Oracle® Retail XBR Loss Prevention and Store Analytics

Remote Desktop Services Configuration Guide
Release 7.0

August 2015

ORACLE

Oracle® Retail XBR Loss Prevention and Store Analytics Remote Desktop Services Configuration Guide, Release 7.0

Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

(i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.

(ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.

(iii) the software component known as **Access Via™** licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.

(iv) the software component known as **Adobe Flex™** licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.

Contact Information

30500 Bruce Industrial Parkway
Cleveland, OH 44139 USA
Toll Free: 888.328.2826
Tel: 440.498.4414
Fax: 440.542.3043

1800 West Park Drive
Westboro, MA 01581
Tel:508.655.7500
Fax:508.647.9495

7031 Columbia Gateway Drive
Columbia, MD 21046-2289
Tel: 443.285.6000

TABLE OF CONTENTS

OVERVIEW

Note: The rebranding for the latest version of this documentation set is in development as part of post MICROS acquisition activities. References to former MICROS product names may exist throughout this existing documentation set.

This document will guide you through the implementation of Remote Desktop Services on a Windows 2008 R2 server and the deployment of XBR on RD Web Access.

Why Remote Desktop Services?

Remote Desktop Services allows Desktop applications such as XBR to be deployed centrally. This makes patch updates and other maintenance easier for administrators.

Why XBR on Remote Desktop Services?

Windows 2008 Server provides a platform that makes it possible to deploy and publish applications on the web, while keeping the connection secure (e.g. SSL support). This is an effective method for allowing remote users with valid authentication to connect securely to the XBR application from anywhere as long as they have internet connectivity.

Audience

This document is intended for IT staff and Operations/Technical teams who will be implementing and configuring Remote Desktop Services.

System Requirements

The system configurations for the server hosting XBR on Remote Desktop Services should meet the following minimum requirements before installing the Remote Desktop Services roles:

- Windows Server 2008 R2 64-bit Operating System
- .Net Frame work 3.5.1
- Memory minimum 8GB

Client systems connecting to Remote Desktop Services must have the following:

- Windows XP SP3 or Windows 7 (64-bit)
- Internet Explorer 7 or higher
- Active X Plugins in the browser must be enabled

Make sure the latest Operating System service packs are installed on both the server and client.

Do not install the XBR application until the Remote Desktop Services installation has been completed.

About deploying RemoteApp programs through RD Web Access

If you use RD Web Access, you can deploy RemoteApp programs from a single terminal server or farm, or a link to the full terminal server desktop, directly through RD Web Access. All RemoteApp programs on the terminal server or farm that are configured for RD Web Access will appear on the RD Web Access Web site.

Additionally, RD Web Access includes the Remote Desktop Web Connection feature, which allows users to connect from a Web browser to the remote desktop of any server or client computer where they have Remote Desktop access. You can determine whether you want this feature to be available to users.

To deploy RemoteApp programs by using RD Web Access, you must complete the following tasks.

Task	Reference
1. Configure the server that will host RemoteApp programs. This includes installing Terminal Server, installing programs, and verifying remote connection settings.	Configure the server that will host RemoteApp programs
2. Use RD RemoteApp Manager to add RemoteApp programs that are enabled for RD Web Access, and to configure global deployment settings.	Add RemoteApp programs and configure global deployment settings
3. Install RD Web Access on the server that you want users to connect to over the Web to access RemoteApp programs.	Install the RD Web Access role service
4. Add the computer account of the RD Web Access server to the RD Web Access Computers group on the terminal server.	Populate the RD Web Access Computers security group
5. Configure the RD Web Access server to populate its list of RemoteApp programs from a single terminal server or single farm.	Configure the data source for RD Web Access

INSTALLATION OF REMOTE DESKTOP SERVICES

> The steps to install and setup Remote Desktop services may vary according to the security policies and implementation standards of each site. The intent of these steps is to provide a framework around a standard installation for Remote Desktop Services and publishing the XBR application on the web.

Perform the following procedure to install Remote Desktop Services:

1. Log in as an Administrator.
2. Access the Server Manager from Administrative Tools in the Control Panel
3. Add a new role by right-clicking on **Roles** option under Server Manager and select **Add Roles** from the popup menu.
4. Select the **Remote Desktop Services** role and click **Next**.

> If "Web Server (IIS)" is not installed, then select that role as well.

