THINMANAGER®

LEARNING SERIES:

Security with ThinManager & Relevance

The architecture of a ThinManager system in inherently more secure than traditional automation systems.

www.thinmanager.com

One of the many advantages of using ThinManager® with Relevance® is the security it adds to your system.

Thin Client Architecture

Thin client architecture replaces dispersed PCs with thin client hardware and moves all processing to a few centralized Remote Desktop servers. The centralization of processing to a few Remote Desktop servers makes security updates and anti-virus scans easier.

Servers are usually kept in a secure area such as a control room or IT facility that prevents access from unauthorized users. Protect the servers and you protect the sessions running for the thin clients.

Communications between the thin clients and servers are encrypted when using the ThinManager platform.

Thin Client Management

ThinManager is only available to administrators by default. Users have no power running the ThinManager interface. Users from other Windows groups can be granted access to specific ThinManager administrative tools and functions through ThinManager Security Groups.

You can control application access and deployment at the thin client with AppLink. This allows the administrator to deploy specific applications instead of full desktops limiting the user to the applications the administrator has allowed.

ThinManager allows you to obscure user accounts and passwords from the operators.

Shadowing allows an administrator to monitor any thin client at any time providing instant supervision. Terminals can be quickly disabled from the ThinManager interface to stop rogue operators.

The ThinManager database is encrypted for security.

Thin Client Hardware

ThinManager thin clients do not have hard drives. Hardware theft is no longer a concern since corporate applications and data are not stored on the thin client terminals.

The USB ports on ThinManager-managed thin clients do not allow USB storage device access by default. This limits the ability to bring viruses into the system through the thin client. There are no CD/DVD drives for installing viruses either.

All of the network ports on a ThinManager thin client are outgoing. A port scan will not find a listening port on the network to exploit.

Traditional thin clients run a Windows operating system embedded on a chip. These are susceptible to the same security issues that plague the PC. They require security updates and patch management. These operating systems can be exploited and the virus stored on the chip for reinfection. ThinManager thin clients download a fresh copy of the encrypted firmware at each boot. Powering off the ThinManager client will clear the memory, returning the thin client to a neutral state.

ThinManager can enforce password protection for the addition of new hardware, limiting this function to authorized personnel.

ThinManager supports a wide variety of hardware saving you from being controlled by one vendor.

Network and Firewalls

It is a good idea to isolate your process control network from the outside world with firewalls and DMZs. Normally the ThinManager, Remote Desktop Servers, and thin clients are in a secure subnet isolated from the public. ThinManager uses certain ports for communication and the boot process. If ThinManager is separated from the Remote Desktop Servers and thin clients you need to allow access through the following network ports, including in the Windows firewall:

UDP/4900 . . . . . .TFTP - Used for the TFTP download of the firmware.

TCP/2031 . . . . . .Configuration - Used to pass the configuration from the ThinManager Server to the thin client.

UDP/67 . . . . . .IP Address Assignment – Used by the PXE Server (if using PXE boot).

UDP/69 . . . . . .TFTP – Used by the PXE Server (if using PXE boot).

TCP/1494 . . . . . .Citrix - Used by the ICA protocol (if using ICA instead of RDP).

TCP/3389 . . . . . .RDP - Used by the RDP protocol (if using RDP in v2.4.1 or later).

TCP/5900 . . . . . .Shadowing - Used to shadow terminals. This can be changed on the Shadow Configuration page of the ThinManager Server Configuration Wizard.

UDP/1758 . . . . . .Used if the default Multicast is used. If the network MTU size is not the default then the packet size needs changed on the Multicast Configuration page of the ThinManager Server Configuration Wizard.

TCP/3268 . . . . . .Used for LDAP queries targeted at the global catalog.

ICMP Echo Packets (Ping) . . .Used by WinTMC and Enforce Primary.

DHCP . . . . . .The Dynamic Host Configuration Protocol can be used to deliver IP addresses.

Figure 1.

