THINMANAGER
A ROCKWELL AUTOMATION TECHNOLOGY

Industrial Network and Infrastructure Security with ThinManager

White Paper

Connecting the Enterprise: A Digital Transformation

As corporations across countless industries adopt technologies and infrastructures that enable connected devices, targeted data delivery and enhanced operator experiences, there is an increased cybersecurity risk to these facilities that must be realized. Whether the initiative is described as The Connected Enterprise, Digital Manufacturing, or Industry 4.0, considerations must be made to secure the industrial control network as enterprise level networks are introduced into these environments. ThinManager by Rockwell Automation is purpose built around providing a safe and secure environment for end device management and content delivery and mitigate the risks as we move to a connected industrial environment.

Risk Mitigation

Industry Trends

Securing industrial networks is an important goal of all who work in the industry and has an increased focus in the time of digital transformation of the industrial space. Best practices widely accepted by industry span networks, application hosting, and end devices. Firewalls, port security, IDMZ deployments, and wireless policies help reduce risk of an outside attack to the industrial zone. Strong password policies, encrypted communication, antivirus software, whitelisting of applications, or passive anomaly detection all help prevent loss of data or functionality within the industrial zone. Restriction of access to applications, encrypting local data storage, prevention of removable storage devices and education against social engineering attacks can all lead to a safer environment by protecting end compute devices. All these concepts and more are easily implemented when delivering content to ThinManager managed end devices.

End Device Management

ThinManager removes a majority - in many cases up to 80% - of the Operating Systems that exist when compared to a traditional PC based approach to plant floor architecture. ThinManager can utilize existing hardware that supports PXE, legacy PXE, UEFI, or UEFI PXE in the BIOS of the device to receive a small firmware package that is delivered over the network. These devices once set to PXE\UEFI boot will request two responses upon powering on: PXE\UEFI and DHCP. ThinManager can respond to both requests. Devices that are aware of ThinManager natively, such as the VersaView 5200 industrial thin client, can receive firmware via a TFTP response and do not require a DHCP response unless that is desired. These devices contain the name of the boot loader file they should locate on the network, which can be configured statically.

Once the hardware, regardless of the type, has received the ThinManager firmware, the firmware will be unpackaged into the running memory of the device. No hard drive is required to function as a ThinManager zero client and there is no allowed local storage of either the firmware or any accessed data from the zero client. All information will be stored and accessed from a network location in the form of an RDP or VNC connection to a remote and managed asset such as a Remote Desktop Server.

Once delivered, ThinManager becomes the Operating System of the device and will remain as the operating system as long as the device has power. If the device is powered off, the operating system (ThinManager in this case) falls out of the memory of the device and will retain no intellectual property or any other information. By default, any device managed by ThinManager will restrict access on all USB ports for any peripheral device other than a mouse or keyboard. If

an external storage device including USB/CD/DVD/floppy or any other device such as a scanner or scale is to be allowed to communicate with a Remote Desktop Session that is delivered to the managed client, the device must be allowed explicitly by adding a Module to the configuration of that device in ThinManager. In addition to restriction of access to peripheral devices, Modules such as the Key Block Module can be configured to prevent undesirable keystroke combinations such as CTRL+ALT+DEL or ALT+F4 from being passed from the keyboard on the device to the session running on the centrally managed server.

When a device is power cycled, the ThinManager server contains the MAC address of the device and associates that with a Terminal Profile, which is a prescription of what is to be visualized on that physical piece of hardware. In the event of a hardware failure of an end device, a process called terminal replacement can be initiated. This process involves replacing the failed hardware with a functional client. When the device receives its firmware and unpackages the firmware into the ThinManager operating system, the ThinManager server will not recognize the MAC address of the new device. The operator needs only to know the name of the device as it is named in ThinManager. This process allows for the old hardware to be quickly replaced and does not require the new hardware to go through a rigorous validation process as there is no local OS or applications installed. For increased security, this process can be password protected, require the same model hardware, or can be turned off completely.

