Session Agenda

- Solution Introduction & Overview
- Available Technology: Strategies, Considerations, & Limitations
- Best Practices
- Resources
- InTouch Application Migration
- Q&A
Technology & Trends

● Mobility: Data consumers & smart devices.
● Internet is everywhere.
● Cloud computing.
● "Is there an app for that?"
● Applications abstracted from devices.
● Increased connectivity requires security.
Why Remote Access?

Information consumers remote from process and/or IT assets.

- Operators (real-time HMI interaction, alarm/event response, workflow)
- Post-activity (overview, reports, analysis, dashboards)

Remote Engineering/Maintenance Support

- Multiple sites with centralized support resources.
- After-hours or off-shift support.
- Integrators and OEMS.
Leverage IT Infrastructure

● Consolidated Hardware/Virtualization/Reduced Administration

● Support new software versions on legacy client hardware.
  ● Operating systems, applications
  ● Access multiple versions (ex. InTouch 9.5, InTouch 10.5)

● Extend industrial applications to administrative assets/users.

● Minimize downtime & risk associated with plant-floor or remote client asset failure.
  ● Replace and re-connect with standard client hardware.
  ● No need to reinstall WW apps on the client machine.
Challenges & Obstacles: Common Characteristics

Industrial Software is Microsoft Platform-Centric

- Operating Systems
- SQL Databases
- Back-end technology: .NET, WCF, DCOM, Visual Studio
- Front-end delivery: IIS, SSRS, XML, ActiveX, .NET Controls

Specific Hardware Requirements:

- Server and Client machines, often multi-node
- CPU, Memory, HDD requirements
- High Availability, Redundancy, Failover
- Network and Power infrastructure
Security Objectives: Right Info to Right People at Right Time

Threats:
- Antivirus/malware
- Hacking/Espionage

Protection:
- Facility/Process/Machine
- Network
- Device
Variety of Solutions Available Today

Technology
- RDS (Microsoft)
- Web Apps (HTML, SSL, HTML5)
- Mobile Devices and OS (iOS & Android)
- Email & SMS Interaction

Strategy: Two Approaches
- Extend the server/workstation experience to the mobile worker.
- Allow the mobile worker to interact with remote systems via mobile-centric technology
Extend the Server/Workstation Experience to the Mobile Worker

- Remote Desktop Services
- Virtual Desktop
- Remote Applications (aka published apps)
- Usually done with gateway or mirror type app on the remote device.
Remote Desktop Architecture Overview
Remote Desktop Services Evolution

Terminal Services
Terminal Services Advanced Client

Terminal Services
RemoteApp™
TS Gateway
TS Session Broker
TS Web Access
Terminal Server

Terminal Services Advanced Client
RemoteApp™
RD Gateway
RD Connection Broker
RD Web Access
RD Session Host
RD Virtual Host
RemoteApp & Desktop Connections
Solution Security Requirements

- Authentication (right user with right credentials)
- Encryption (securing data transmitted across the web)
- Solutions: VPN, SSL, HTML5

  - Endpoints:
    - Applications
    - Devices
    - Protocol (IPSec, SSL, etc.)
  - Clients
  - Limitations and challenges:
    - Infrastructure (technology & cost)
    - Supported devices and OS vary
    - Administrative requirements
Remote Desktop Protocol (RDP)

- Proprietary protocol developed by Microsoft
- Enables GUI extension from one computer to another.
- Requires both server & client software components.
- IP port 3389 (default)
RDP 7.0 Performance Enhancements

Improved Bulk Compression: Applied to all data, including graphics

Four choices controlled by server group policy:
1. Optimized to use less memory
2. Balanced use of memory and bandwidth
3. Default: Optimized to use less bandwidth
4. Disable bulk compression

Bandwidth - Kbps

<table>
<thead>
<tr>
<th>Typing and Scrolling</th>
<th>Scrolling</th>
</tr>
</thead>
<tbody>
<tr>
<td>XP (RDP 5.2)</td>
<td>Vista (RDP 6.0)</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
</tr>
</tbody>
</table>

Bandwidth Improvement per release

<table>
<thead>
<tr>
<th>Executive PPT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7 (RDP 7.0)</td>
</tr>
<tr>
<td>Min. 20% Gain!</td>
</tr>
</tbody>
</table>

Typing and Scrolling: XP (RDP 5.2) improves by 20%, Vista (RDP 6.0) improves by 10%.