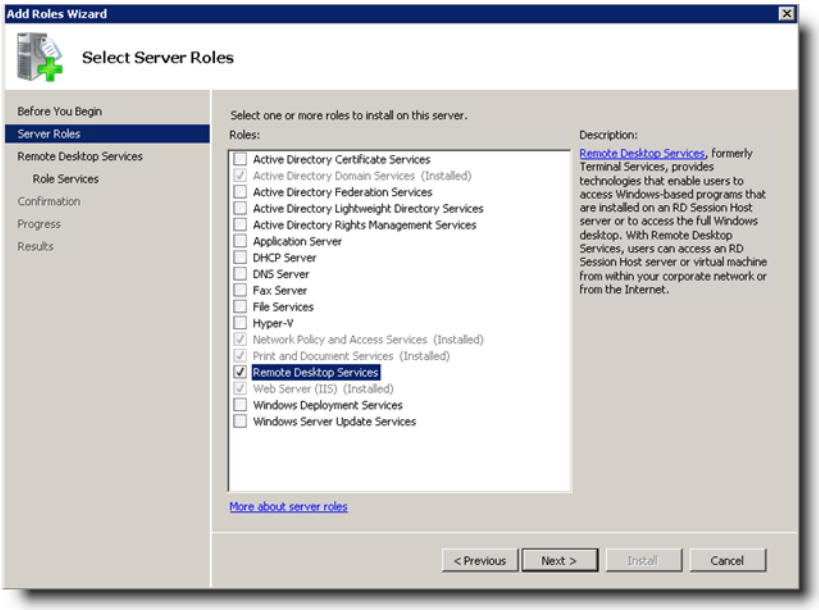


Figure 1-1: Select Server Roles

5. This is an Introduction screen. Click **Next** to continue.

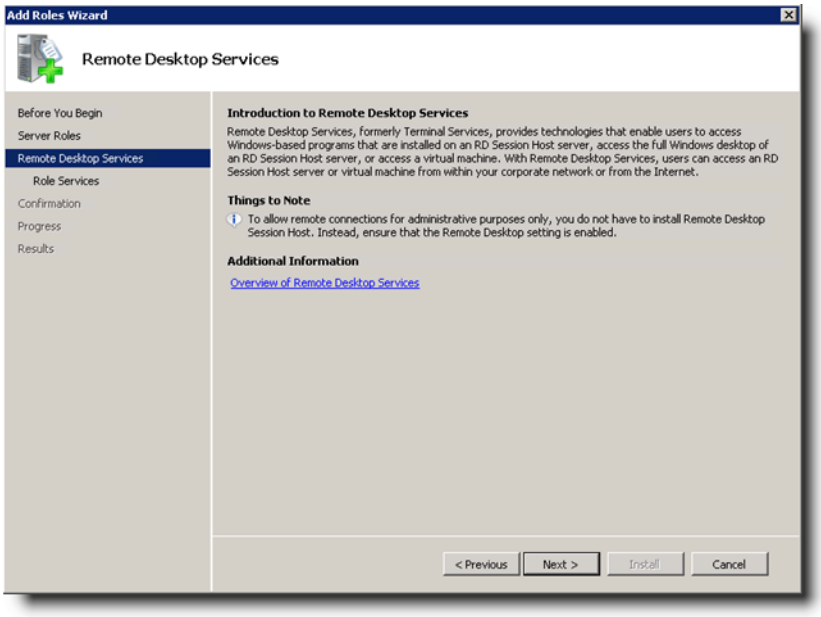


Figure 1-2: Introduction to Remote Desktop Services

6. Click **Next** until you reach the "Select Role Services" option.

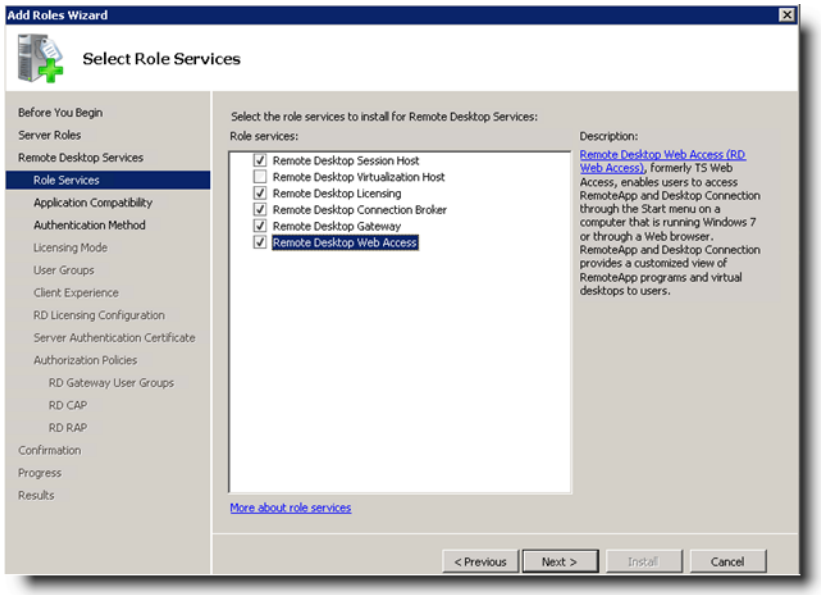
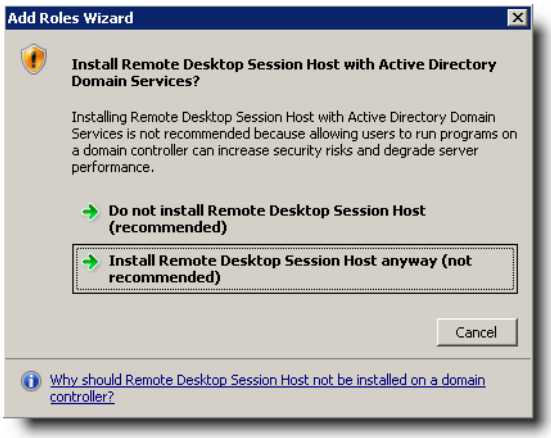


Figure 1-3: Role Services

Select the following Roles services:

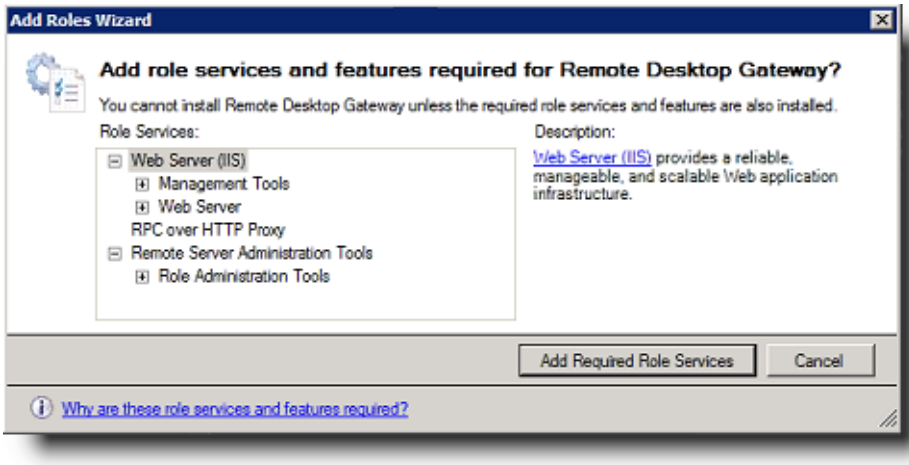
- Remote Desktop Session Host.

When selecting this option, you may receive the warning shown at the right. Select the second option to "Install Remote Desktop Session Host anyway."



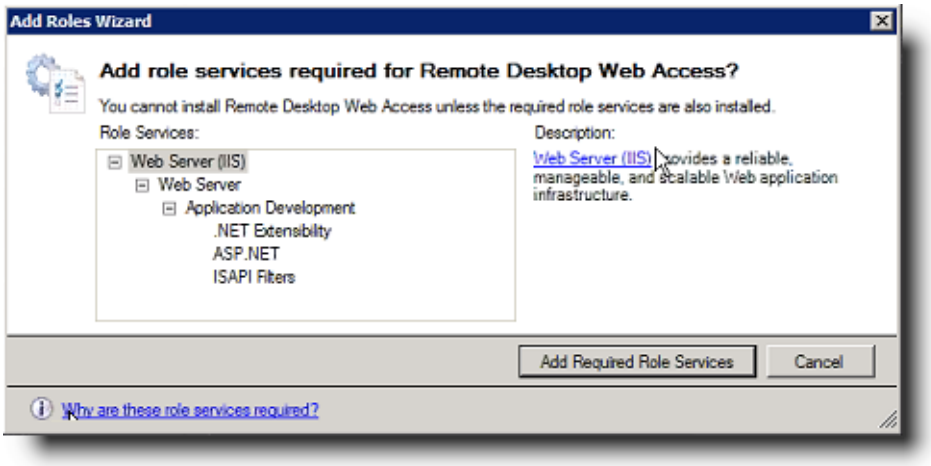
- Remote Desktop Licensing.
- Remote Desktop Connection Broker.
- Remote Desktop Gateway

When selecting this option, you may receive the warning shown below. Select **Add Required Role Services**.



- Remote Desktop Web Access

When selecting this option, you may receive the warning shown below. Select **Add Required Role Services**.



Once these roles are selected, click **Next**.

7. You may receive the following warning screening alerting you that Remote Desktop Session Host should be installed prior to installing the applications that will be accessed remotely (i.e. - XBR). Click **Next**.

