AutomaTech Application Note – July 2015

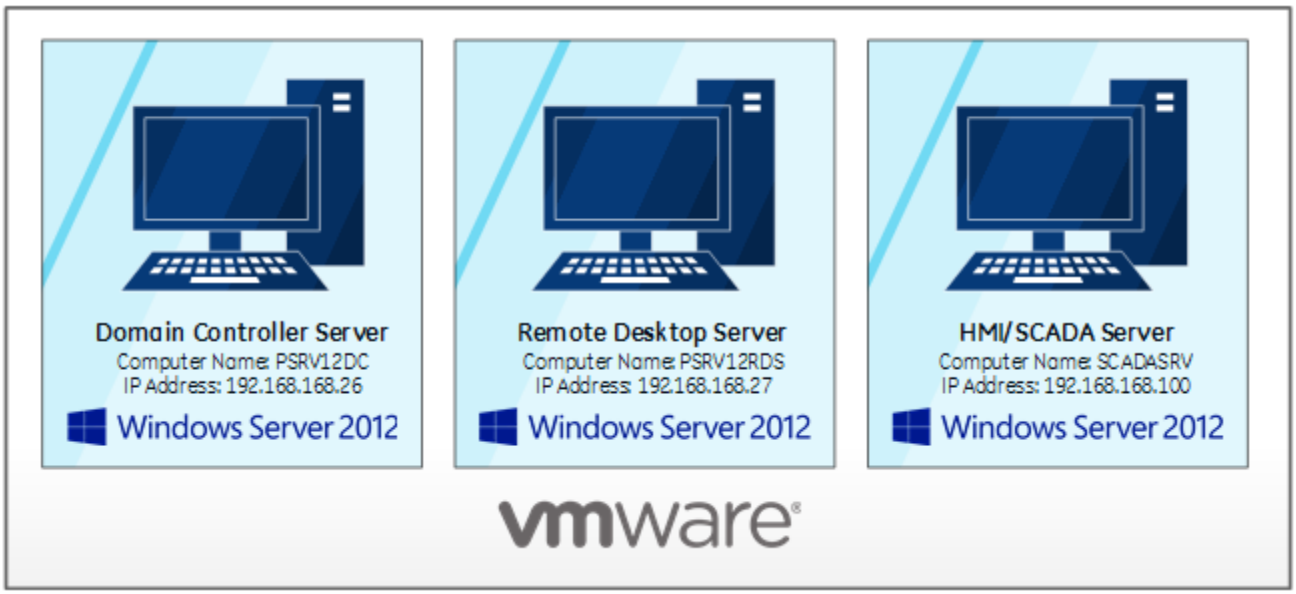
Installing Active Directory Domain Services (AD DS), Remote Desktop Services (RDS), GE Advantage Licensing, and GE Proficy SCADA Thin Clients on Windows Server 2012 R2

SUMMARY

This application note provides a high level overview for deploying Thin Client (Remote Desktop Services) Proficy HMI/SCADA Clients under Microsoft's Windows Server 2012 R2 Operating System. The following topics are covered in this application note:

1. Installing and Configuring Active Directory Domain Services (AD DS) on a Domain Controller Server computer running Windows Server 2012 R2
2. Installing, Configuring, and Licensing Remote Desktop Services (RDS) on a Remote Desktop Server computer running Windows Server 2012 R2
3. Installing, Configuring, and Activating GE Advantage Licensing on a Local License Server for use with GE Proficy SCADA Thin Clients
4. Overview of Installing and Configuring GE Proficy HMI/SCADA iFIX for use in a Remote Desktop Services Environment
5. Overview of Installing and Configuring GE Proficy HMI/SCADA CIMPLICITY for use in a Remote Desktop Services Environment

This application note assumes you have a solid understanding of Microsoft Windows Operating Systems, Networking, Virtualization, GE Proficy HMI/SCADA products, and that your HMI/SCADA infrastructure has already been established. A simplified architecture of the computers used in this application note are depicted below.



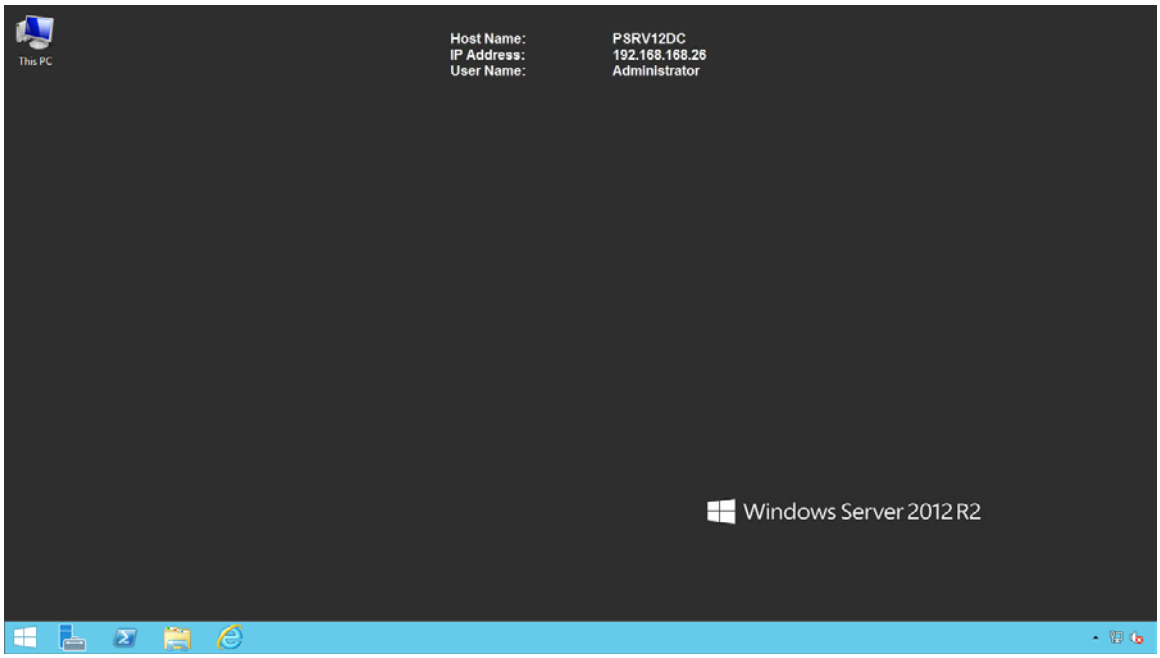
The following conditions have been taken into account in the writing of this application note:

- GE Intelligent Platforms & AutomaTech recommend that the Thin Client/Remote Desktop Server exist on a separate, dedicated Server (physical or virtual) from the HMI/SCADA Server.
- Remote Desktop Services infrastructure requires that all Servers join a Domain under the Windows Server 2012 R2 Operating System.
- Remote Desktop Services role cannot co-exist with an Active Directory Domain Controller role under the Windows Server 2012 R2 Operating System.
- As a result of the conditions outlined above, this application note will walk through the process to setup two Windows 2012 R2 Servers: a Domain Controller Server and a Remote Desktop Server referred to throughout.
- The Windows 2012 R2 Operating Systems Domain Controller Server and Remote Desktop Server have been preinstalled and setup with a default configuration.

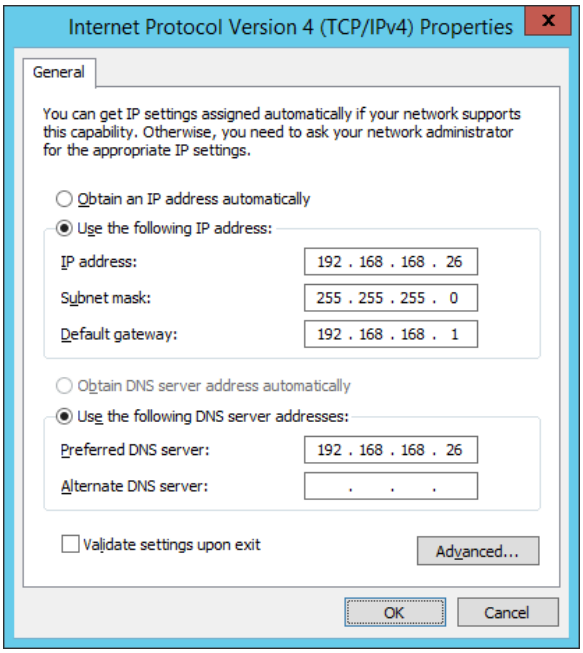
1. Installing and Configuring Active Directory Domain Services (AD DS) on a Domain Controller Server computer running Windows Server 2012 R2

In the following steps you will walk through the process to setup the Active Directory Domain Services (AD DS) Role on the Domain Controller Server computer running Windows Server 2012 R2. In order to setup the Domain Controller Server you will need to understand the IP schema of the network. It is common to use a DHCP Server in the network for automatically assigning IP addresses to Client computers. A Domain Controller must be configured with a Static IP Address, and it is best practice to assign Static IP Addresses to Servers.

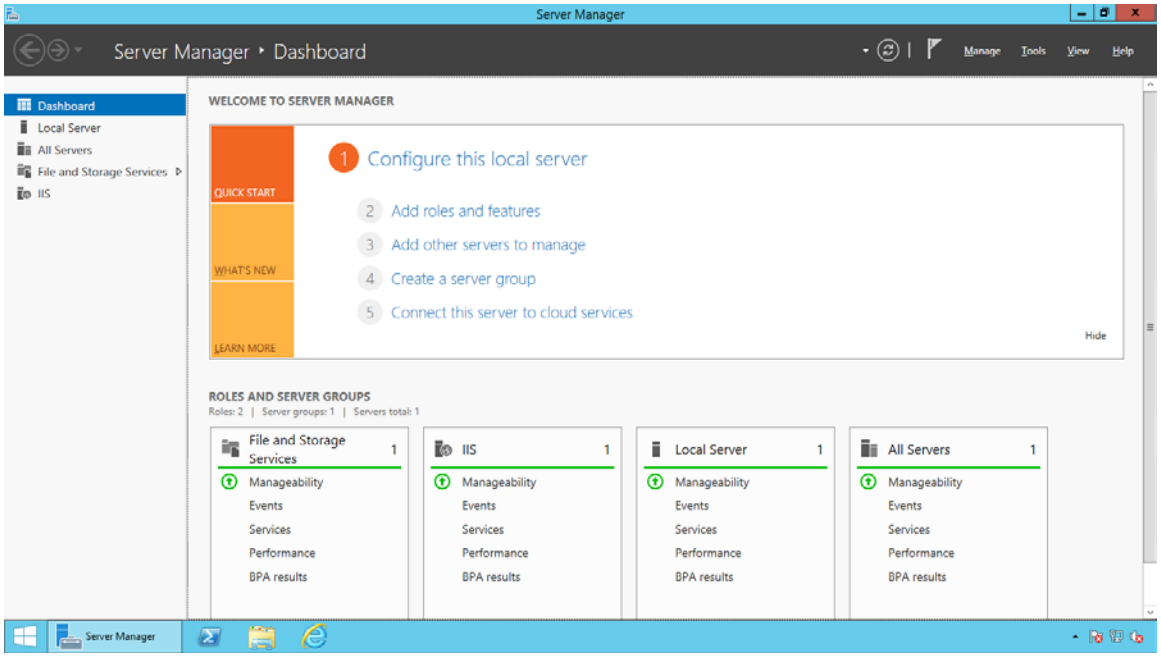
STEP 1: Login to your Domain Controller Server computer as the local Administrator, as pictured below.



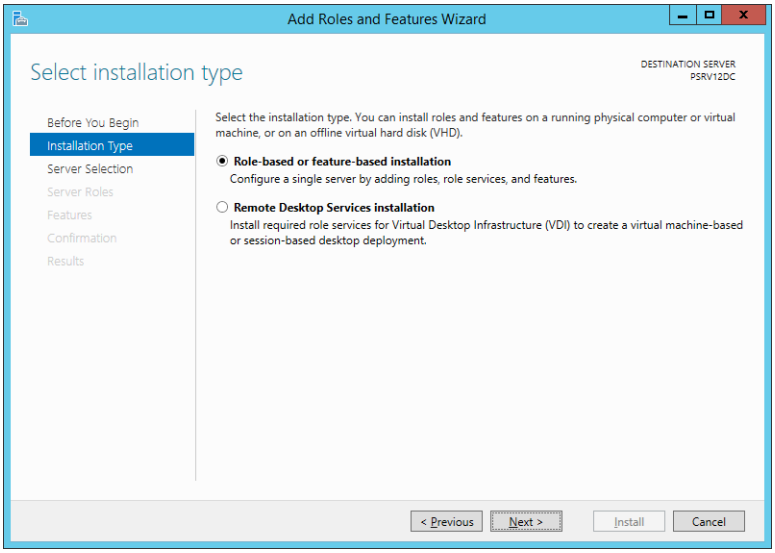
STEP 2: If you are using a single Domain Controller you will also need to specify the Preferred DNS server IP Address as the Server's own IP Address, as pictured below. This step is required for the Active Directory Role to successfully install since the Active Directory service requires a DNS server installed somewhere on the network. If you do not have a DNS server installed on the network, the installation process will automatically install the DNS role on this machine.



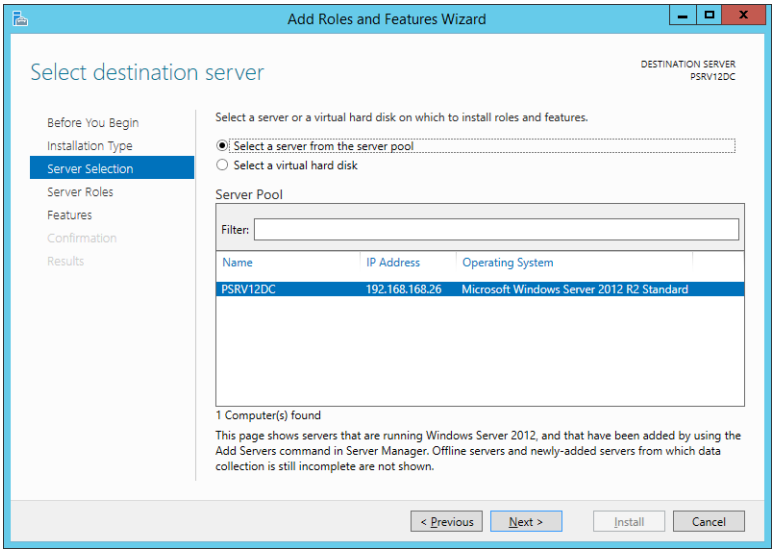
STEP 3: You will now be ready to add the Active Directory role. Launch the **Server Manager** by clicking the icon pinned to the Task Bar. After a few moments the Dashboard will refresh with a complete list of installed Roles.



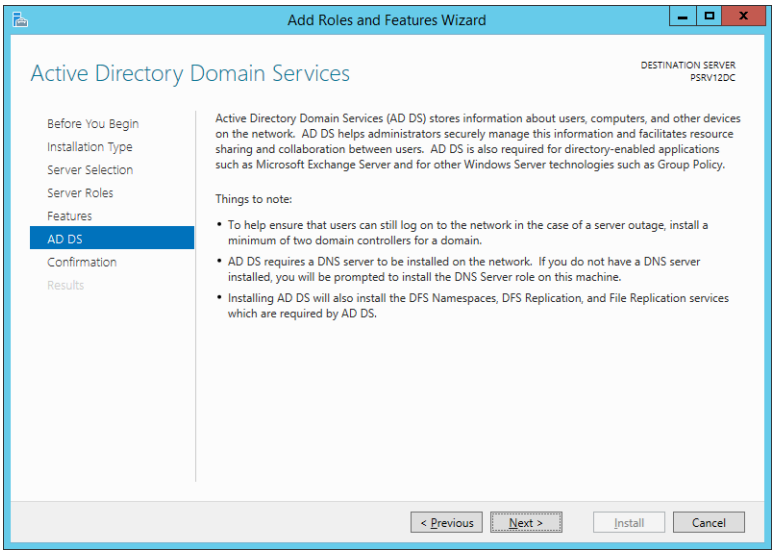
STEP 4: Click the **Add roles and features** link to launch the Add Roles and Features Wizard. Select the Installation Type as **Role-based or feature-based installation** and click **Next.**



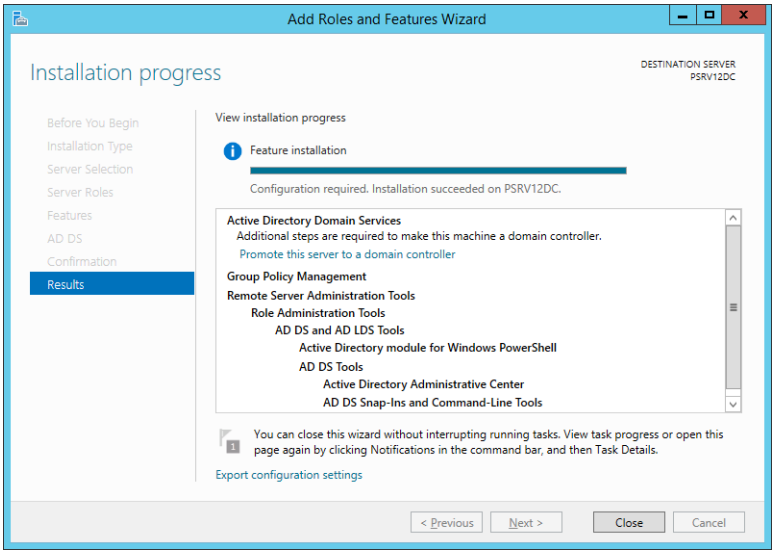
STEP 5: Select your local server name from the Server Pool and click **Next.**



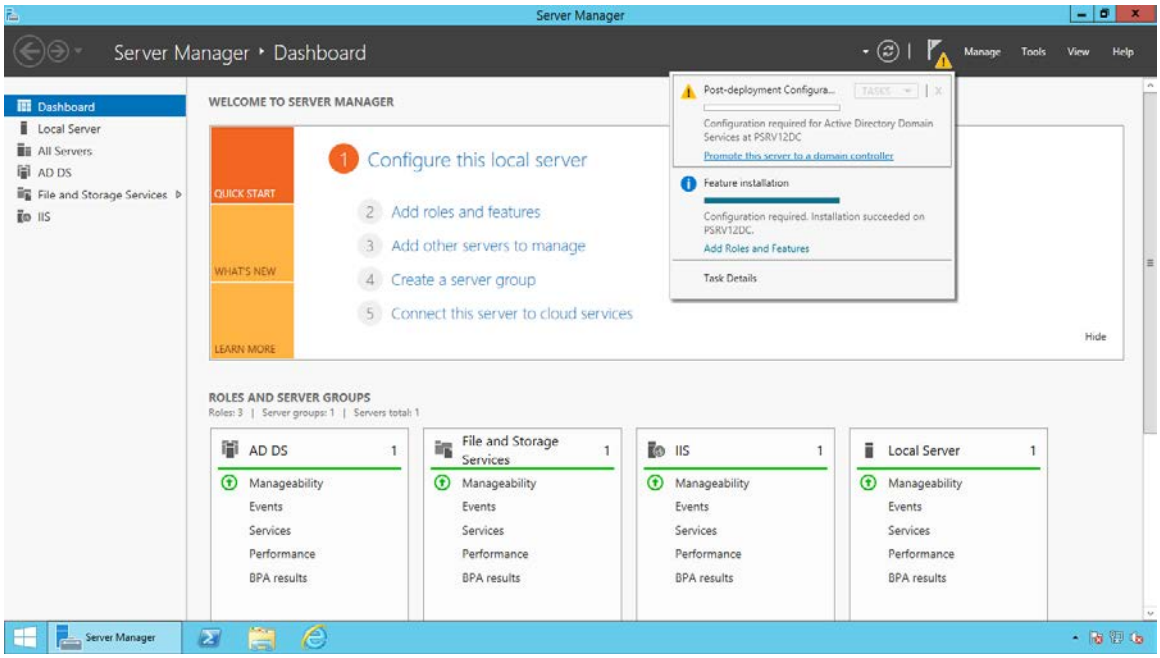
STEP 6: Add the **Active Directory Domain Services** Role from the Server Roles list and click **Next.** Click **Next** on the Features list since you will not be adding new Features. You will be presented with some useful information to note on the AD DS screen, click **Next** to proceed.



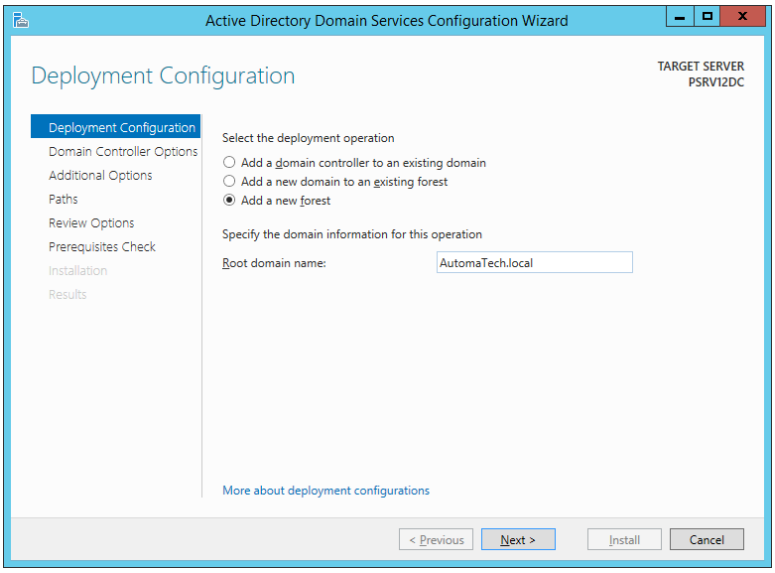
STEP 7: On the Confirmation screen, click **Install** to install the Active Directory Services role and you will see the installation process begin. Upon completion you can click **Close** to complete the installation process.



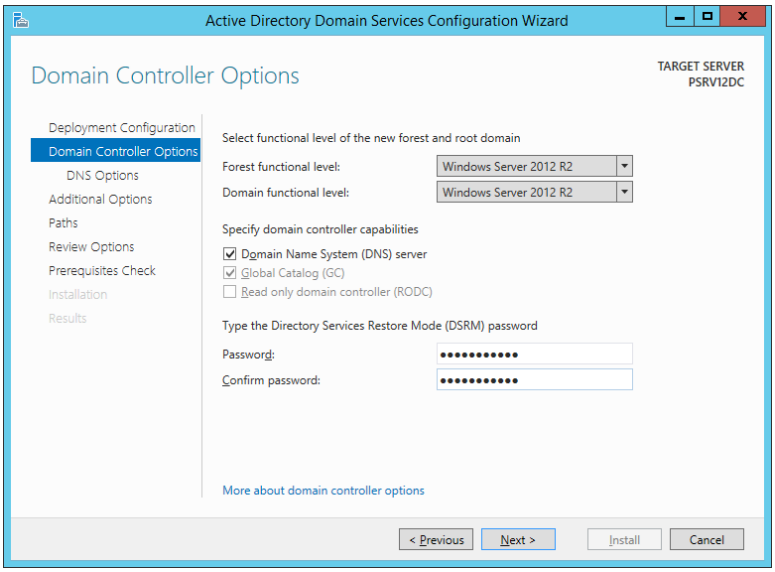
STEP 8: You will notice the yellow exclamation point in the Notifications area indicating additional configuration is required. Click the **Promote the Domain Controller** link to launch the Active Directory Domain Services Configuration Wizard.



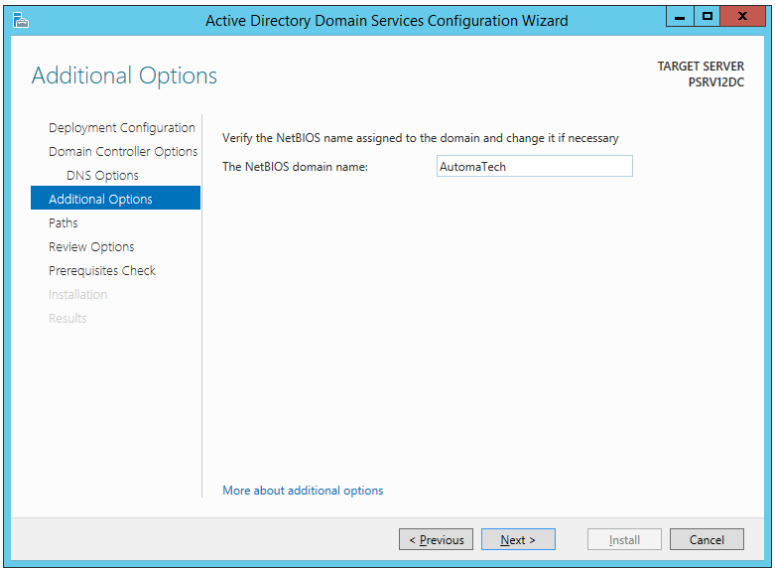
STEP 9: Select the **Add a new forest** option and specify a **Root domain name** and click **Next**. In this example AutomaTech.local will be used as the domain name.



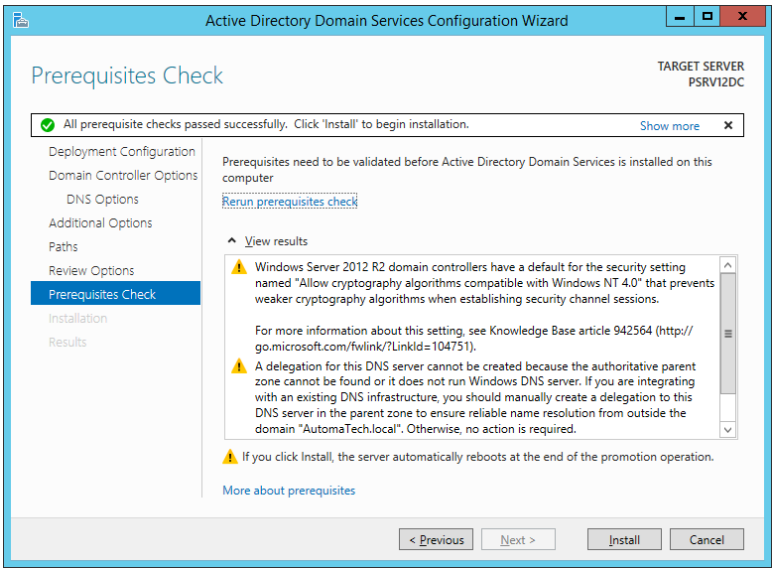
STEP 10: On the Domain Controller Options screen, select the **Forest functional level** and **Domain functional level** to meet your network's requirements. You will notice the Domain Controller will include DNS Server capability by default. Specify the **Directory Services Restore Mode (DSRM)** password and click **Next**.



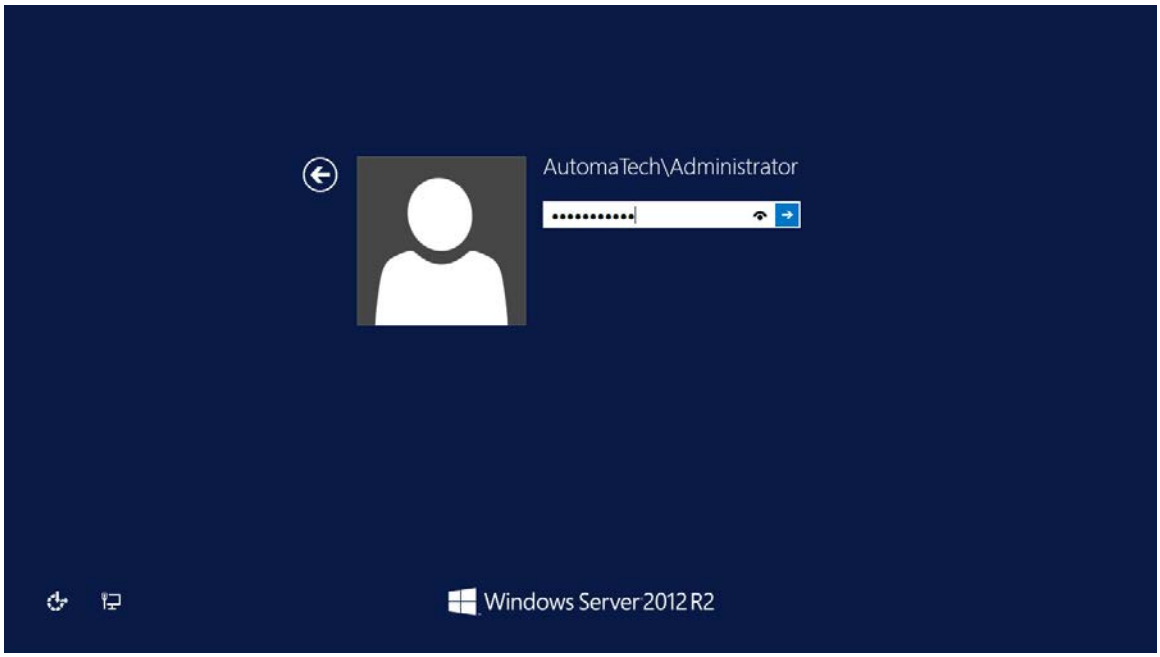
STEP 11: Click **Next** to accept the default DNS Options. Confirm and update the **NetBIOS domain name** if necessary and click **Next.**



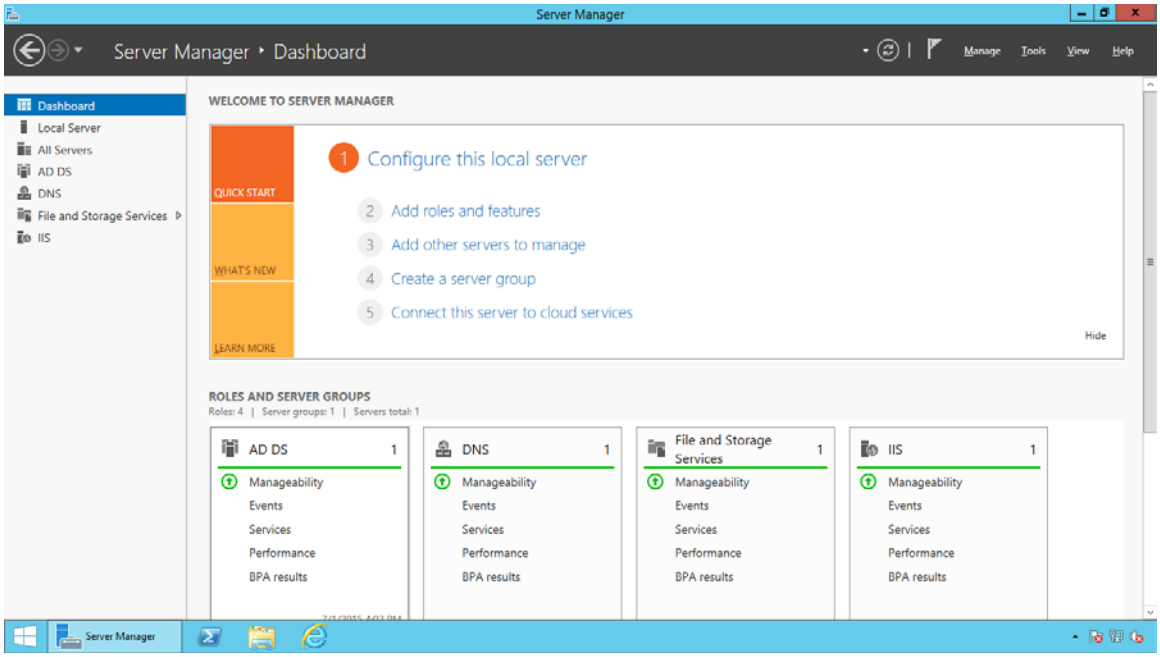
STEP 12: Click **Next** on the Paths screen to accept the default Paths and the Review Options screen will be displayed. Click **Next** to perform a Prerequisites Check. If all the rules checks pass you will see a note and green check mark that all prerequisite checks passed successfully. Click **Install** to complete the Domain Controller Promotion process.