Scrolling: XP (RDP 5.2) improves by 15%, Vista (RDP 6.0) improves by 5%.
RDP Servers & Clients

Servers:

● Remote Desktop (OS-integrated)
● Remote Desktop Services (server role)

Clients:

● Remote Desktop Connection
● RDS RemoteApps
● 3rd-Party solutions using RDP.
Remote Desktop Session Host

- Formerly known as “Terminal Server”
- Multiple user sessions run on one server.
- Scalable via server farms.
  - Load balancing
  - Redundancy
- Historically used with InTouch HMI
  - Multiple users
  - Thin clients
- Best Practice: Install RDS before installing user applications.
Remote Desktop Connection Broker

- RDS Load Balancing & Failover in multi-server RDS environment.
- Requires MS Active Directory domain.
Remote Desktop Connection (RDC)

- Microsoft RDP Client solution.
- Included with Windows XP and newer OS.
RemoteApps

- Applications launched from Web Page
- Programs look like they are running locally
- Extend applications without exposing remote desktop & files
- Assign specific apps to groups/users via Active Directory
- Create MSI or RDP files (MSI not available on 2012R2)
- Not natively supported on iOS platform
- Best Practice: Use RemoteApps to run Wonderware runtime applications
  - RD Session opens and closes with RemoteApp (vs. RDC.)
  - InTouch 2012 R2 LogonCurrentUser function enables OS pass-through of session user credentials to InTouch
Remote Desktop Web Access

- Web portal for published RemoteApps or RD sessions.
- Simple convenient extension of available apps for specific user groups on unspecific hardware.
- Not supported on non-Microsoft platform, due to reliance on RDP and ActiveX.
Remote Desktop Gateway

- Extend Remote Web Access beyond intranet firewall to outside users.
- Encapsulates RDP in SSL (HTTPS)
- Secure connection:
  - User Authentication
  - Security Certificate
  - Data encryption
Remote Desktop Virtualization Host

- Personal Virtual Desktops
- Pooled Virtual Desktops

RD Client
RD Connection Broker
Active Directory
## RDS Roles Summary

<table>
<thead>
<tr>
<th>Role</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoteApp</td>
<td>Publishes applications with just the application UI, and not a full desktop UI</td>
</tr>
<tr>
<td>RD Session Host</td>
<td>Hosts centralized, session-based applications and remote desktops</td>
</tr>
<tr>
<td>RD Virtualization Host</td>
<td>Hosts centralized, virtual-machine-based (virtual) desktops on top of Hyper-V for VDI environment</td>
</tr>
<tr>
<td>RD Connection Broker</td>
<td>Creates unified administrator experience for session-based and virtual-machine based remote desktops</td>
</tr>
<tr>
<td>RD Gateway</td>
<td>Allows connection from clients outside the firewall, using SSL, and proxies those to internal resources</td>
</tr>
<tr>
<td>RD Web Access RemoteApp &amp; Desktop Connections (Windows 7 and later)</td>
<td>RD Web Access provides Web-based connection to resources published by RD Connection Broker. Supports traditional web page, as well as new RemoteApp &amp; Desktop Connections</td>
</tr>
</tbody>
</table>
Windows Server 2012

New features of Windows Server 2012:

- Predictable user experience to ensure that one user does not negatively impact the performance of another user’s session.
- Dynamically distributes available bandwidth across sessions.
- Prevents sessions from over utilizing disk.
- Dynamically distributes processor time across sessions.

RD Virtualization Host (2012):

- Integrates with Hyper-V to deploy pooled or personal virtual desktop collections by using RemoteApp and Desktop Connection.
Windows Server 2012 R2

- Session Shadowing - monitor or control an active session of another user.
- Quick Reconnect improves connection performance enabling users to reconnect to their existing virtual desktops, RemoteApp programs, and session-based desktops more quickly display changes on the client to be automatically reflected on the remote client.
- Additional Hyper-V virtualization features supporting fast live migration, live export, live vhdx resize, export snapshot, and replica for disaster recovery.
Microsoft Remote Desktop Licensing

In addition to a Windows Server Client Access License, Microsoft Core CAL Suite, or Microsoft Enterprise CAL Suite, you must acquire a Windows Server 2012 RDS CAL for each user or device that directly or indirectly accesses the server software to interact with a remote graphical user interface.

