Office of Information & Technology Security

Video Teleconference (VTC) systems provide two way video and audio communications to two or more remote locations over the Internet. The VTC systems allow people virtually meet face to face to facilitate meetings and online collaboration.

The basic security requirement section contains configuration instructions required for all new and existing VTC systems. These requirements are designed to harden the VTC against common threats and user misuse.

The enhanced security recommendation section provides steps to create an encrypted communication channels between VTC systems in order to prevent third party eavesdropping over the Internet. Any sensitive or confidential communications done over the VTC should use encryption.

Basic Security Requirements

Note: some features may not be available on all VTC systems

1. Change all default passwords
    a. The default passwords for VTC devices are documented and available on the Internet.
    b. Use different passwords for administrative and user accounts
    c. Use complex passwords requirements for added security
    d. Change the password for non-web services such as SSH, Telnet, and FTP
2. Disable Unnecessary Protocols and Services
    a. VTC devices often have services such as SSH, Telnet, and FTP enabled by default. These services can be used as a point of attack for the device. Disable these services if they are not needed.
3. Use Latest Firmware, Software, and Patches
    a. Manufactures will release updates to fix known vulnerabilities. Keep the system up to date to prevent attackers from exploiting these vulnerabilities.
4. Disable Remote (Web) Monitoring
    a. Some VTC devices allow for remote monitoring via a webpage. Disable this feature to prevent a third party from viewing and listening in on a meeting without the participants' knowledge.
5. Disable auto-answer
    a. Auto-answer allows the VTC to automatically answer any incoming call. A third party could call the VTC and automatically be given access to the video and audio of the conference room.
6. Cover the camera when not in use
    a. Point the cameras towards the wall or cover with a manufacture supplied lens cover. If the lens cover is not available a piece of solid cloth will suffice.
    b. A covered lens will prevent third parties from unauthorized viewing of a conference room
7. Disable or mute the microphones when not in use

   a. A muted microphone will prevent third parties from unauthorized listening of a conference room and surrounding areas
8. Display incoming call number and ID of the caller
   a. Identifying the caller will prevent an unknown third party access to the conference room
9. Set a timeout for established administrator sessions
   a. The timeout will force the administrator account to log out after a set period of time
   b. The timeout will prevent a third party from accessing the VTC administrator interface after the administrator has finished.
10. Power-Off VTC when Inactive
   a. Powering off the VTC when not in use will limit the amount of time attackers can try to access the system from the network
   b. Standby or sleep mode does not limit access to the device from the network as the system is still partially powered on.
11. Disable wireless connections
   a. Some VTC have the ability to connect wirelessly in addition to a wired network connection. If wireless is not needed disable or turn off the wireless connection.
   b. Disabling the wireless connection will prevent attackers from connecting to the VTC with a wireless Device.
12. Keep device firmware and software up to date
   a. Device manufactures routinely push out updates with new functionality and security patches. The updates should be applied to close any known security holes that would leave the device vulnerable to attack.

Enhanced Security Recommendations

Note: some features may not be available on all VTC systems

1. Use encryption for conference and point-to-point calls
   a. If AES is not an option use DES encryption. DES is less secure than AES but it is better than no encryption.
2. Display an on screen notice indicating that encryption is active and being used
3. Create a meeting password for all attendees
   a. The password must be one-time use only, do not repeat for additional meetings
   b. Meeting password must be different from any other VTC system passwords (administrator, user, etc.)
4. Passwords typed and echoed to the conference screen must be obfuscated and not displayed in plain text