

# Remote Desktop Services with Vijeo Citect 2015

August 2015 – Rev1 - Whitepaper

Jacky Lang  
Martin Lalanne  
Warwick Black

# Summary

<b>1.</b>	<b>Remote Desktop Services (RDS)</b>	<b>3</b>
1.1.	<i>Benefits at a glance</i>	3
1.2.	<i>Supported Operating Systems</i>	3
1.3.	<i>SCADA Licensing</i>	3
1.4.	<i>Windows Remote Desktop Client License</i>	4
1.5.	<i>Architectures</i>	4
<b>2.</b>	<b>SCADA Installation</b>	<b>6</b>
2.1.	<i>Project Setup – Computer Setup Editor</i>	6
<b>3.</b>	<b>RDSH Installation (Windows Server 2012 R2)</b>	<b>7</b>
3.1.	<i>Deploy RDS</i>	9
3.2.	<i>Add an RDS License Server</i>	11
3.3.	<i>Configure RDS Session Timeouts</i>	16
3.4.	<i>Publish RemoteApp</i>	18
<b>4.</b>	<b>RDSH Installation (Windows Server 2008 R2)</b>	<b>23</b>
4.1.	<i>Setup Remote Desktop Licenses</i>	28
4.2.	<i>Publish RemoteApp</i>	30
<b>5.</b>	<b>Run the RemoteApp</b>	<b>38</b>
<b>6.</b>	<b>Appendix A – Installer Known Issue</b>	<b>40</b>
<b>7.</b>	<b>Appendix B – License Server Known Issue</b>	<b>41</b>

# 1. Remote Desktop Services (RDS)

For the purpose of this document, Microsoft's **Remote Desktop Services (RDS)** (formerly Terminal Services) allow **Remote Desktop Clients (RD Clients)** to connect to **RemoteApps** hosted on a **Remote Desktop Session Host (RDSH)** via the **Remote Desktop Protocol (RDP)**.

In a **Vijeo Citect 2015** system, the **RDSH** is configured to host **SCADA Clients**, by publishing a **RemoteApp**. When an **RD Client** runs the **RemoteApp**, they view and interact with the program as if it were locally installed, whilst leveraging the processing power and connectivity of the **RDSH**. In addition, **RDP** uses 128 bit encryption, and **RD Clients** are not limited to Windows-based devices.

These attributes make it a good candidate to allow Remote Access to a SCADA System, and can be used with other standard security products, such as two-factor authentication and VPNs.

For more detailed information regarding RDS, refer here:

<https://technet.microsoft.com/en-us/video/remote-desktop-services-rds-explained.aspx>

## 1.1. Benefits at a glance

RDS provides the following benefits:

- No SCADA installation on Clients
- Project files centrally managed
- Secure Remote Access
- No need to directly expose SCADA Servers
- Remote Desktop Protocol (RDP) traffic is 128 bit encrypted (RC4)
- FIPs compliant (regulatory compliance)
- SSL can be added for additional Security
- VPN access can be added for additional Security
- Integrate with enterprise two-factor authentication
- Cross-Platform Clients

## 1.2. Supported Operating Systems

The Remote Desktop Server must be running one of the following Operating Systems:

- Windows Server 2008 R2
- Windows Server 2012 R2

## 1.3. SCADA Licensing

The Citect client process on the server machine acts as a local license manager. The Citect server components act as a provider to distribute "Floating License" to remote clients that make a connection and request a license. The client process along with other server components are managed by the Citect Runtime Manager. In an RDS environment, several SCADA client sessions cannot be launched by Citect Runtime Manager because multiple instances are not supported. Therefore, the RDS Clients must use the switch /x to run without Citect Runtime Manager. SCADA clients launched with switch /x are basically "remote" clients and they thus obtain their license from a connected server component through the 'Floating License' mechanism. In the scenario where the SCADA Server and RDS Clients are all running on the same machine, softkey licenses are not supported. This is because the first RDS Client to startup will acquire all softkey licenses available on the machine and not have a mechanism to share them with other clients. This is a known issue and will be addressed in the future release. The hardware dongle license is the only option supported in this architecture, as the RDS Clients will not touch any licences on the dongle and always acquire a licence through the "Floating License" mechanism..

The client licence entitlement can be also specified with switch /l (l for licence), with /l:1 for a view-only client, while /l:2 is for a control client. This assumes that the default Citect.ini file will be used and switch /l simply overrides the [Client]ComputerRole setting. In this case, there is no need to create a separate Citect.ini for each type of clients. It should be noted that switch /l can only be used with switch /x.

## 1.4. Windows Remote Desktop Client License

Remote Connection Sessions using Remote Desktop Services require a standard Microsoft Client Access License (CAL) for each connection to the server.

## 1.5. Architectures

### 1.5.1. SCADA and RDS on the same Server

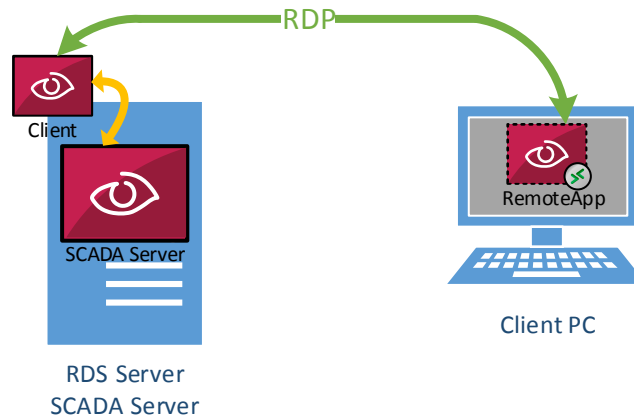
It is possible to host the **SCADA Servers** on the same PC as the hosted **Client Sessions**.

This requires the smallest infrastructure, however, as all Servers and Clients now rely on the same hardware, this becomes a **single point of failure** for the entire system.

**Note:** Softkey licensing is not supported in this architecture. Only hardware licenses (USB keys) are supported through the floating license mechanism to connected server components. For more details see section 1.3.

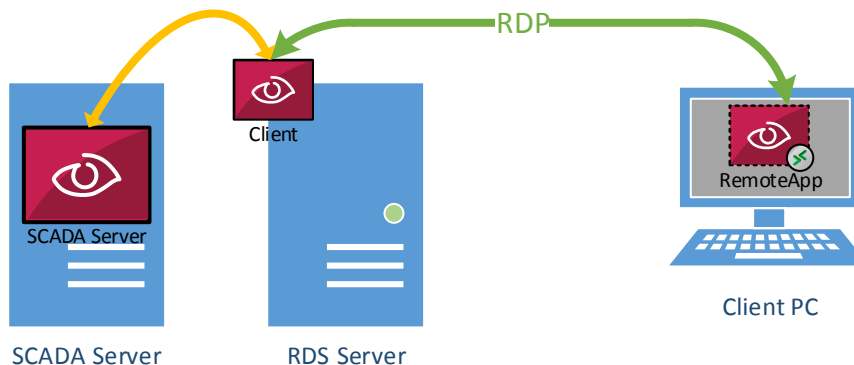
In this architecture, you may consider installing the SCADA Server as a Windows Service.

This allows the SCADA Server to run on the RDS Server without the need for a logged in interactive user. Other benefits and instructions can be found in the [‘Vijeo Citect 2015 Run as a Windows Service’](#) whitepaper.



### 1.5.2. SCADA and RDS on different Servers

A more likely scenario is that the **RDS Server** only hosts **SCADA Clients**, and serves them as **RemoteApps**. These Client Sessions then connect to the required independent **SCADA Servers** for their IO, Alarm, Report and Trend data. This allows the usage of RDS for the Clients, and retains Citect's redundancy capabilities for the SCADA Servers, removing the single-point of failure.

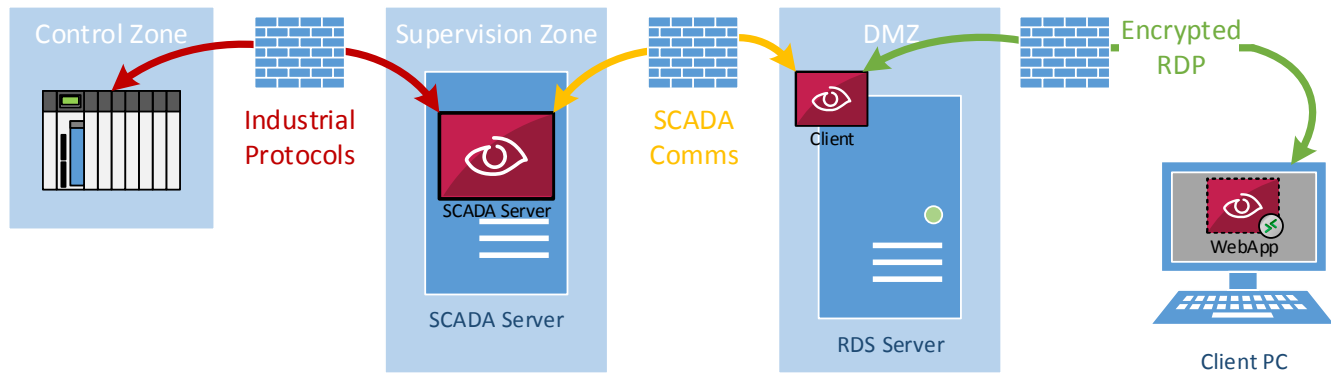


### 1.5.3. RDS for Secure Remote Access

The use of RDS allows advanced architectures that allow for Secure Remote access. Following the principles of the IEC-52443 (ISA 99) standard, functional 'Zones' can be created and the interactions ('Conduits') between these zones controlled via heavily restricted firewall rules.

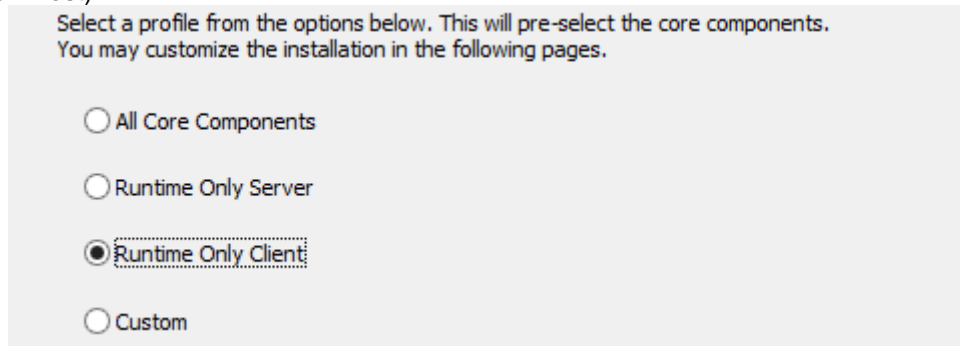
In the configuration below, all the traffic leaving the premises is encrypted via the Remote Desktop Protocol. Additional VPN technology could be used to further protect the data on the wire.

Since RDS is a standard Windows technology, additional authentication methods such as Two-Factor Authentication could easily be applied.



## 2. SCADA Installation

At a minimum, the Vijeo Citect SCADA 'Runtime Only Client' installation is required on the **RDSH** (Remote Desktop Session Host):



Select a profile from the options below. This will pre-select the core components. You may customize the installation in the following pages.

- ☐ All Core Components
- ☐ Runtime Only Server
- ☒ Runtime Only Client
- ☐ Custom

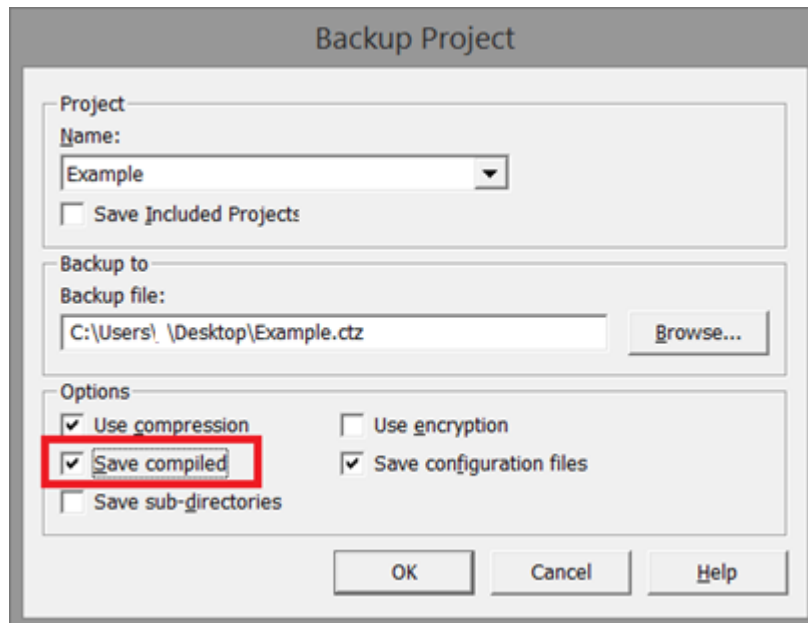
This can be installed following the '**Installation Guide**' provided on the installation Media.

**Note:** If you install Vijeo Citect SCADA after installing Remote Desktop Services, the installer may not complete. This is a known issue and [Appendix A](#) outlines a workaround.

### 2.1. Project Setup – Computer Setup Editor

Restore your project backup from your development machine:

- Ensure the 'Save Compiled' option was selected, since you will not be able to compile on a machine with a 'Runtime Only Client' installation



The 'Backup Project' dialog box contains the following sections:

- Project:** A dropdown menu showing 'Example' and a checkbox for 'Save Included Projects'.
- Backup to:** A text field showing 'C:\Users\ \Desktop\Example.ctz' and a 'Browse...' button.
- Options:** A group of checkboxes: 'Use compression' (checked), 'Use encryption' (unchecked), 'Save compiled' (checked and highlighted with a red box), 'Save configuration files' (checked), and 'Save sub-directories' (unchecked).

At the bottom are 'OK', 'Cancel', and 'Help' buttons.

- Run '**Computer Setup Wizard**', and add any required Citect.INI customizations
- Start the Client to test configuration and connectivity
- Shutdown the Client instance

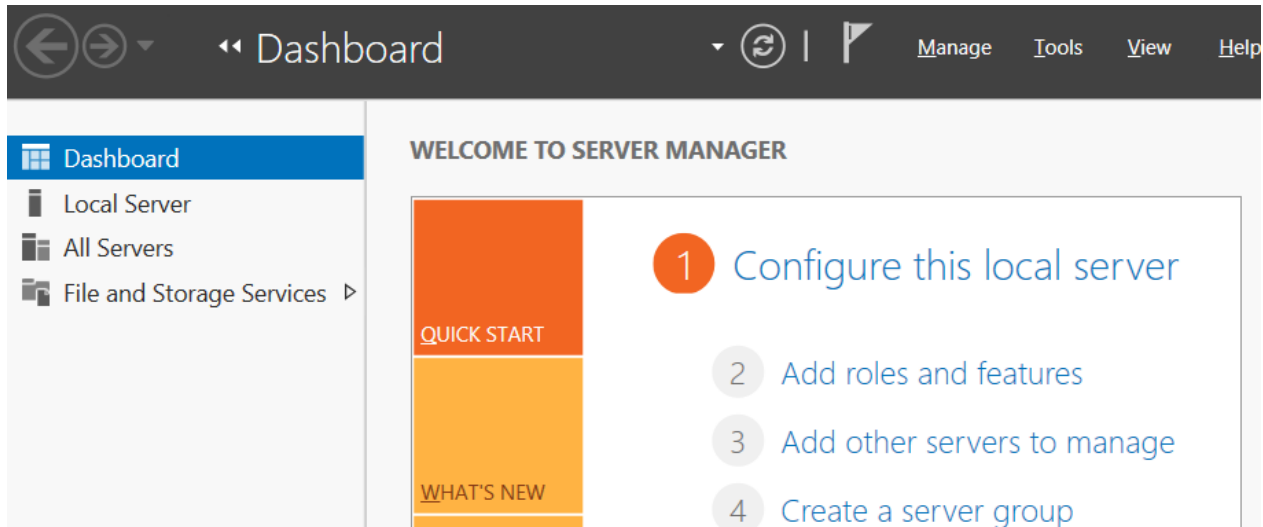
**Note:** Other methods of distributing project files are documented in the product help, under: '**Distributing the Project**'

### 3. RDSH Installation (Windows Server 2012 R2)

**Note: You must be logged in as a Domain user**

The following steps must be followed to install Remote Desktop Services on Windows 2012 R2:

- Open Server Manager >> Click Manage and 'Add Roles and Features':



- Select 'Next and use the 'Role-based' option

#### Select installation type

[Before You Begin](#)[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[Confirmation](#)[Results](#)

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**  
Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**  
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

- Select your server:

#### Select destination server

[Before You Begin](#)[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[Confirmation](#)[Results](#)

Select a server or a virtual hard disk on which to install roles and features.