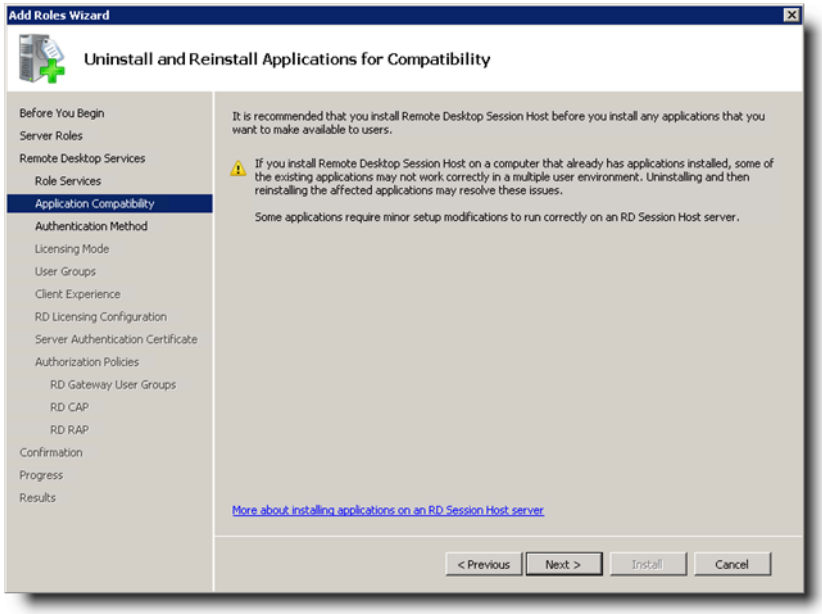


Figure 1-4: Remote Desktop Session Host Warning

8. Select **Do not require Network Level Authentication** for the Authentication Method.

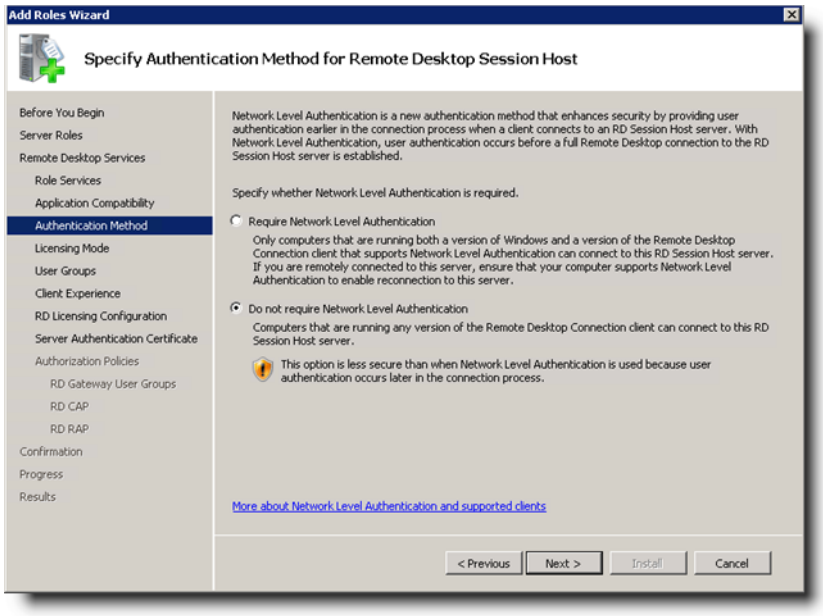


Figure 1-5: Authentication Method

9. If the following screen is displayed, select either **Per Device** or **Per Use** license for the Licensing Mode and click **Next**. The option you select depends on the license model you have purchased.

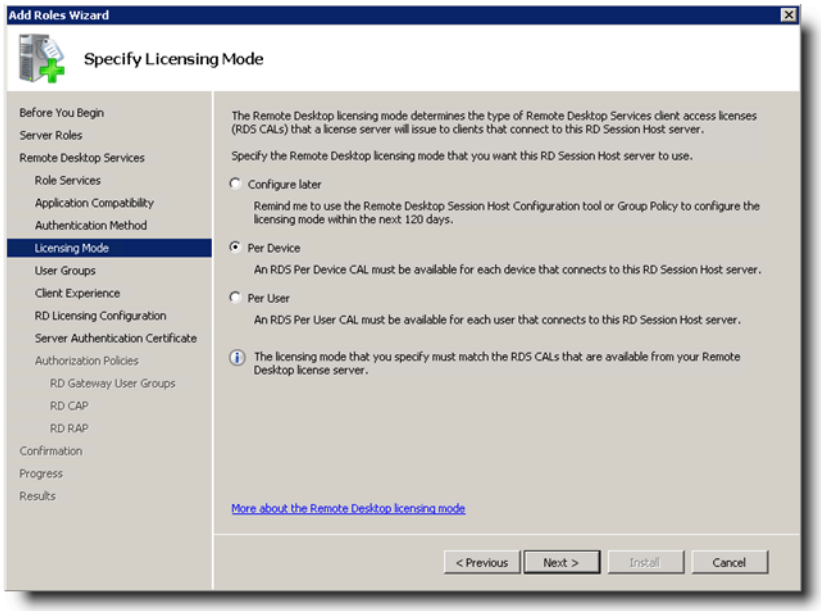


Figure 1-6: Licensing Mode

If you have set up licensing through a Group Policy, you will see the following screen, click **Next**.