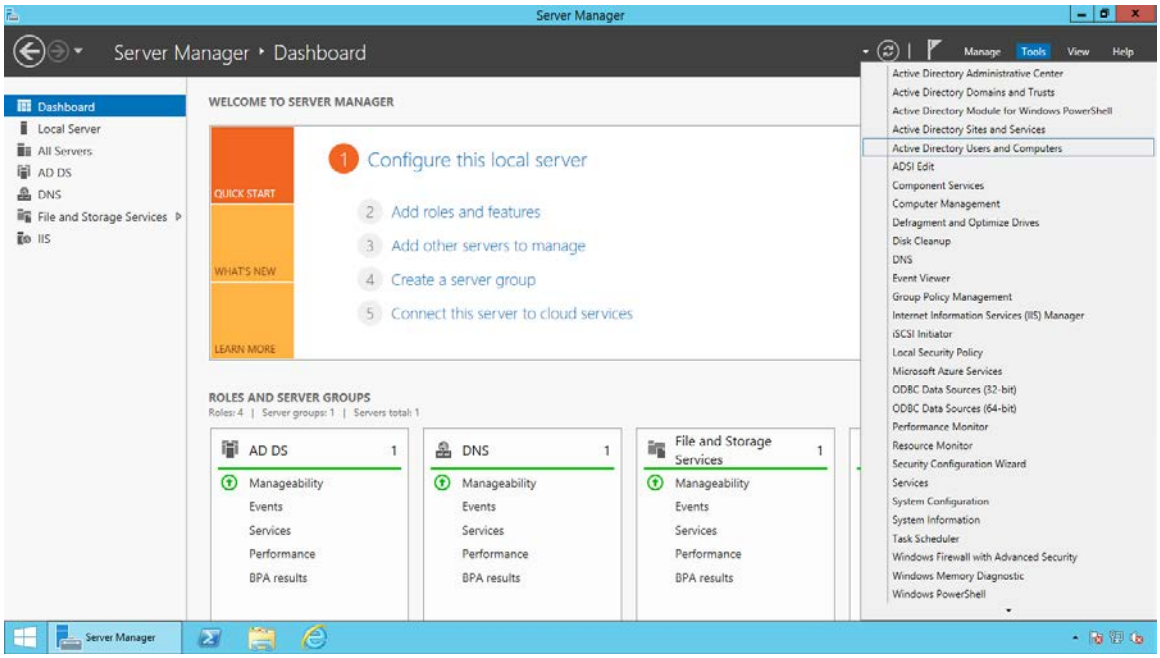
STEP 13: The Server will automatically restart when applying changes. Upon restart, notice you will now need to login as the Domain account including the Domain prefix.



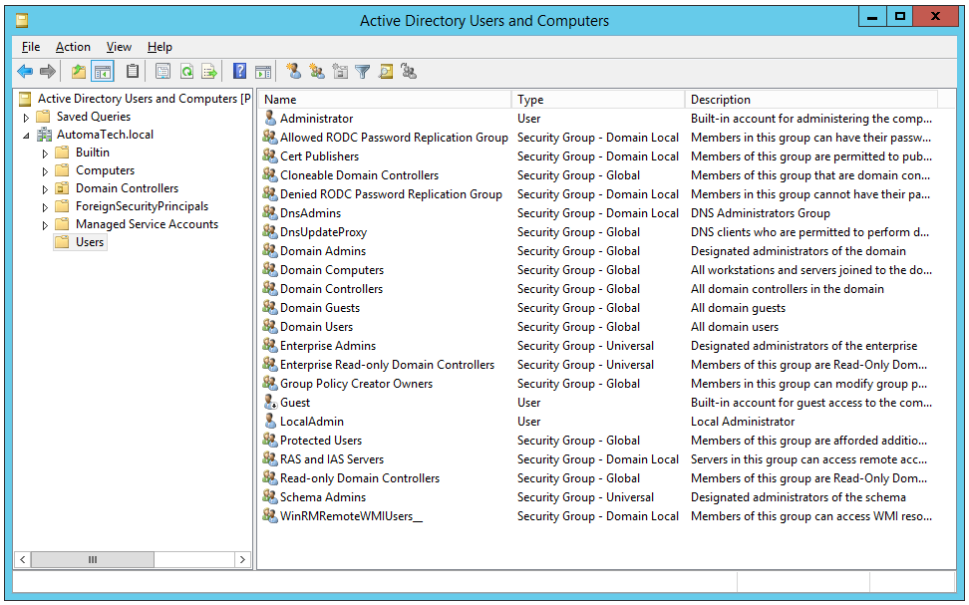
STEP 14: After logging in to the Domain, return to the Server Manager. The new AD DS Role has been added to the Server Manager Dashboard. You can click the link or status card for additional details about the Server Role.



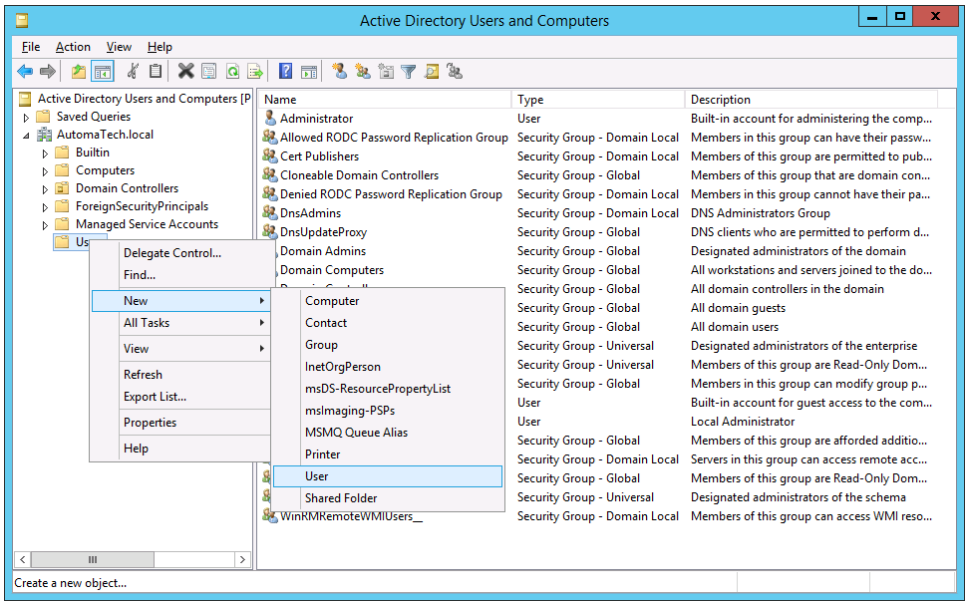
STEP 15: Click the **Tools** link at the top of the Server Manager and observe the newly added tools. Click the **Active Directory Users and Computers** link to launch the management console.



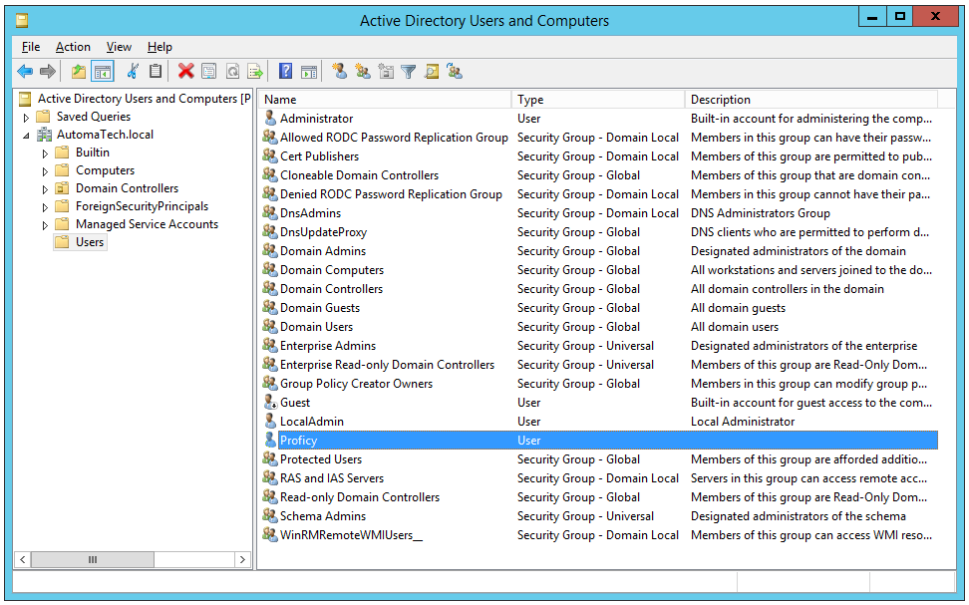
STEP 16: Expand the **Domain** name and the **Users** folder to view a list of configured Users, Groups, and other resources. This is where you would configure various permissions and functions of each resource in the Domain. For the purposes of this example a single Domain User will be added.



STEP 17: Right-click the **Users** folder, select **New**, and select **User** to create a new User. Complete the next three screens with the User details and credentials and click **Finish** to create the User.



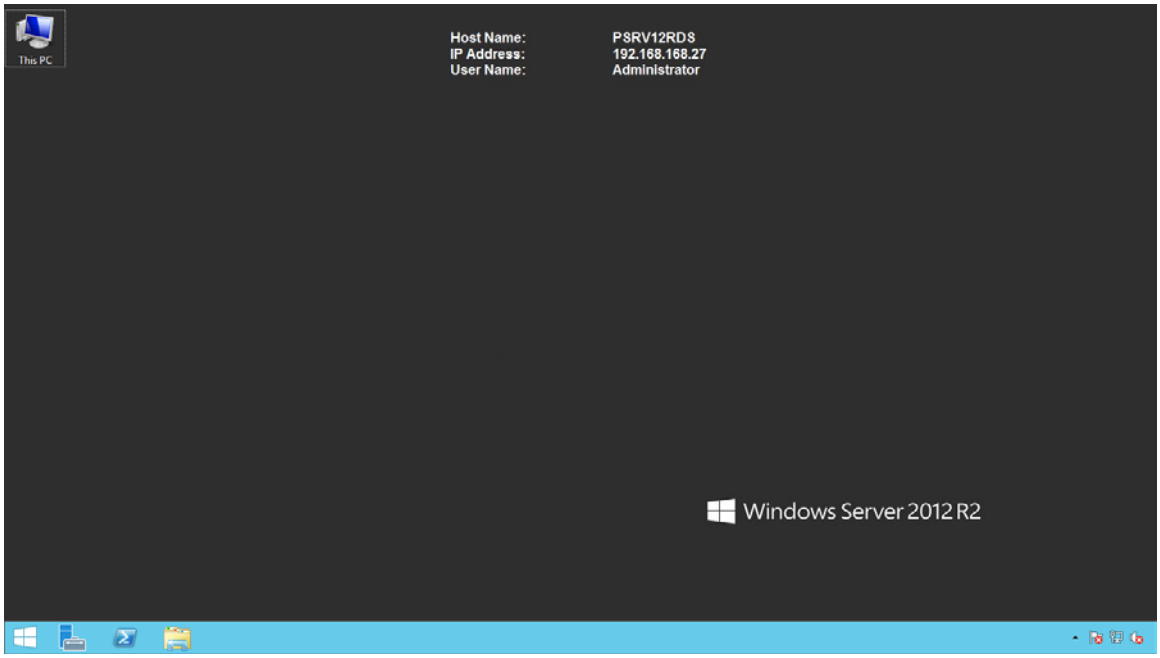
STEP 18: In this example the Domain User 'Proficy' has been created and will be used to access the Remote Desktop Server in later steps. By default all Domain Users will be given Remote Desktop Server access, so at this point you could further define your security groups and roles if desired. These steps have completed the Domain Server configuration required at this time.



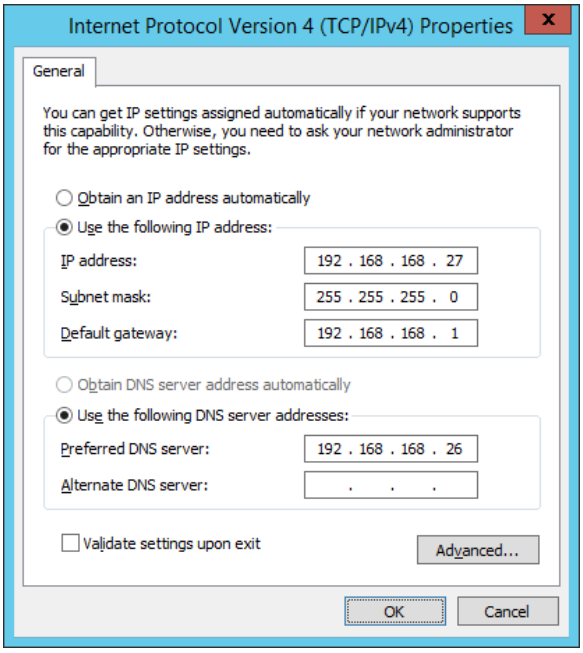
2. Installing, Configuring, and Licensing Remote Desktop Services (RDS) on a Remote Desktop Server computer running Windows Server 2012 R2

Now that the Domain Controller Server setup has completed you will need to configure the Remote Desktop Server. The Remote Desktop Server will need to be joined to the Domain created in the previous section, have the necessary Roles enabled, and setup with the appropriate licensing.

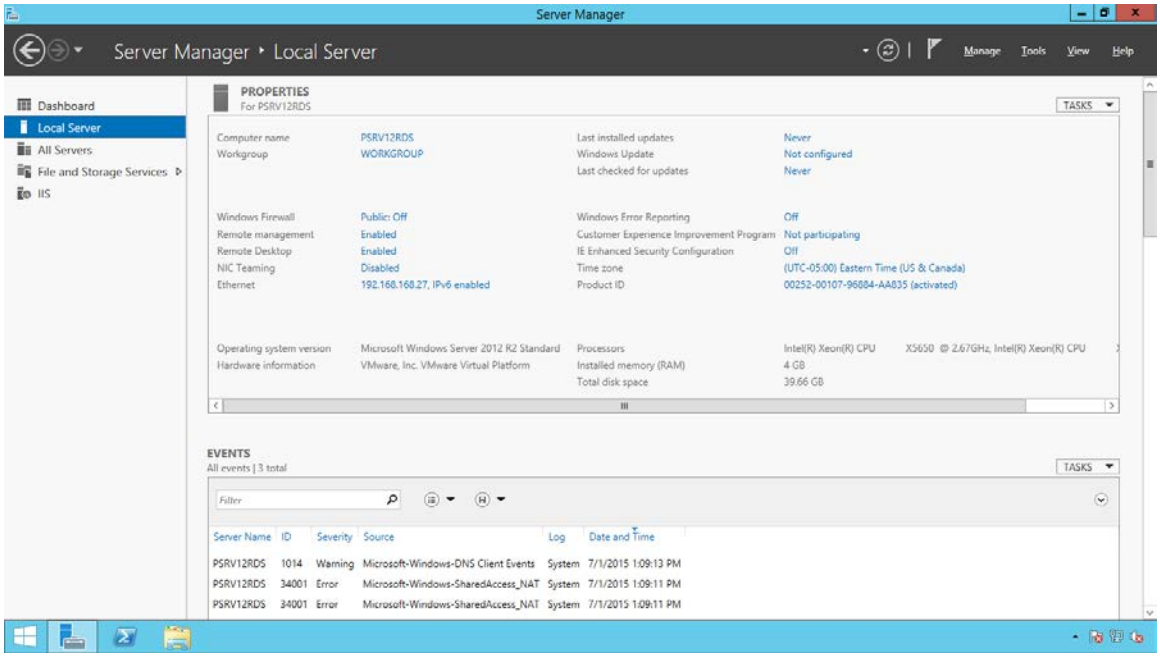
STEP 1: Login to your Remote Desktop Server computer as the local Administrator, as pictured below.



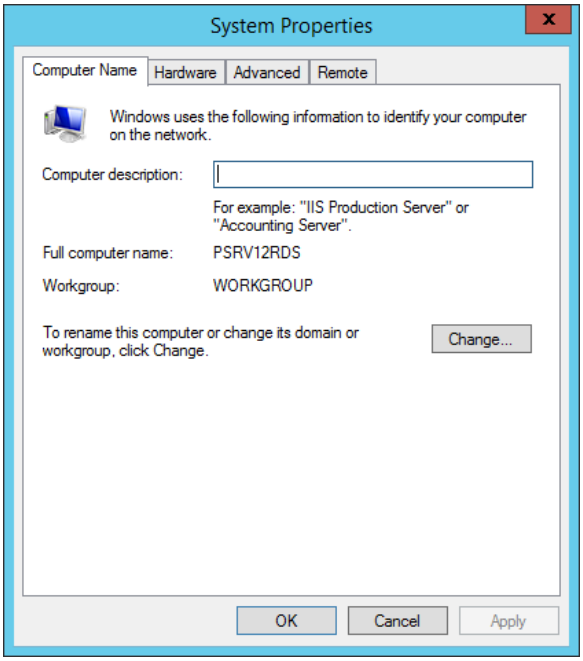
STEP 2: Verify that you have the appropriate network settings configured and that the Domain Controller Server's IP address is configured for the **Preferred DNS server**, as pictured below.



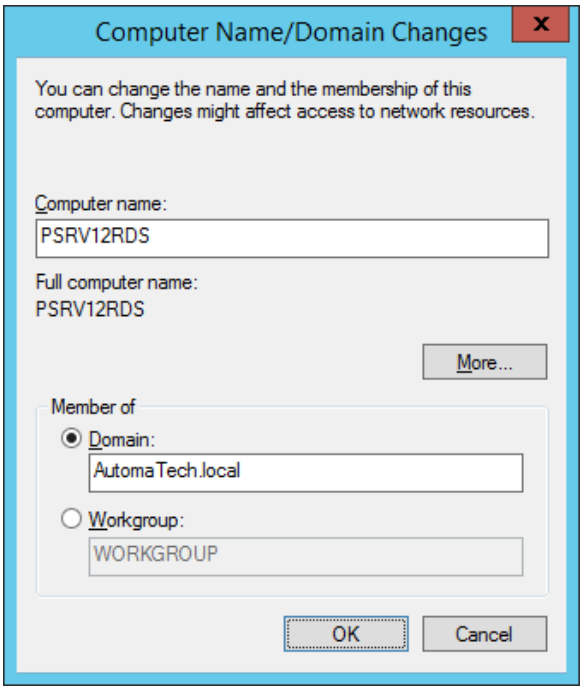
STEP 3: You will now need to join the Remote Desktop Server to the Windows Domain created in the previous steps. Launch the **Server Manager** application from the Taskbar and click the **Local Server** link on the left side to view a snapshot of the Local Server configuration.



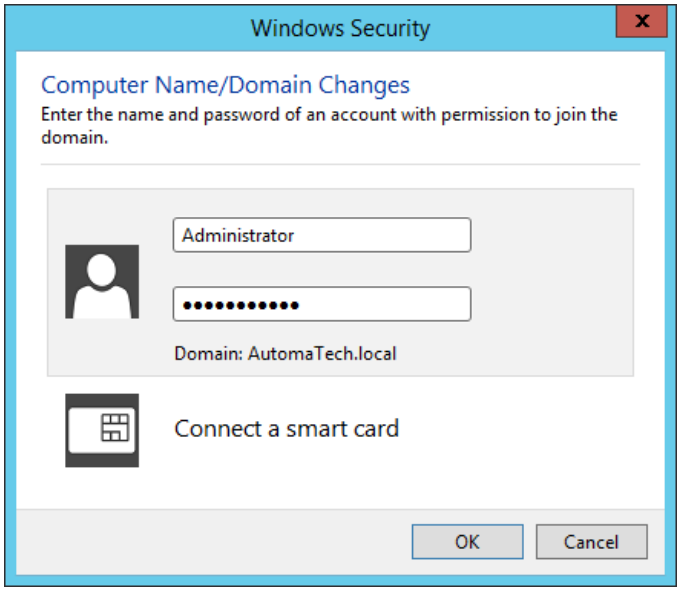
STEP 4: Click the **Computer name** or **Workgroup** link to open the System Properties window.



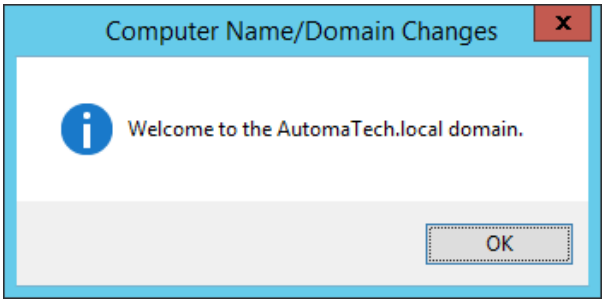
STEP 5: Click the **Change** button to launch the Computer Name/Domain Changes window. Enter the **Domain Name** that was created in the previous section.

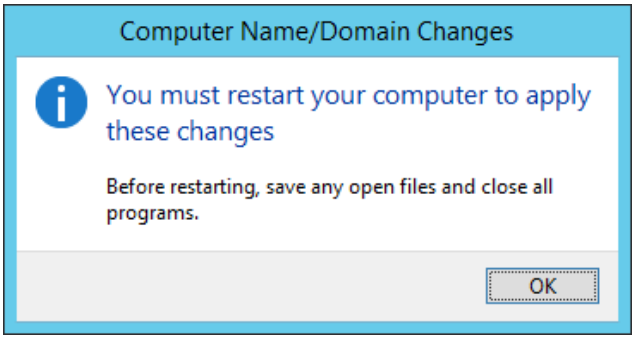


STEP 6: Click **OK** and you will be prompted with the Windows Security window, enter the Username and Password for your **Domain Administrator** account, as pictured below.

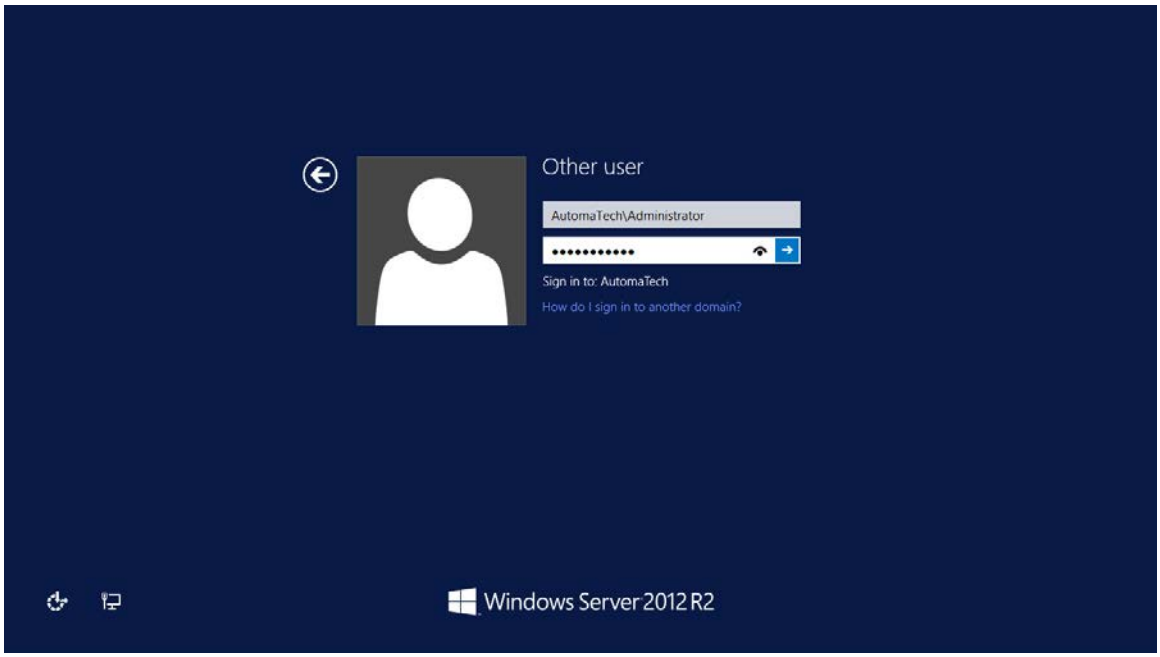


STEP 7: Click **OK** to authorize the addition of the computer to the Domain, you will be prompted with a welcome message, as pictured below. Click **OK** and click **OK** again when prompted that you must restart your computer to apply these changes and then **restart the computer.**

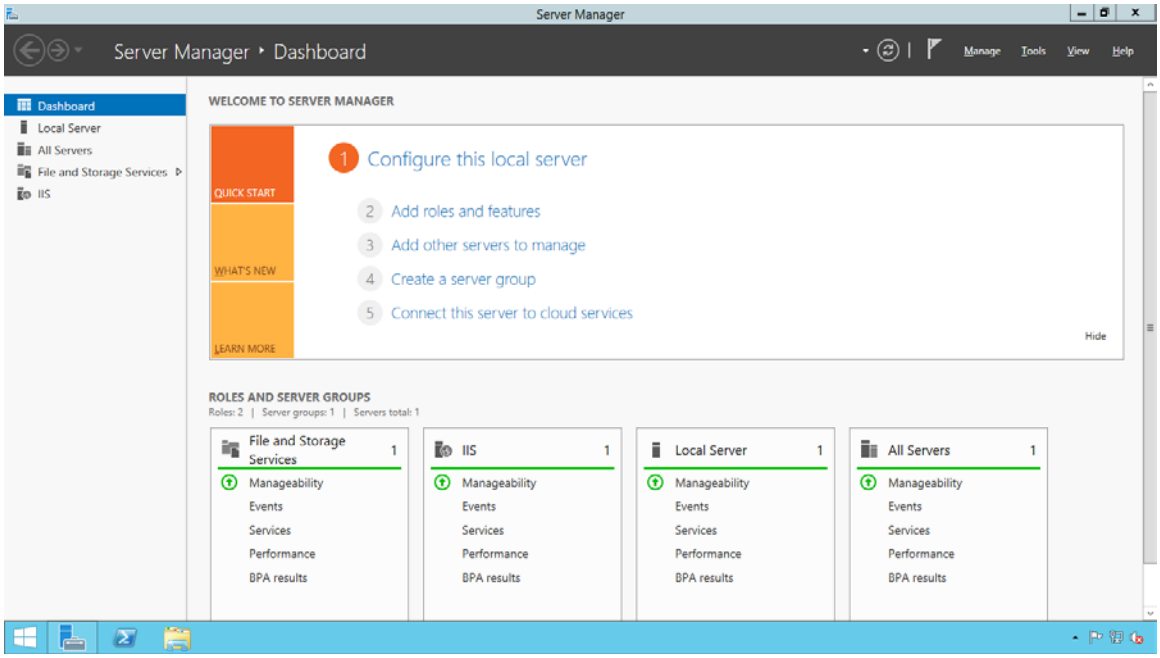




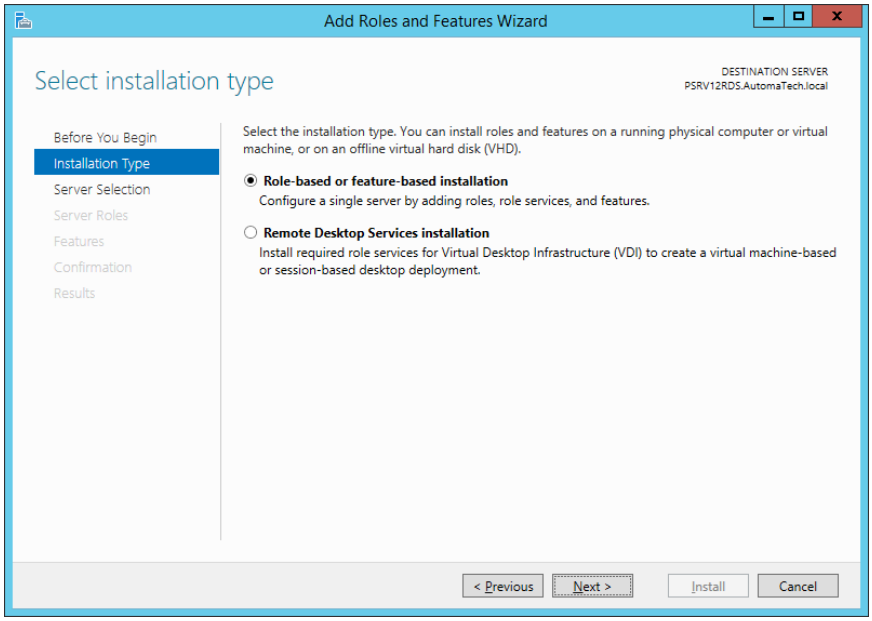
STEP 8: After the computer has restarted, you will need to login as the Domain User and not the Local User. Click the **Other User** link on the Windows Login screen. Specify your Administrator credentials including the new Domain Name prefix to login to the server, as pictured below.



