AdderView Secure

{ AVSV1002 (2 port)
  AVSV1004 (4 port)
  AVSC1102 (2 port)
  AVSC1104 (4 port)

User Guide

ADDERVIEW
SECURE

CONTENTS

Contents

Welcome

Installation

Operation

Further information

IMPORTANT: Before using this product

Prior to use, a prospective user of the product should ensure that individuals with the appropriate authority implement the following objectives in the environment where the product is to be used:

- The operational environment procedures must ensure that all users are duly authorized and possess the necessary privileges to access the information transferred via the product. This should be implemented physically and in terms of supporting IT infrastructure.

- Operational procedures must (e.g. re staff vetting and training) ensure that, as far as is reasonably possible, the product is received, installed and managed in accordance with the manufacturer's directions. This should also ensure that users are not malicious or hostile.

- The product should be installed in an environment that is physically secure.

Additionally, the security office in the organisation purchasing the product should be aware the product is not responsible for security vulnerabilities in computers, IT components or peripherals outside its physical boundary. The security of other system components connected to the product will require separate management to ensure IT security best practice.

Welcome

Introduction

The AdderView Secure range of products are highly robust KVM switches for critical applications. When information absolutely must not be leaked between systems or networks, the AdderView Secure units combine the necessary isolation with a desirable ease of use.

AdderView Secure units combine a number of overlapping strategies that are designed and proven to defeat potential points of infiltration or protect against user error.

Firstly, all channel switching is controlled only from the front panel buttons. No keyboard or mouse switching commands are permitted.

Secondly, *Data Diodes*, implemented within hardwired electronic circuitry, rather than software, are liberally employed to ensure that critical data paths can flow only in one direction. These data diodes ensure that a compromised peripheral, a keyboard for instance, cannot read information back from a connected system in order to transfer such details to another system. Whenever a channel is changed, the connected keyboard and mouse are always powered down and re-initialized to provide yet another level of protection against hidden peripheral malware.

In general, the role of software within the unit has been reduced to an absolute minimum to avoid the possibility of subversive reprogramming. Additionally, all flash memory has been banished from all security critical areas of the design, to be replaced by one-time programmable storage which cannot be altered.

The outer casing contains extensive shielding to considerably reduce electromagnetic emissions. Additionally, the casing has been designed with as few apertures as possible to reduce the possibility of external probing and several primary chassis screws are concealed by tamper-evident seals to indicate any unauthorized internal access. Shielding extends also to the internal circuitry with strong levels of electrical crosstalk isolation between ports to protect against signals from one computer becoming detectable on another.

AdderView Secure units are available in two port and four port sizes. Each size can be ordered in standard and enhanced versions. The enhanced versions allow you to attach a smart card reader that can be securely shared between the connected systems. The enhanced versions also contain anti-subversion and authentication features that guard against intrusion and allow you to prove that the unit is genuine, respectively.
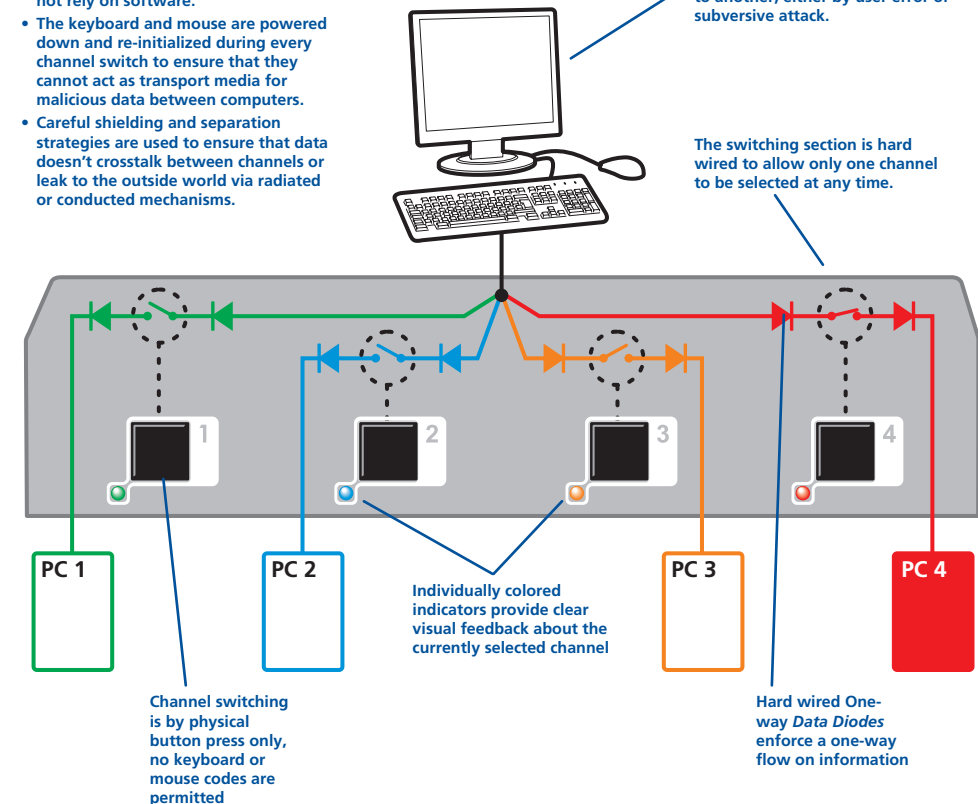
These are just a few of the many strategies and innovations that have been combined to reinforce the separation between differing systems. Numerous other defences lie in wait to defeat any potential threat.

Various strategies are employed to ensure complete separation between the switched channels:
- One-way *Data Diodes* are used on keyboard and mouse communication channels so that data isolation does not rely on software.
- The keyboard and mouse are powered down and re-initialized during every channel switch to ensure that they cannot act as transport media for malicious data between computers.
- Careful shielding and separation strategies are used to ensure that data doesn't crosstalk between channels or leak to the outside world via radiated or conducted mechanisms.

Common keyboard, mouse and video monitor are able to access multiple high security computers/networks, safe in the knowledge that data will not be transferred from one to another, either by user error or subversive attack.

The switching section is hard wired to allow only one channel to be selected at any time.

Channel switching is by physical button press only, no keyboard or mouse codes are permitted

Individually colored indicators provide clear visual feedback about the currently selected channel

Hard wired One-way *Data Diodes* enforce a one-way flow on information

PC 1

PC 2

PC 3

PC 4

3

Model features

There are four models within the AdderView Secure range. Their varying features are summarized as follows:

|	Standard 2-port AVSV1002-XX	Standard 4-port AVSV1004-XX	Enhanced 2-port AVSC1102-XX	Enhanced 4-port AVSC1104-XX
Uni-directional keyboard / mouse data paths	✓	✓	✓	✓
High port-to-port crosstalk isolation	✓	✓	✓	✓
Heavy shielding for low emissions	✓	✓	✓	✓
Single key per port for selection	✓	✓	✓	✓
USB or PS/2 computer connections	✓	✓	✓	✓
Tamper protection	✓	✓	✓	✓
Secure DDC EDID strategy	✓	✓	✓	✓
Smartcard reader support			✓	✓
Combined keyboard/smartcard reader support			✓	✓
Advanced tamper protection / reporting			✓	✓
Authentication function			✓	✓

AdderView Secure - front and rear layout

The AdderView Secure is housed in an electromagnetically shielded robust casing that measures just [w x d x h] 9.25" x 5.9" x 1.73" (235mm x 150mm x 44mm) - the height is 1U within a 19" rack. All channel switching is achieved solely using the front panel buttons which are clearly indicated, as are the rear panel connections.