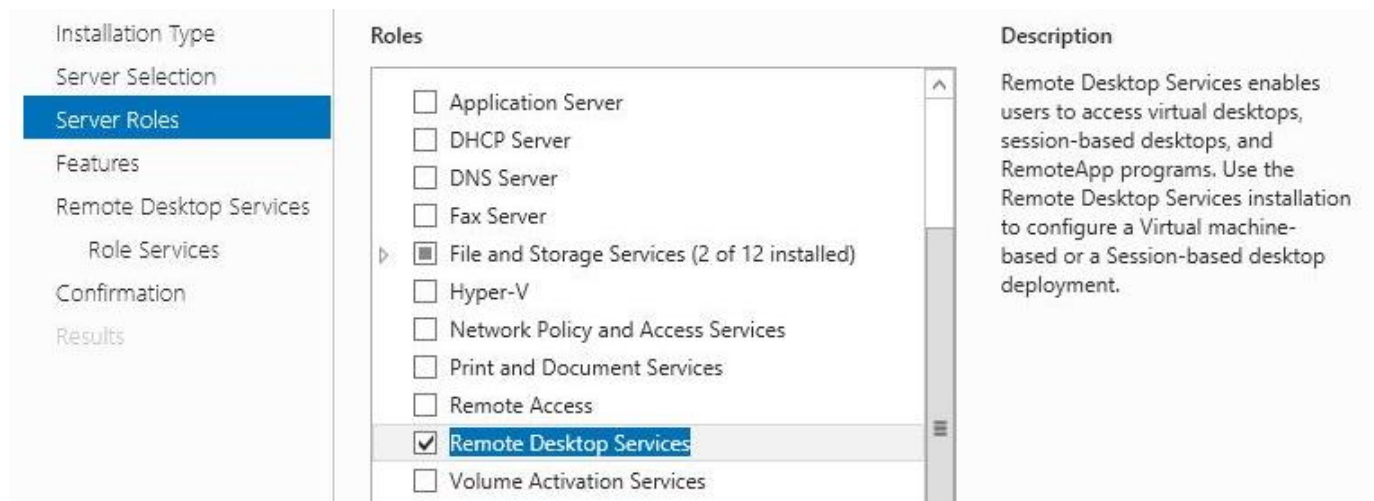
☒ Select a server from the server pool

☐ Select a virtual hard disk

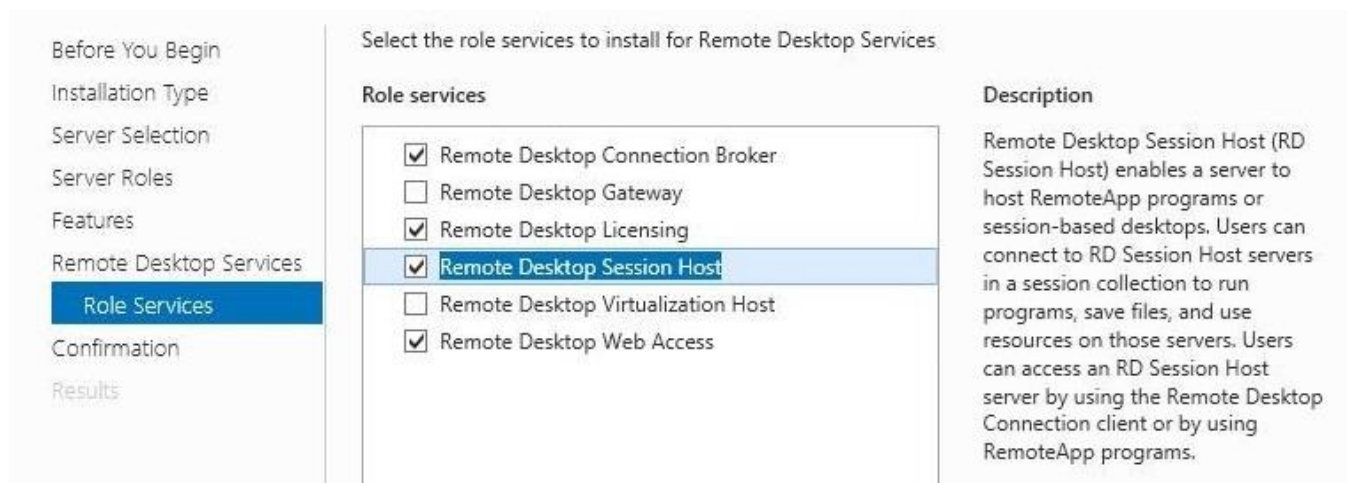
Server Pool

Name	IP Address	Operating System
Microsoft Windows Server 2012 R2 Datacenter		

- Add the remote Desktop Services Feature in the list:



- Select the following Remote Desktop Services (RDS) options:



- Proceed through the wizard, confirming your selection then click '**Install**'



## 3.1. Deploy RDS

**Note: You must be logged in as a Domain user**

The next step is to deploy the RDS Service on the Host machine:

- Open Server Manager >> Click Manage and Add Roles and Features
- Select Remote Desktop Services installation

The screenshot shows the 'Select installation type' wizard. On the left, a navigation pane lists steps: 'Before You Begin', 'Installation Type' (highlighted), 'Deployment Type', 'Deployment Scenario', 'Role Services', 'RD Connection Broker', 'RD Web Access', 'RD Virtualization Host', 'Confirmation', and 'Completion'. The main area has the title 'Select installation type' and a sub-header 'DESTINATION SERVER No servers are selected.' Below this, it says 'Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).' There are two radio button options: 'Role-based or feature-based installation' (unselected) and 'Remote Desktop Services installation' (selected). The description for the selected option states: 'Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.'

- Select Quick Start in the Deployment Type

The screenshot shows the 'Select deployment type' wizard. The navigation pane on the left is the same as the previous screen, with 'Deployment Type' highlighted. The main area has the title 'Select deployment type' and the same sub-header 'DESTINATION SERVER No servers are selected.' It begins with the text: 'A Remote Desktop Services deployment already exists in the server pool. Select an RD Connection Broker on which to create the Remote Desktop Services deployment.' Below this is a dropdown menu labeled 'RD Connection Broker'. Further down, it says 'Remote Desktop Services can be configured across multiple servers or on one server.' There are two radio button options: 'Standard deployment' (unselected) and 'Quick Start' (selected). The description for 'Quick Start' states: 'A Quick Start allows you to deploy Remote Desktop Services on one server, and creates a collection and publishes RemoteApp programs.'

- Select 'Session-Based Desktop Deployment':

## Select deployment scenario

DESTINATION SERVER  
Quick Start selected

Before You Begin

Installation Type

Deployment Type

**Deployment Scenario**

Server Selection

Confirmation

Completion

Remote Desktop Services can be configured to allow users to connect to virtual desktops, RemoteApp programs, and session-based desktops.

☐ Virtual machine-based desktop deployment

Virtual machine-based desktop deployment allows users to connect to virtual desktop collections that include published RemoteApp programs and virtual desktops.

☒ Session-based desktop deployment

Session-based desktop deployment allows users to connect to session collections that include published RemoteApp programs and session-based desktops.

## Select a server

DESTINATION SERVER  
Quick Start selected

Before You Begin

Installation Type

Deployment Type

Deployment Scenario

**Server Selection**

Confirmation

Completion

The Quick Start will be deployed on the RD Connection Broker server. To proceed, click Next.

**Server Pool**

Filter:

Name	IP Address	Operating

<   >

1 Computer(s) found

**Selected**

Computer

▲ .COM (1)

▶

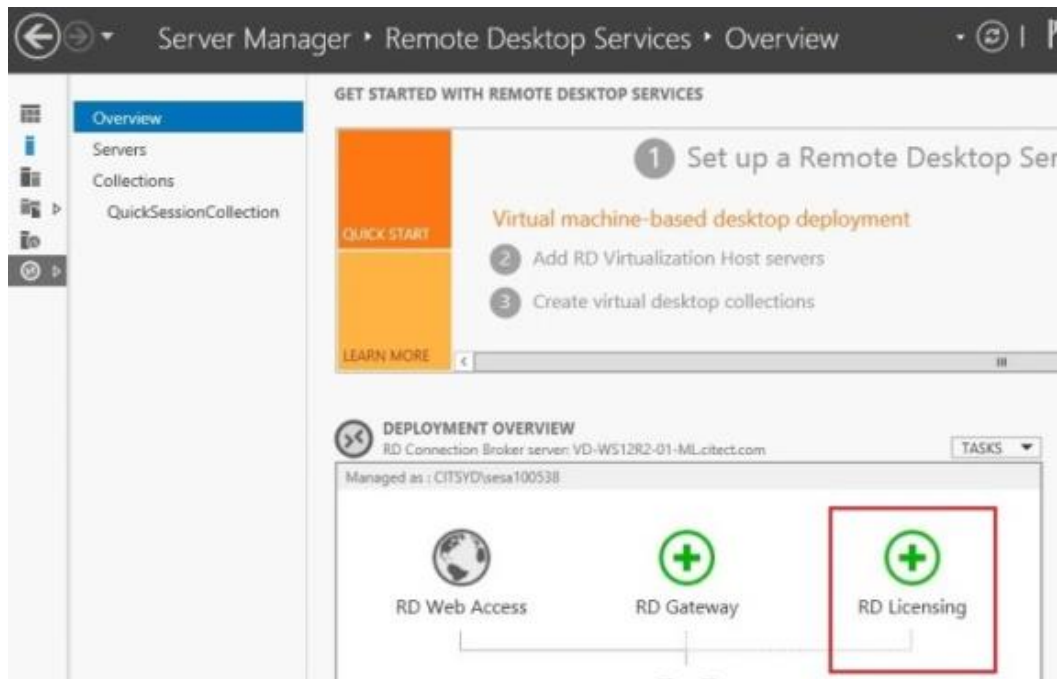
1 Computer(s) selected

- Select Deployment Machine
- Confirm the selection and '**Install**'

## 3.2. Add an RDS License Server

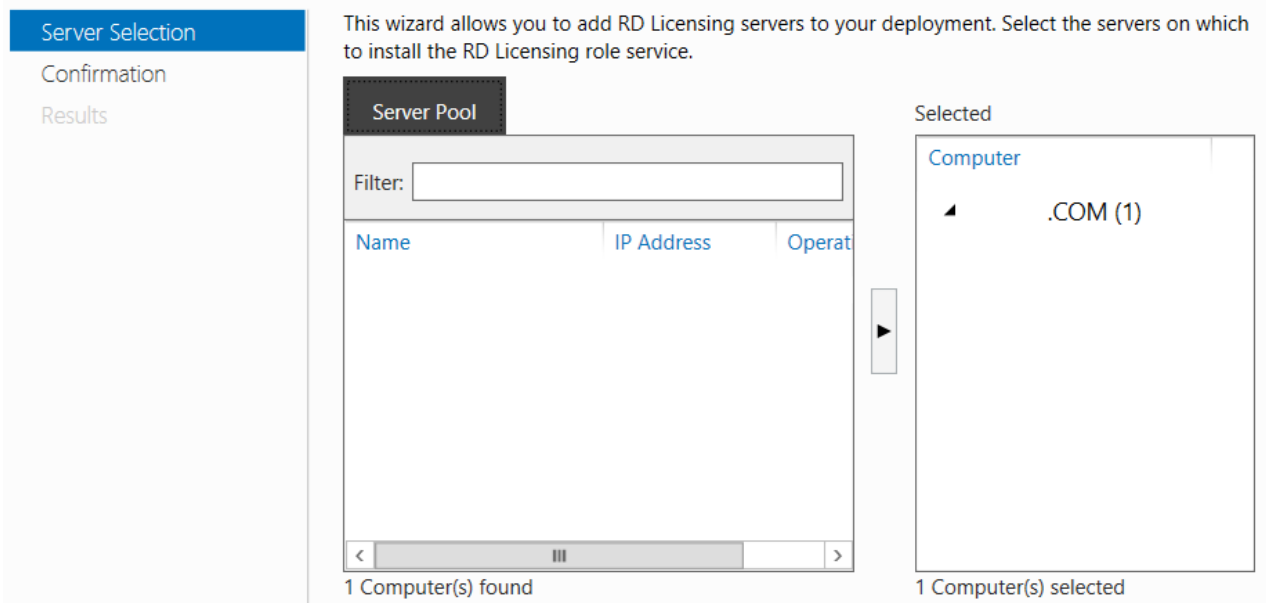
In order to license the RDS Sessions, we need to add a Licensing Server, which will provide the required CALs (Client Access Licenses). To configure the license server follow these steps:

- Open Server Manager >> Remote Desktop Services >> Overview:



- Click on the RD Licensing icon

### Select a server



- Select the server used for RDS, confirm the selection and install

- The RD Licensing is ready and is displayed in the Overview view:

The screenshot displays the 'Remote Desktop Services' Overview page. The top navigation bar includes 'Remote Desktop Services' and 'Overview'. A left-hand navigation pane lists 'Overview', 'Servers', 'Collections', and 'QuickSessionCo...'. The main content area is titled 'GET STARTED WITH REMOTE DESKTOP SERVICES' and features a 'QUICK START' section with a 'LEARN MORE' link. Below this, a 'DEPLOYMENT OVERVIEW' section shows a diagram of the RD architecture: 'RD Web Access' (globe icon), 'RD Gateway' (green plus icon), and 'RD Licensing' (medal icon). The 'RD Gateway' icon is highlighted with a green circle. To the right, a 'DEPLOYMENT SERVERS' section shows a list of servers, with 'Server PQDN' visible. The 'RD Licensing' component is shown as ready.

Remote Desktop Services Overview

GET STARTED WITH REMOTE DESKTOP SERVICES

1 Set up a Remote Desktop Services deployment

Virtual machine-based desktop deployment

Session-based desktop deployment

2 Add RD Virtualization Host servers

3 Create virtual desktop collections

2 Add RD Session Host servers

3 Create session collections

DEPLOYMENT OVERVIEW

RD Connection Broker server:

Managed as: CITSYD\SESA100538

RD Web Access

RD Gateway

RD Licensing

DEPLOYMENT SERVERS

Last refreshed on 4/12/2014 1:03

Filter

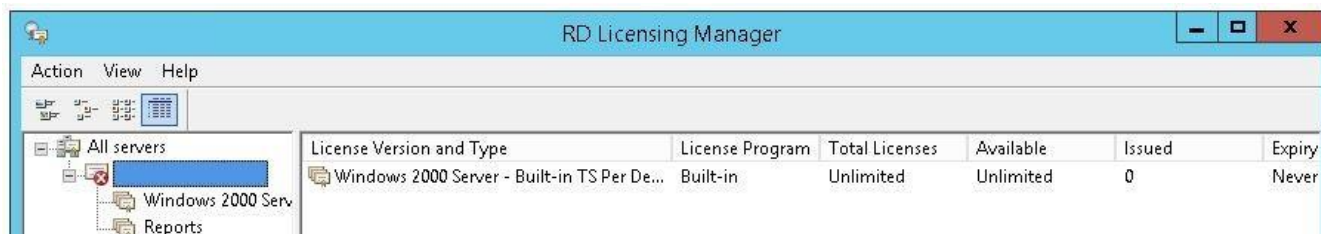
Server PQDN

### 3.2.1. Add CALs to License Server

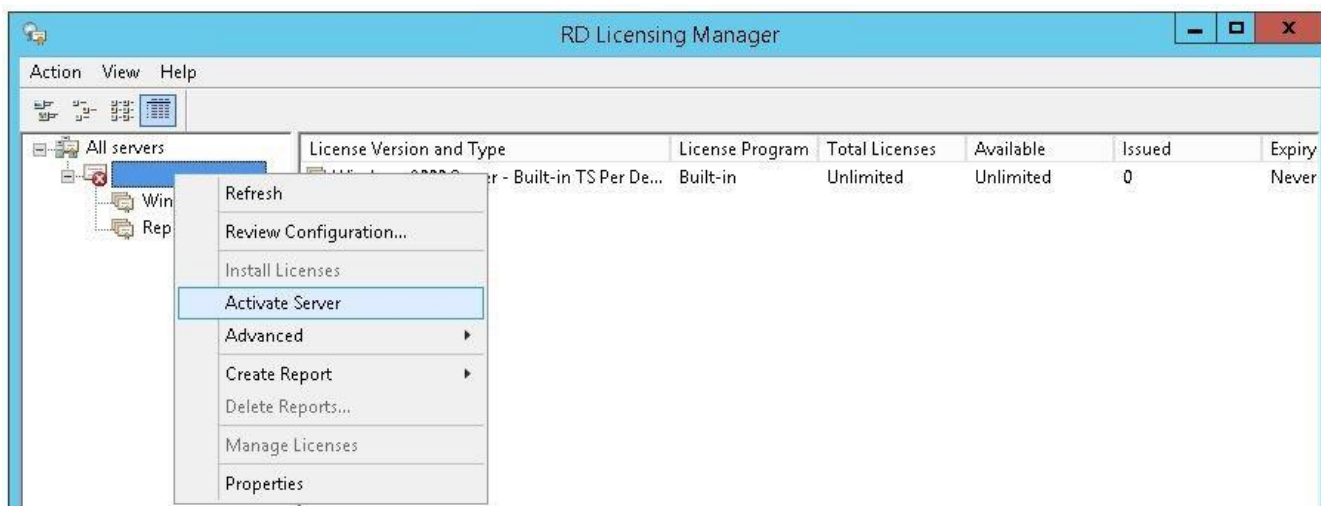
RDS Sessions require a standard Microsoft Client Access License (CAL) for each connection to the server, these need to be added into the RD Licensing Manager. You may need to purchase additional licenses from Microsoft.

