CHAPTER 1 - INTRODUCTION

CHAPTER OVERVIEW

This chapter provides an introduction to the V-Station 4G and V-Flex 4G devices, their specifications and features, and safety guidelines that should be observed when using or handling the devices.

1.1 INTRODUCTION

This manual provides step-by-step procedures for installing a L-1 Identity Solutions V-Station 4G or V-Flex 4G device.It covers the entire process of physically installing the device, making the necessary power, ground, and network connections, and registering the device in SecureAdmin.Instructions for field repairs and cleaning are also provided.

1.1.1 SYMBOLS USED IN THIS GUIDE

The symbols shown below are used throughout this manual.They denote special issues the user might encounter. Their definitions are given below.

DANGER

This symbol denotes a danger condition that may cause death or excessive damage to property.

WARNING

This symbol denotes a warning condition that may cause severe injury or major damage to property.

CAUTION

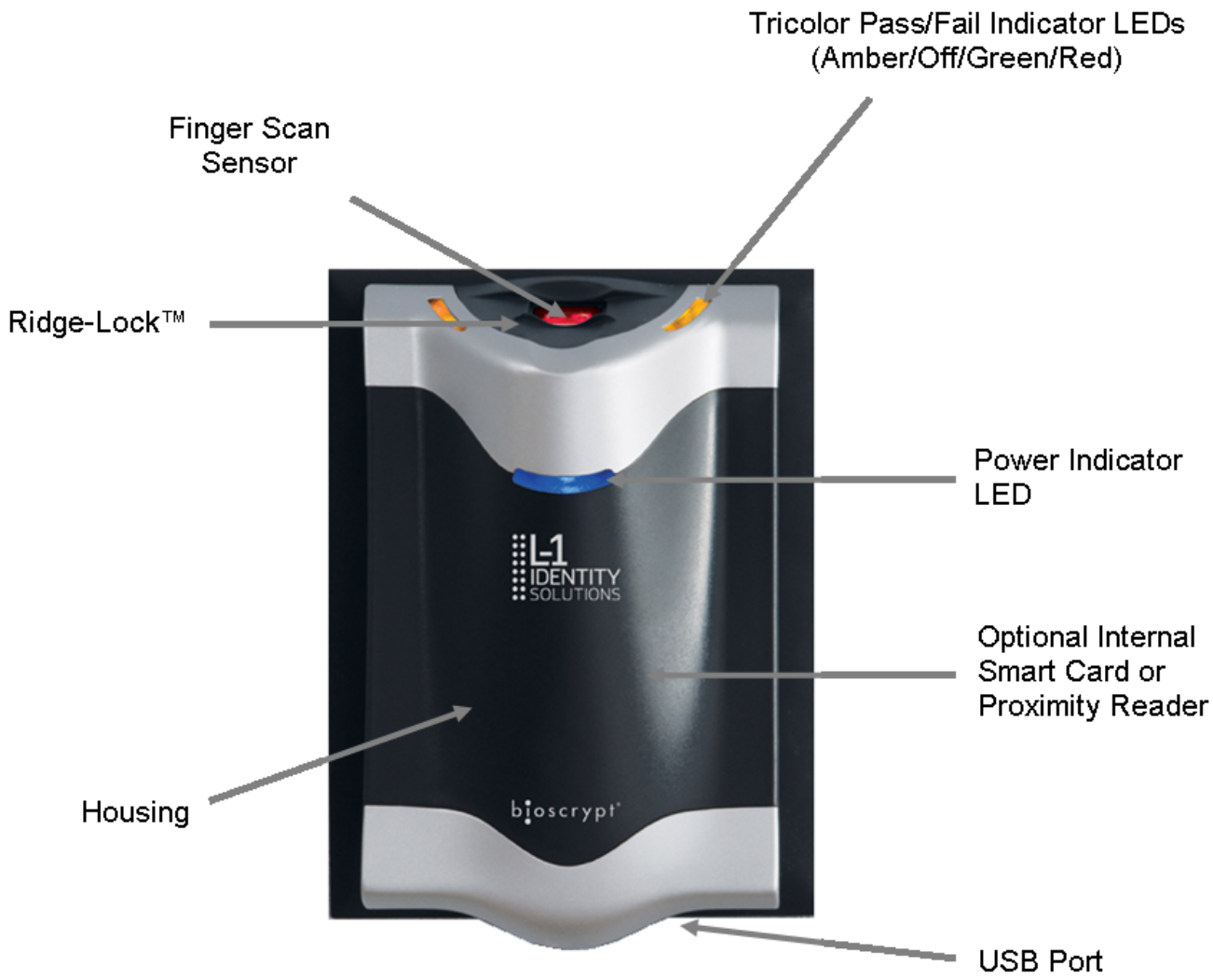
This symbol denotes a cautionary condition that may cause injury or minor damage to property.

	NOTICE
	This symbol denotes a situation needing additional advice to avoid incorrect usage.

1.2 PRODUCT OVERVIEW

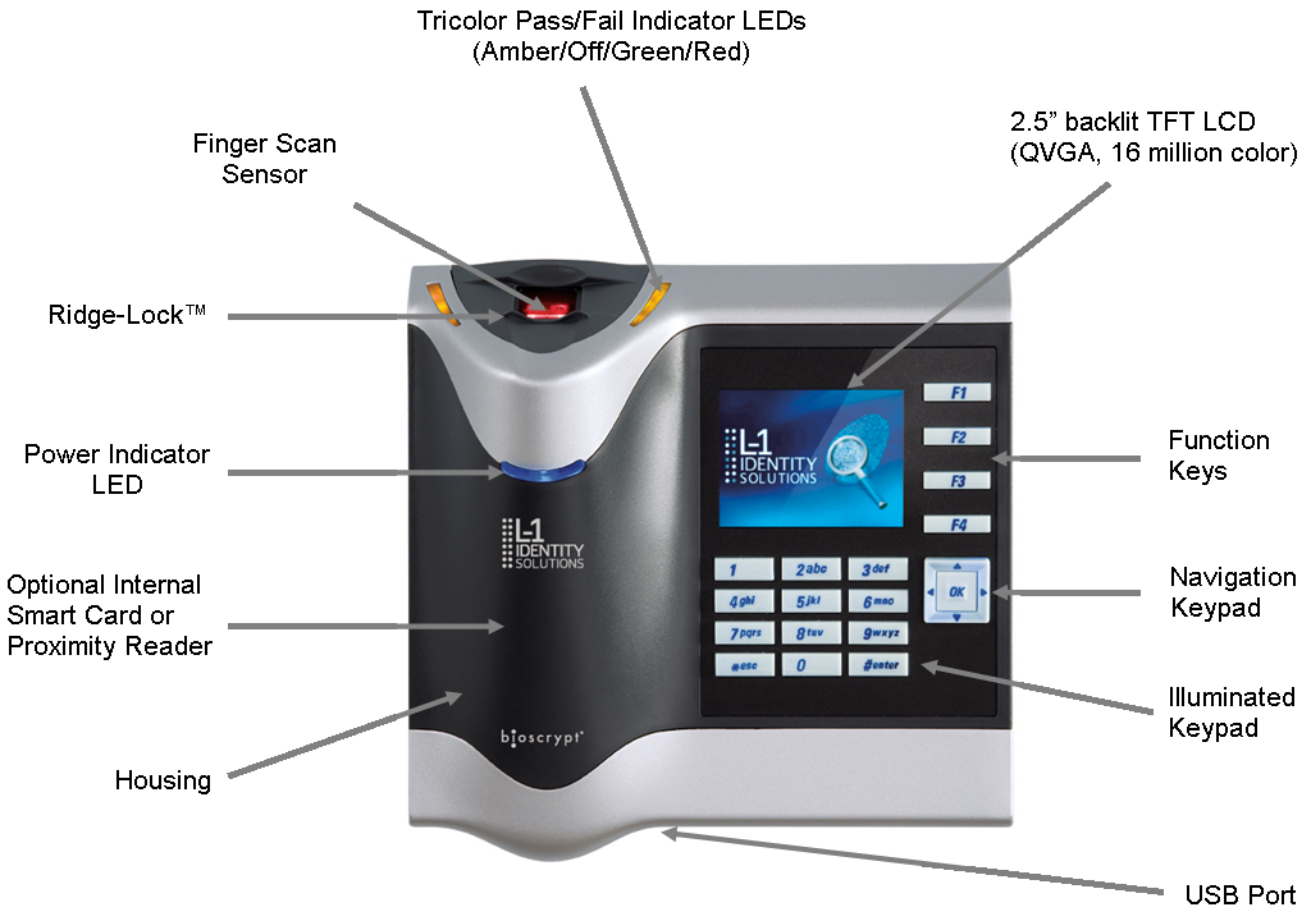
1.2.1 V-FLEX 4G

Figure 1-1 4G Flex Device



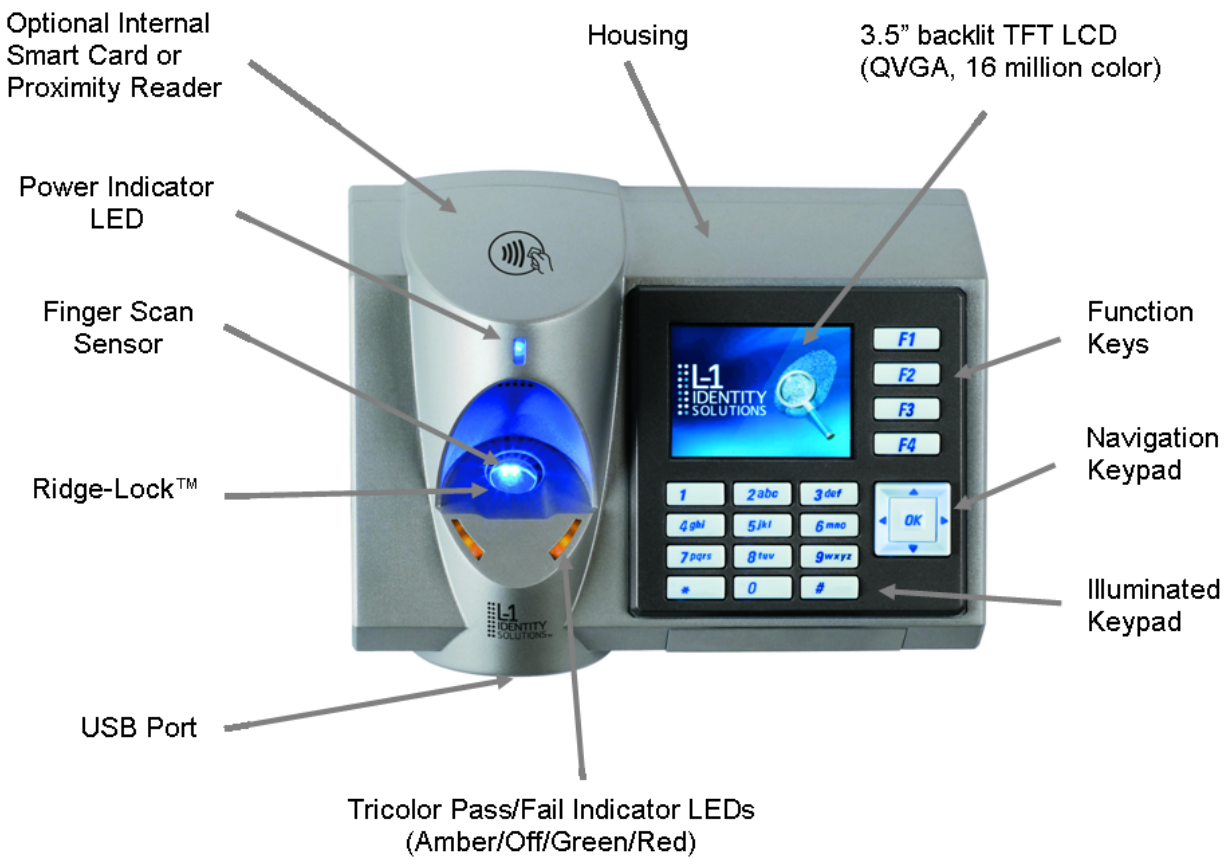
1.2.2 V-STATION 4G

Figure 1-2 V-Station 4G Device



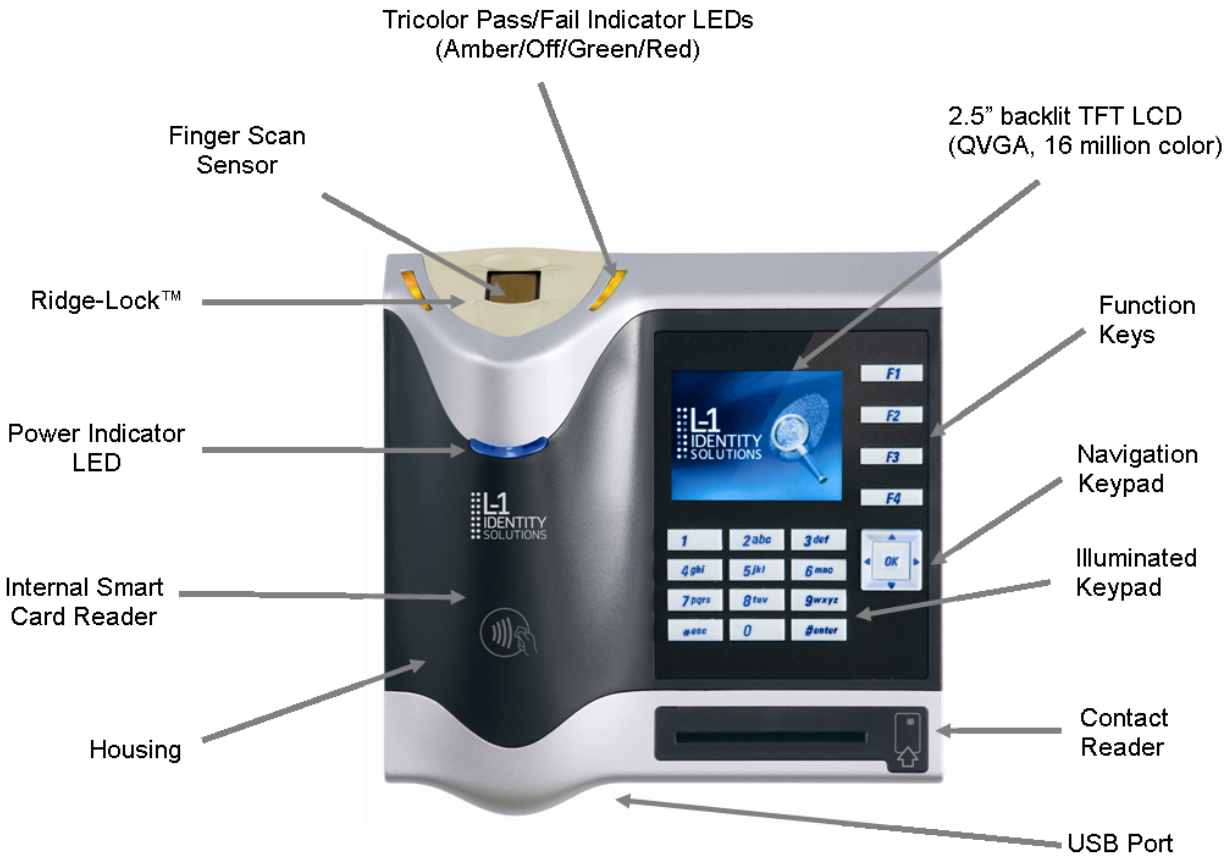
1.2.3 V-STATION 4G EXTREME DEVICE

Figure 1-3 V-Station EXTREME Device



1.2.4 V-STATION 4G PIV/TWIC INDOOR

Figure 1-4 V-Station 4G PIV/TWIC Indoor



1.2.5 V-STATION 4G EXTREME PIV/TWIC

Figure 1-5 V-Station 4G Extreme PIV/TWIC

1.2.6 SENSORS

The V-Station 4G and V-Flex 4G devices offer three types of sensor interfaces.

1.2.6.1 UPEK TCS

Figure 1-6 UPEK TCS Sensor

Key Features:

- Active Capacitive Fingerprint sensing
- 256 x 360 Sensor Array 508 DPI
- +/- 15kV Air ESD Resistance

1.2.6.2 SECUGEN OPTICAL

Figure 1-7 Secugen Optical Sensor

Key Features:

- Optical Fingerprint sensing
- 256 x 336 Sensor Array 500 DPI
- +/- 15kV Air ESD Resistance

1.2.6.3 LUMIDIGM VENUS OPTICAL SENSOR

Figure 1-8 Lumidigm Venus Optical Sensor

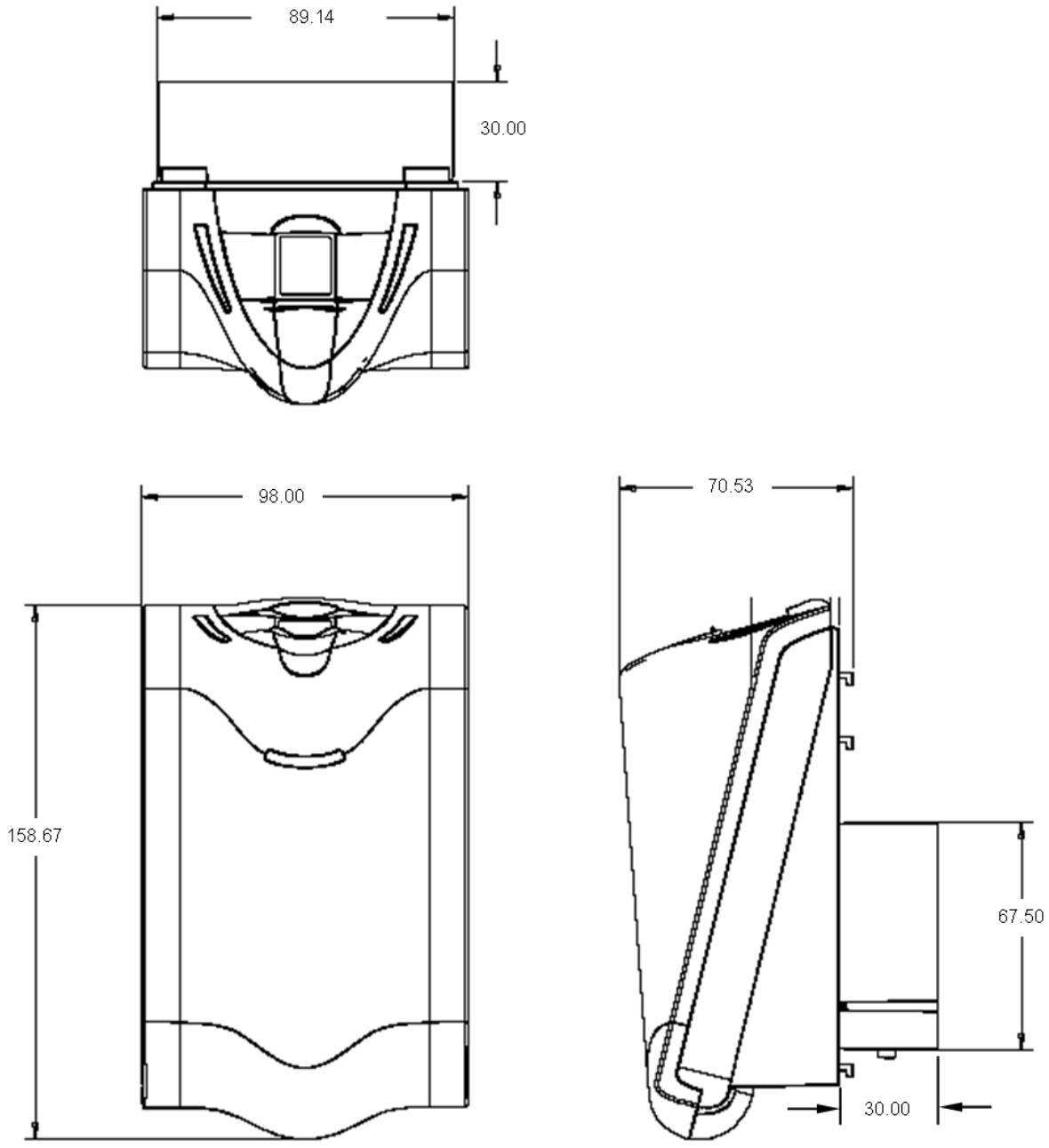
Key Features:

- TBD
- TBD
- TBD

1.2.7 DEVICE DIMENSIONS

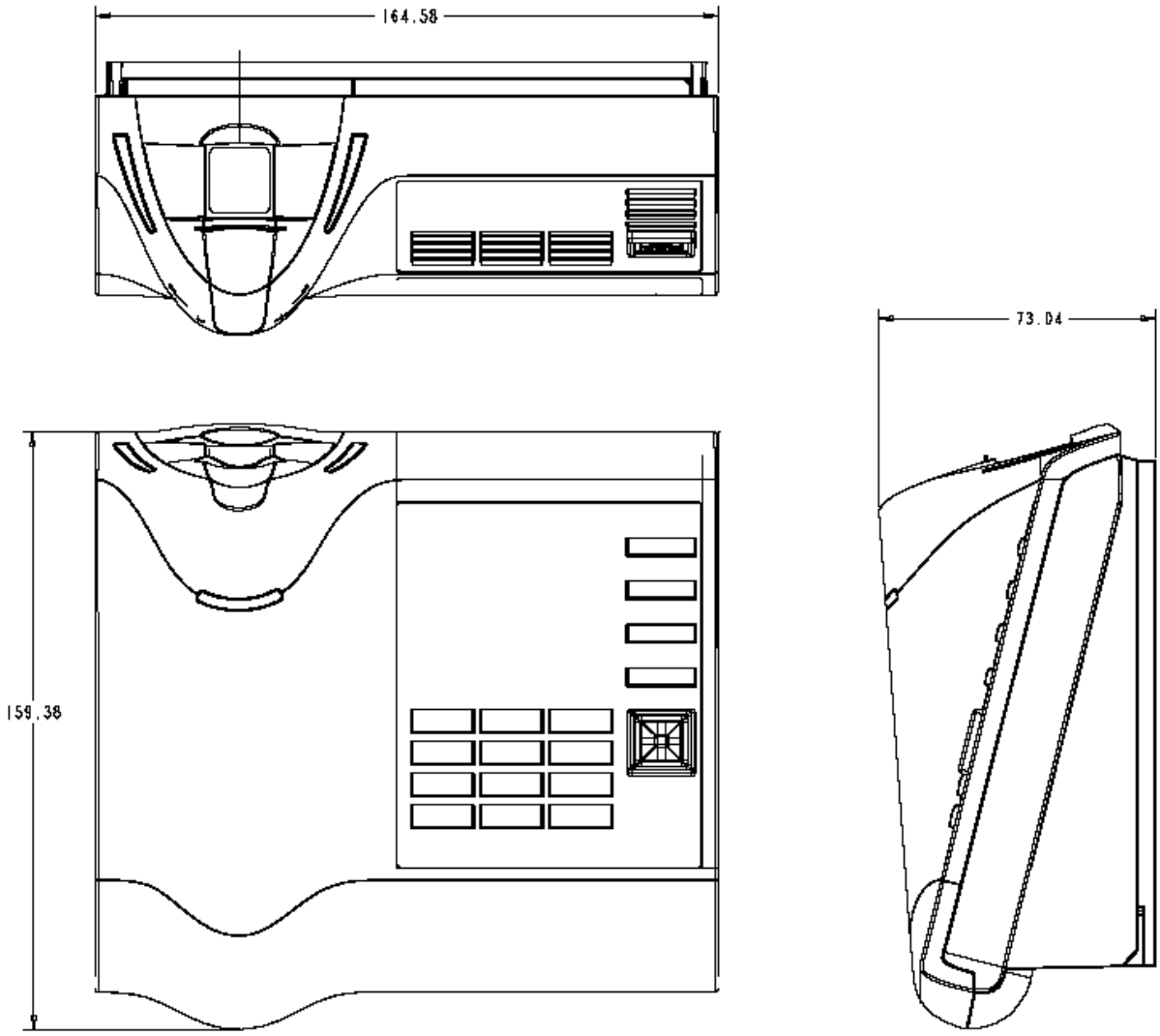
1.2.7.1 V-Flex 4G Device

Figure 1-9 V-Flex 4G Dimensions



1.2.7.2 V-STATION 4G

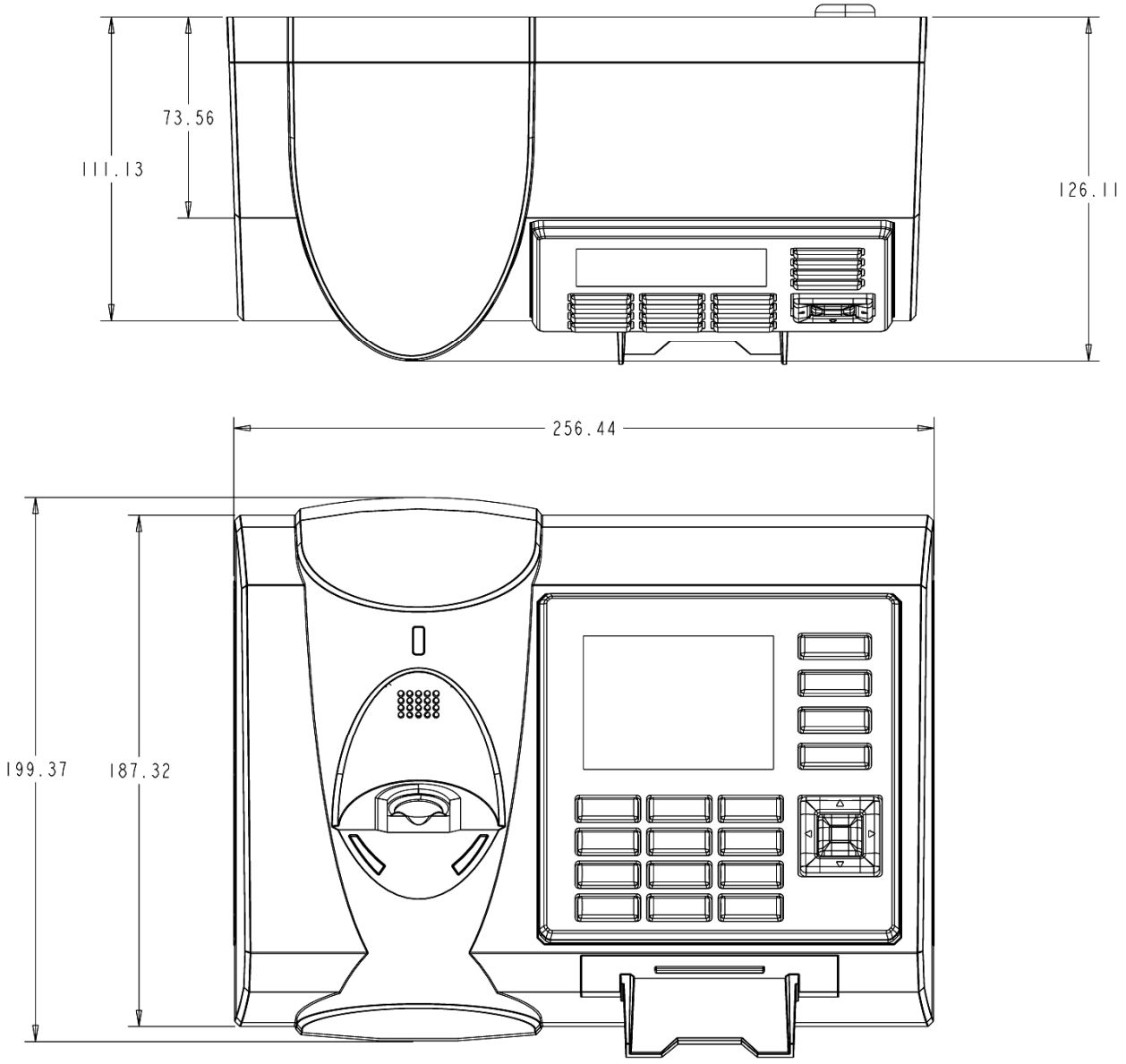
Figure 1-10 V-Station 4G Dimensions



1.2.7.3 V-STATION EXTREME PIV/TWIC DEVICES

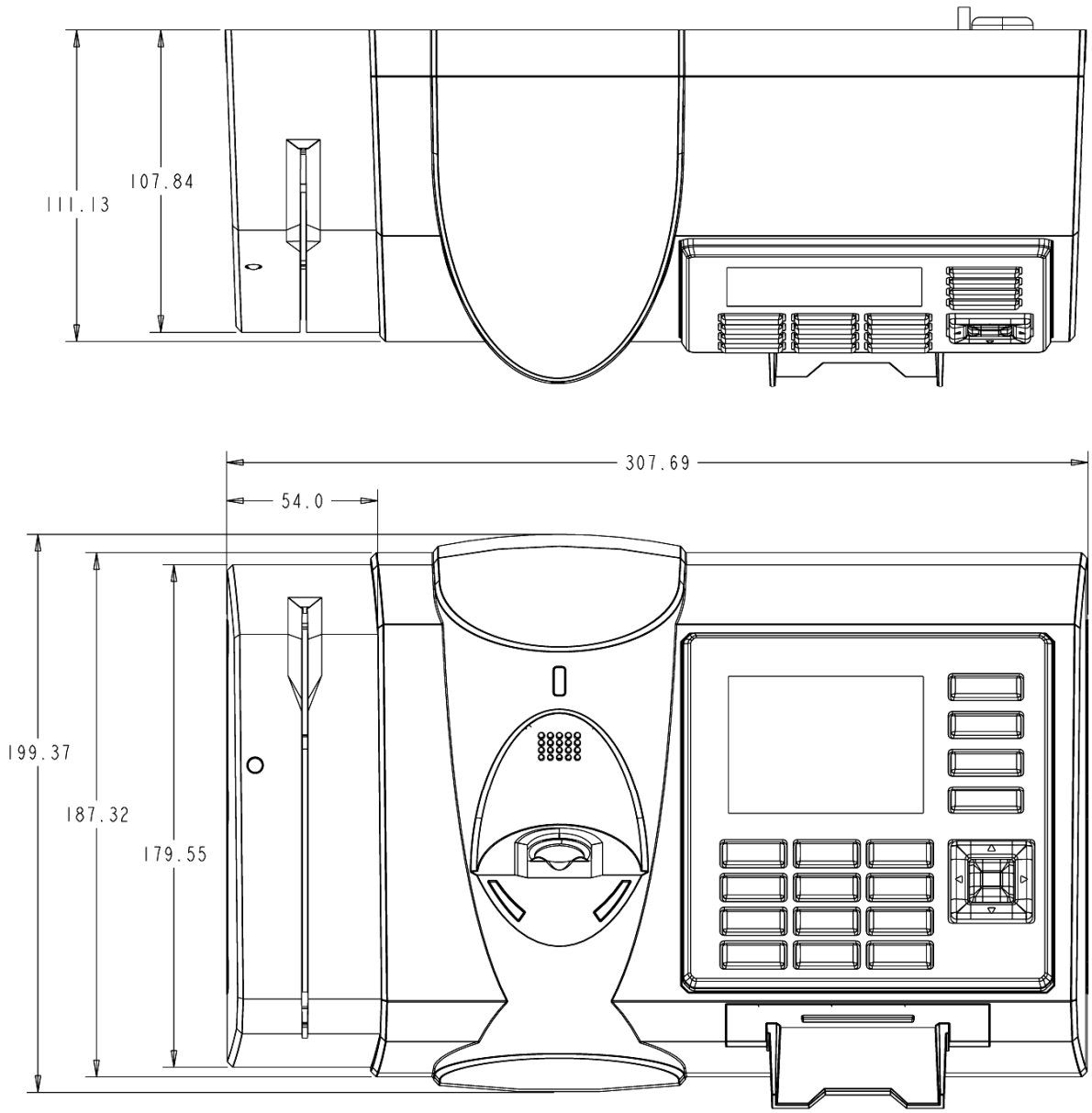
1.2.7.3.1 V-STATION 4G EXTREME

Figure 1-11 V-Station 4G Extreme Dimensions



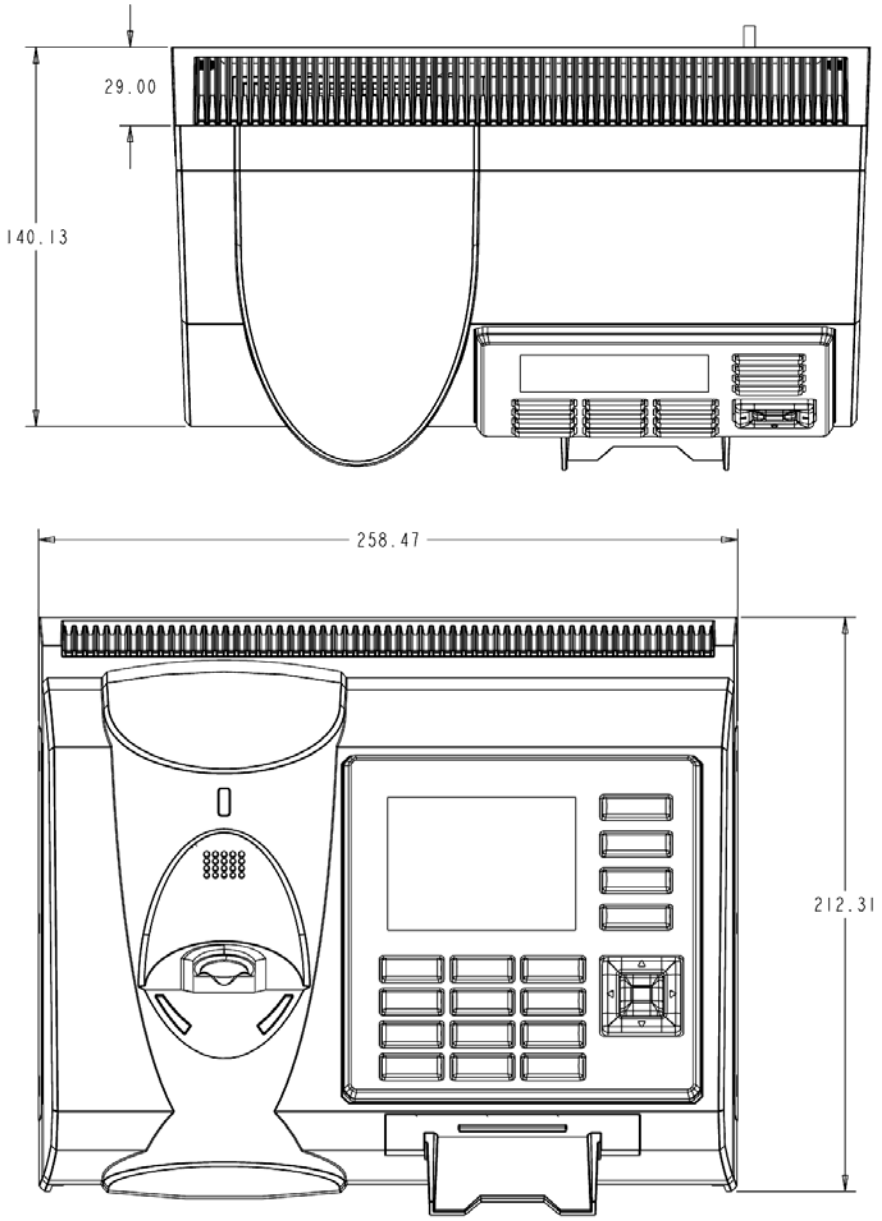
1.2.7.3.2 V-STATION 4G EXTREME WITH ACCESSORIES

Figure 1-12 V-Station 4G Extreme with Accessories Dimensions



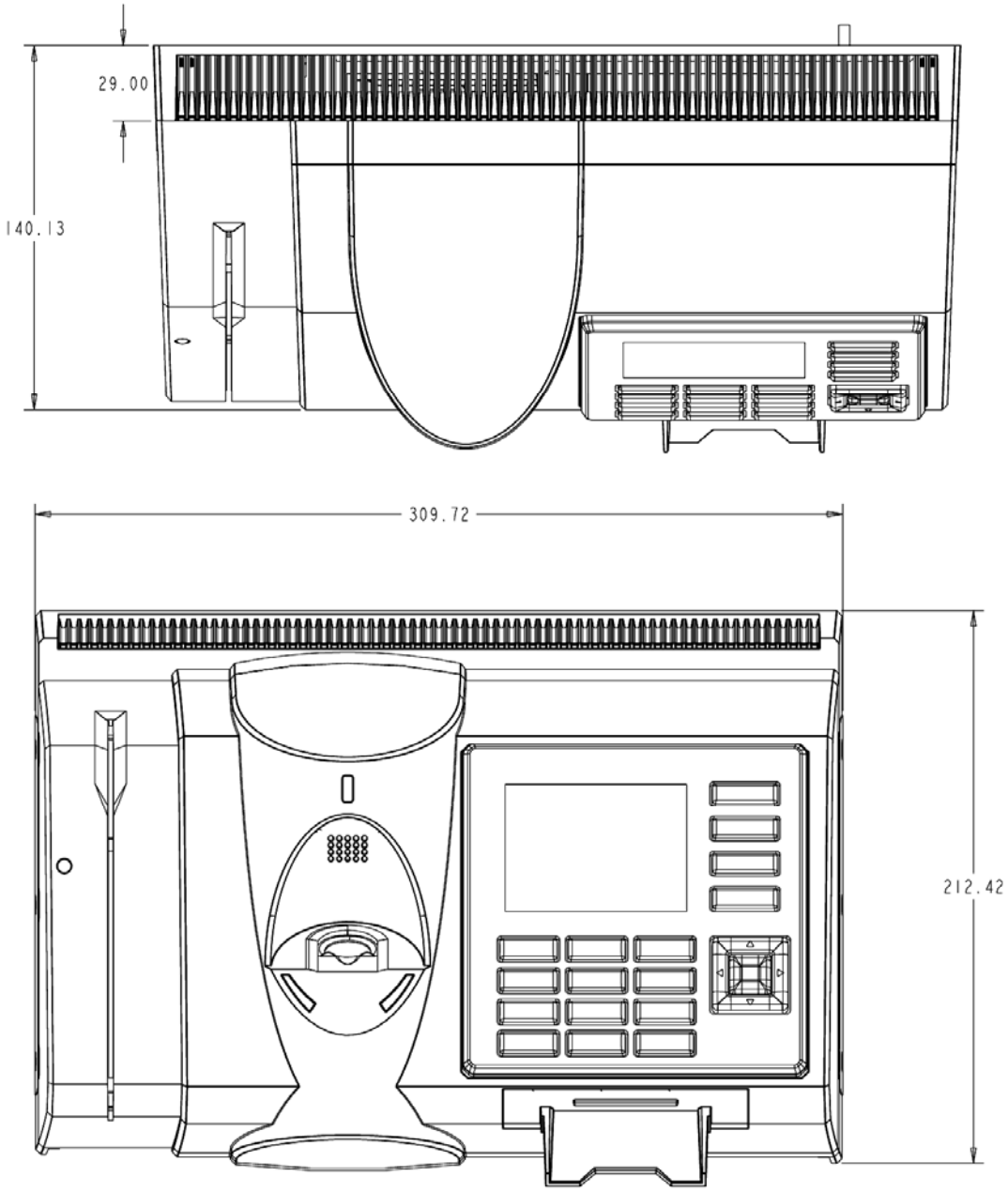
1.2.7.3.3 V-STATION 4G EXTREME PIV/TWIC

Figure 1-13 V-Station 4G Extreme PIV/TWIC



1.2.7.3.4 V-STATION EXTREME PIV/TWIC WITH ACCESSORIES

Figure 1-14 V-Station 4G Extreme PIV/TWIC with Accessories Dimensions



1.2.8 SAFETY PRECAUTIONS

Below are safety precautions that should be observed when operating or installing a device.

1.2.8.1 ELECTRO-STATIC DISCHARGE

L-1 Identity Solutions recommends that Administrators inform Users of these points during the enrollment process:

- ✓ Always use the Ridge-Lock to position a finger *before* touching the sensor.
- ✓ Always stand on the ESD-dissipative floor covering (if installed).
- ✓ Do not touch other people or objects when touching the sensor.
- ✓ Always maintain at least 12 inches of space around yourself when touching the sensor.
- ✓ Do not allow articles of clothing to touch the sensor.

L-1 Identity Solutions recommends that Installers always follow these points (in addition to the points listed above):

- ✓ When installing or working on a unit, always use a grounding wrist-strap that is connected to a quality Earth ground.
- ✓ Check the device's cabling for ground faults.
- ✓ Ensure that the device's ground connection (located on the rear of the device) is connected to a quality Earth Ground.

1.2.8.2 DEVICE HANDLING GUIDELINES

- ✓ Do not install the device in locations where the device would be exposed to direct sunlight, high levels of relative humidity, particulate matter, or flammable vapors.
- ✓ Do not install the device near radiators or other heat sources.
- ✓ Do not allow magnetic objects to come within close proximity to the device.
- ✓ Strong magnetic fields might damage the device.
- ✓ Do not let liquids Card the device.
- ✓ Do not attempt to alter the device for any reason.Modifications will void the product guarantee.
- ✓ Do not attempt to disassemble the device in any way beyond what is necessary for sensor field replacement.
- ✓ Do not use the device for any purpose other than for what it was designed.

- ✓ Do not plug any equipment into the USB port other than flash memory devices.
- ✓ Do not allow users to place or hang objects on the device, such as coffee cups or purses.
- ✓ Do clean the device regularly to remove dust, grime, and fingerprint residue.

CHAPTER 2 - PLANNING THE INSTALLATION

CHAPTER OVERVIEW

This chapter details how to plan a successful installation, recommended steps, and explains the hardware and software components of typical setup scenarios.

2.1 PLANNING THE INSTALLATION

Planning the installation is the single most important aspect of a successful installation. In general, you need to consider the access controller, the door locks, the devices, and the need for a network. By the time you are ready to install the system, all of the details presented in the list below should be known. Take a moment to go through them now before starting your installation.

During the planning phase, you should determine:

- ✓ What type of authentication is required for your application?
- ✓ How many doors need to be secured?
- ✓ What type of device will be on each door? Doors already inside a secure area might not need the same type or level of security.
- ✓ If multiple V-Series 4G devices require networking for template distribution/management, then a dedicated PC is recommended to administer the system, as well as an RS-485 to RS-232 converter, and cabling for serial communications or cabling for Ethernet.
- ✓ Verify that the chosen access controller supports the Wiegand formats supported by V-Station 4G devices.
- ✓ Identify all wiring by the signal levels it is to carry. Use separate cables and conduits for different signal groups to avoid cross talk. Plan to separate them by these groups:

Power distribution: Wires carry power to devices, door strikes, etc.

Data communication: RS-485, RS-232, USB, Wiegand, Ethernet, etc.

Signal: Door contact, request-to-exit push button, alarm input, etc.

- ✓ When planning device placement, determine the distance limitation of each signal type and use repeaters if necessary.

- ✓ V-Series 4G devices are intended for indoor use only.

If you have any unresolved issues with the items on this list, contact L-1 Identity Solutions Technical Support for additional information before beginning any installation.

WARNING

V-Station 4G and V-Flex 4G devices should be installed by only a qualified technician. If you are not qualified to perform an installation task, call L-1 Identity Solutions Technical Support or contact a qualified installer.

2.1.1 RECOMENDED STEPS FOR A SUCCESSFUL INSTALLATION

Every installation is unique. Sometimes the issues are well defined and can be handled in a standard fashion; sometimes the issues are very specific and may not be immediately recognizable.

L-1 Identity Solutions recommends following these steps for a successful installation:

- ✓ Plan the installation Choose the type of hardware required, decide if a network is required, and decide on the location and number of required devices.
- ✓ Unpack all items Unpack all items and check against the packing list.
- ✓ Install network hardware components Install the cabling and components needed to run the system.
- ✓ Install software Install the software needed to set up the devices.
- ✓ Preconfigure device Connect the device to the USB cable, supply power to the device, and preconfigure the device.
- ✓ Mount devices Mount the devices in their final locations
- ✓ Power distribution and device hook up Connect the device wiring via the back panel.
- ✓ Power-up procedure Check the power connections and start the system safely. Enroll users Enroll users into the system (for user enrollment procedures).

Chapters 3 through 7 in this document present more information on these steps.

2.1.2 REQUIREMENTS

- ✓ PC workstation with:
- ✓ 1 GHz Intel(r) Pentium(r) 4 processor or equivalent
- ✓ 1 GB RAM (2 GB recommended)
- ✓ CD-ROM drive
- ✓ One available COM port or USB port
- ✓ Ethernet card
- ✓ Display: 1024 x 768 high color (minimum)
- ✓ Regulated DC Power supply
- ✓ Door controller
- ✓ TCP/IP network environment
- ✓ RS-232 to RS-485 converter with power supply (for advanced administrative features).

2.1.2.1 HARDWARE REQUIREMENTS

- ✓ Deadbolt/door strike
- ✓ Snubber diode required to protect regulated DC power supply from inductive kickback(1 N4007 diode or equivalent recommended)
- ✓ Separate power supply for the deadbolt/door strike based on supplier's recommendations.
- ✓ External relay (if required)
- ✓ Networking cable

2.1.2.2 COMPUTER REQUIREMENTS

2.1.2.2.1 SECURE ADMIN SERVER REQUIREMENTS

- ✓ Hard disk space: 10 MB

2.1.2.2.2 SECUREADMIN CLIENT REQUIREMENTS

- ✓ Hard disk space: 25 MB http://2.2.2.3.microsoft.net/

2.1.2.2.3 MICROSOFT .NET FRAMEWORK 3.5 SP1 REQUIREMENTS

- ✓ Hard disk space: Up to 600 MB might be required

2.1.2.2.4 SUPPORTED OPERATING SYSTEMS

SecureAdmin Server and SecureAdmin Client support these operating systems:

- ✓ Windows Server 2003 R2
- ✓ Windows Server 2008
- ✓ Windows Vista
- ✓ Windows XP Service Pack 2 or higher

2.1.2.2.5 SQL SERVER 2008 EXPRESS EDITION

- ✓ Hard disk space: 350 MB of available hard-disk space for the recommended installation. Approximately 425 MB of additional available hard-disk space for SQL Server Books Online, SQL Server Mobile Books Online, and sample databases.
- ✓ During installation of SQL Server 2008, Windows Installer creates temporary files on the system drive. Before running setup to install or upgrade SQL Server, verify that at least 2.0 GB of disk space is available on the system drive for these files
- ✓ Actual Hard Disk Space Requirements: 280 MB for the recommended installation.

2.1.2.2.6 ORACLE 10G EXPRESS

- ✓ Hard disk space:
- ✓ Server component: 1.6 GB Client component: 75 MB

2.1.2.3 NETWORK REQUIREMENTS

- ✓ The V-Station 4G and V-Flex 4G devices function on 100 baseT networks.

2.1.2.4 SOFTWARE REQUIREMENTS

Both SecureAdmin Server and SecureAdmin Client require these software applications as prerequisites:

- ✓ .net Framework 3.5
- ✓ Windows Installer 4.5

If these applications are not already installed, they will get installed during the setup process.

SecureAdmin Server and SecureAdmin Client also require System Administrator access to install the application.

SecureAdmin uses a self-signed certificate (x.509 certificate) with a file extension of .pfx.

You have the option of installing your own certificate, which must be purchased from a recognized authority in advance. The SecureAdmin self-signed certificate is installed only with the SecureAdmin server component. No certificate is installed with the SecureAdmin client component, and during the client installation, you are asked to specify which type of certificate SecureAdmin server will be using (the self-signed certificate provided with the SecureAdmin server component installation or a signed certificate from another authority such as VeriSign.

2.1.3 UNPACK EQUIPMENT

Unpack all items and check against the packing list.