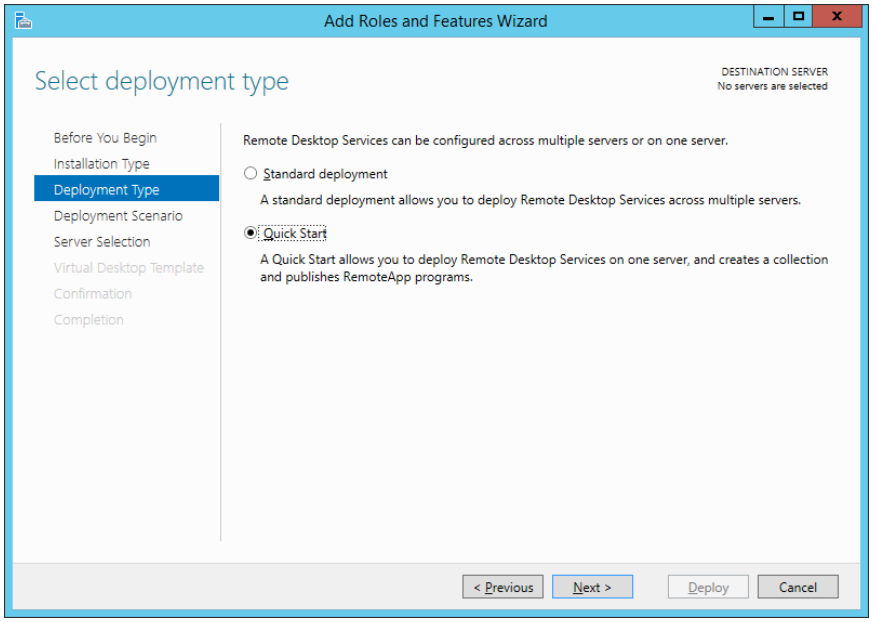
STEP 9: You will now be ready to add the Remote Desktop Services role. Launch the **Server Manager** by clicking the icon pinned to the Task Bar. After a few moments the Dashboard will refresh with a complete list of installed Roles.



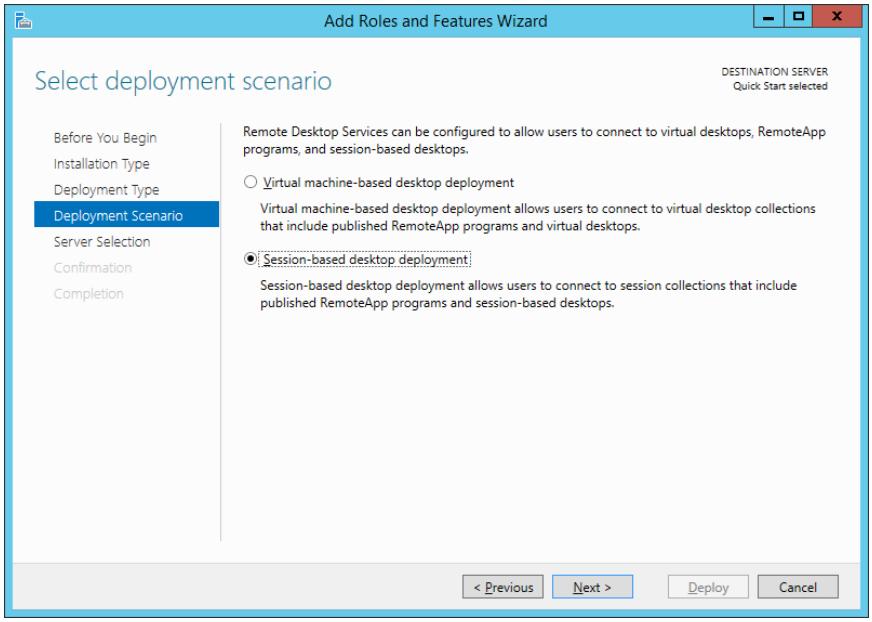
STEP 10: Click the **Add roles and features** link to launch the Add Roles and Features Wizard. Select the Installation Type as **Remote Desktop Services Installation** and click **Next.**



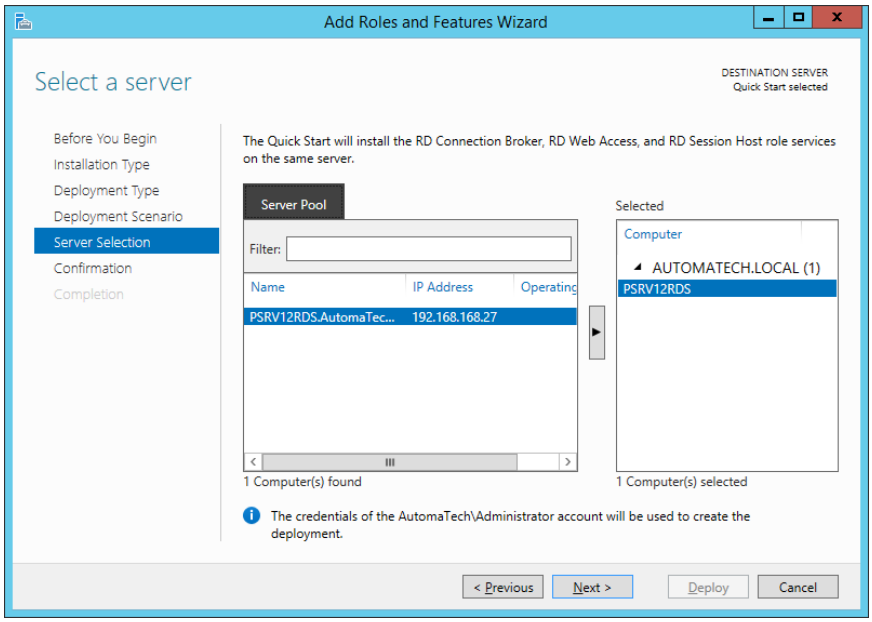
STEP 11: Select the **Quick Start** option for a typical deployment on a single Remote Desktop Server. If you plan to create a distributed deployment you would choose the Standard deployment option and configure some additional options. Click **Next** to continue.



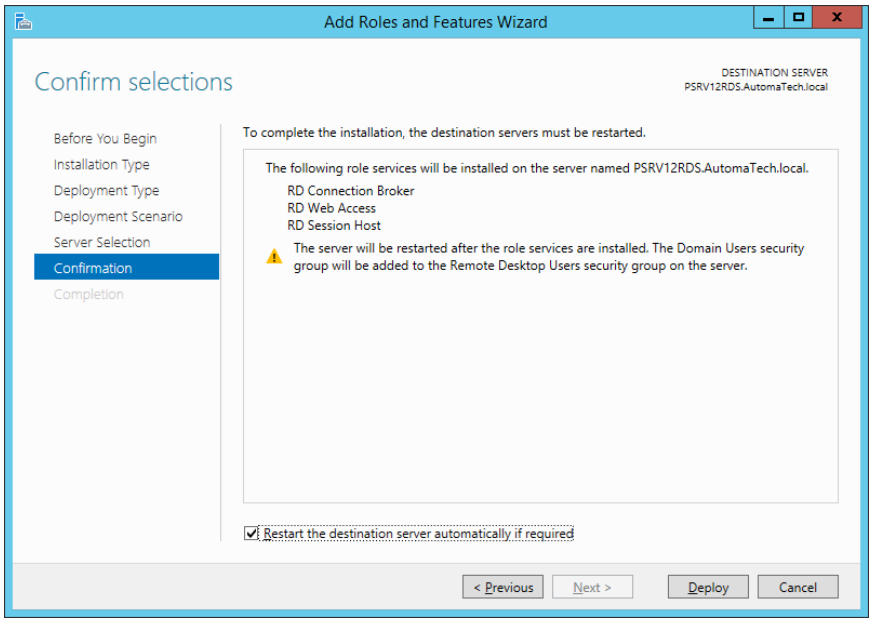
STEP 12: Choose the **Session-based desktop deployment** option on the Deployment Scenario screen and click **Next.**



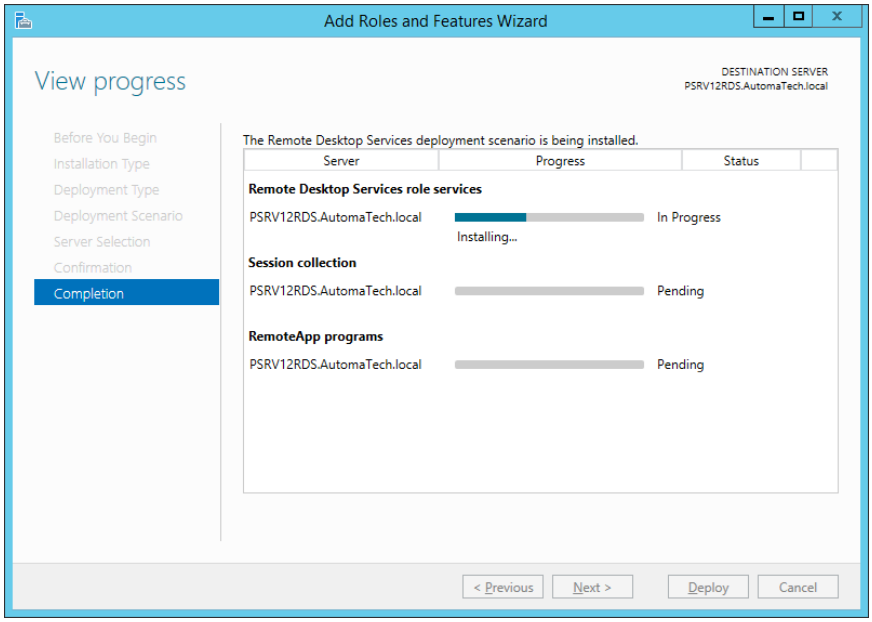
STEP 13: You will be prompted that the Quick Start will install the RD Connection Broker, RD Web Access, and RD Session Host services on the same server. Select your local server from the Server Pool and click **Next.**



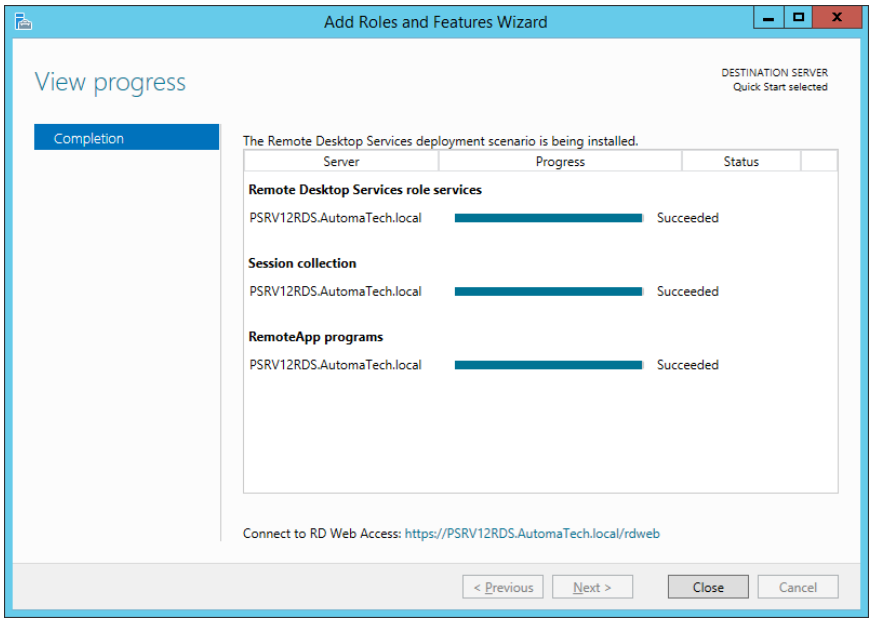
STEP 14: The Confirmation screen will perform a rules check and notify you that the server must be restarted to complete the installation. Check the **Restart the destination server automatically if required** check box and click the **Deploy** button.



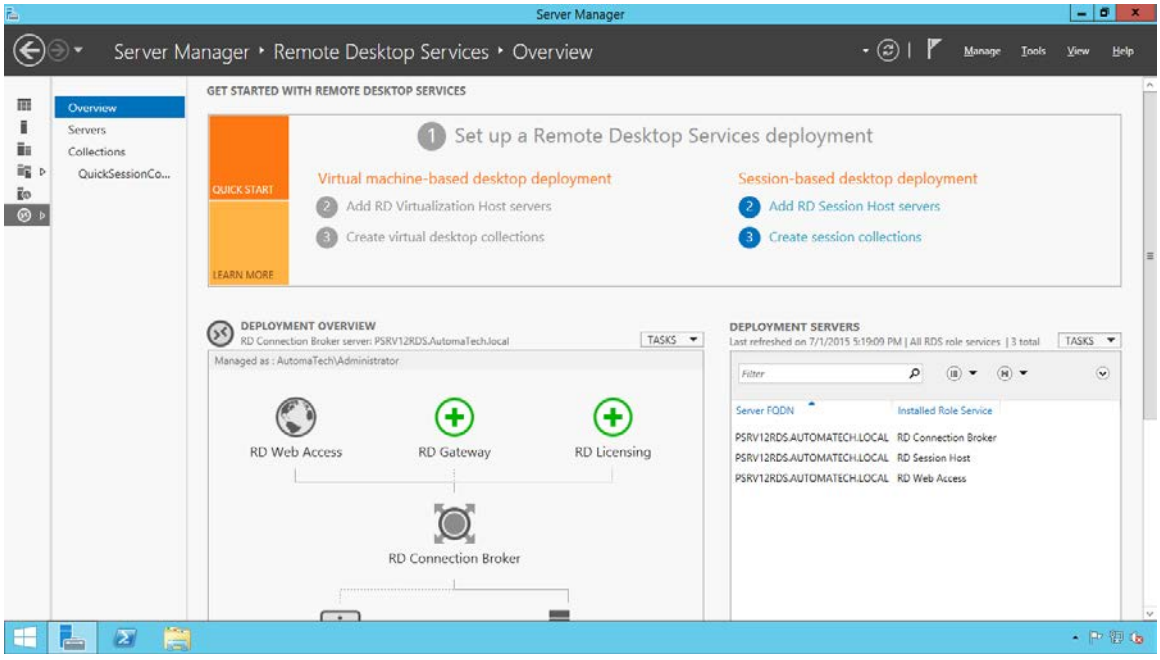
STEP 15: The installation process will begin and display the progress, as pictured below. When the initial role services installation is complete the server will restart automatically.



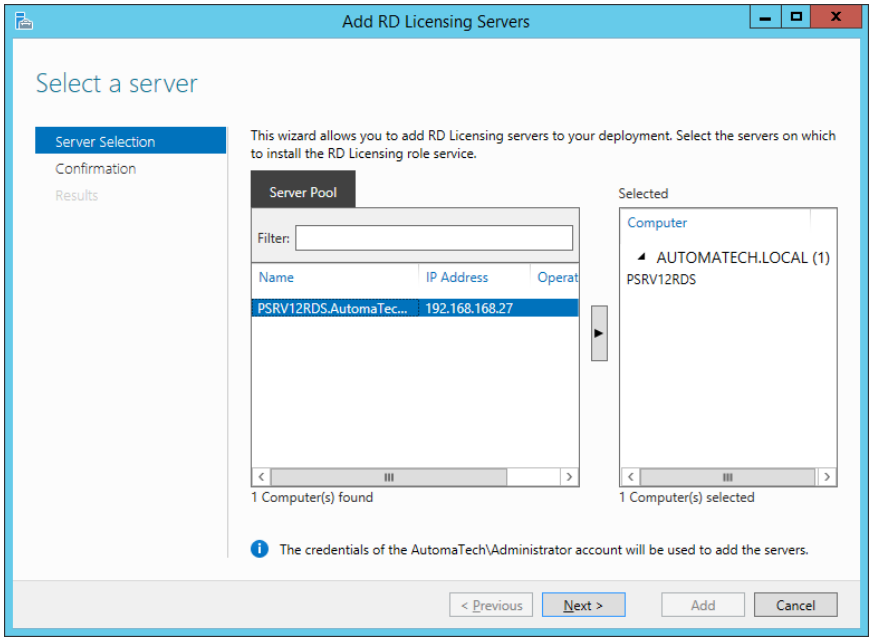
STEP 16: After the server restarts, login again as the Domain Administrator and return to the **Server Manager**. You will see the installation progress continue. Upon completion, click the **Close** button to acknowledge that the installation succeeded.



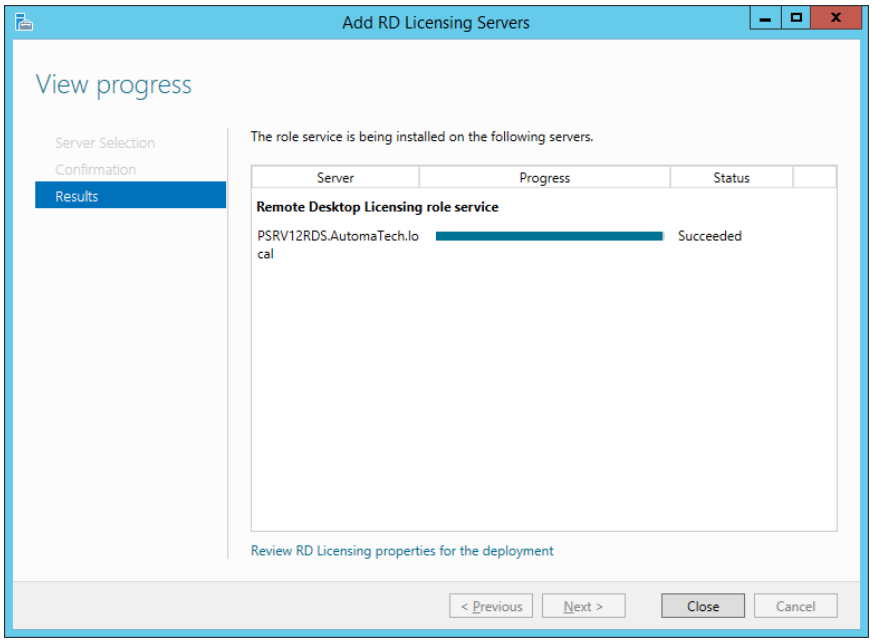
STEP 17: Click on the new **Remote Desktop Services** Role available in the Server Manager Dashboard. You will see the Remote Desktop Services deployment overview screen.



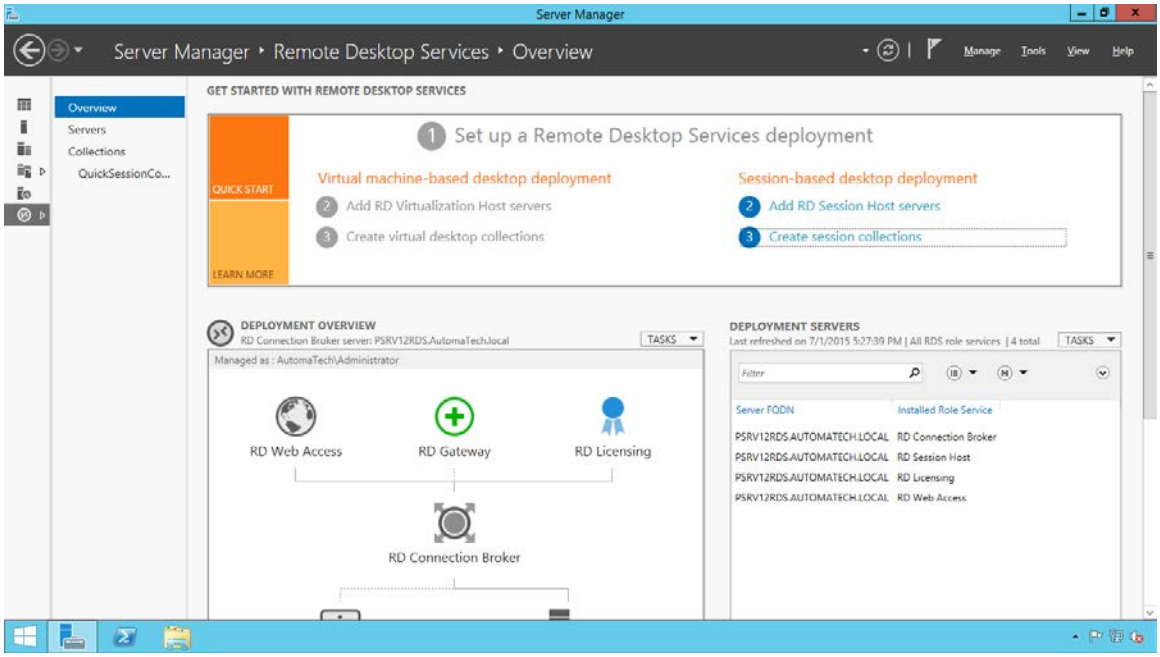
STEP 18: You need to enable Licensing in order for Users to access the Server. Click the green **RD Licensing plus sign** to launch the Add RD Licensing Servers window. Select the Local Server from the Server Pool.



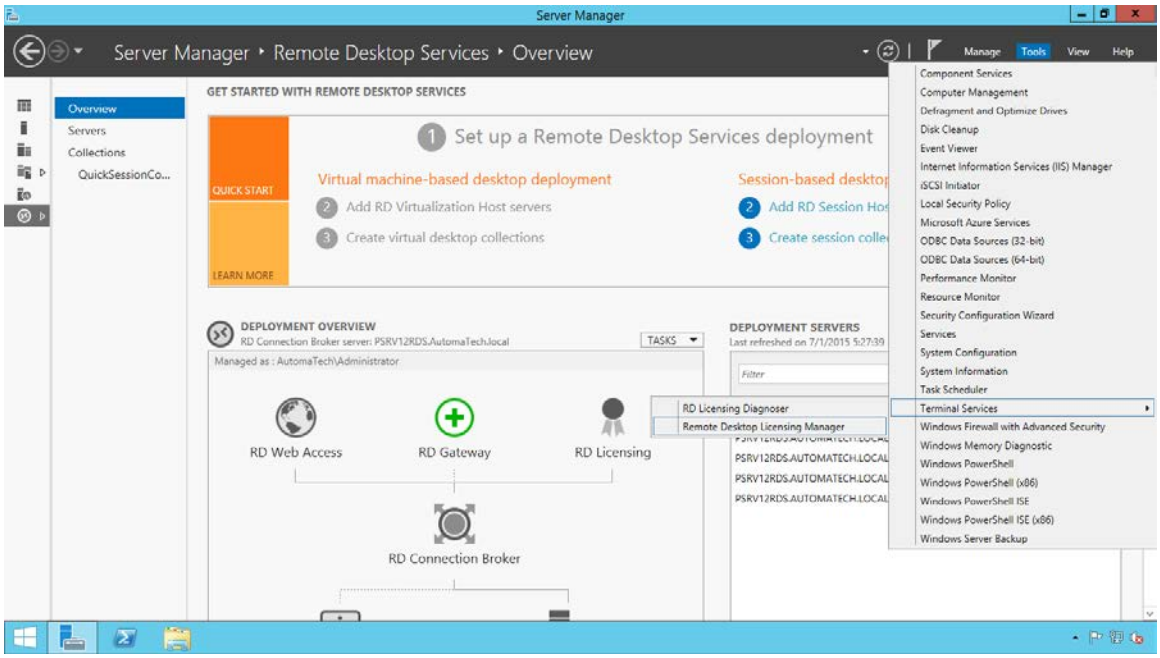
STEP 19: Click **Next** and you will be prompted with a confirmation that The RD Licensing role service will be installed on the servers and added to the deployment. Click the **Add** button and you will be notified when the Remote Desktop Licensing role service installation succeeded, as pictured below.



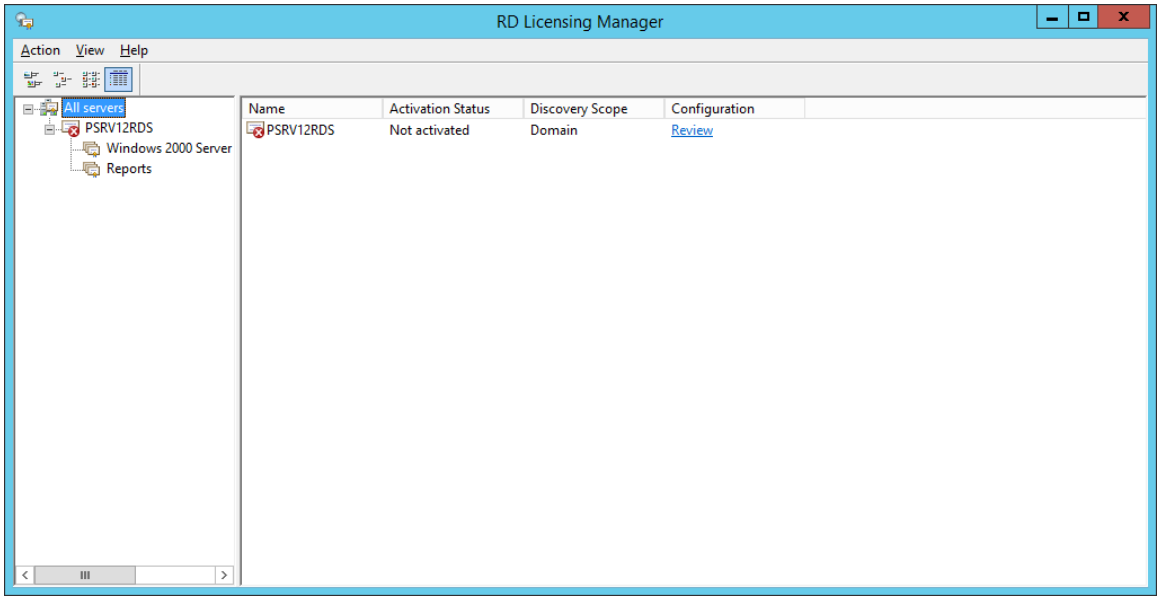
STEP 20: Click **Close** to complete the installation. You will now see the blue ribbon badge indicating the RD Licensing has been installed, as pictured below.



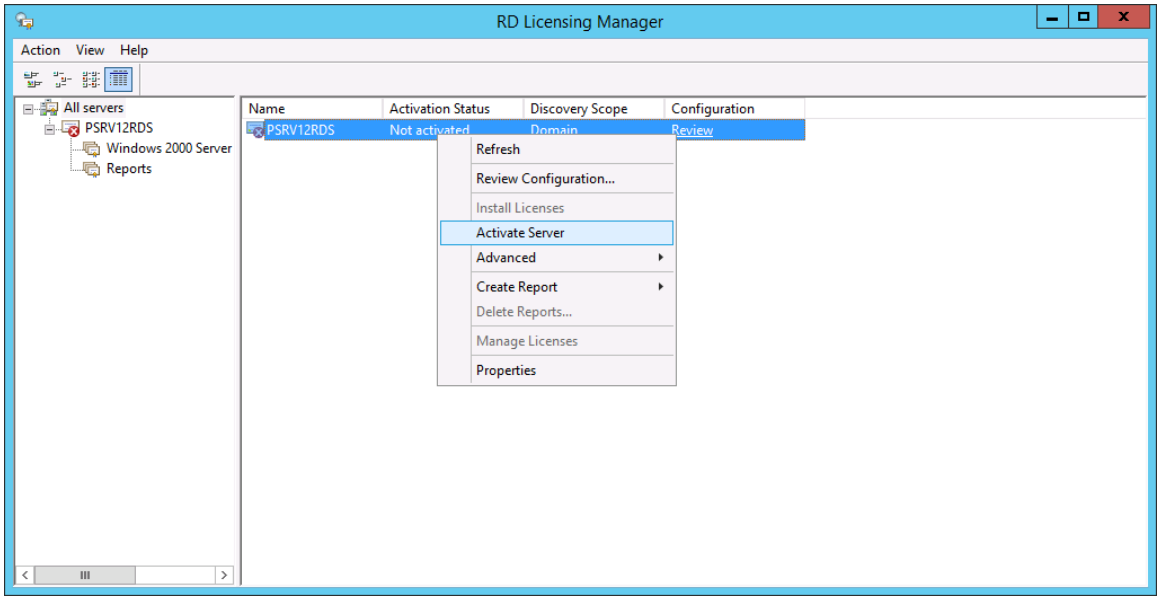
STEP 21: Click the **Tools** link at the top of the Server Manager and observe the newly added tools for Terminal Services. Click the **Remote Desktop Licensing Manager** link to launch the management console.



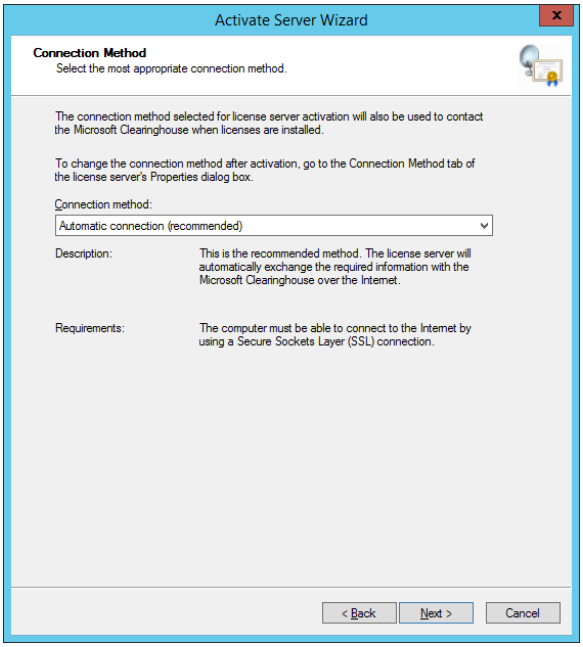
STEP 22: Expand the view, you will notice the RD Licensing Manager indicates that the server is not yet activated.



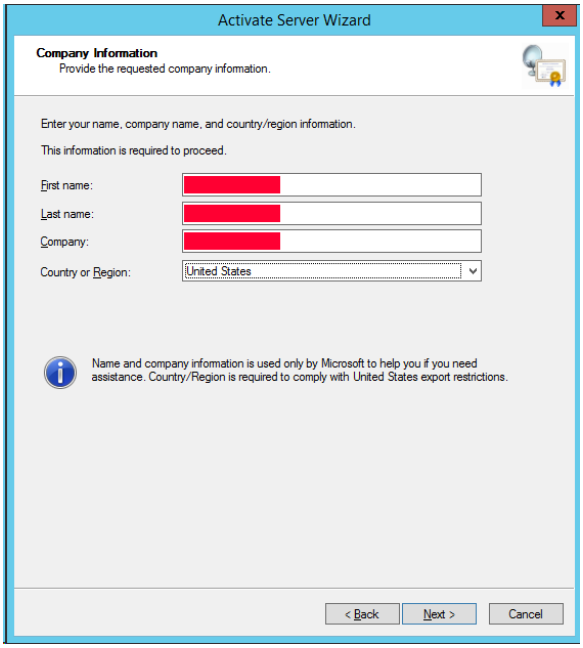
STEP 23: Right-click on the Local Server and select **Activate Server** to launch the Activate Server Wizard and click **Next** on the Welcome screen to start the activation process.