To add CALs on the RDS Host machine follow these steps:

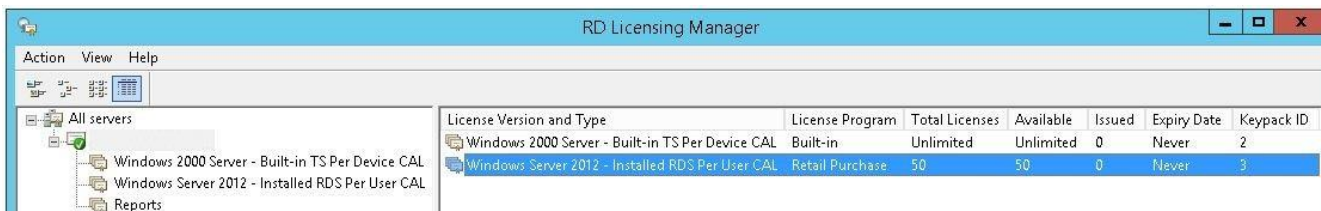
- Open RD Licensing Manager on Start >> All Programs >> Administrative Tools >> Remote Desktop Services > Remote Desktop Licensing Manager



- Select 'Activate Server' and follow the Wizard's prompts



- The Wizard will connect you to the 'Microsoft Clearinghouse' where you can activate your previously purchased CAL licenses
- If you need to purchase additional CALs, you will need to do that via:  
<http://go.microsoft.com/fwlink/?LinkId=81077>
- After completing the Wizard, the CAL Licenses will be displayed on the RD Licensing Manager:



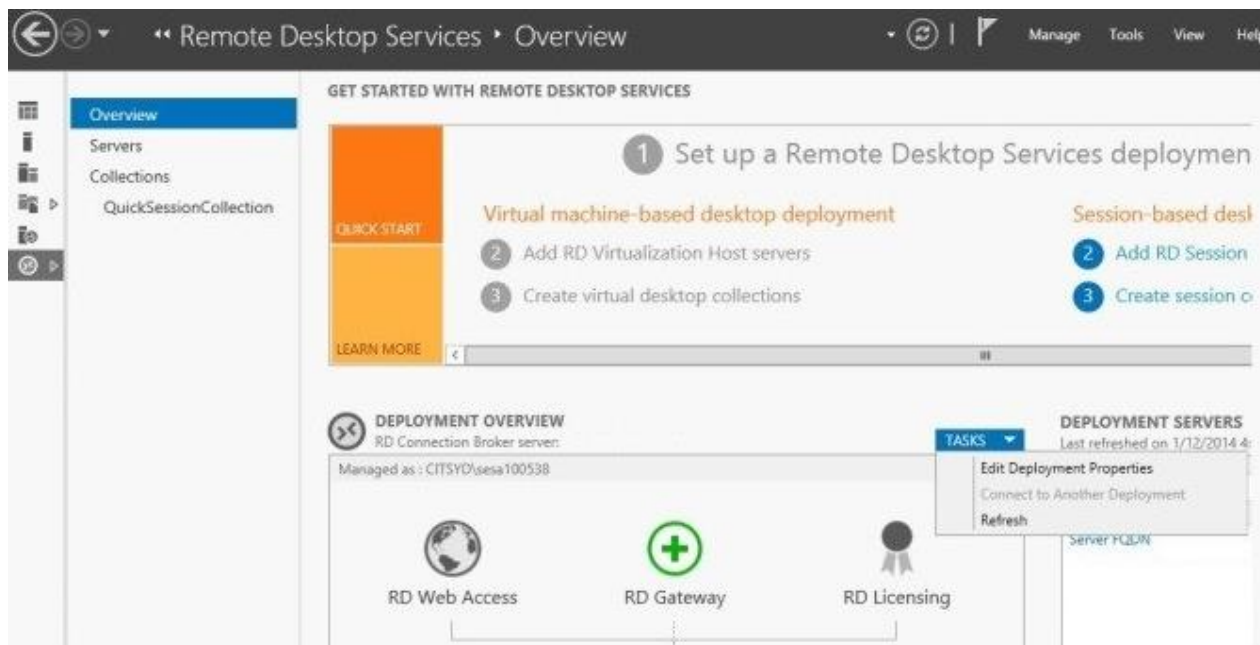
### 3.2.2. 'No License Server' – Known Issue

If the RDSH server complains about no licensing server being set, please follow the instructions in [Appendix B](#).

### 3.2.3. Configure the RD Licensing Mode

Configure the RD Licensing Mode:

- Server Manager >> Remote Desktop Services >> Overview >> Deployment Overview >> Tasks >> Edit Deployment Properties:



- Configure 'Per User' mode in the RD Licensing section:

#### Configure the deployment

Configure the deployment

RD Gateway +

**RD Licensing -**

RD Web Access +

Certificates +

RD Licensing

Select the Remote Desktop licensing mode:

☐ Per Device

☒ Per User

Specify a license server, and then click Add:

Add...

Select the order for the Remote Desktop license servers:

The RD Session Host server or the RD Virtualization Host server sends requests for licenses to the specified license servers in the order in which you list them.

Move Up

Move Down

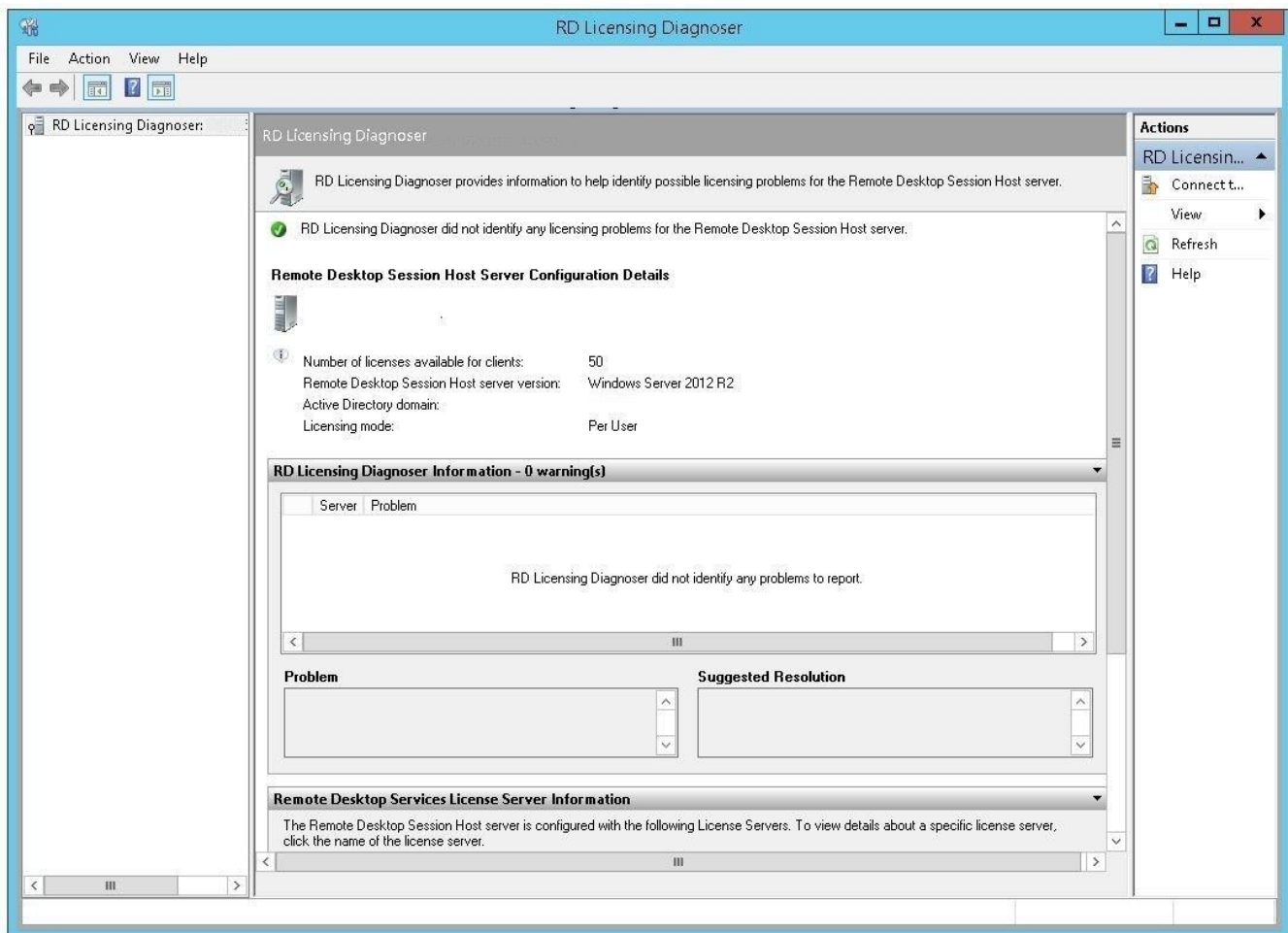
Remove

- Click OK to finish the license configuration

### 3.2.4. License Diagnostics

You can see relevant information about licensing in the RD Licensing Diagnoser:

- Open RD Licensing Diagnoser: Start >> Programs >> Administrative Tools >> RD Licensing Diagnoser





### 3.3. Configure RDS Session Timeouts

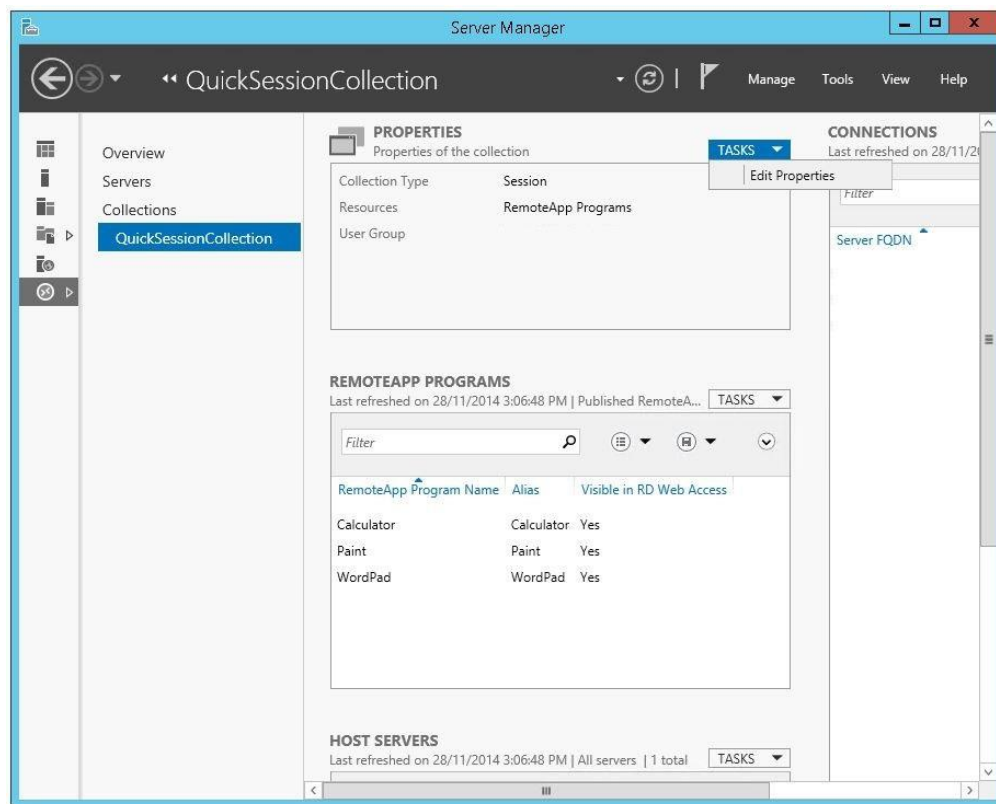
Once the RD Client session starts and runs the Citect application, the license it obtains from the SCADA system will not be released until the session is closed.

By default, the RDS session will not terminate just because the RDS Client closes its window to the server. The server will continue to process this session indefinitely.

To keep operators from creating unused sessions, the Remote Desktop Services Host can be setup to automatically end sessions that have been disconnected. In this way the Citect licenses will release properly back to the Citect Server components where they will be available for future sessions.

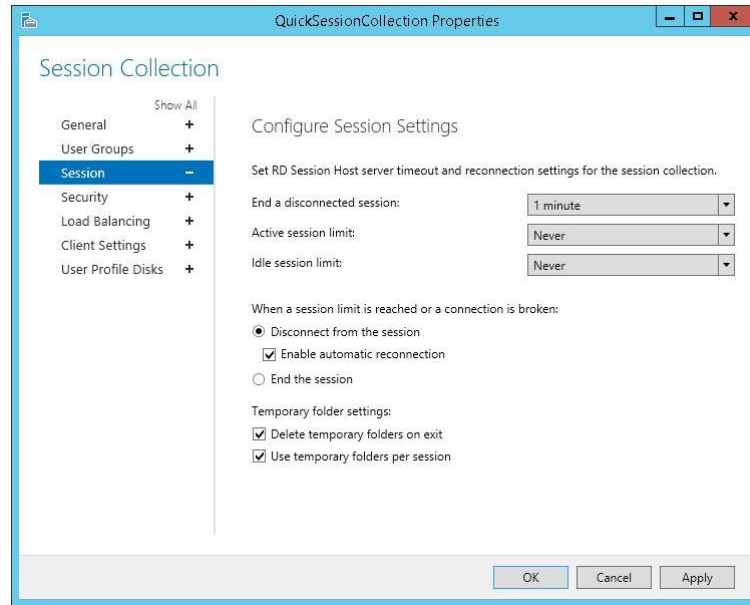
Below are the required steps to configure an automatic expiry of any disconnected session. This means that a Citect license will not be tied up in a disconnected session for more than 1 minute:

- Open Server Manager >> Remote Desktop Services >> QuickSessionCollection >> Properties >> Tasks >> Edit Properties





- In the Session section, set 'End a disconnected session' to the desired level, i.e 1 minute

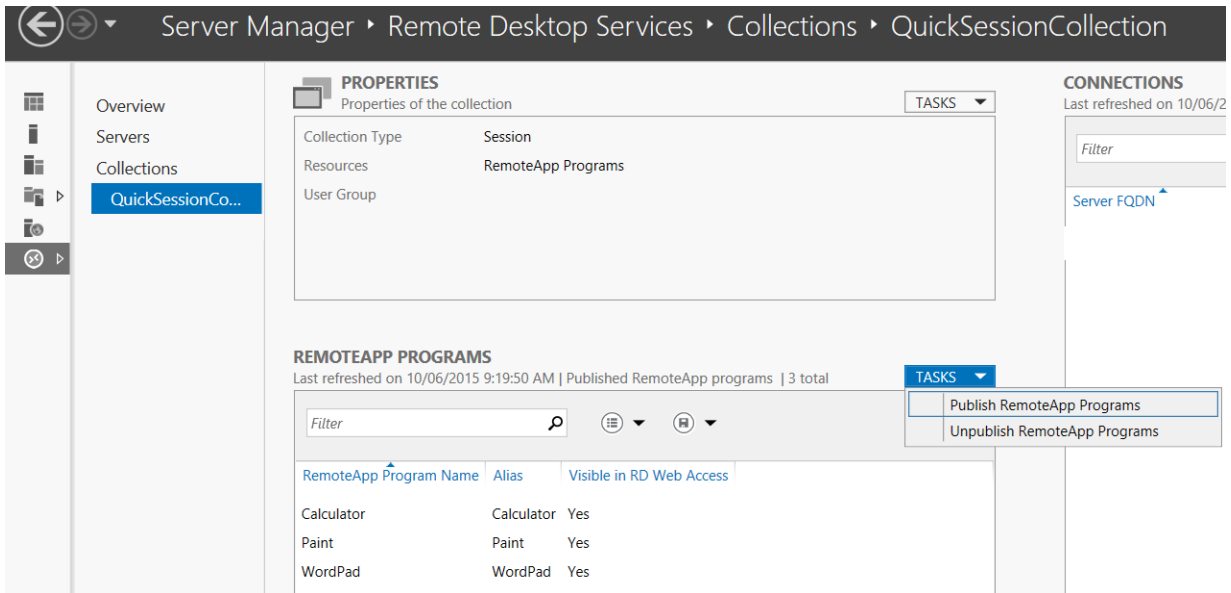


- Click OK to validate and finish

## 3.4. Publish RemoteApp

The following steps show how to publish a RemoteApp in Windows Server 2012 R2:

- Open: Server Manager >> Remote Desktop Services >> QuickSessionCollection >> RemoteApp Programs >> Tasks >> Publish RemoteApp Programs
- By default, Calculator, Paint and WordPad are already published, these can be removed



- Select 'Vijeo Citect Runtime'

### Select RemoteApp programs

**RemoteApp Programs**

Confirmation

Publishing

Completion

Select the RemoteApp programs to publish to the QuickSessionCollection collection. To add a RemoteApp program to the list, click Add.

