



BLACK BOX[®]

NETWORK SERVICES[®]

© 2005. All rights reserved.
Black Box Corporation.

Security with the ServSwitch Wizard IP

A white paper



February 2005

Table of Contents

1.0	Introduction	3
2.0	Product overview	3
3.0	The need for security	5
4.0	Access control	5
4.1	Identification	5
4.2	Passwords	5
4.3	Logging	6
4.4	Private mode	6
4.5	Screen lock	6
5.0	Local access method	6
6.0	Dial-in access method	7
7.0	IP network access method	7
7.1	Other product approaches	7
7.2	Wizard IP approach	8
7.3	Wizard IP security specification	8
7.4	IP address filtering	9
7.5	Java viewers	9
8.0	Firmware upgrade	10
9.0	Configuration and management	10
9.1	Single remote connection	10
9.2	Deployment scenarios	11
10.0	General security advice	11
10.1	Deployment advice	11
10.2	Additional security measures	12
11.0	References	13

1.0 Introduction

Traditional KVM switches enable you to switch keyboard, video monitor, and mouse (KVM) consoles between a group of computers so you don't need to attach a keyboard, monitor, and mouse to each computer, which saves space, money, and power. KVM switches don't require any special software to be loaded on the computers yet they provide simple-to-use and robust computer management that continues to work even if the attached computers crash. The one major drawback is that the KVM consoles must have a direct cable connection to the KVM switch, which limits their range to a few hundred metres.

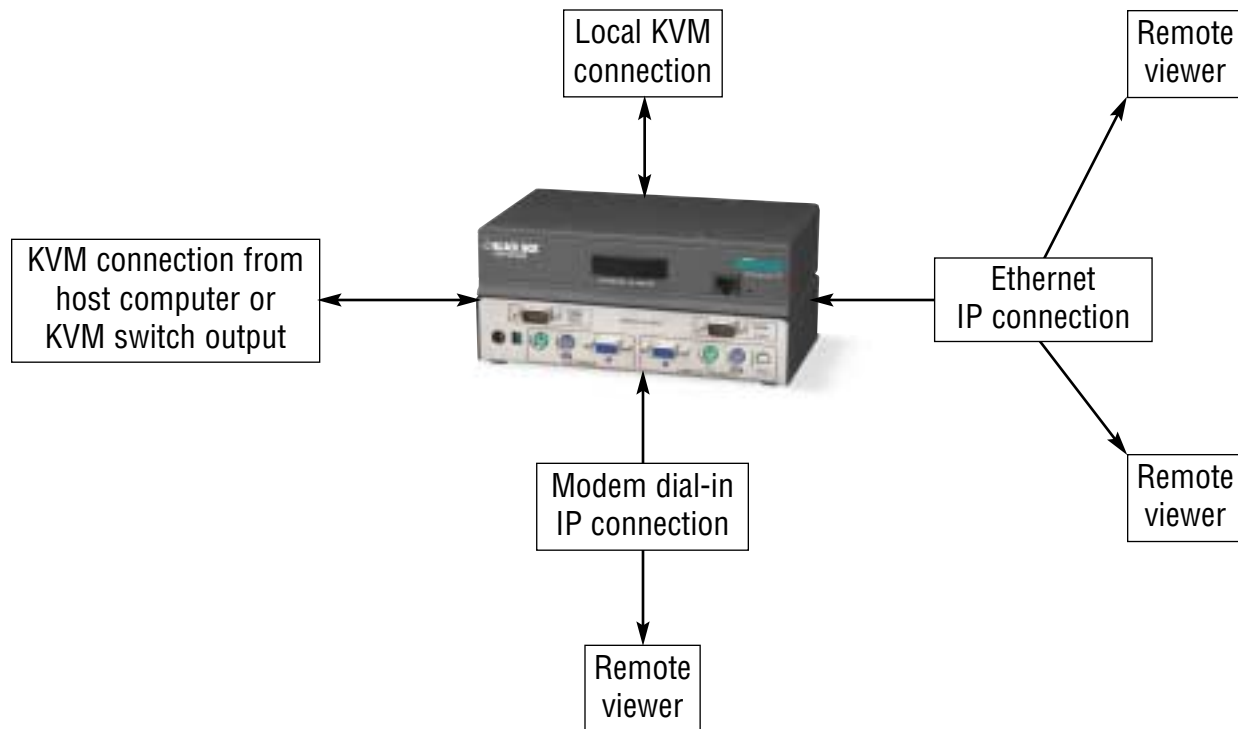
Remote access software enables computers to be controlled from anywhere in the world using a dial-in, a network, or an IP-style connection. This software is available in many varieties, but they all share the same basic operating principles. Software is loaded onto the "host" computer that intercepts the keyboard, video, and mouse signals. The software communicates these signals to a second software program running on a remote "viewer" computer in a manner that enables the user of the "viewer" computer to view and control the "host" computer. Unfortunately, these software remote control systems can't cope with boot time problems and don't work if the host computer crashes.