RDS Device CAL: Permits one device (used by any user).
RDS User CAL: Permits one user (using any device).
RDS External Connector: Permits multiple external users to access a single Remote Desktop server (ie. Non-Employees)
Microsoft Remote Desktop Desktop Licensing

Temporarily reassign your device CAL to a loaner device while the first device is out of service your user CAL to a temporary worker while the worker is absent

RDS CAL is required when using a third-party technology (e.g. ACP).

RDS CAL is required when hosting on Vmware.
Wonderware InTouch Licensing

Wonderware licensing:

- Read Only/Read Write
  - Device licenses
  - Concurrent licenses
- Failover/Load Balance

Client always needs a WWCA when connecting to a WW Historian and always needs an MSCA when connecting to any Microsoft MSSQL database

- CAL is included with InTouch for System Platform
Wonderware InTouch Licensing

Can't mix TSE license types on a Remote Desktop Services server.

- Concurrent vs Device
- 2104 R2 allows Read Only/Read Write on same node

InTouch for Terminal Services 2012 Feature line:

VENDOR_STRING=count:5 Sample InTouch 2012 License FEATURE InTouch Wonderware 10.5 1-jan-00 uncounted \ VENDOR_STRING=ltags:61402; rrefs:61402; mode:3 HOSTID=ANY \ FEATURE InTouch_TSE Wonderware 10.5 1-jan-00 uncounted \ VENDOR_STRING=count:5 HOSTID=ANY
Introducing InTouch Access Anywhere

- Full web-based access to InTouch applications from anywhere anytime regardless of platform or location.
- Runs in HTML5-compliant browsers (IE, Safari, Chrome, Firefox, etc.)
- No Flash, Java, ActiveX, Silverlight or other special software needed.
- Doesn’t require installing or configuring any client-side applications.
- Platform-agnostic:
  - Runs on a variety of devices (Desktops, Laptops, Tablets, Smart Phones, Smart TVs and more)
  - Running on a variety of platforms (Windows, iOS, Android, Linux,…)
- Provides secure access
  - Same OS-based security as Remote Desktop
  - Supports HTTP, HTTPS, and SSL.
  - Natively supports RDP encryption.
InTouch Access Anywhere

Plant

Any location

REMOTE ACCESS

Casual Users

Mobile Users

Remote Access

Automation Object Server

Automation Object Server

Galaxy Repository

Historian

InTouch Terminal Server

+ InTouch Access Anywhere

I/O Data Server

Industrial Computer

Visualization Node

Engineering Station

InTouch Access Anywhere
Technology Overview

- Remote Desktop Protocol (RDP): Remote display protocol developed by Microsoft, included with Windows OS.
- Remote Desktop Services – Terminal Services
  - RDS Host (RD Server, Terminal Server)
  - RDS Client (RD Connection, 3rd-party applications)
  - RDS hosts & clients communicate via RDP
- HTML5 <canvas> tag: draws 2D graphics on the fly via scripting.
- WebSockets: Secure full-duplex single socket TCP connection between HTML5 servers and clients. Connection remains open once established.
- InTouch Access Anywhere Server: Securely translates RDP from RD Server to HTML5 format for remote HTML5 clients. Secure communication occurs via WebSockets.
RDP Compression and Acceleration

- Enhances remote desktop performance over the Internet.
- Image compression: Compresses images before transmitting them to the browser for rendering.
- Packet shaping: Optimizes the network messages to improve network utilization and performance.
- Whole frame rendering: The display is updated as a whole rather than in blocks, as performed by standard RDP. Coupled with the other optimization features, it results in a smoother display that more closely resembles the functionality on local desktops.
Topologies: Behind the Firewall

1. The user initiates the process by pointing an HTML5 browser to the machine hosting the InTouch Access Anywhere software.

Security.

A. OS security is used to start a session. User provides his/her Windows Username and Password.
B. Communications between server and client take place using WebSockets over HTTP or Secure HTTP (HTTPS).
C. By default, the client (browser) connects to InTouch Access Anywhere using port 8080. This port can be changed in the configuration.

No data is transferred, only mouse clicks, keystrokes and gestures from the remote user to the RDP host and graphics from the RDP host to the client end.
Topologies: Beyond the Firewall

1. The user initiates the process by pointing an HTML5 browser to the machine hosting the InTouch Access Anywhere software.
2. When using the Secure Gateway, the Access Anywhere browser session will connect through it.