Secure and shielded casing
The casing is shielded to reduce electromagnetic emissions to an absolute minimum, access apertures are minimized and vital access screws have tamper-evident seals.
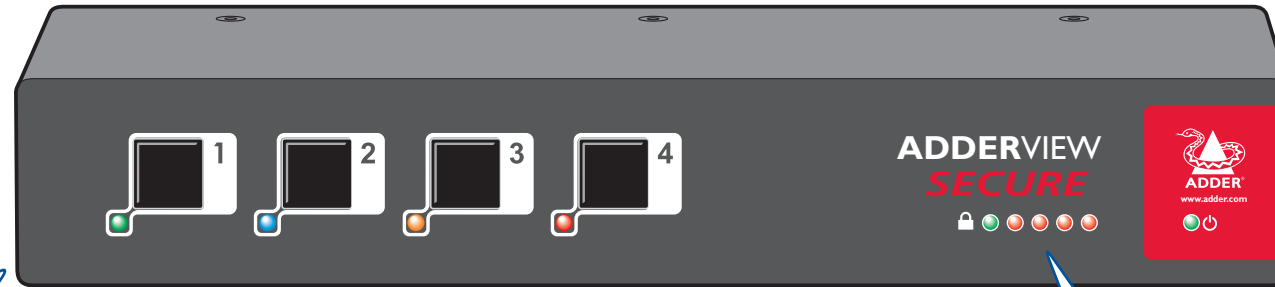
2 port version
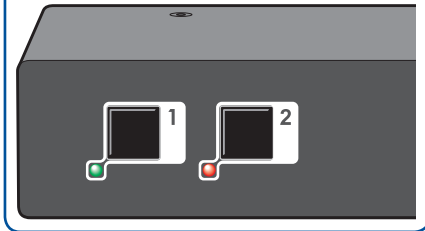
Switching is controlled solely by the clearly labeled front panel buttons
Each selected channel is represented by an individually colored indicator to provide additional visual feedback.

Clear error indication
On enhanced models, any unexpected operation will be signalled by these indicators, accompanied by complete isolation of all channels. See Anti-subversion monitoring for details. The indicators are also used when authenticating enhanced models.
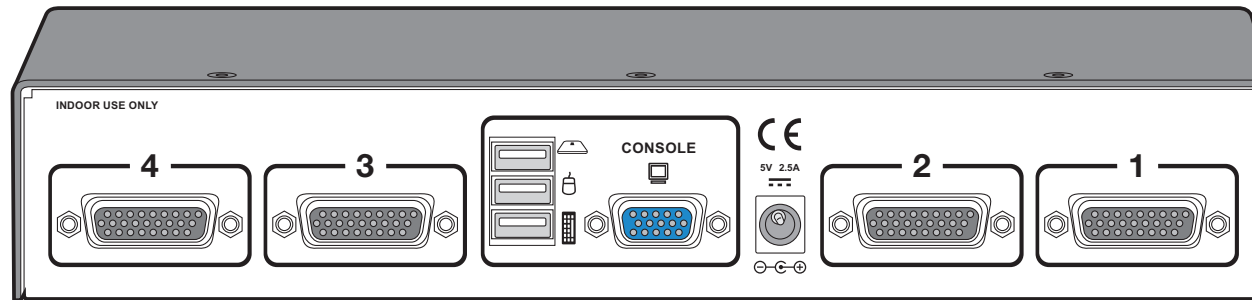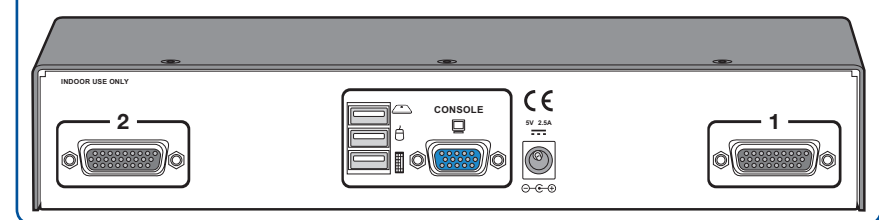
Optional smart card reader
An optional smart card reader can be connected and used in conjunction with user authentication schemes.

Clear and simple connections
All connections are clearly marked to avoid any ambiguity. Specially designed foil and braid shielded multi-connection cables are used for the system links.

2 port version

INDOOR USE ONLY

CONSOLE

5V 2.5A

Devices used with the AdderView Secure

Keyboard devices

The keyboard used with the switch must be approved against the security policy of your organization and must be plugged directly into the switch's USB keyboard port with no adapters or converters.

During the life of the product, the user should make periodic checks to ensure that the keyboard remains directly connected into the switch's USB keyboard port.

The keyboard is powered down and reset at every switchover to clear stored states.
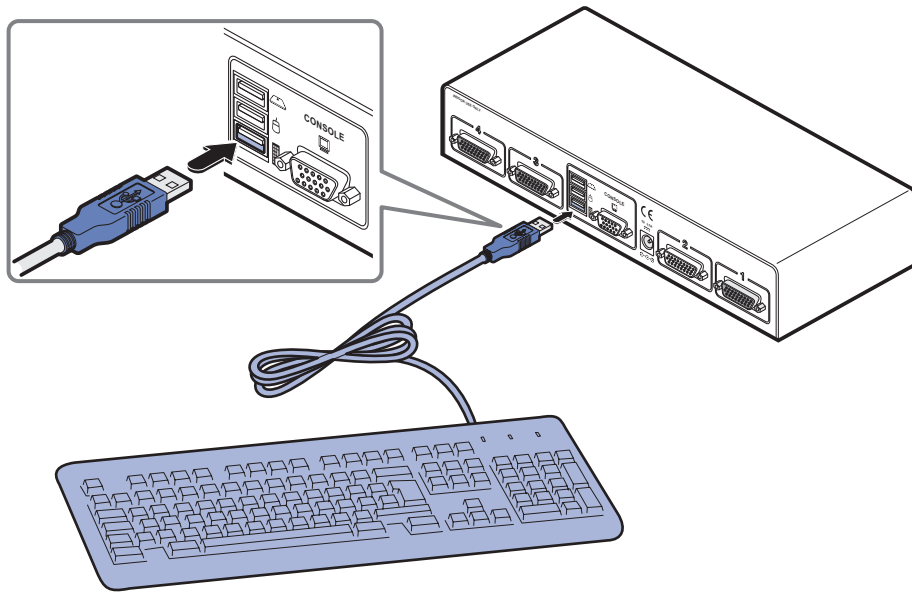
Mouse devices

Although pointing devices don't generally process confidential data and are therefore considered to pose a lower risk, you should ensure that the mouse used with the switch is approved against the security policy of your organization and plugged directly into the switch's USB mouse port with no adapters or converters.

The mouse is powered down and reset at every switchover to clear stored states.
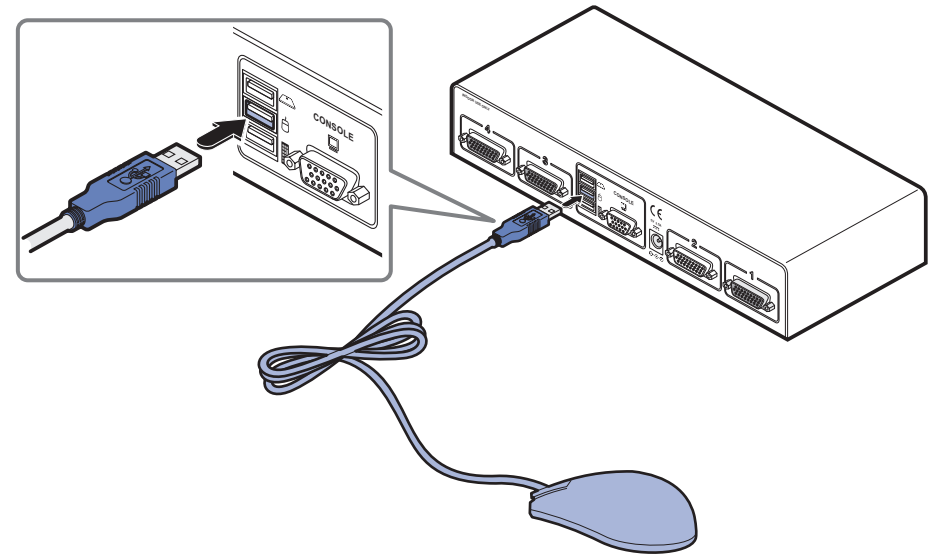
Smartcard devices (supported only on enhanced models)

The smartcard reader and smartcards, used with enhanced models of the switch (AVSC1102-XX and AVSC1104-XX), must be approved against the security policy of your organization. The smartcard reader must be plugged directly into the switch's USB card reader port with no adapters or converters. The smartcard reader is powered down and reset at every switchover to clear stored states.