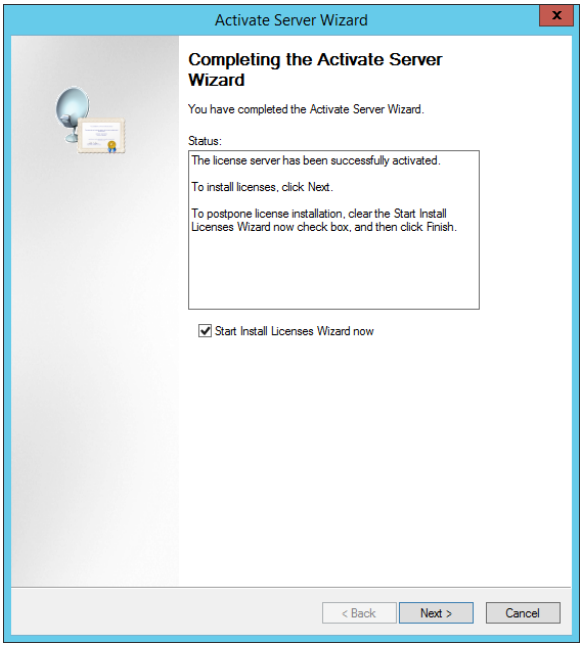
STEP 24: Select the appropriate Connection Method from the list and click **Next**. Licensing can be activated automatically through your Internet connection, through a web browser, or over the phone.



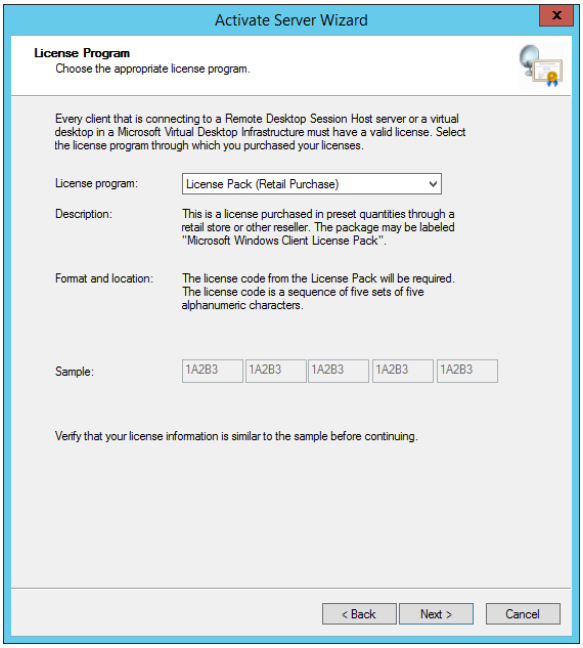
STEP 25: Complete the **Company Information** fields with the information that corresponds with to your Remote Desktop Licenses and click **Next.**



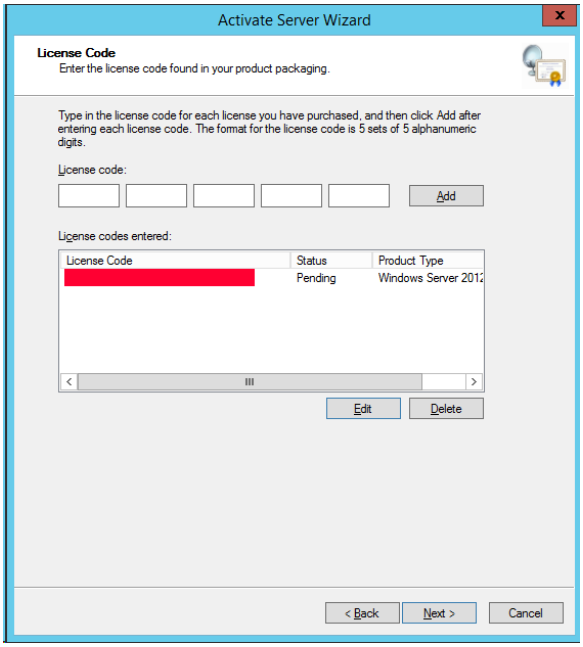
STEP 26: You will be prompted that the license server has been successfully activated. Obtain your Remote Desktop Server Client Access License (CAL) keys and click **Next** to start the Install Licenses Wizard.



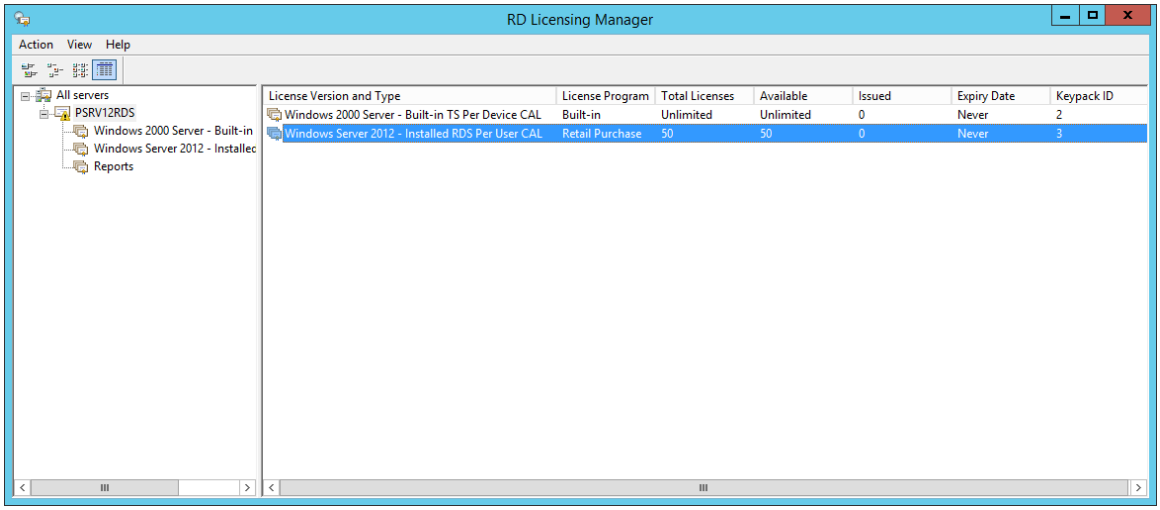
STEP 27: Select the appropriate License program for your licenses and click **Next.**



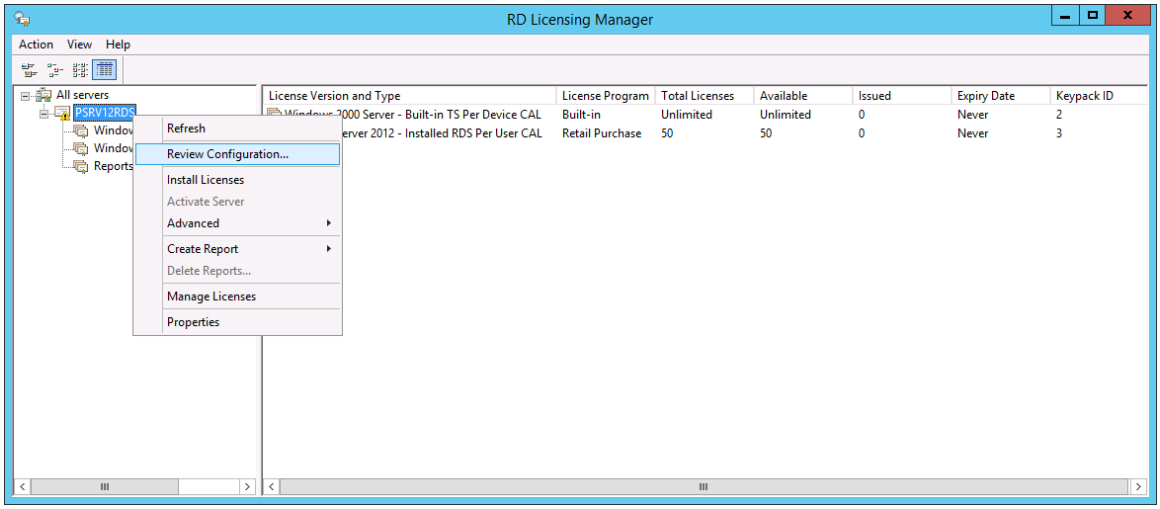
STEP 28: Type in or Paste your license code(s) per your Microsoft Licensing Agreement and click **Next.** You will be notified that the licenses have been successfully activated, click **Finish** to close the activation wizard



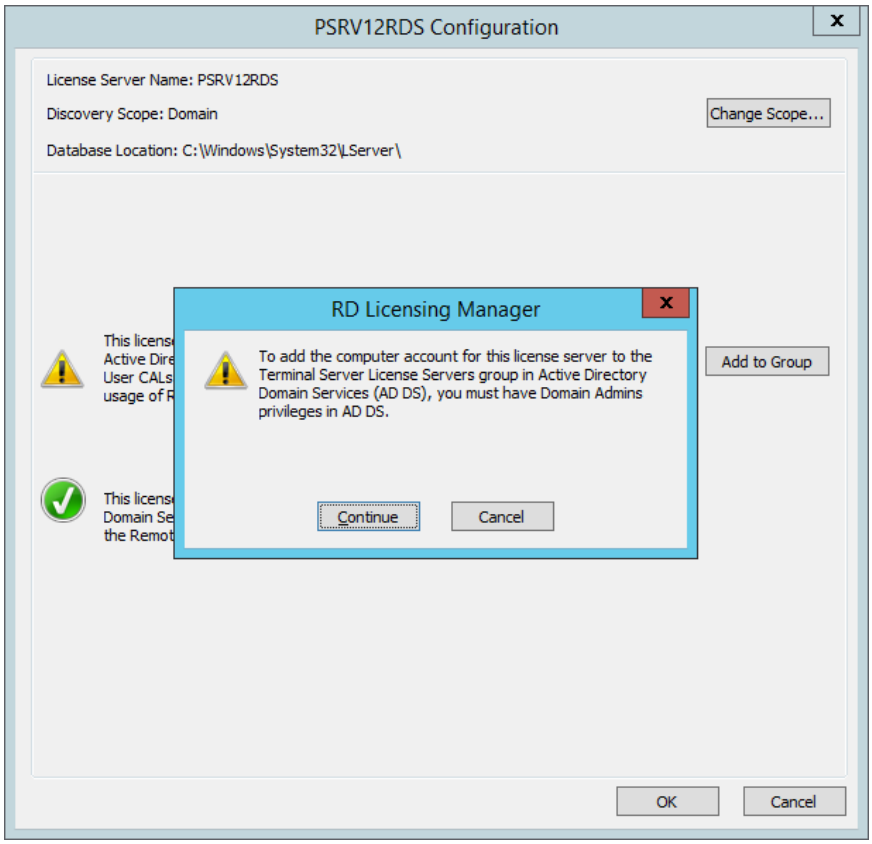
STEP 29: You will now see a summary of the Client Access License versions, types, and quantities in the RD Licensing Manager window. This server has been activated with 50 Per User RDS CALs, as pictured below.

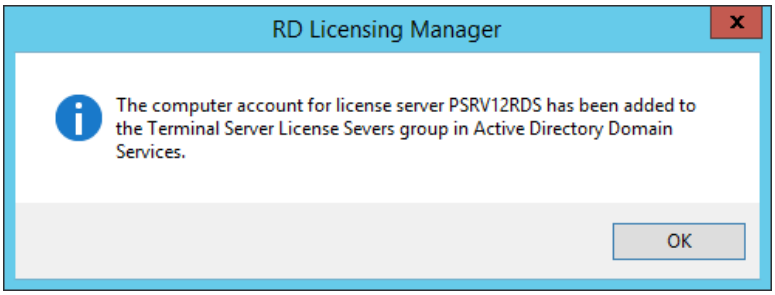


STEP 30: Right-click the server name and select the **Review Configuration** option to open the Server Configuration window.

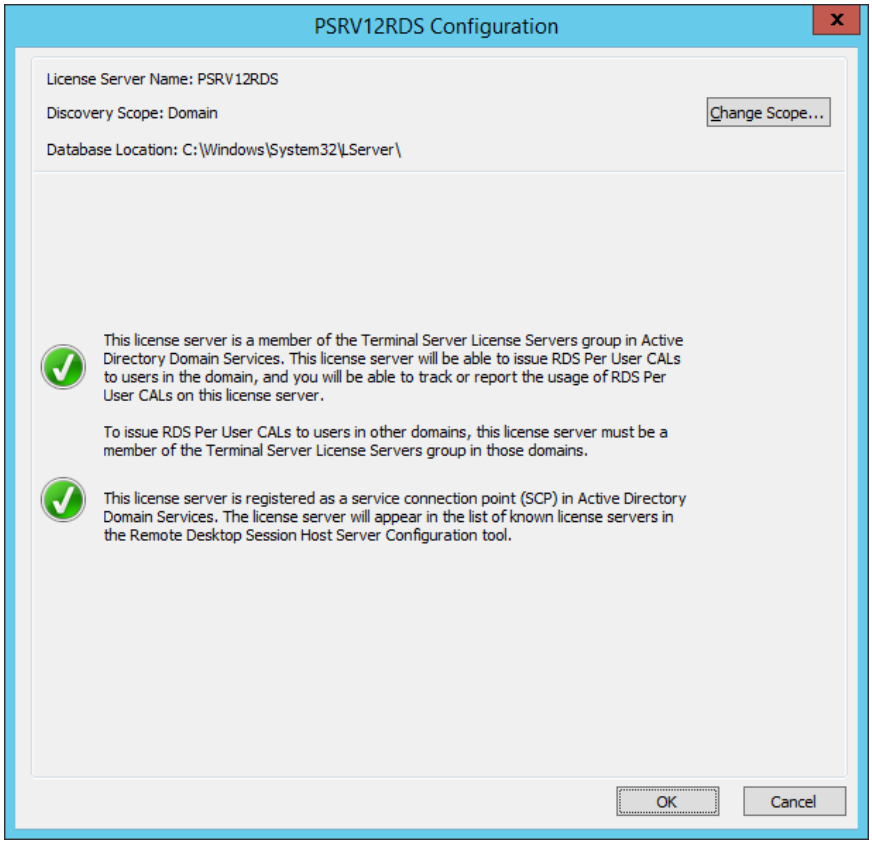


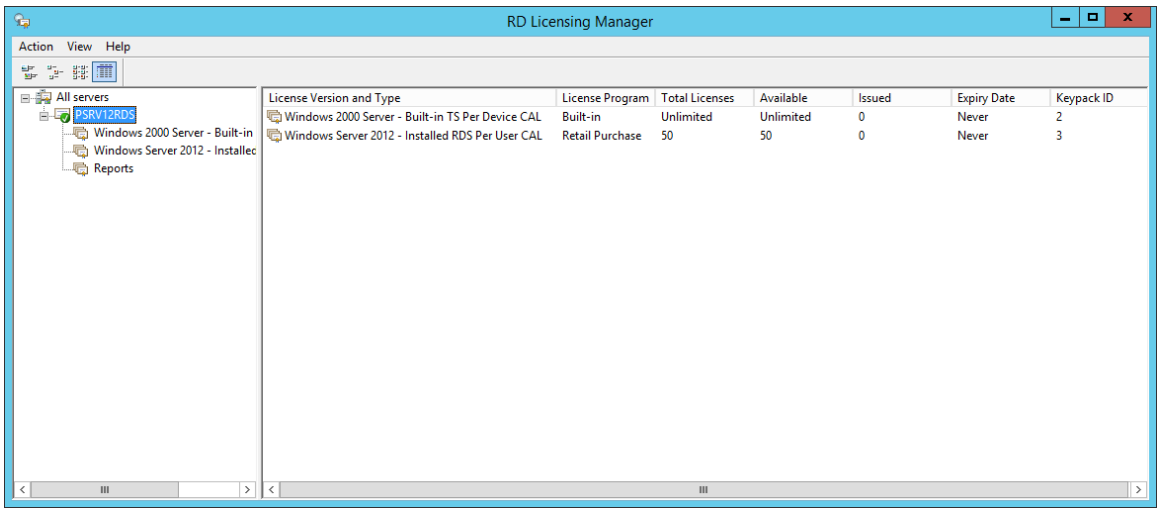
STEP 31: Click the **Add to Group** button and you will be prompted to add the License Server to the Active Directory Domain Services Group. Click **Continue** to authorize the change on the Active Directory Server. When prompted that the License Server has been added to the License Servers group in Active Directory Domain Services, click **OK.**



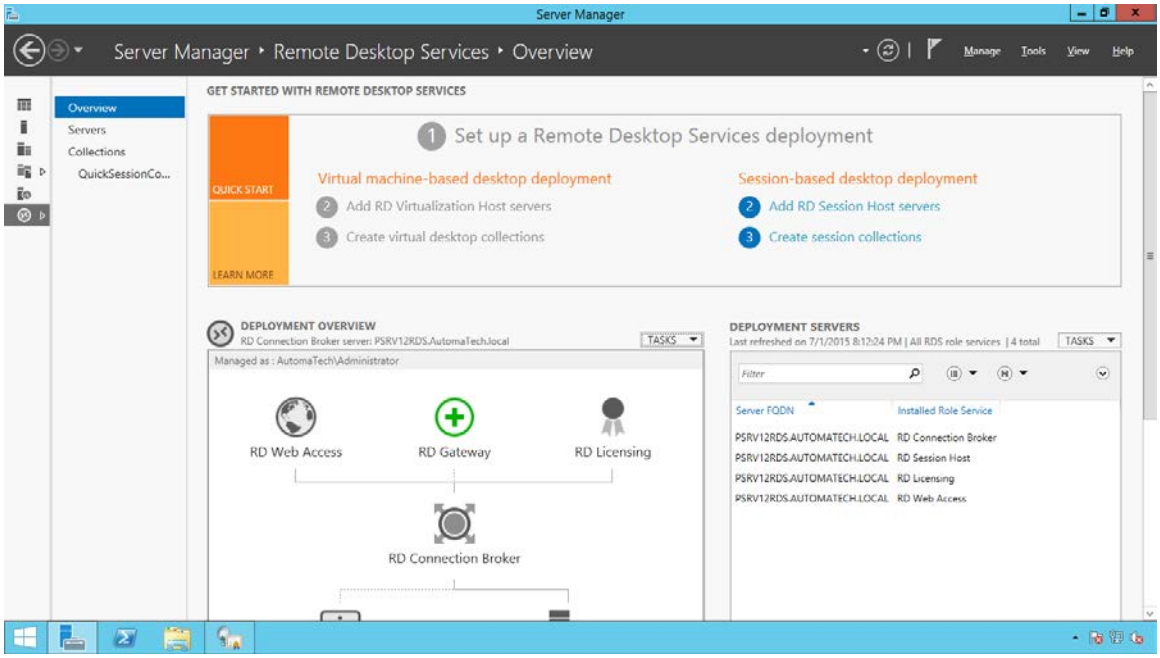


STEP 32: You will now see the completed Server Configuration and have two green check marks confirming the licensing and activation process, click **OK** to accept the changes.

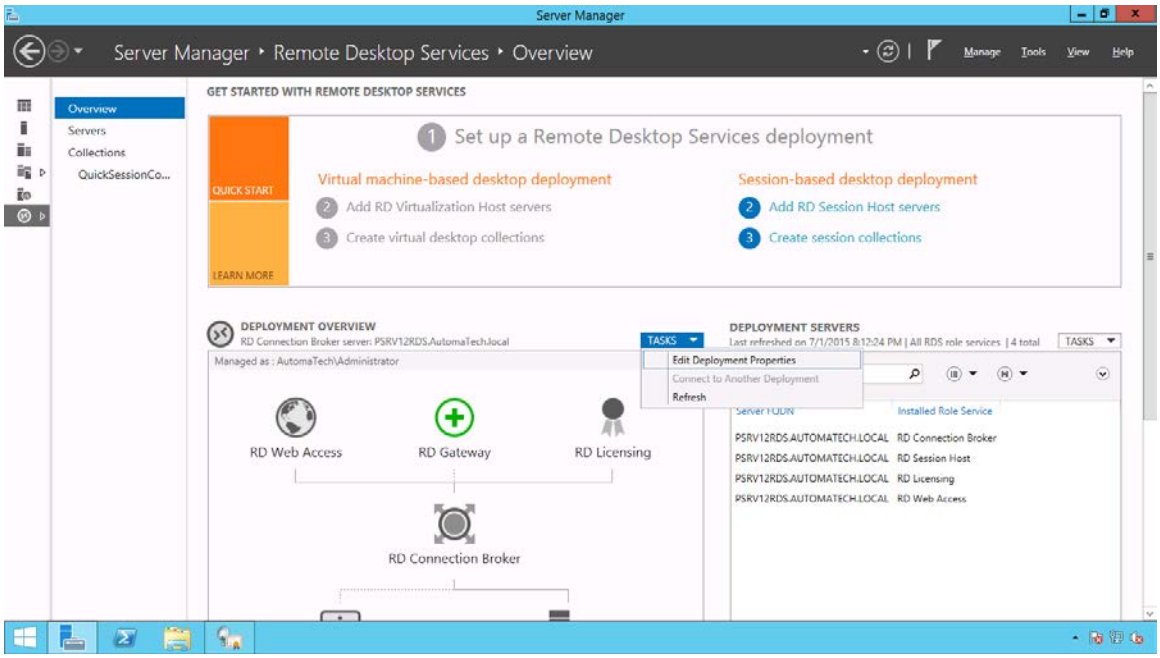




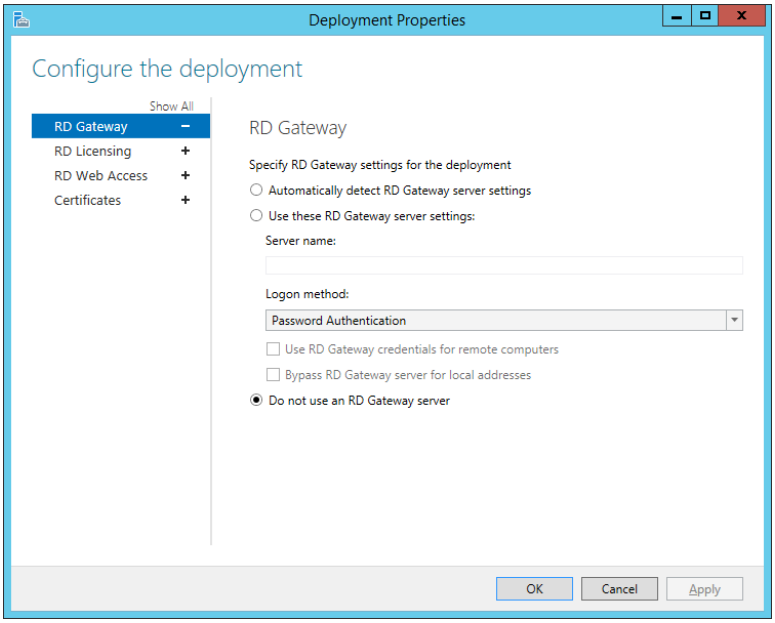
STEP 33: Return to the **Server Manager** and expand the **Remote Desktop Services Overview** screen.



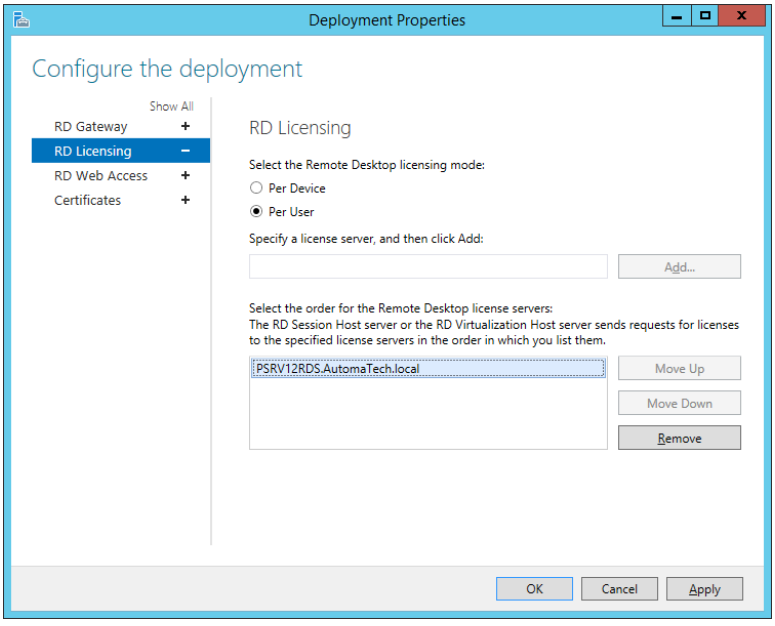
STEP 34: Click the **Tasks** drop down button and select the **Edit Deployment Properties** option.



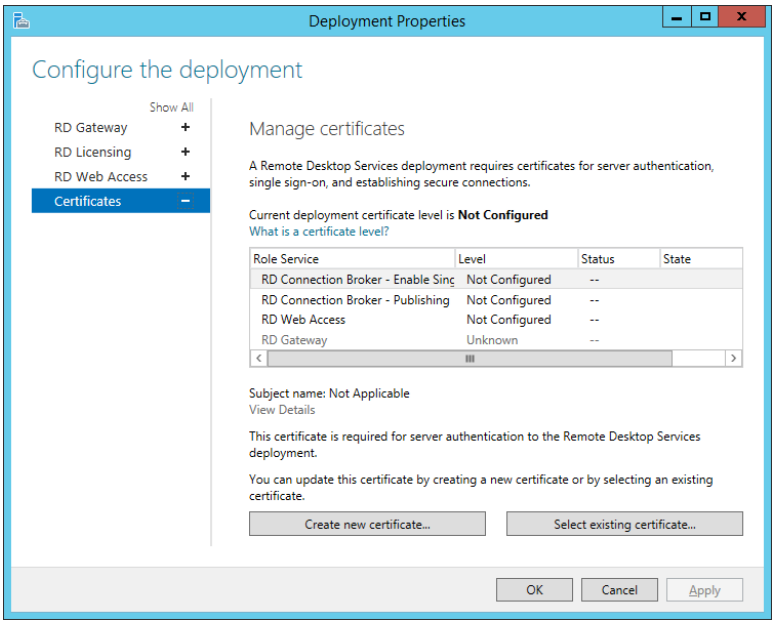
STEP 35: The Deployment Properties window will appear. If an RD Gateway is required in your deployment, you would configure it on this screen.



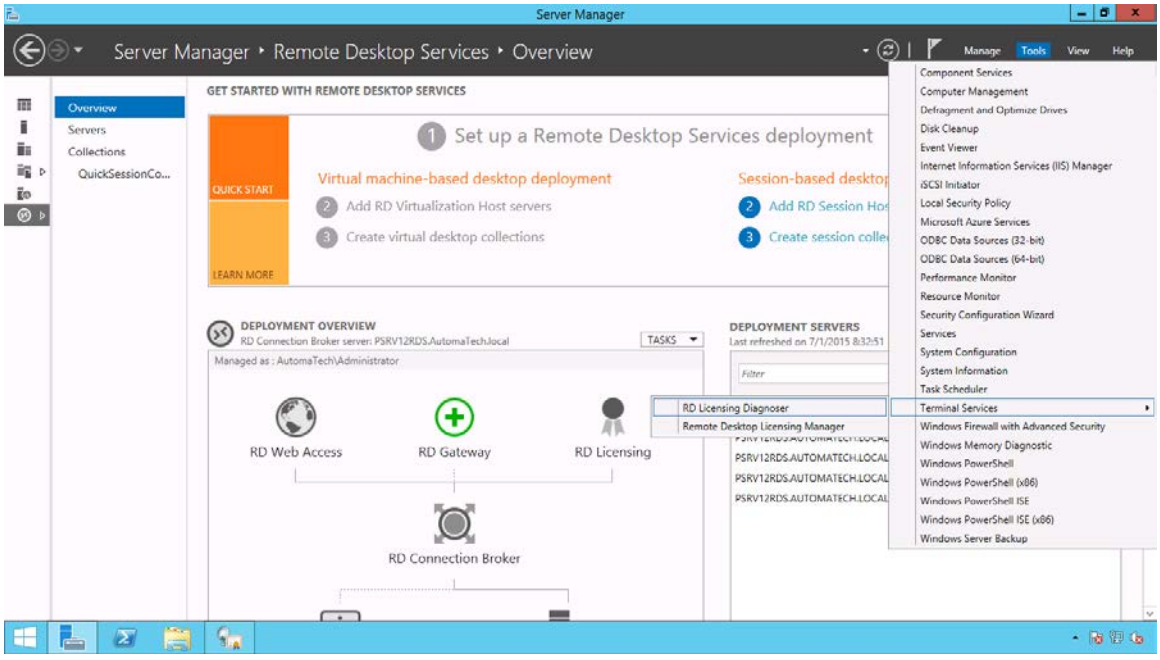
STEP 36: Click the **RD Licensing** section and select **Per Device** or **Per User** under the Remote Desktop licensing mode options that is relevant to your Microsoft licensing agreement. This server uses User CALs, so we will select the **Per User** mode, as pictured below. Click **Apply** to accept the changes for the RD Licensing mode.



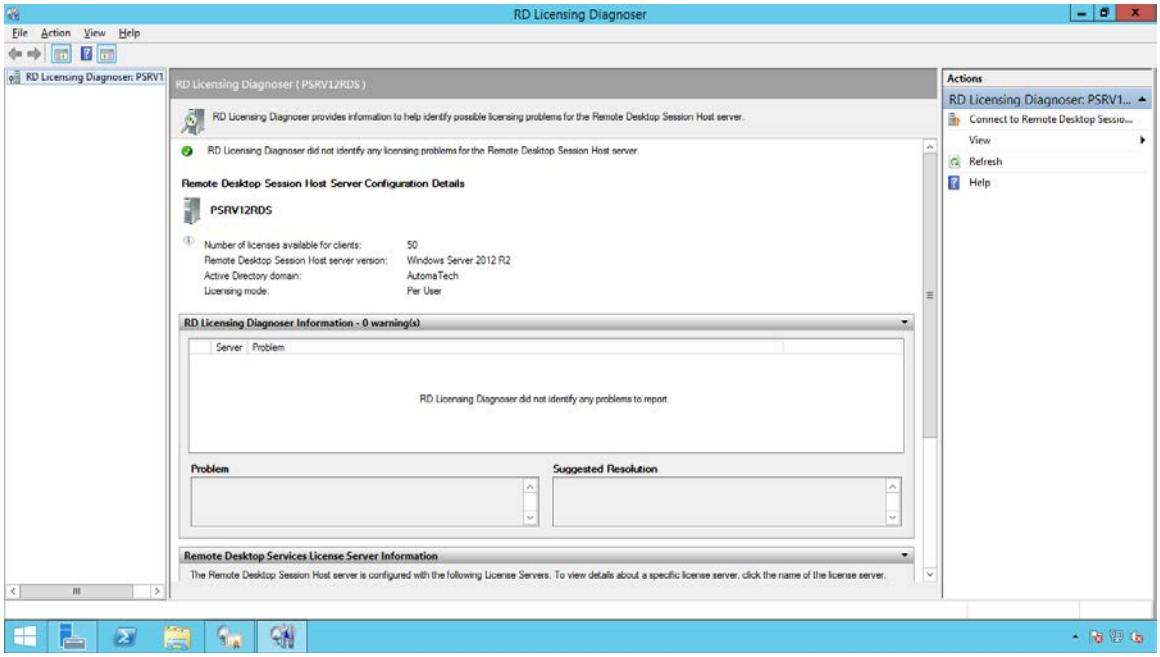
STEP 37: The Deployment Properties window also provides information about the RD Web Access and RDS Certificates. As an optional step you can configure Certificates for the RDS Services in order to secure the connections. Click **OK** to accept the changes.



