the PC clock. If the interval in seconds is greater than the "Laptop Return Timer" value, then the laptop return timer has expired. The "Finish Pending Laptop Return" process checks to make sure the laptop is present by querying Velocity for the laptop's Expansion Input state. If the laptop is present, the transaction gets saved as a successful laptop return, the laptop user get saved to user history, and the laptop return date gets saved. Otherwise the transaction ends as a failed laptop transaction.

For all other transactions that are not "Return Laptop" transactions for an M16 controller:

The date/time stamp when the transaction data was first created (at the time the relay was fired in the Control Grant event) is compared to the current date/time from the PC clock. If the interval in seconds is greater than the "Relay Timeout" value, then the transaction has timed out. The transaction ends as a failed laptop transaction.



TROUBLESHOOTING





Electronics Bay

The electronics Bay has four LED status indicators. In addition, each drawer has a single LED indicator.

Name	Normal	<u>Fault</u>
MAIN RELAY	Green	Off
SIDE RELAY	Green	Off
FAN FAIL	Off	RED
PWR ON	Green	Off

MAIN RELAY – Normally ON (Green).

Turns off 2 minutes after a fan failure in the 10-drawer cabinet to prevent overheating.

SIDE RELAY – Normally ON (Green).

Turns off 2 minutes after a fan failure in the 6-drawer cabinet to prevent overheating.

FAN FAIL – Normally OFF.

Turns RED when any of the cooling fans slows down or stops. This can be caused by an obstruction in the blades, motor or bearing failure, etc.

PWR ON – Normally ON (Green). Indicates that the Hirsch Interface board has power and is operating normally.

Drawers

Each drawer has an LED indicator next to it. This can be Red, Amber, or Green.

<u>Colors</u>	Function
Flash Red / Green	Power-on Self Test
Steady Green	Locked and full
Flash Green	Unlocked for checkout
Flash Red	Unlocked for checkin
Steady Red	Locked and empty
Amber	Open
Flash Red / Green / Amber	Fault

Flash Red / Green

Can last up to 2 minutes after power-on.

Flash Red / Amber / Green – Fault condition.

This pattern indicates that the Drawer Module has lost communication with the system controller for at least 5 minutes.

<CD-drive>:\Velocity\Unsupported\snib2config.exe

Replacement Part Numbers

<u>All Cabinets</u> Fan Filter Media Fan Assembly Emitter Assembly Drawer Swivel Caster with Lock Swivel Caster	 015-2364-000-0P 163-0071-000-0C 163-0255-000-0C 163-0041-000-0C 015-2063-000-0P 015-2065-000-0P 	
<u>Gen-2</u> Cabinet p/n: 510-1230-F50-00 Rev 0 510-1230-F50-00 Rev A 510-1233-F00-00 Rev 0 510-1233-F00-00 Rev A	Electronics Bay: 163-0008-000-0C Rev 0	Drawer Module: 163-0044-000-0C Rev. C
Gen-2.5 Cabinet p/n: 510-1230-F50-00 Rev B 510-1230-F50-00 Rev C 510-1233-F00-00 Rev C 510-1233-F00-00 Rev C 563-0111-F00-00 Rev 0 563-0104-F00-00 Rev 0 563-0104-F00-00 Rev 0 563-0104-F20-00 Rev 0 563-0104-F20-00 Rev A 563-0104-F21-00 Rev A 563-0104-F21-00 Rev A 563-0104-F22-00 Rev A 563-0104-F22-00 Rev A 563-5001-F00-00 Rev A 563-5001-F00-00 Rev A 563-5001-F20-00 Rev A 563-5001-F20-00 Rev A 563-5001-F20-00 Rev A	Electronics Bay: 163-0008-000-0C Rev B	Drawer Module: 163-0044-000-0C Rev. G
<u>Special</u> Cabinet p/n: 563-0104-F23-00 Rev 0 563-0104-F23-00 Rev A 563-5001-F00-01 Rev 0 563-5001-F00-01 Rev A	Electronics Bay: 163-0082-000-0C Rev 0	Drawer Module: 163-0044-000-0C Rev. G






AIR FILTERS

As with any air-cooled system, the air filters must be serviced or replaced periodically. Air filters are located on the cabinet rear wall. Clean the filter medium by running warm water through it in the reverse direction of the airflow. Recommended time between cleanings and/or replacement is a maximum of 90 days. Note: the filter medium must be dry before replacement. Spare filter media is included with each cabinet.