Smartcards may contain memory that can be both readable and writable. Care must therefore be taken when configuring a system using smartcards.

The smartcard system inside the switch is designed to introduce no greater risk than would be present if each computer had a separate card reader and the card was moved between them. To achieve this, the switch provides a layer of isolation between the computers and the shared card reader. This protects against threats involving sharing a physical card reader hardware device. As an additional precaution against theoretical leakage threats, the circuitry associated with providing the generic card reader function is powered down and its memory is actively cleared at every channel switchover. The switch does not decode or store the smartcard data flowing between the computer and the smartcard itself.
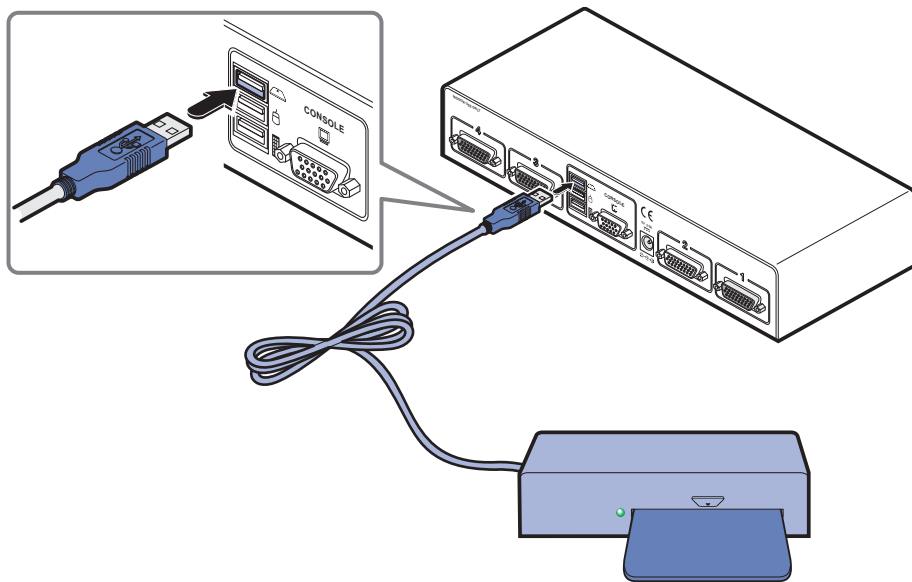
Note: Standard models of the switch (AVSV1002-XX and AVSV1004-XX) also have a smartcard USB socket at the rear panel (labeled ⬜), however, it is not functional on these models.

When using enhanced models, if smartcard capabilities are not required for a particular computer, then use a non-smartcard cable (without the yellow smartcard connector). This will ensure that the computer does not see any smartcard reader function as all the smartcard functionality is presented to the computer on the yellow USB connector only. Any computers that would not normally have card readers connected should not be connected to the switch using the yellow USB connector.

Smartcard access required?: ✓
Use cable set: **VSCD6**
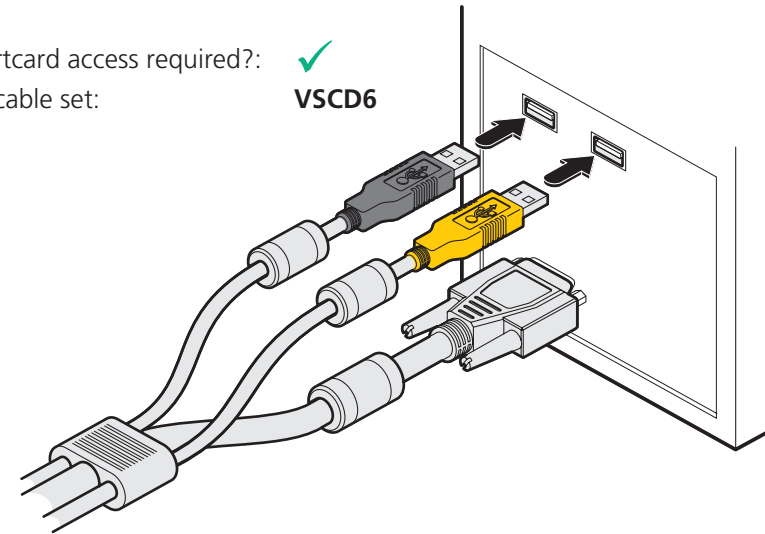
Smartcard access required?: ✗
Use cable set: **VSCD7**

7
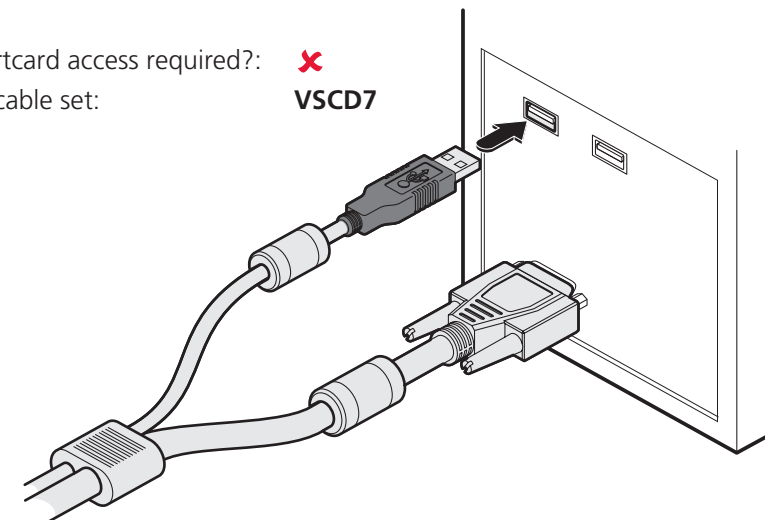
Keyboards with integrated smartcard readers
(supported only on enhanced models)

A combined keyboard/smartcard reader (and smartcards), used with enhanced models of the switch (AVSC1102-XX and AVSC1104-XX), must be approved against the security policy of your organization. The combined keyboard/smartcard reader must be plugged directly into the switch's USB card reader port with no adapters or converters.

During the life of the product, the user should make periodic checks to ensure that the combined keyboard/smartcard reader remains directly connected into the switch's USB smartcard port.

The combined keyboard/smartcard reader is powered down and reset at every switchover to clear stored states.