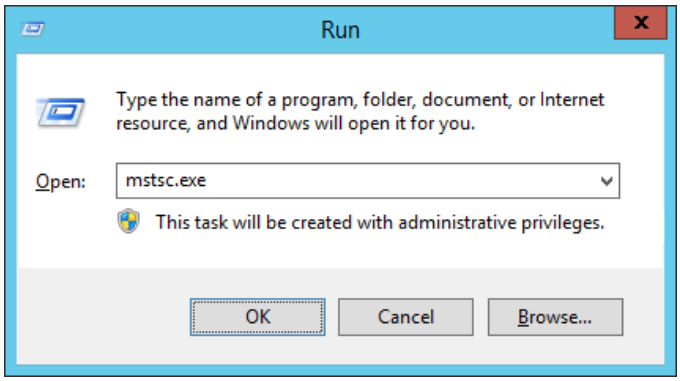
STEP 38: Click the **Tools** link at the top of the Server Manager and click the **RD Licensing Diagnoser** link to launch the Licensing Diagnoser window.



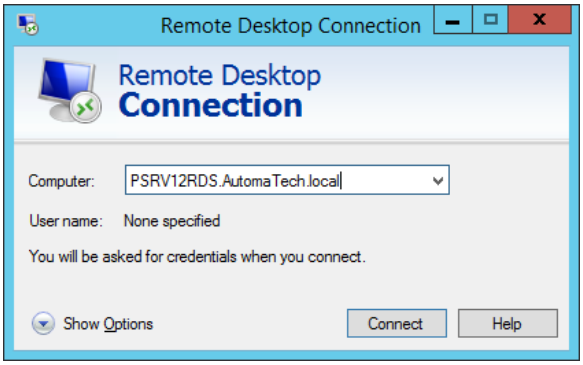
STEP 39: Upon successful configuration and licensing of Remote Desktop Services you will see a healthy RD Licensing Diagnoser status with green check mark, as pictured below.



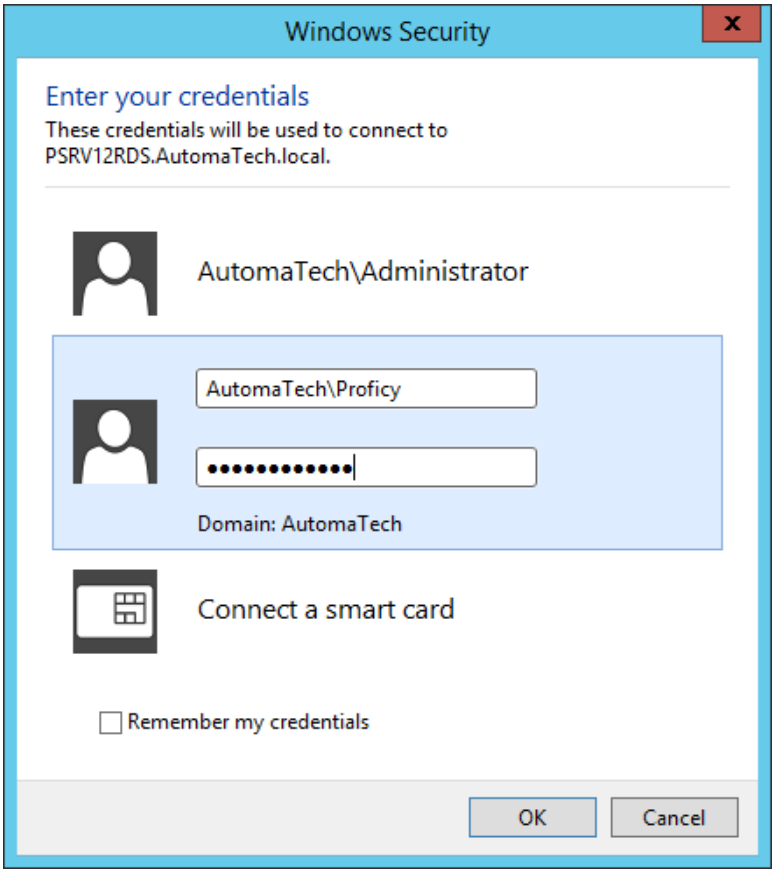
STEP 40: The final step will be to test the Remote Desktop connection. Execute **mstsc.exe** from the **Run** command or launch from the Start Screen to open the Remote Desktop Connection client application.



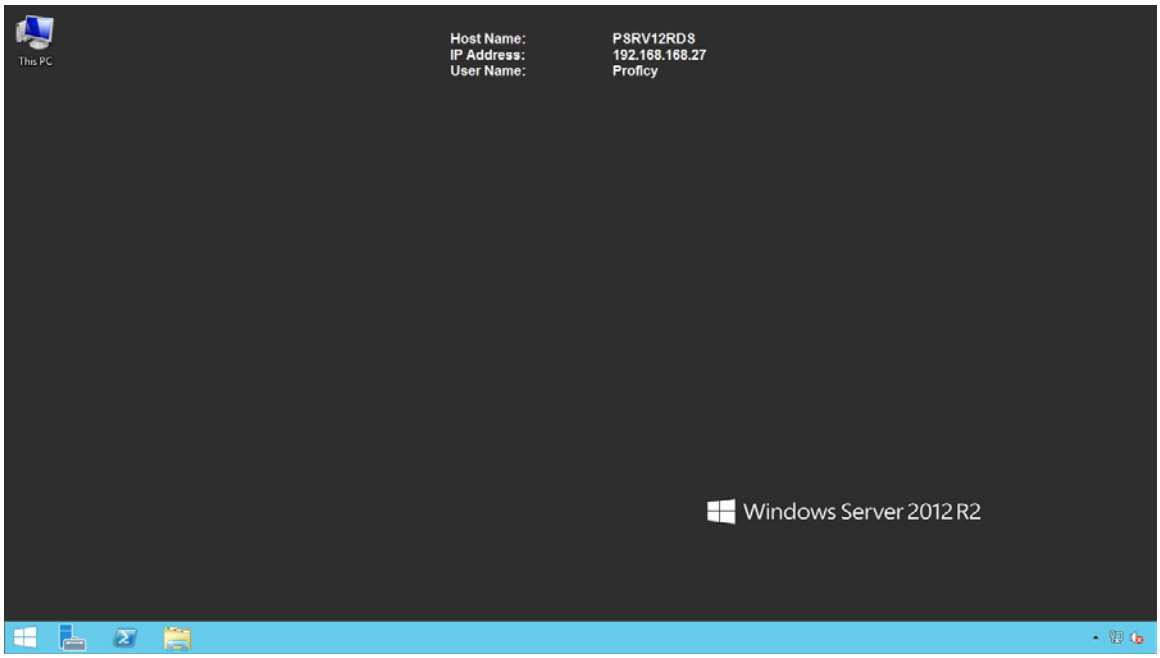
STEP 41: Enter the Fully Qualified Domain Name of the Remote Desktop Server that you are going to connect to. Click the **Connect** button to launch the Windows Security window.



STEP 42: Enter the credentials for the Proficy User that was created in the earlier steps at the Active Directory Domain Server level and click **OK** to connect.

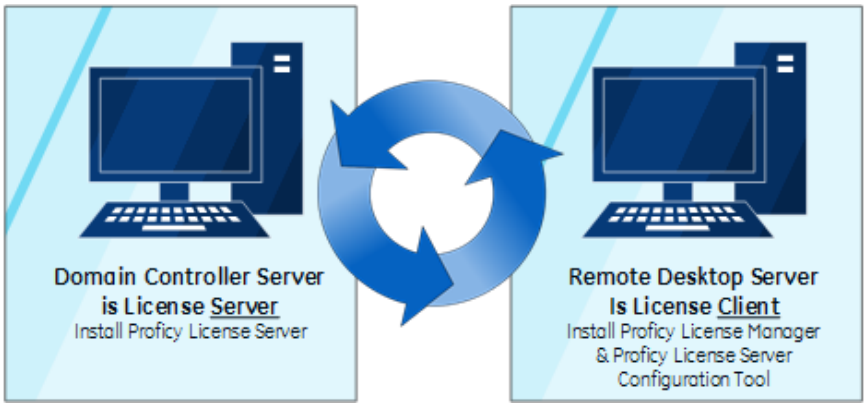


STEP 43: You will now see the Remote Desktop Session created for the Proficy Domain User, as pictured below. You now have successfully followed the steps required to setup and connect to a Windows 2012 R2 Server using Active Directory and Remote Desktop Services!



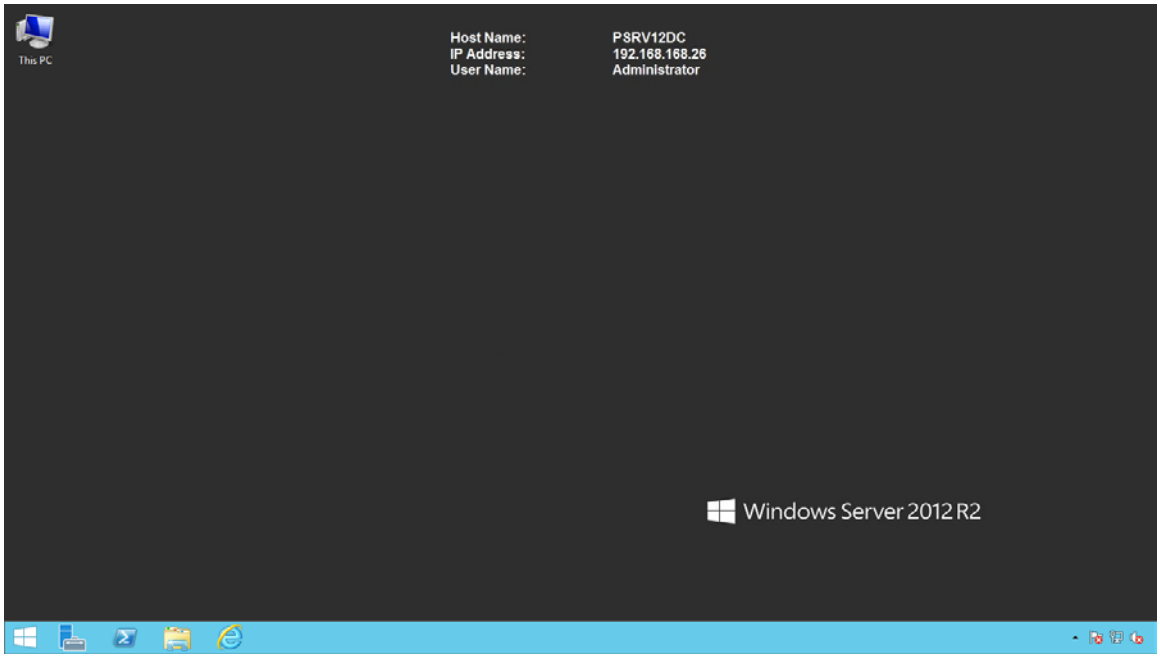
3. Installing, Configuring, and Activating GE Advantage Licensing on a Local License Server for use with GE Proficy SCADA Thin Clients

Now that the Domain Controller Server and Remote Desktop Server have been successfully configured, you are ready to begin installing GE Software and Licensing. You will start by installing the necessary Proficy Licensing components on the Servers. The Domain Controller Server will act as the Proficy License Server and the Remote Desktop Server will act as the License Client where the applications will run. The License Client will periodically verify active licenses with the License Server, as depicted below.



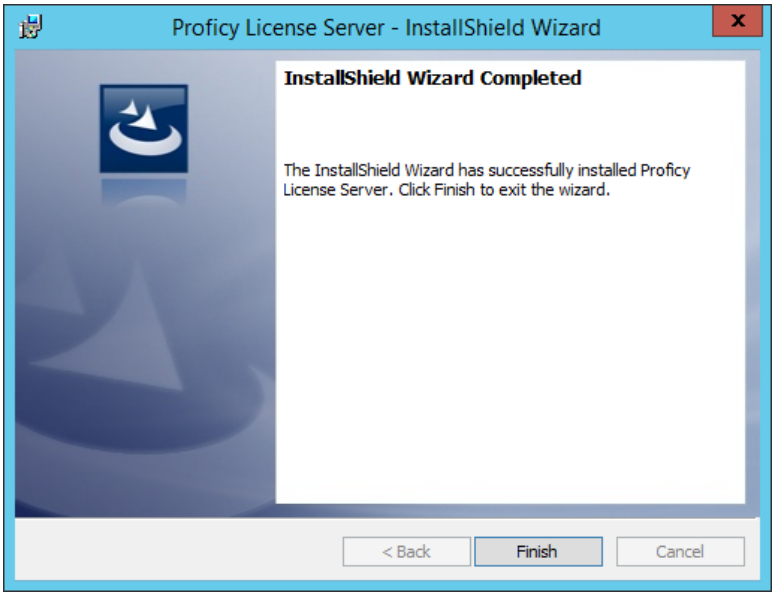
To download the latest Proficy Licensing Software and for detailed instructions on installing and activating Proficy Licensing software please visit the GE Customer Center: https://ge-ip.force.com/communities or the GE Support Site: http://support.ge-ip.com/licensing. This app note follows the Online Activation procedures for when an Internet connection is available on the network. For Offline Activation procedures please refer to the Proficy Licensing software documentation.

STEP 1: Login to your Domain Controller Server computer as the Domain Administrator.

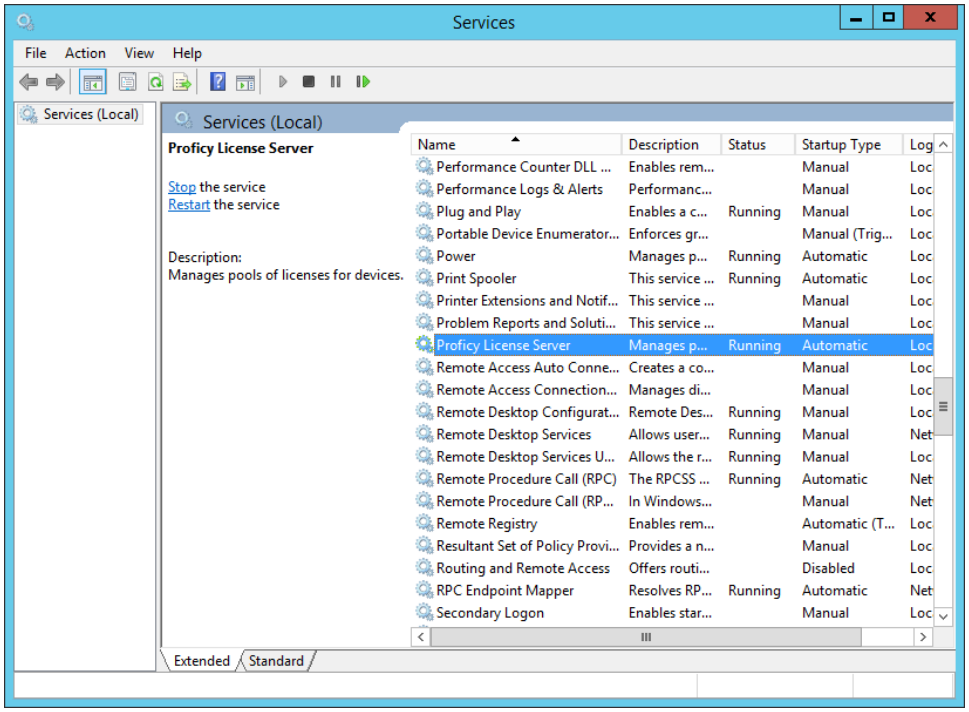


STEP 2: Run the Proficy Licensing Installation application, select the **Install License Server** option.

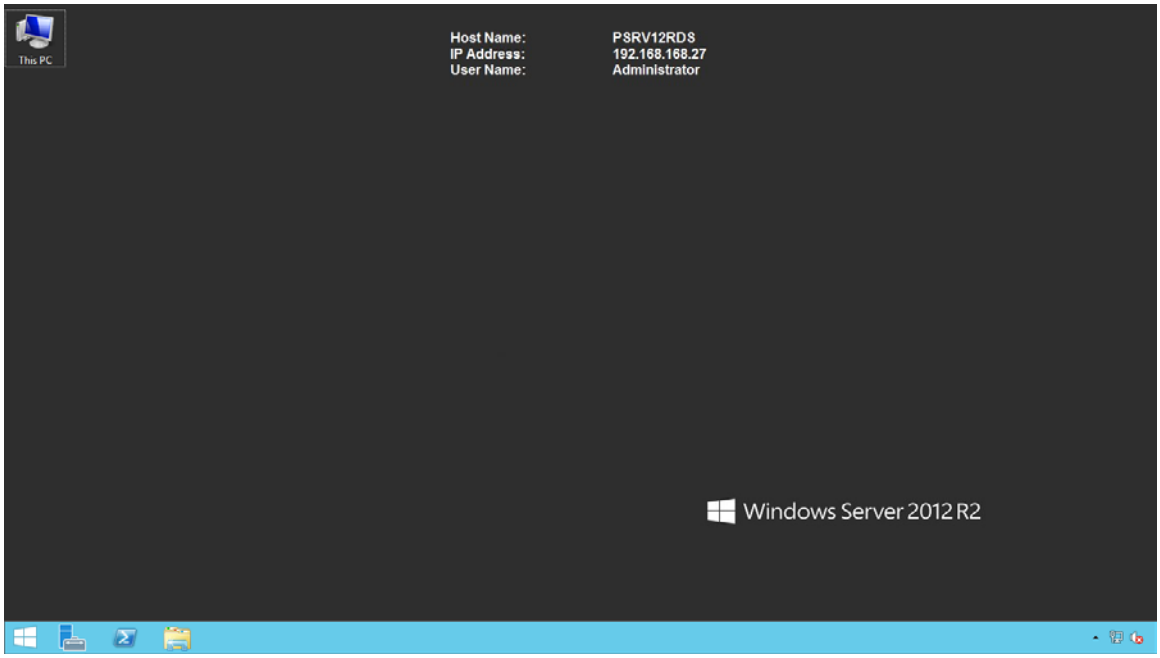
STEP 3: After a few moments you will be notified that the Installation has completed, click the **Finish** button to complete the Proficy License Server installation.



STEP 4: Launch the Windows **Services** and observe that the Proficy License Server service Status is listed as Running.

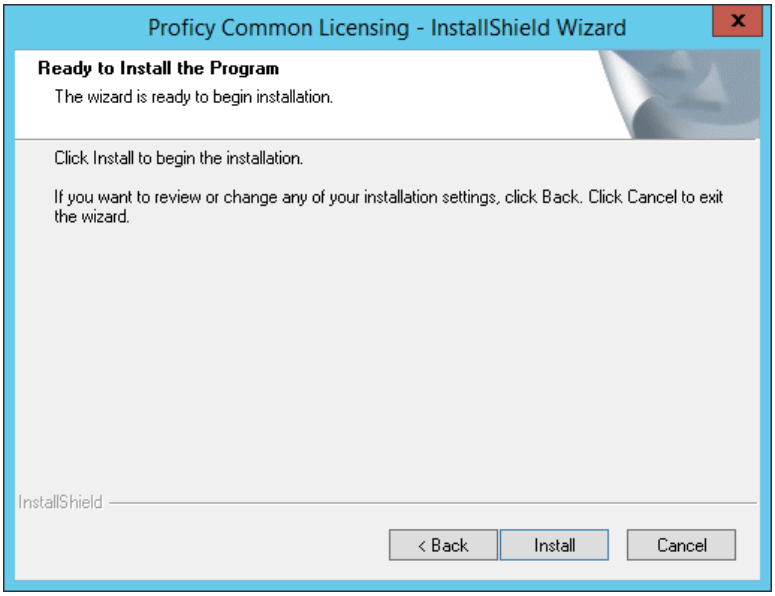


STEP 5: Login to your Remote Desktop Server computer as the Domain Administrator.

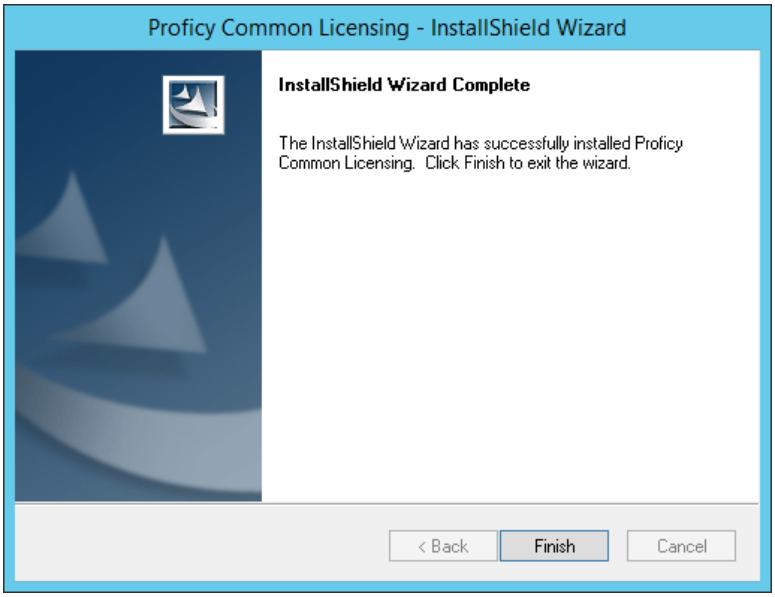


STEP 6: Run the Proficy Licensing Installation application, select the **Install License Client** option.

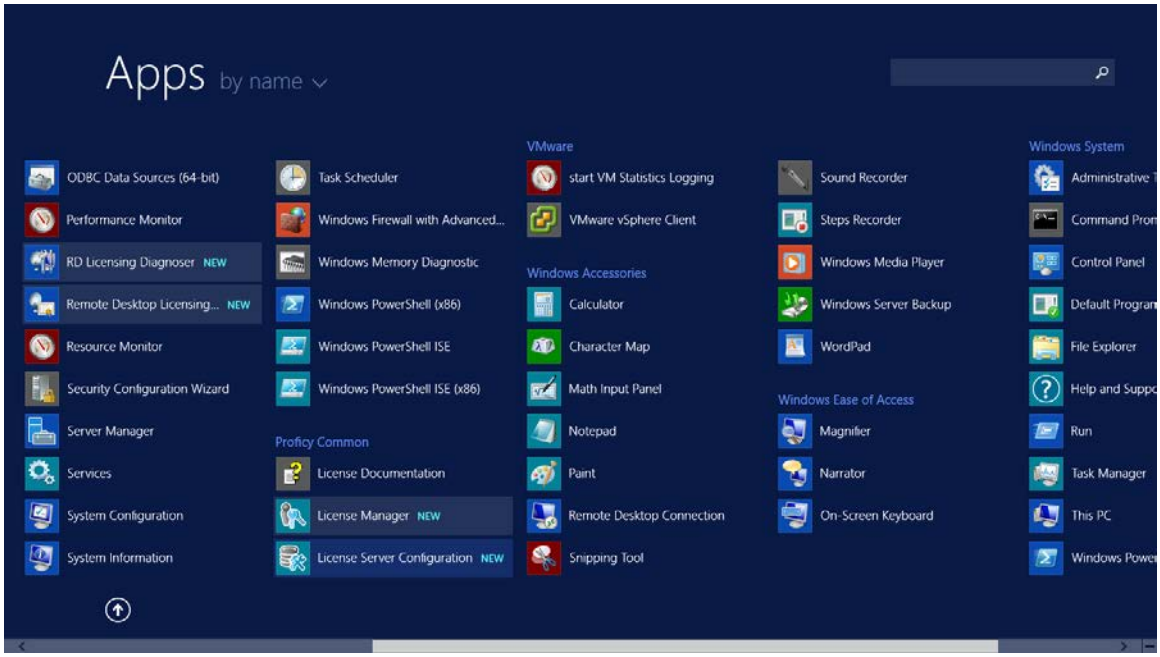
STEP 7: Click through the prompts, accept the License Agreement, and click **Install** to install the Proficy Common Licensing application.



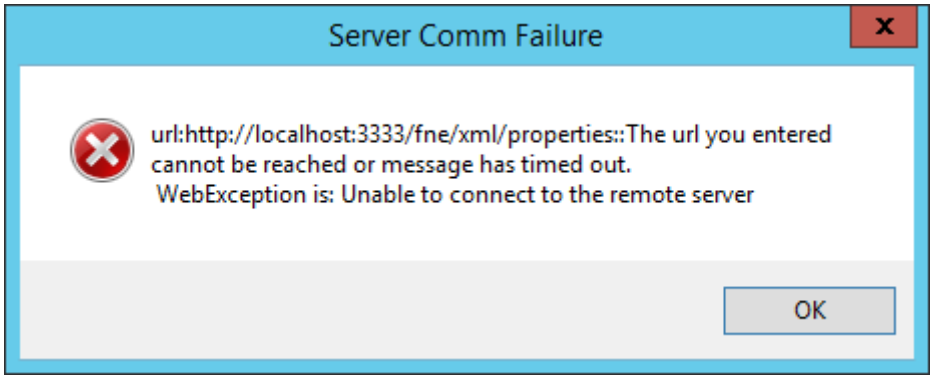
STEP 8: Click **Finish** to complete the Proficy Common Licensing installation.



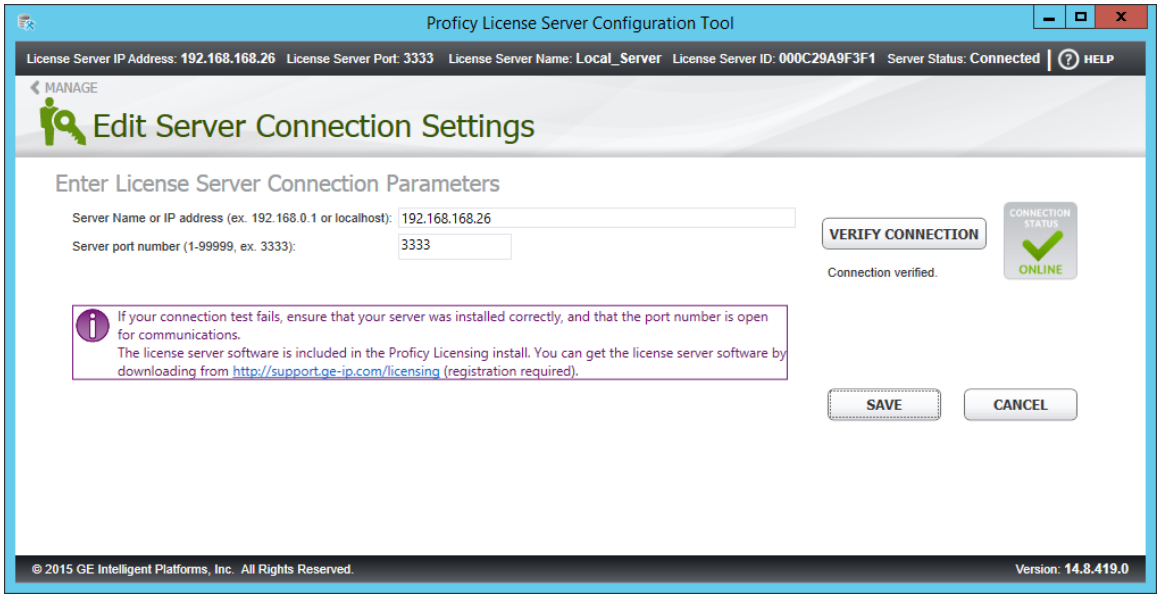
STEP 9: On the Start Screen, you will notice two new applications have been installed in the Proficy Common folder. Click the **License Server Configuration** icon.



STEP 10: You will be notified that a Server Comm Failure occurred because the application is trying to communicate with a License Server running on the local machine, which does not exist. Click **OK** to accept the message and launch the Edit Server Connection Settings screen.

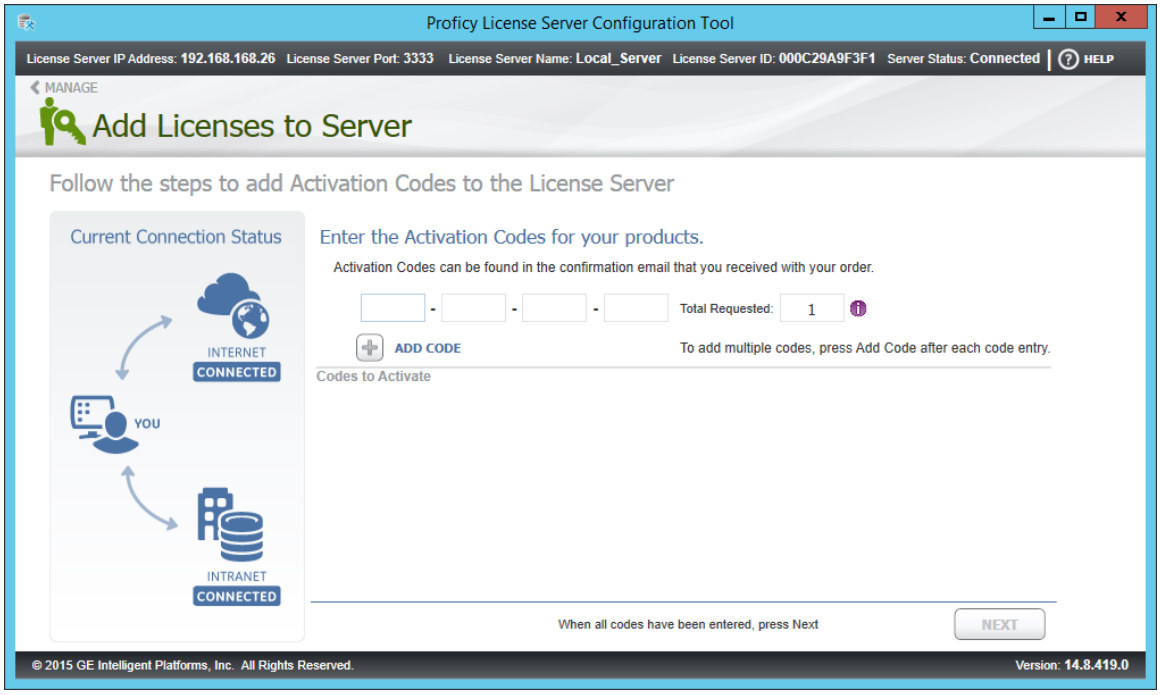


STEP 11: Update the settings to point to the **Server Name or IP Address of the Domain Controller Server**. Click the **Verify Connection** button to test the connection and click **Save** to accept the changes.