Secure Delivery of Content and Application Centralization

ThinManager provides the platform to deliver content to an end device such as a mobile device or zero client without the need to locally host applications or data on any of those end devices or terminals. Reducing the number of operating systems reduces the number of applications that need to be maintained and patched. ThinManager centralizes the deployment of applications to end devices and secures and encrypts the communication from the application hosts (Remote Desktop Servers, VNC Servers, IP cameras, and Workstations) to the end devices. Encrypted RDP communications if allowed by the host servers (Sever 2008 or newer) will negotiate the security level to the TLS 1.2 protocol. ThinManager utilizes a low port count for deployments

Port	Protocol	Description
UDP 67	DHCP -	Used by the PXE Server (if using PXE boot hardware).
UDP 69	TFTP	Used to TFTP the firmware and modules to ThinManager Compatible thin clients.
TCP 443[O]	HTTPS	Used for establishing HTTPS SSL tunnels to the RD Gateway.
TCP 1494[O]	ICA	Used by the ICA protocol (if using Citrix ICA instead of RDP).
UDP 1758[C]	Multicast TFTP	Used if Multicast is enabled in ThinManager.
TCP 2031	Proprietary	Used to pass the configuration from the ThinManager Server to the terminal and used for automatic Synchronization between ThinManager servers.
TCP 3268	LDAP	Used for domain authentication using the Lightweight Directory Access Protocol.
TCP 3389[C]	RDP	Used by the RDP protocol. Connection is initiated by thin client to RD server
UDP 3391[O]	Datagram	Allows the transport to create connection to RD Gateway (Only required if RDP over UDP is enabled, otherwise defaults to TCP 443).
UDP 4011	DHCP	Used by the ThinManager PXE Service when a standard DHCP server is installed on the same computer as ThinManager. This port is used when booting ThinManager Compatible PXE boot thin clients using the UEFI (Unified Extensible Firmware Interface) BIOS. (ThinManager 11)
UDP 4900	TFTP	Used to TFTP the firmware to ThinManager Ready thin clients
TCP 5900[C]	Proprietary VNC	Proprietary Shadow Protocol, VNC initiated by thin client to VNC Server.

which further increases the security of the system reducing the total number of firewall rules that need to be created across servers and network layers. The following port list outlines the ports which are used for deployment of a ThinManager managed system. Ports listed with an O are optional and are not required for core functionality and ports listed with the C designation are configurable within the product.

Utilizing the ApplicationLink feature of ThinManager restricts access to anything on the end device other than the application required by the end user to perform their required job. Delivery of applications as opposed to full desktop experiences is suggested and supported within ThinManager and reduces an operator's access to applications such as File Explorer, web browsers, or other system level information. This will also prevent operators from establishing RDP connections from one server to another. ApplicationLink can be configured on a Remote Desktop Server by either publishing RemoteApps as a part of a Session Collection in the Remote Desktop Services Deployment or by changing the Group Policy of the Remote Desktop Host to allow the remote start of unlisted applications. In either case, operator terminals will only provide access to the set of applications allowed by the ThinManager administrator. When running the FactoryTalk View SE application on a ThinManager managed terminal, there is native functionality called Authentication Pass-Through which will log in any named user that logs into that device. When the user logs into a device, the service account that was used for auto-login will be logged out of the FactoryTalk View SE client and will login the named user, regardless of the authentication method they are using. This is native integration between the products that checks out and checks in the RNA security token as a part of FactoryTalk Security. Note that Authentication Pass-Through requires the use of domain users.

ThinManager can further increase the security of the system by increasing the level of authentication to the system in requiring multiple authentication factors for applications that currently do not require more than one form of authentication. Additional login authentication can take the form of a badge being passed over a badge reader, PIN number, smart bands or biometrics. Any of the authentication methods can also be used as an alternative to using Windows credentials. To use an alternative login method, the Windows username and password must either be stored in the encrypted ThinManager database or can be cached for a configurable duration of time. Password caching would prompt a user for their credentials once during the configured time limit and allow for an alternative login method to be used to establish a connection to Windows applications for the duration of that time.