The keyboard data and smartcard data are separated from each other as soon as they enter the switch. The keyboard data is then sent uni-directionally through the switch in the same way that data from a simple keyboard is processed. Only the smartcard data is handled by the smartcard circuit.
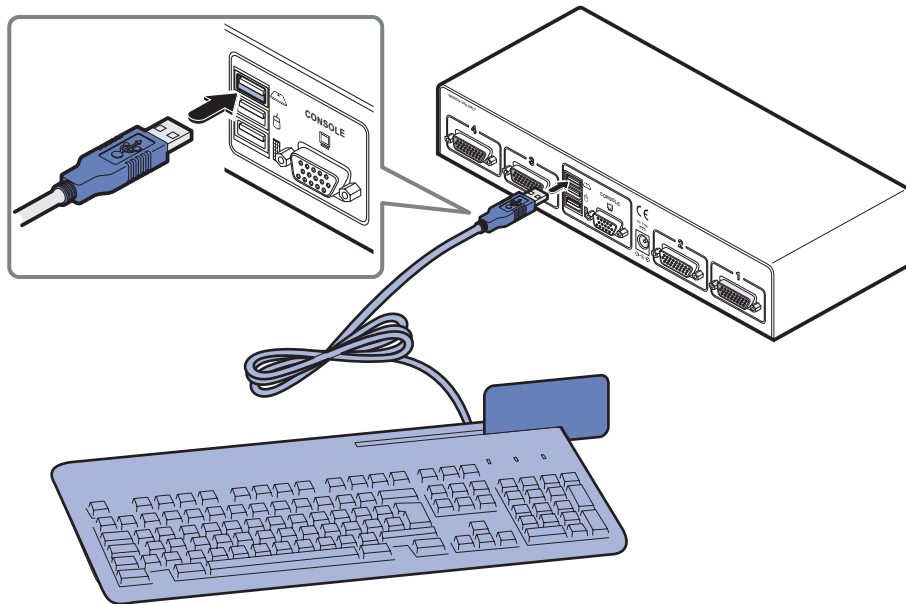

Note: Standard models of the switch (AVSV1002-XX and AVSV1004-XX) also have a smartcard USB socket at the rear panel (labeled ⌨), however, it is not functional on these models.

Standard items
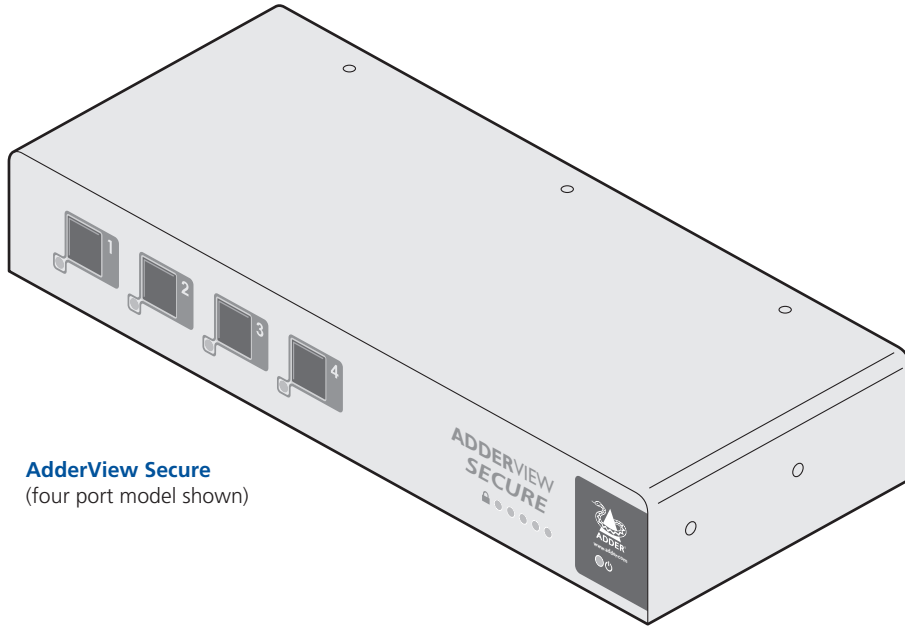
AdderView Secure
(four port model shown)
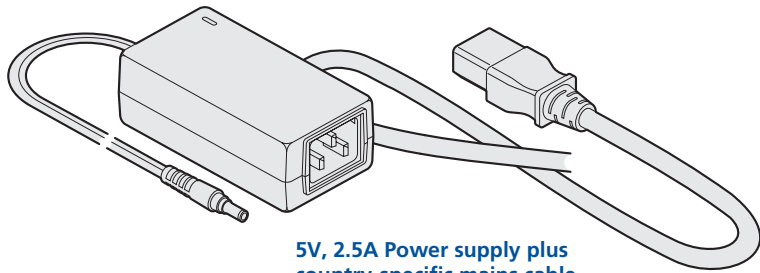
5V, 2.5A Power supply plus country-specific mains cable
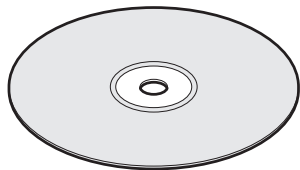
CD-ROM

Four self-adhesive rubber feet

Additional items

Shielded link cable (VGA, PS/2 keyboard, PS/2 mouse)
Part code: VSCD5 (length 1.8m/6ft)
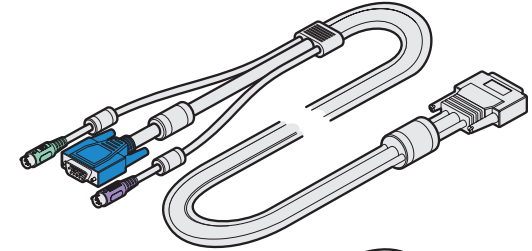
Shielded link cable (VGA, USB keyboard/mouse, USB card reader)
Part code: VSCD6 (length 1.8m/6ft)
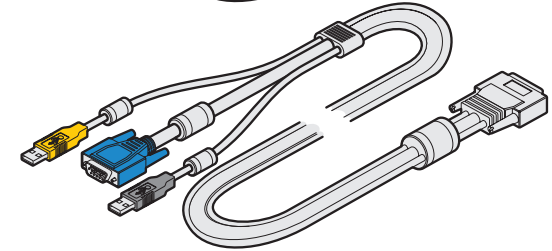
Shielded link cable (VGA, USB keyboard/mouse)
Part code: VSCD7 (length 1.8m/6ft)
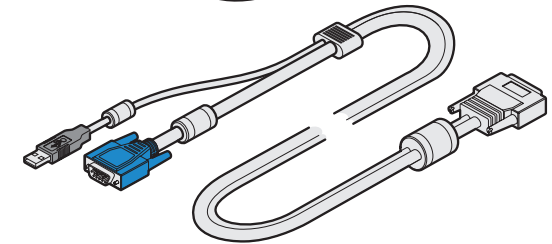
Shielded link cable (VGA only)
Part code: VSCD9 (length 1.8m/6ft)
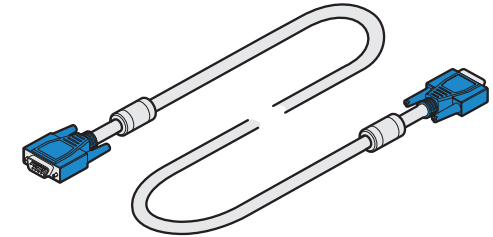
Rack brackets
Including four screws
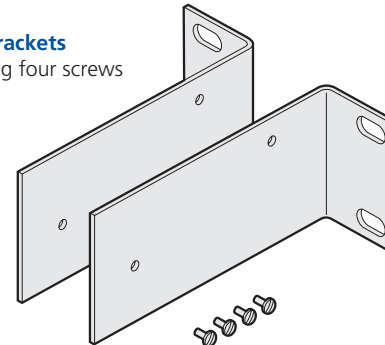
Installation

Locations

Please consider the following important points when planning the location of the AdderView Secure unit:

- Situate the unit close to the host computers to which it will be connected and also the user console peripherals.
- The unit requires a power supply input, so a nearby spare mains power outlet will be required.
- As keyboard and mouse switching codes are not possible for security reasons, the only way to change channels is via the front panel buttons. Therefore, the unit should be easily accessible from the user's normal position.
- Please consult the precautions listed within the Safety information section.