2.1.3.1 PARTS LIST

2.1.3.1.1 V-STATION 4G or V-FLEX 4G DEVICES

Hardware

- ✓ 1 V-Station 4G or V-Flex 4G device
- ✓ 1 Wall mounting plate/mullion mounting plate
- ✓ 6 #6-32 3/4" Philips pan-head screw
- ✓ 6 #6 1" Philips pan-head self-tapping screws
- ✓ 6 #4-8 1" nylon wall anchors
- ✓ 29 Crimp connector, B Wire (RoHS)
- ✓ 2 6-32 security screw, pin-in hex, 3/8
- ✓ 2 0.013" ID, 3/8" OD, 1/32" thick, fiber washers
- ✓ 1 Ethernet ferrite core
- ✓ 1 DC & I/O lines ferrite core
- ✓ 1 External power cable
- ✓ 1 External signal cable

- ✓ 1 Micro-USB device cable
- ✓ 1 Micro-USB PC cable

Tools

- ✓ 1 1/8" pin-in-hex security key 2.5

2.1.3.1.2 V-STATION 4G EXTREME DEVICES

Hardware

- ✓ 1 V-Station Indoor or Outdoor 4G device
- ✓ 29 Super B-Wire Connectors, Dolphin DC-100-S
- ✓ 2 dielectric grease (maybe 1 is enough, need to try out)
- ✓ 1 Cable, User Wiegand, 4G Outdoor
- ✓ 8 wall mount anchor, conical, for #8 screws
- ✓ 1 8-32x11/32"UNC K-Lot Hex nut RoHS
- ✓ 1 8-32-MALE-FEMALE-HEXSTAND-1.25L
- ✓ 1 mech, AS101001_ACTUATOR_MAGNET
- ✓ 8 #8x1" thread forming screw, pan head, philips,
- ✓ 6 6-32 Security Screw 1/8" pin-in-hex 3/8" length
- ✓ 1 Stainless Steel, Wall Mount Plate with Magnetic Reader, 4G Outdoor
- ✓ 1 Cable, MicroUSB PC, NGV
- ✓ 1 Cable, MicroUSB Device, NGV
- ✓ 1 Cable, User Comm and Ctrl, 4G Outdoor
- ✓ 1 Cable, User TTL, 4G Outdoor

2.1.3.1.3 DOCUMENTATION

- ✓ 1 Installation Guide (on Installation CD)

- ✓ 1 Operator's Manual (on Installation CD)
- ✓ 1 Quick Start Guide (on Installation CD and printed copy in package)

Documentation for your new device is installed onto your computer when you install the SecureAdmin software. The product documentation is also available online at: http://www.l1id.com/pages/450-product-manuals

The documentation is provided in Adobe Acrobat format (PDF). The Adobe Acrobat Reader application is available on the Installation CD or at: http://www.adobe.com

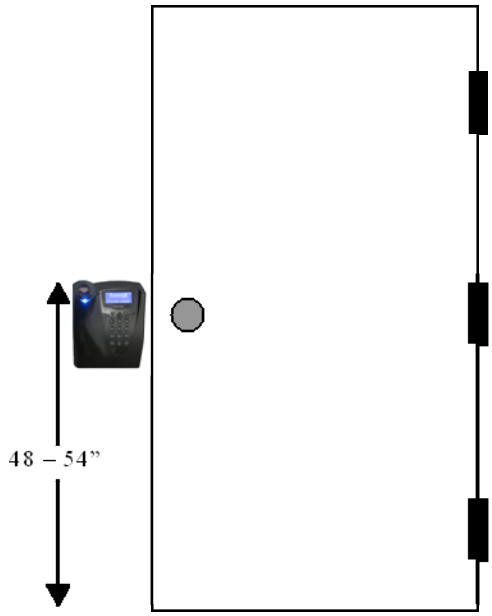
2.1.4 CHOOSING THE INSTALL LOCATION

V-Station 4G and V-Flex 4G devices are designed to mount on either a double-gang electrical box or on any flat surface. Consult with local professionals regarding any building and safety codes that might affect your installation. The correct mounting height is shown below.

Factors to consider when determining the position of a device on the wall:

- ✓ Proximity to other switch plates or fixtures (the device should ideally be mounted in-line with other plates or fixtures)
- ✓ Distance from the floor to the top of the device (L-1 Identity Solutions recommends using a height between 48 and 54 inches).
- ✓ The device should be mounted on the knob-side of the door
- ✓ Compliance with the Americans with Disabilities Act if in the United States. Information about http://www.usdoj.gov.

Figure 2-1 Correct Mounting Height



2.1.5 PLAN DEVICE NETWORK

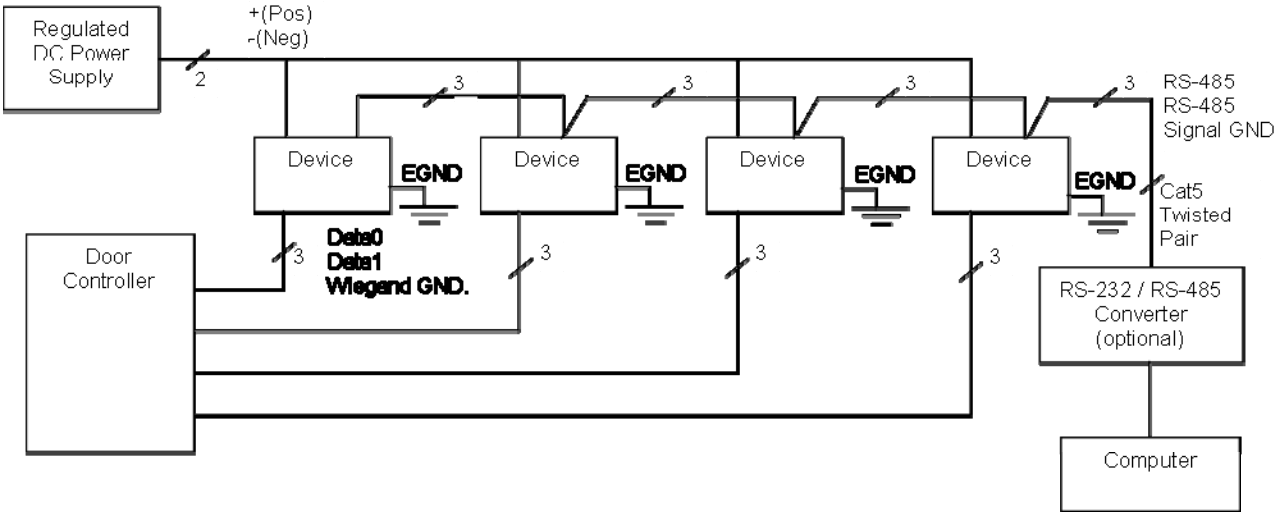
The 4G devices feature a built-in single-door relay that allows them to control a single door lock. They can therefore function on their own or as part of a larger access control system.

System component selection is specific to each installation, but a minimum system would consist of a finger-scan device mounted on or near an access point, an electric lock, and cabling.

A more complex system might consist of devices at multiple access points (each with an electric door lock), a multi-point controller, networking, and a PC to run the access controller and SecureAdmin Server software.

See the diagram below for an example (non-Ethernet) system diagram.

Figure 2-2 Example RS-485 System Diagram



Installation of locks and access controllers should be completed according to their respective manufacturers' specifications and in accordance with all local codes. Final connections to the device are explained in more detail in Chapter 4.

To avoid externally generated transients, do not run any wires near utility AC power wiring, lightning rod grounding wire, etc. Grounding equipment is required for ESD protection and safety.

2.1.6 CHOOSE NETWORK TYPE

If your installation requires the use of network communications, then the choice of cable, the cable run length, the network topology, and the termination of the network are important aspects that must be considered. The V-Station 4G and V-Flex 4G devices can be networked using RS-232, RS-485, or Ethernet protocols.

The table below outlines relevant parameters of the RS-485, RS-232, and 100 baseT Ethernet communication protocols.

Table 2-1 Communications Network Comparison

Spec	**RS-485**	**RS-232**	**100BaseT**
Mode of Operation	Differential DC Coupled	Single-ended DC Coupled	Multi
DC Isolation	No	No	No
Maximum Distance	4000 feet	150 feet	330 feet

Spec	RS-485	RS-232	100BaseT
Number of Devices on one line	31	1	Unlimited
Maximum Data Rate	56 Kbps (recommended)	56 Kbps* (recommended)	Auto-negotiated

2.1.6.1 RS-232

If your system has only one device, or a few devices (each only a short distance away from the SecureAdmin PC) then RS-232 can be used, provided that each device can have a dedicated RS-232 port.

With RS-232 at 9600 baud, a distance of 150 feet is possible with shielded cable, but at 56 Kbps, a maximum of only 20 feet is recommended.

2.1.6.2 RS-485

RS-485 has two distinct advantages over the more common RS-232. First, it allows you to connect up to 31 4G devices to a PC with an external RS-232 to RS-485 converter (available from L-1 Identity Solutions). Second, the RS-485 specification allows for cable

run lengths up to 4000 feet (1200 meters) at modest baud rates.

An RS-485 network is required instead of RS-232 if:

- ✓ Multiple devices must be connected together so that templates can be distributed among the devices
- ✓ The installation has only a single device, but it is over 150 feet (45 meters) from the host PC.

2.1.6.2.1 RS-485 CABLE SPECIFICATION

V-Station 4G devices provide a 2-wire, half-duplex RS-485 interface. The main cable run should be low capacitance, twisted-pair cable, with approximately 120 -ohm characteristic impedance. Category-5 rated communications cable is used in RS-485 networks and its characteristics are defined below. This is the recommended cabling for RS-485 communications. The cable connection includes a differential line (+ and -) and a GND connection.

Table 2-2 Category 5 Cable Characteristics

Specification	Recommendation
Capacitance (conductor to conductor)	<20 pF/ft.
Characteristic Impedance	100 - 120 ohms
Nominal DC resistance	<100 ohms/1000 ft.
Wire gauge	24 AWG stranded
Conductors/Shielding	>2 pair (shielding is recommended)

2.1.6.2.2 RS-485 CABLE LENGTHS

As outlined in the RS-485 specification, the total length of the communication cable (adding up all of the segments of the run) should not exceed 1200 meters (4000 feet). Although the RS-485 specification calls for a maximum cable length of 1200 meters and provides a maximum baud rate well above that of the 4G device, a more conservative system should be configured to no more than 1000 meters and run at a baud rate of 9600 bits per second. After the network is configured and is running in a stable manner, the baud rate can be increased if faster network communications are desired.

Drops (down-leads, stubs, T-connections, etc.) to equipment are not recommended, but if required, should not exceed one foot) and should use the same cable recommended above. On a long stub, a signal that travels down the wire reflects to the main line after hitting the input impedance of the device at the end. This impedance is high compared with that of the cable and the net

effect is degradation of signal quality on the bus.

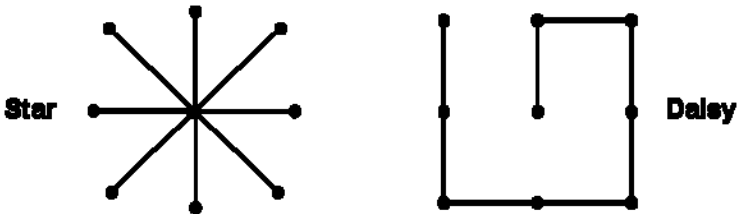
2.1.6.2.3 RS-485 NETWORK TOPOLOGY

Communication cables for RS-485 should be laid out in a daisy chain configuration (See Figure 2-3 below). Long stubs or drop downs and the star configuration should be avoided because they create discontinuities and degrade signal quality. The star configuration usually does not provide a clean signaling environment even if the cable runs are all of equal length. The star configuration also presents a termination problem, because terminating every endpoint overloads the driver. Terminating only two endpoints solves the loading problem, but creates transmission line problems at the unterminated ends. A true daisy chain configuration avoids these problems.

NOTICE

The device on the end of the network should be terminated with a 120 ohm resistor.

Figure 2-3 Network Topologies Star and Daisy Chain Configurations



NOTICE

A Daisy configuration is recommended over a Star configuration..

2.1.6.3 ETHERNET

If your system is to be configured for use over Ethernet, the wiring will be slightly different. Communication cables for Ethernet logically form a straight line bus but the more devices on that bus, the less efficient the network becomes due to increased collisions, and the weaker the signal will get over distance. Repeaters can be used to boost the signal strength; however, a better solution is to place switches at intermediate positions along the bus. The most common Ethernet topology in use today is the star configuration with a hub or switch in the center.

2.1.6.4 WIRELESSNETWORK DESIGN CONSIDERATIONS

A wireless network of V-Station 4G offers several advantages over wired networks, such as convenience, speed of installation, and less wiring. If you

are planning to design a wireless network, consider these points:

Wireless signal interference Metal masses such as HVAC ducts, fire doors, vents, stairs, etc. disrupt wireless signals. Building and stairwell structures, as well as internal building walls, also impede wireless signals. Some electrical equipment, such as

microwaves, large-screen TVs, cordless telephones are also known to affect wireless signals. Consider the proximity of devices to these objects.

Distance from access points How far a device is from the closest access point plays a major factor in determining the stability and strength of the wireless signal.

Multiple Access Points "Repeaters" or multiple access points can solve signal strength problems that may be caused by either distance or loss due to interference.

2.1.7 CHOOSE POWER SOURCE

V-Station 4G and V-Flex 4G devices can be powered by several methods:

- ✓ 1 2V DC regulated adapter/bullet jack (4G Indoor only)
- ✓ Power Over Internet (POE) through an inline PoE 802.3af power injector
- ✓ Power Over Internet (POE) through an inline PoE36U-1AT-R power injector (4G Extreme with heater only)
- ✓ 2-pin mini connector with dedicated power source (4G Indoor only)
- ✓ 3-wire cable (4G Extreme).

Power sources should be:

- ✓ Isolated from other equipment
- ✓ Filtered
- ✓ Protected by an Uninterruptible Power Supply (UPS) or battery backup
- ✓ Protected by a voltage suppression device if transient electrical surges are an issue in the location.

When planning a system, know the power requirement of each device. If multiple devices are to share a common power supply, exercise care to avoid excessive voltage loss on the wires. Voltage loss can lead to communication problems when devices are talking and/or listening on different ground references.

Voltage loss is directly proportional to wire resistance and the current the wire carries. Always place the device as close as possible to the power supply and always select a wire size appropriate for the load. V-Station 4G devices run on DC power between 12.5 and 24 VDC.

Power requirements for all V-Station 4G and V-Flex 4G models are listed below.

Table 2-3 V-Station 4G and V-Flex 4G Power Requirements

Power Requirement:	12 watts
Input Voltage Range:	12-24.0 VDC
Peak Current (12 VDC)	1 A
Peak Current (24 VDC)	500 mA

Table 2-4 V-Station 4G Extreme Power Requirements

Power Requirement	12 watts
Input Voltage Range	12-24.0 VDC @ 3 Amps
Peak Current (12 VDC)	1 A
Peak Current (24 VDC)	500 mA
Cooler Module	12 to 24VDC @ 10Amps

Most power supplies on the market today provide good input and output isolation. However, power supplies which do not provide isolation (or have high leakage capacitance), coupled with accidental AC power line interchanges, present serious ground fault problems for installers. With a ground fault, the signal reference between subsystems may be 115 VAC apart. If these subsystems are interconnected, the large potential difference can cause equipment damage or personal injury. L-1 Identity Solutions recommends using a dedicated regulated DC power supply.

All factory-supplied power supply assemblies are either switching or regulated linear supplies and are isolated for safety and to minimize ground loop problems.

CHAPTER 3 - INSTALL SOFTWARE

CHAPTER OVERVIEW

This chapter shows how to install, repair, modify, upgrade, and uninstall the SecureAdmin Server and Client software packages.

3.1 INSTALL SOFTWARE

To install the SecureAdmin software, the user must have Administrator rights. Any software required to install SecureAdmin is detected and installed automatically during the setup process.

3.1.1 SECUREADMIN SERVER

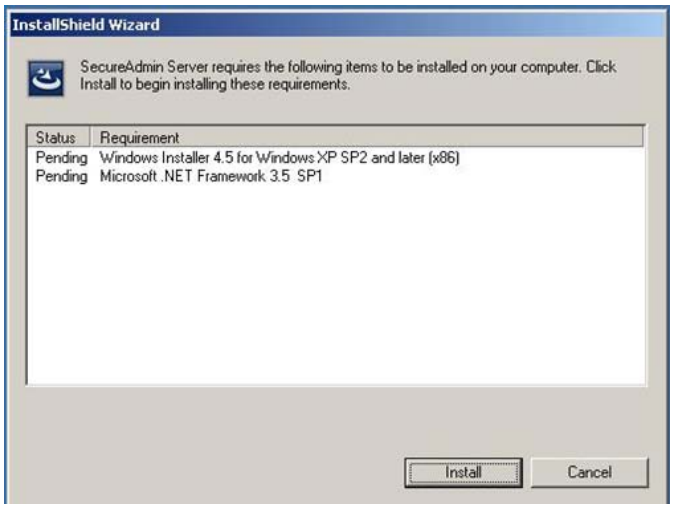
To install the SecureAdmin Server software, follow these steps:

Insert the CD into the optical drive. If Autoplay is enabled, the installation process will start automatically. A menu is displayed. If Autoplay is not enabled, start the installation process manually by doubleclicking the Setup.exe file located in the "Bioscryptsetup" folder on the root of the CD.

Figure 3-1 Install Menu

Click **Server Installation**. The **InstallShield Wizard** starts and the target system is examined for prerequisite software. Any necessary software is listed.

Figure 3-2 Prerequisites



Click **Install** . Microsoft .NET Framework 3.5 SP1 is installed. Restart the computer when asked. The installation process continues automatically after the computer is restarted. Repeat the same process for Windows Installer 4.5.

Figure 3-3 Restart Message

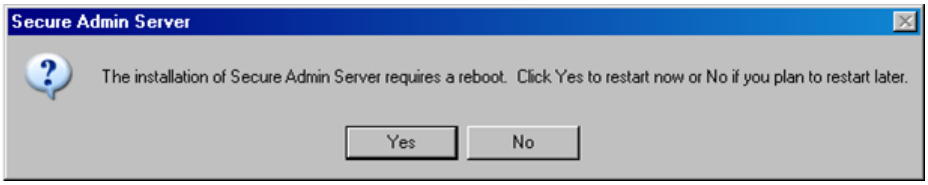
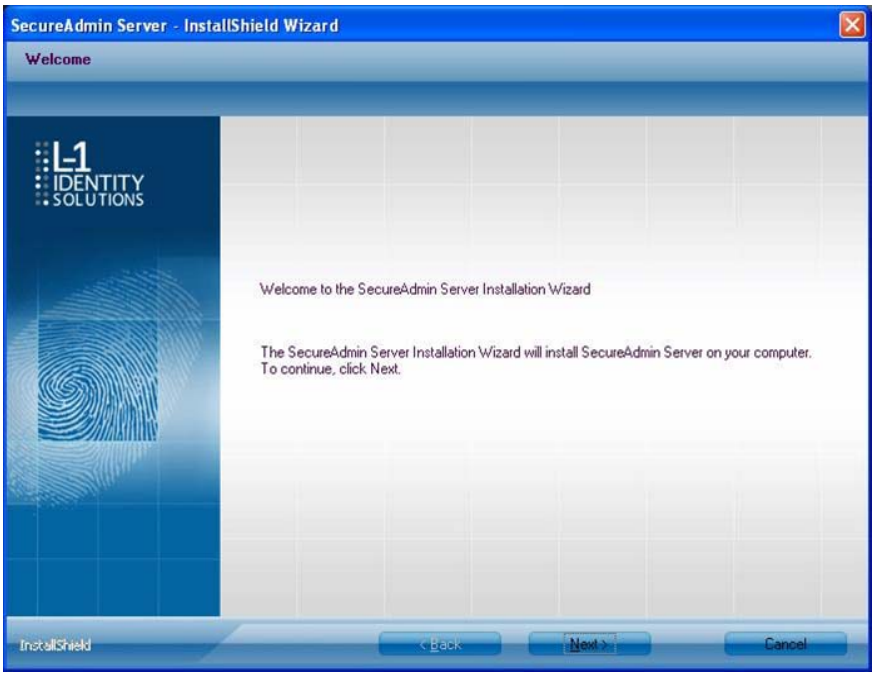
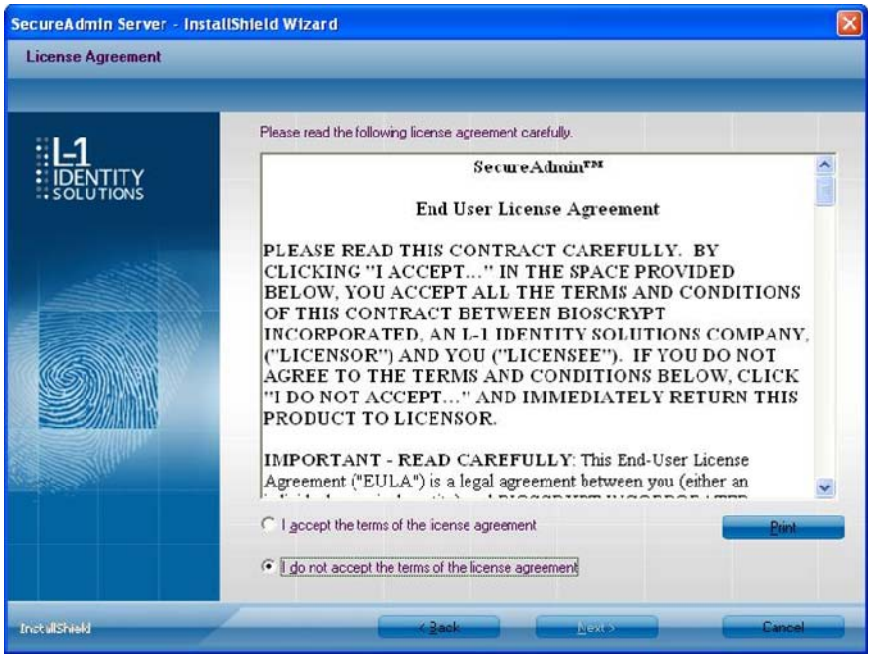


Figure 3-4 SecureAdmin Server Installation Wizard



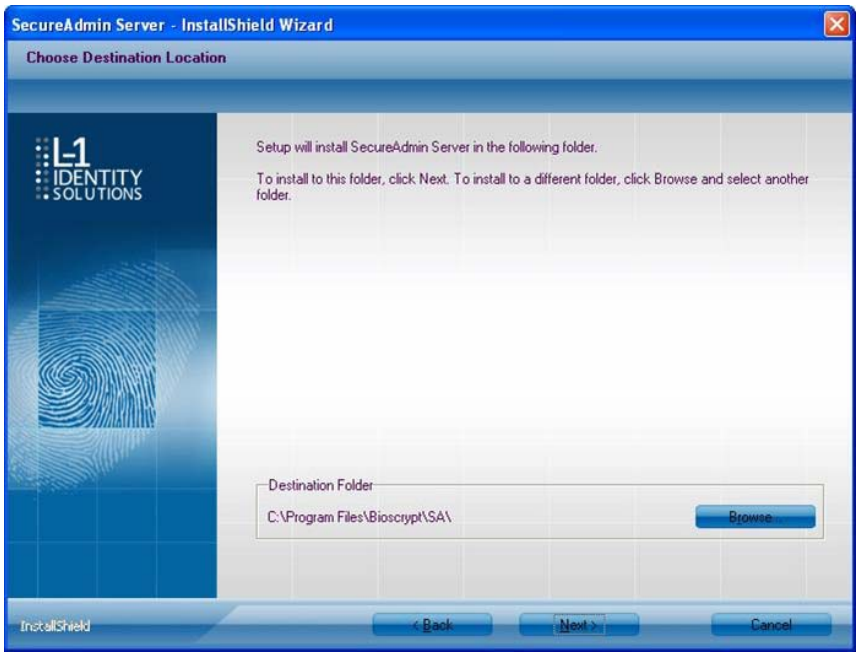
The **Secure Admin Server Installation Wizard** is displayed. Click Next to continue the setup process.