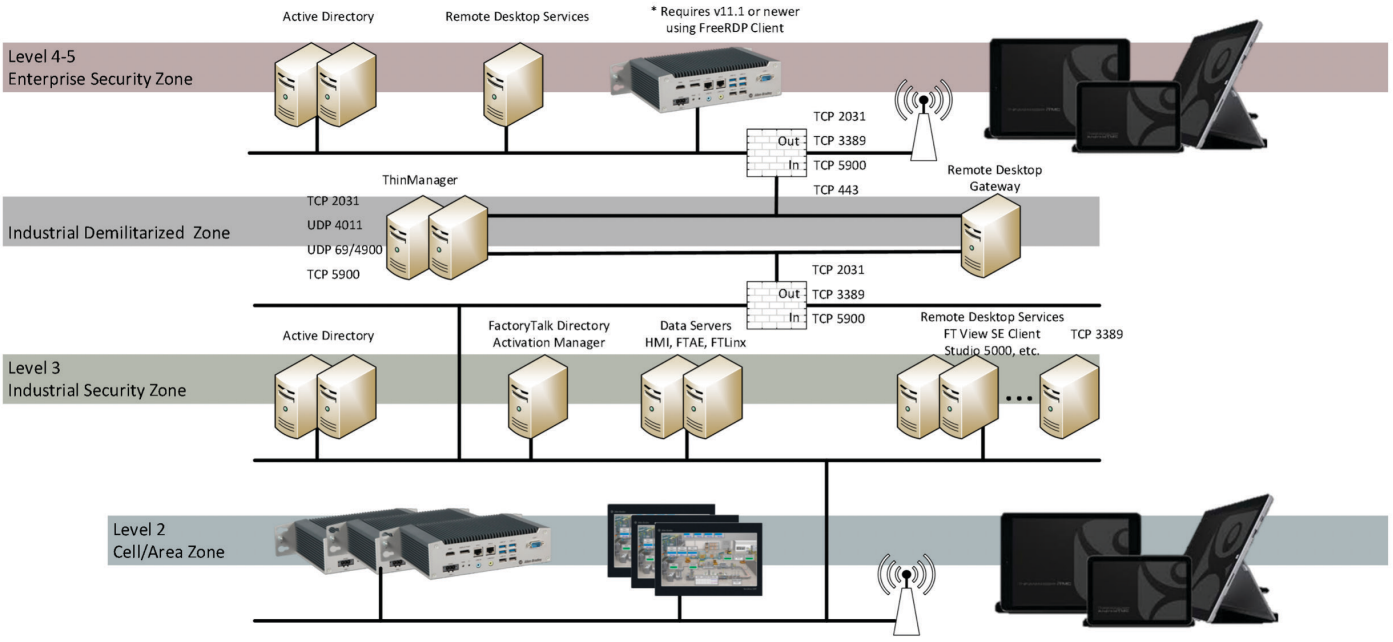
ThinManager supports users to be members of an Active Directory Group or Organizational Unit within Active Directory. Accounts that would typically be used as service accounts or generic device accounts, if stored in the encrypted database to allow auto-login of the applications on the end devices, can be synchronized such that they will be updated and maintained by ThinManager. Enabling Active Directory Synchronization within ThinManager maintains that all service accounts used to auto-login applications on devices will be updated regularly inside of Active Directory and re-synchronized with ThinManager so that these accounts comply to any IT mandated password retention policies.

To manage access to the ThinManager user interface, ThinManager Security Groups can be configured to allow different accesses to the application for different Windows Security Groups. By default, all Administrators have full access to the ThinManager user interface. An Engineering group could be configured to be granted a subset of those permissions, for example, granted permissions to change the terminal, but not granted access to manage the Remote Desktop Servers that are members of the deployment.