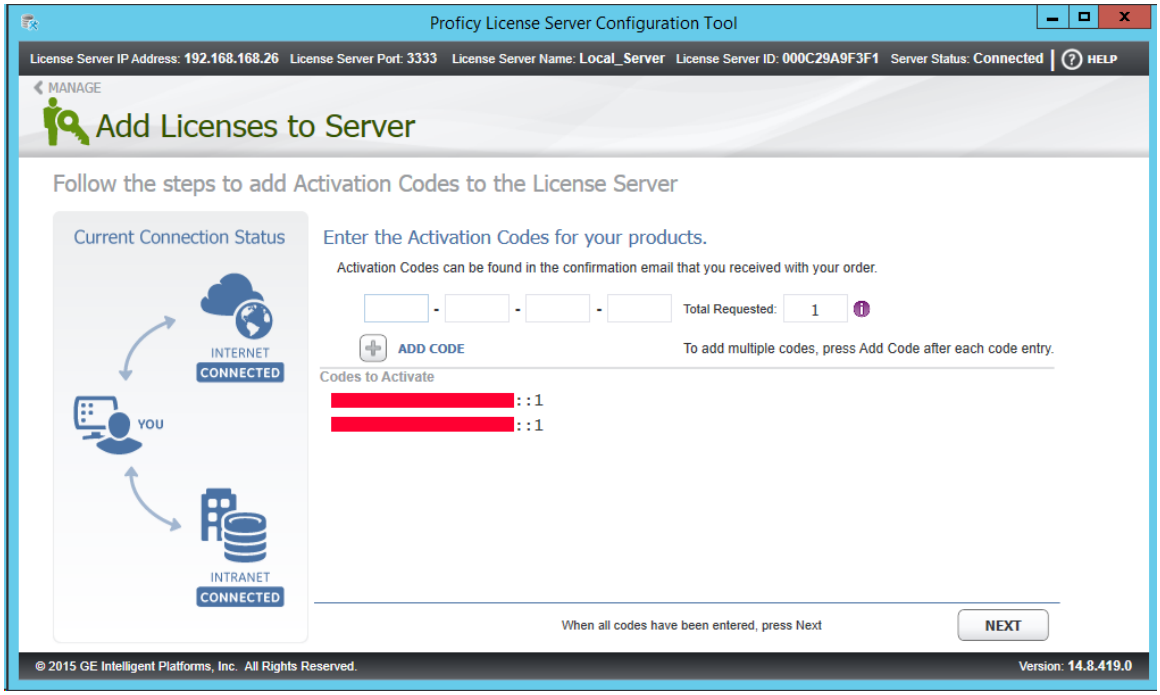


STEP 12: Click the **< MANAGE** link in the upper left corner to view the License Server Manager Overview screen. Take notice of the status bar at the top of the window. You are now connecting through the network to remotely access the License Server service running on the Domain Controller Server computer.

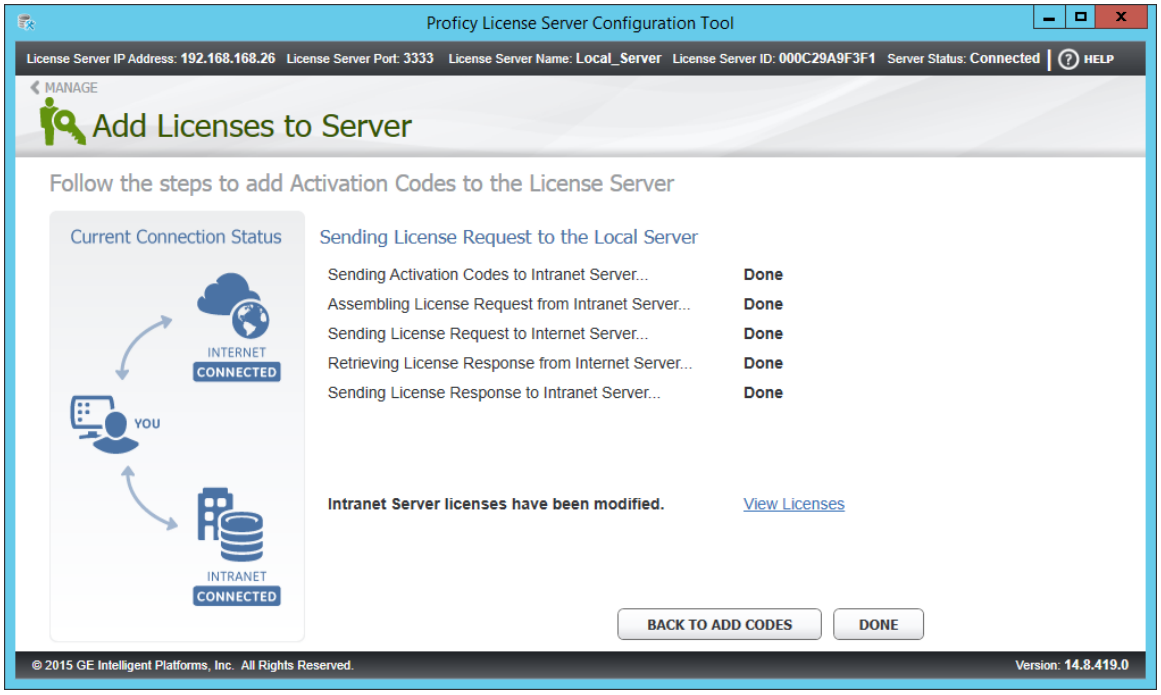
STEP 13: Click the **Add Licenses to Server** button in the Manage Licenses section. The Add Licenses to Server window will appear, take notice this system is Internet connected and will allow us to perform Online Activations.



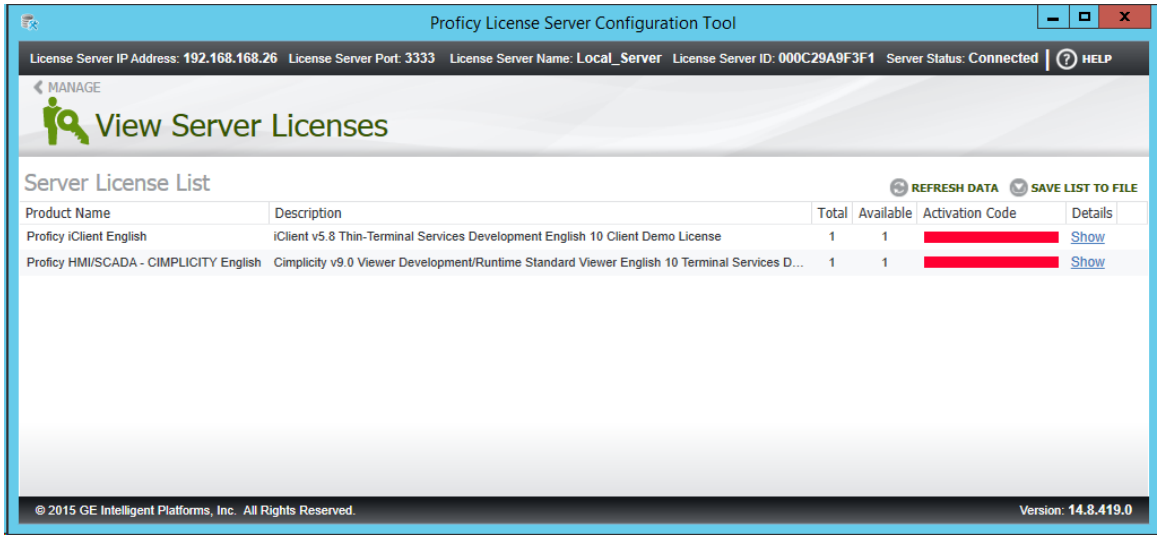
STEP 14: Type in or paste in your activation codes and quantities then click the **Add Code** button. You will see a summary of codes listed that will be used for activation.



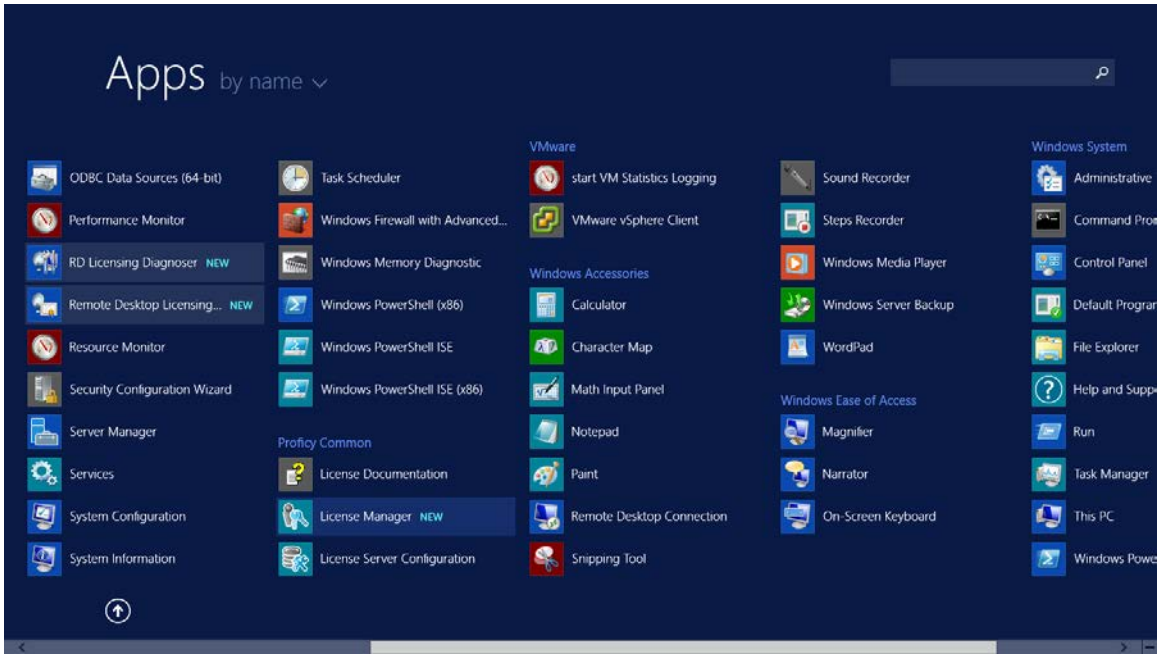
STEP 15: Click **Next** to complete the activation, when successful you will be notified on the screen when each part of the activation process has completed.



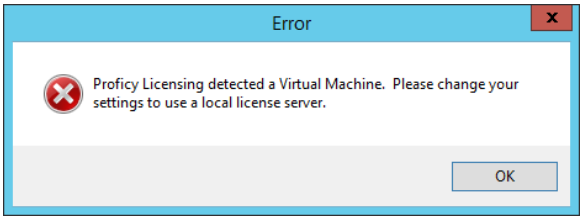
STEP 16: Click **View Licenses** to view the newly installed licenses on the Local License Server. You will notice each license status is shown as Available, they are now ready to be assigned to the License Client. This application note demonstrates activation of Terminal Services Client licenses for both iFIX and CIMPLICITY.

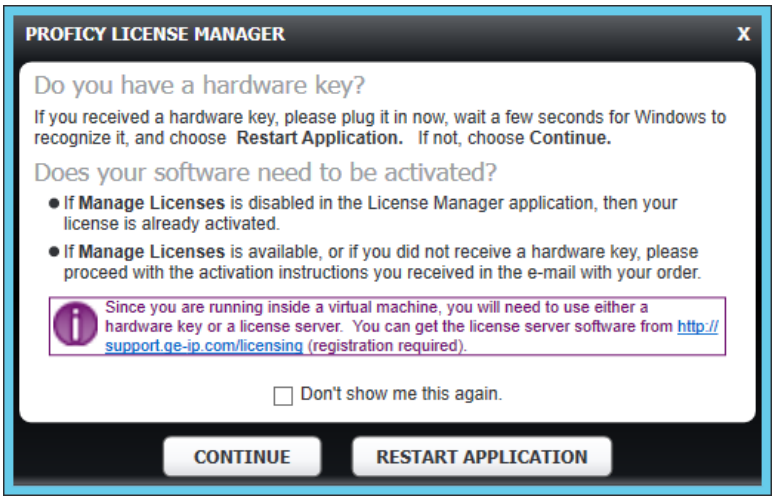


STEP 17: Return to the Start Screen, click the **License Manager** icon.

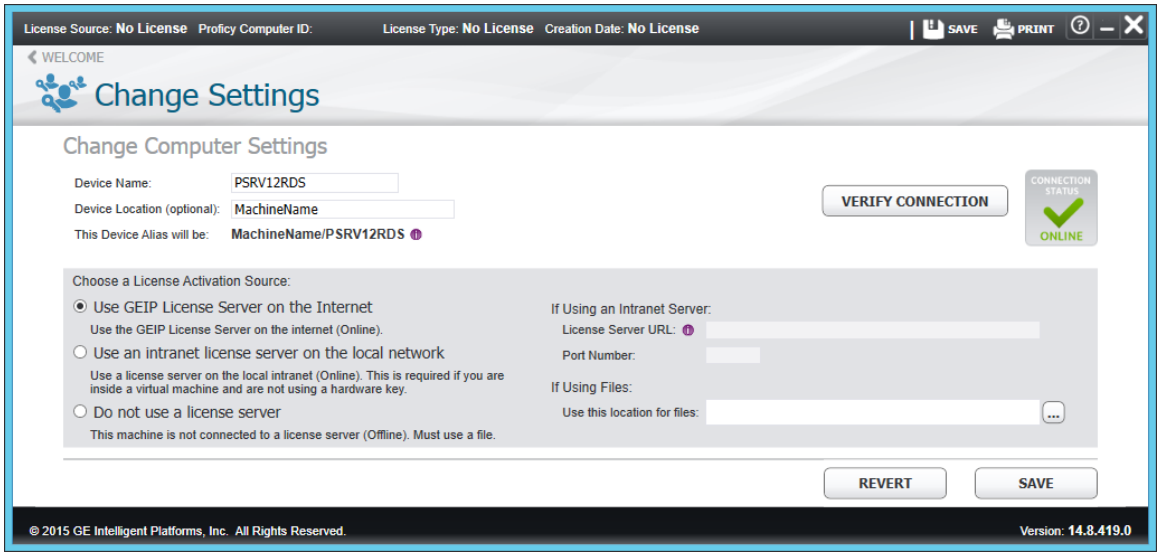


STEP 18: When running in a Virtual Machine you will be notified that you will need to change your settings to use a Local License Server. Click **OK** to accept the notification and click **Continue** to acknowledge the licensing messages.

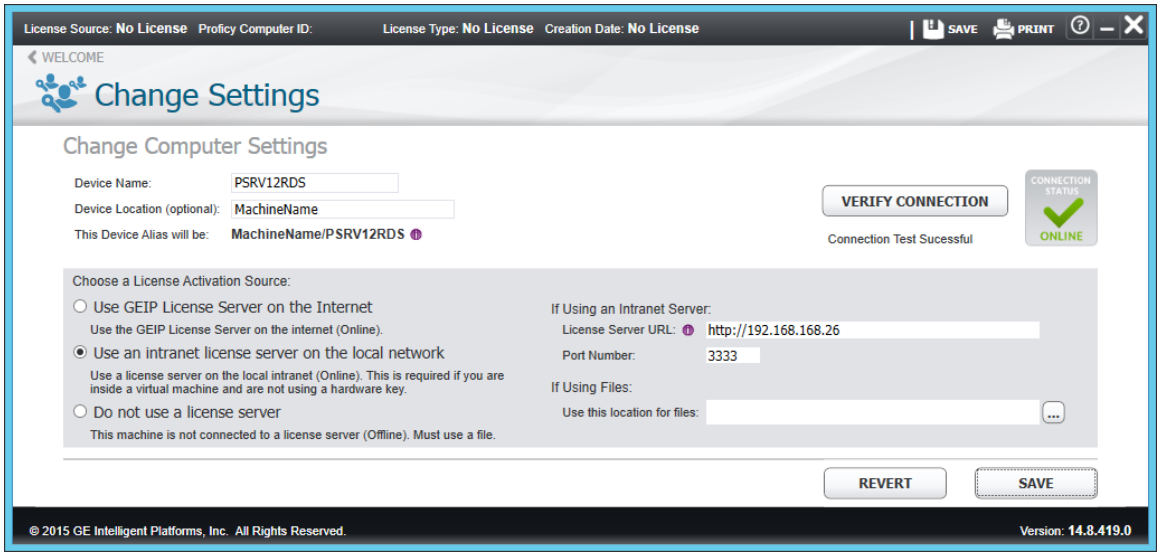




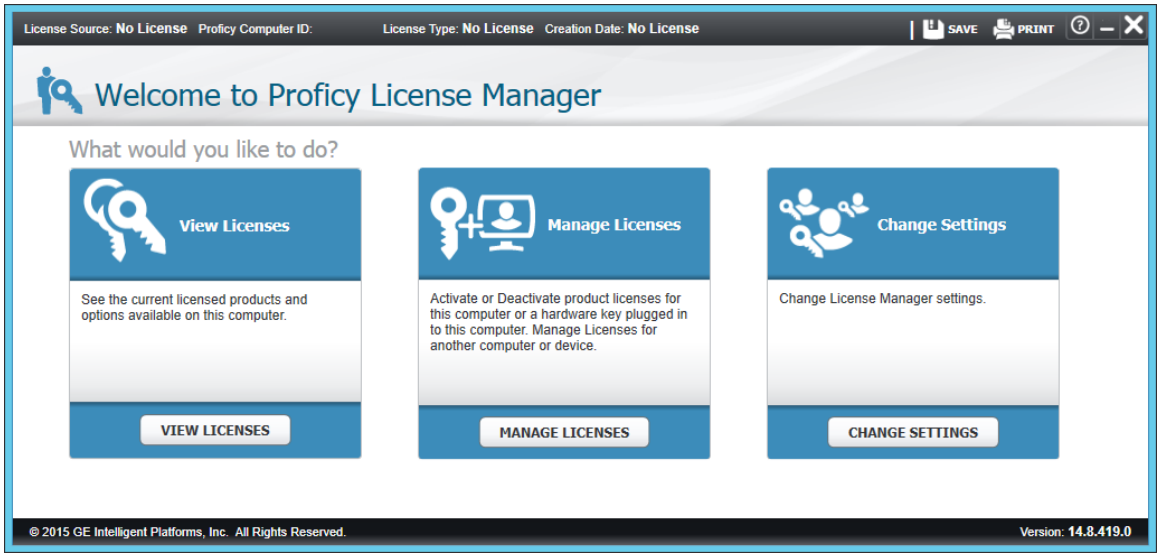
STEP 19: You will be directed to the Change Settings window, by default the Licensing software wants to use the GEIP License Server on the Internet.



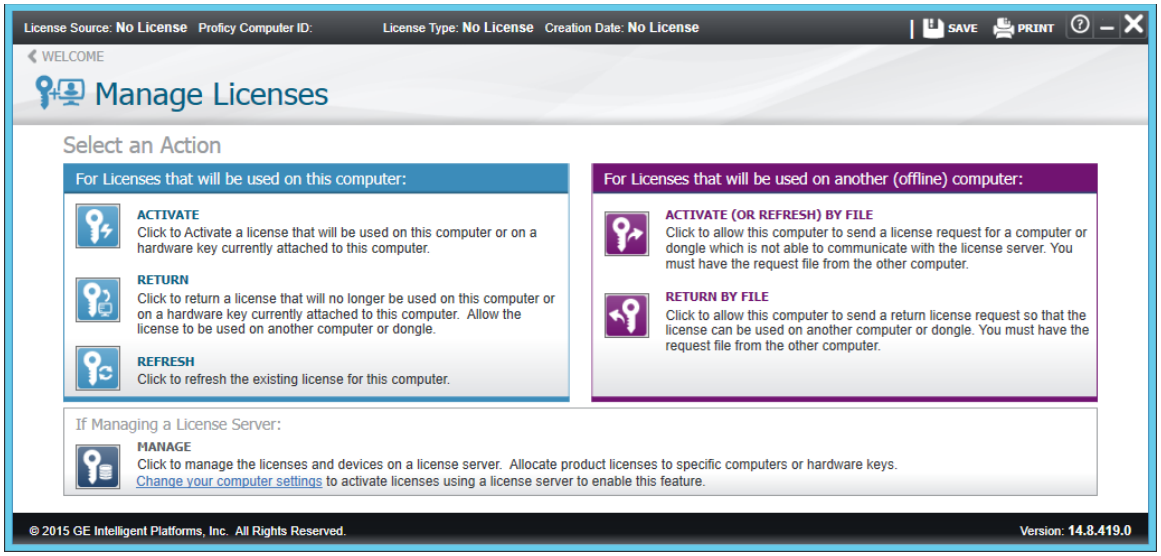
STEP 20: Select the option to **Use an intranet license server on the local network**, set the License Server URL to include the **IP Address of your License Server** (the Domain Controller Server computer). Click the **Verify Connection** to test the connection and click the **Save** button to complete the configuration, as pictured below.



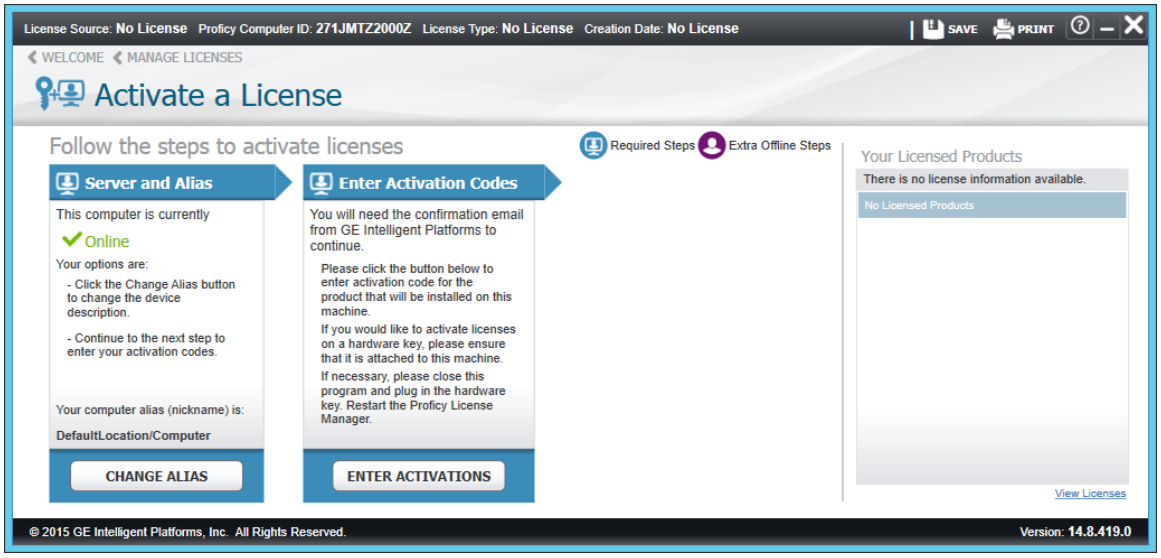
STEP 21: Click the **< WELCOME** link in the upper left corner to view the Proficy License Manager Overview screen.



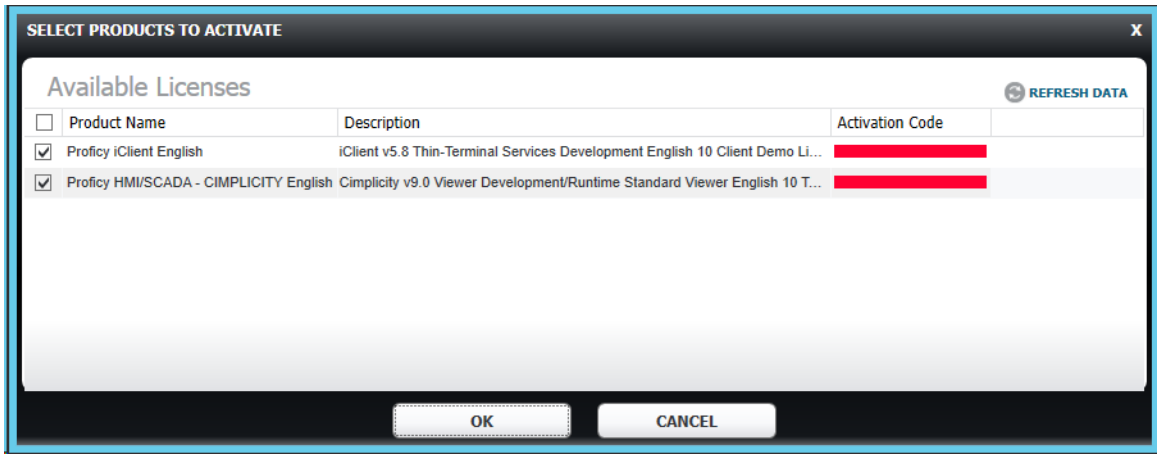
STEP 22: Click the **Manage Licenses** button to open the Manage Licenses screen.



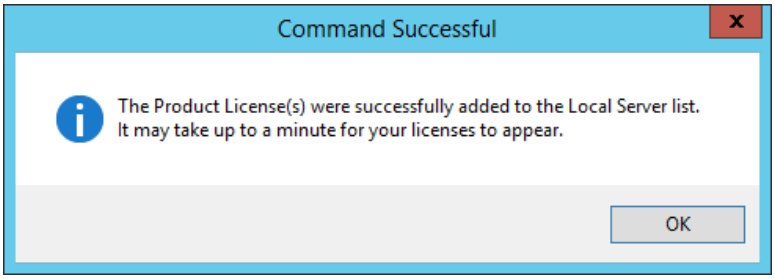
STEP 23: Click the **Activate** button to open the Activate a License screen.

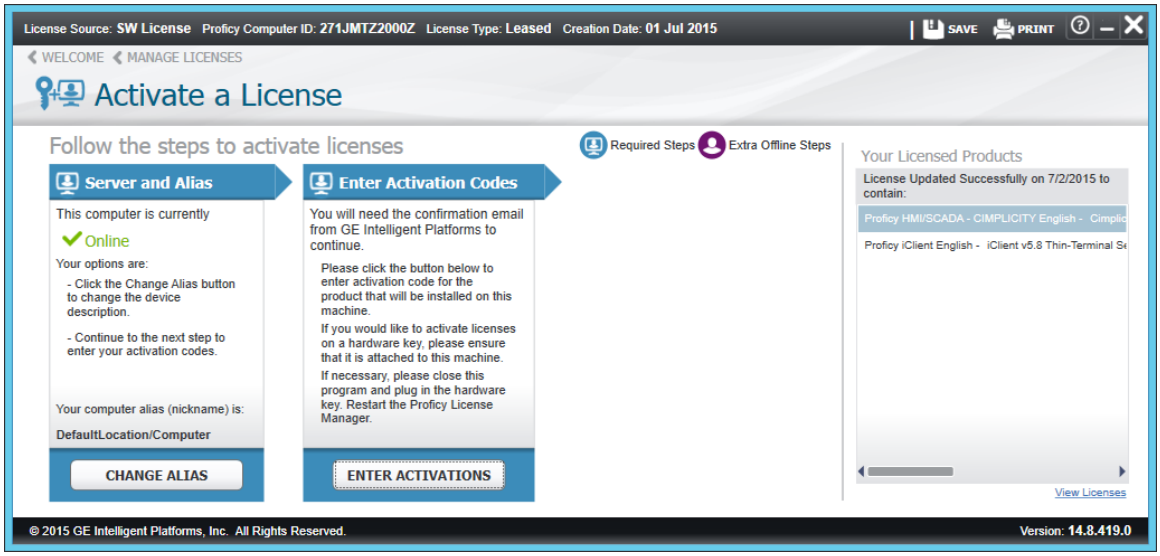


STEP 24: Click the **Enter Activations** button and you will be prompted with the Select Products to Activate window which provides a summary of the licenses installed on your Local License Server. Check the boxes to select both Product Names. Click **OK** to accept the selections.

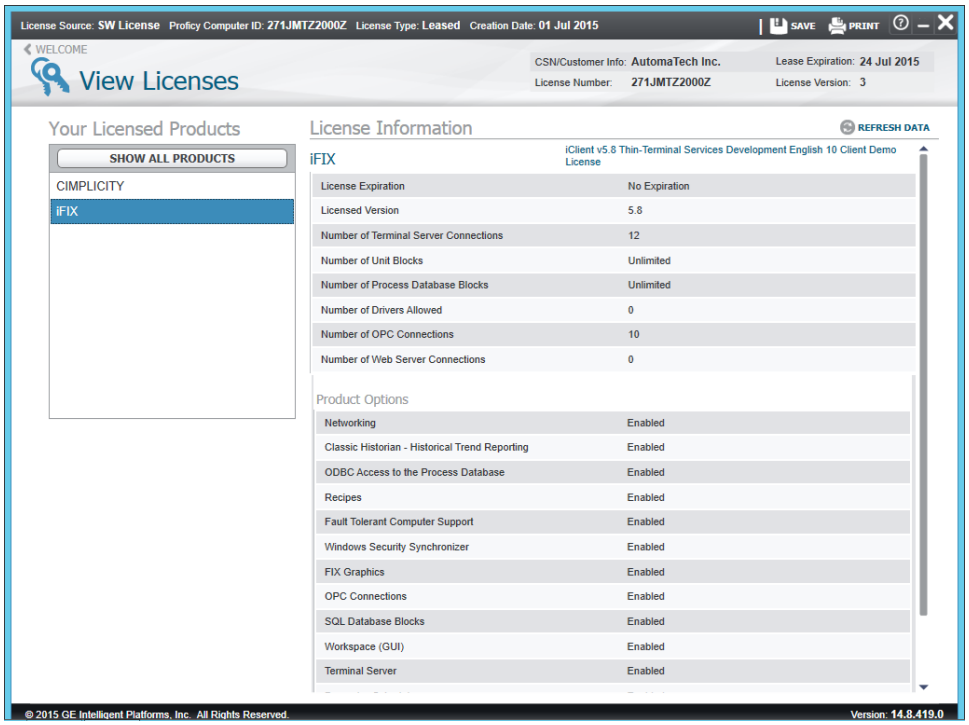


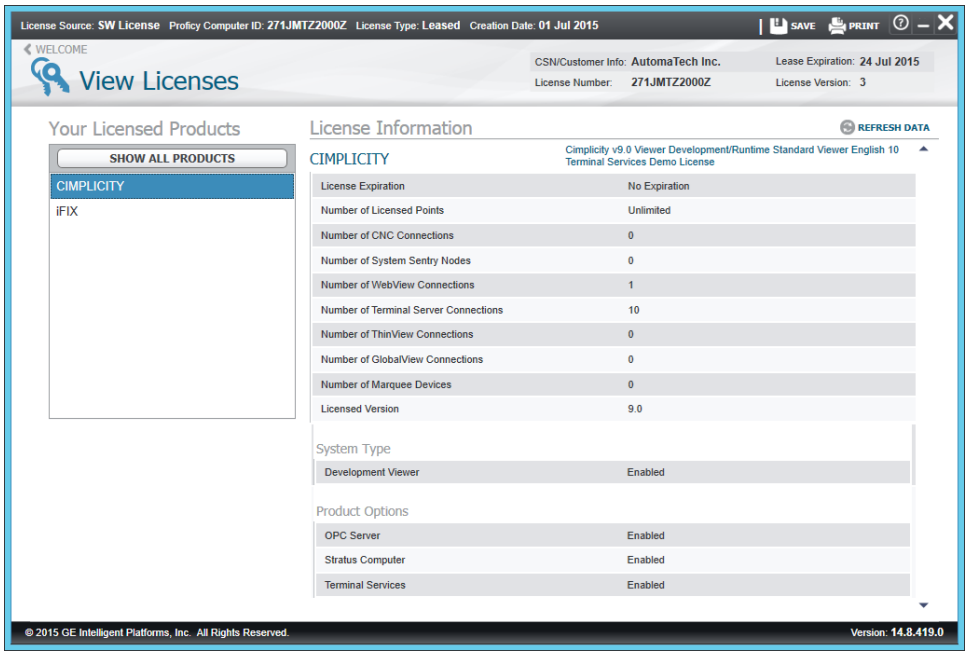
STEP 25: Click the **Activate** button on the Enter Activation Codes window, you will be prompted that the licenses were successfully added, click **OK**. Notice the licenses are now listed in the Your Licensed Products section.