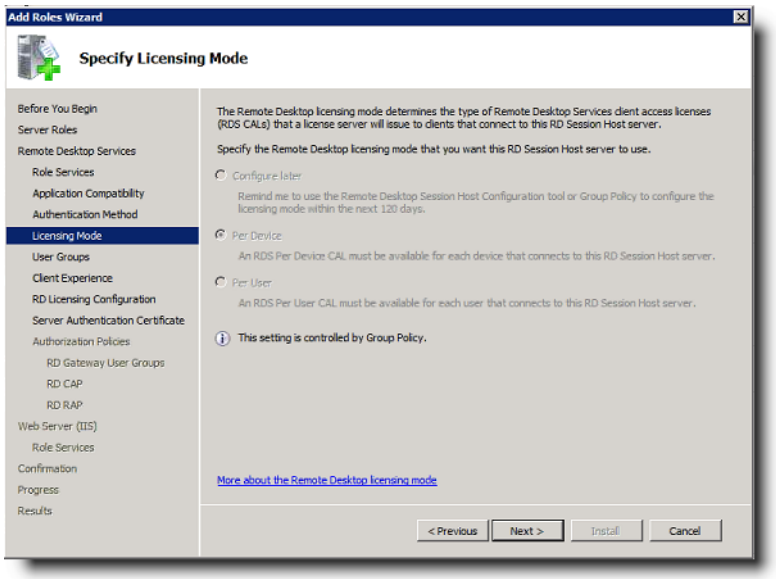


Figure 1-7: Licensing Controlled by Group Policy

10. Select the Users or User Groups that are going to connect to RD Session Host Server and click **Next**.

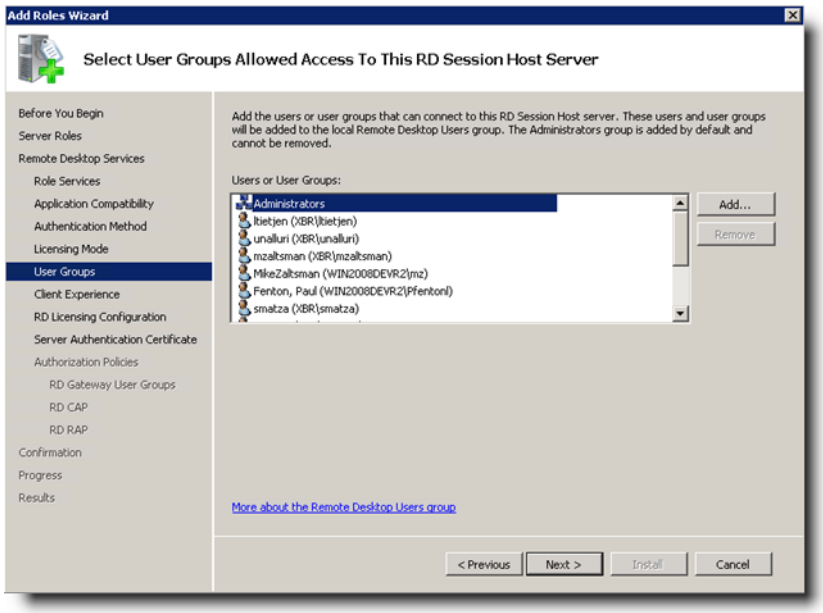


Figure 1-8: Users/User Groups Allowed Access

11. Leave all options on the Client Experience screen unchecked and click **Next**.

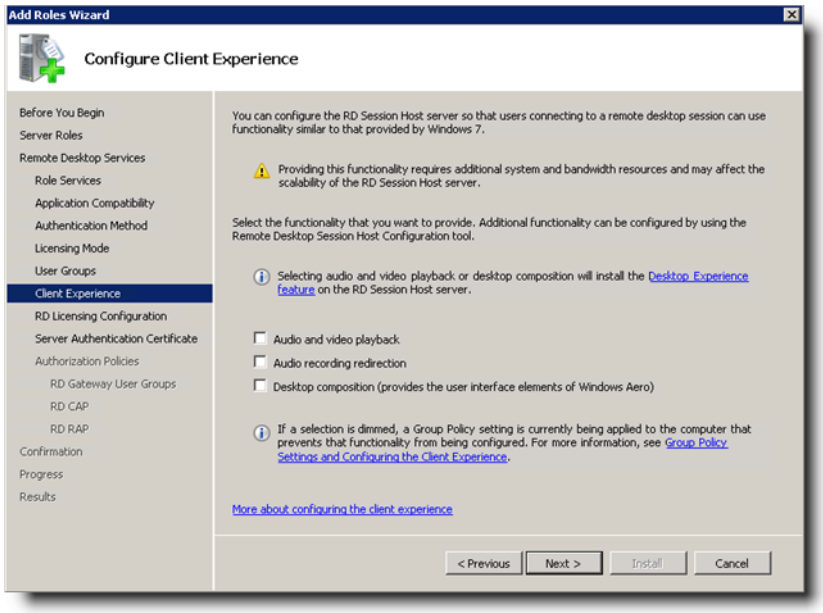


Figure 1-9: Client Experience

12. On the *Configure Discovery Scope for RD Licensing* window, select **Configure a discovery scope for this license server**, choose **This domain**, and click **Next**.

If the License Server is already populated, you do not need to configure a Discovery Scope. Click **Next**.

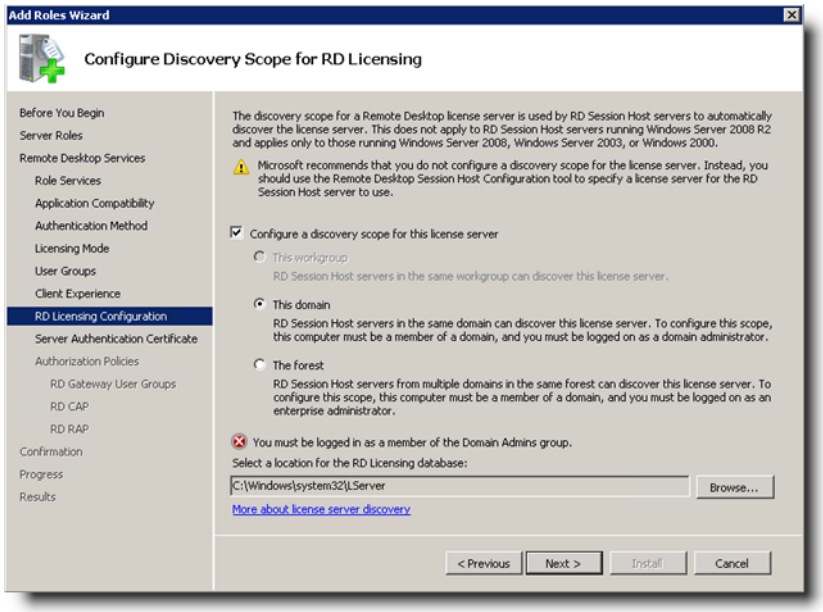


Figure 1-10: Discovery Scope for RD Licensing

13. When selecting a Server Authentication certificate:

If the SSL certificate already exists, select **Choose an existing certificate for SSL encryption**, select the applicable certificate, and click **Next**.

If the SSL certificate does not already exist, you can **Import** the certificate at this time or select **Create a self-signed certificate** and click **Next**.