Secure Architectures

Network Segmentation

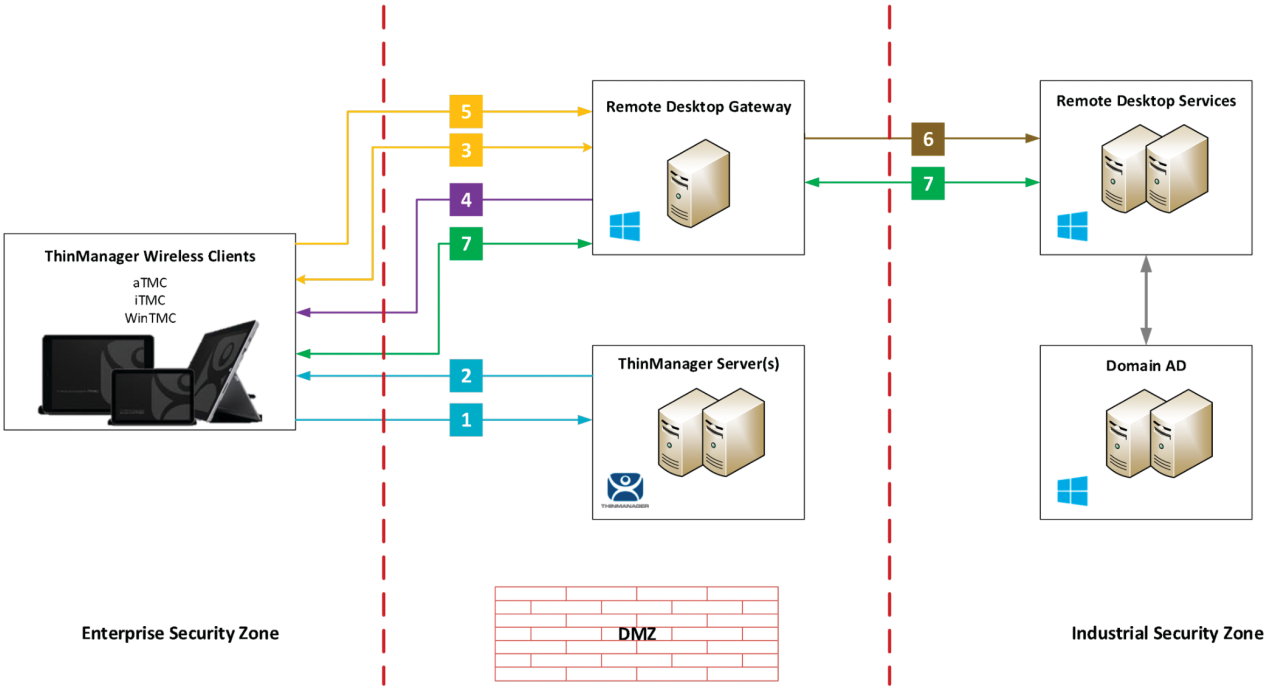
Network segmentation is critical to maintaining a secure environment across multiple layers of a control network. In the drawing below, the ThinManager server is located inside of the Industrial Demilitarized Zone (IDMZ). This separates the Industrial Security Zone and the Enterprise Security Zone and does not permit, by rule, any network traffic to traverse the zone without being redirected by some form of proxy. By placing ThinManager inside of the IDMZ, no traffic is required to traverse directly across the IDMZ in order to deliver terminal profiles or firmware from the ThinManager server to the zero clients or mobile devices. *NOTE: The ThinManager servers can also be placed on either side of the IDMZ to mitigate any challenges faced if the IDMZ were to become unreachable.*



ThinManager Reference Network Architecture Segmentation

Network Architecture Development

RD Gateway will be a critical component of the deployment that will be required to deliver content from the Industrial Security Zone to the Enterprise Security Zone. In addition to traditional ThinManager thin client devices, ThinManager clients (WinTMC, aTMC, or iTMC) can be used to visualize content in this direction from a Remote Desktop Server containing industrial data or applications. These will be discussed in detail in the next section. Remote Desktop Gateway (RDG) is a very important component in securing an RDS deployment, RDG is a server that sits usually in a DMZ and acts as a middleman. When a client initiates a connection, RDG first establishes SSL tunnels between itself and the external client. Next, RDG vets the client's user (and optionally the computer) credentials to make sure that the user / computer are authorized to connect to RDG. Then RDG makes sure the client is allowed to connect to the requested resource. If the request is authorized, then RDG sets up an RDP connection between itself and the internal resource. All communication between the external client and the internal endpoint goes through RDG.