The RemoteApp programs are populated from SYD-VLDN-SVR51.CITECT.COM.

<input type="checkbox"/> RemoteApp Program	Location
<input type="checkbox"/> System Configuration	%SYSTEMDRIVE%\Windows\system32\msconfi...
<input type="checkbox"/> System Information	%SYSTEMDRIVE%\Windows\system32\msinfo3...
<input type="checkbox"/> Task Manager	%SYSTEMDRIVE%\Windows\system32\taskmgr...
<input type="checkbox"/> Time Synchronization Config	%SYSTEMDRIVE%\Program Files (x86)\Schneide...
<input type="checkbox"/> Update License	%SYSTEMDRIVE%\Program Files (x86)\Schneide...
<input type="checkbox"/> Vijeo Citect Computer Setup	%SYSTEMDRIVE%\Program Files (x86)\Schneide...
<input checked="" type="checkbox"/> Vijeo Citect Runtime	%SYSTEMDRIVE%\Program Files (x86)\Schneide...
<input type="checkbox"/> Vijeo Citect Runtime Manager	%SYSTEMDRIVE%\Program Files (x86)\Schneide...
<input type="checkbox"/> VirusScan Console	%SYSTEMDRIVE%\Program Files (x86)\McAfee\...
<input type="checkbox"/> Windows Memory Diagnostic	%SYSTEMDRIVE%\Windows\system32\MdSche...
<input type="checkbox"/> Windows PowerShell	%SYSTEMDRIVE%\Windows\System32\Window...

Add...

Verify that the program is installed on all the RD Session Host servers in the collection.

- Confirm the selection and publish the RemoteApp

## Confirmation

RemoteApp Programs


Confirmation

Publishing

Completion

Confirm that the list of RemoteApp programs to be published is correct, and then click Publish.

1 RemoteApp program:

RemoteApp Program	Location
 Vijeo Citect Runtime	%SYSTEMDRIVE%\Program Files (x86)\Schneide...

- Highlight the new '**Vijeo Citect Runtime**' entry, right click and select '**Edit Properties**'

Server Manager > Remote Desktop Services > Collections > QuickSessionCollection

Overview  
Servers  
Collections  
QuickSessionCo...

**PROPERTIES**  
Properties of the collection

Collection Type: Session  
Resources: RemoteApp Programs  
User Group:

**REMOTEAPP PROGRAMS**  
Last refreshed on 10/06/2015 10:40:09 AM | Published RemoteApp programs | 4 total

RemoteApp Program Name	Alias	Visible in RD Web Access
Calculator	Calculator	Yes
Paint	Paint	Yes
<b>Vijeo Citect Runtime</b>	<b>Citect32</b>	<b>Yes</b>
WordPad	WordPad	Yes

**HOST SERVERS**  
Last refreshed on 10/06/2015 10:37:22 AM | All servers | 1 total

Server Name	Type	Virtual Desktops	Allow New Connections
RD Session Host	N/A		True

**CONNECTION**  
Last refreshed on

Filter

Server FQDN

- Under 'Parameters'
- Set the '/x' flag so that Clients do not load '**Runtime Manager**'

## Vimeo Citect Runtime (QuickSessionCollection Collection)

Show All

General +

**Parameters -**


User Assignment +

File Type Associati... +

### Command-line Parameters

☐ Do not allow any command-line parameters

☐ Allow any command-line parameters

 By allowing this RemoteApp program to run with any command-line parameter, your server may be vulnerable to malicious software.

☒ Always use the following command-line parameters

/x

- Under '**User Assignment**', select '**Only Specified Users and Groups**', then click '**Add**' in order to add which windows Users / Groups should have access to the RemoteApp

## Vimeo Citect Runtime (QuickSessionCollection Collection)

Show All

General +

Parameters +

**User Assignment -**

File Type Associati... +

### User Assignment

RemoteApp programs can be limited so that only selected users and groups can see the icon when they log on to RD Web Access.

Specify the users and groups who should see this RemoteApp program:


☐ All users and groups that have access to the collection

☒ Only specified users and groups

Users and groups:

Add...

Remove

 For a user account to have access to a RemoteApp program, the user account must have access to both the RemoteApp program and the collection to which it is published. Updating the user access at the collection level will not change the user access at the RemoteApp program level.

### 3.4.1. Custom INI Paths

Custom INI paths can be set for the RemoteApp, this is especially important if you are also running your SCADA Servers on the same machine, or if you have a mix of **'View-Only'** and **'Control'** Clients. It is also possible to specify the license type and override the default citect.ini settings using the switch /l (l for license). For more details see section 1.3.

Ensure any custom INI files are accessible by the intended users.

#### 3.4.1.1 INI Parameters

The INI Parameters that govern which type of license the Client will take are:

[Client] ComputerRole

0 = Server and Control Client

1 = Control Client (enables [Client]FullLicense)

2 = View-Only Client

[Client] FullLicense

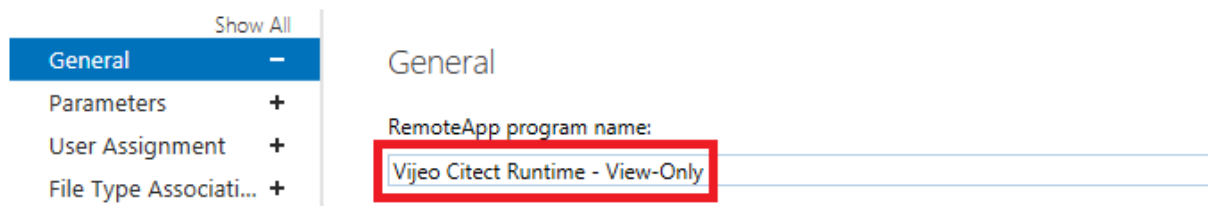
0 = Do not use a full license

1 = Use a Full licenese

#### 3.4.1.2 View-Only Client

- Copy, rename and edit the INI file to contain: [Client] ComputerRole = 2
- Under **'General'**, rename your RemoteApp to indicate it is **'View Only'**
- Modify the **'Parameters'** to point to this new INI file:  
'/x' to prevent Runtime Manager from loading  
'/i' followed by a custom INI path (encased in double quotes)

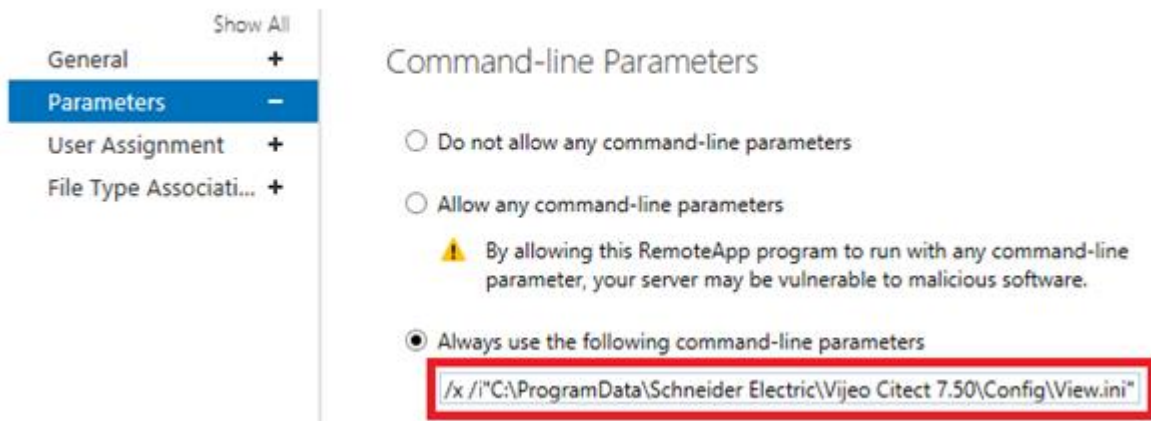
### Vijeo Citect Runtime (QuickSessionCollection Collection)



General

RemoteApp program name:  
**Vijeo Citect Runtime - View-Only**


### Vijeo Citect Runtime (QuickSessionCollection Collection)



Command-line Parameters

☐ Do not allow any command-line parameters

☐ Allow any command-line parameters

 By allowing this RemoteApp program to run with any command-line parameter, your server may be vulnerable to malicious software.

☒ Always use the following command-line parameters

**/x /i"C:\ProgramData\Schneider Electric\Vijeo Citect 7.50\Config\View.ini"**

- Alternatively, if you don't want to specify a custom citect.ini file, you can override the local citect.ini role setting to force a view-only client, by using the /l switch in conjunction with /x:  
**/x /l:1**

### 3.4.1.3 Control Client

- Copy, rename and edit the INI file to contain:  
[Client] ComputerRole = 1  
[Client] FullLicence=0
- Publish a second instance of the RemoteApp
- Under '**General**', rename it to indicate it is a '**Control**' Client
- Modify the '**Parameters**' to point to this new INI file:  
'/x' to prevent Runtime Manager from loading  
'/i' followed by a custom INI path (encased in double quotes)

## Vijeo Citect Runtime (QuickSessionCollection Collection)

Show All	
General	—
Parameters	+
User Assignment	+
File Type Associati...	+

General

RemoteApp program name:

Vijeo Citect Runtime - Control


## Vijeo Citect Runtime (QuickSessionCollection Collection)

Show All	
General	+
Parameters	—
User Assignment	+
File Type Associati...	+

Command-line Parameters

☐ Do not allow any command-line parameters

☐ Allow any command-line parameters

 By allowing this RemoteApp program to run with any command-line parameter, your server may be vulnerable to malicious software.

☒ Always use the following command-line parameters

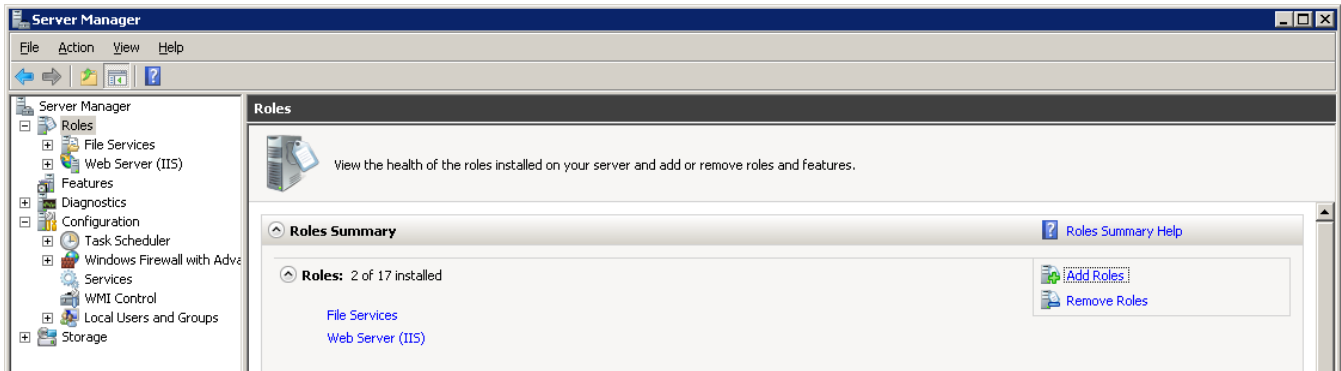
"/x /i"C:\ProgramData\Schneider Electric\Vijeo Citect 7.50\Config\Control.ini"

- Alternatively, if you don't want to specify a custom citect.ini file, you can override the local citect.ini role setting to force a **control client**, by using the /i switch in conjunction with /x:  
**/x /i:2**

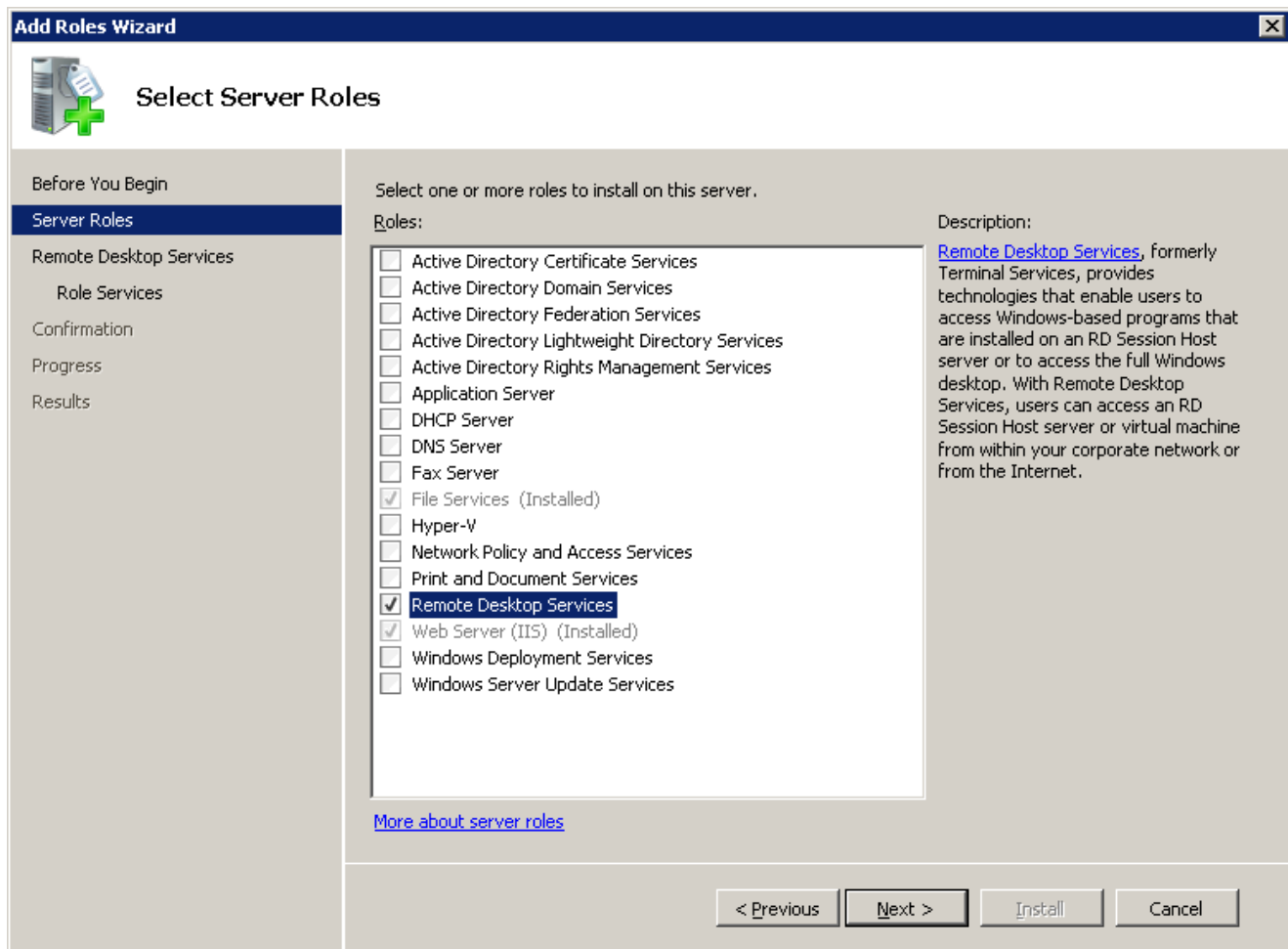
## 4. RDSH Installation (Windows Server 2008 R2)

To install RDS service on your host machine:

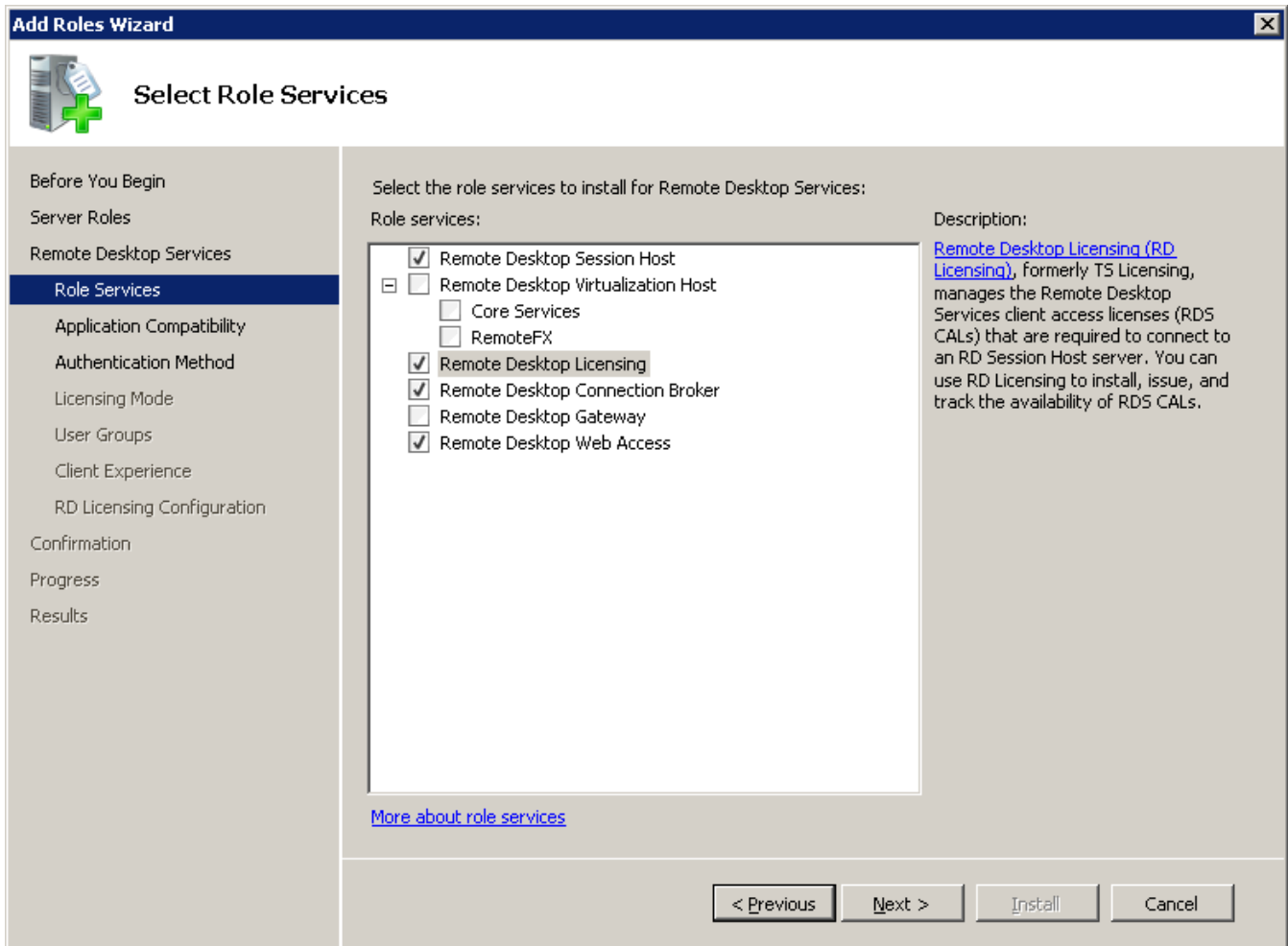
- Open Server Manager >> Click Roles and Add Roles



- Under 'Server Roles', select 'Remote Desktop Services' then click 'Next'



- Select the following 'Role Services':
  - Remote Desktop Connection Broker
  - Remote Desktop Licensing
  - Remote Desktop Session Host
  - Remote Desktop Web Access



**Add Roles Wizard**

**Select Role Services**

Before You Begin  
Server Roles  
Remote Desktop Services  
**Role Services**  
Application Compatibility  
Authentication Method  
Licensing Mode  
User Groups  
Client Experience  
RD Licensing Configuration  
Confirmation  
Progress  
Results

Select the role services to install for Remote Desktop Services:

Role services:

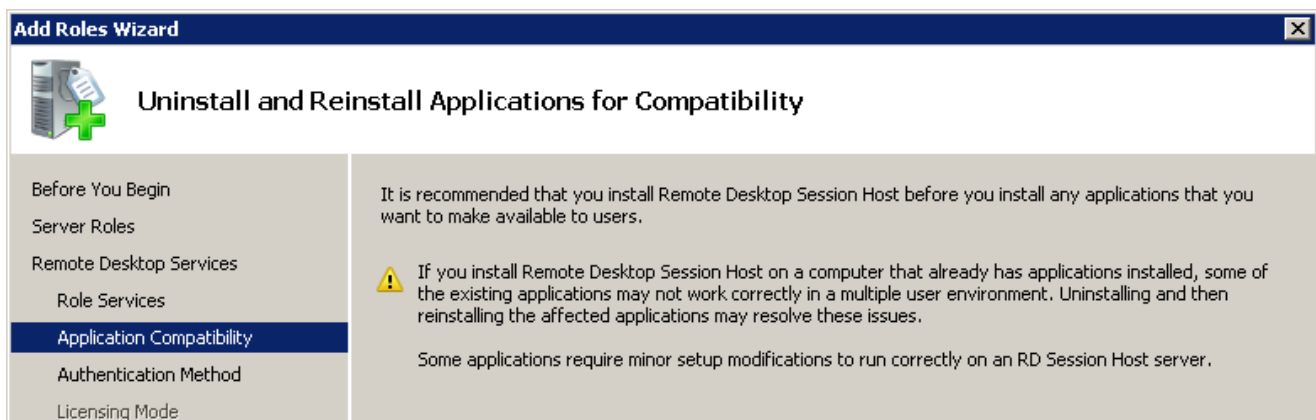
- ☒ Remote Desktop Session Host
- ☐ Remote Desktop Virtualization Host
  - ☐ Core Services
  - ☐ RemoteFX
- ☒ Remote Desktop Licensing
- ☒ Remote Desktop Connection Broker
- ☐ Remote Desktop Gateway
- ☒ Remote Desktop Web Access

Description:  
[Remote Desktop Licensing \(RD Licensing\)](#), formerly TS Licensing, manages the Remote Desktop Services client access licenses (RDS CALs) that are required to connect to an RD Session Host server. You can use RD Licensing to install, issue, and track the availability of RDS CALs.

[More about role services](#)

< Previous   Next >   Install   Cancel

- Take note of the 'Uninstall and Reinstall Applications for Compatibility' warning, then click 'Next' if you wish to proceed



**Add Roles Wizard**

**Uninstall and Reinstall Applications for Compatibility**

Before You Begin  
Server Roles  
Remote Desktop Services  
Role Services  
**Application Compatibility**  
Authentication Method  
Licensing Mode

It is recommended that you install Remote Desktop Session Host before you install any applications that you want to make available to users.


**Warning:** If you install Remote Desktop Session Host on a computer that already has applications installed, some of the existing applications may not work correctly in a multiple user environment. Uninstalling and then reinstalling the affected applications may resolve these issues.

Some applications require minor setup modifications to run correctly on an RD Session Host server.



- Depending on your needs, choose whether '**Network Level Authentication**' is required

**Add Roles Wizard**

 **Specify Authentication Method for Remote Desktop Session Host**


Before You Begin  
Server Roles  
Remote Desktop Services  
    Role Services  
    Application Compatibility  
**Authentication Method**  
Licensing Mode  
User Groups  
Client Experience  
RD Licensing Configuration  
Confirmation  
Progress  
Results

Network Level Authentication is a new authentication method that enhances security by providing user authentication earlier in the connection process when a client connects to an RD Session Host server. With Network Level Authentication, user authentication occurs before a full Remote Desktop connection to the RD Session Host server is established.

Specify whether Network Level Authentication is required.


☐ **Require Network Level Authentication**  
Only computers that are running both a version of Windows and a version of the Remote Desktop Connection client that supports Network Level Authentication can connect to this RD Session Host server. If you are remotely connected to this server, ensure that your computer supports Network Level Authentication to enable reconnection to this server.

☒ **Do not require Network Level Authentication**  
Computers that are running any version of the Remote Desktop Connection client can connect to this RD Session Host server.

 This option is less secure than when Network Level Authentication is used because user authentication occurs later in the connection process.

- Choose the correct licensing model for your Client Access Licenses (CALs)

**Add Roles Wizard**

 **Specify Licensing Mode**

Before You Begin  
Server Roles  
Remote Desktop Services  
    Role Services  
    Application Compatibility  
    Authentication Method  
**Licensing Mode**  
User Groups  
Client Experience  
RD Licensing Configuration  
Confirmation  
Progress  
Results


The Remote Desktop licensing mode determines the type of Remote Desktop Services client access licenses (RDS CALs) that a license server will issue to clients that connect to this RD Session Host server.

Specify the Remote Desktop licensing mode that you want this RD Session Host server to use.

☐ **Configure later**  
Remind me to use the Remote Desktop Session Host Configuration tool or Group Policy to configure the licensing mode within the next 120 days.

☐ **Per Device**  
An RDS Per Device CAL must be available for each device that connects to this RD Session Host server.

☒ **Per User**  
An RDS Per User CAL must be available for each user that connects to this RD Session Host server.

 The licensing mode that you specify must match the RDS CALs that are available from your Remote Desktop license server.

- Add the Users or Domain Groups that require RDS Access

**Add Roles Wizard**

**Select User Groups Allowed Access To This RD Session Host Server**

Before You Begin  
Server Roles  
Remote Desktop Services  
Role Services  
Application Compatibility  
Authentication Method  
Licensing Mode  
**User Groups**  
Client Experience  
RD Licensing Configuration  
Confirmation

Add the users or user groups that can connect to this RD Session Host server. These users and user groups will be added to the local Remote Desktop Users group. The Administrators group is added by default and cannot be removed.

Users or User Groups:

- Administrators
- TERMINAL SERVER USER

Add... Remove

- On 'Configure Client Experience', you could leave everything as default and then click on Next

**Add Roles Wizard**

**Configure Client Experience**

Before You Begin  
Server Roles  
Remote Desktop Services  
Role Services  
Application Compatibility  
Authentication Method  
Licensing Mode  
User Groups  
**Client Experience**  
RD Licensing Configuration  
Confirmation  
Progress  
Results

You can configure the RD Session Host server so that users connecting to a remote desktop session can use functionality similar to that provided by Windows 7.

**Warning:** Providing this functionality requires additional system and bandwidth resources and may affect the scalability of the RD Session Host server.

Select the functionality that you want to provide. Additional functionality can be configured by using the Remote Desktop Session Host Configuration tool.

**Information:** Selecting audio and video playback or desktop composition will install the [Desktop Experience feature](#) on the RD Session Host server.

☐ Audio and video playback  
☐ Audio recording redirection  
☐ Desktop composition (provides the user interface elements of Windows Aero)

- Check 'Configure a discovery scope for RD licensing', select 'This Domain', then click 'Next'

The screenshot shows the 'Add Roles Wizard' window with the title bar 'Add Roles Wizard'. The main title is 'Configure Discovery Scope for RD Licensing'. On the left is a navigation pane with the following items: 'Before You Begin', 'Server Roles', 'Remote Desktop Services', 'Role Services', 'Application Compatibility', 'Authentication Method', 'Licensing Mode', 'User Groups', 'Client Experience', 'RD Licensing Configuration' (which is highlighted), 'Confirmation', 'Progress', and 'Results'. The main content area contains the following text: 'The discovery scope for a Remote Desktop license server is used by RD Session Host servers to automatically discover the license server. This does not apply to RD Session Host servers running Windows Server 2008 R2 and applies only to those running Windows Server 2008, Windows Server 2003, or Windows 2000.' Below this is a yellow warning icon and the text: 'Microsoft recommends that you do not configure a discovery scope for the license server. Instead, you should use the Remote Desktop Session Host Configuration tool to specify a license server for the RD Session Host server to use.' There are three radio button options: 'This workgroup' (selected), 'This domain', and 'The forest'. Below 'This workgroup' is the text: 'RD Session Host servers in the same workgroup can discover this license server.' Below 'This domain' is the text: 'RD Session Host servers in the same domain can discover this license server. To configure this scope, this computer must be a member of a domain, and you must be logged on as a domain administrator.' Below 'The forest' is the text: 'RD Session Host servers from multiple domains in the same forest can discover this license server. To configure this scope, this computer must be a member of a domain, and you must be logged on as an enterprise administrator.' At the bottom, there is a red 'X' icon and the text: 'You must be logged in as a member of the Domain Admins group.' Below this is the text: 'Select a location for the RD Licensing database:' followed by a text box containing 'C:\Windows\system32\LServer' and a 'Browse...' button.

**Add Roles Wizard**

### Configure Discovery Scope for RD Licensing

Before You Begin  
Server Roles  
Remote Desktop Services  
Role Services  
Application Compatibility  
Authentication Method  
Licensing Mode  
User Groups  
Client Experience  
**RD Licensing Configuration**  
Confirmation  
Progress  
Results

The discovery scope for a Remote Desktop license server is used by RD Session Host servers to automatically discover the license server. This does not apply to RD Session Host servers running Windows Server 2008 R2 and applies only to those running Windows Server 2008, Windows Server 2003, or Windows 2000.

Microsoft recommends that you do not configure a discovery scope for the license server. Instead, you should use the Remote Desktop Session Host Configuration tool to specify a license server for the RD Session Host server to use.

☒ **Configure a discovery scope for this license server**

☐ **This workgroup**  
RD Session Host servers in the same workgroup can discover this license server.

☐ **This domain**  
RD Session Host servers in the same domain can discover this license server. To configure this scope, this computer must be a member of a domain, and you must be logged on as a domain administrator.

☐ **The forest**  
RD Session Host servers from multiple domains in the same forest can discover this license server. To configure this scope, this computer must be a member of a domain, and you must be logged on as an enterprise administrator.

You must be logged in as a member of the Domain Admins group.

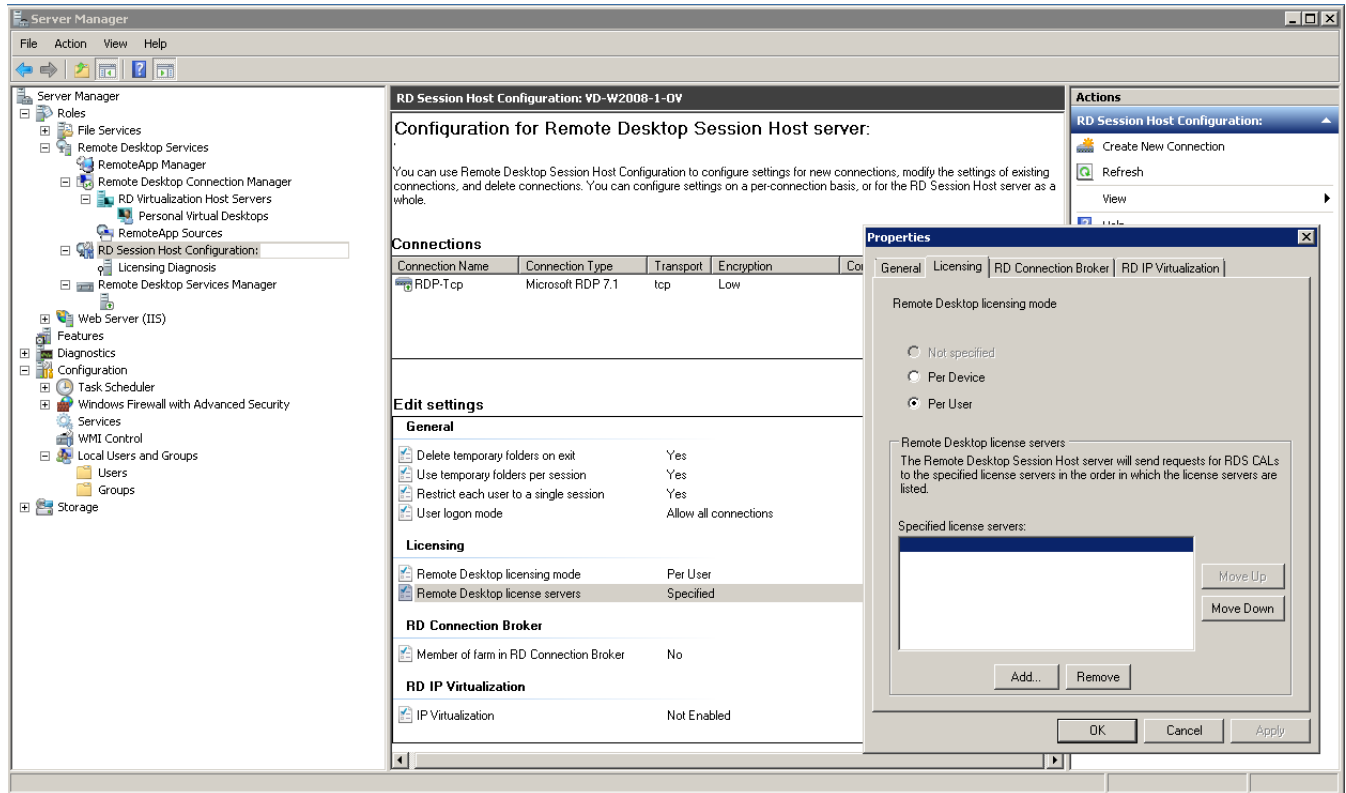
Select a location for the RD Licensing database:  
C:\Windows\system32\LServer Browse...