Cabling recommendations

The special cables available for connections to each system are carefully constructed with braid and foil to provide excellent screening against signal emissions that could otherwise be eavesdropped. A similarly constructed cable is also available for the monitor connection (VSCD9).

The special cables already have ferrite cores fitted to assist with signal suppression. For USB peripheral connections, we strongly recommend that (if not already fitted) you attach ferrite cores to those cables to further assist with emission suppression.

Tamper-evident seals

The primary casing access screws are pre-fitted with tamper-evident seals. It may be a policy of your organisation to fit proprietary tamper-evident labels across certain chassis screws. Additionally, seals could be added between each connection and the unit to highlight any connections that have been altered.

IMPORTANT: Do not use the unit if the tamper-evident seals are damaged. Do not use if there are any signs of damage to the unit or its power supply.

Links overview

The rear panel of the unit is well marked, however, the diagram below offers additional clarity on how best to arrange your connections.

You may have noticed that the indicators on the front panel use different colors to represent the various channels. This is done to provide quick and effective visual feedback to the operator. Channel 1 has a green indicator and is traditionally used for the lowest security connection. The final channel, numbered 2 on the two port version and 4 of the four port version, uses a red indicator and is usually connected to the highest security connection. These are configuration conventions only and are offered as a suggestion - there are no technical differences in the operational specifications of the four channels.

Channel 4 or channel 2 on two channel models (red indicator) Usually used for connection to the highest security computer/network.

Channel 3 (amber indicator)

Console connections Connect directly to the operator's keyboard, mouse, video display and card reader (if used).

Channel 2 (blue indicator)

Channel 1 (green indicator) Usually used for connection to the lowest security computer/network.

WARNING: Do not open the case of the switch or remove any screws (other than the rack mounting screws, if fitted) - the switch will become unusable if the case is opened.

Mounting

The AdderView Secure unit offers two main mounting methods:

• Supplied four self-adhesive rubber feet

• Optional rack brackets

CONTENTS

WELCOME

INSTALLATION

OPERATION

FURTHER
INFORMATION

Making connections

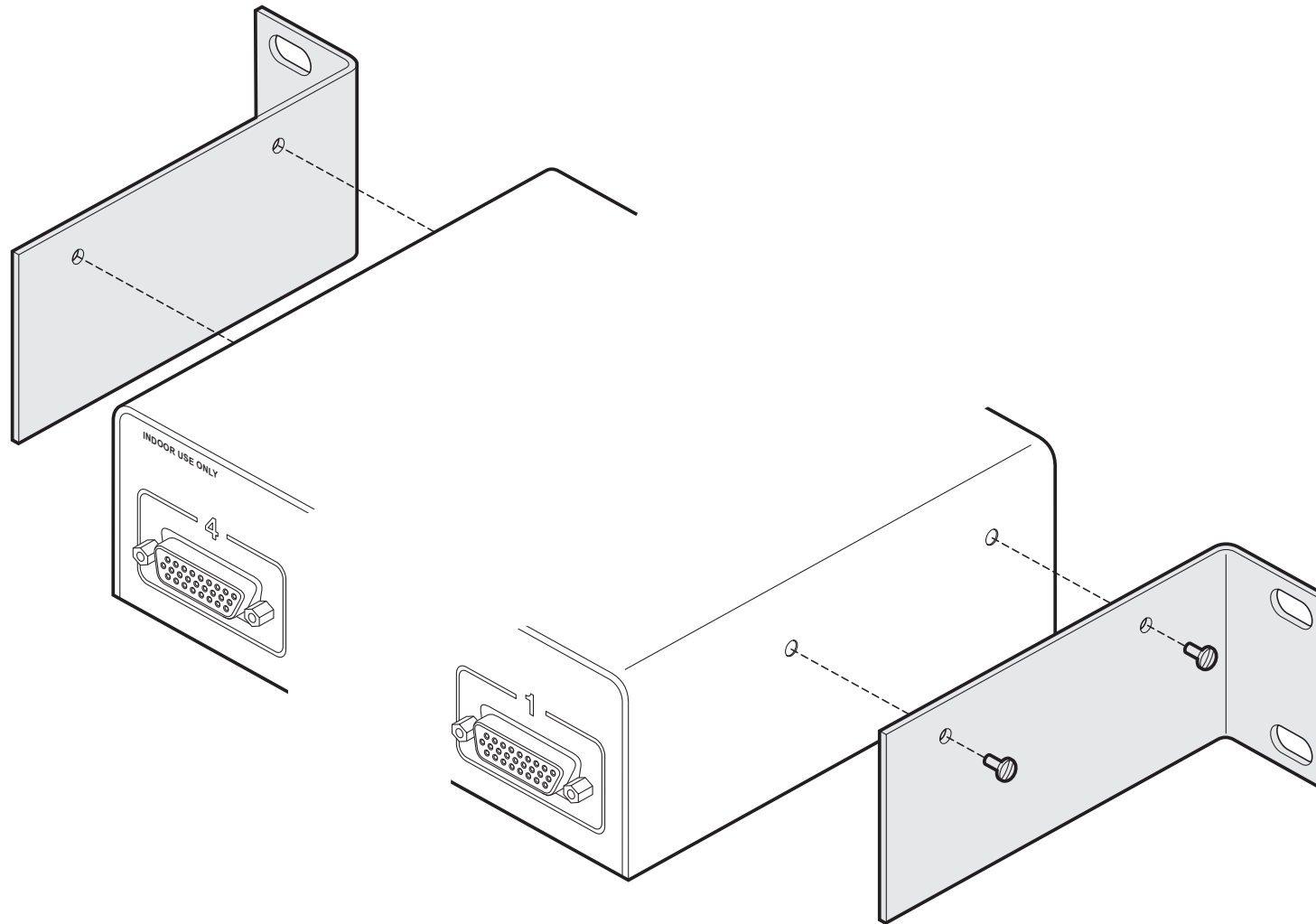Connections to the AdderView Secure unit do not need to follow the precise order given in this user guide, although if one or more systems must be hot-plugged, connect these after all other connections have been made.

IMPORTANT: To achieve the high levels of signal isolation and low emissions profile that the switch is capable of delivering, it is necessary to use the only the cables listed in the Additional items *section. These have been very carefully designed and tested to maximize the performance levels of the switch.*

Note: For additional security, use tamper-evident tape to bridge the computer cable connections to the switch's case once installed.

Connections to computer systems

All connections to computer systems are achieved using combined shielded link cables of which there are several different types to suit the various ports used - see the Additional items section for details.

See also Devices used with the AdderView Secure for advice about linking devices to the AdderView Secure unit.

To connect a system link

1 Wherever possible, ensure that power is disconnected from the unit and the host computer(s) to be connected.

2 At the rear panel of the unit, connect the appropriate link cable to the 26-way connector of the appropriate channel.
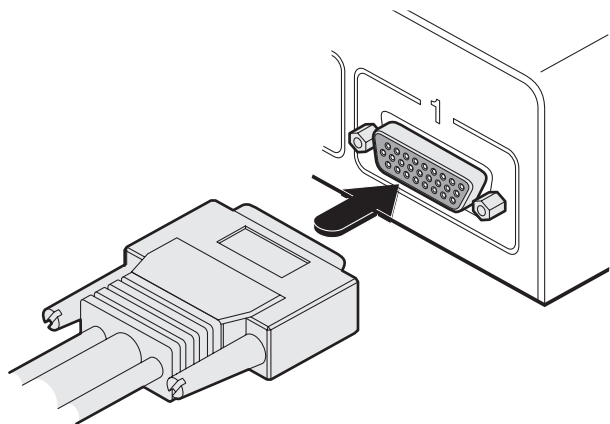
3 Attach the connectors at the other end of the link cable to the appropriate ports of the computer, i.e. VGA video, USB (or PS/2 keyboard and mouse) and the smart card reader, if used - see below.