KVM-via-IP products combine the advantages of remote access software with the benefits of KVM technology. Like KVM switches, KVM-via-IP products don't require software to be loaded on the host computers and instead interface directly with the keyboard, monitor and mouse connectors of the host computer or KVM switch. The difference is circuitry within the KVM-via-IP appliance digitizes the incoming video signal and processes it into digital data that is communicated to a viewer program running on a remote computer over a LAN, a VPN, or the public Internet.

The ServSwitch Wizard IP is an innovative KVM-via-IP product designed to address the demanding needs of enterprise applications. The requirement for robust security ranks high, and this white paper explains how the security architecture of the ServSwitch Wizard IP fits that need.

2.0 Product overview

The Wizard IP product is a standalone unit, which is easy to configure to enable local, dial-in, or remote IP connections to the target host or KVM switch. By using the local connection on the Wizard IP, you can have both local KVM console access and remote IP access to your servers. This mix of local and remote access is highly attractive to system administrators because it enables them to have direct local KVM access to computers in their server room while also enabling access from their office or from any remote location. The ability to simultaneously support IP network and dial-in modem connections offers system administrators the convenience of "in-band" access via the network and the security of reliable out-of-band access if the IP network is disrupted.



The Wizard IP implements an enhanced VNC server embedded within its hardware. VNC is the world-wide de-facto standard for cross-platform software remote control and is the natural choice for KVM-via-IP products. VNC is currently installed and in use on many millions of computers in homes, small enterprises, government organizations, schools, university campuses, and in most larger companies. An enhanced VNC viewer is included with the Wizard IP. You can also install it directly from the RealVNC Web site [1]. In addition, a Java viewer is embedded in the Wizard IP; you can run it by connecting a Web browser so you don't need to install software on the remote viewing computer.

3.0 The need for security

Traditional KVM switches are inherently very secure, requiring physical access to the equipment. This can be controlled with locks and keys. For users who have already gained physical access, a simple password system entirely local to the KVM switch is sufficient to provide a further level of secure access control to individual users and groups of users.

Access control is a much more worrisome and difficult issue for products connecting to networks of any kind—from LANs and WANs to VPNs and, of greatest concern, the public Internet. When you use a KVM-via-IP product to remotely access a privileged server console, such as a file server, there's the potential for a security breach, which could be very damaging. For this reason, the KVM-via-IP product's security is extremely important.

Security is often an afterthought, added on late in the development of a product. But security has a fundamental impact on the design and implementation of a complete system, and late consideration usually leads to flaws, loopholes, and clumsy setup and configuration. Security for the ServSwitch Wizard IP product was considered from the outset, and a fully thought out and formally analyzed security architecture was drawn up before any implementation and integration. Drawing on the expertise and advice of security experts within the Cambridge academic community, the ServSwitch Wizard IP meets the challenging requirements of Internet-connected products.

We'll now discuss the range of security measures included in the Wizard IP product, which, in combination, enable you to use it with confidence across the most hostile of environments.

4.0 Access control

4.1 Identification

All access to the ServSwitch Wizard IP, whether local, dial-in, or Internet, requires a valid user name and password. A privileged user “admin” has complete access to the configuration and management of the unit. The “admin” user can create other user names, which are able to gain access to the host, but only have restricted capability to configure the unit. Each user profile has a number of capabilities that can be granted by the “admin” user, including the local and remote access rights. The table of user names and passwords is stored privately and securely on the unit itself, and is not duplicated or accessible externally. User names and passwords form the last line of defense for anyone who has gained physical or network access to the unit.

4.2 Passwords

For maximum security, it is important to choose strong passwords, which are not easy to guess. When passwords are set, the Wizard IP tests for the cryptographic strength of the password and displays a warning if the chosen password is considered weak. Similarly, a warning is displayed if no password is set. The Wizard IP temporarily locks out a user name if there have recently been repeated failed attempts to login. This scheme effectively prevents automated brute force attacks from discovering passwords by probing.