Typical Network Deployment

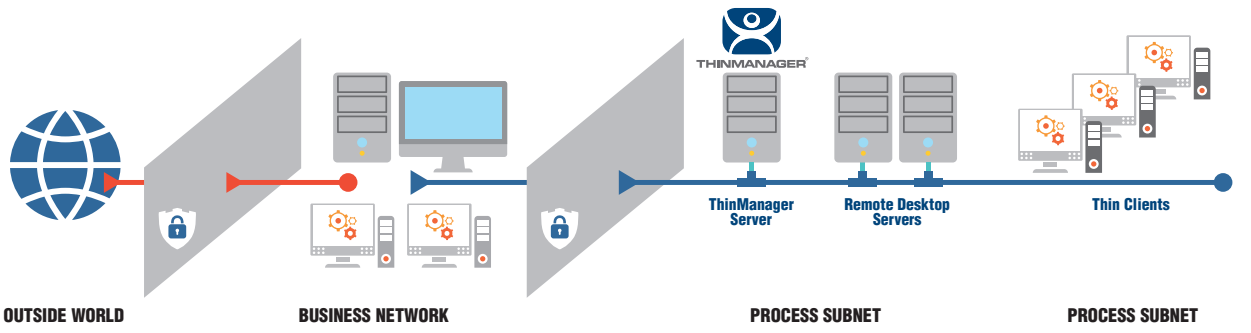
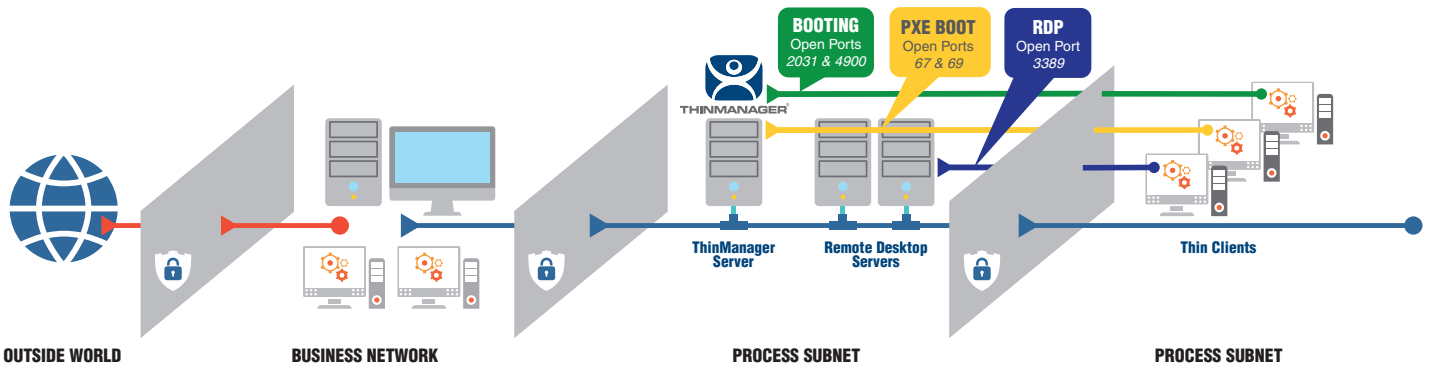


Figure 2.

Subnet Deployment



Anti-Virus and Patching

Anti-virus protection and operating system patching are important for system security and should not be ignored. ThinManager provides two major aids to keep a system protected.

First, the number of servers to protect is greatly reduced by using Remote Desktop Services instead of individual PCs. This reduces the number of tasks to perform.

Second, ThinManager can remove the thin clients from a server and have them automatically switch to a backup with the

Tools>Disable Terminal Server command. The thin clients will stop using the disabled server and will switch to a backup server. Production doesn't stop because the terminals are running on a backup server. This allows you to patch, scan, and reboot the servers one at a time without interfering with production.

Relevance

Relevance uses the TermSecure function to allow you to grant or deny access to applications based on location, permissions and/or group membership. This puts the application deployment under tight administrative control.

Relevance can allow an authorized user to access their apps anywhere in the system while preventing unauthorized users from accessing them.

Encryption

ThinManager uses the Remote Desktop Server encryption for the RDP connection between the Remote Desktop Server and thin clients. The encryption level is set on the server.