IMPORTANT: If only certain computers require the use of the smart card reader, for those systems use a link cable that has only one USB connector - do not leave a spare USB link unconnected.

Connections to user console peripherals

To connect a keyboard and mouse
IMPORTANT: To reduce the risk of radiated snooping, do not use wireless keyboard or mouse devices.

See also Devices used with the AdderView Secure for advice about linking devices to the AdderView Secure unit.

1 Wherever possible, ensure that power is disconnected from the unit and the host computer(s) to be connected.

2 In the middle of the rear panel, connect the cables from the keyboard and mouse to the USB sockets marked ⌨ and 🖱 respectively.

Note: If using a combined keyboard and smartcard reader then connect the keyboard/reader to the socket labeled ⌨. Any keyboard connected to the keyboard socket should then be removed as it will become non-functional).
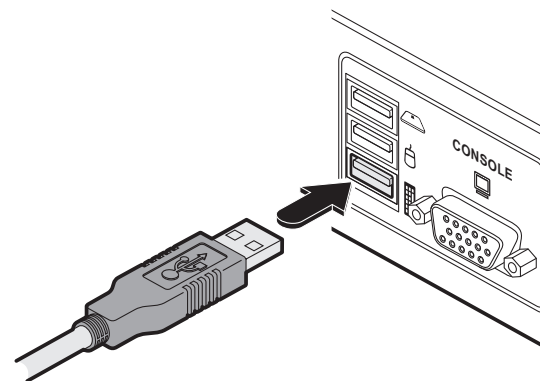
3 If using a smart card reader, connect the cable from the reader to the USB socket labeled ⌨.

Note: The smartcard port is not active on standard models (AVSV1002-XX and AVSV1004-XX) which do not contain smartcard circuitry.

To connect a display monitor

1 Wherever possible, ensure that power is disconnected from the unit and the host computer(s) to be connected.

2 Connect a suitable VGA video display to the port labeled ▢ within the Console section on the rear panel. Ensure that the securing screws are used to maintain reliable links.

Note: We strongly recommend that you use a video cable that has been correctly screened against signal emissions (such as the VSCD9 cable).
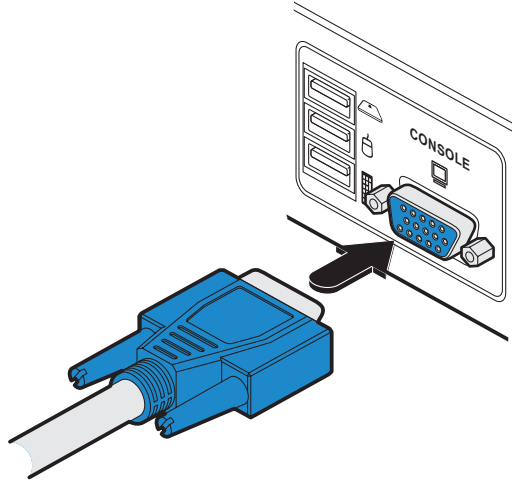
Note: The use of EDID information (automatically provided by the video display) could cause issues in certain high security installations - please see the Video display (EDID) information section for further details).

Video display (EDID) information

The Display Data Channel (or DDC) communication scheme was introduced to allow video displays to provide details (using the information format of EDID - Extended Display Identification Data) about themselves and their capabilities to the computer's graphic adapter circuitry. In most applications this is a useful and positive feature. However, in a highly secure environment this presents two potential problems:

- Most video displays provide manufacturer, model and serial number information as part of their EDID transfer. This unique information could possibly be used as a marker by anyone attempting to compromise security within one or more of the connected computers/networks.

- The operation of the DDC scheme could theoretically provide a means to transfer a small packet of EDID information to the computers at each power on cycle of the AdderView Secure.

If your organisation wishes to protect against such scenarios then it is recommended that the DDC lines are disconnected in the cable between the AdderView Secure and the monitor. Alternatively, Adder would be happy to discuss configuring the AdderView Secure with a DDC policy to suit your organisation.

AdderView Secure EDID policy
The AdderView Secure maintains individual EDID memories for each connected computer port. During manufacture, these memories are each loaded with a default EDID packet.

When the AdderView Secure is powered on, its response will be determined by the condition of the DDC signalling pins of the video monitor connector:

- **If the DDC pins are connected as standard**: The AdderView Secure reads the EDID information from the attached video monitor and loads a copy into each port memory, which can then be made available to the connected computers.

- **If no video monitor is connected or the monitor's DDC signalling pins are disconnected**: The AdderView Secure will maintain the existing data held in the EDID memories and make them available to the computers.

- **If the video monitor's DDC signalling pins have been connected to ground**: The AdderView Secure will load a set of default data to the EDID memories and no data will be made available to the computers. This provides a means of clearing information about previously attached monitors.

Note: Most analog video cards will output a video signal without EDID information. In such installations it may be acceptable to disconnect the DDC connections from the AdderView Secure so that no EDID information is made available to the computers. However, some graphics cards will not output a video signal unless they can read the EDID information.

To determine how EDID information is used
Note: The information given here is provided purely as an overview. It is beyond the scope of this document to provide detailed instructions on how to modify video display cables, which should only be attempted by a qualified engineer.

If the transfer of EDID information is unsuitable for your installation, you can take steps to bypass or disable its use. EDID information is sent from the video display on the following pins of the connector:

- VGA (15-pin D-type) connector: pins 12 and 15

As mentioned earlier, the AdderView Secure unit responds in the different ways, depending upon how the DDC data lines within the video display cable have been wired:

DDC pin conditions	AdderView Secure unit response
Connected	EDID information is harvested from the connected video display during unit power on and written to all computer port memories.
Not connected	Unit retains the EDID information that is already held in the port memories and continues to present them to the attached computers. No new EDID information can be sought from the currently connected video display.
Grounded	Unit overwrites all EDID information held in memory with default information but does not present anything to the attached computers.

In situations where no EDID information is being supplied, it may be necessary to use a special driver on the connected computers to inform their graphic adapters on the appropriate signals to send.

Alternatively, a 'surrogate' video display of the appropriate type could be temporarily connected to the AdderView Secure unit in order to harvest the necessary EDID information. The surrogate video display could then be replaced by the real one, which has its DDC pins disconnected (not grounded).

Connection to power supply

Important: Please read and adhere to the electrical safety information given within the Safety information *section of this guide. In particular, do not use an unearthed power socket or extension cable.*

To connect the power supply

1 Attach the output connector of the power supply (country specific power supplies are available) to the socket located in the centre of the rear panel.
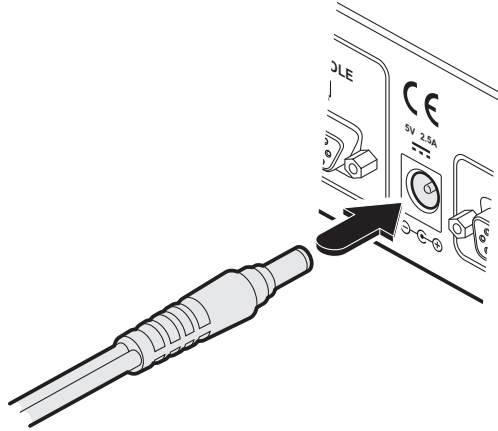
2 When all other connections have been made, connect the main body of the power supply to a nearby earthed mains socket.

Operation

In operation, the AdderView Secure unit allows you to quickly and securely switch between up to four systems. Strictly only one system may be accessed at a time, whereupon the common keyboard and mouse (and smart card reader, if used) are linked to that system.

Important security features

Tamper-evident seals

Given the high security nature of most installations that incorporate this unit, tamper-evident seals are fitted as standard across certain chassis screws. As part of a best practice policy, you are recommended to check any applied seals on a regular basis to ensure that the unit has not been opened without authorization.