Figure 3-5 SecureAdmin Server License Agreement



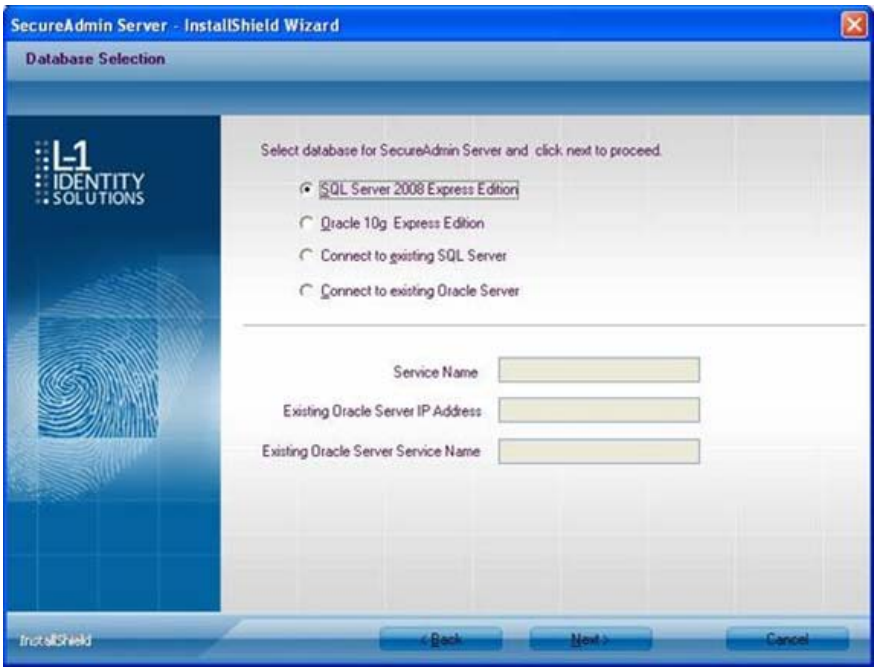
The L-1 Identity Solutions License Agreement is displayed. Select the appropriate radio button to agree with the terms and then click the **Next** button (You must accept the terms of the licence agreement to continue the installation process).

Figure 3-6 SecureAdmin Server Choose Destination Location



The **Choose Destination Location** screen is displayed. Accept the default installation folder and click the Next button or click Browse to choose your own installation path. After you specify a destination folder, the Database Selection screen is displayed.

Figure 3-7 Database Selection

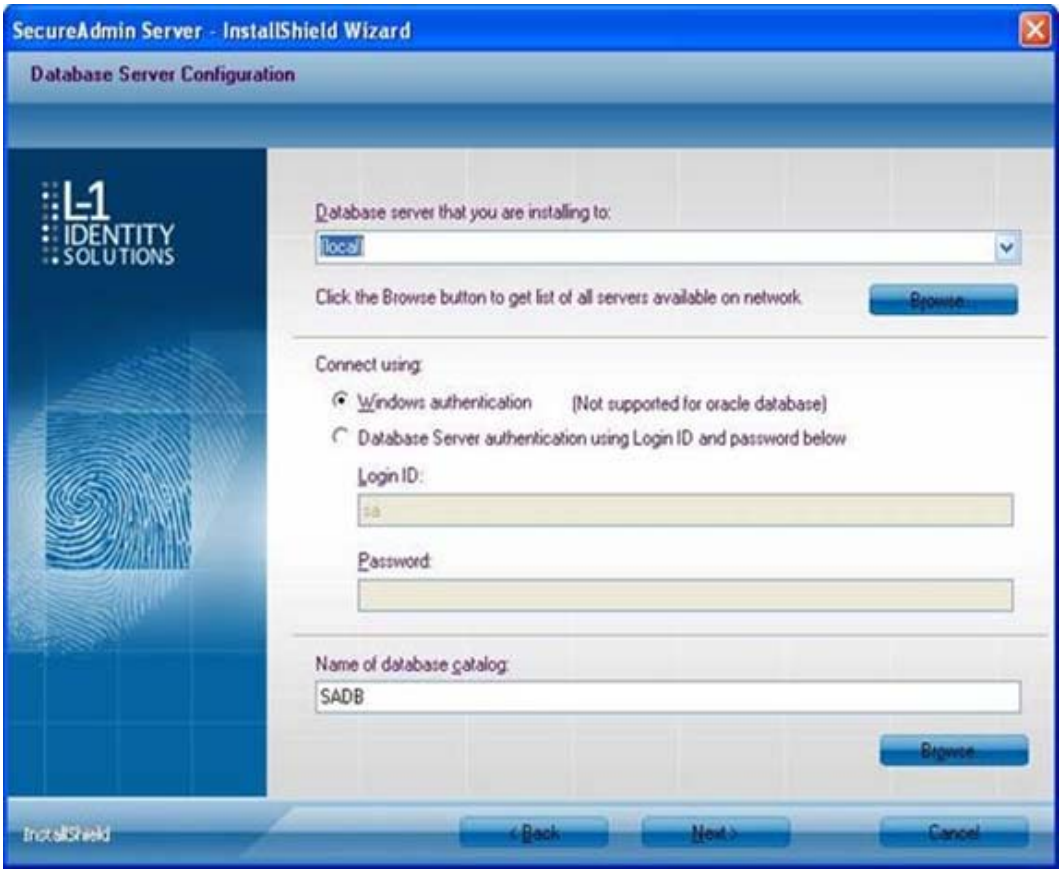


Using the radio buttons, select the type of database application you intend to work with, or select an existing database. Click the **Next** button.

If you selected the SQL Server 2008 Express Edition option, it will be installed locally if it is not already installed.

- ✓ Select **SQL Server 2008 Express Edition** option to install SQL Server 2008 on the local machine and Click **Next**.
- ✓ Select Windows **authentication or Database server authentication** option and enter a valid login ID and password values.
- ✓ Enter the **name of the database catalog** or click **Browse** to select an existing database catalog.
- ✓ Click **Next** to continue.

Figure 3-8 Connecting to SQL Server option



If you selected Connect to Existing SQL Server option,

- ✓ Select **Connect to Existing SQL Server** option and Click on Next.

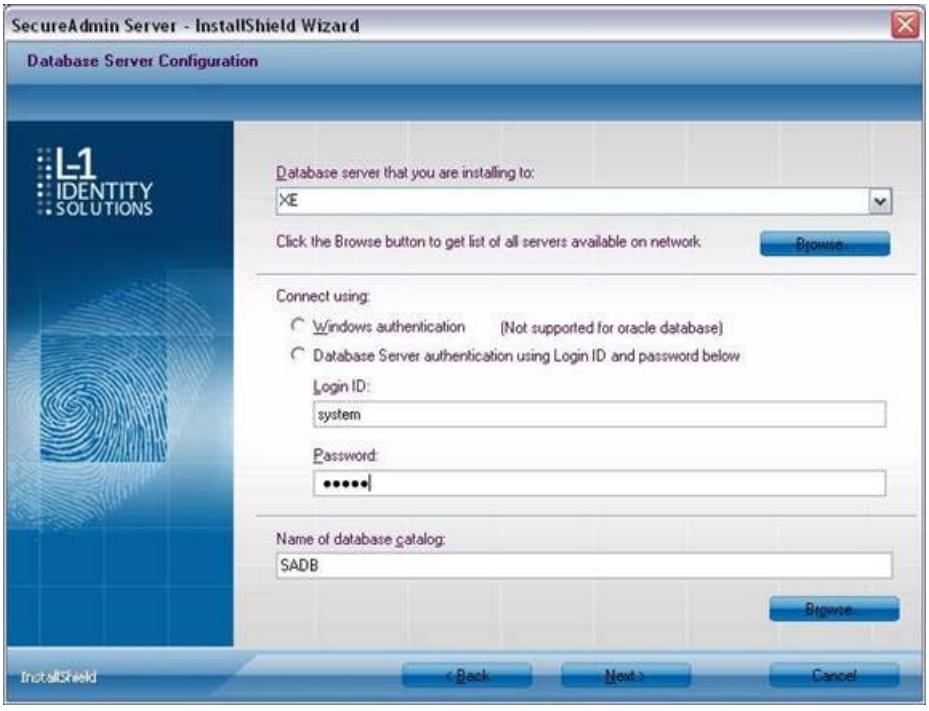
- ✓ You can select existing database instance of SQL Server 2005 or SQL Server 2008 as required from the drop-down of **Database server that you are installing to**.
- ✓ Select the **Database server authentication** option and enter valid Login ID and password values.
- ✓ Accept the default database catalog or click **Browse** to select a different database catalog.
- ✓ Click **Next** to continue

If you selected the Oracle 1 0G Express Edition option, it will be installed locally if it is not already installed.

If you selected Connect to Existing Oracle Server option,

- ✓ Select **Connect to Existing Oracle Server** option and Click **Next**.
- ✓ Select the **Service name**, existing **Oracle Server IP Address** and **Existing Oracle Server Service** name.
- ✓ Accept the default database catalog or click **Browse** to select a different database catalog.
- ✓ Click **Next** to continue.
- ✓ Select **database server** and enter valid Login Id and password. Accept the default database catalog or click **Browse** to select a different database catalog.
- ✓ Click **Next** to continue.

Figure 3-9 Database Server Configuration



3.1.1.1 REPAIRING AN INSTALLATION OF SECUREADMIN SERVER

To repair an installation:

1. Login as **Administrator** and go to the Install.

Double-click the **Setup.exe** installer file to start the installer.

On the L1 Identity Solutions screen, select the **Server Installation** option.

On the **SecureAdmin Welcome** screen, select the **Repair** option. Click **Next** to continue.

On the **Maintenance Complete** screen, click the **Finish** button to complete the repair installation process.

3.1.1.2 UNINSTALLING SECUREADMIN SERVER

Uninstall SecureAdmin Server by using either the **Add/Remove Program** function in Windows or by using the **Remove** option from the installation file as outlined below.

You can also uninstall SecureAdmin Server by using the Remove option within the installation file. Follow the instructions above for repairing an Installation. Select the Remove option instead of the **Repair** option, then follow the prompts.

3.1.1.3 UPGRADING AN INSTALLATION OF SECUREADMIN SERVER

Installer of SecureAdmin supports upgrading SecureAdmin server from existing (currently installed) version to a newer one.

1. When you run the setup of SecureAdmin server, it checks to see if previous version of SecureAdmin server is already installed on the machine. If yes, it prompts to upgrade SecureAdmin server. Click **Yes** to continue with upgrade install.

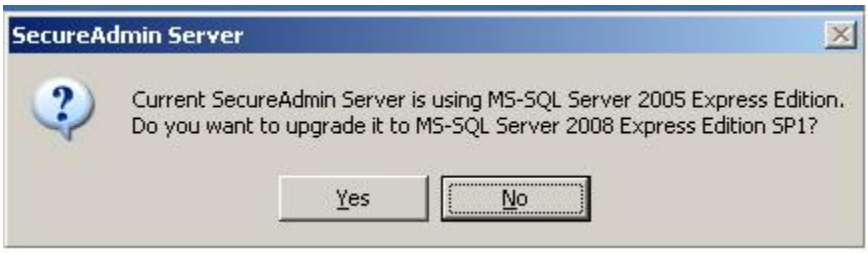
Figure 3-10 Upgrade Confirmation

If you have installed previous version of SecureAdmin server with SQL Server 2005, installer prompts to upgrade from SQL Server 2005 to SQL Server 2008. Click **Yes** if you intend to migrate to SQL Server 2008.

Clicking **Yes** will install SQL Server 2008 locally if it is not installed. It will upgrade existing SQL Server 2005 database catalog and migrate it to SQL Server 2008.

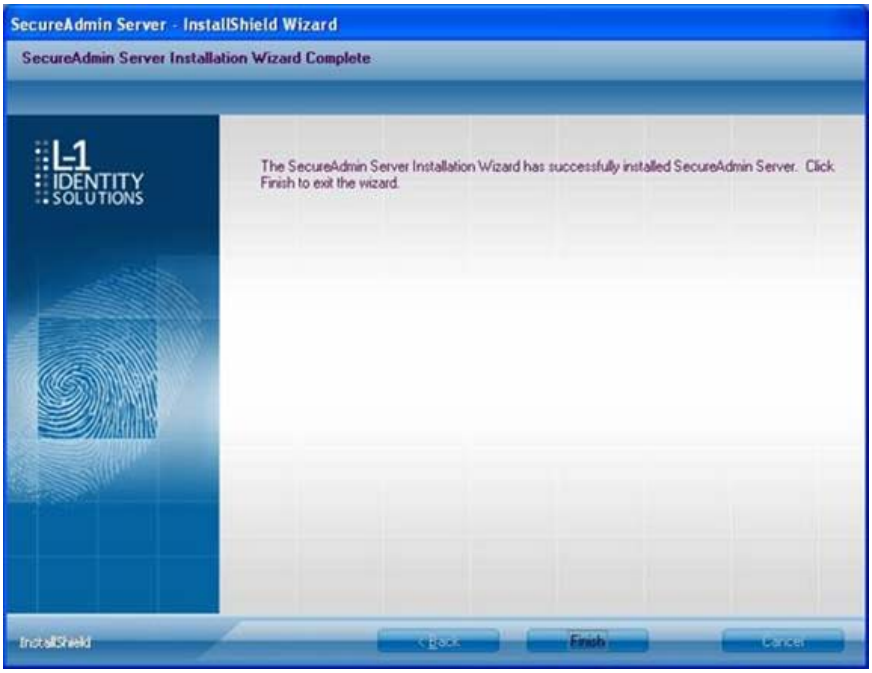
Clicking **No** will upgrade existing SQL Server 2005 database catalog.

Figure 3-11 Upgrade from MS-SQL Server 2005 Express Edition Confirmation



Click Finish. This completes the SecureAdmin server installation and exits the installer

Figure 3-12 SecureAdmin Server Installation Complete

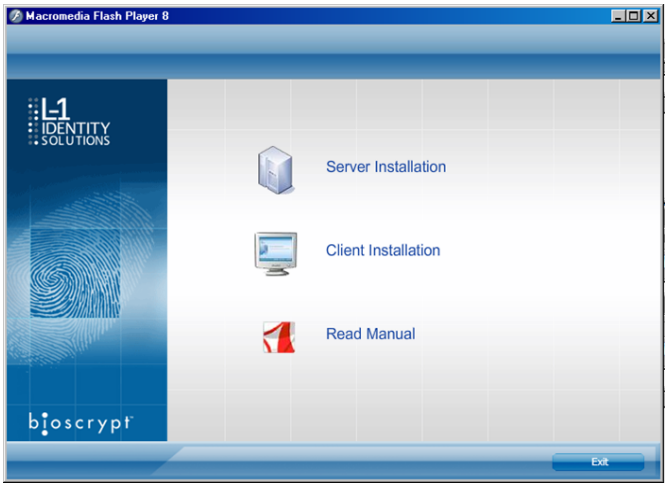


3.1.2 SECUREADMIN CLIENT

To install the SecureAdmin client software, follow these steps:

1. Insert the CD into the optical drive. If Autoplay is enabled, the installation process will start automatically. A menu is displayed. If Autoplay is not enabled, start the installation process manually by doubleclicking the **Setup.exe** file located in the SecureAdmin folder on the CD.

Figure 3-13 Menu



Click **Client Installation**. The InstallShield Wizard is started and the target system is examined. The **Welcome** screen is displayed.

Figure 3-14 InstallShield Wizard

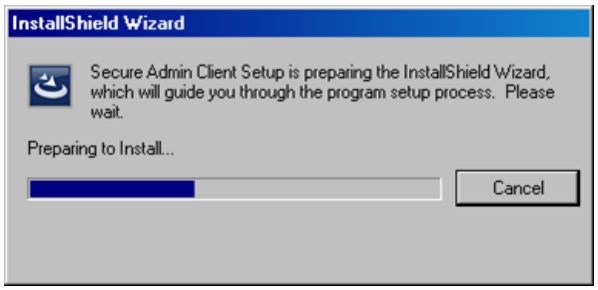
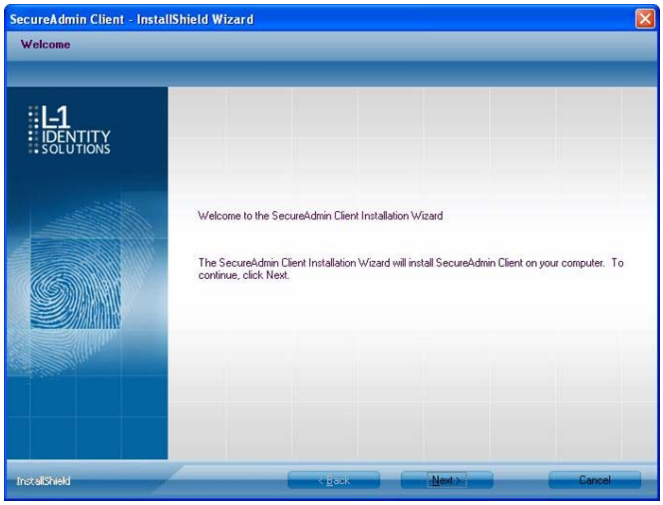
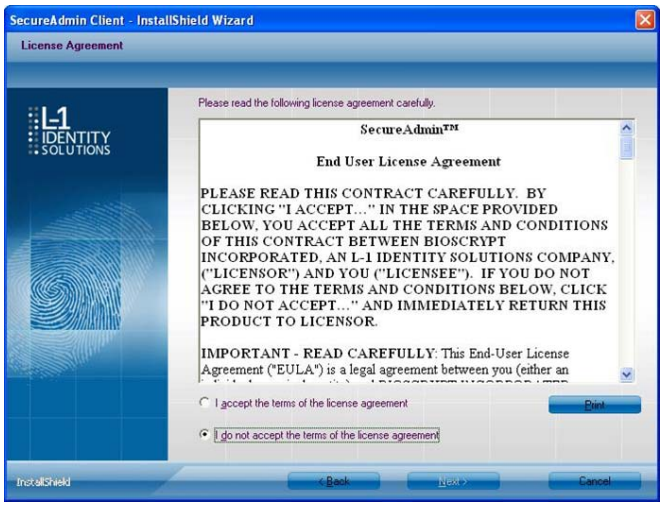


Figure 3-15 Welcome Screen



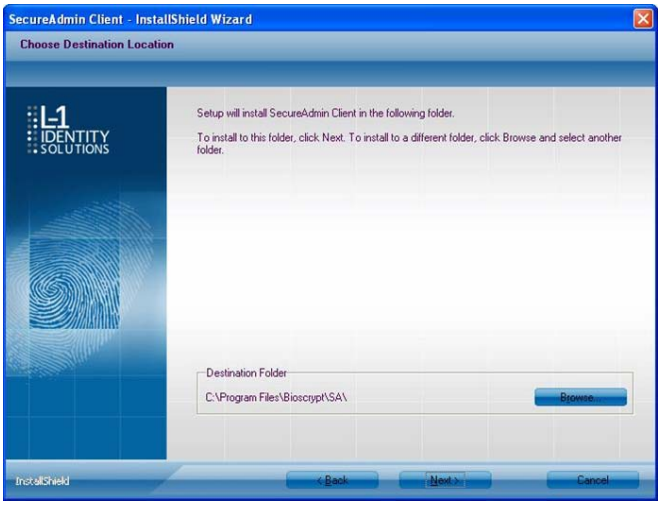
Click the **Next** button to continue. The **License Agreement** screen is displayed.

Figure 3-16 SecureAdmin Client License Agreement



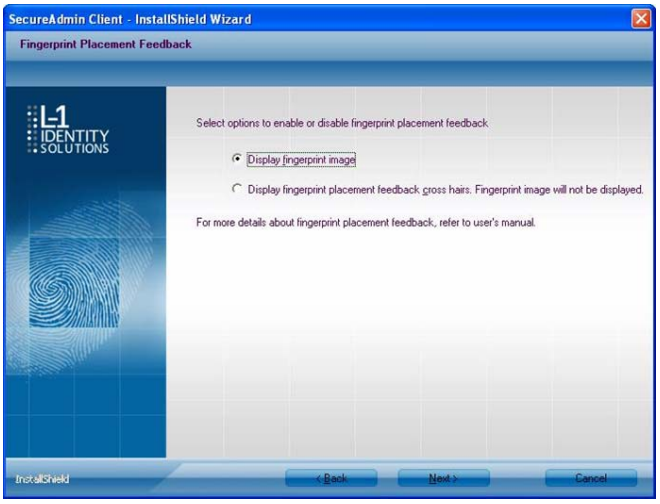
The L-1 Identity Solutions License Agreement is displayed. Select the appropriate radio button to agree with the terms and then click the **Next** button. The **Choose Destination Location** screen is displayed.

Figure 3-17 SecureAdmin Client Choose Destination Location



Accept the default installation folder and click the **Next** button or click Browse to choose your own installation path. After you specify a destination folder, the **Fingerprint Selection Feedback** selection screen is displayed.

Figure 3-18 Fingerprint Placement Feedback Option Selection

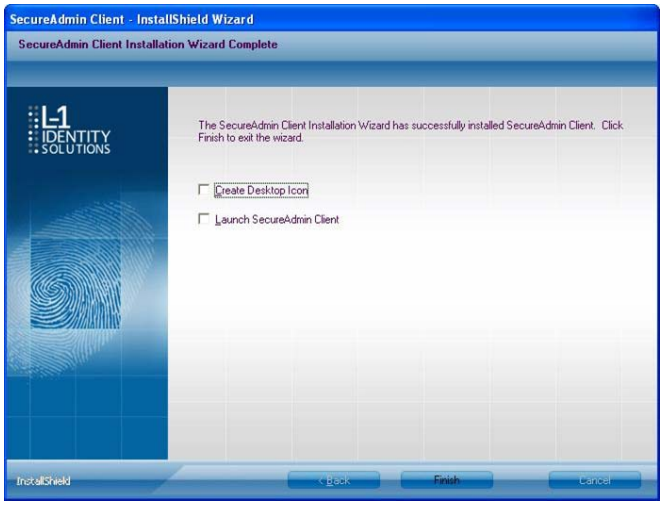


Select the appropriate radio button to either display or to not display fingerprint data. If **Display Fingerprint Image is selected**, a fingerprint will be displayed while enrolling templates. If the **Display Fingerprint Placement Feedback** option is selected, then SecureAdmin displays crosshair placement feedback instead of fingerprint images while enrolling templates.

Click the **Next** button. The InstallShield Wizard completes the installation and displays a **Finished** screen.

Select either or both of the optional Check **Create Desktop** Icon and **Launch Secure Admin** Client check boxes.

Figure 3-19 InstallShield Wizard Finished



Click the **Finish** button.

3.1.2.1 MODIFYING AN INSTALLATION OF SECUREADMIN CLIENT

To modify an installation:

1. Login as **Administrator** and go to the Secure Admin installer.

Double-click the **Setup**.exe installer file to start the installer.

On the L1 Identity Solutions screen, select the **Client Installation** option.

On the Secure Admin Welcome screen, select the **Modify** option. Click **Next** to continue.

Select the appropriate **Fingerprint Placement Feedback** option. If **Display Fingerprint Image** is selected, fingerprints will be displayed while enrolling templates. If **Display Fingerprint Placement Feedback** is selected, SecureAdmin displays crosshair feedback instead of fingerprint images while enrolling templates.

Click **Next** to continue.

On the **Maintenance Complete** screen, click the **Finish** button to complete the modified installation.

3.1.2.2 REPAIRING AN INSTALLATION OF SECUREADMIN CLIENT

To repair an installation:

1. Login as **Administrator** and go to the Secure Admin installer.

Double-click the **Setup.exe** installer file to start the installer.

On the L1 Identity Solutions screen, select the **Client Installation** option.

On the SecureAdmin Welcome screen, select the **Repair** option. Click **Next** to continue.