Tools: 1 Medium size flat blade screwdriver



Loosen thumbscrews (might require screw driver to start)



Hinge down



Remove filter material and replace with a clean piece



Hinge up Tighten thumbscrews

FANS

The 16-drawer cabinet has two fans in the 10-drawer side and one fan in the 6-drawer side. Fans are on the rear side of the cabinet (Figure x).

TOOLS: #2 Phillips screwdriver Medium flat-blade screwdriver Small wire cutters

Remove power



Loosen thumbscrews



Hinge down



Remove two flat-head Phillips screws securing filter frame to cabinet



Slide filter frame upwards and pull out to remove



Remove four Phillips screws holding fan panel to cabinet



Pull out panel and fan, cut wire tie



Disconnect fan wire harness and remove fan panel assembly

Connect replacement fan

Secure connector to finger guard with wire tie

Secure fan panel with four Phillips screws

Replace filter frame by inserting hooks into slots, then sliding the frame downward

Secure filter frame to cabinet with two flat-head screws

Hinge up

Tighten thumbscrews

DRAWER

TOOLS: Drawer Key

#2 Phillips screwdriver

Remove power



Use key to open drawer, extend completely



Remove computer and network cable Remove and save four screws (and washers) on rear wall



Press locks on chassis slides Remove drawer



Install drawer on slides

Hold wiring arm against rear panel using finger holes *Caution AC power present*



Insert four screws with washers Push drawer all the way in Open with key and install contents

DRAWER MODULE

TOOLS: #2 Phillips screwdriver Medium flat-blade screwdriver Small wire cutters

Hot swap



See proceeding Drawer Removal instructions



Hook wiring arm on holder on left inside wall of the cabinet



Loosen drawer module retaining screw (#1 Phillips bit)



Push module rearwards



Pull module out



Remove three connectors



Note DIP switch settings

Set DIP switches on replacement module



Connect two data cables and one sensor emitter cable



Install module so it sits flat against the right side wall

Pull Module forward until it is up against the cabinet front rail

Tighten retaining screw; be careful not to over-tighten or strip the head

Unhook the wiring arm from the left sidewall and pull it all the way out

Install drawer (see above)

DRAWER EMITTER

Each drawer has an infrared light emitter on the left sidewall. This is part of the sensor system that detects the laptop or other asset inside the drawer.

TOOLS: Drawer Key #2 Phillips screwdriver

Remove drawer (see above)





Park the wiring arm on the left sidewall behind the emitter assembly





Remove the retaining screw Push the emitter assembly rearward

Slide the emitter assembly rearward until the front face contacts the strengthening bend in the cabinet sidewall, then upward to remove. Note that the right face of the assembly is behind a tab in the left side sheet metal. The assembly is held in place by a spring tab and hook on bracket.





Remove the wire harness connector. The connector-locking tab can be depressed through the large round hole in the bracket.

- 5 Attach the wire harness to the new assembly.
- ⁶ Place the assembly against the left side of the cabinet and slide it downward behind the short tab. Then slide it forward so the spring tab on the assembly engages the vertical tab on the cabinet.
- 7 Replace the screw and tighten it to hold the assembly in the forward position. Do not over tighten.

ELECTRONICS BAY

The Electronics Bay contains the system power supply and most of the control electronics. Items in the Electronics Bay are not replaceable individually. Everything is mounted on a single shelf that is replaced as a whole.