IMPORTANT: Do not use the unit if the tamper-evident seals are damaged. Do not use if there are any signs of damage to the unit or its power supply.

The security indicators

The front panel includes five indicators that are dedicated to the AdderView Secure's internal security system.

Green authentication channel indicator
Illuminates whenever the authentication channel is selected. The indicator will be on immediately after power up, until a computer channel is selected.

Four red anti-subversion (and authentication) indicators
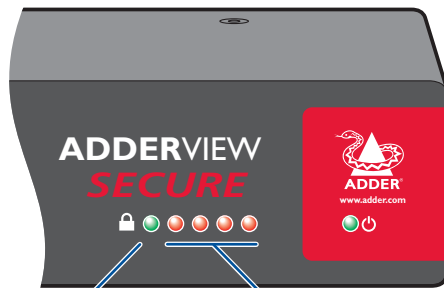On enhanced models, these indicate the current state of the anti-subversion function (discussed in the next section) and also provide responses whenever you use the authentication process.

Anti-subversion monitoring (enhanced models only)

The enhanced models (AVSC1102-XX and AVSC1104-XX) continually monitor their various defences for potential subversions (even when power is removed), such as:

- Dismantling of the case,
- Tampering with the circuitry,
- Loss or corruption of authentication security information.

To confirm that such checks are taking place, every five seconds the red security indicators will display a brief scanning sequence where one light appears to track right and then left along the row:
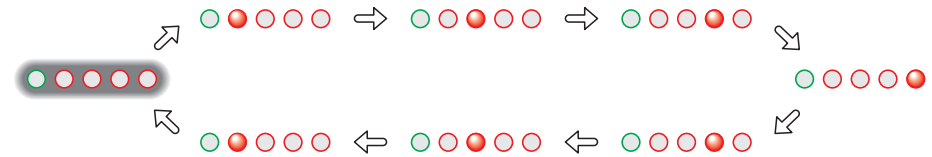
Note: Although anti-subversion monitoring continues to take place while the unit is powered down, indications are only given once power is reapplied.

If any subversions are suspected by the unit then it will immediately enter a lock down state where the following will take place:

- The computer channels become isolated and will not respond to the front panel buttons,
- The green authentication channel indicator will illuminate,
- The four red security will continually show the following flashing alert sequence:

Once the alert state occurs, it is irreversible. The unit can no longer be used and must be replaced.

Authentication checking (enhanced models only)

In addition to the anti-subversion scans that occur continuously, enhanced versions (AVSC1102-XX and AVSC1104-XX) of the AdderView Secure also provide a trusted mechanism whereby you can confirm their authenticity.

At manufacture, qualifying AdderView Secure units have a unique identity code configured within their circuitry. On request, Adder can provide you with an Authentication Certificate when you provide the following information:
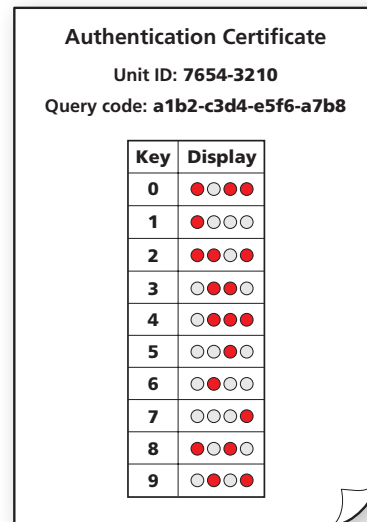
- The 8-digit **Unit ID**, and
- The 16-digit **Request Code**.

Both of these codes are listed on the AdderView Secure unit.

Once the validity of your request has been confirmed, you will be sent an Authentication Certificate containing the following:

- Confirmation of the 8-digit **Unit ID**,
- A unique 16-digit **Query Code**, and
- A **Key Map** which shows a series of indications that the AdderView Secure unit must give in response to particular key presses that you can enter.

Authentication Certificate

Unit ID: 7654-3210

Query code: a1b2-c3d4-e5f6-a7b8

Key	Display
0	○●●●
1	●○○○
2	●●○●
3	○●●○
4	○●●●
5	○○●○
6	○●○○
7	○○○●
8	●○●○
9	○●○●

If you make a mistake when entering

- If you press an incorrect key, press the **Esc** key to start the same code again.
- While entering a code, if you do not press a key for 30 seconds, the unit will timeout and you will need to begin whole process again.
- IMPORTANT: You have ten attempts to enter the **Query Code** correctly (this is counted each time the Enter key is pressed - using Esc to start the code again or going beyond the 30 second timeout do not count as one of the ten attempts). After the tenth consecutive incorrect attempt, the AdderView Secure will enter its alert state and will lock out irreversibly.

To use your Authentication Certificate

1 Apply power to the AdderView Secure unit.

   Note: If the unit is already on, remove power, wait five seconds and then re-apply power.

   The green 🔒 indicator will be on to show that the keyboard is switched to the internal authentication channel (also the red indicators should be performing their intermittent scan procedure):··································· 🔒 ●○○○○

2 Using the attached keyboard, enter the characters: **a u t h e n t i c a t e** and press Enter. *Note: The video display is not used during this process - take care to enter characters correctly.*

   The first of the four red indicators will begin to flash: ···· 🔒 ●☀○○○

3 Enter the 8-digit **Unit ID** code and press Enter.

   If the code is correct, the first red indicator will illuminate and the second will begin to flash:································· 🔒 ●●☀○○

4 Enter the 16-digit **Query Code** code from the Authentication Certificate (do not enter the dashes) and press Enter. *Take care, you have ten attempts to enter the correct code - see the section 'If you make a mistake when entering'.*

   If the code is correct, the red indicators will extinguish, leaving only the green illuminated: ································· 🔒 ●○○○○

5 Using the attached keyboard, press a numeric key (using the number keys above the main keyboard, not the numeric keypad) and observe how the four red indicators illuminate in response. Check the pattern against the one listed on the certificate for the pressed numeric key. You can check as many of the listed codes as appropriate. However, if any response does not match the pattern shown on the certificate, do not use the AdderView Secure unit and seek immediate advice from Adder technical support.

Selecting computers

In order to guard against the possibility of malicious software and also to minimize the chance of accidental switching, the AdderView Secure unit offers only one method to change between channels. All switching is done using the front panel switches.

- The buttons are clearly labeled to eliminate any ambiguity.
- Press the appropriate button to select the labeled channel.
- When the chosen channel has been connected, the adjacent indicator will illuminate (continuously) to confirm. If the indicator flashes, then the selected computer is either switched off or disconnected.
- Each channel uses a differently colored indicator to provide additional visual feedback about the chosen channel. Channel 1 has a green indicator and is generally configured to link with the lowest security computer/network, whereas channel 4 (or channel 2 on two-port versions) has a red indicator and is generally configured to link with the highest security computer/network.

Note: If a keyboard key is held down during a channel change then the key will be sent to the selected computer upon release of the channel change button. Do not hold down keys during a channel change.

Smart card reader

Your AdderView Secure unit can be attached to an optional smart card reader that allows you to insert your security card for authorization. The instructions given here are general advice and may differ for the model of card reader fitted or be superseded by procedures stipulated within your organisation.

Note: The channel can be changed before or after inserting the smart card.

To use the smart card reader
1 Align your smart card correctly with the reader slot.
2 Press the required channel select button (if the required channel is not already selected).
3 Follow the on screen instructions issued by the selected computer.

Further information

Troubleshooting

If you experience problems when installing or using the AdderView Secure unit, please check through this section for a possible solution. If your problem is not listed here and you cannot resolve the issue, then please refer to the 'Getting assistance' section.