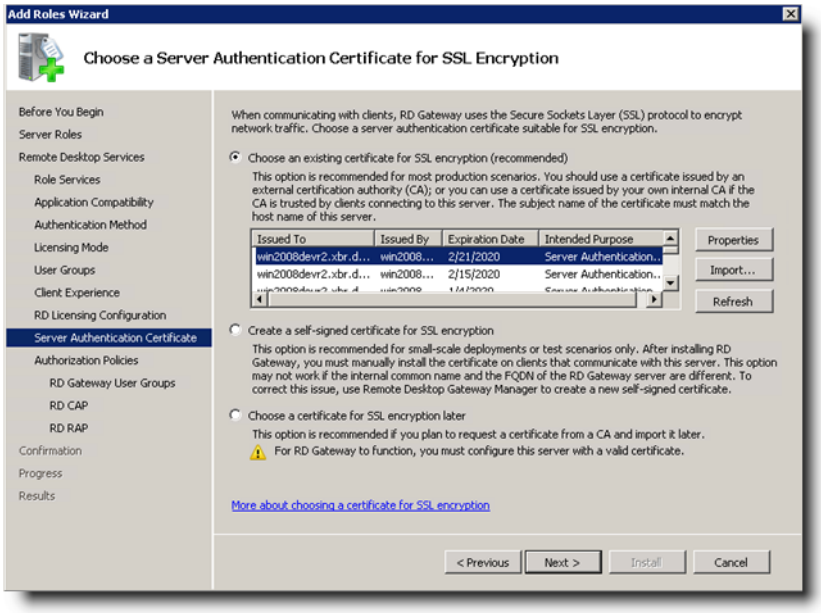


Figure 1-11: SSL Server Authentication Certificate

14. Select **Now** to create the authorization policies for the RD Gateway and click **Next**.

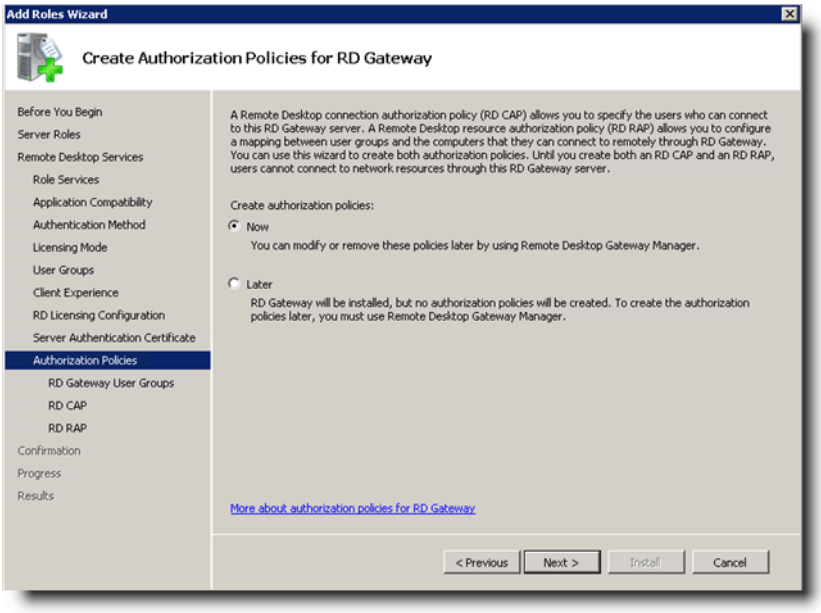


Figure 1-12: Authorization Policies

15. Select the User groups who should be able to Authorize through RD Gateway Server and click **Next**.

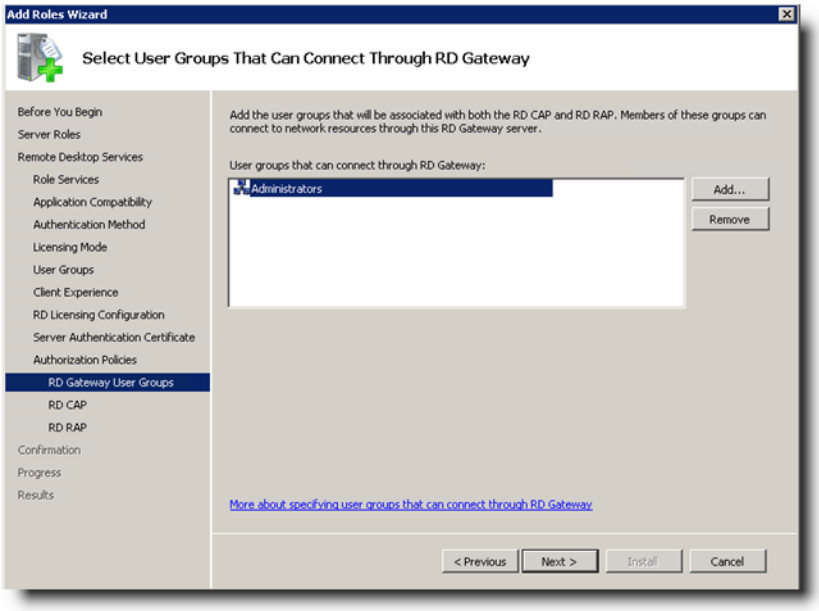


Figure 1-13: User Groups That Can Connect Through RD Gateway

16. Enter a name for the RD Connection Authorization Policy (CAP), check **Password** for the authentication method, and click **Next**.

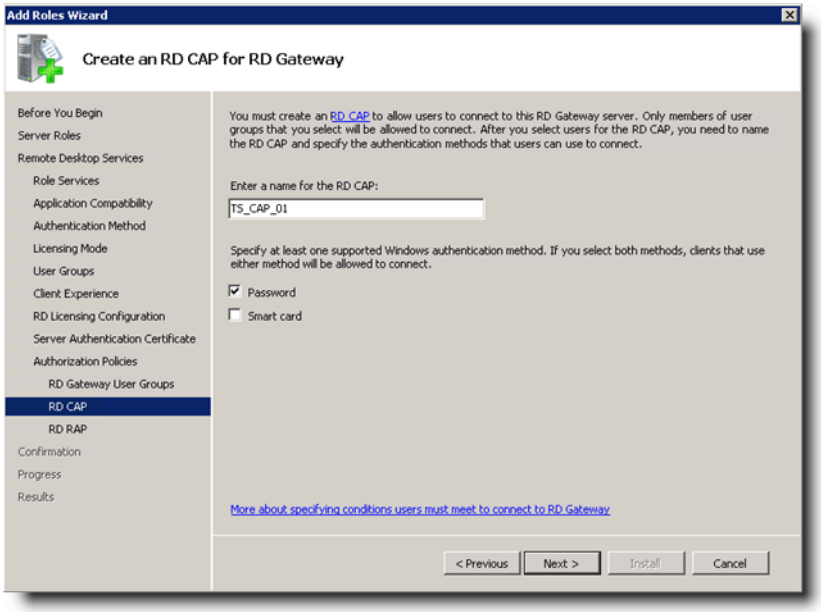


Figure 1-14: RD CAP for RD Gateway

17. Enter a name for the RD Resource Allocation Policy (RAP), select the computers from which you can connect to the RD Gateway (use the Browse button if necessary), and click **Next**.

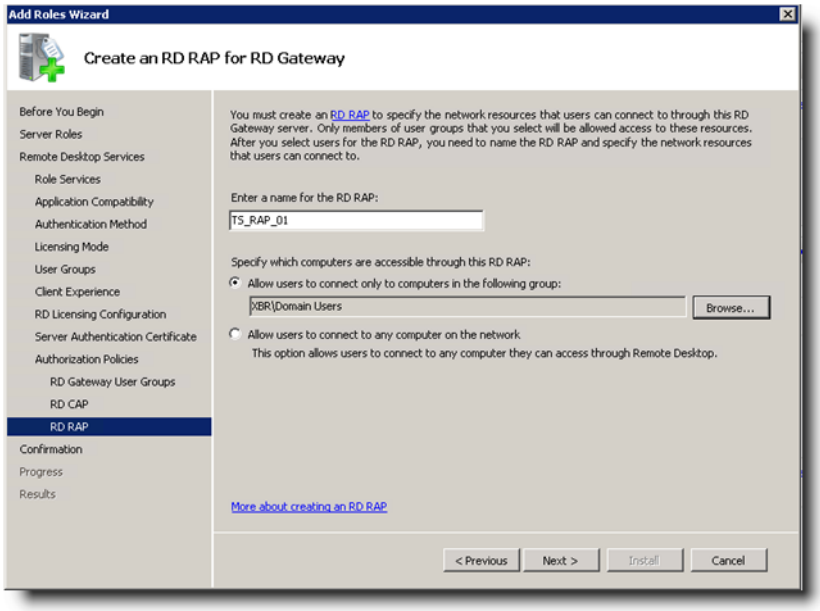


Figure 1-15: RD RAP for RD Gateway

18. If Web Server (IIS) needs to be installed, you will see the screen shown below. Click **Next**.

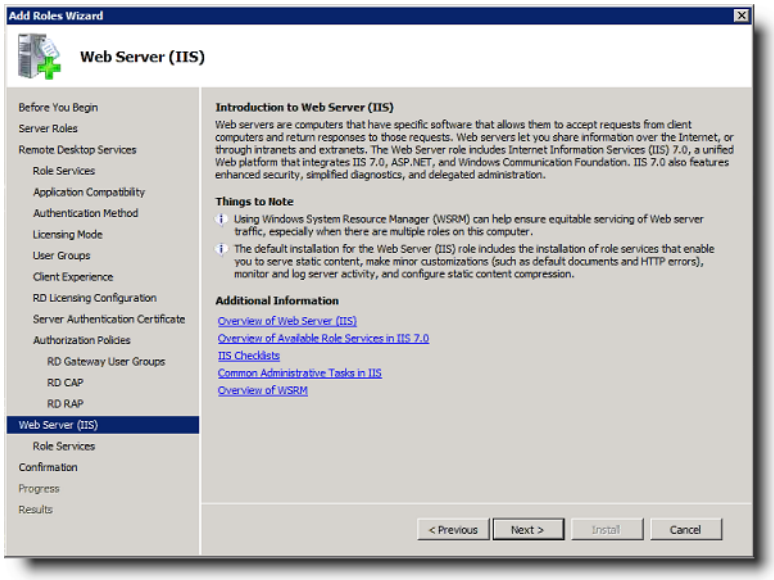


Figure 1-16: IIS Introduction

19. Accept the defaults and click **Next**.

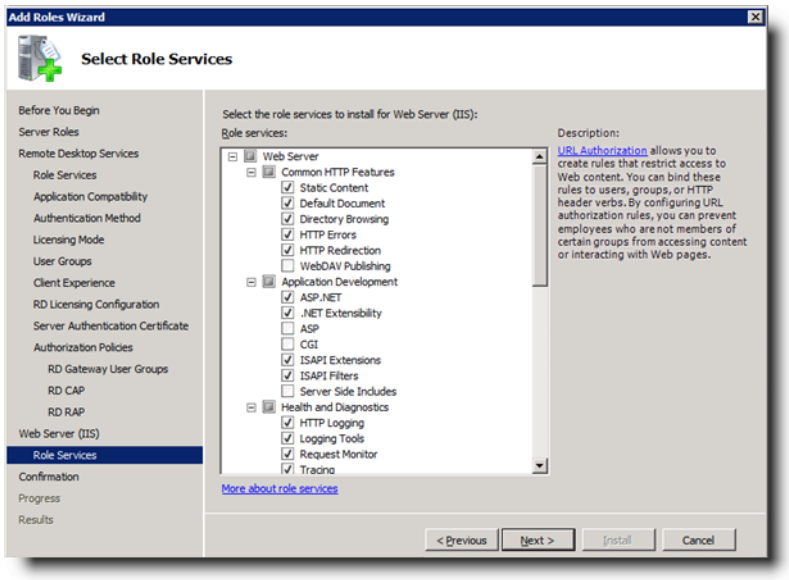


Figure 1-17: IIS Role Services

20. You will see a confirmation screen similar to the one below prior to the installation starting. Confirm the options and click **Install**.