On the **Maintenance Complete** screen, click the **Finish** button to complete the repair installation process.

3.1.2.3 UNINSTALLING SECUREADMIN CLIENT

Uninstall SecureAdmin Client by using either the **Add/Remove Program** function in

Windows or by using the **Remove** option from the installation file.

To uninstall SecureAdmin client by using the **Remove** option within the installation file, follow the instructions for repairing an installation. Select the **Remove** option instead of the **Repair** option, then follow the prompts.

3.1.2.4 UPGRADING AN INSTALLATION OF SECUREADMIN CLIENT

To upgrade a previous version of SecureAdmin Client, first uninstall the older version using Windows **Add/Remove** Programs or the SecureAdmin installer, then re-install the new version of SecureAdmin Client.

CHAPTER 4 - INSTALL HARDWARE

CHAPTER OVERVIEW

This chapter explains how to install a V-Station 4G or V-Flex 4G device, how to mount a wall plate, how to attach a device to a wall plate, and how to make the required electrical connections to the device.

4.1 INSTALL HARDWARE

4.1.1 WALL-MOUNTING SCHEMES

The V-Station 4G and V-Flex 4G devices are mounted, by use of a mounting plate, either directly to a wall or to an electrical box recessed in the wall. The V-Station 4G device can be flush mounted only. The V-Flex 4G device can be either flush or recess-mounted on a wall.

The V-Station 4G Extreme devices are mounted, by use of a stainless steel mounting plate, directly to a wall.

4.1.2 INSTALLING A MOUNTING PLATE

The procedure for mounting a wall plate directly to a wall is as follows:

Hold the mounting plate onto the wall in the desired location, trace the square hole that will be cut out, and mark the mounting screw locations. Note that for the V-Flex 4G, the large square hole is at the bottom and for the V-Station 4G the hole is to the right.

Cut out the square hole with a jigsaw or drywall saw. If the V-Flex 4G device is to be recess-mounted, cut out a hole in the drywall to accommodate the rear extension on the device housing.

Drill holes for the nylon wall anchors and install them.

Fish wires through the wall to the square hole.

Align the hole in the wall plate with the hole in the wall.

Fasten the mounting plate to the nylon wall anchors in the wall with the provided screws.

If the V-Flex 4G device is to be recess-mounted on an electrical box, a double gang box is required to accept the rear extension of the housing.

If mounting the V-Station 4G device to an electrical box, attach the mounting plate to a single

gang box and use wall anchors on the remaining four holes for additional security.

To install the mounting plate on to an electrical box, screw the mounting plate to the box with the provided 6-32 screws.

	***CAUTION***
	When installing a recess-mounted V-Flex 4G device, be careful not to damage the tamper switch, as careless handling can shear it off.

Figure 4-1 V-Flex 4G Flush-mount Mounting Plate

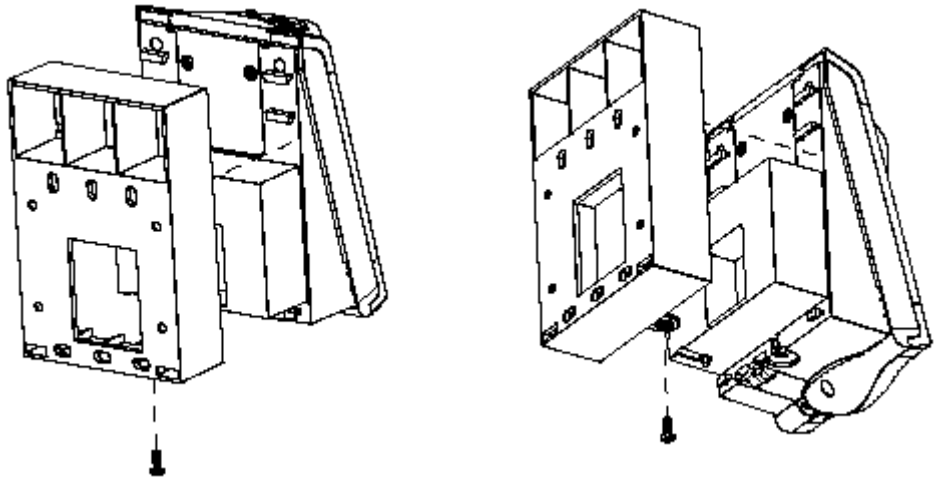


Figure 4-2 V-Flex 4G Recessed-mount Mounting Plate

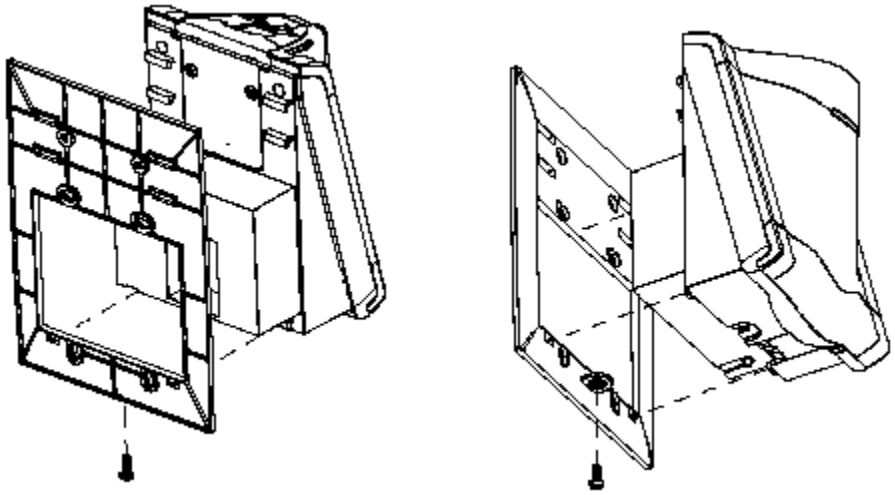
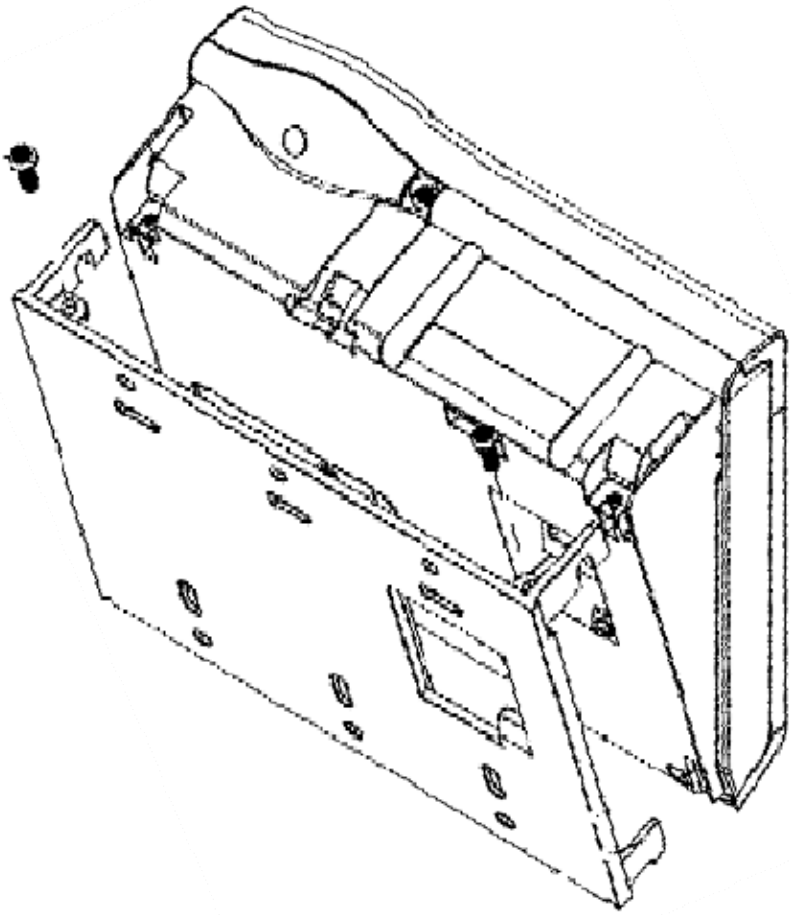


Figure 4-3 V-Station 4G Mounting Plate



	NOTICE
	The V-Station 4G device can only be flush mounted.

Figure 4-4 V-Station 4G Extreme Mounting Plate

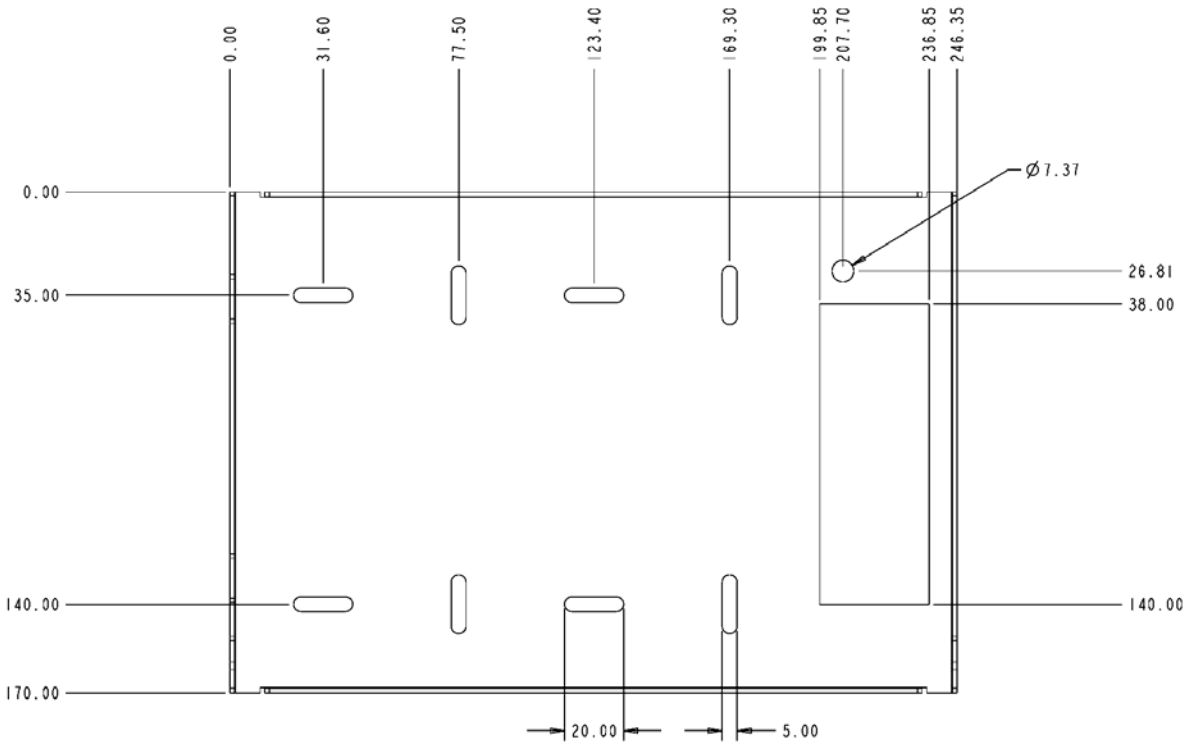
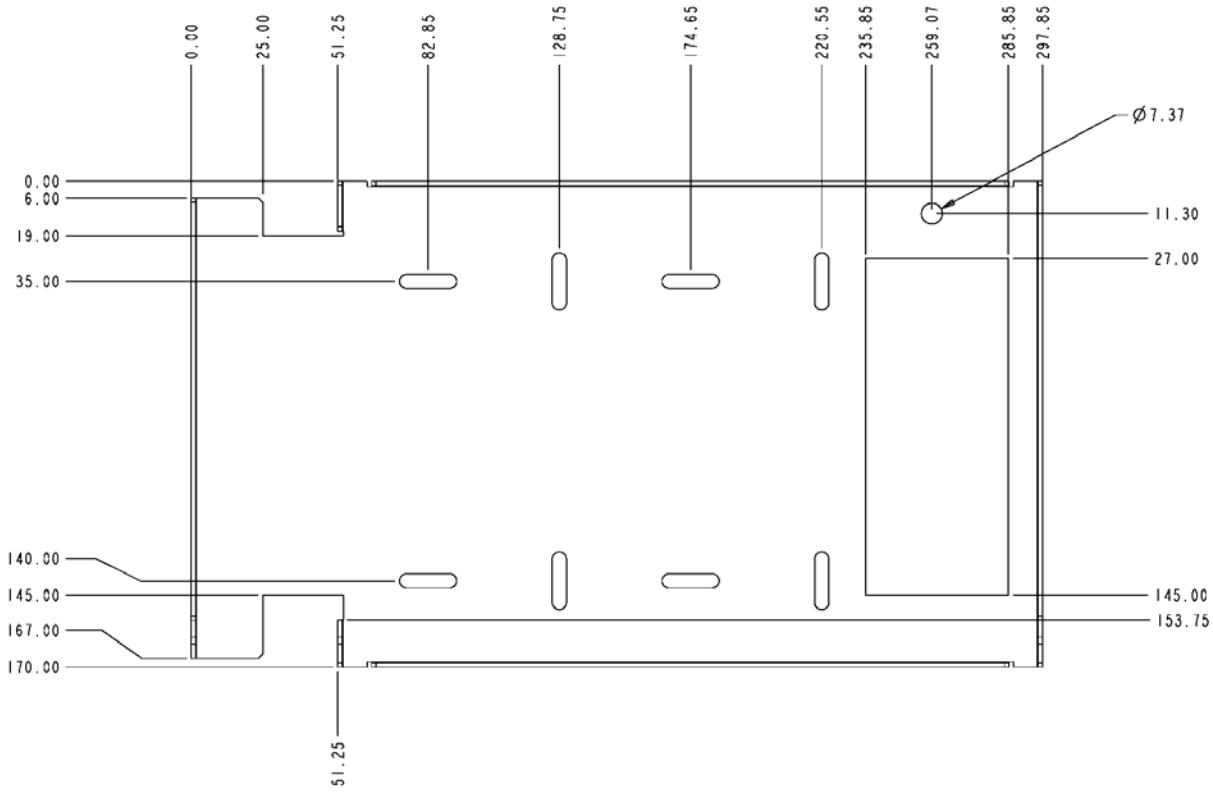


Figure 4-5 4G Extreme PIV/TWIC Mounting Plate



4.1.3 INSTALLATION HARDWARE

4.1.3.1 4G V-Station and V-Flex Indoor devices

Quantity

- ✓ 1 Wall mounting plate/mullion mounting plate
- ✓ 6 #6-32 3/4" Philips pan-head screw
- ✓ 6 #6 1" Philips pan-head self-tapping screws
- ✓ 6 #4-8 1" nylon wall anchors

The hardware shown above is provided to mount the mounting plate to the wall and the V- Station 4G or V-Flex 4G device to the mounting plate.

4.1.3.2 4G Extreme Devices

- ✓ 1 Stainless Steel, Wall Mount Plate
- ✓ 8 wall mount anchor, conical, for #8 screws
- ✓ 6 6-32 Security Screw 1/8" pin-in-hex 3/8" length

- ✓ 8 #8x1" thread forming screw, pan head, Philips
- ✓ 8 wall mount anchor, conical, for #8 screws

4.1.4 ATTACH DEVICE TO MOUNTING PLATE

4.1.4.1 4G V-STATION AND V-FLEX INDOOR DEVICES

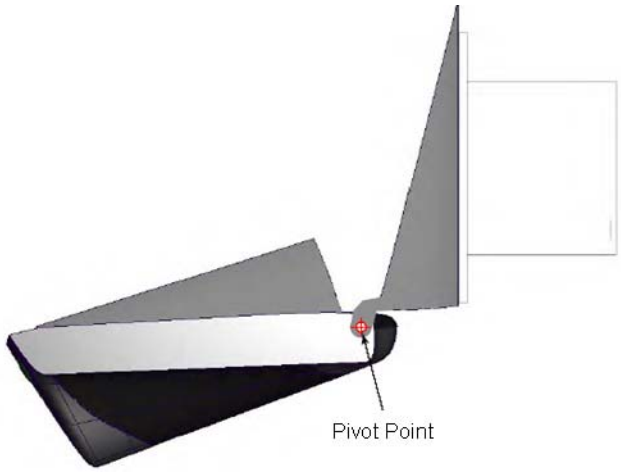
Once all the electrical connections have been made to the device, it can be attached to the mounting plate as follows:

For the V-Flex 4G, insert the four hooked protrusions on the rear of the device into the corresponding slots on the mounting plate. Hold the device against the plate and gently press it in a downward direction to engage the hooks. Insert the star-shaped screw at the bottom center of the mounting plate and tighten with the wrench provided. Do not over-tighten.

For the V-Station 4G, hold the device with the top slightly tilted toward you, at about a 30-degree angle to the wall. Hold the bottom of the device against the mounting plate and lower it so that the two hooks on the bottom of the mounting plate engage the corresponding slots on the device. When the hooks are properly engaged, the top of the device can be pivoted up against the mounting plate. It will drop down slightly, locking itself in the closed position, and should be secured in this position with the star-shaped screws in the holes at the right and left ends on the bottom of the device. Do not over-tighten.

With the securing screws removed, the V-Station 4G device can be pivoted down 90 degrees from the wall, to allow access for making connections, etc. The device can be removed from the mounting plate by tilting it at an angle approximately 30 degrees to the wall and gently lifting it up off the hooks on the mounting plate.

Figure 4-6 Device Open for Installation or Service



4.1.4.2 4G EXTREME DEVICES

TBD

4.1.5 CONNECT DEVICE TO POWER SOURCE

The V-Station 4G and V-Flex 4G, and 4G Extreme devices can be powered by 12V-24V DC power sources, or through a Power Over Ethernet (PoE) injector for V-Station 4G and V-Flex 4G.

The two options for providing 1 2V power to V-Station 4G and V-Flex 4G devices are by using an external wall plug-in adapter (Figure 4-7), or through external wiring and a mini plug (Figure 4-8).

12V power can be provided to 4G Extreme devices only through the 3-Wire back cable (Figure 4-9).

Figure 4-7 Connections for an External Wall Adapter (4G Indoor)

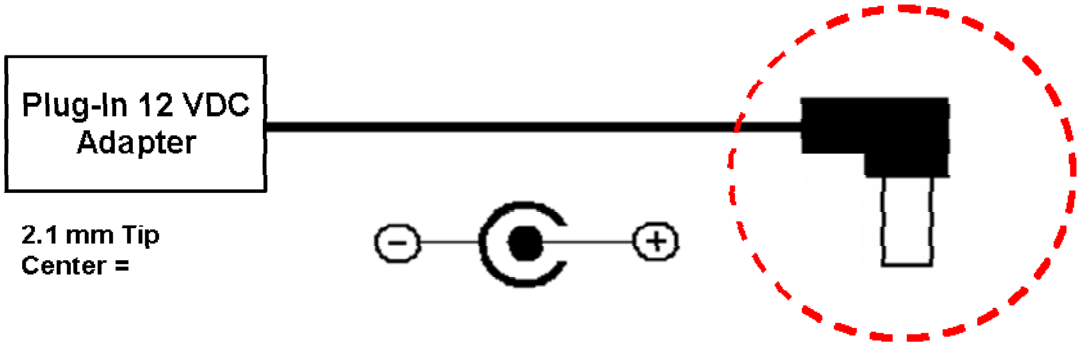


Figure 4-8 Connections for an External Power Source (4G Indoor)

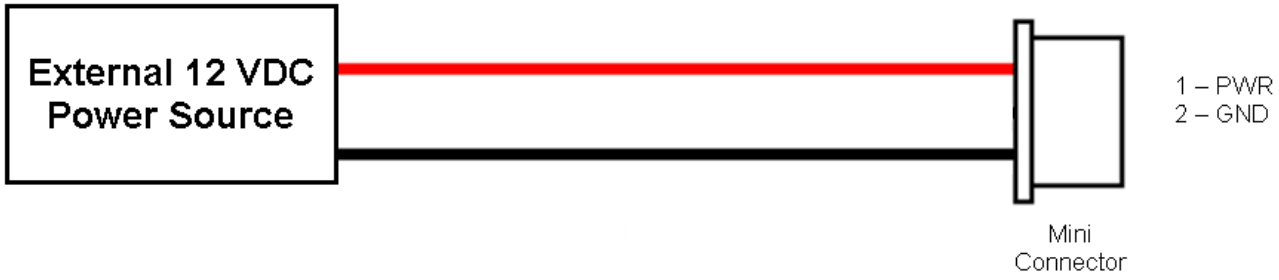


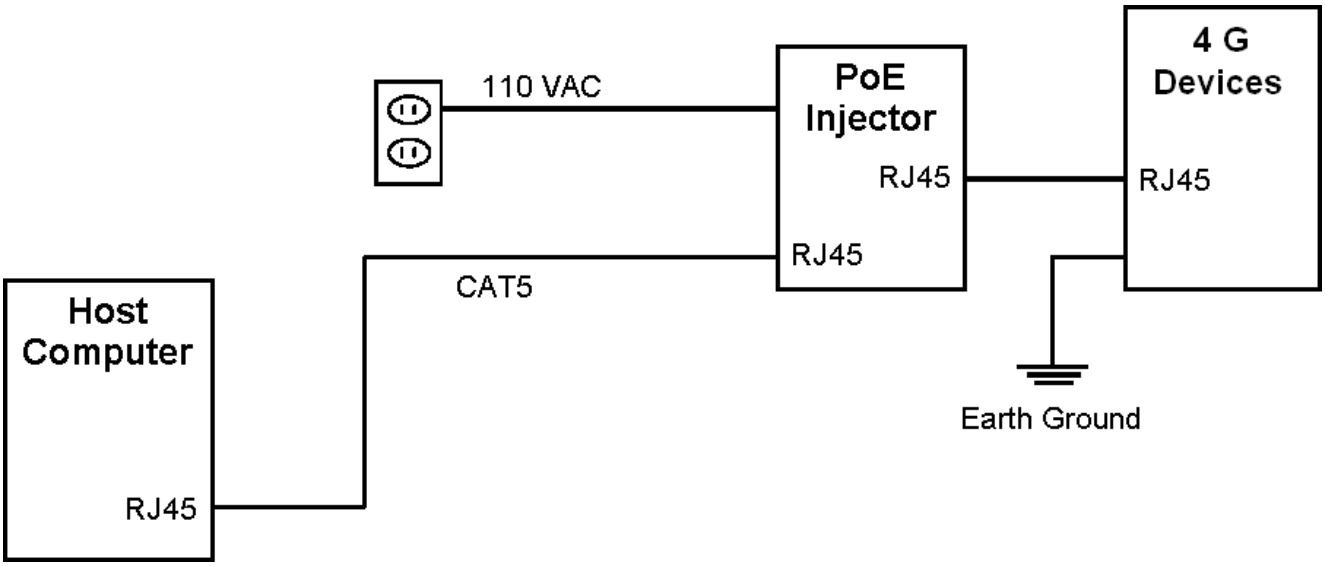
Figure 4-9 Connections for an External Power Source (4G Extreme)

The V-Station 4G, V-Flex 4G devices both support Power over Ethernet (PoE), using their RJ-45 Ethernet interface. When these devices are to be powered over Ethernet, an IEEE 802.3af compliant Active Midspan Injector must be used. Such an injector is not supplied with L-1 Identity Solutions products. An example of a suitable PoE injector is Model No. AT-61 01 G from Allied Telesis Inc. (http://www.alliedtelesis.com).

Any such device should carry at least one of the certifications shown below and should be FCC listed.

Figure 4-10 Certification Marks

Figure 4-11 Power Over Ethernet Connection



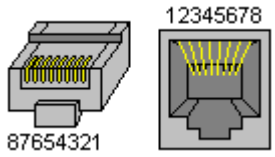
Specifications for suitable PoE Injectors for 4G Indoor devices are as follows:

- ✓ Input voltage: 90-264 VAC, 60 Hz
- ✓ Input current: 0.4A @ 100 VAC
- ✓ Output voltage: -48 VDC
- ✓ Output current: 0.32A
- ✓ Power: 15.36 W

For Power over Ethernet, RJ-45 pin numbers 4, 5 are considered VB1 (+) positive DC supply, and pin numbers 7, 8 are VB2(-) DC return.