No video from computer
- This is most likely to be associated with a mismatch between the host computer's video output and the DDC data held within the AdderView Secure. Computers often need read the correct DDC data before they will output a video signal.

  Depending on your DDC connection policy (see Video display (EDID) information for details), remember that the AdderView Secure will only attempt to read the DDC data from your monitor when the AdderView Secure is first powered on. To ensure that your monitor's DDC data is read and stored correctly, ensure that it is attached and powered on when you switch on the AdderView Secure.

Summary of threats and solutions

This section provides a list of potential security threats that the AdderView Secure might face during operation and the special steps that have been taken to counteract them.

Threat	Solution
Microprocessor malfunction or unanticipated software bugs causing data to flow between ports.	Unidirectional data flow is enforced by hardware "data diodes" so data isolation doesn't rely on software integrity.
Subversive snooping by means of detecting electromagnetic radiation emitted from the equipment.	Carefully shielded metal case with dual shielding in critical areas.
Detection of signals on one computer by monitoring for crosstalk (leakage) signals on another computer.	No connection to sensitive analogue inputs (such as computer microphone ports) are provided. A very high level of crosstalk separation is provided between signals from different computers.
Malicious modification of microprocessor software causing data to leak between ports.	Data isolation is assured by hardware and so is not compromised by any changes to the microprocessor software. Microprocessors use one time programmable memory so flash upgrades are not possible. Case uses counter-sunk screws which can be protected by tamper-evident seals.
Buffered data within a keyboard or mouse is sent to the wrong computer after switchover.	Keyboard and mouse are powered down and reset between each switchover to ensure that all buffers are cleared out.
Data leakage by means of monitoring conducted emissions on mains power.	The power circuitry provides strong protection against signal leakage via the power cable.

Threat	Solution
Data being sent to ports by means of faulty or subverted keyboards or mice causing the channel to switch and sending data in turn to each port.	Channel switching is controlled by the front panel buttons only with all keyboard hotkey or mouse switching capabilities removed from the design.
Data transfer by means of common storage.	USB ports support keyboard and mouse (and optional card reader) connections only. The product does not enable a USB memory stick or disk drive to be shared between computers. Unidirectional keyboard and mouse data signalling protects against data transfer across the switch.
Timing analysis attacks.	If a connection exists between a computer and a shared microprocessor system, it is potentially possible to determine what may be happening on the micro by timing the responses to repeated requests that the micro must service. For example, if a high data bit takes longer to transmit through the system than a low bit it may be possible to detect the pattern of data flowing between other ports by attempting to time the responses to otherwise normal requests. In the AdderView Secure, each port has a dedicated processor that only has input signals from the rest of the system. These input signals are only active when the port is selected. Consequently a timing analysis attack from one computer would yield no information about data flowing to another computer.
The user selects the wrong port.	Only one simple method of selecting computers is provided. The selected port is clearly and unambiguously indicated on the front panel by means of colored lights adjacent to each key switch. For high levels of security, the screens of high and low security computers should be arranged to look visibly different in general appearance.

Threat	Solution
Forced malfunctions due to overloaded signalling.	It is potentially possible to create forced malfunctions by constantly and quickly sending a stream of valid requests (such as the request to update the keyboard lights). A well known example of an undesirable KVM malfunction is a "crazy mouse" which was quite common with early KVM switches and was caused by data loss on PS/2 systems with the result that the mouse darted around the screen randomly clicking and opening windows. The unidirectional design of the AdderView Secure ensures that the influence of signalling on one port cannot flow past the data diodes. This means that overload signalling on one port will not affect the operation of another port. USB signalling is not susceptible to the failure mechanism that caused the crazy mouse on PS/2 systems.
Signalling by means of shorting the power supply or loading the power supply.	Each port is independently powered by its USB port. Shorting the power supply on one port will not cause the power on other ports to be switched off.
Tampering with the switch.	The switch is fitted with tamper protection measures.
Data transfer by means of a shared smartcard.	The switch provides a layer of isolation between the physical smartcard reader and the computer. This will counter threats associated with sharing the same physical card reader. The result is to deliver the same security level as would be present if multiple card readers were used and the card was swapped between them. A further level of security is provided by making the smartcard function absent from certain computers (by means of using cables that lack the yellow smartcard USB connector).
Non-authentic facsimile switches.	The enhanced models enable the authenticity of the switch to be checked by means of security certificates.

Getting assistance

If you are still experiencing problems after checking the list of solutions in the Troubleshooting section then we provide a number of other solutions:

- Adder Technology website – *www.adder.com*

  Check the Support section of our website for the latest solutions and driver files.

- Email – *support@adder.com*

- Fax   in the UK: **01954 780081**

                in the US: **+1 888 275 1117**

- Phone   in the UK: **01954 780044**

                in the US: **+1 888 932 3337**

Safety information

- For use in dry, oil free indoor environments only.
- Warning - live parts contained within power adapter.
- No user serviceable parts within power adapter - do not dismantle.
- Plug the power adapter into a socket outlet close to the module that it is powering.
- Replace the power adapter with a manufacturer approved type only.
- Do not use the power adapter if the power adapter case becomes damaged, cracked or broken or if you suspect that it is not operating properly.
- Do not attempt to service the unit yourself.
- Not suitable for use in hazardous or explosive environments or next to highly flammable materials.
- Do not use the power adapter if the power adapter case becomes damaged, cracked or broken or if you suspect that it is not operating properly.
- If you use a power extension cable, make sure the total ampere rating of the devices plugged into the extension cable do not exceed the cable's ampere rating. Also, make sure that the total ampere rating of all the devices plugged into the wall outlet does not exceed the wall outlet's ampere rating.
- The power adapter can get warm in operation – do not situate it in an enclosed space without any ventilation.

Warranty

Adder Technology Ltd warrants that this product shall be free from defects in workmanship and materials for a period of two years from the date of original purchase. If the product should fail to operate correctly in normal use during the warranty period, Adder will replace or repair it free of charge. No liability can be accepted for damage due to misuse or circumstances outside Adder's control. Also Adder will not be responsible for any loss, damage or injury arising directly or indirectly from the use of this product. Adder's total liability under the terms of this warranty shall in all circumstances be limited to the replacement value of this product.

If any difficulty is experienced in the installation or use of this product that you are unable to resolve, please contact your supplier.

Radio Frequency Energy

All interface cables used with this equipment must be shielded in order to maintain compliance with radio frequency energy emission regulations and ensure a suitably high level of immunity to electromagnetic disturbances.

European EMC directive 89/336/EEC

This equipment has been tested and found to comply with the limits for a class A computing device in accordance with the specifications in the European standard EN55022. These limits are designed to provide reasonable protection against harmful interference. 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 or television reception. However, there is no guarantee that harmful interference will not occur in a particular installation. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference with one or more of the following measures: (a) Reorient or relocate the receiving antenna. (b) Increase the separation between the equipment and the receiver. (c) Connect the equipment to an outlet on a circuit different from that to which the receiver is connected. (d) Consult the supplier or an experienced radio/TV technician for help.

FCC Compliance Statement (United States)

This equipment generates, uses and can radiate radio frequency energy and if not installed and used properly, that is, in strict accordance with the manufacturer's instructions, may cause interference to radio communication. It has been tested and found to comply with the limits for a class A computing device in accordance with the specifications in Subpart J of part 15 of FCC rules, which are designed to provide reasonable protection against such interference when the equipment is operated in a commercial environment. Operation of this equipment in a residential area may cause interference, in which case the user at his own expense will be required to take whatever measures may be necessary to correct the interference. Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

Canadian Department of Communications RFI statement

This equipment does not exceed the class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le règlement sur le brouillage radioélectriques publié par le ministère des Communications du Canada.

CONTENTS

WELCOME

INSTALLATION

OPERATION

FURTHER
INFORMATION