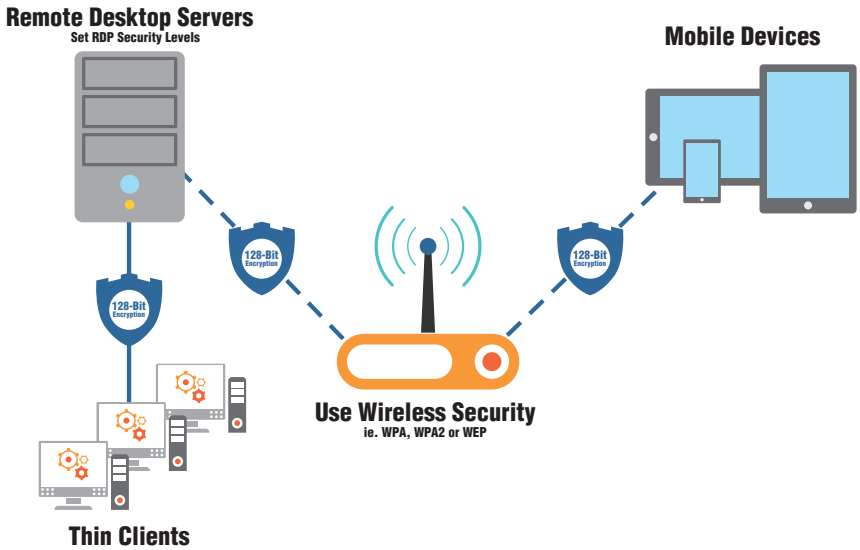
ThinManager supports Network Level Authentication.

The ThinManager Server database is encrypted. Passwords are encrypted again in the database.

The communication between the ThinManager Server and thin clients is encrypted with a 128-bit encryption.

Mobile applications should run on a wireless network protected with WPA, WPA2, or WEP. The communication between the mobile device and the Remote Desktop Servers is encrypted as are all terminal to server communications.

Figure 3.



Mobile Security

Mobile devices can be configured to limit who can run them and where the applications can be run.

Relevance controls deployment of applications to mobile devices sending connections only to the right people in the right places. Relevance limits access on mobile devices to authorized users.

The important part of mobile computing isn't sending applications to mobile devices but is controlling the application from running in unwanted locations. Relevance Fencing creates access zones with Bluetooth, GSP, or Wi-Fi to limit delivery of applications to specific locations. This prevents access in unwanted locations and prevents spoofing of local resolvers like QR codes. The applications will run within the fence but will be unavailable outside the fence.

Active Directory

Active Directory can be integrated into ThinManager on ThinManager Servers that are members of a domain.

ThinManager can use Active Directory to centrally manage Relevance Users. Adding or removing a user in the Active Directory will add or remove the user as a Relevance user in ThinManager.

ThinManager can rotate and update passwords so that the passwords are hidden and automatically changed, obscuring the password from the users. Service accounts can be created using the IT password complexity and duration rules. ThinManager can then be configured to keep them updated automatically following these IT guidelines without requiring manual password control.

High Availability

ThinManager is designed to prevent downtime and provide a short time for recovery if a failure occurs.

ThinManager Failover allows the use of multiple Remote Desktop Servers so that if a server fails the thin client will automatically switch to a backup, log in, and start the deploy applications. Instant Failover allows a second session on a hot backup cutting the time of recovery to a second or two without losing production.

ThinManager can use the Failover function to move terminals from a main Remote Desktop Server to a backup. This allows the thin clients to continue running on the backup without losing production while the main server has maintenance service, patching, updates, and virus scans performed. This allows you to keep your servers updated without losing productivity in a 24/7 operation.

ThinManager thin clients have no moving parts and have a long mean time to failure but are easily replaced if they do fail. The addition of replacements can be controlled by a password so that only authorized personnel can replace them.

Login Strategies

ThinManager provides several login strategies to control access.

Terminals can use physical devices such as HID card readers, biometric fingerprint scanners, or Smart Card readers to log in to the terminal. ThinManager allows you to also require a password with the physical device for authentication.

Public terminals can be configured to automatically log in so operators don't need to know the password. Additional features or applications can be revealed when the user logs in with their specific Relevance User account.

The Key Block module traps unwanted key combinations like CTL+ALT+DEL and ALT+F4 as needed.