- Confirm selection and click 'Install'

## 4.1. Setup Remote Desktop Licenses

Installing and configuring a RDS CAL license in Windows Server 2012 R2 has been discussed in the previous chapter. Here it is demonstrated how to use the RDS licensing server available on the local network (domain).

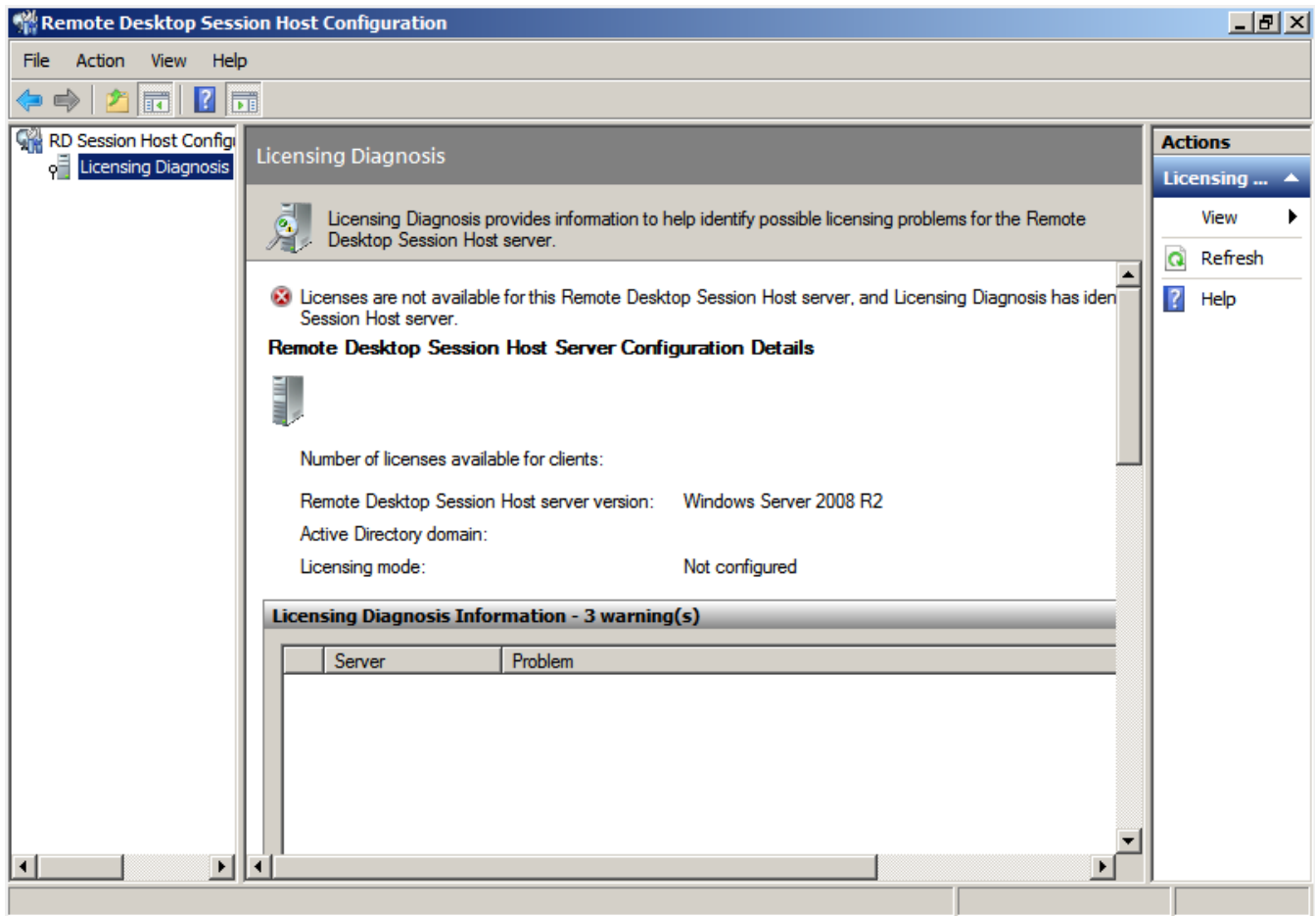
- Launch 'Server Manager'
- In the Left Pane - Select 'RD Session Host Configuration'
- In the Right Pane - Right click 'Remote Desktop license servers' and select 'Properties'
- Fill in the details of your specified License Server



#### 4.1.1. License Diagnostics

The Licensing Diagnosis tool is available to assist troubleshooting any Remote Desktop CAL licensing issues:

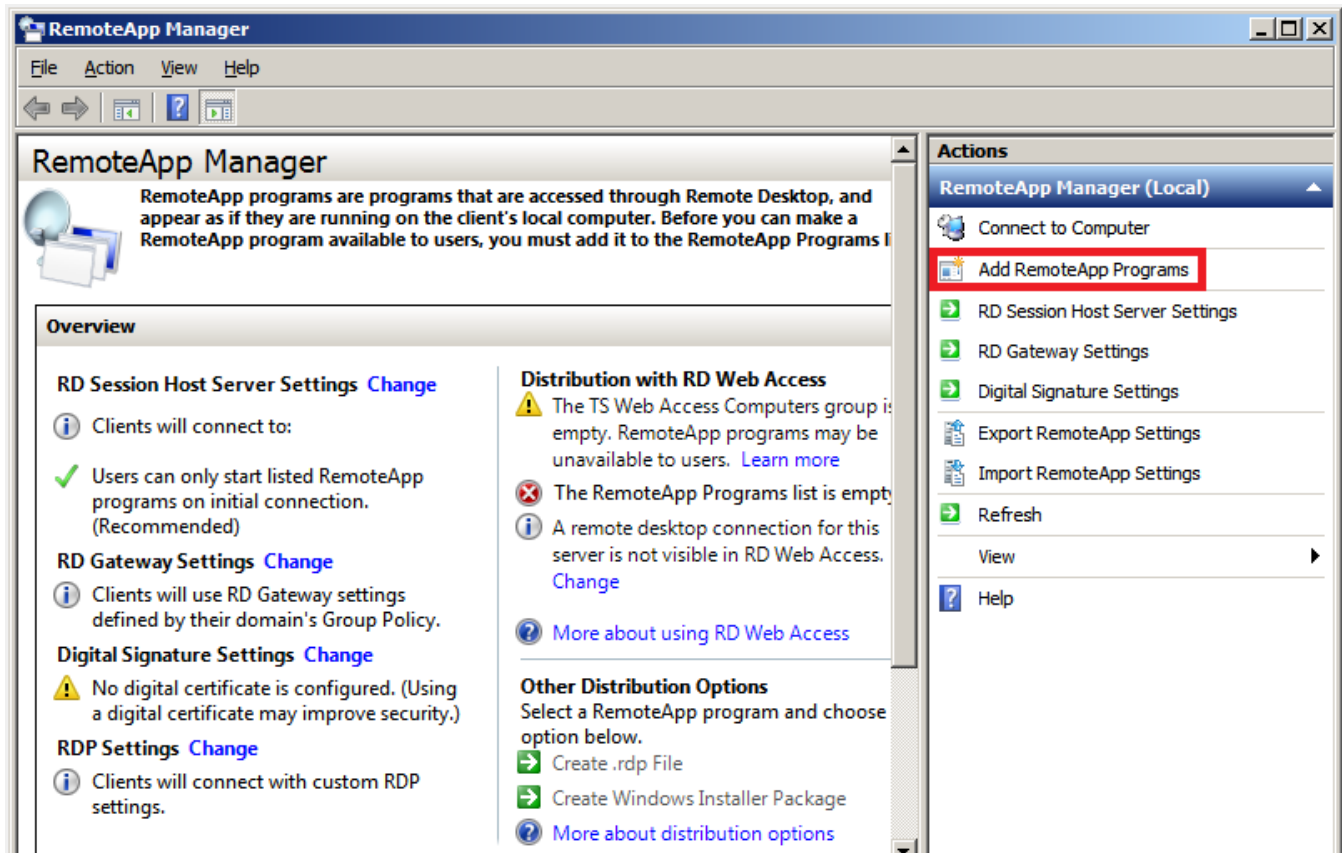
- Launch 'TSconfig.msc' from the Windows 'Run' dialog



## 4.2. Publish RemoteApp

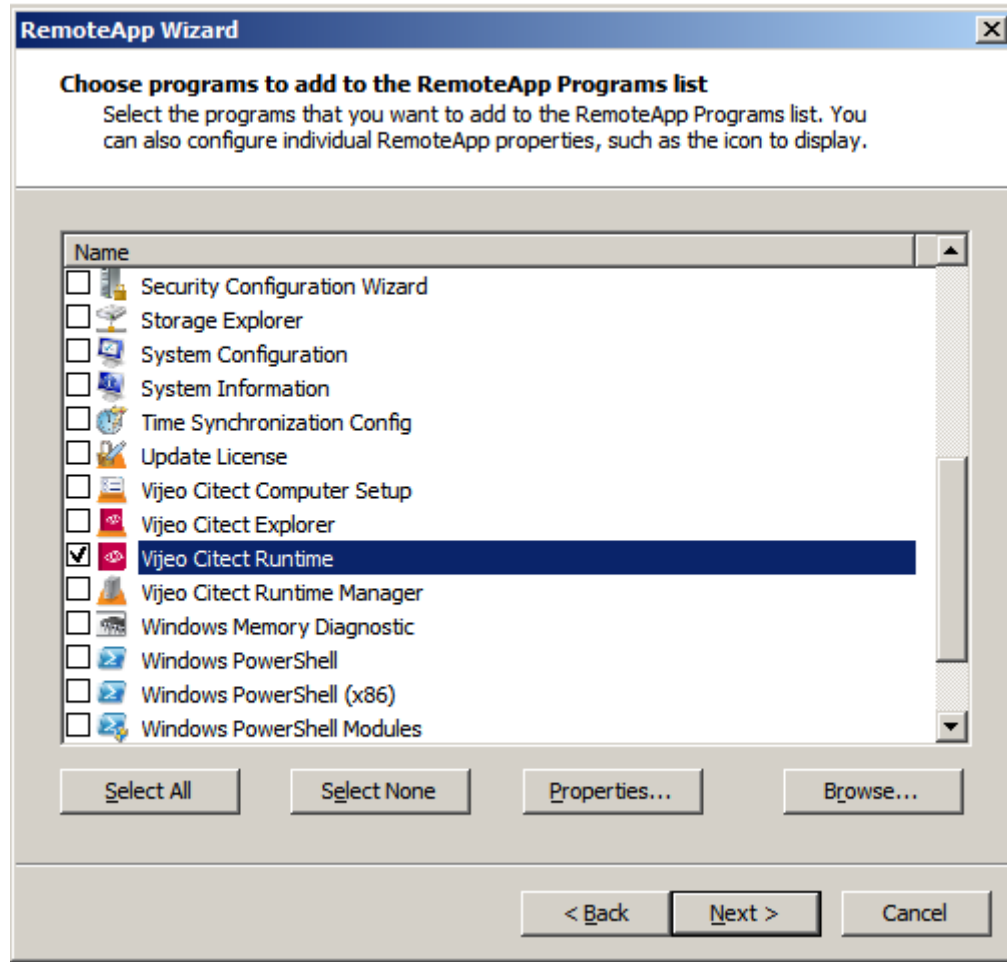
To publish a RemoteApp in Windows Server 2008 R2 follow these steps:

- **Start > Administrative Tools > Remote Desktop Services**, then click 'RemoteApp Manager'.



- Click 'Add RemoteApp Programs'


- Progress through the Wizard:



- Select '**Vijeo Citect Runtime**' and click '**Properties**'

**RemoteApp Properties** [?] [X]

Properties | User Assignment

 RemoteApp program name:

Location:

Alias:

☒ RemoteApp program is available through RD Web Access

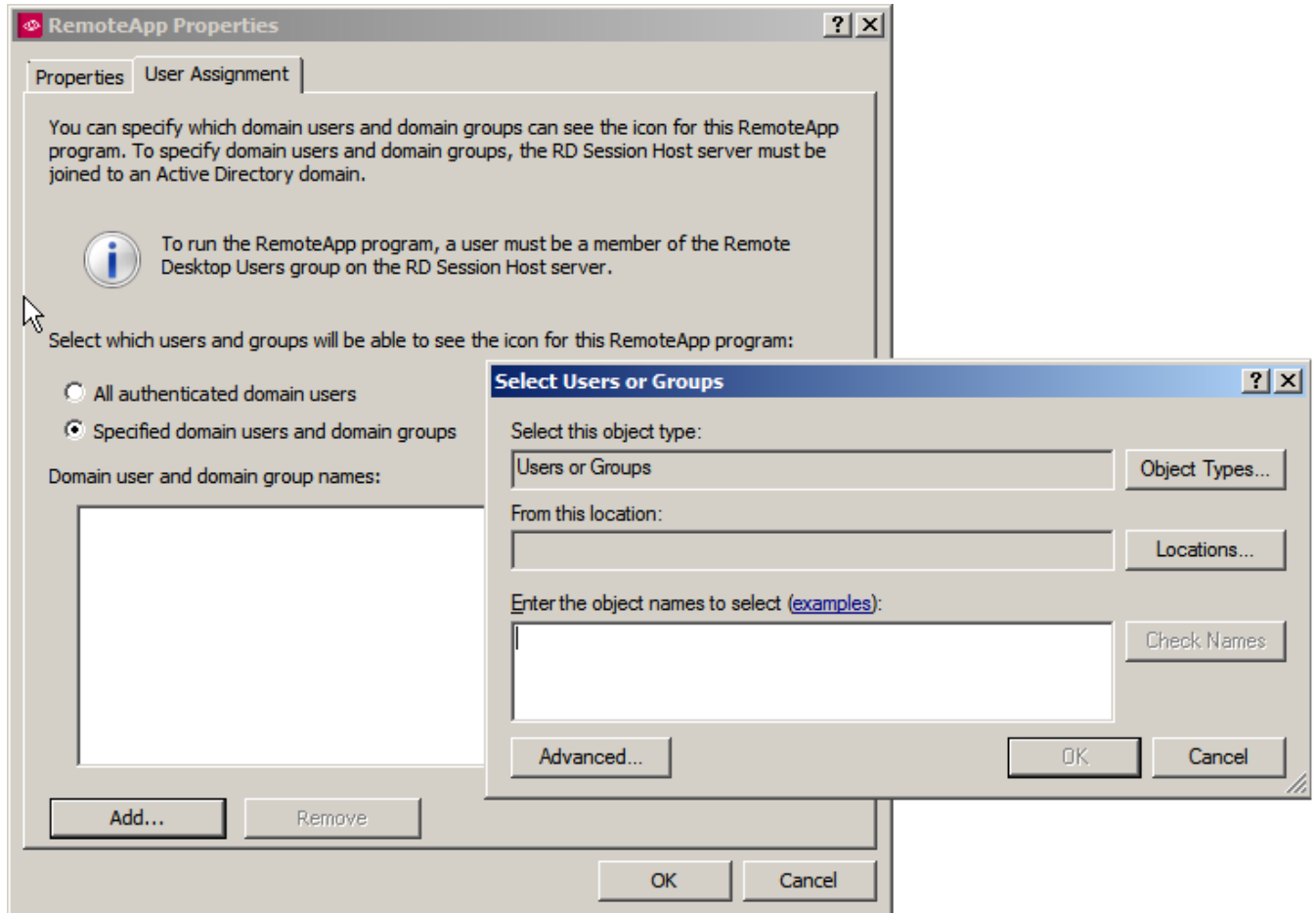
Command-line arguments

☐ Do not allow command-line arguments  
☐ Allow any command-line arguments  
☒ Always use the following command-line arguments:

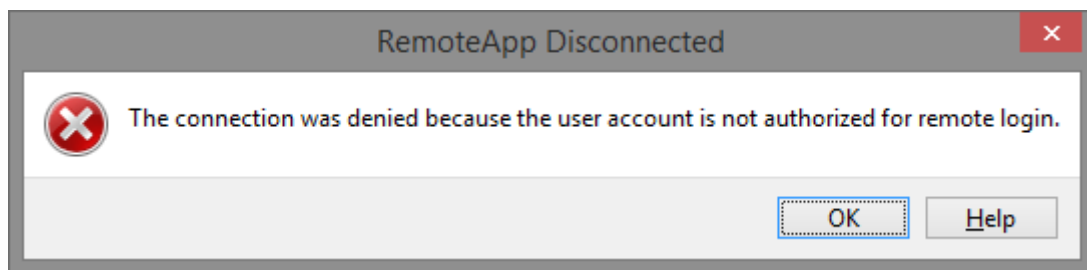
**IMPORTANT:** Specify “/x” as a command-line argument, this will ensure that only a Client process is run, without the Runtime Manager. This is necessary to ensure that the multiple Client instances do not interfere with each other.