STEP 26: Click the **< WELCOME** link in the upper left corner to return to the Proficy License Manager Overview screen and click the **View Licenses** button to open the View Licenses screen, as pictured below. You will notice that licenses have successfully been added for both 10 iFIX Terminal Services connection and 10 Cimplicity Terminal Services connections, successfully completing the Proficy Licensing process!

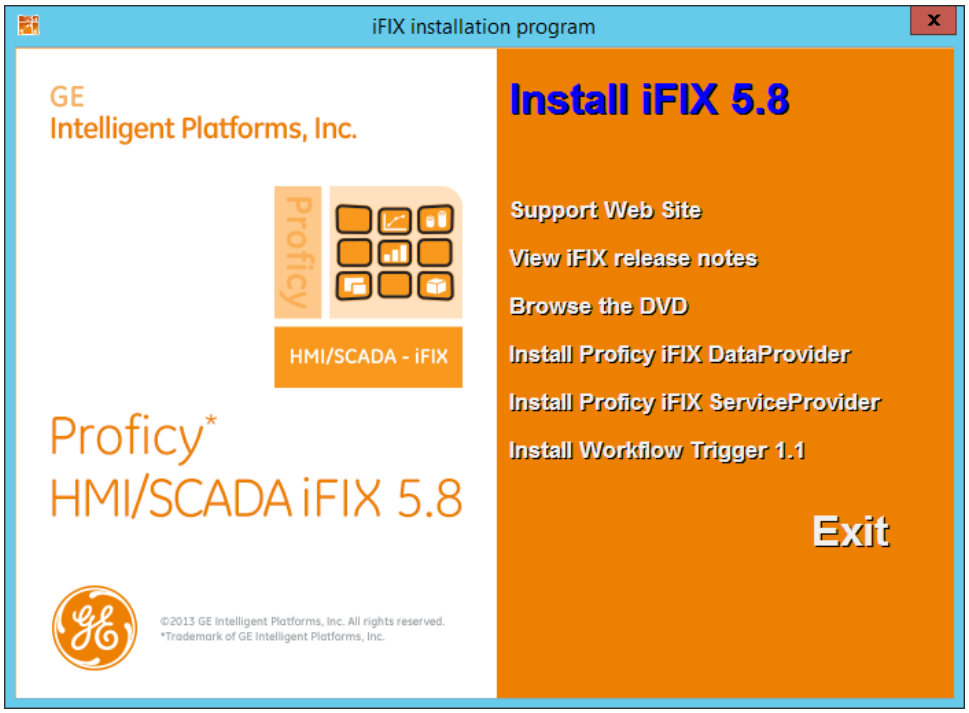




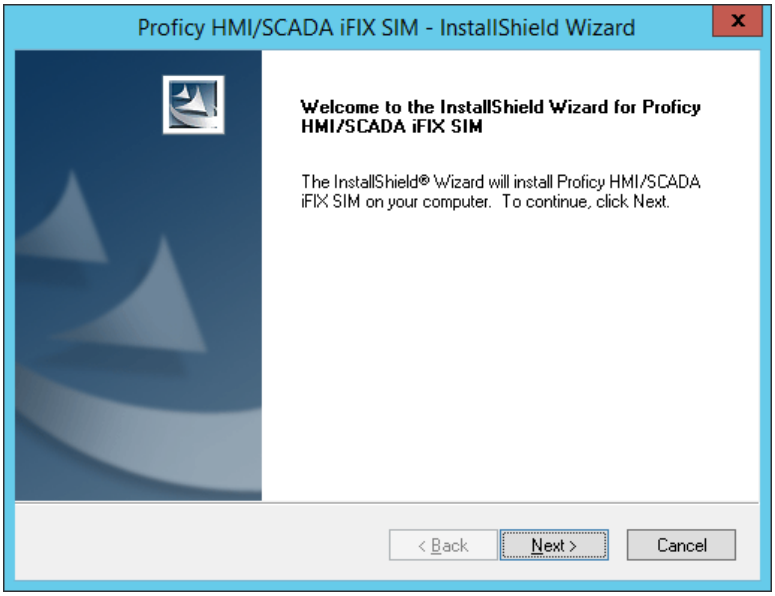
4. Overview of Installing and Configuring GE Proficy HMI/SCADA iFIX for use in a Remote Desktop Services Environment

This section provides a very high level overview of the steps for deploying Proficy HMI/SCADA iFIX in a Remote Desktop Services (formerly Terminal Services) Environment. For additional considerations, detailed configurations, compatibility requirements, and best practices when working with Terminal Services please refer to the iFIX Electronic Books included with the product or available on the GE Support Site: http://support.ge-ip.com

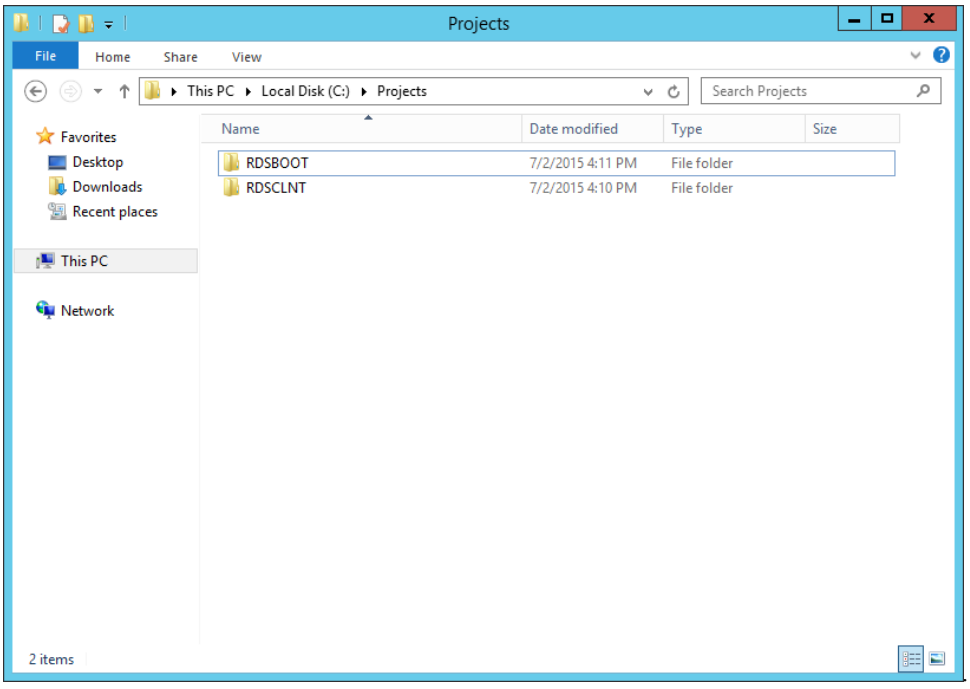
STEP 1: Insert or connect the Proficy HMI/SCADA iFIX 5.8 media to the Remote Desktop Server computer. Click the **Install iFIX 5.8** option on the splash screen and follow the prompts to complete the installation. NOTE: iFIX 5.8 as released only supports Windows Server 2012, iFIX 5.8 SP1 is required for Windows Server 2012 R2 support. A reboot will be required after completing the iFIX 5.8 installation.



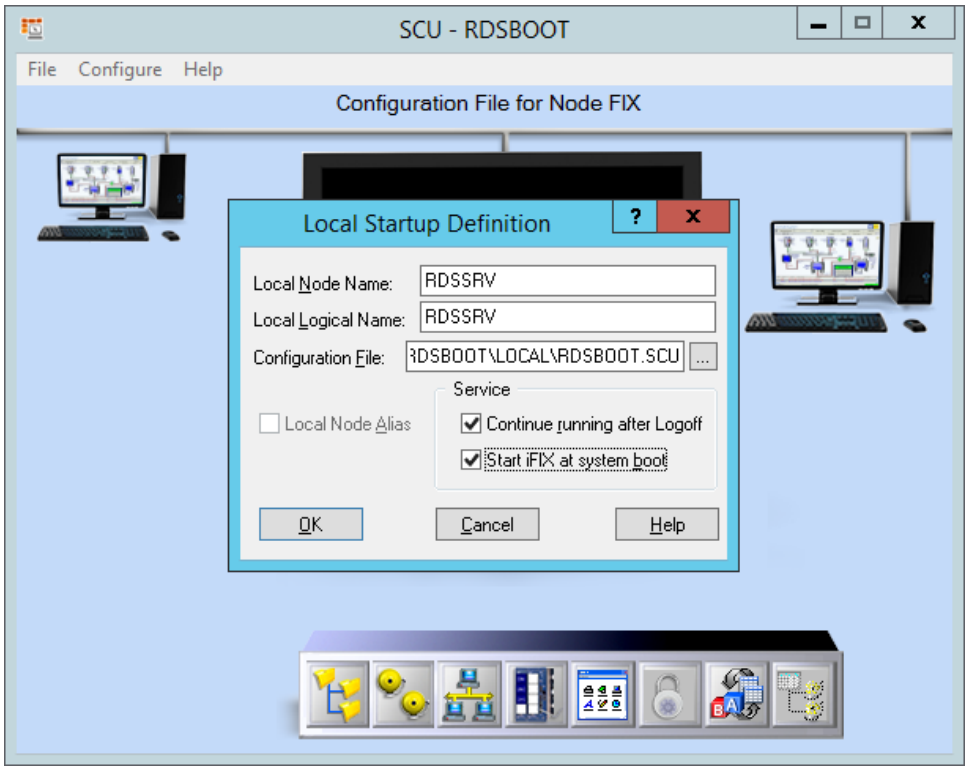
STEP 2: After rebooting, install iFIX 5.8 SP1 and the latest SIMs. Follow the prompts to complete the installation and you will be prompted again to restart the computer.



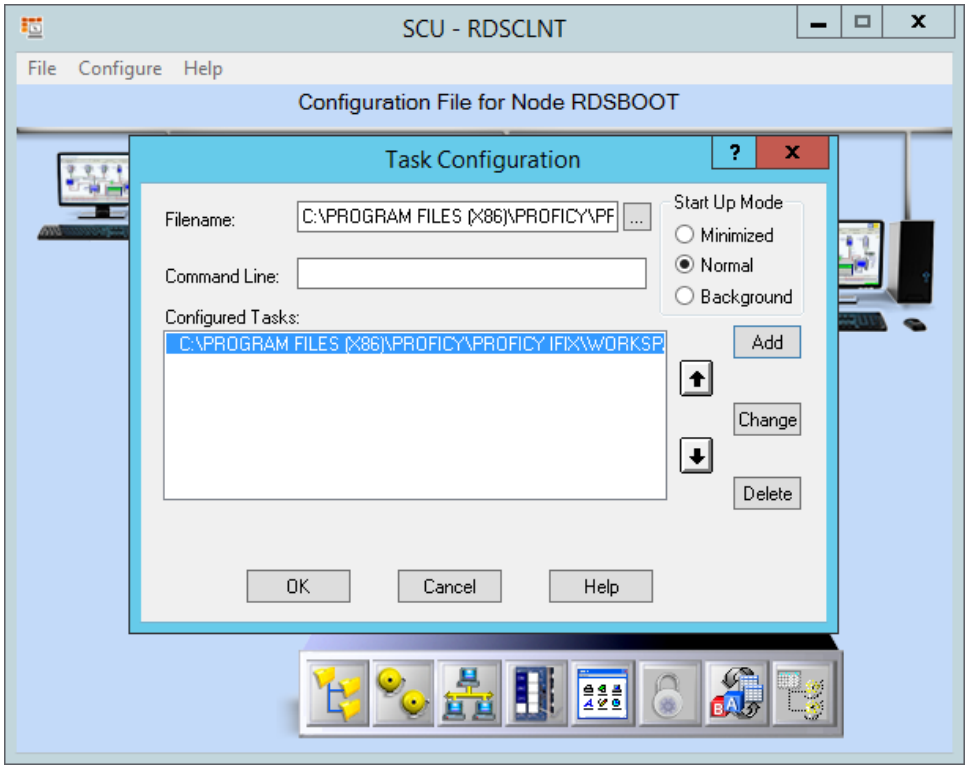
STEP 3: After rebooting you will need to build the necessary number of SCUs for your deployment based on requirements for Users, Roles, Projects, Security, etc. in your system architecture. For this example, two simple SCUs have been created, one for the iFIX Service account (RDSBOOT) and another for the Client access (RDSCLNT). Two project folders have been created with the appropriate iFIX files for RDSBOOT and RDSCLNT, as pictured below.



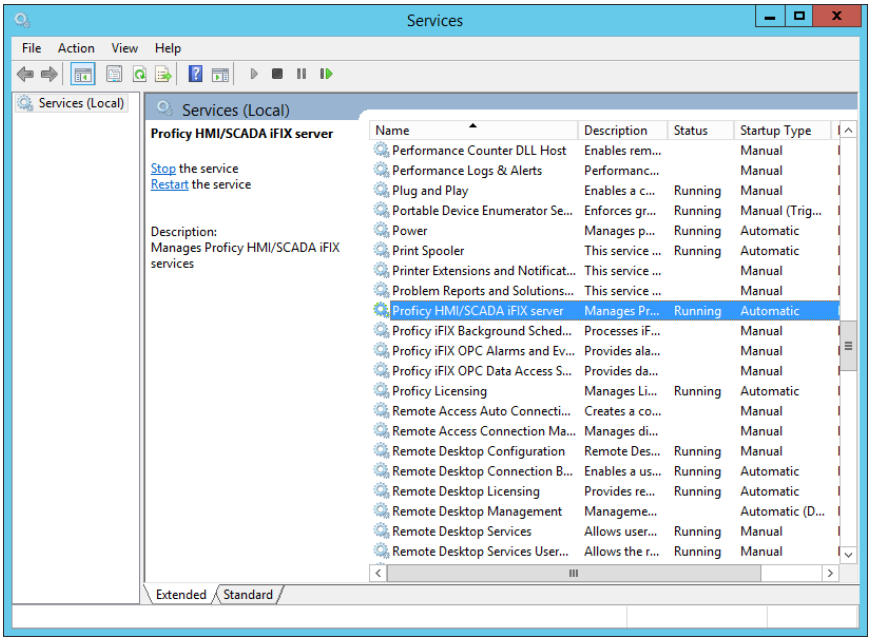
STEP 4: Open the RDSBOOT.SCU and edit the Local Startup properties. **Assign a Node Name** to identify the local session for the Remote Desktop Services Server (like RDSSRV) and **link the RDSBOOT.SCU Configuration File** for the Service account, as pictured below. Check the boxes for **Continue running after Logoff** and **Start iFIX at system boot** to ensure that iFIX runs as a Service and starts automatically without user interaction.



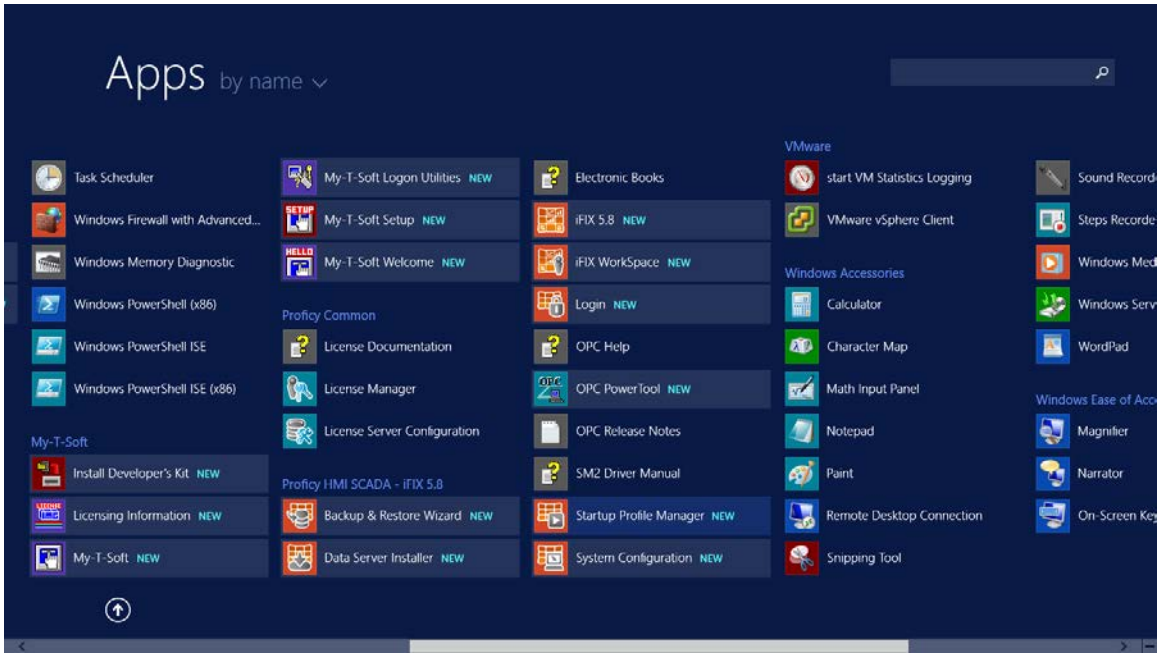
STEP 5: Open the RDSCLNT.SCU and confirm that Workspace.exe is listed in the Task Configuration to ensure that iFIX Workspace starts when clients connect to the Remote Desktop Server.



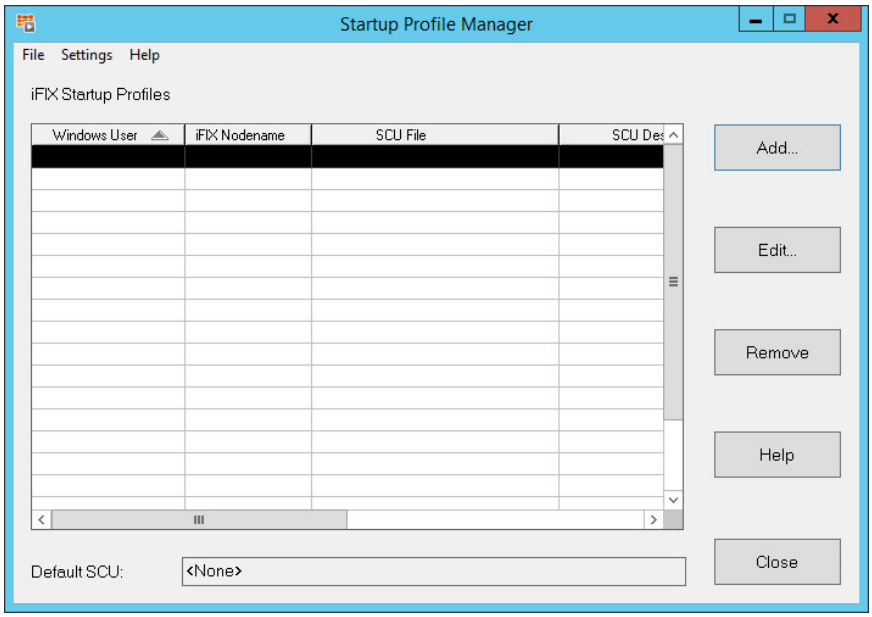
STEP 6: Reboot the server, with the updated configuration iFIX will start automatically at system boot. Open the Windows Services to confirm that iFIX is running, as pictured below.



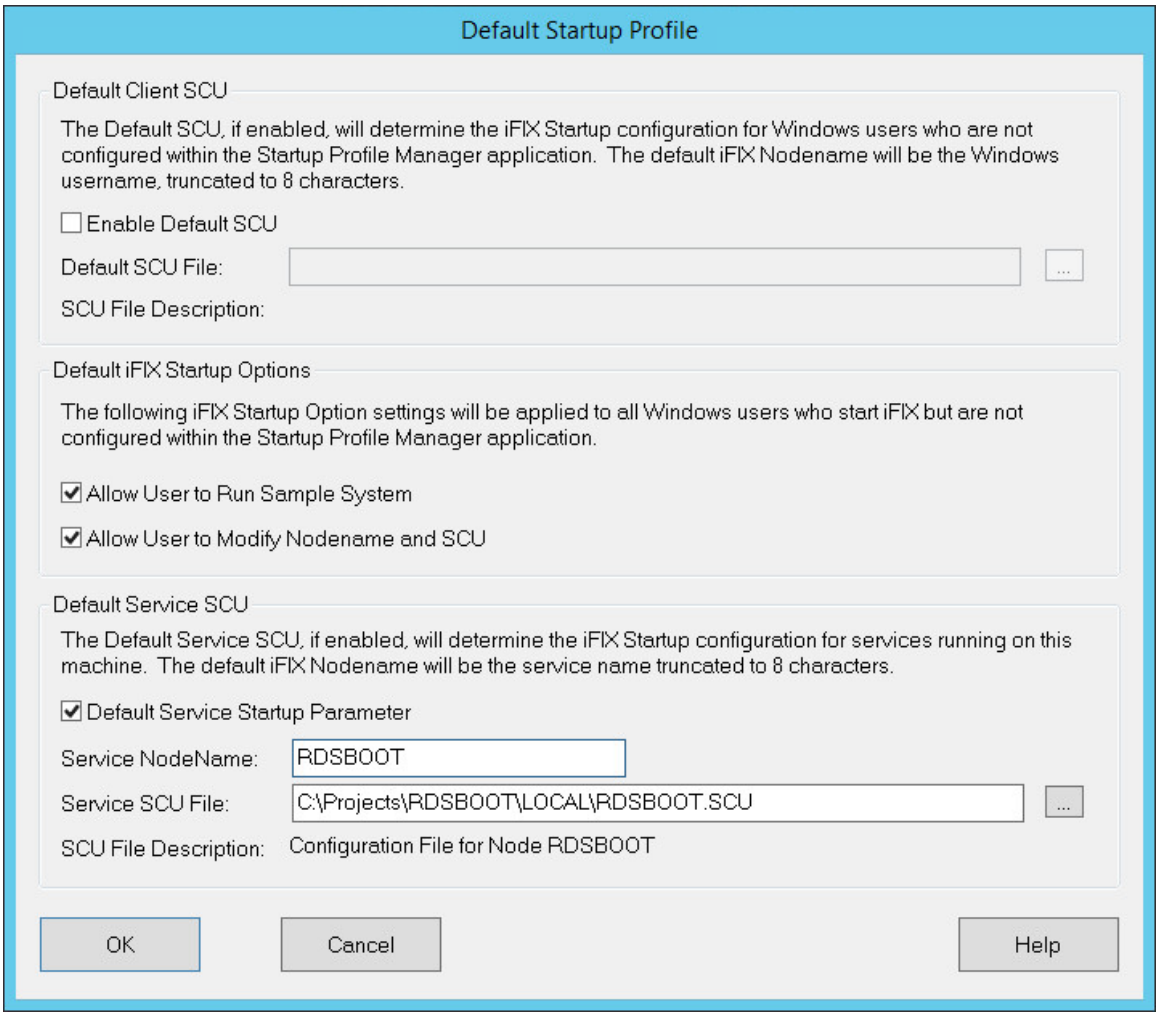
STEP 7: On the Start Screen, browse to the Proficy HMI SCADA – FIX 5.8 folder and click on the **Startup Profile Manager** icon.



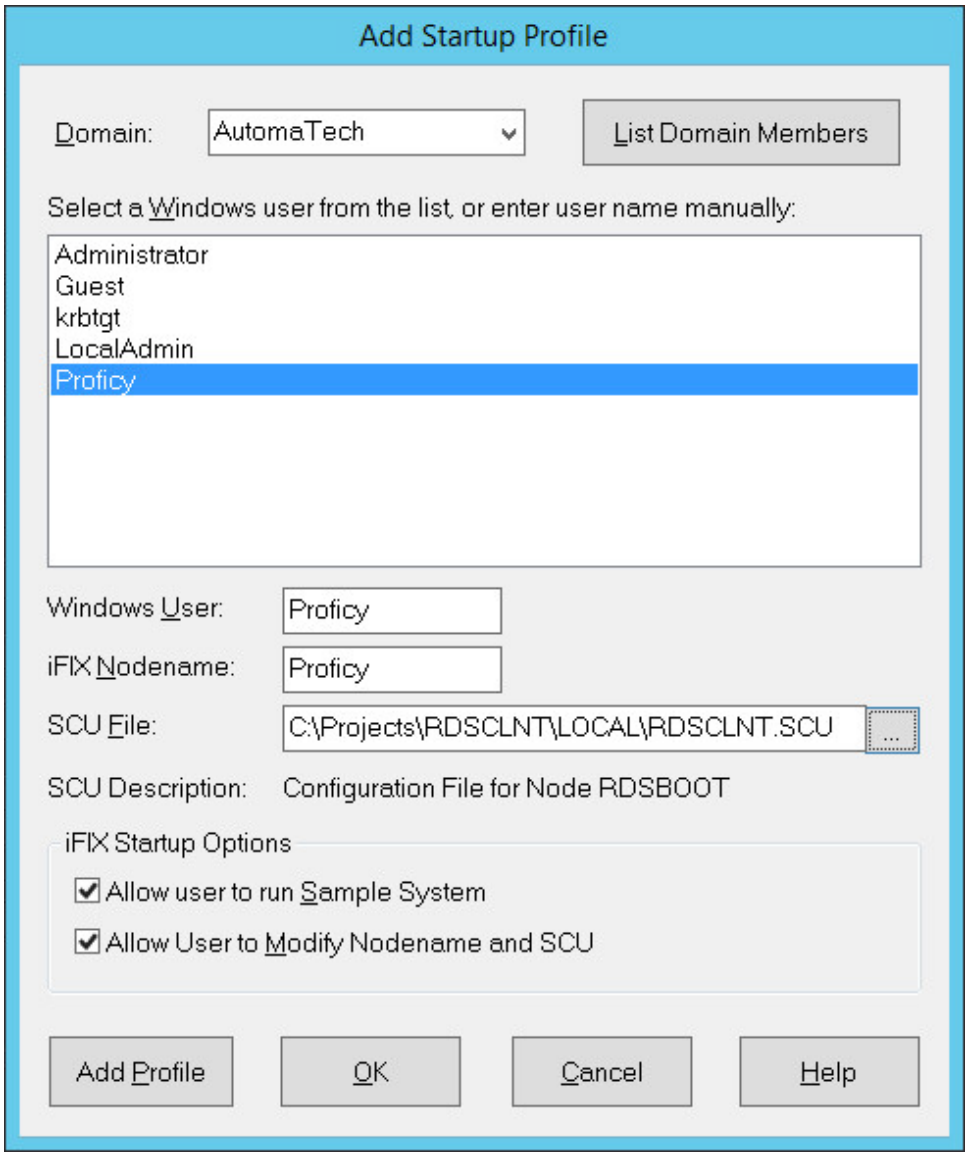
STEP 8: Notice by default, the Startup Profile manager is blank, you will have the ability to link iFIX Project Files and SCUs like the ones created in the earlier steps. The Startup Profiles allow you to associate Windows Users with a specific iFIX Project Configuration. For complete details on working with the Startup Profile Manager and iFIX Projects please refer to the iFIX Electronic Books.



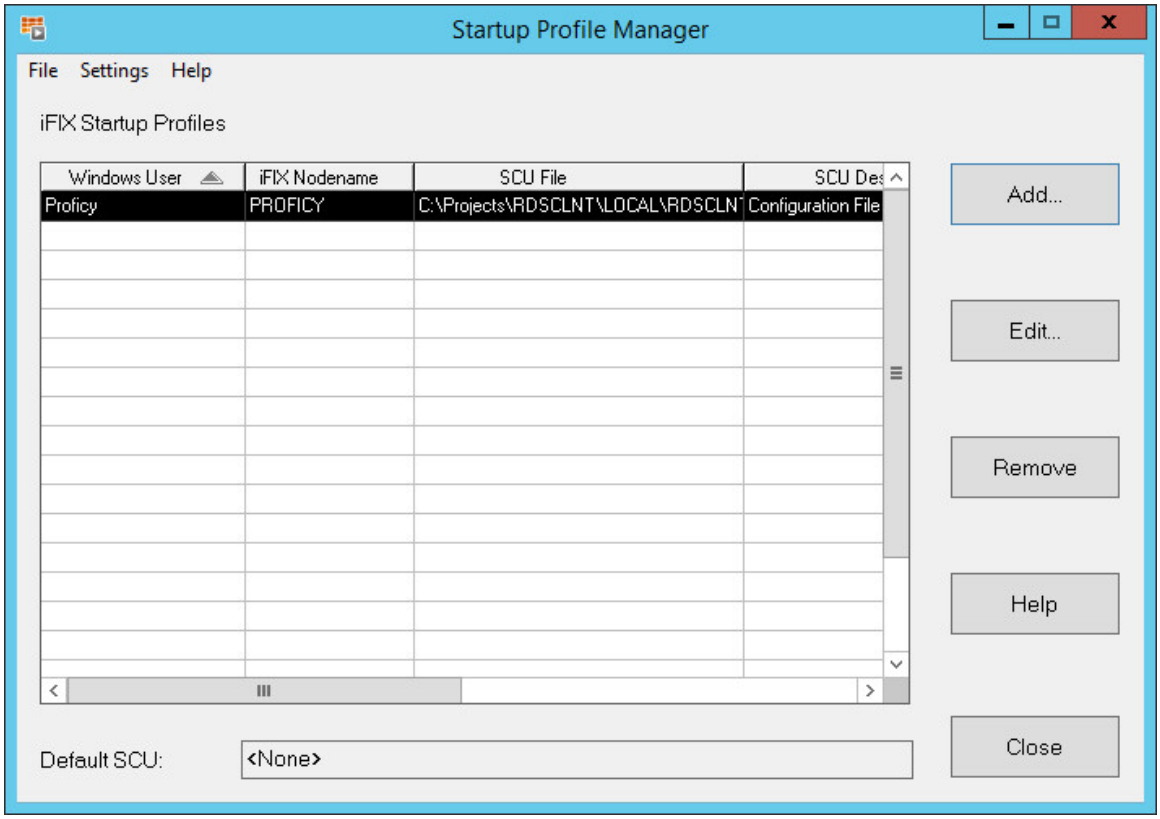
STEP 9: In this application note, we configure a very simple iFIX Terminal Services setup using the Startup Profile Manager. We will configure a default SCU for the iFIX Service and another SCU for the Proficy User that was created in the earlier steps. Click the **Settings** option in the Menu Bar and select **Default Startup Profile** to open the Default Startup Profile options window. In the Default Service SCU section, specify a **Service NodeName** and **Service SCU File**, as pictured below. Click **OK** to accept the changes.