Security.
A. OS security is used to start a session. User provides his/her Windows Username and Password.
B. Communications between server and client take place using WebSockets over HTTP or Secure HTTP (HTTPS).
C. By default, the client (browser) connects to the InTouch Access Anywhere Server using port 8080. This port is can be changed in the configuration.
D. InTouch Access Anywhere supports strong SSL encryption.
E. By default InTouch Access Anywhere uses the same security settings as Microsoft RDP. If Microsoft RDP is encrypted, then InTouch Access Anywhere will be encrypted.
F. When using the Secure Gateway, the connection between InTouch Access Anywhere browser client and the Secure Gateway is always secured.
G. The Secure Gateway Authentication Service must authenticate against an Active Directory.
System Requirements

Server side

- Windows Server OS (Windows 2008 Server SP2, Server 2012,R2)
- Remote Desktop
- InTouch 2012 R2 and later
- InTouch TSE Concurrent licenses

Client End: HTML5 compatible browser including, but not limited to:

- Internet Explorer 10 or IE6 - IE9 (with Google Chrome Frame)
- Chrome 12 or higher
- Safari 5 or higher
- Firefox 6 or higher
- Opera 11 or higher
- Amazon Silk
Remote User Log-In

1. Open a web browser
2. Enter URL or IP of the InTouch Access Anywhere Server
3. Select InTouch application (if more than one exists on the server.)
4. Enter valid credentials
5. Click on “Connect”
InTouch Thin Client Implementation

BEST PRACTICES
Windows Server 2012 & 2012 R2

**** Microsoft Numbers******
● Up to 5000 users per server.
● Up to 1000 Remote Desktop sessions VIA Connection Broker.
● Recommended up to 150 sessions per physical host.
● Recommended SSD disk storage.
● Recommended up to 150 sessions per virtual host.
● Best with 64-bit OS, multiple core, lots of GHz, large L2/L3 cache, virtualized, page file separate storage, RAID disk, “green” balanced power plan.
● Network adapters - server rated
System Implementation Options

- Network Load Balancing - round robin allocation of sessions within a cluster of servers
- High availability – Hyper-V or VMware virtual Remote Desktop Services servers
  - Appropriate attention to Hard Drive Resources
- Managed Apps - deploy a SINGLE Engine to the Remote Desktop Server
  - Each client session manages its own instance
- InTouch Published - NAD recommended
- ACP ThinManager increases the available client types to non Windows-based
  - ThinManager clients run on workstations, including UNIX, Linux, and industrial display panels.
RDS Security Best Practices

- Standard RDP (port 3389) via VPN
- SSL RDP (port 443) via RD Gateway or ITAA Secure Gateway
- Network Level Authentication (NLA)
  - Requires RDP version 6.0 (Windows Vista) or later.
- Prevent access to the OS for most users.
  - Use RD RemoteApps (previously “Published Applications” in TS)
  - Don’t allow Remote Desktop Connection if not necessary.
  - Use InTouch Access Anywhere
- Obtain commercial security certificates, rather than creating self-signed certificates.
Remote Desktop Services Setup

Session configuration

- End a disconnected session [minutes or never]
- Active session limit [minutes or never]
- Idle session limit [minutes or never]
- When a session limit is reached [disconnect - enable automatic reconnection or end]

User profiles

- Local [created first time logged on]
- Roaming [copy of local profile]
- Mandatory [local lost when logged off]
- Temporary [upon error]
InTouch TSE: Basic Rules

- Application development and client visualization are placed on separate computers
  - Licensing Conflict - you will lose a View session if you combine Dev and TSE
- Deploy each InTouch application to the server running InTouch TSE
  - Managed Application 10.x or later ("push" from dev to runtime.)
    - InTouch for SP or Tag Based
  - InTouch VIEW.EXE automatic startup (Environment) or RemoteApp
  - Remote Desktop Services client session unique user logon - determines which InTouch application is launched
  - Selected App stored in Win.ini - C:\Users\<UserName>\AppData\Local\Wonderware
  - ITAA or InTouch App Manager allows Application Selection
- InTouch runs as application, not as a service
- When communicating to another view session, include the server node name and append the IP address of the desired session to the application name. Example: view:10.103.25.6
Sizing Guidelines