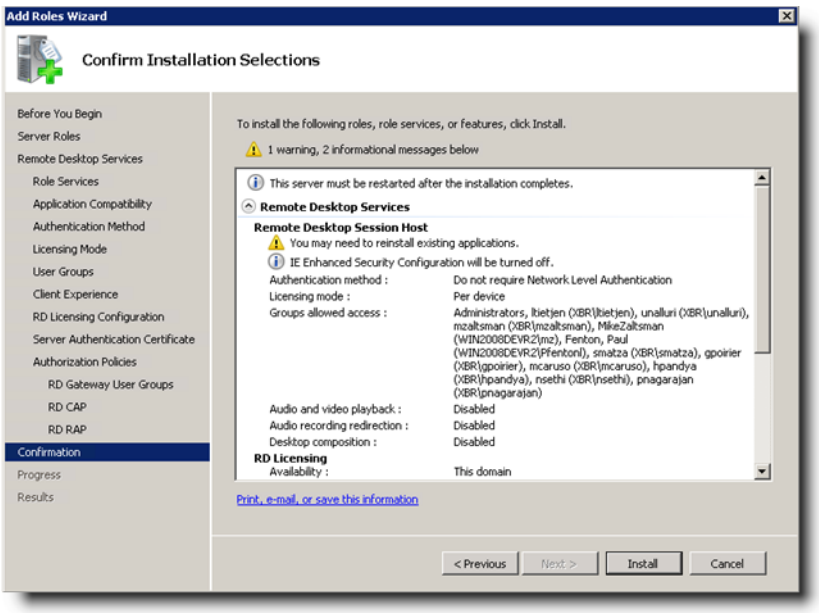


Figure 1-18: Confirm Installation Selections

21. Once the installation is complete, you will be prompted to restart the computer. Click **Close**.

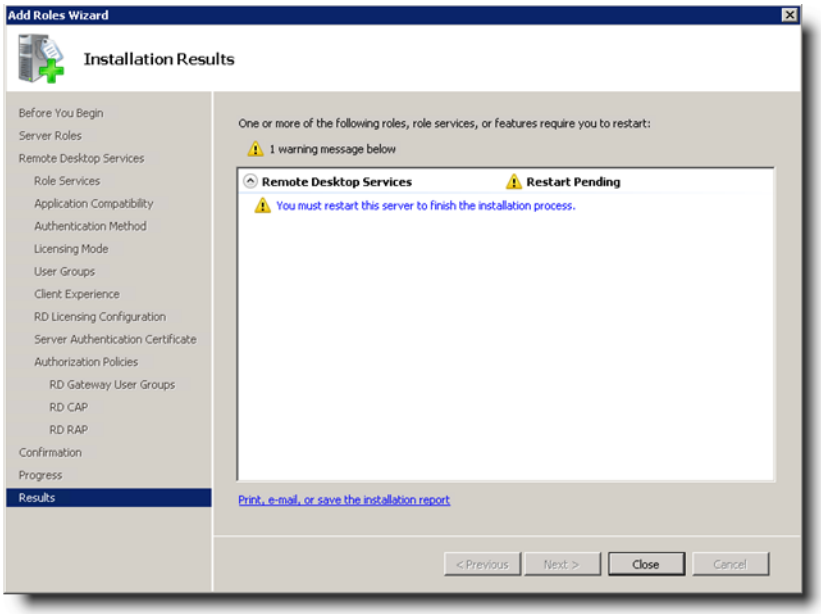


Figure 1-19: Installation Results

Sometimes after a restart, the License service may not start due to invalid authentication associated with the service. Check the status of the Licensing service before proceeding further.

22. After the computer restarts, installation and configuration will continue. When the installation and configuration is complete, you will see a window that shows the list of components that were installed successfully. Click **Close** to complete the installation.

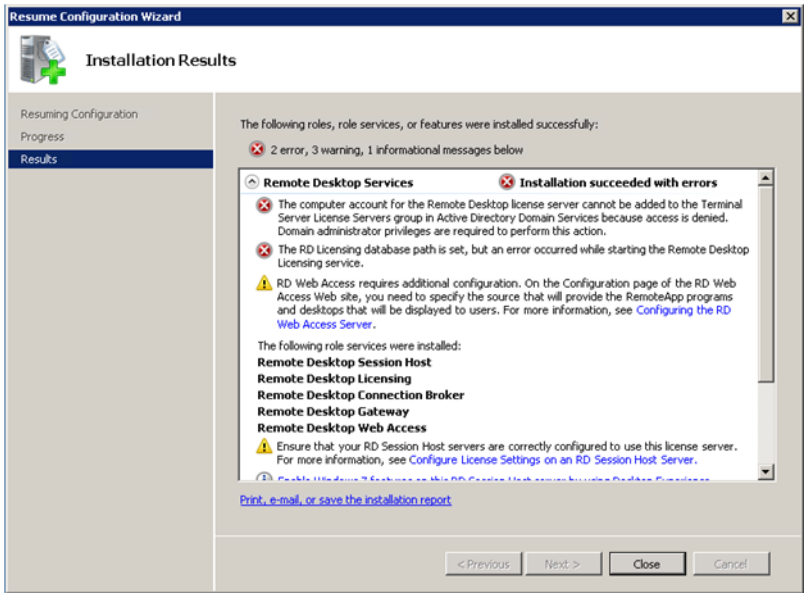


Figure 1-20: Installed Components

XBR INSTALLATION

> *If you have not set up the Remote Desktop Services Role, please return to "Installation of Remote Desktop Services" on page 3 and set up the role before installing the XBR Desktop application.*

Now that the Remote Desktop Services installation has been completed, the XBR application should be installed so it can be configured for Remote Access. Use the following steps to install the XBR Desktop application:

1. Select **Control Panel -> Programs**.
2. Click **Install Application on Remote Desktop**.

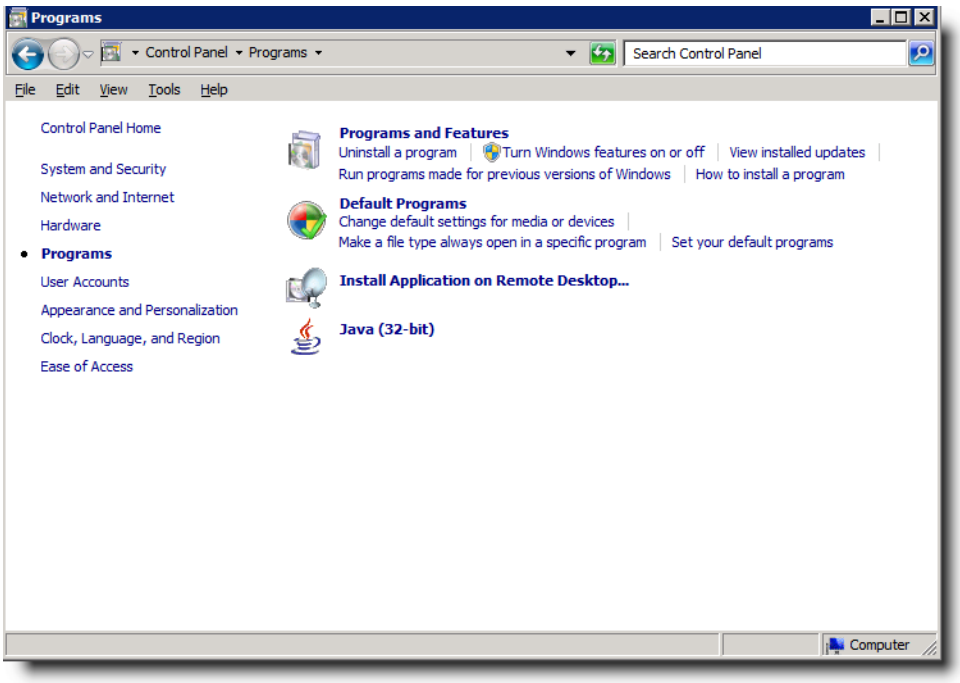
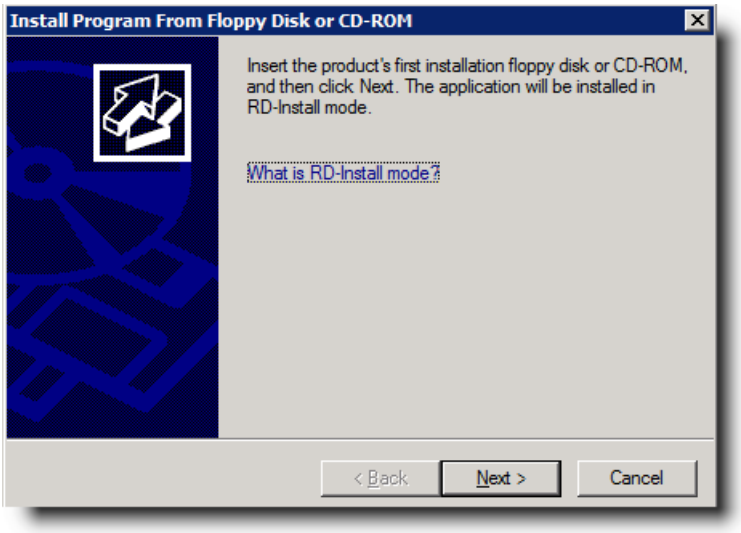


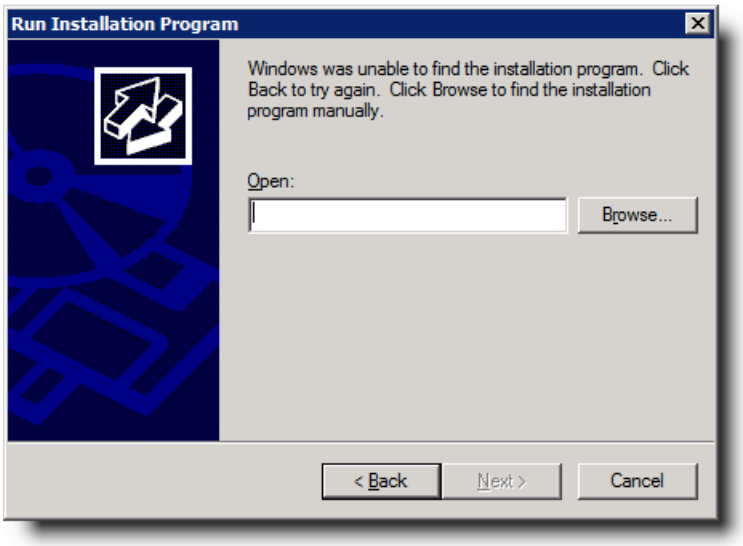
Figure 1-21: Control Panel - Programs

3. Insert the XBR Installation CD into the CD-ROM drive.

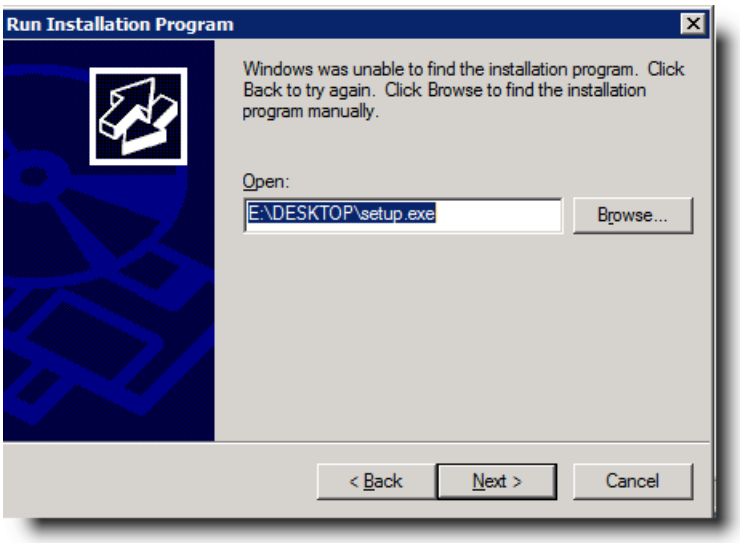
4. Click **Next**.



5. The Application Installer will not be able to find the XBR installation file:
   a. Click **Browse**.
   b. Navigate to the Installation CD.
   c. Select `setup.exe`.

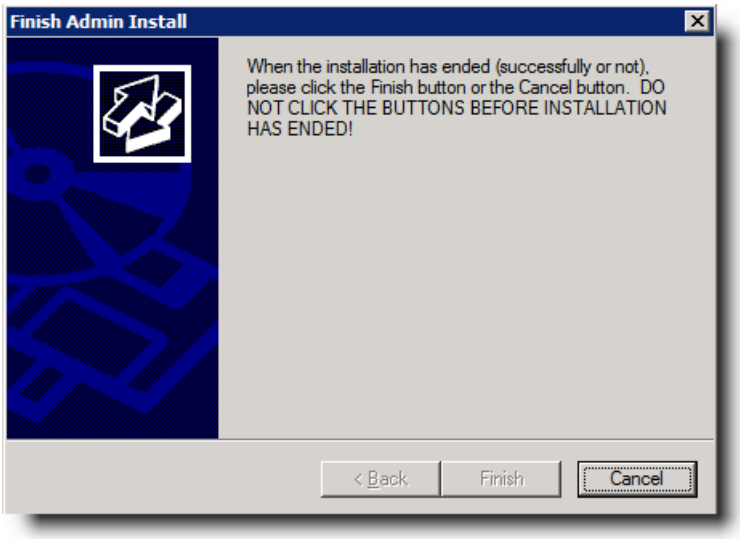


6. Click **Next**. The XBR installation will begin.



7. Follow the instructions in the XBR Implementation Guide as the XBR Desktop Installation Wizard progresses.

8. When the XBR Desktop installation is complete, click **Finish**.



CONFIGURE REMOTEAPPS FOR RD WEB ACCESS

Once XBR has been installed, it must be installed onto the RD Gateway server so the application can be configured as a RemoteApp. This will allow it to be launched from the Windows Server 2008 RD Web Access page.

Applications are configured as RemoteApps using the RD RemoteApp Manager which is accessed by selecting **Control Panel -> Administrative Tools -> Remote Desktop Services-> RemoteApp Manager**.