Detailed RJ-45 pin assignments for PoE are given in Table PoE Pin Assignments, and the physical location of the pins in the RJ-45 connector.

Figure 4-12 RJ45 Pin Location



4.1.6 CONNECT DEVICE TO NETWORK

The V-Station 4G and V-Flex 4G devices support both RS-232/RS-485 and Ethernet 1 0baseT and 1 00baseTX network protocols.

4.1.6.1 ETHERNET NETWORK CONNECTIONS

Ethernet connections to the device are made through a standard RJ-45 connector on the back of the device.

4.1.6.2 RS-232/RS-485 NETWORK CONNECTIONS

To connect a device to an RS-232 or RS-485 network, connect the appropriate wires to the provided pigtail in accordance with the pin-out diagram.

Table 4-1 Pin-out Diagram

Connector Pin No.	Wire Color	Connector Pin No.	Wire Color
Pin1 *(RS485A)*	Blue	Pin2 *(RS232_RX)*	Violet/White
Pin3 *(RS485B)*	Blue/Black	Pin4 *(RS232_TX)*	Violet
Pin5 *(SGND)*	Black/Red	Pin6 *(SGND)*	Black/Red
Pin7 *(WIEGAND_LED_IN0)*	Grey/Black	Pin8 *(WIEGAND_DIN0)*	Green/White
Pin9 *(Not Connected)*		Pin10 *(WIEGAND_DIN1)*	White/Black
Pin11 *(WIEGAND_LED_OUT0)*	Brown/Green	Pin12 *(WIEGAND_DOUT0)*	Green
Pin13 *(WIEGAND_LED_OUT1)*	Brown/Black	Pin14 *(WIEGAND_DOUT1)*	White
Pin15 *(TTLOUT_0H)*	White/Brown	Pin16 *(WGND)*	Black/White
Pin17 *(TTLOUT_0L)*	White/Red	Pin18 *(TTLIN0)*	Yellow/Blue
Pin19 *(TTLOUT_1H)*	Brown/White	Pin20 *(TTLIN1)*	Blue/Brown
Pin21 *(TTLOUT_1L)*	Yellow/Black	Pin22 *(TTLIN2)*	Brown/Violet
Pin23 *(TTLOUT_2H)*	Grey/Orange	Pin24 *(TTLGND)*	Green/Brown
Pin25 *(TTLOUT_2L)*	White/Green	Pin26 *(RELAY_NC)*	Orange
Pin27 *(RELAY_NO)*	Yellow	Pin28 *(RELAY_COM)*	Grey

When connecting the device to the network, the following procedures must be followed:

- ✓ Use Category 5 cabling with a characteristic impedance of 120 ohms for RS-485 networks. Category 5 cables with a characteristic impedance of 100 ohms can also be used, but with lower performance.
- ✓ Cable manufacturers provide cables with multiple twisted pairs designed for this type of communication (characteristic impedance is 120 ohm).
- ✓ Unused pairs within the cable must be terminated with characteristic impedance (100 or 120 ohm) on both ends.
- ✓ AWG 24 should be considered as the minimum gauge.
- ✓ Choose one twisted pair of conductors to use for RS-485 differential connections, other conductors should be used for Signal Ground (RS-485 GND on Weidmuller connection).
- ✓ The RS-232 to RS-485 converter must support Sense Data to be able to switch from Send to Receive mode.
- ✓ Check each device's cabling for ground faults before connecting to an RS-485 network.
- ✓ Each device should have pin 3 of the mini-connector connected to earth ground.

After all devices are configured and connected to the RS-485 network, the baud rate can be increased to the highest supported rate (some experimentation might be required).

4.1.6.3 WIRELESS NETWORK CONNECTIONS

After the physical installation, the device can be configured for wireless network connection. The wireless network can be set up either through SecureAdmin (see Chapter 7 in the Operator's Manual) or through the front panel of the V-Station 4G device.

To set up wireless operation through the front panel of a V-Station 4G device, perform the following steps:

2. Power up the device.

Ensure that the wireless network is functioning.

Use one of these supported modes:

- ✓ WEP Open
- ✓ WPA Personal

✓ WPA2 Personal.

NOTICE

L-1 Identity Solutions does not recommend using the "No encryption" mode.

Enter the Admin menu on the device by pressing the Left arrow and Enter keys simultaneously.

Key in the Admin password (default is "0000") and press OK.

Select the Communications icon and press OK

Select "Network Interface" and press OK.

Select "WLAN" Configuration and press OK.

Select Managed/Adhoc mode from WLAN Network type.

Select the intended wireless networks.

Enable WLAN mode from WLAN parameters.

Choose Encryption mode and encryption .

Enter the key.

Select "DHCP" or "Static" and press OK. If you selected "DHCP", the device reboots. Afterwards, it will have a dynamic IP address. If you selected "Static IP", specify an IP, a Net Mask, a Gateway, and then press OK.

SecureAdmin can scan for and auto-detect wireless devices. If you want to use SecureAdmin to scan for wireless devices, ensure that the "multicasting" option is enabled in your router.

NOTICE

The maximum recommended distance from an access point is 25 feet.

4.1.7 SINGLE-DOOR CONTROLLER INSTALLATION

The V-Station 4G and V-Flex 4G devices incorporate an internal relay that enables them to operate a deadbolt/door strike directly.

WARNING

The internal relay is limited to a maximum current of 170 mA. If the deadbolt/ doorstrike to be controlled draws more than 170 mA, damage to the device may occur. If the deadbolt/door strike load exceeds 170 mA, an external relay must be used, as described below. Do not use the same power supply to power a V-Series 4G device and a door strike.

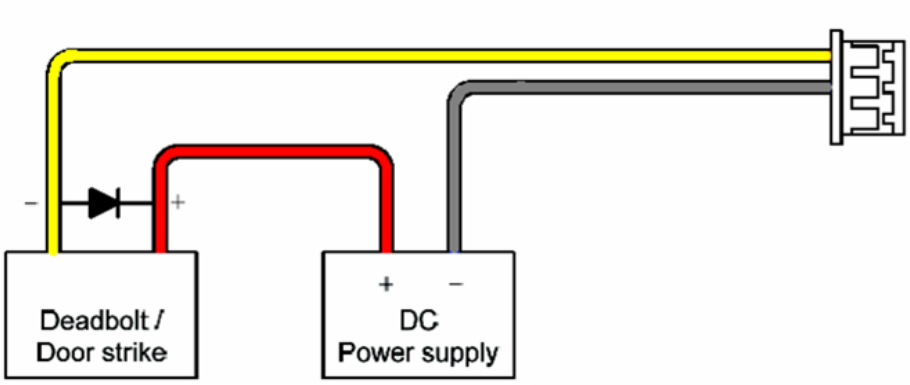
Assuming the current drawn by the deadbolt/door strike is less than 170 mA, the connections between the V-Station 4G or V-Flex 4G device, deadbolt/door strike, and power supply for the deadbolt/door strike should be made. Note that a snubber diode (1 N4007 or equivalent) must be connected across the deadbolt/door strike to protect the DC power supply from inductive kickback.

CAUTION

The snubber diode and DC power supply for the deadbolt/door strike are not supplied with the V-Station 4G and V-Flex 4G devices. The power supply should be specified in accordance with the voltage and current requirements of the deadbolt/door strike, but it must be ensured that the current to operate the dead bolt/door strike does not exceed 170 mA.

If the current required to operate the deadbolt/door strike exceeds 170 mA, an external relay must be used in conjunction with the V-Station 4G or V-Flex 4G device. The external relay must be specified so that its contacts are rated to carry the current required by the deadbolt/door strike, and that the current required to operate its energizing coil is within the 170 mA capacity of the V-Station 4G or V-Flex 4G device's internal relay.

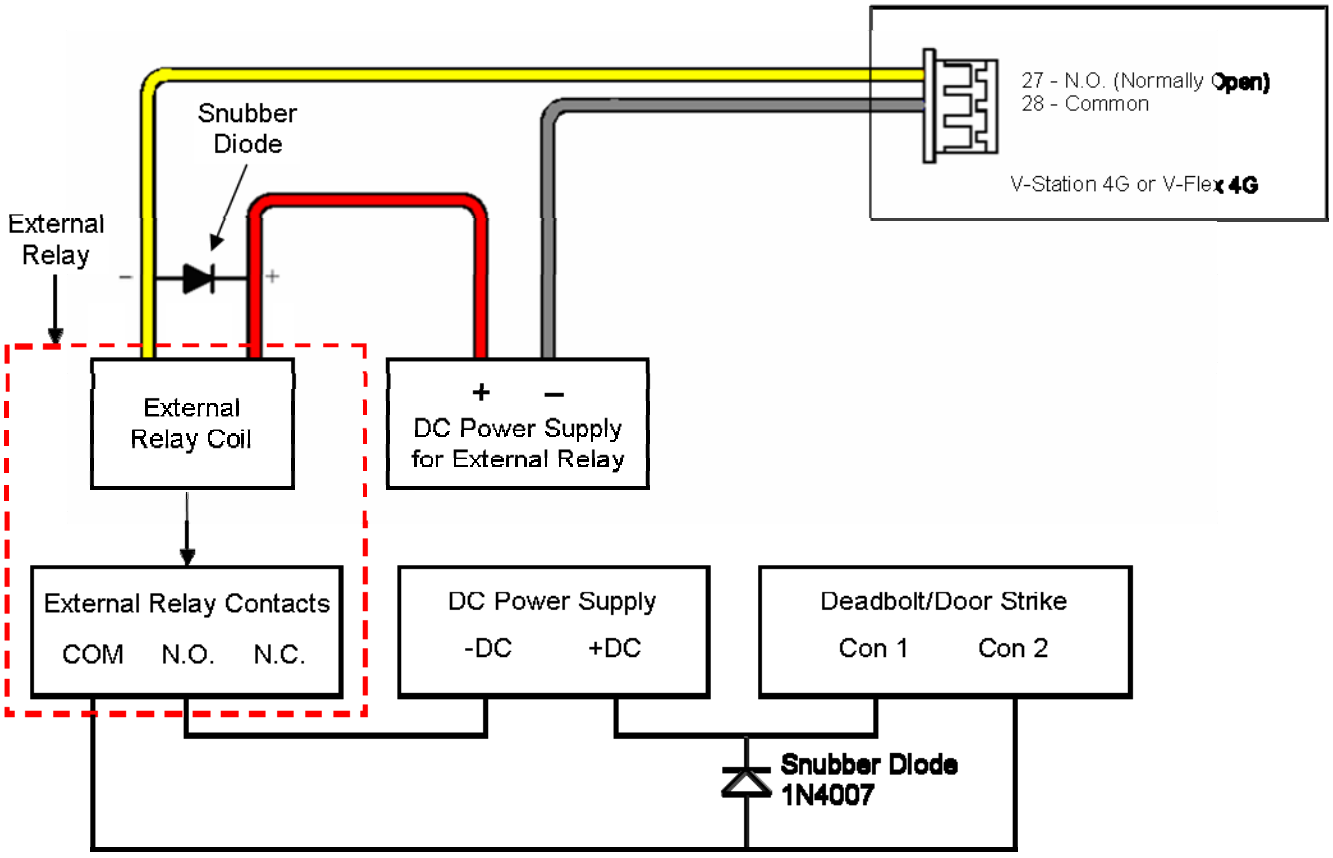
Figure 4-13 Connections for Internal Relay Operation



The power supply for the external relay must be chosen to match the operating voltage and current of the external relay coil, but its voltage must not exceed the V-Station 4G or V-Flex 4G device's internal relay maximum voltage rating of 250 volts.

The external relay should be connected. Note that snubber diodes (1 N2007 or equivalent) should be connected across the external relay coil and the deadbolt/door strike.

Figure 4-14 Connections for External Relay Operation



4.1.8 AUX PORT

The Aux port is a USB 2.0 auto-negotiate connector located on the bottom of the device. To access the Aux port, the Aux port door must first be removed. Use the provided pin-in-hex security key to remove the #6-32 security screw retaining the plastic Aux port door. Gently remove the plastic Aux port door to reveal the USB connector.

To attach a USB memory key or other "gadget" serial device by way of the Aux port, use the USB Type A female to USB Micro A/B male adapter cable provided in the installation kit.

The Aux port is used to transfer files to and from the device. Audio, images, firmware, logs, and configuration files can be transferred quickly and easily to a device without the need for a computer.

	CAUTION
	Current rating of the Aux port is not to exceed 100 mA Maximum.

Figure 4-15 Location of Aux Port (V-Station 4G)

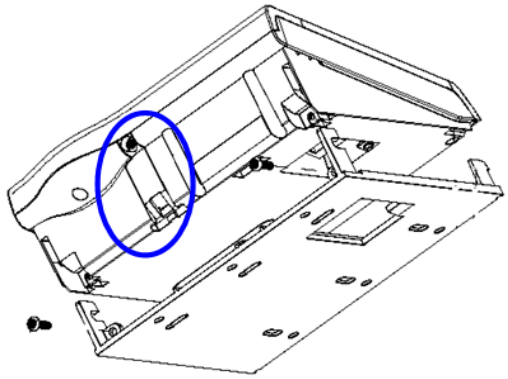


Figure 4-16 Location of Aux Port (4G Extreme)

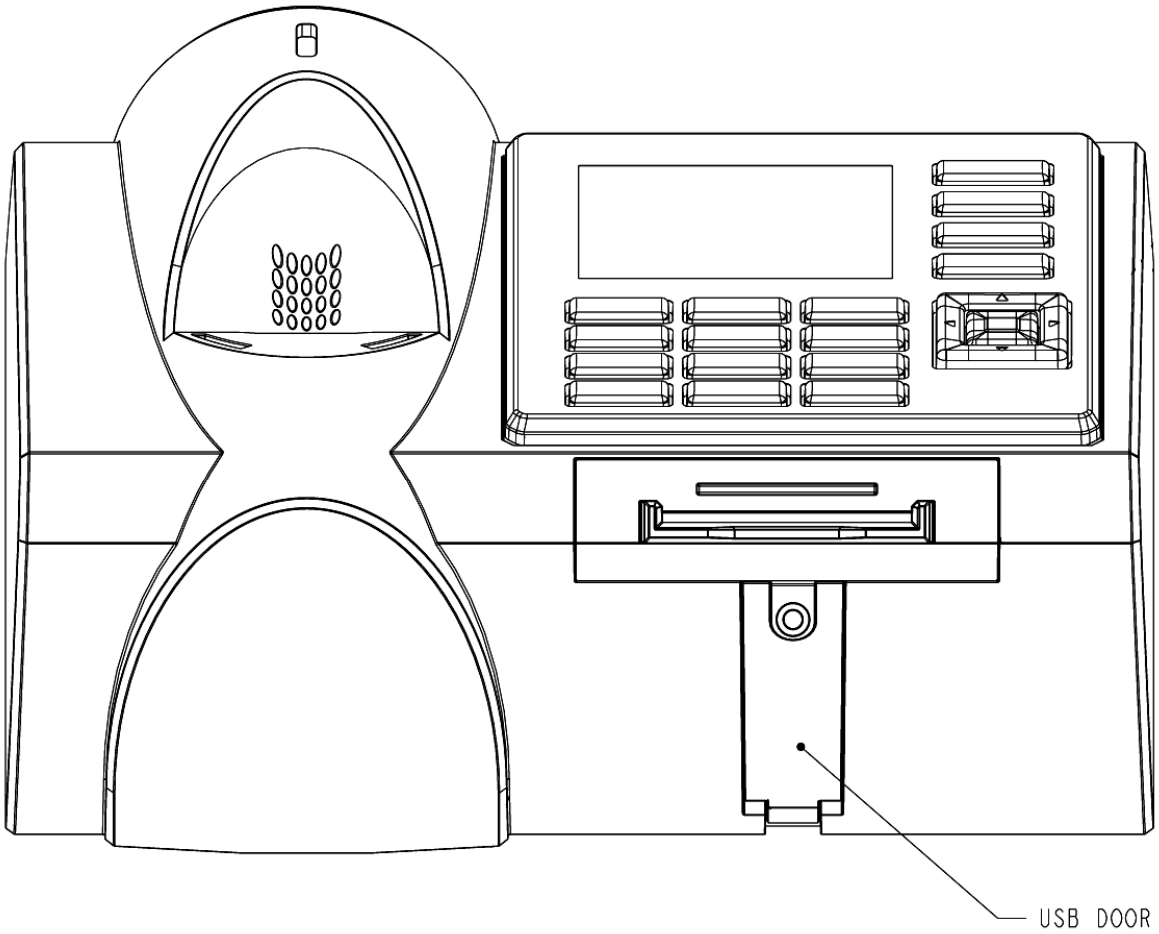


Figure 4-16 USB Memory Key

4.1.9 INSTALL FERRITE CORE

In order for the V-Station 4G and V-Flex 4G devices to comply with FCC Class B & CISPR 22 Class B regulations, the installer and/or end user is required to use the supplied Ferrite Material on the Ethernet, DC, and all I/O cables exiting the rear of the device. This ferrite material is located within the installation kit that is supplied with each product.

Ethernet Ferrite P/N: STEWARD 28A2432-0A2 DC & I/O Lines P/N: STEWARD 28A4155-0A2

Install the ferrite cores as close to the device as possible.

Figure 4-18 Installation of Ferrite Cores

CHAPTER 5 - SYSTEM START-UP PROCEDURES

CHAPTER OVERVIEW

This chapter explains the various start-up procedures and checks that should be performed before applying power to a device.

Chapter Index

5.1 SYSTEM START-UP PROCEDURES

To avoid the need for difficult troubleshooting, system start-up must follow this step-by-step procedure. Never wire up a system and apply power to it all at once.

SYSTEM START-UP OVERVIEW

L-1 Identity Solutions recommends always following these system start-up steps:

Do not apply power to any device.

Check all wiring and device configurations.

Disconnect all devices from the communication line.

Check the supply voltage for correct voltage.

Power up the PC running SecureAdmin.

Power up the RS-232 to RS-485 converter (if installed).

Configure SecureAdmin.

Perform a ground fault check for the converter (if installed).

Connect the PC and converter (if installed) to the communication line.

Verify that the device powers up correctly, but do not connect it to the communication line. The power LED should be illuminated. Check the power lines with a voltmeter.

Perform a ground fault check for the device (if using RS-485, see below).

Connect the device to the communication line.

Verify that the device communicates with SecureAdmin.

If there are more device, repeat Steps 10 through 13 for each device.

5.1.1 DEVICE CONFIGURATION CHECK

Devices must be configured correctly before they can communicate. Common problems include incorrect Host Port Protocol settings, mismatched Baud rates, and incorrect

device Net-work IDs. Each device sharing a communication line must have a unique device Network ID.

5.1.2 RS-232 TO RS-485 CONVERTER GROUND FAULT CHECK

Before a device can be connected to an RS-485 subsystem, it must be checked for ground faults. An uncorrected ground fault can damage all devices connected to the RS-485 communication line.

To check for a ground fault on the RS-232 to RS-485 converter:

3. Apply power to the RS-232 to RS-485 converter.

Connect the signal ground of the RS-485 line through a 10k ohm current-limiting resistor to the signal ground of the RS-232 to RS-485 converter. There should be no more than 1 volt across the resistor.

5.1.3 DEVICE GROUND FAULT CHECK

To check for a ground fault on a new V-Station 4G or V-Flex 4G device:

4. Apply power to all devices already successfully connected to the RS-485 line.

Power up the new device but do not connect it to the RS-485 line.

Connect the signal ground of the RS-485 line through a 10k ohm current-limiting resistor to the signal ground of the V-Station 4G device.

There should be no more than 1 volt across the resistor. If there is, find and clear the fault.

Repeat Steps 1 through 3 with each of the RS-485 signal lines (+ and -).

Connect the new device to the RS-485 line only if no ground fault is found.

6.1 CONFIGURE DEVICE

V-Station 4G and V-Flex 4G devices must be configured before use. This includes setting various communication parameters and calibrating the device's sensor

6.1.1 REGISTER DEVICE

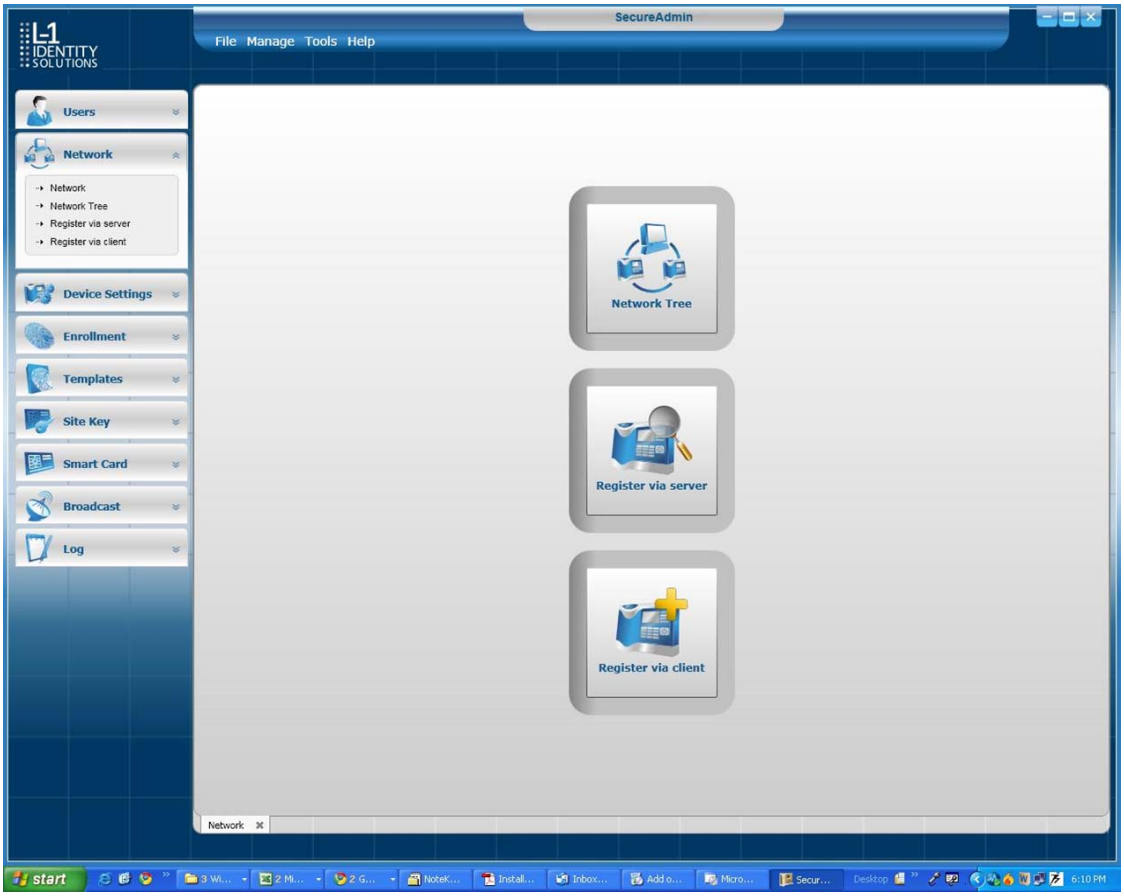
After a device is physically installed, it must registered. This can be done several ways -- when a device is connected by means of a network (this is the recommended method), or when the device is connected directly to the host computer upon which SecureAdmin is running.

6.1.1.1 TO REGISTER A NETWORKED DEVICE

Launch SecureAdmin.