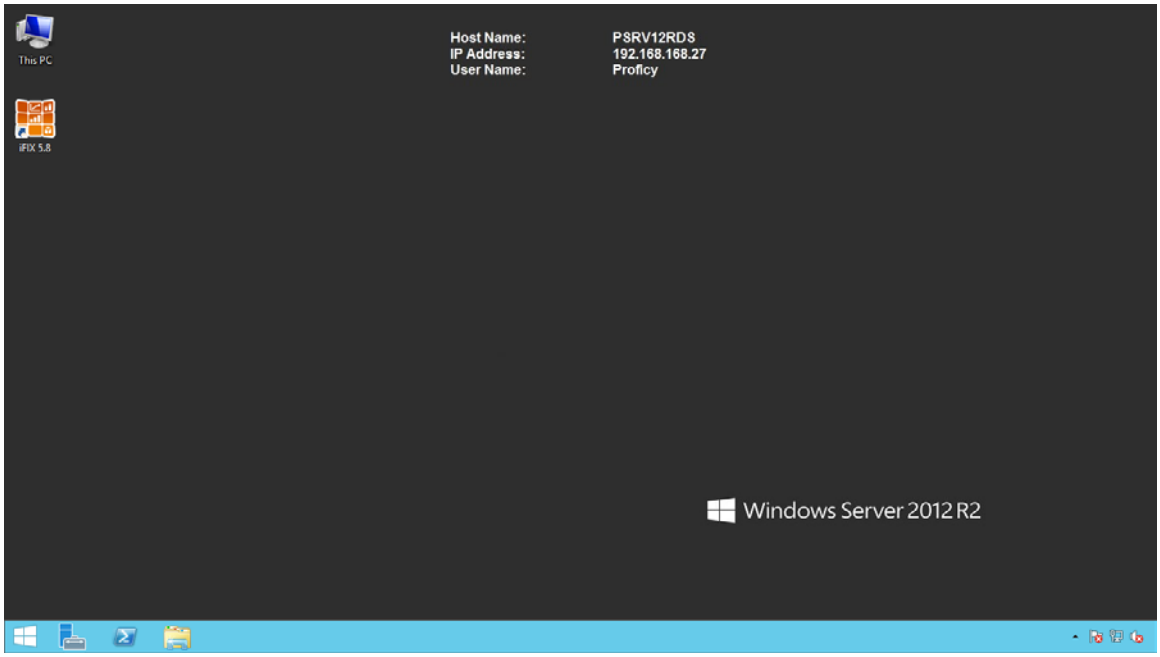
STEP 10: You will now link a profile to the Proficy User. Click the **Add** button to launch the Add Startup Profile window. You will notice you can browse the local computer or the Domain accounts by clicking the **List Domain Members** button. Browse the Domain and select the **Proficy** User that was created earlier. Browse to the RDSCLNT.SCU file that to link these two together, as pictured below. You can edit the other settings if necessary based on the user, click **OK** to accept the changes and add the profile.



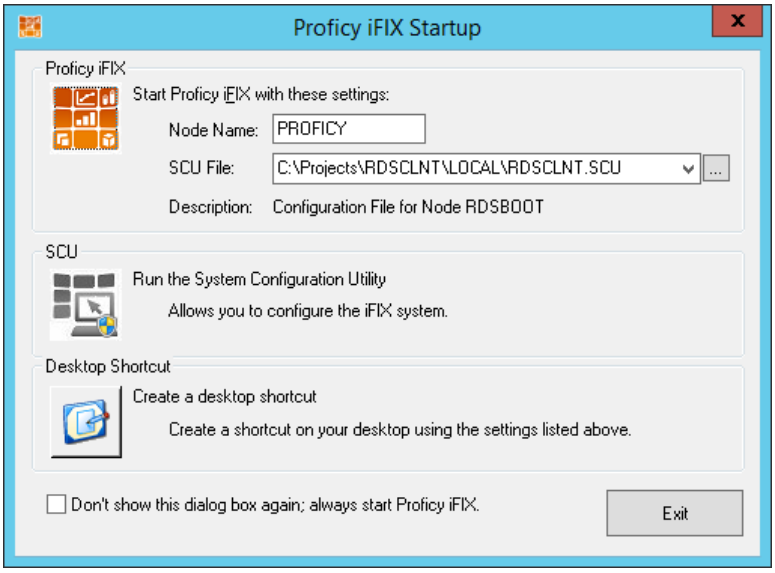
STEP 11: You can add the necessary number of profiles to the Startup Profiles list to fit your system architecture. **Save** the changes in the Startup Profile Manager and click **Close.**



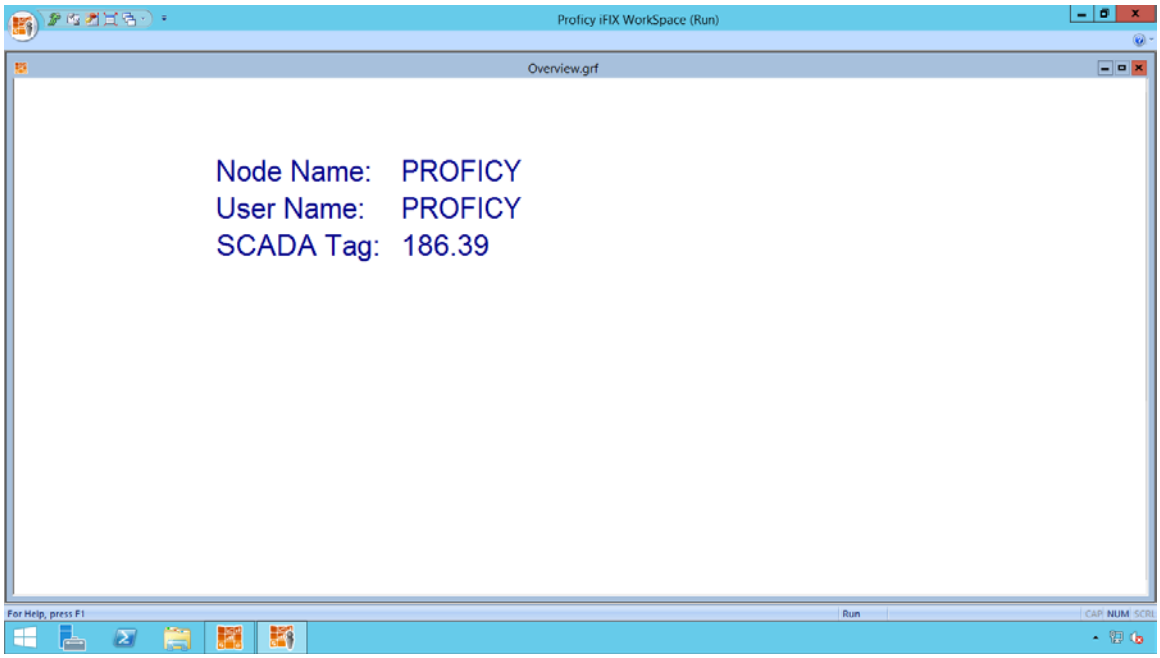
STEP 12: **Launch a Remote Desktop client** session and login to the Remote Desktop Server as the **Proficy** User. Based on the permissions, you will be brought to the Desktop.



STEP 13: Double-click the **iFIX 5.8** icon located on the desktop to open the Proficy iFIX Startup window. Based on the configuration in the Startup Profile Manager, you will see the appropriate node name and SCU file has been linked to this user.



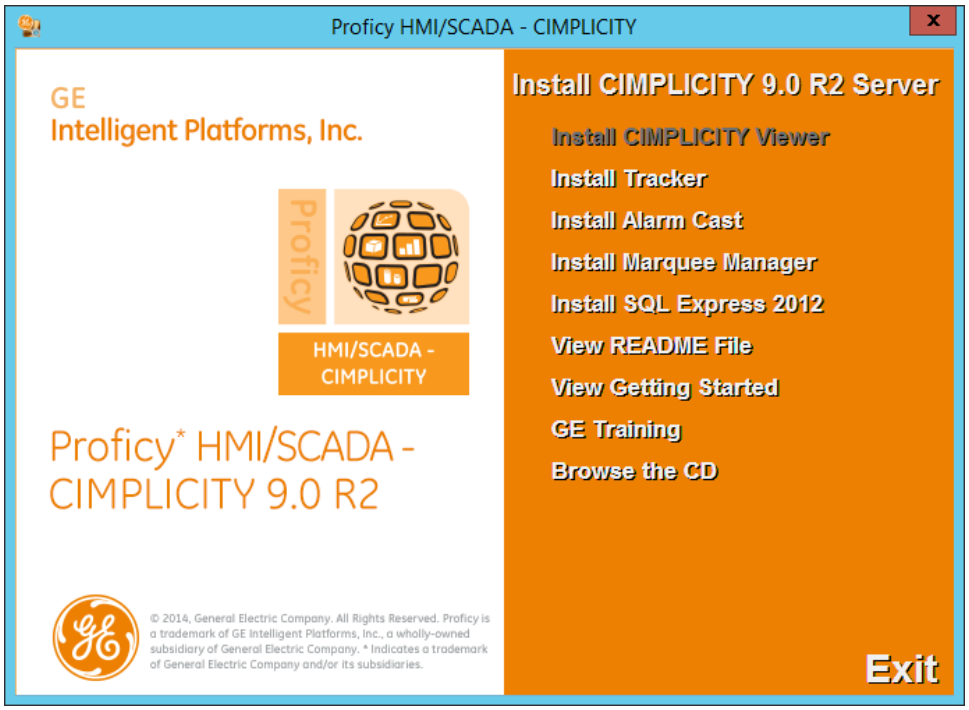
STEP 14: Click the orange **Start Proficy iFIX with these settings** button to launch the iClient session for this user. You will now see the iFIX Remote Desktop session for this user, successfully completing the basics of configuring iFIX in a Remote Desktop Services environment!



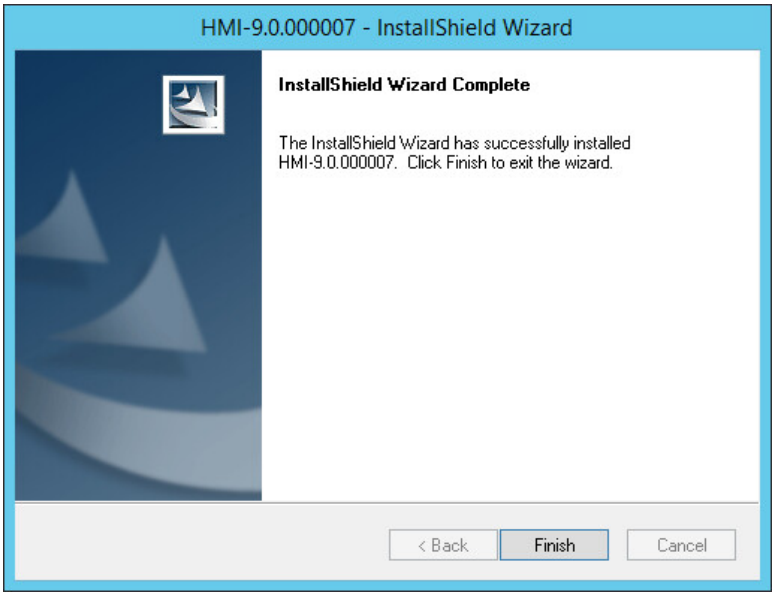
5. Overview of Installing and Configuring GE Proficy HMI/SCADA CIMPLICITY for use in a Remote Desktop Services Environment

This section provides a very high level overview of the steps for deploying Proficy HMI/SCADA CIMPLICITY in a Remote Desktop Services (formerly Terminal Services) Environment. For additional considerations, detailed configurations, compatibility requirements, and best practices when working with Terminal Services please refer to the CIMPLICITY Electronic Books included with the product or available on the GE Support Site: http://support.ge-ip.com

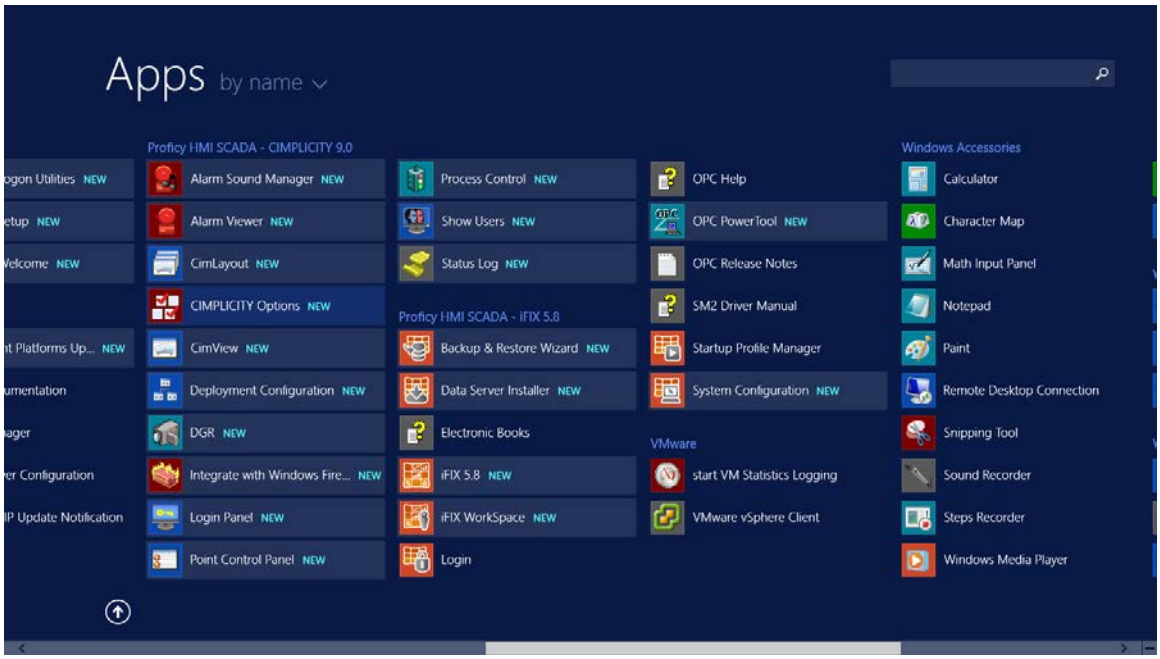
STEP 1: Insert or connect the Proficy HMI/SCADA CIMPLICITY 9.0 R2 media to the Remote Desktop Server computer. Click the **Install CIMPLICITY Viewer** option on the splash screen and follow the prompts to complete the installation. NOTE: You also have the option to perform a full CIMPLICITY Server installation if you require access to the CIMPLICITY development environment like Workbench and CimEdit.



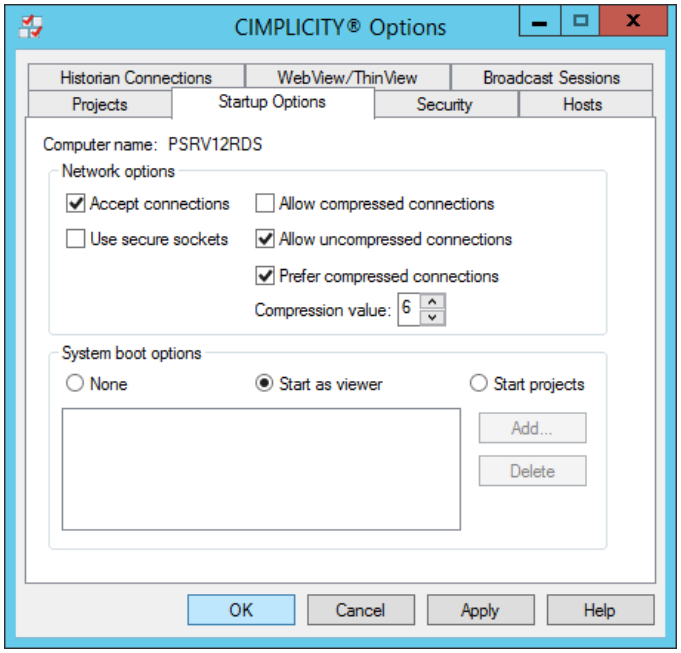
STEP 2: After completing the installation and rebooting, install the latest CIMPLICITY SIM. Follow the prompts to complete the installation process.



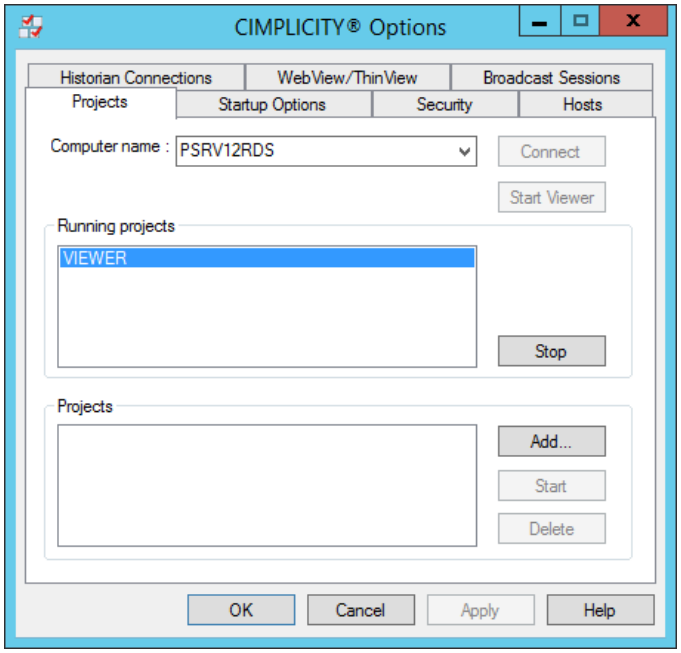
STEP 3: Now you will need setup CIMPLICITY to run as a Windows Service. Click **CIMPLICITY Options** from the Start Screen.



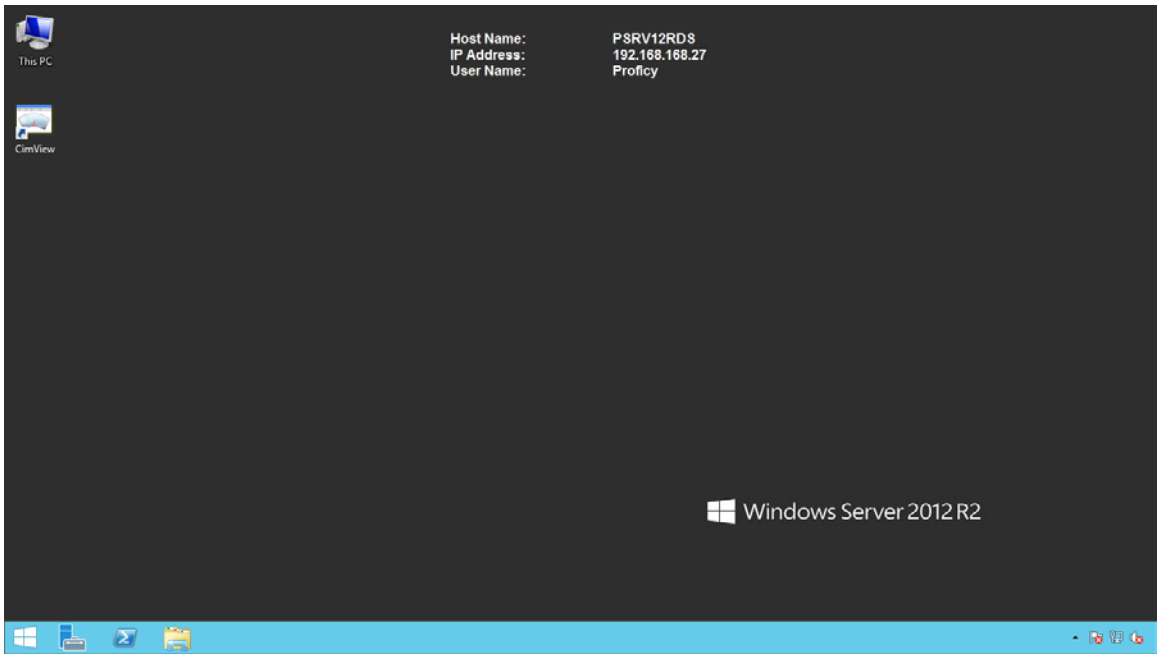
STEP 4: Switch to the **Startup Options** tab and select the **Start as viewer** option in the System boot options section. Click **OK** to accept the changes and reboot the computer.



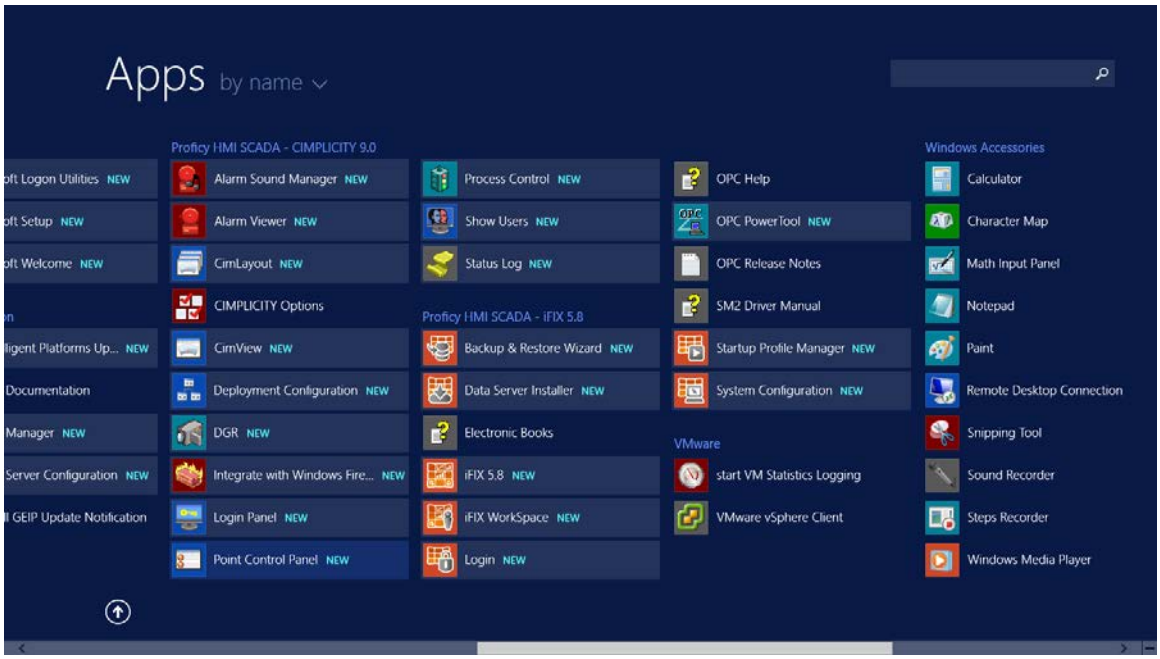
STEP 5: Return to the **CIMPLICITY Options** and confirm that VIEWER is present in the Running Projects list on the Projects tab, as pictured below.



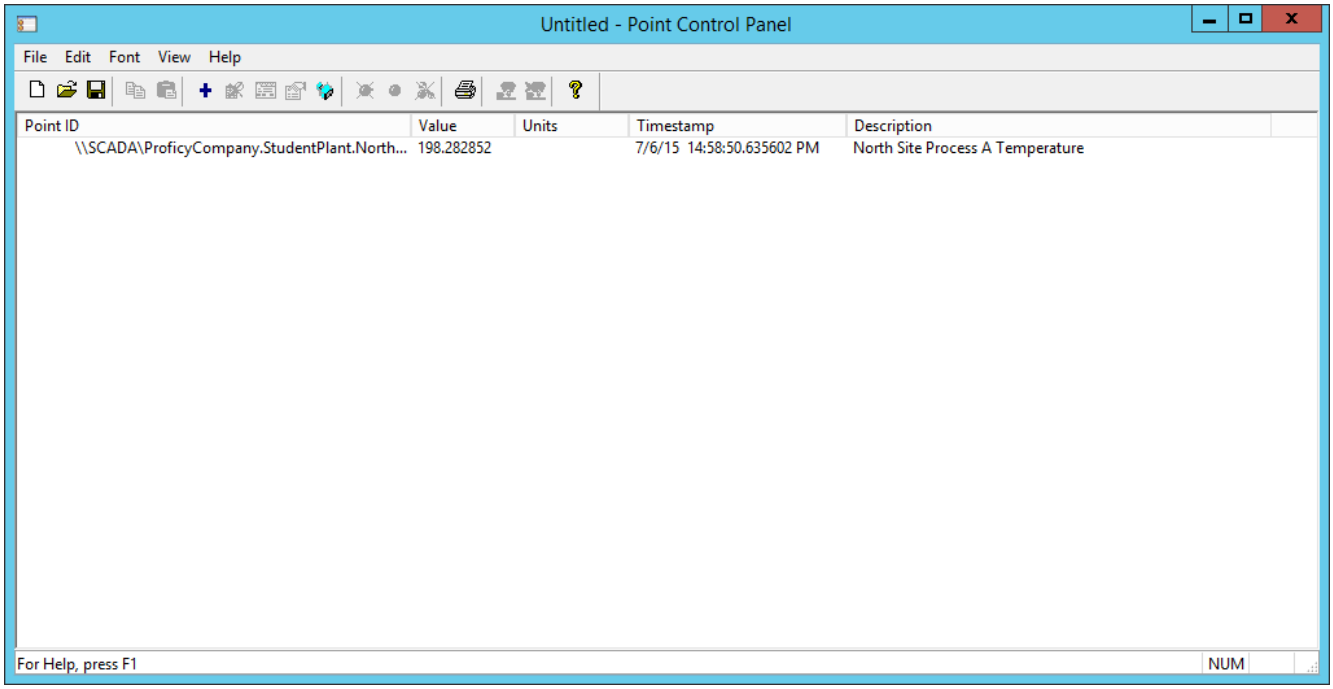
STEP 6: **Launch a Remote Desktop client** session and login to the Remote Desktop Server as the **Proficy** User. Based on the permissions, you will be brought to the Desktop. A CIMPLICITY CimView shortcut was manually copied to the Desktop after installation.



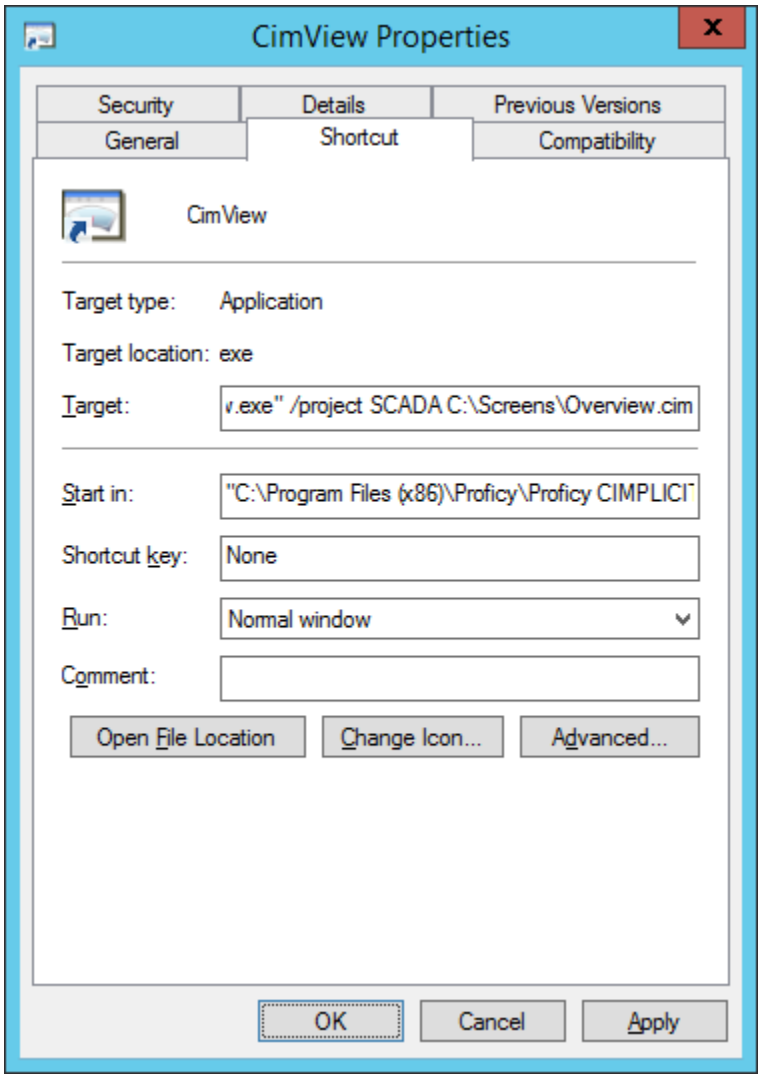
STEP 7: You now can connect to CIMPLICITY projects running on the network. Click **Point Control Panel** from the Start Screen to launch a new Point Control Panel window.



STEP 8: Click the **Add Points** button and browse for your SCADA project and add a Point to confirm communications between the Remote Desktop Server and the SCADA Server.



STEP 9: In order connect to your SCADA server you will need to properly qualify the Points with CimView. Right-click the CimView icon on the desktop open the **Properties**. Edit the Target field to include the **/project** switch and the **path of your initial Screen**, as pictured below. Click **OK** to accept the changes.



STEP 10: Double-click the **CimView** icon on the Desktop. You will now see the CIMPLICITY Remote Desktop session for this user, successfully completing the basics of configuring CIMPLICITY in a Remote Desktop Services environment!