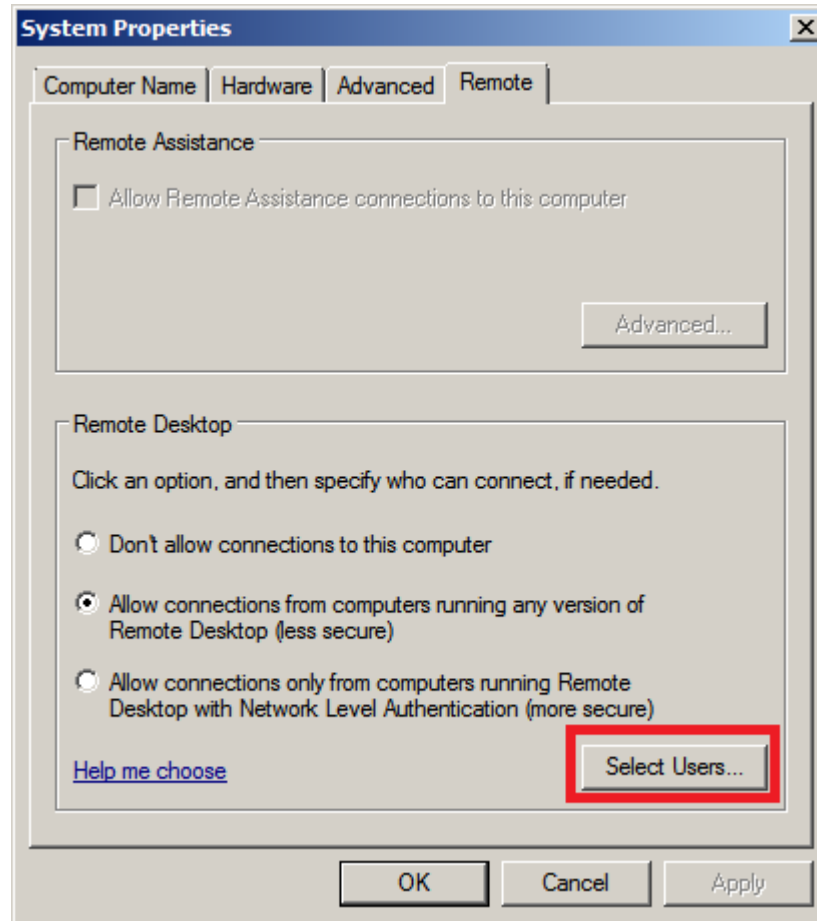
- Select the 'User Assignment' Tab.



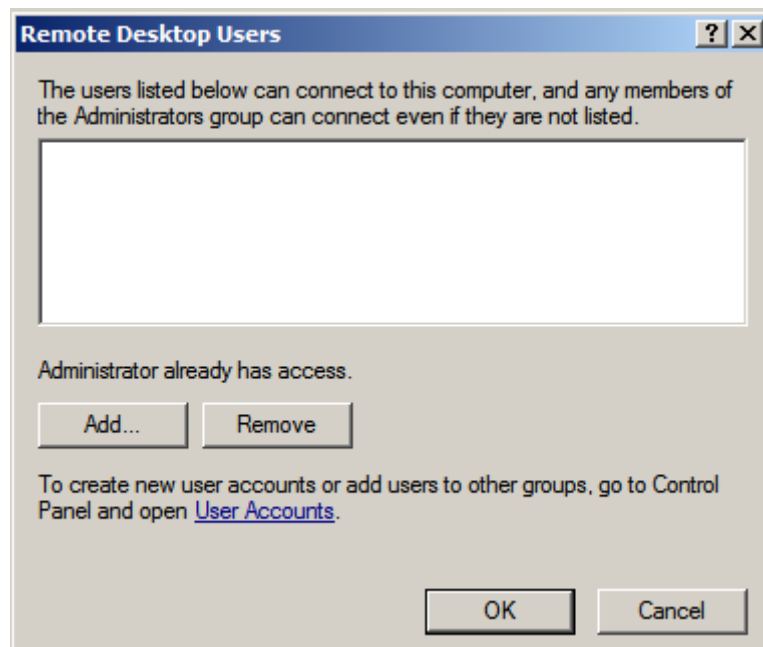
- Set your desired security
- We recommend restricting to only the required users or limited domain groups
- In addition you will need to add the user/group to the list of allowed 'Remote Desktop Users', otherwise you will get the error below when trying to launch the **RemoteApp**



- Open **'System Properties'** - from the **'Run'** dialog, type **'SystemPropertiesRemote'**



- Click **'Select Users'**
- Add the required Users / Groups.



### 4.2.1. Custom INI Paths - View-Only & Control Clients

Custom INI paths can be set for the RemoteApp, this is especially important if you are also running your SCADA Servers on the same machine, or if you have a mix of '**View-Only**' and '**Control**' Clients. It is also possible to specify the license type and override the default citect.ini settings using the switch /l (l for license). For more details see section 1.3.

Ensure any custom INI files are accessible by the intended users.

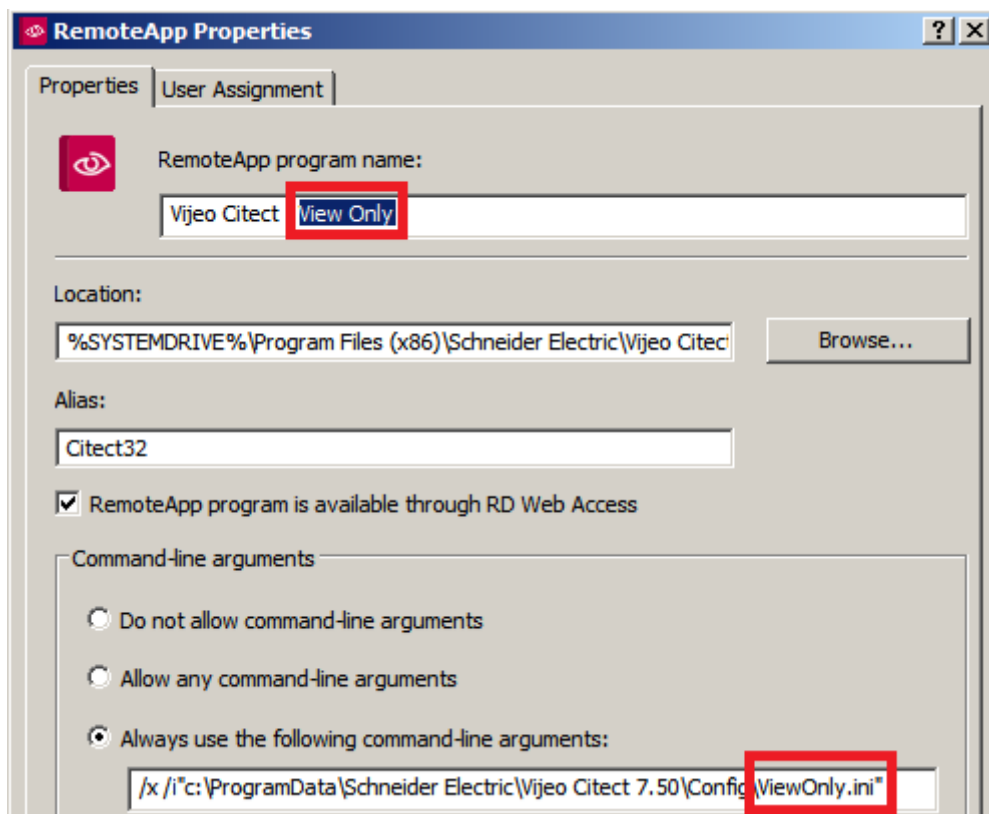
#### 4.2.1.1 INI Parameters

The INI Parameters that govern which type of license the Client will take are:

[Client] ComputerRole  
0 = Server and Control Client  
1 = Control Client (enables [Client]FullLicense)  
2 = View-Only Client  
[Client] FullLicense  
0 = Do not use a full license  
1 = Use a Full license

#### 4.2.1.2 View-Only Client

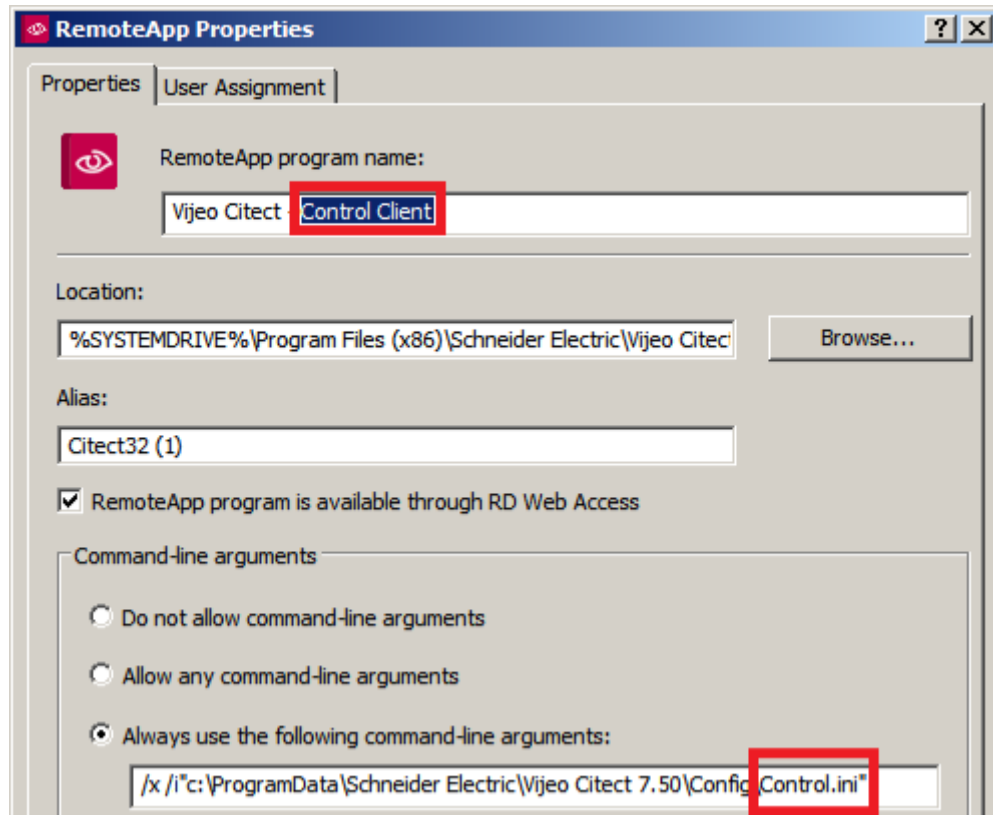
- Copy, rename and edit the INI file to contain:  
[Client] ComputerRole = 2
- Rename your RemoteApp to indicate it is '**View Only**'
- Modify the '**command-line arguments**' to point to this new INI file:  
'/x' to prevent Runtime Manager from loading  
'/i' followed by a custom INI path (encased in double quotes)



- Alternatively, if you don't want to specify a custom citect.ini file, you can override the local citect.ini role setting to force a **view-only client**, by using the /l switch in conjunction with /x:  
**/x /l:1**

#### 4.2.1.3 Control Client

- Copy, rename and edit the INI file to contain:  
[Client] ComputerRole = 1  
[Client] FullLicence=0
- Publish a second instance of the RemoteApp
- Under '**General**', rename it to indicate it is a '**Control**' Client
- Modify the '**Parameters**' to point to this new INI file:  
'/x' to prevent Runtime Manager from loading  
'/i' followed by a custom INI path (encased in double quotes)



- Alternatively, if you don't want to specify a custom citect.ini file, you can override the local citect.ini role setting to force a **control client**, by using the /l switch in conjunction with /x:  
**/x /l:2**
- Two newly created instances can now be seen on the [http://your\\_server/rdweb](http://your_server/rdweb) page:



### Remote Desktop Services Default Connection

RemoteApp and Desktop Connection

RemoteApp Programs

Remote Desktop

Help

Sign out



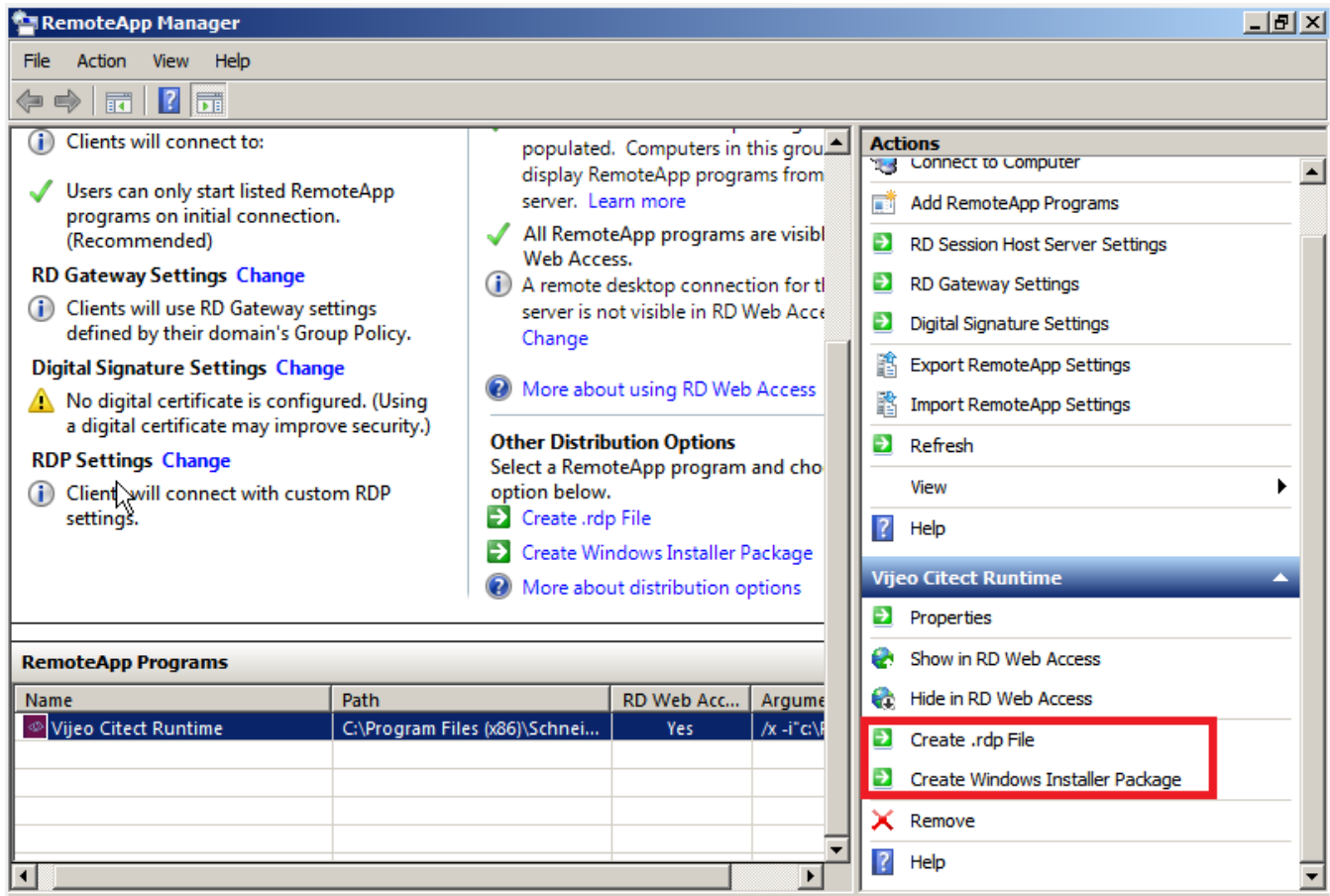
Vijeo Citect -  
Control  
Client



Vijeo Citect -  
View Only

### 4.2.2. Alternative Distribution Method

Instead of navigating via the RDWeb webpage, you could also create an .rdp file, or even an installation package, which can be distributed to the Client machines, and run directly.