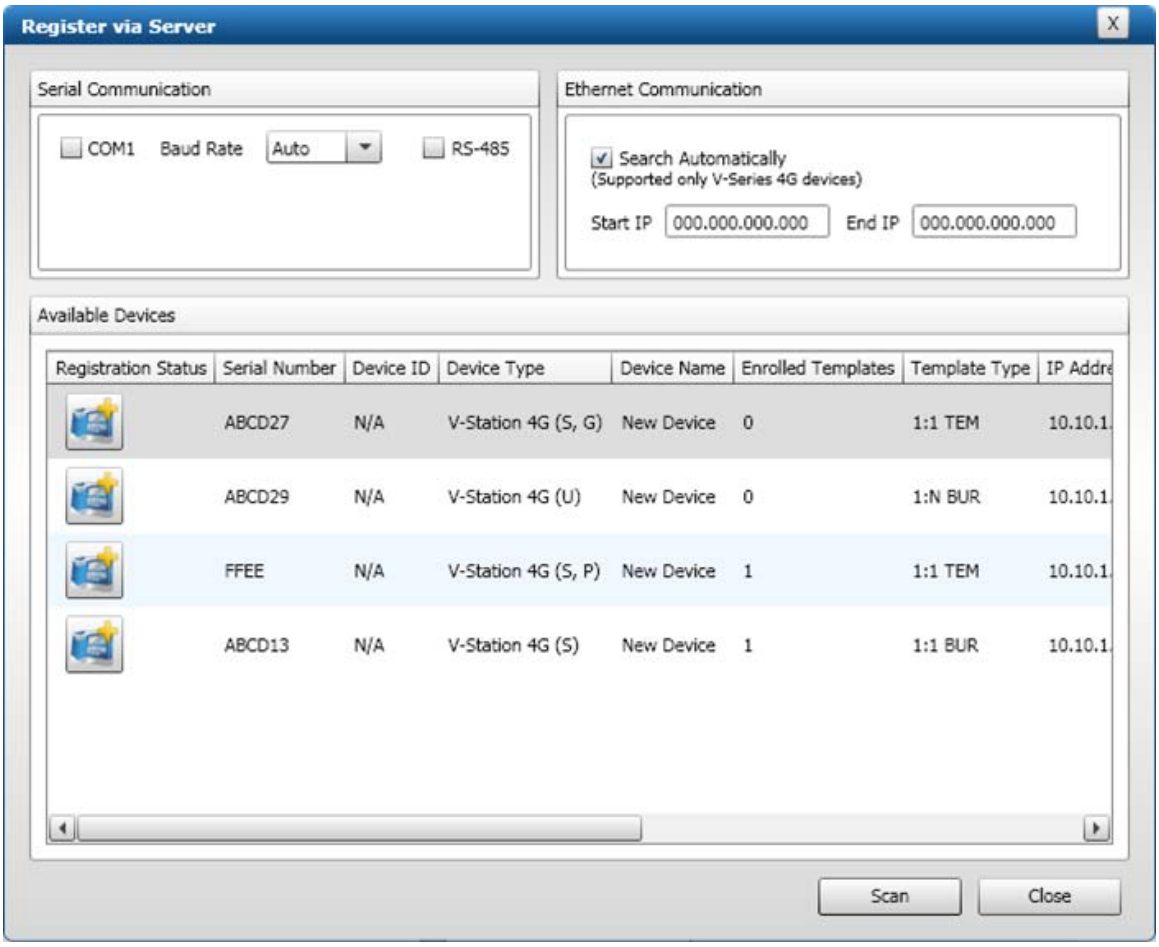
Double-click the **Network** tab. Three buttons are displayed.

Figure 6-1 Network Sidebar Tab



Click the **Register via Server** button. A **Register via Server** dialog box is displayed.

Figure 6-2 Register via Server Dialog Box

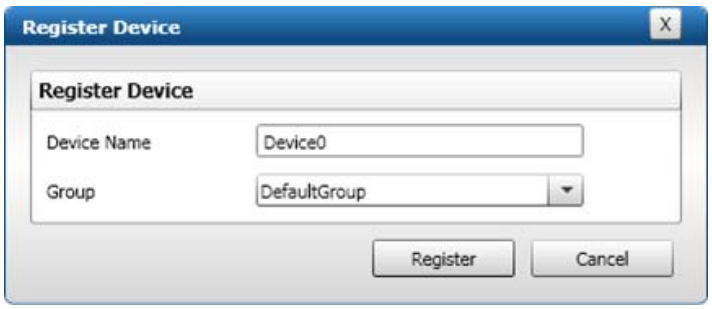


Select the **Search Automatically** check box (UDP protocol must be enabled on the net-work.

Click the **Scan** button. SecureAdmin scans the network for connected devices and lists the results. Devices with "plus" signs in their icon are available to add.

In the list, click the **icon of the device** you want to register. The server communication parameter dialog box is displayed. A **Register Device** dialog box is displayed. Select the **communication parameter** (if connecting via RS-232 or RS-485), enter the appropriate Port, Baud Rate, Device ID, and select the communication protocol from the drop-down. If connecting via enter the network IP address of the device (selectthe DHCP check box if dynnamic IP addressing is used).

Figure 6-3 Register Device Dialog Box

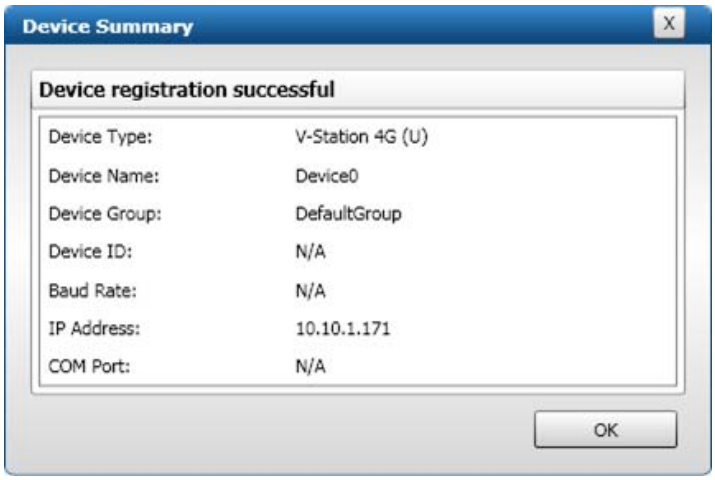


Enter a **Device Name**.

Select a **Group**.

Click **Register**. A Device Summary is displayed.

Figure 6-4 Device Summary Dialog Box



Click **OK**.

Click **Close**. The device is registered.

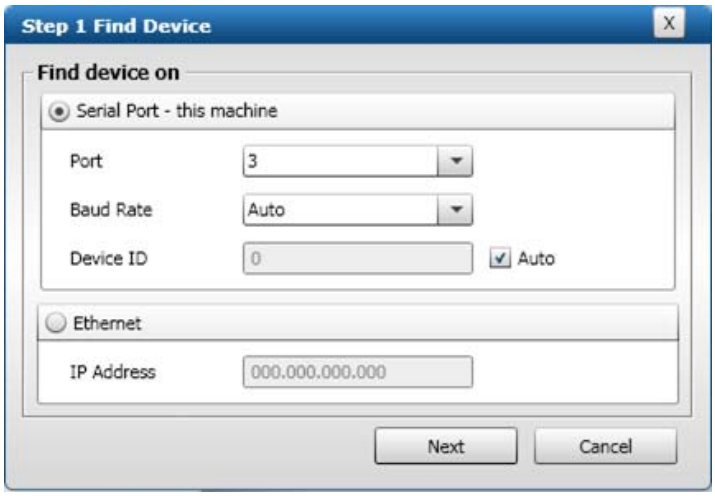
6.1.1.2 TO REGISTER A DEVICE VIA A CLIENT

5. Launch **SecureAdmin**.

Double-click the **Network** tab. Three buttons are displayed.

Click the **Register via client** button. The Step 1 Find Device dialog box is displayed.

Figure 6-5 Step 1 Find Device Dialog Box



Select either **Serial Port - this machine** or **Ethernet** radio button.

Enter the appropriate connection details.

If you are connecting via USB/RS-232:

Enter the appropriate **Port Number** (to determine the correct port number, look in the Win-dows Device Manager for a "Gadget Serial" entry under the "Ports (COM & LPT)" heading), Baud Rate, and Device ID.

If you are connecting via RS-485:

Enter the appropriate **Port Number** (to determine the correct port number, look in the Win-dows Device Manager for your RS-485 entry under the "Ports (COM & LPT)" heading), Baud Rate, and Device ID.

If you are connecting via Ethernet:

Enter the network **IP Address** of the device you want to connect to.

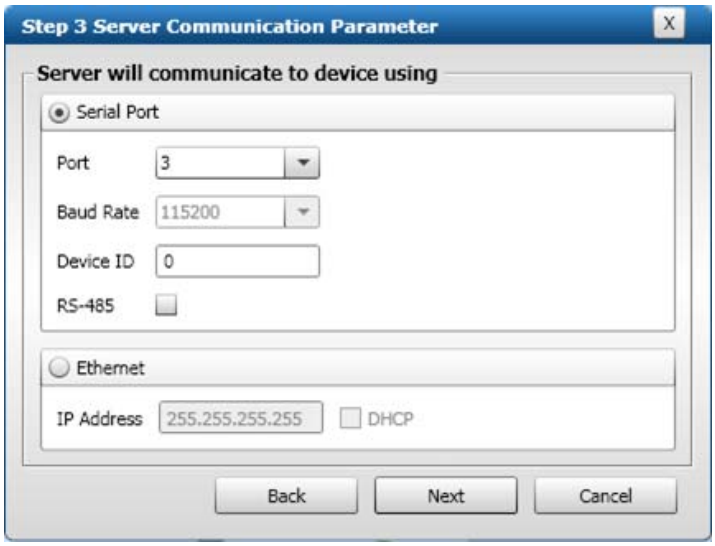
	NOTICE
	The first time a V-Station 4G or V-Flex 4G device is connected to the computer via the USB/RS-232 interface, the Windows Found New Hardware Wizard might start. As all required device drivers are installed when Secu-reAdmin is installed, simply follow the prompts, accepting the default choices when possible, to install the device.

Click **Next**. The Step 2 **Device Information** dialog box is displayed.

Figure 6-6 Step 2 Device Information Dialog Box

Click **Next**. The Step 3 **Server Communication Parameter** dialog box is displayed.

Figure 6-7 Step 3 Server Communication Parameter Dialog Box

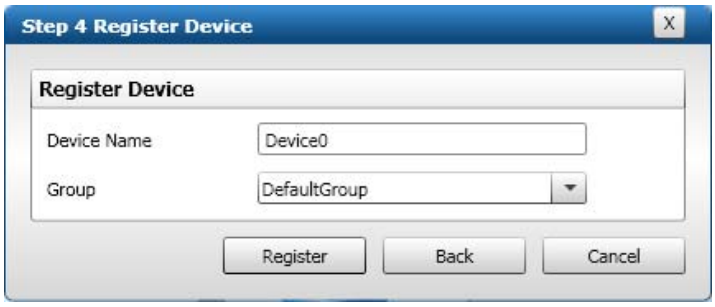


Select the **radio button** that corresponds how the server will connect to the device, either by **Serial Port** or by **Ethernet**.

If connecting via RS-232 or RS-485, enter the appropriate **Port, Baud Rate**, and **Device ID** and select the communication protocol from the dropdown. If connecting via Ethernet, enter the network **IP Address** of the device (select the **DHCP** check box if dynamic IP addressing is used).

Click **Next**. The Step 4 **Register Device** dialog box is displayed.

Figure 6-8 Step 4 Register Device Dialog Box

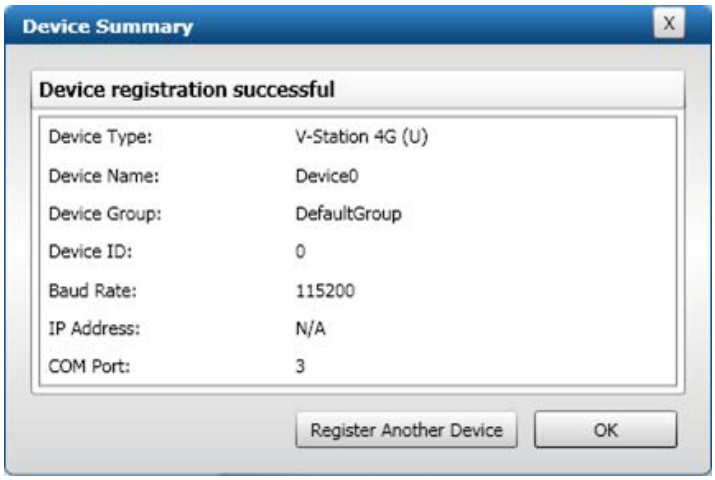


Enter a **Device Name**.

Select the **Group** the device will belong to from the drop-down menu.

Click **Register**. The **Device Summary** dialog box is displayed.

Figure 6-9 Device Summary Dialog Box



CHAPTER 7 - MAINTENANCE AND CLEANING

CHAPTER OVERVIEW

This chapter explains how to replace and calibrate the fingerprint sensor module, and how to clean the device sensor.

7.1 MAINTENANCE AND CLEANING

The V-Station 4G and V-Flex 4G devices require very little in the way of daily maintenance except for occasional cleaning and disinfecting. The V-Station 4G and V-Flex 4G devices feature field-replaceable sensors.

7.1.1 FIELD MAINTENANCE

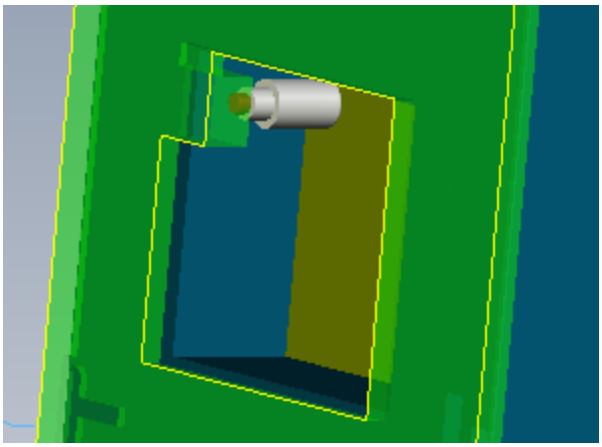
V-Station 4G and V-Flex 4G fingerprint sensors can be replaced quickly and easily in the field. The following sections explain in detail the steps required to replace a sensor.

7.1.1.1 DISARMING THE TAMPER PROTECTION

The Tamper Switch is a momentary push-button switch on the back of the device within the I/O cable interface pocket.

The tamper protection feature allows the device to sound an audio alert, flash LEDs, send a pre-defined Wiegand string to the control panel, or disable biometrics if the tam-per switch is triggered.

Figure 7-1 Tamper Switch Location For V-Station 4G



With the wall mounting plate mounted and the device secured to the mounting plate, the tamper switch is depressed, closing the electrical circuit. When the device is removed from the wall by removing the security screws or in the event that the device is removed from the wall by force, the tamper switch opens.

To access the tamper-protection setting on the V-Station 4G device using the keypad:

Enter the **Admin** menu on the device by pressing the **Left** arrow and **Enter** keys simultaneously.

Key in the **Admin** password (default is "0000") and press OK.

Select the **System** icon and press **OK**.

Select **Device Settings** and press **OK**.

Select **SDC/Tamper Settings** and press **OK**.

Select **Tamper Settings** and press **OK**.

If the alarm has sounded, select **Clear** and **Re-enable**. The Tamper protection setting is set to disabled by default.

7.1.1.2 REPLACING THE SENSOR

WARNING

The sensors can only be replaced with the same type as previously used. L-1 EAS does not support changing the type of sensor. Different types of sensors are not interchangeable, and the device will fail to operate.

NOTICE

- Power to the device MUST BE DISCONNECTED prior to servicing.
- If the device is secured to the wall please be sure to follow the Disable instructions.
- Tamper settings prior to the removal of the device from the wall.
- ESD protective handling procedures must be followed before any service is applied to the device.

7.1.1.2.1 V-FLEX 4G

To replace the sensor module in a V-Flex 4G device, follow these steps:

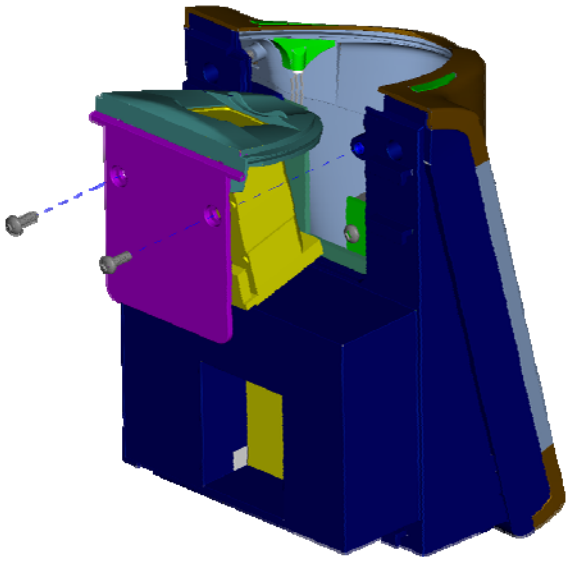
6. Remove the security screw and slide the V-Flex 4G device up until the hooks are free from the wall-mounting plate.

Remove two Philips screws.

Gently slide the sensor back plate, sensor mask, and sensor out of the V- Flex 4G device. Be careful not to damage any internal wiring.

Disconnect the sensor module wiring harness from the internal device connector. It might be necessary to rock the connector back and forth to work it out. Do not pull with excessive force as you might damage the mating connector.

Figure 7-2 Removal of Sensor Module from V-Flex 4G Device

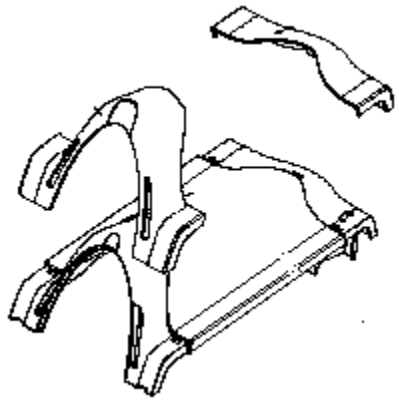


Disconnect the sensor module wiring harness from the sensor module. Do not damage the wiring harness as it will be re-used with the new sensor module.

Reassembly is the reverse of disassembly.

	***CAUTION***
	The parts are assembled at the factory and are not meant to be removed by the end user. Removing any of these parts will void the warranty.

Figure 7-3 Non-Removable Parts (V-Flex 4G)



7.1.1.2.2 V-STATION 4G

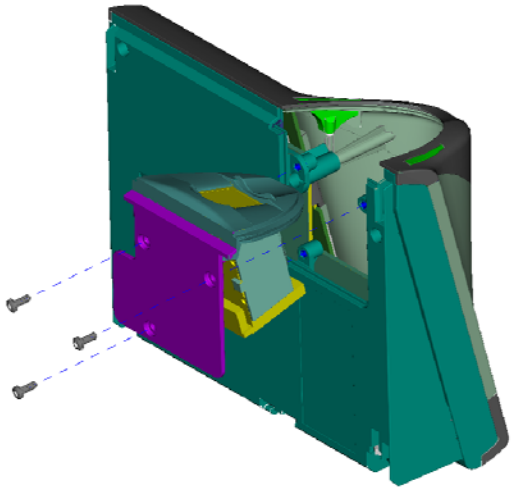
To replace the sensor module in a V-Station 4G device, follow these steps:

7. Remove the security screw.

Tilt the device at an angle approximately 90 degrees to the wall.

Remove the three Philips screws.

Figure 7-4 Removal of Sensor Module from V-Station 4G Device



Gently slide the sensor back plate, sensor mask, and sensor out of the V- Station 4G device. Be careful not to damage any internal wiring.

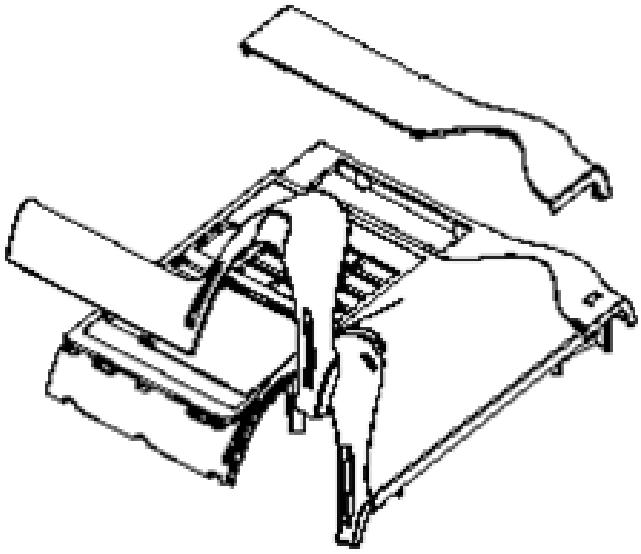
Disconnect the sensor module wiring harness from the internal device connector. It might be necessary to rock the connector back and forth to work it out. Do not pull with excessive force as you might damage the mating connector.

Disconnect the sensor module wiring harness from the sensor module. Do not damage the wiring harness as it will be re-used with the new sensor module.

Reassembly is the reverse of disassembly.

	***CAUTION***
	The parts shown are assembled at the factory and are not meant to be removed by the end user. Removing any of these parts will void the warranty.

Figure 7-5 Non-Removable Parts (V-Station 4G)



7.1.1.3 CALIBRATING THE SENSOR

After a device sensor is replaced, it must be calibrated before it can be used (Only available for UPEK sensors).

To calibrate a device:

8. Select **Sensor Calibration** in the **Tools** drop-down menu. The Calibration Wizard appears.

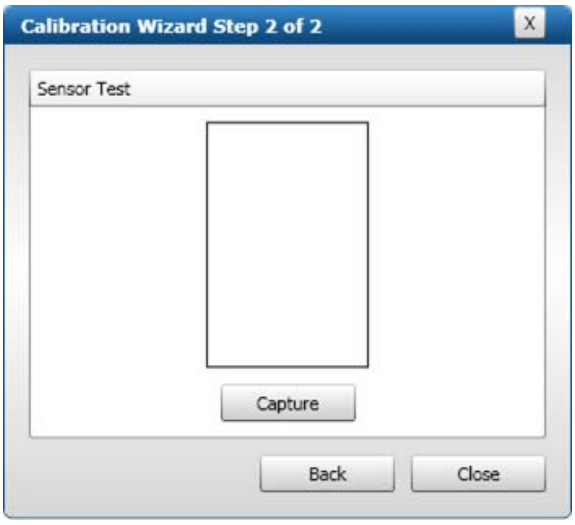
Figure 7-6 Calibration Wizard Step 1 of 2 Dialog Box

Select the device you want to calibrate in the **Current Device** menu.

Click **Calibrate**. Wait as the device sensor is calibrated.

Click **Next.** The **Calibration Wizard Step 2** dialog box is displayed.

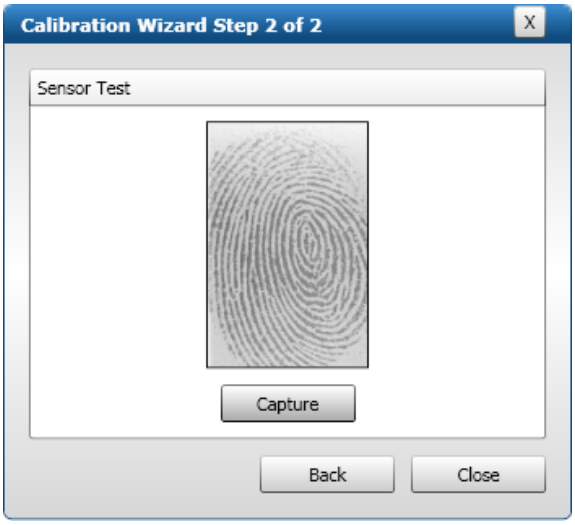
Figure 7-7 Calibration Wizard Step 2 of 2 Dialog Box



Click **Capture**.

Place a finger on the sensor, hold it, and remove it as directed by the on-screen prompts. The capture results are displayed.

Figure 7-8 Calibration Wizard Capture Results Dialog Box



Click **Close**. The device sensor is now fully calibrated and ready to use.

7.1.2 CLEANING

Sensors become soiled with residue, oils, or other contaminants due to contact with fingers and exposure to the elements. The sensor surface should be cleaned periodically for performance, aesthetic, and hygienic reasons. Care must be taken when cleaning the sensor to prevent dam-aging the sensor surface or surrounding components.