TOOLS: Drawer Key #2 Phillips screwdriver Small wire cutters

Remove power from cabinet



Remove four screws from rear (#2 Phillips bit)







Remove four screws from front (#2 Phillips bit)



Open drawer #1 with the drawer key Pull down on locking pin



Pull Electronics Bay out about 4"



Remove six connectors from left side of Hirsch Interface Board



Remove one LAN cable from right side of top board



Remove two data cables from right side of Interface Board







Remove AC line cord from power supply





Cut wire ties on AC line cord

Cut wire ties on LAN and data cables



Cut wire ties on left side wire harnesses



Remove shelf from front of cabinet



To reinstall, reverse these steps, replacing all cut wire ties.

ELECTRONIC ASSEMBLIES

The Electronics Bay has four assemblies that can be replaced in the field: the Keypad (PAC Terminal), the SNIB2 (network interface card, or NIC), the Interface Board, and the system power supply. Also, there is an audible alarm that can be disconnected if desired. For the keypad, the two circuit boards, and the alarm, the Electronics Bay does *not* have to be removed completely from the cabinet. To replace the system power supply, the Electronics Bay must be completely removed.

Note: All components in the Electronics Bay are sensitive to ESD. A grounding strap must be worn at all times. The strap can be clipped to any unpainted metal structure within the Bay.

Audible Alarm

TOOLS: Drawer Key #1 and #2 Phillips screwdriver Small wire cutters, wire ties

Remove power from cabinet.

Open the Electronics Bay as described above.





The Interface Board is the lower board on the stack. Locate the Alarm Input connector on the right side of the board. Press the small tab to release it and pull the connector out of the socket. Use a wire tie to secure the cable with the connector not touching the board.

Keypad

TOOLS: #1 Phillips screwdriver

Small flat blade screwdriver

The keypad is attached to a mounting plate with two hooks along the top edge and a recessed setscrew in the center of the curved bottom side.



The keypad has a data connector and a power connector.





Remove the data connector by gently prying out one side part way and then rocking the connector back and forth.



Remove the power connector the same way.





Remove the setscrew from the bottom of the keypad with a #1 Phillips bit.



Pull out the bottom of the keypad part way, then lift it up off of the mounting plate.

To install a replacement, reverse these steps.

SNIB2

Inside the front panel of the electronics Bay is a two-board stack. The SNIB2 network card is the upper board.

TOOLS: #1 Phillips screwdriver Small wire cutters Wire ties

Unplug the network cable from the right side connector.



Unplug the small connector in the wire harness to the COMM/RESET switch.





Cut all wire ties between the SNIB2 and the connector.



Unplug the 50-pin ribbon cable by pressing outward on the two ejector tabs.







Remove 4 Phillips screws and all washers. Remove the SNIB2 board. To install the replacement board, reverse these steps, replacing all cut wire ties.

Interface Board

To remove the Interface Board, the SNIB2 must be moved out of the way but it does not have to be removed completely. The ribbon cable does not need to be removed. After removing the four screws, the board can be folded over toward the rear of the Bay with the ribbon cable acting as a hinge.

TOOLS: #2 Phillips screwdriver

¹⁄4" Nut Driver Small wire cutters Wire ties



Remove 4 Phillips screws and all washers.





Lift up the SNIB2 board and flip it over toward the rear of the cabinet, using the ribbon cable as a hinge.

Remove two datacomm cables (RJ-re connectors) from the right side.



Remove the alarm input cable from the right side.



Remove the six cables along the left side.



Remove the 12V power connector from the rear side, to the right of the ribbon cable connector.



Unplug the 50-pin ribbon cable by pressing outward on the two ejector tabs.





Remove 4 hex male-female spacers. Remove the Interface Board. To install the replacement board, reverse these steps.

Power Supply

TOOLS: #2 Phillips screwdriver 5/16" Nut Driver Small wire cutters Wire ties

Follow the previous instructions to remove the Electronics Bay from the cabinet.



If the AC line cord is held in place by a bracket, loosen two nuts and slide the retaining bracket out of the way.

Unplug the AC line cord from the front of the supply.





On the rear of the supply, remove the six screws and all of the wiring. Note where each wire is installed. Each wire *must* be reinstalled exactly as removed. Use tape to mark the black wires so they can be reconnected correctly.









Remove 4 screws from the bottom of the supply. Remove the power supply from the Electronics Bay. To install the replacement board, reverse these steps.