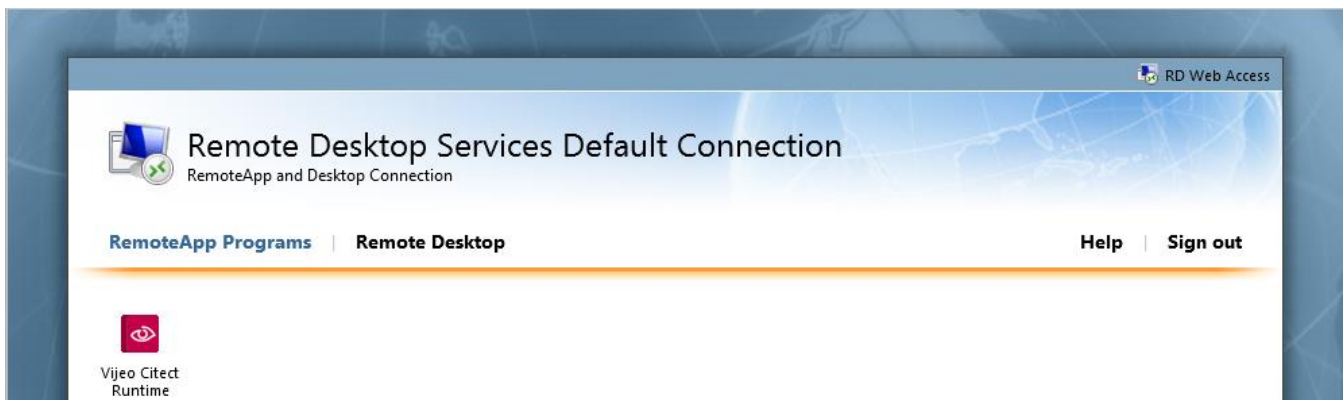


## 5. Run the RemoteApp

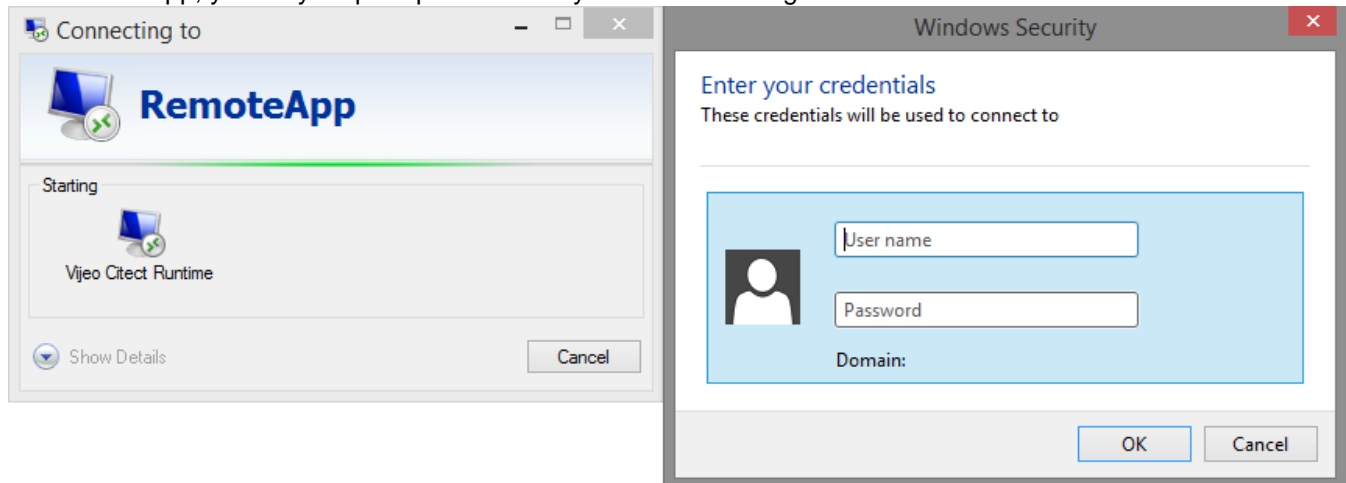
- From another PC, navigate Internet Explorer to: [http://your\\_server/rdweb](http://your_server/rdweb)



- Login as a privileged user

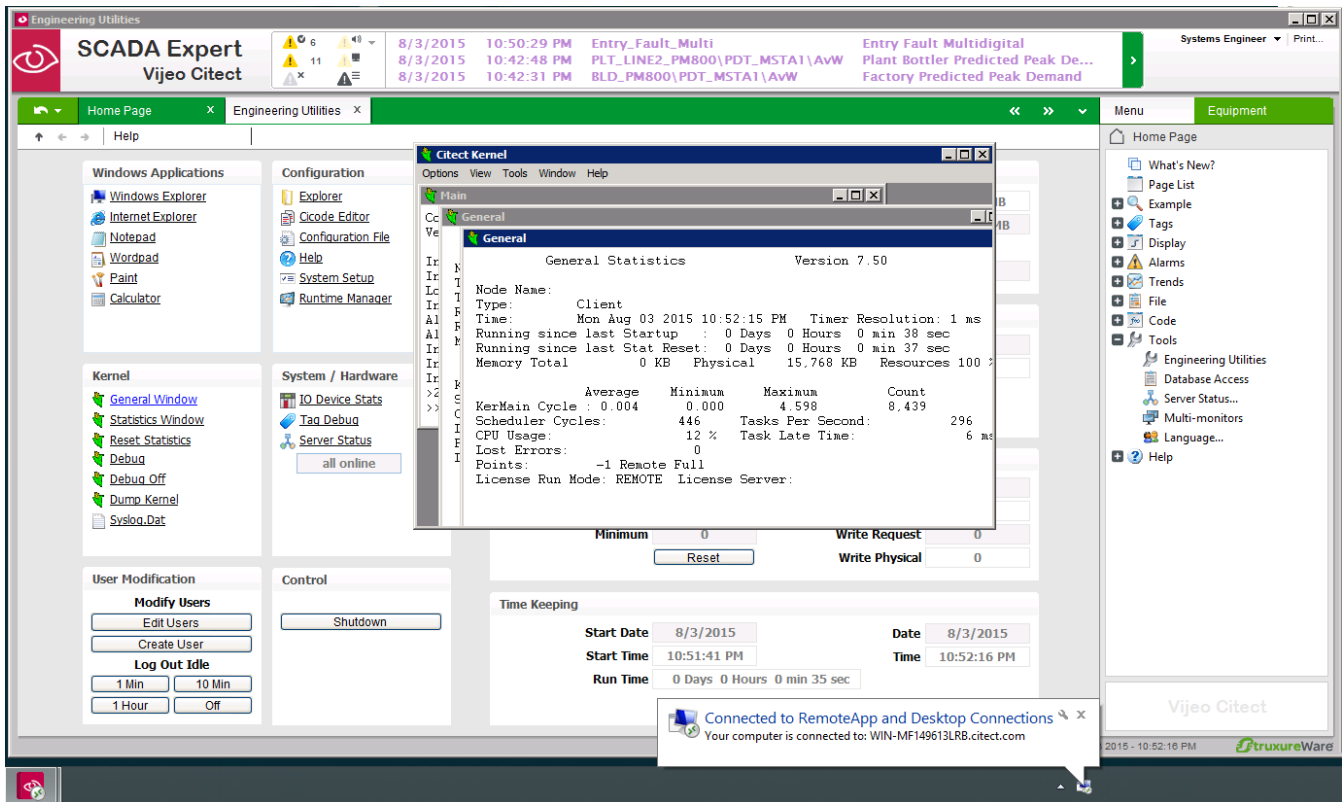


- We can see our RemoteApp is available
- Launch the App, you may be prompted to enter your credentials again:

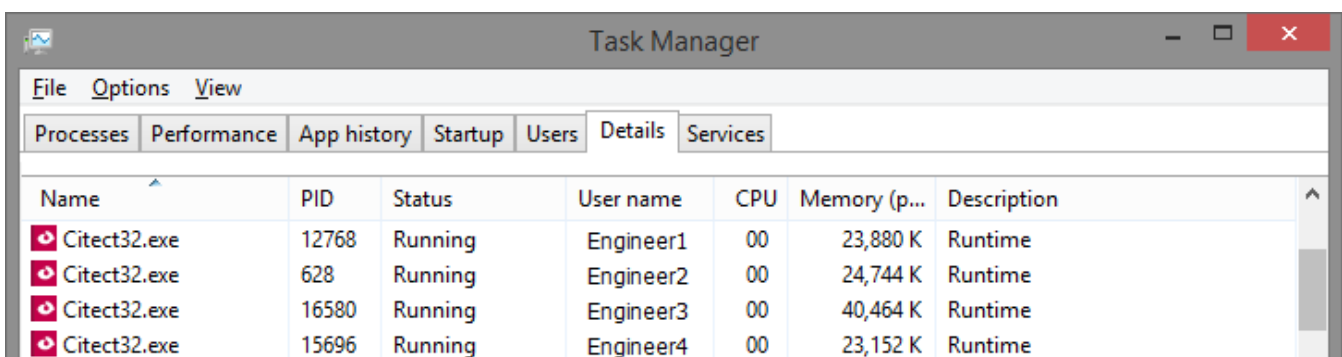


- You may be prompted with a dialog asking which local resources you wish to share

- Typically none are required, but this may be project-dependent



- The Client will launch much the same as a local client
- The modified logo and the System Tray messages show that it is running as a **RemoteApp**
- Unlike a WebClient, the Kernel is still accessible
- On the RDSH machine, Task Manager will reveal the RemoteApp connections, showing additional Citect32.exe instances being spawned under different accounts:



## 6. Appendix A – Installer Known Issue

**Note:** Group Policies only apply to Domain Accounts.  
You must use a Domain Account for this workaround.

If the RDS service is already installed when you try to Install VJC, the '**Windows Installer Coordinator**', will appear to 'hang' and the installer will never complete.

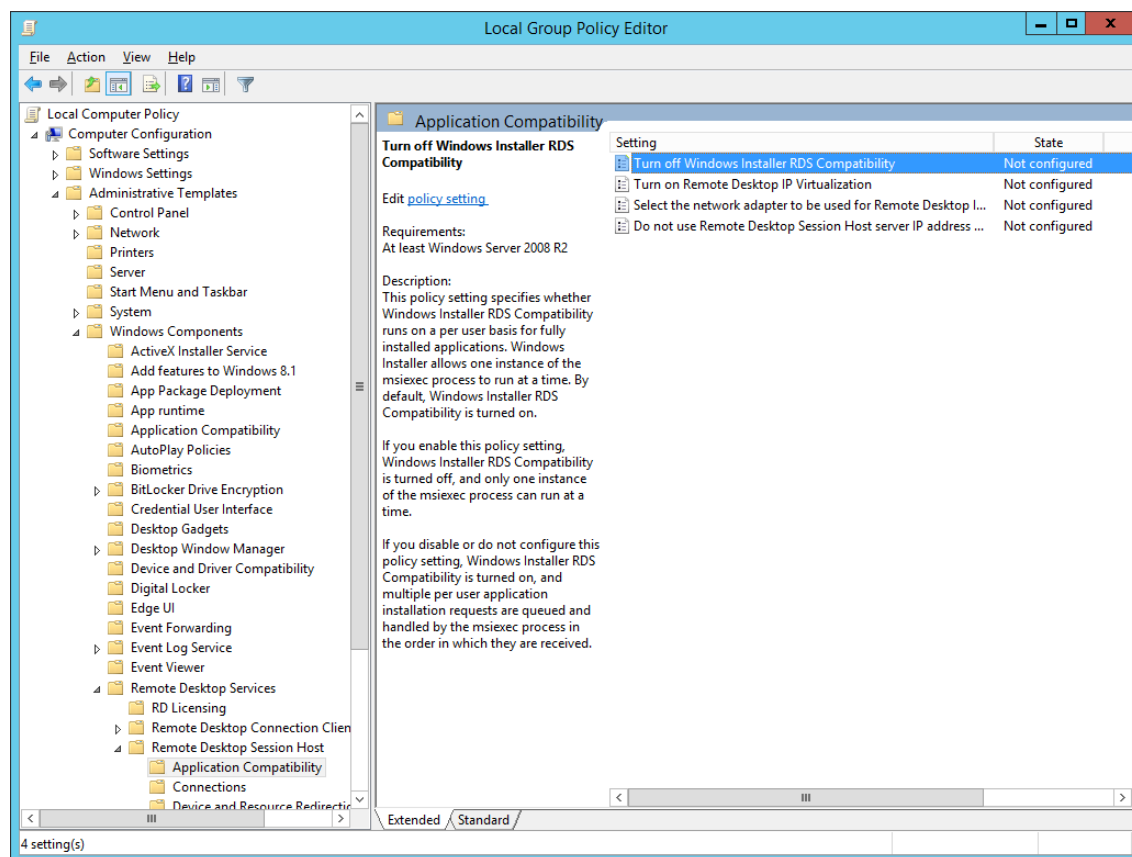
This problem is caused by an incompatibility with the Embedded MSI technology and the Windows Installer Coordinator. The Coordinator is responsible for keeping multiple MSI installations from running concurrently.

The work around for this issue is to disable the '**Remote Desktop Session Host Windows Installer**' for the duration of the installation:

- Run 'Gpedit.msc' to launch 'Local Group Policy Editor'
- Go to:

Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Application Compatibility

- Set "Turn off Windows Installer RDS Compatibility" to **ENABLED**
- Once this property is turned off, **Windows Installer Coordinator** should immediately continue to the next task, however, you may need to restart the installation
- This setting can be reverted once the installer has completed



More information on the following KB from Windows Support: <http://support.microsoft.com/kb/2655192>



## 7. Appendix B – License Server Known Issue

If the RDSH server returns an error about no licensing server being set, please follow the instructions below.

Use the following query to see what is currently set on the server (use Windows PowerShell running as Administrator):

```
$obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TerminalServiceSetting
$obj.GetSpecifiedLicenseServerList()
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

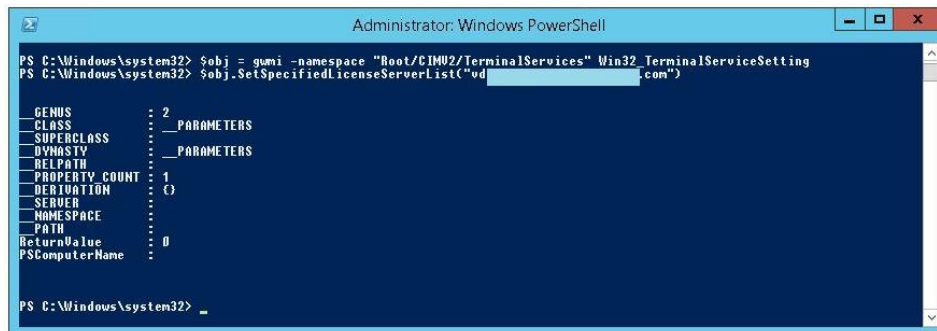
PS C:\Windows\system32> $obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TerminalServiceSetting
PS C:\Windows\system32> $obj.GetSpecifiedLicenseServerList()

GENUS              : 2
CLASS              : _PARAMETERS
SUPERCLASS         : _PARAMETERS
DYNASTY            : _PARAMETERS
RELPATH            :
PROPERTY_COUNT     : 2
DERIVATION         : {}
SERVER             :
NAMESPACE          :
PATH               :
ReturnValue        : 0
SpecifiedLSList    : {}
PSComputerName     :

PS C:\Windows\system32>
```

If there is no licensing server specified in the SpecifiedLSList, we can set this manually using the following command lines:

```
$obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TerminalServiceSetting
$obj.SetSpecifiedLicenseServerList("LicenseServerName.DomainName.com")
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

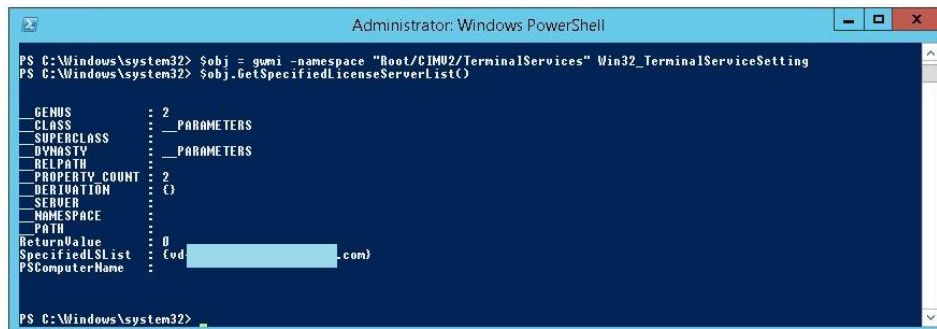
PS C:\Windows\system32> $obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TerminalServiceSetting
PS C:\Windows\system32> $obj.SetSpecifiedLicenseServerList("vd[redacted].com")

GENUS              : 2
CLASS              : _PARAMETERS
SUPERCLASS         : _PARAMETERS
DYNASTY            : _PARAMETERS
RELPATH            :
PROPERTY_COUNT     : 1
DERIVATION         : {}
SERVER             :
NAMESPACE          :
PATH               :
ReturnValue        : 0
SpecifiedLSList    : {}
PSComputerName     :

PS C:\Windows\system32>
```

Running the followings query again to show the value set:

```
$obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TerminalServiceSetting
$obj.GetSpecifiedLicenseServerList()
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> $obj = gwmi -namespace "Root/CIMV2/TerminalServices" Win32_TerminalServiceSetting
PS C:\Windows\system32> $obj.GetSpecifiedLicenseServerList()

GENUS              : 2
CLASS              : _PARAMETERS
SUPERCLASS         : _PARAMETERS
DYNASTY            : _PARAMETERS
RELPATH            :
PROPERTY_COUNT     : 2
DERIVATION         : {}
SERVER             :
NAMESPACE          :
PATH               :
ReturnValue        : 0
SpecifiedLSList    : {vd[redacted].com}
PSComputerName     :

PS C:\Windows\system32>
```