Operating System Sizing

- InTouch RDS Server
  - Windows 2008 R2
  - Lots of Cores (16), Lots of Memory (48GB)
  - Solid State Disks
  - 25 - 75 Sessions per Server (YMMV)
Additional InTouch TSE Considerations

● Application security is configured according to the Managed Application Galaxy model or Standalone or Published applications individual security model
● User credentials if needed are passed in from the RDP session client - available via LogonCurrentUser()
● Use TseGetClientId( ) in QuickScript to manage location based behavior
InTouch Access Anywhere: Best Practices

- Develop InTouch application for client device resolution.
- Create different applications for different users, roles, or devices.
- Plan RDS session timeout period based on user role:
  - Short timeout for casual users.
  - Longer or no timeout for operators.
- Not supported with NLA enabled on the RDS server.
- Leverage multiple virtual servers to distribute load and/or to allocate different InTouch TSE license types (Concurrent separated from Device and User)
Migrating InTouch to RDS

• The Vast majority of InTouch Applications require no major modifications.
  • Tag Server apps are a breeze – Deploy the Tag Client App in RDS

• IO Server
  • By default The InTouch Session will look to the Host Name
  • DAS Server configured as Service

• Alarm Provider(s) - Client AlarmViewer query must be configured appropriately for TSE
  • This is the primary task in migrating to RDS - #1 cause of problems
    • “Console” Application (Host IP address)
Microsoft Resources

- Remote Desktop Services Deployment Guide
  
- Remote Desktop Services Home Page

- Remote Desktop Services TechNet Site

- Remote Desktop Services Blog
  http://blogs.msdn.com/rds/

- Desktop Virtualization and VDI
Wonderware Resources

- Documentation: InTouch for Terminal Services Deployment Guide
  - InTouch_TSE_DG_10.pdf
- Tech Note 538: InTouch© TSE version 10.0 Application Configuration: Managed, Published and Standalone Methods
- TechNote 971: Configuring Resolution Settings for InTouch Running on Terminal Services Sessions
- Deployment: Hosting Applications with Terminal Server
Migrating InTouch to RDS

- The Vast majority of InTouch Applications require no major modifications.
  - Tag Server apps are a breeze – Deploy the Tag Client App in RDS

- IO Server
  - By default The InTouch Session will look to the Host Name

- Alarm Provider(s)
  - This is the primary task in migrating to RDS
    - “Console” Application (Host IP address)
    - `\nodeabc:253.127.148.120\intouch!$system`
Questions?

- Do I have to have RDS installed somewhere?
Related Support, Services, Training & Expo Demos

Support
- [insert Support options here]
- [sample: Proactive System Monitoring]
- [sample: Software Asset Manager]
- [sample: …]

Training
- [insert Training options here]
- [sample: Application Server 2012 R2 Web-Based Training]
- [sample: InTouch Alarms Webinar]
- [sample: …]

Services
- [insert Services options here]
- [sample: Project Mgmt Services]
- [sample: …]
- [sample: …]

Expo Demos
- [insert related Expo Demos here]
- [sample: Control Room Console for W&WW (booth #2)]
- [sample: Process Information with Historian (booth #4)]
- [sample: …]
Thank you!
REFERENCE
Remote Desktop Virtualization Host

Remote Desktop Virtualization Host (RD Virtualization Host) is a Remote Desktop Services role service included with Windows Server 2008 R2. RD Virtualization Host integrates with Hyper-V to provide virtual machines by using RemoteApp and Desktop Connection. RD Virtualization Host can be configured so that each user in your organization is assigned a unique virtual machine, or users are redirected to a shared virtual machine pool where a virtual machine is dynamically assigned.

RD Virtualization Host uses Remote Desktop Connection Broker (RD Connection Broker) to determine where the user is redirected. If a user is assigned and requests a personal virtual desktop, RD Connection Broker redirects the user to this virtual machine. If the virtual machine is not turned on, RD Virtualization Host turns on the virtual machine and then connects the user. If the user is connecting to a shared virtual machine pool, RD Connection Broker first checks to see if the user has a disconnected session in the pool. If the user has a disconnected session, they are reconnected to that virtual machine. If the user does not have a disconnected session, a virtual machine in that pool is dynamically assigned to the user, if one is available.