4.3 Logging

The Wizard IP product internally stores a comprehensive, time-stamped activity log. This allows the “admin” user to see a record of power on, reboot, and firmware upgrade events. Access activity is shown in the form of successful or failed login attempts and includes the user name and the type of access (local, modem, or remote). For remote access, the IP address of the remote computer is shown. In addition to providing information about normal operation, logs of this kind offer valuable diagnostics for detecting and analyzing suspicious activity.

4.4 Private mode

A convenient feature of the Wizard IP is the ability of any user to temporarily request exclusive access to the target host. The Wizard IP sends a warning message to other users and locks them out for the duration of the exclusive user’s access. Available both locally and remotely, this feature provides an additional safeguard when configuring secure systems or accessing sensitive information.

4.5 Screen lock

Further security is provided by a screen lock, which automatically comes on after a period of local keyboard and mouse inactivity, preventing a screen that has been left unattended from being misused. This feature works with local and remote connections.

5.0 Local access method

Physical access to any equipment provides an opportunity for misuse, and despite all internal security measures a product has, facilities security is always a vulnerability. But with the ServSwitch Wizard IP, access to the local KVM connection is protected by user name and password in the same way as for a remote connection. With local access, an on-screen display provides the login dialog. For maximum security, you can place the Wizard IP in a highly secure and restricted environment, with only the local KVM connection in a less secure environment where the user name and password can provide strong access control.

6.0 Dial-in access method

By connecting an external modem, the Wizard IP provides remote access via a standard telephone line. Dial-in access provides an inherent first level of security because an attacker needs to know the telephone number to which the unit is connected to be able to attempt to connect. Unlike an IP network, the public telephone network is difficult and costly to probe automatically. It is also widely acknowledged that the public telephone network and a dial-in connection is very difficult to snoop or intercept. The Wizard IP incorporates a PPP server [2], allowing you to make an IP connection using a standard dial-in network configuration from a remote host. You can run the enhanced VNC viewer—including the full range of encryption and authentication measures—over the IP connection as described in the next section.

7.0 IP network access method

The full use of the Wizard IP becomes apparent when you connect it to an IP network. Because IP networks are so prevalent, the target host can potentially be controlled from anywhere in the world, and for convenience, many users expect to be able to access KVM-via-IP products via an Internet connection. This requires a special level of care where security is concerned.

7.1 Other product approaches

Other KVM-via-IP products have implemented security schemes based around HTTPS [3], which is used primarily for secure Web transactions. HTTPS was not specifically designed for use with KVM-via-IP products and consequently has some drawbacks. Each HTTPS site needs to be issued with an SSL [4] certificate from an authority such as Verisign [5] or Thawte [6], which has been signed by them using a private key. Web browsers are designed and built to trust these authorities and can verify that any certificate presented to the browser by the HTTPS site is signed by such an authority. This is easily done using the authority's public key.

To use HTTPS effectively in a KVM-via-IP product, the owner of each unit must obtain a certificate and configure that unit with the certificate. This represents a significant administrative and financial overhead, with a certificate typically costing in excess of \$100 per annum. Furthermore, certificates are based on IP addresses or DNS names, so a KVM-via-IP product has to be previously configured to have an IP address or a DNS name that would remain static for the lifetime of the certificate. In effect, it is simply not feasible to obtain signed certificates in practical installations.

Instead, KVM-via-IP products that use HTTPS create their own self-signed SSL certificates. When you connect a browser to the unit, the certificate is shown to the user in a pop-up window, and the browser asks if this certificate is to be trusted or not. On the very first connection, this can be considered to be an acceptable policy. Indeed, secure remote login shells such as SSH [7] operate in the same manner. However, because it is extremely difficult and in some cases impossible to arrange for browsers to cache these certificates, the pop-up window will appear every time you connect the browser to the unit.

This means the KVM-via-IP product is open to “man in the middle” attacks, because it is left to the user to visually verify that a certificate has not changed between successive connections to the same unit. Experience shows that users do not take this degree of care, and habitually accept the new certificate. This is worse than the situation with SSH, where the certificate is cached in the computer’s file system, and the user more carefully considers the situation where the certificate appears to have been changed.

7.2 Wizard IP approach

For these reasons, the Wizard IP does not rely on HTTPS for secure access and avoids the corresponding certificate management issues. Furthermore, HTTPS and SSL implementations are bulky and complex, and contain many features that are not relevant to a remote access product. The Wizard embodies the philosophy of SSH and some concepts from SSL. With its custom design and implementation, the ServSwitch Wizard IP has a very tightly focused integration, avoiding many of the security loopholes that have plagued the third-party HTTPS and SSH implementations because of their size and many additional functions. The security implementation has undergone rigorous testing and evaluation through large-scale deployment in a number of multinational companies.