RD Gateway and ThinManager Mobile Clients Data Flow Overview

Network flow number	Ports Used
1	TCP 2031: ThinClient initiated connection to ThinManager server
2	TCP 2031: Used to pass the configuration (terminal profile) from the ThinManager Server to the terminal (connection initiated from ThinClient)
3	TCP 443: RD Gateway establishes HTTPS SSL tunnels, (allows HTTPS traffic to the RD Gateway
4	RD Gateway authenticate the client's user
5	UDP 3391: Allows the transport to create that connection (Only required if RDP over UDP is enabled, otherwise defaults to TCP 443).
6	TCP 3389: Allows the RD gateway to forward RDP packets
7	Communications between the thin client and RDS server

1. TMC request terminal profile from ThinManager server (Port 2031 TCP).
2. ThinManager informs TMC to use RD Gateway for the connection point requested display content.
3. RD Gateway establishes HTTPS SSL tunnels (Port 443 TCP) between itself and the external client (one for incoming data and one for outgoing data).
4. Next, RD Gateway authenticates the client's user (and optionally the computer) credentials to make sure that the user / computer are authorized to connect to RD Gateway. Once the tunnels are established, the client and RD Gateway establish a main channel over each tunnel.
5. Once the HTTPS transport channels are enabled, to optimize the transport of data UDP sets up two side channels (Port 3391 UDP), to provide both reliable (RDP-UDP-R) and best-effort (RDP-UDP-L) delivery of data. The UDP tunnel uses DTLS to secure its communications so will also utilize the SSL certificate in place on the RD Gateway server.
6. Then RD Gateway makes sure the client is allowed to connect to the requested resource. If the request is authorized, then RD Gateway sets up an RDP connection (Port 3389 TCP) between itself and the internal resource. All communication between the external client and the internal endpoint goes through RD Gateway.
7. TMC is commenced via RD Gateway to the RDS/ThinManager server and content is delivered to the TMC.

Secure Mobility

Relevance is the commercial terminology used by the product that encompasses the delivery of content to users and locations. Relevance delivers user and/or location-based content delivery that promotes a line of sight to machine control that will be enabled on a mobile device, places security around access to applications and can transfer ownership of an application from one terminal to another. Relevance user and location services do not replace the need for traditional hardware for safety purposes but can help enhance the users experience and productivity. There are three different applications that can be utilized to turn a mobile device or PC into a ThinManager terminal: iTMC (iOS ThinManager client), aTMC (Android) and WinTMC (Windows). For mobile devices, firmware is not delivered to replace or act as the local operating system, but rather an application is installed from the respective online store and used to connect to the ThinManager server by specifying the DNS name or IP address of the ThinManager server.

When delivering content to a mobile device using ThinManager, there is no local installation or management of the desired applications. Applications get delivered to the device when the application is launched and is connected to the appropriate network. If the mobile device has not correctly authenticated on the network, none of the client applications will be able to establish connection to the device.

Security can be placed around applications once connected to the network by requiring a specific user or member of a user group to be logged into the mobile device to access an application. If the user is not logged in, the application will not be visible.

Safety can also be included in the solution by utilizing Location Resolvers, or location identifiers. There are four ways that ThinManager can identify or resolve a location: QR Codes, Bluetooth Beacons, Wireless Access Points, and GPS. When a mobile device comes within the configurable range of one of the resolvers, content is delivered to the device. When the resolver is out of range, content is removed from the device.

Integrating the concepts of user and location delivered content together completes the Relevance solution offering ensuring that content is only available to the right person and the right place. If an application is only visible to an engineer, an operator would not be able to scan a QR code to receive that content. If that content was something related to machine control, line of sight should be maintained to whatever process of which the engineer had control. Multiple location resolvers could be used to accomplish this action. For example, the engineer could log into the mobile client, scan a QR code that was near a Bluetooth Beacon to receive an application for machine control. If that engineer then took the mobile client outside of the configured Bluetooth range, they would lose the content, preventing them from performing dangerous activities without having line of sight to the equipment they were controlling.

The aggregation of device, user, and location delivered content from ThinManager safely and securely achieves device management and centralized content management and delivery.

TM-WP001C-EN-P

Revised 3/3/22

ThinManager
1220 Old Alpharetta Rd
Suite 390
Alpharetta, GA 30005

www.thinmanager.com
1-877-239-4282
sales@thinmanager.com