For more information about installing and configuring RD Virtualization Host, see the RD Virtualization Host Step-by-Step Guide (http://go.microsoft.com/fwlink/?LinkId=137796).
Overview of RD Virtualization Host

Remote Desktop Virtualization Host (RD Virtualization Host) is a Remote Desktop Services role service included with Windows Server 2008 R2. RD Virtualization Host integrates with Hyper-V to provide virtual machines by using RemoteApp and Desktop Connection. RD Virtualization Host can be configured so that each user in your organization is assigned a unique virtual machine, or users are redirected to a shared virtual machine pool where a virtual machine is dynamically assigned.

RD Virtualization Host uses Remote Desktop Connection Broker (RD Connection Broker) to determine where the user is redirected. If a user is assigned and requests a personal virtual desktop, RD Connection Broker redirects the user to this virtual machine. If the virtual machine is not turned on, RD Virtualization Host turns on the virtual machine and then connects the user. If the user is connecting to a shared virtual machine pool, RD Connection Broker first checks to see if the user has a disconnected session in the pool. If the user has a disconnected session, they are reconnected to that virtual machine. If the user does not have a disconnected session, a virtual machine in that pool is dynamically assigned to the user, if one is available.
Remote Desktop Connection Broker

- Remote Desktop Connection Broker (RD Connection Broker), formerly Terminal Services Session Broker (TS Session Broker), is a role service that provides the following functionality:

- Allows users to reconnect to their existing sessions in a load-balanced RD Session Host server farm. This prevents a user with a disconnected session from being connected to a different RD Session Host server in the farm and starting a new session.

- Enables you to evenly distribute the session load among RD Session Host servers in a load-balanced RD Session Host server farm.

- Provides users access to virtual desktops hosted on RD Virtualization Host servers and to RemoteApp programs hosted on RD Session Host servers through RemoteApp and Desktop Connection. RD Connection Broker keeps track of user sessions in a load-balanced RD Session Host server farm. The RD Connection Broker database stores session information, including the name of the RD Session Host server where each session resides, the session state for each session, the session ID for each session, and the user name associated with each session. RD Connection Broker uses this information to redirect a user who has an existing session to the RD Session Host server where the user’s session resides.

- If a user disconnects from a session (whether intentionally or because of a network failure), the applications that the user is running will continue to run. When the user reconnects, RD Connection Broker is queried to determine whether the user has an existing session, and if so, on which RD Session Host server in the farm. If there is an existing session, RD Connection Broker redirects the client to the RD Session Host server where the session exists.
Overview of Remote Desktop Gateway

● Remote Desktop Gateway (RD Gateway) is a role service that enables authorized remote users to connect to resources on an internal corporate or private network, from any Internet-connected device that can run the Remote Desktop Connection (RDC) client. The network resources can be Remote Desktop Session Host (RD Session Host) servers, RD Session Host servers running RemoteApp programs, or computers with Remote Desktop enabled.

● RD Gateway uses the Remote Desktop Protocol (RDP) over HTTPS to establish a secure, encrypted connection between remote users on the Internet and the internal network resources on which their productivity applications run.
Overview of RD Web Access

● Remote Desktop Web Access (RD Web Access), formerly Terminal Services Web Access (TS Web Access), enables users to access RemoteApp and Desktop Connection through the Start menu on a computer that is running Windows 7 or through a Web browser. RemoteApp and Desktop Connection provides a customized view of RemoteApp programs and virtual desktops to users.

● Additionally, RD Web Access includes Remote Desktop Web Connection, which enables users to connect remotely from a Web browser to the desktop of any computer where they have Remote Desktop access.
2013 USER CONFERENCE (WYGANT)
50/50
Approx. 50% of InTouch Licenses sold as TSE

Cost effective
Full HMI experience
TSE Guidelines for InTouch

InTouch for Terminal Services Deployment Guide
Planning and Implementation Guidelines 1.0 - January 2013
- Written for Windows Server 2008 R2 Remote Desktop Services

RDP: Remote Desktop Protocol for Remote Desktop Services
DirectAccess: automatically establishes a bi-directional connection from client computers to a corporate network

Client application connection
- Remote Desktop Client or embedded in a web browser
- IPv4 or IPv6
- Security credentials
Windows Server Options

• RD Session Host - enables a server to host RemoteApp programs or session-based desktops
• RD Web Access - enables users to access RemoteApp and Desktop Connection through the Start menu
• RD Licensing - manages the licenses required to connect to a Remote Desktop Session Host server or a virtual desktop
Windows Server Options

● RD Gateway - enables authorized users to connect to virtual desktops, RemoteApp programs, and session-based desktops on an internal corporate network from any Internet-connected device.