First, public key authentication is carried out with 2048-bit RSA cryptography [8] (extendable to larger keys). This involves running a key generation algorithm to generate a pair of large primes. The key generation algorithm uses a number of entropy sources from the unit to ensure that the generated keys are truly random and cannot be predicted. Entropy sources include keystrokes and mouse movements, which the user is required to provide during the key generation phase. Then, encryption is carried out using the AES stream cipher [9] with a 128-bit key, which is generated and exchanged securely as a result of the authentication phase.

7.3 Wizard IP security specification

The notation $P_k\{m\}$ is used to indicate that a message m is to be encrypted with public key P_k . The notation $S_s\{m\}$ indicates that the message m is to be encrypted with the symmetric key S_s . The symbols V and U are used to refer to the viewer and unit in the protocol exchange. First, the unit sends its public key to the viewer. At this stage, the viewer compares the unit’s IP address and public key against values stored in the local file system or registry cache to warn the user if it has changed since the previous access.

$U \rightarrow V : P_U$

$V \rightarrow U : P_V$

Then, randomly generated strings or nonces N , upon which to base the session key, are generated. Because these are encrypted with each party’s public keys, only the holders of the corresponding private keys can obtain the nonces. This prevents an eavesdropper from intercepting them.

$U \rightarrow V : P_V\{N_U\}$

V -> U : P_U{N_V}

128-bit session keys are calculated based upon the two nonce values, using SHA-1 hashing [10].

S_{V2U} = H(N_V, N_U)

S_{U2V} = H(N_U, N_V)

Using the new session keys, the AES protocol is used to encrypt some well-known information (the ServSwitch Wizard IP uses a hash of the public keys), enabling both parties to verify that the other has correctly calculated the session keys.

U-> V : S_{U2V}{H(P_U, P_V)}

V -> U : S_{V2U}{H(P_V, P_U)}

Following this secure exchange of session keys, all subsequent message exchanges between the Wizard IP and the viewer are similarly AES encrypted using a stream cipher mode to provide protection from in-depth analysis or replay attacks. The first such message exchange is the unit access control phase, in which a user name and password are transmitted from viewer to the Wizard IP.

7.4 IP address filtering

The ServSwitch Wizard IP allows IP filtering of incoming packets. This enables the “admin” user to establish a pattern of IP addresses from which remote connections will be accepted. All other attempts to connect are refused. This means you can configure the unit to work only on a specific IP address range, such as a corporate LAN. Also, the Wizard IP allows access from specified external IP addresses, such as from a system administrator’s home. This gives additional control and security when enabling access through the company firewall.

7.5 Java viewers

A Java viewer that’s downloadable from the unit itself provides a convenient method of gaining access without installing any software on the remote computer. All browsers provide a safe execution environment for the Java program, which prevent it from accessing the local file system or registry. It is therefore impossible for a Java viewer to cache any certificates issued by any KVM-via-IP product. In the absence of authority signed certificates, Java viewers are potentially vulnerable to man-in-the-middle attacks. However, a human-readable certificate fingerprint is presented to the user by the viewer at connection time. This gives the user an opportunity to visually check the certificate against a known value and so verify the server identity before continuing.

8.0 Firmware upgrade

The ServSwitch Wizard IP might require an occasional upgrade to introduce new functionality and performance enhancements. Full firmware upgrades are supported either locally over the serial port or optionally over the IP network connection. It is vital that you only download and install certified upgrades from a verifiable source. The Wizard IP's security architecture specifically addresses this through the use of public/private key digital signatures.

All firmware upgrades and accompanying digital signatures are distributed by Black Box. Firmware upgrades are binary and do not require encryption. The signature is computed in two stages. First, a fingerprint of the binary is calculated using a public SHA-1 hash function. The fingerprint is then signed using RSA cryptography, within the Wizard IP private key known only to Black Box.

When you download a firmware upgrade and accompanying digital signature, the Wizard IP verifies the authenticity of the 2048-bit signature using RSA cryptography derived from the Wizard IP public key, installed at manufacture. The resulting fingerprint can be checked against the fingerprint of the downloaded binary calculated using the same SHA-1 hash function.

This method of signing firmware is extremely secure, because it is computationally infeasible for a malicious third party to create a binary firmware upgrade with a matching RSA signature pair. This prevents upgrade data from being spoofed.

9.0 Configuration and management

The Wizard IP product has a simple, streamlined approach to unit configuration and management. Initial configuration, such as setting up IP network parameters, is carried out on the local KVM connection by attaching a monitor and keyboard. An on-screen display presents a simple menu system to lead the user through the necessary steps. All other configuration is carried out over the IP connection itself.

