

Xyloc Security Appliance



Key Features

- ▶ Full-time Security with Convenience
- ▶ Work Place and Enterprise solutions
- ▶ Central Management for larger Installations

Fulltime Security with Convenience
Every company knows the importance of information security. Firewalls are used to prevent outsider intrusion. VPNs are created for secure remote access. But security procedures are nothing without employee compliance. Requiring a password for network logon does nothing to secure information once a user has walked away from the computer.

With so much business being conducted in open cubicle environments, protecting the network is more challenging than ever. XyLoc Enterprise was developed to provide companies with full-time security for the network while making it convenient for employees to use.

For the user, XyLoc Enterprise works just like XyLoc Solo — approach your XyLoc-secured computer and you are automatically logged on. But for the administrator, XyLoc Enterprise is even easier to use, thanks to the Web-based XyLoc Security Server (XSS).

The Power of Central Management

XSS simplifies the overall management of XyLoc: it allows administrators to access, update, maintain and audit all aspects of the XyLoc system from any PC with a VPN or Internet connection. Administrators can quickly:

- Create new users and issue new Keys;
- Create user groups (like "engineering"

or "human resources") with the same logon requirements and access privileges;

- Disable Keys in the case of loss, theft, or termination of employment;
- Print detailed audit logs on the user activity and the operation of the XSS itself.

A Security Safety Net

The XyLoc Security Server provides another measure of security-complete system reliability. The XSS's robust and reliable architecture keeps an encrypted authentication database both on the server XSS and a smaller encrypted database on the client PC. Any changes to the XSS's central database are automatically updated only to the appropriate local PC client authentication databases. In the unlikely event of a XSS or network failure, the local PC's client database continues to provide secure and uninterrupted Full Time Authentication to the user of the computer. This same architecture provides ongoing protection to Notebook computers when they are disconnected from the network. And by using a secure Internet connection, XSS is also able to control workstations at branch locations as well as workstations on the LAN.

How XyLoc Works

XyLoc is the only security solution that continues to protect the network after a user has logged on. XyLoc consists of a radio transceiver "Lock" that plugs in to the computer and a discrete wireless radio transmitter "Key" worn by the user. The Lock and Key stay in constant radio communication (up to 15 meters) to determine user identity and location relative to the computer.

When you approach a computer protected by XyLoc while wearing a XyLoc Key, the Key automatically transmits a unique, 32-bit encrypted ID code to the Lock. The Lock verifies your identity with the XyLoc administration software; if authorized, the XyLoc system will unlock the computer's keyboard and screen. If unauthorized, the system remains locked and information secure.

Hands-free or Multi-factor Authentication

XyLoc was built to be a flexible tool, adaptable for any environment where security is needed. While the hands-free AutoLogon feature might be right for some situations, others will require the user to select their name from a menu and/or enter their password. XyLoc can also be integrated into other security measures, from tokens to biometrics. For example, many companies have been arming their employees with

RSA Security's SecurID solution for two-factor authentication while accessing the corporate network. While XyLoc can provide multi-factor authentication on its own for the PC, it can also work with and add another level of security to RSA SecurID. In this case the XyLoc Key becomes the "authenticator", eliminating the need for the user to manually transfer a numerical code to access the VPN, providing convenient two-factor security for remote access.

Secure Logon and Unlock Options

- Hands-free AutoLogon - When an authorized user approaches the PC while wearing the XyLoc Key, it automatically logs the user on
- AutoLogon with keystroke confirm - Press any key to gain access while wearing the Key
- Select username -Users select their name from a list of authorized XyLoc users detected in the area. Particularly useful for XyLoc MD installations.
- Password Required - Users must enter their unique password in addition to wearing the Key
- Select username and enter password - Users must enter their unique password after selecting their name from a list of authorized XyLoc users within the range of the XyLoc-protected PC

More about XSS

The XyLoc Security Server software that comes with XyLoc Enterprise, XyLoc Enterprise AI and XyLoc MD makes the administration, reporting and management of XyLoc easy and cost efficient, no matter how large the installation. All of XyLoc's advanced features, including application integration and the kiosk accounts offered by XyLoc MD, are managed through XSS. Each XSS is capable of handling thousands of users and computers, and the system can store

up to 32 username/passwords for each user on a given computer.

XSS makes both local and remote Web-based central management of XyLoc simple. If a user forgets his Key, there are several options the administrator can choose. Users can be provided with override passwords, so they can access their workstations in the case of a forgotten Key. The XSS records each user override, and can notify the administrator of this action through the XSS auditing feature (see below). If the user is not assigned an override password, the XyLoc administrator can issue a temporary override password on each of the user's computers, or suspend the user's current Key and issue a temporary Key. New employees are quickly assigned Keys, and Keys used by outgoing employees can easily be disabled. Every aspect of managing a XyLoc installation can be performed quickly and easily using the XyLoc Security Server.