● RD Connection Broker - allows users to reconnect to their existing virtual desktops, RemoteApp programs, and session-based desktops; enables you to evenly distribute the load among RD Session Host servers; provides access to virtual desktops; disconnect from a session (whether intentionally or because of a network failure) the applications you were running will continue to run subject to server settings for timeout.
Scaling Up and Out

Scaling: Platforms do not have App Engines

10 Platform nodes, filtered Alarm Provider, 100 clients
Security for Remote Desktop Services

Microsoft:

By default, Remote Desktop Services connections are encrypted at the highest level of security available. However, some older versions of the Remote Desktop Connection client do not support this high level of encryption. If your network contains such legacy clients, you can set the encryption level of the connection to send and receive data at the highest encryption level supported by the client.

NLA - Network Level Authentication is an authentication method that can be used to enhance RD Session Host server security by requiring that the user be authenticated to the RD Session Host server before a session is created.
IPv6

Administration: Remote Desktop Protocol (RDP) is used to manage the server, which supports IPv6 without any configuration

Dual stack is enabled by default – IPv4 and IPv6

Direct Access - native IPv6

needs policy settings to avoid IPv4 vs. IPv6 mixups

DHCPv6 is configured by IT department on Domain servers

ping6 – used to diagnose connections

traceroute6 – used to diagnose connections
Remote Desktop Protocol 7

RDP 7.0 - For remote client computers to use DirectAccess to connect to computers on the internal corporate network, these computers and their applications must be reachable over IPv6. This means the following:


You have deployed native IPv6 connectivity or Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) on your intranet. ISATAP allows your internal servers and applications to be reachable by tunneling IPv6 traffic over your IPv4-only intranet.
InTouch Access Anywhere

● InTouch Access Anywhere contains technology for RDP compression and acceleration

● InTouch Access Anywhere is licensed for use with InTouch WindowViewer only, more specifically for use with InTouch 2012 R2 TSE Concurrent licenses only. Per Device licenses are not supported.

● Before using InTouch Access Anywhere to connect to your TSE server, it is also important to logon using a standard Remote Desktop Client, select an application from the InTouch Application Manager and to launch it in WindowViewer. This configures the initial setup and allows InTouch Access Anywhere clients to determine the list of available InTouch applications.

● InTouch Access Anywhere can work in HTTPS mode such that all communication will be sent via HTTPS only. To enable this feature, the InTouch Access Anywhere Secure Gateway is required.

● InTouch Access Anywhere does not support NLA.
InTouch Access Anywhere

Connection Details:
- InTouch Access Anywhere Server: mainwin1
- Username: username on host
- Password: password on host
- Domain: domain on host
- Enable SSL encryption for remote session
- Compression and Acceleration: Very Fast / Good Quality (Recommended)
- Application Name: New InTouch application

About | Advanced | Connect | Reset

Copyright © 2013 Inovance Systems, Inc. All rights reserved.

Business Network
InTouch Access Anywhere Troubleshooting

Checking Connectivity

If a user is having trouble connecting remotely to the InTouch Access Anywhere environment that has been installed, ask the user to connect to the InTouch Access Anywhere demo site on the Internet. If the demo site appears and the user can successfully launch an InTouch application then the browser is compatible. If the demo site works for the user, verify the following:

- Can they connect locally at the InTouch Access Anywhere node itself by using a supported browser?
- Is the InTouch Access Anywhere service running?
- Windows Firewall configuration: InTouch Access Anywhere port between the user’s browser and the InTouch Access Anywhere environment is available [8080]
InTouch Access Anywhere Troubleshooting

A trusted certificate may be required for the InTouch Access Anywhere Secure Gateway or the InTouch Access Anywhere Server.

Can the client device reach the InTouch Access Anywhere Server or the InTouch Access Anywhere Secure Gateway node?

   The Ping and Traceroute commands come in handy in a Windows based system.
   Third party tools exist for certain mobile devices to provide equivalent functionality.

If you cannot reach a node by name, try using its IP address