To clean the fingerprint sensor in a V-Station 4G or V-Flex 4G device:

9. Remove the electrical power from the device.

Moisten (do not saturate) a clean cotton swab or a lint-free cloth with rubbing (Isopropyl) alcohol.

	CAUTION
	Do not use chlorine-based cleaners, such as bleach, or chlorine-based bath-room or mildew cleaners. Chlorine-based cleaners will not adversely affect the fingerprint sensor, but they could damage the electronic circuitry sur-rounding the fingerprint sensor. Do not use solvents such as acetone, methyl ethyl ketone, lacquer thinner, etc. Solvents will not adversely affect the sensor, but they are likely to damage the reader housing or other peripheral components.

WARNING

Never use products such as abrasive cleaning powders, steel wool, scouring pads, or fine sandpaper to clean the sensor surface. These types of cleaning products will damage the sensor surface.

Rub the sensor surface with the moistened cotton swab or lint-free cloth. Do not allow the cleaning product to drip onto any electronic components near the sensor.

Rub the sensor with a clean dry cotton swab or lint-free cloth to remove any traces of clean-ing product.

Reconnect power to the device.

NOTICE

Disposable ESD-safe wipes, such as ACL Staticide wipes, can be used to disinfect the sensor and buttons on a daily (or even more frequent) basis. Be aware that some wipes might not offer the same cleaning power as the prod-ucts mentioned above and thus should not be relied upon to thoroughly re-move all residue. Use of wipes does, however, helps keep sensor and button surfaces hygienic and makes an excellent complement to periodic cleaning.

CHAPTER 8 - TROUBLESHOOTING

CHAPTER OVERVIEW

This chapter information about any error messages that might be experienced during the installation process.

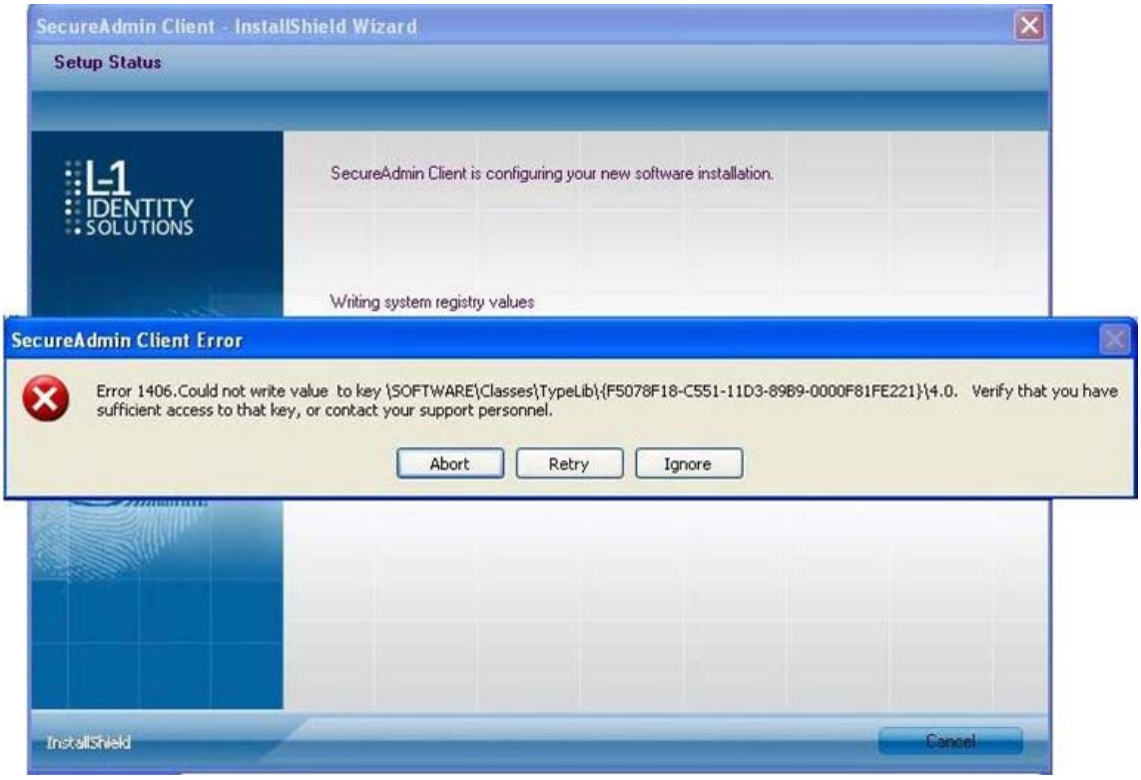
8.1 TROUBLESHOOTING

8.1.1 INSTALLATION ERROR MESSAGES

These error messages might occur during the SecureAdmin installation process.

8.1.1.1 ERROR 1406 - INSUFFICIENT PRIVILEGES

Figure 8-1 Error 1406

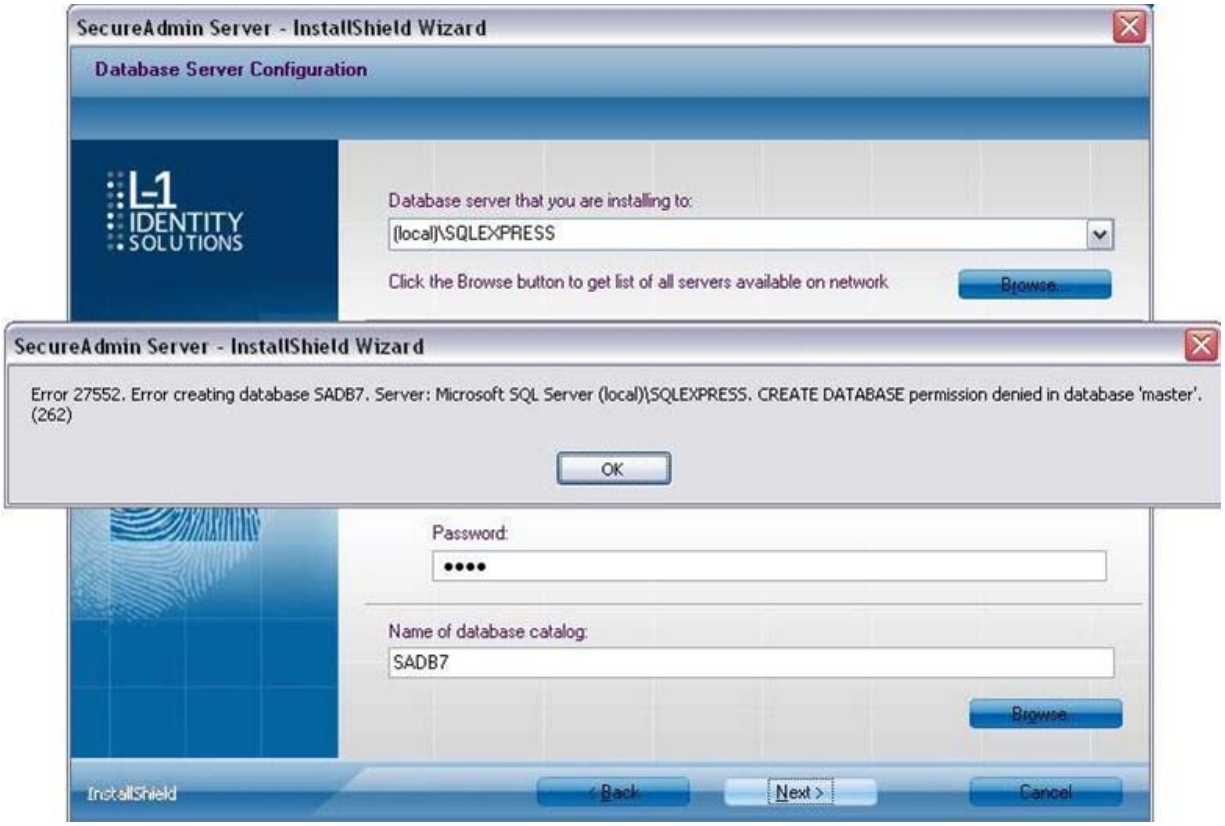


This error can occur during SecureAdmin Client installation at the last step (right before "Finish"). If it occurs, it means that the user does not have sufficient rights to install software on the computer.

Log off and log on either as a Administrator or another user that has sufficient privileges to install software and perform the setup process again.

8.1.1.2 ERROR 27552 - ERROR CREATING DATABASE

Figure 8-2 Error 27552

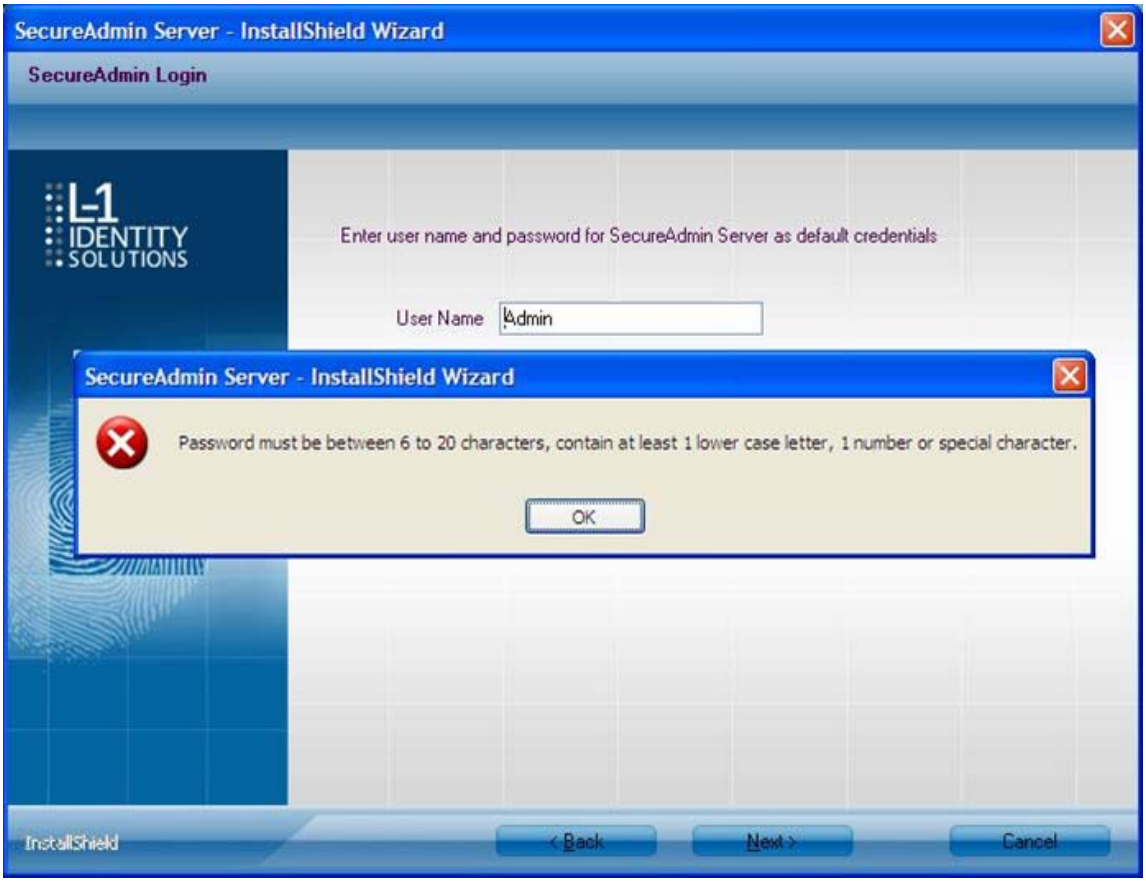


This error can occur during SecureAdmin Server installation process. If it occurs, it means that the user does not have sufficient privileges to access a specific SQL database.

Contact your IT department to ensure that your privileges are correct for the specified database.

8.1.1.3 INVALID PASSWORD

Figure 8-3 Invalid Password

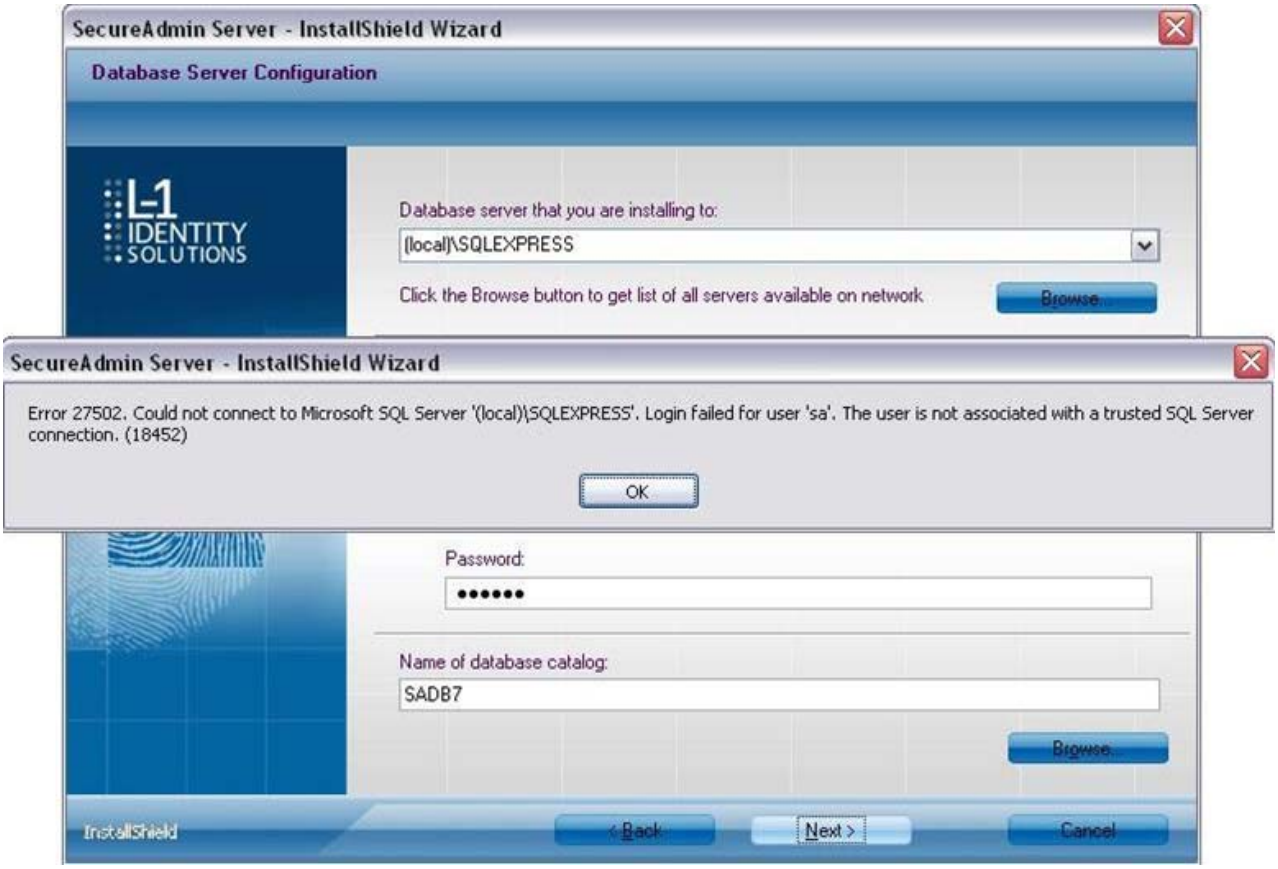


This error can occur during SecureAdmin Server installation process on the User configuration screen (after the database configuration screen).

If it occurs, it means that the password provided is not strong enough. Click OK, and re-enter a password that is considered more secure. The password should be between 8 and 30 characters long and contain at least one capital letter, one number, and one non-alphanumeric character.

8.1.1.4 ERROR 27502 - USER NOT ASSOCIATED WITH TRUSTED SQL SERVER

Figure 8-4 Error 27502 - User Not Associated

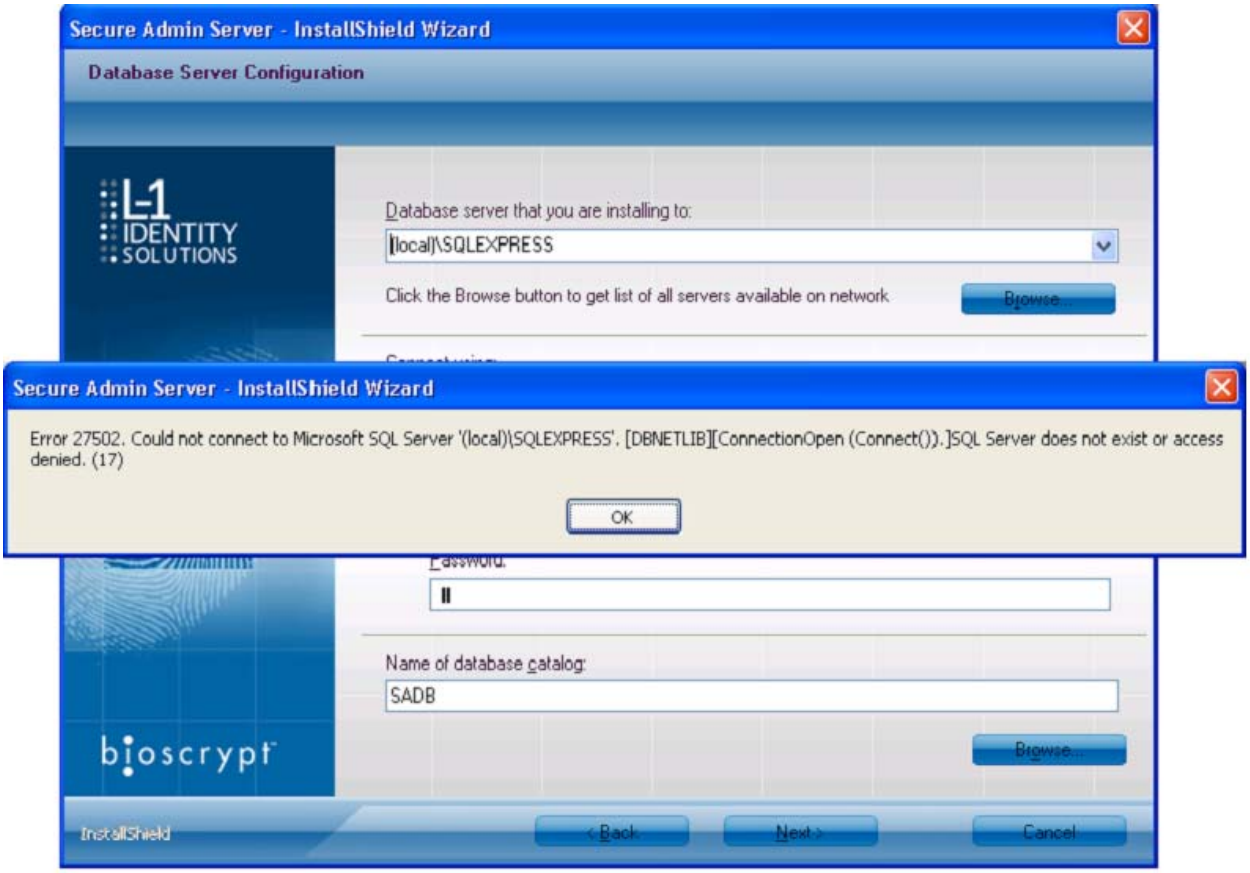


This error can occur during the SecureAdmin Server installation process. If it occurs, it means that the InstallShield Wizard could not access the specified SQL database.

Check your user name and password or contact your IT department to ensure that your user name is associated with the specified SQL database.

8.1.1.5 ERROR 27502 - SQL SERVER DOES NOT EXIST

Figure 8-5 Error 27502 - Server Does Not Exist



This error can occur during the SecureAdmin Server installation process (at the time of database configuration, after the database selection screen). If it occurs, it means that the InstallShield Wizard could not connect to the specified SQL database because it does not exist or because the user is not authorized to access that database

Check your user name and password or contact your IT department to ensure that your user name is authorized to access the specified SQL database.

8.1.1.6 INSUFFICIENT SYSTEM MEMORY

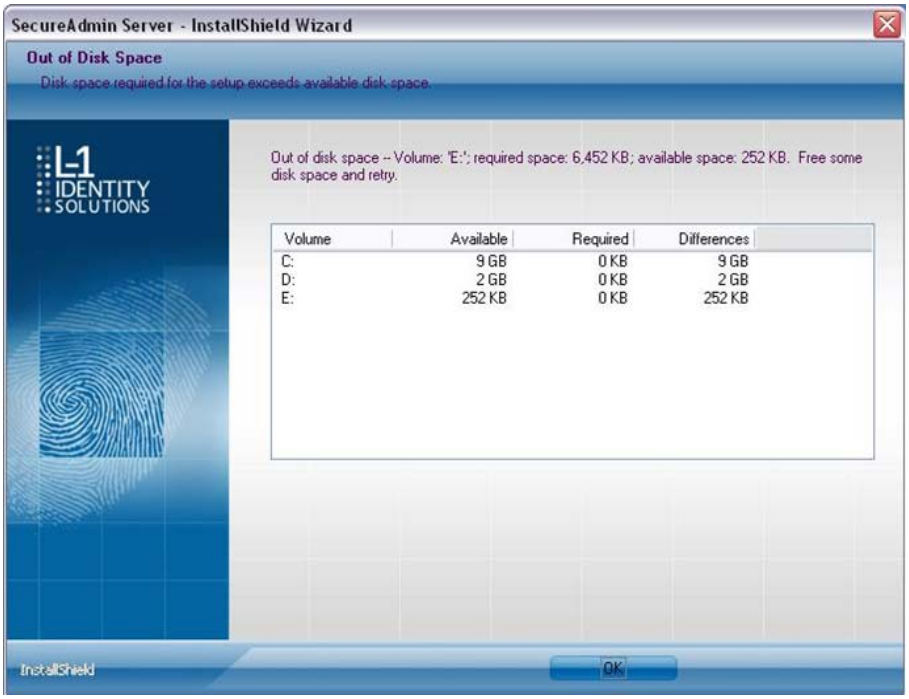
Figure 8-6 Insufficient System Memory

This error can occur during the SecureAdmin Server installation process at the first screen after selecting server installation from the options screen.

If it occurs, it means that the computer you are trying to install SecureAdmin Server on does not have sufficient system memory. Install more memory or install on a different machine.

8.1.1.7 OUT OF DISK SPACE

Figure 8-7 Out of Disk Space



This error can occur during the SecureAdmin Client installation process when Secu-reAdmin starts to configure components, after the fingerprint feedback options selection.

9.1 CHAPTER 9 - NOTICES

The 4G lines of products have been tested for compliance with all applicable international standards. The resulting approvals are listed below, and are additionally printed on the labelling located on the rear panel of the product.

V- Flex 4G	FCC, CE
V- Station 4G	FCC, CE
PIV-TWIC Station 4G	FCC, CE

9.1.1 FCC Information to Users

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTICE

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- ✓ Reorient or relocate the receiving antenna.
- ✓ Increase the separation between the equipment and receiver.
- ✓ Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

This Class B digital apparatus complies with Canadian ICES-003.

Applicable only to V-Station 4G and PIV-TWIC Station 4G series product: This product complies with FCC radiation exposure limits set forth for an uncontrolled environment. To comply with FCC RF exposure requirements, it must be installed and operated in accordance with provided instructions. The unit requires minimum 20cm (8inch) spacing between the unit and all person's body (excluding hands and feet) during wireless modes of operation.

9.1.2 CE Information to Users

All Veri-Series 4G devices have the CE mark, for compliance with CISPR22/EN55022 requirements. For European Union (EU) countries, V-Flex 4G and V- Station 4G are

compliant with CE under the R&TTE Directive, related to the radio transceivers that are part of their design.

9.1.3 Warning to Users

	***CAUTION***
	Changes or modifications not expressly approved by L-1 Identity Solutions Inc. could void the user's authority to operate the equipment.