XSS and Auditing

XSS also creates detailed audit logs of both user activity and the operation of the XSS itself. When a user logs on to the network, XSS records how they logged on (with their Key or with an override password) and the time and date of the logon. Every time the user leaves and comes back to the XyLoc-protected machine, this activity is also logged. And, in the case of XyLoc Enterprise AI and XyLoc MD, XSS records every application the user launches. No other security solution monitors user activity after the initial logon. XSS constantly monitors the entire network to ensure full-time security. XyLoc can detect a stationary Key-one that is not being worn-and can secure a computer after detecting that the Key is stationary for too long. This allows companies to ensure all employees are adher-

ring to security procedures.

Other features of XSS:

- A local encrypted Time to Live authentication database on each PC gives the XyLoc administrators control over mobile computers. Any time there is a network connection, be it dial-up, VPN or Ethernet, this local database synchronizes with the central authentication database on the XSS. It can be set to specific a period of time in which synchronization must occur again before the system is completely secured. When the time to live has expired, the administrator's assistance is required to unlock the PC.
- XyCrypt File Encryption prevents unauthorized access to data files on the hard drive of a XyLoc-protected notebook or desktop PC, even if other security measures have been surmounted. XyCrypt extends XyLoc's convenience and security by automatically and transparently encrypting the user's data files, creating an additional and powerful level of information security. Every time a user is automatically logged off of their applications, their files are encrypted. Even if a laptop is stolen and the hard drive is removed, the information remains complete protected.
- XyLoc Power Management helps organizations reduce energy consumption, thereby saving money and improving the environment. XyLoc Power Management automatically activates Windows' power management capabilities when a user walks away from the PC. And when the user returns, XyLoc can reactivate the monitor as well as unlock the computer. By putting computers on standby (turning off

monitors and hard disks) when they are not in use, companies with large XyLoc installations can save significant amounts of money.

XyLoc System Requirements:

- PC compatible, Pentium class processor, portable or desktop computer
- Windows 95/98, Me, NT, 2000 or XP (95B required for USB support)
- CD-ROM drive or a network connection to a server running XSS
- Available serial or USB port
- 5 MB available hard disk space

XyLoc Security Server System Requirements:

- Pentium II 350 MHz processor with 128 MB of RAM and 250 MB of hard disk space
- Windows NT 4.0 Server Service Pack 5 or higher, Windows 2000 Server, or XP
- Internet Information Services (IIS) 4.0 or higher

XyLoc and Wireless Technology

XyLoc's standard Lock and Key technology is based on 300, 800 or 900 MHz radio signals, depending on the country of installation. Ensure is also working on a version of XyLoc to leverage the 802.11b wireless LAN infrastructure that is gaining popularity. The 802.11b version of XyLoc, scheduled to be released in 2002, eliminates the need for an external XyLoc Lock. Rather, XyLoc uses a computer's existing 802.11b capabilities to maintain the RF connection with a special 802.11b version of the XyLoc Key. Using a computer's 802.11b capabilities to lock and unlock access to the machine does not affect the wireless LAN in any way.

Ordering information

ITEM	CODE
Xyloc SOLO, Set Einzelplatzversion	.XES10S
Xyloc Key Card	.XES10K
Xyloc USB Transceiver Lock Enterprise	.XES10T
XSS Enterprise, 25 Userlicenses	.XES10E-0
XSS Enterprise, 50 Userlicenses	.XES10E-1
XSS Enterprise, 100 Userlicenses	.XES10E-2
XSS Enterprise, 250 Userlicenses	.XES10E-3
XSS Enterprise, 500 Userlicenses	.XES10E-4
XSS Enterprise, 1000 Userlicenses AI Enterprise	.XES10E-5
XSS-AI Enterprise, 25 Userlicenses	.XES10A-0
XSS-AI Enterprise, 50 Userlicenses	.XES10A-1
XSS-AI Enterprise, 100 Userlicenses	.XES10A-2
XSS-AI Enterprise, 250 Userlicenses	.XES10A-3
XSS-AI Enterprise, 500 Userlicenses	.XES10A-4
XSS-AI Enterprise, 1000 Userlicenses	.XES10A-5

Ordering information

ITEM	CODE
MD Enterprise	
XSS-AI Enterprise, 25 Userlicenses	.XES10M-0
XSS-AI Enterprise, 50 Userlicenses	.XES10M-1
XSS-AI Enterprise, 100 Userlicenses	.XES10M-2
XSS-AI Enterprise, 250 Userlicenses	.XES10M-3
XSS-AI Enterprise, 500 Userlicenses	.XES10M-4
XSS-AI Enterprise, 1000 Userlicenses	.XES10M-5



Black Box Network Services - The world's largest network services company

We are, with 25 years of experience, the world leader in network infrastructure services.

On the Phone — no charge, answer calls in less than 20 seconds, find the right product with our technical experts.

On-site — superior design and engineering, Certified installations, end-to-end service.

On-line — receive technical knowledge on-line, including technology overviews, BLACK BOX Explains and the Knowledge Box.

Most comprehensive TECHNICAL SUPPORT — our best Product! Free hotline TECH SUPPORT!

The world's best customer service — Custom design services and products, the best warranties, money-saving discount programs.

BLACK BOX exclusives — Certification Plus. Guaranteed-for-life products and services.