9.1 Single remote connection

The key feature of the ServSwitch Wizard IP is that you should use a single connection from the remote computer to the Wizard IP for both the remote control function *and* for the configuration menus. This unique combination of interactive remote control and configuration menus overlaid in a single window on the remote computer screen provides a fully integrated and remarkably intuitive user interface. Unlike other KVM-via-IP products, which have separate applications and connections for remote control and for configuration, the ServSwitch Wizard IP uses a single software application, the VNC viewer. This means that there are no other configuration tools to install and run separately and no cascades of disjointed and dissimilar windows.

In addition to providing a completely consistent look and feel, the integrated approach simplifies security management by requiring only a single IP port to be open through the firewall. The security architecture described in the previous paragraph makes this single channel secure. In another significant simplification, the Wizard IP can respond both as a Web server or a VNC server on the same IP port, by autosensing the type of client connection. This enables the user to either connect with a Web browser and download and run the Java viewer, or to connect with a native VNC viewer installed on the remote computer. Other KVM-via-IP products often have different ports for remote control protocol and for Web server connections, and require more complicated configuration through firewall and routing equipment.

9.2 Deployment scenarios

You can use the ServSwitch Wizard IP in a variety of applications with different security requirements. On a completely trusted private network, security may not be a concern and the most basic user name and password scheme will be sufficient to control access to the Wizard IP. On larger or public networks, stronger security may be required, in which case you can authenticate and encrypt the ServSwitch Wizard IP remote access stream to provide protection against a variety of attacks including snooping, brute force attacks, and man-in-the-middle attacks.

10.0 General security advice

If you make the Wizard IP accessible from the public Internet or from a modem, you should take care to ensure that the maximum security available is activated. We advise you to enable encryption and use a strong password. Security may be further improved by restricting client IP addresses, using a nonstandard port number for access or limiting remote access to dialup connections only. For more information, refer to the “Networking Issues” section of the ServSwitch Wizard IP product manual.

10.1 Deployment advice

The security capabilities offered by the Wizard IP are only truly effective when they are used correctly. An open or a weak password or an unencrypted link can cause security loopholes, which are opportunities for potential intruders. For network links in general and direct Internet connections in particular, you should carefully consider and implement the following:

- Ensure that encryption is enabled on the Wizard IP.
- Ensure that you have selected secure passwords with at least eight characters and a mixture of upper- and lower-case and numeric characters.
- Reserve the admin password for administration use only and use a nonadmin user profile for day-to-day access.
- Use the latest Secure VNC viewer (this has more in-built security than is available with the Java viewer).
- Use nonstandard port numbers.

- Restrict the range of IP addresses that are allowed to access the Wizard IP to only those that you will need to use.
- Do *not* Force VNC protocol 3.3.
- Add a further level of inherent security by restricting access only via modem or ISDN dialup.
- Ensure that the computer accessing the Wizard is clean of viruses and spyware and has up-to-date firewall and antivirus software loaded that it is configured appropriately.
- Ensure that the computer accessing the Wizard IP has had all the latest operating system security patches and updates applied.
- Avoid accessing the Wizard IP from public computers.
- Ensure that passwords are updated or removed when no longer needed (e.g. when an employee leaves).

10.2 Additional security measures

- Use a KVM switch with on-screen-display-driven security access and an auto-logout after inactivity feature to provide a second level of security. We recommend KVM switches such as the ServSwitch Affinity, ServSwitch Octet, or ServSwitch Quadro.
- Place the Wizard IP behind a firewall and use the port numbers to route the VNC network traffic to an internal IP address.
- Review the activity log from time to time to check for unauthorized use.
- Lock your server consoles after they have been used.

11.0 References

1. <http://www.realvnc.com>, RealVNC Web site
2. <http://www.ietf.org/rfc/rfc1332.txt>, PPP protocol
3. <http://www.ietf.org/rfc/rfc2616.txt>, HTTP/HTTPS protocol
4. <http://wp.netscape.com/eng/ssl3/draft302.txt>, SSL protocol
5. <http://www.verisign.com>, trusted certificate authority
6. <http://www.thawte.com>, trusted certificate authority
7. <http://www.ietf.org/internet-drafts/draft-ietf-secsh-filexfer06.txt>, SSH protocol
8. <http://www.faqs.org/rfcs/rfc2437.html>, RSA cryptography specifications
9. <http://csrc.nist.gov/CryptoToolkit/aes/rijndael/>, AES specification
10. <http://www.ietf.org/rfc/rfc3174.txt>, SHA-1 specification