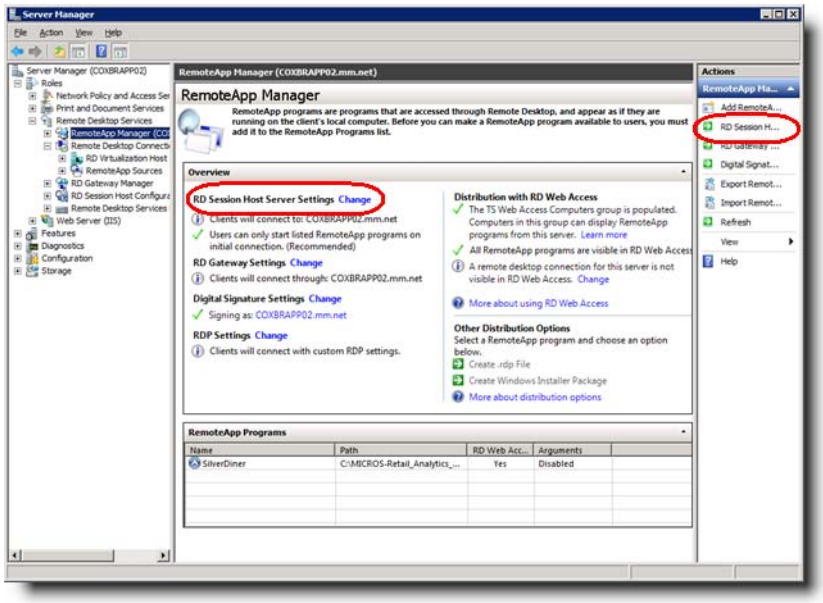


Figure 1-22: RemoteApp Manager

Configure RemoteApp Deployment Settings

1. In the Action menu section of RemoteApp Manager, click **RD Session Host Server Settings** or click **Change** next to **RD Session Host Server Settings** in the Overview pane. Refer to Figure 1-22 for locations.

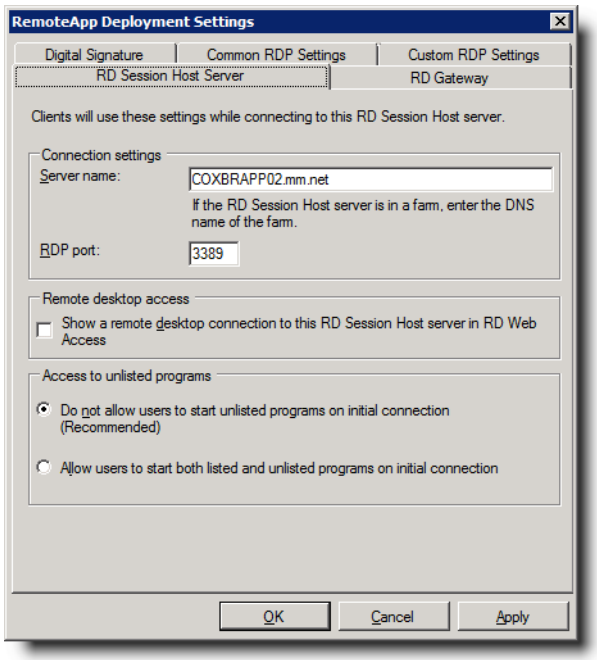
2. Select the RD Session Host Server tab and perform the following settings:

   a. Modify the server name to be the fully qualified internal domain name.

   b. Leave the Remote Desktop Protocol (RDP) port number as 3389.

   c. Uncheck **Show a remote desktop connection to this RD Session Host server in RD Web Access**.

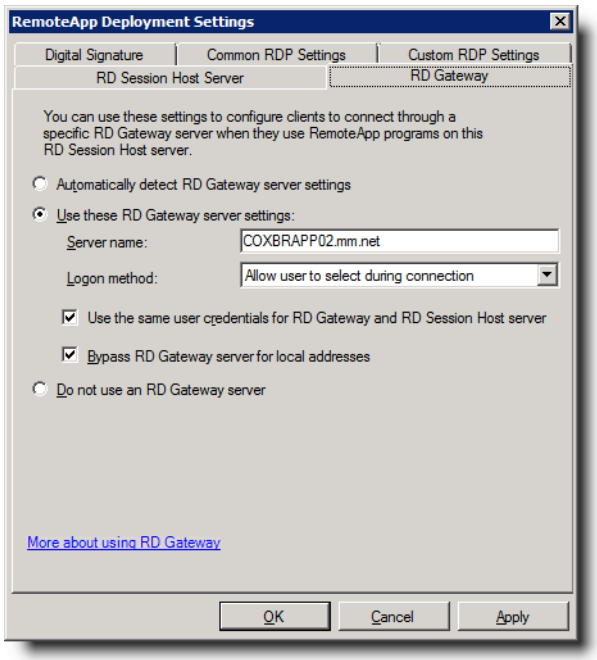
   d. Select **Do not allow users to start unlisted programs on initial connection (Recommended)**.



3. Select the RD Gateway tab where you can configure the desired RD Gateway behavior. You can configure whether to automatically detect RD Gateway server settings, to use RD Gateway server settings that you specify, or to not use a RD Gateway server.

   a. Select **Use these RD Gateway server settings.**

   b. Enter/verify the RD Gateway server name (RDGateway.company.com) and the logon method (Ask for password (NTLM)).

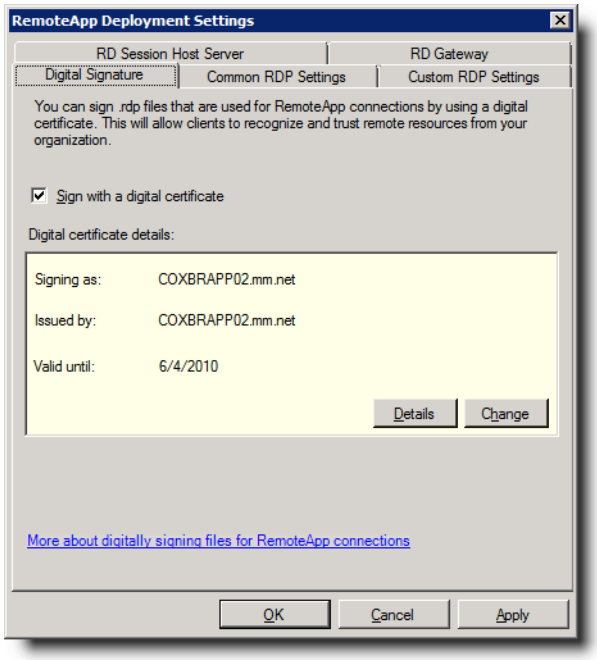


The server name must match what is specified in the SSL certificate for the RD Gateway Server.

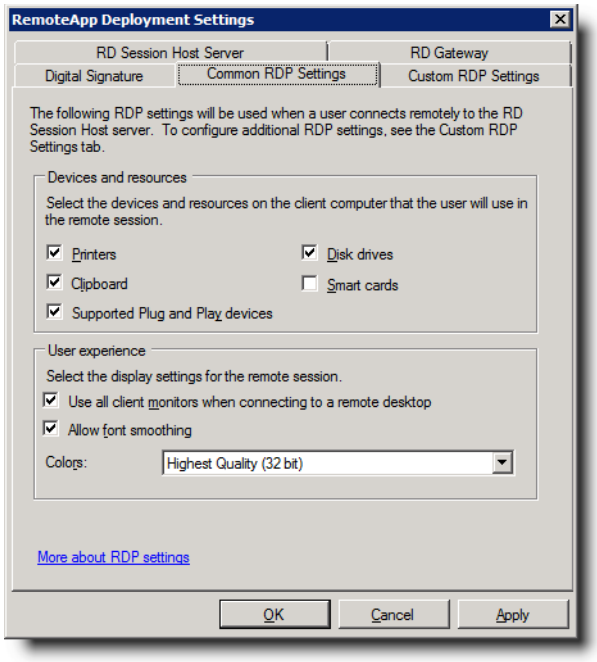
   c. Check **Use the same user credentials for RD Gateway and RD Session Host server**.

   d. Check **Bypass RD Gateway server for local addresses**.

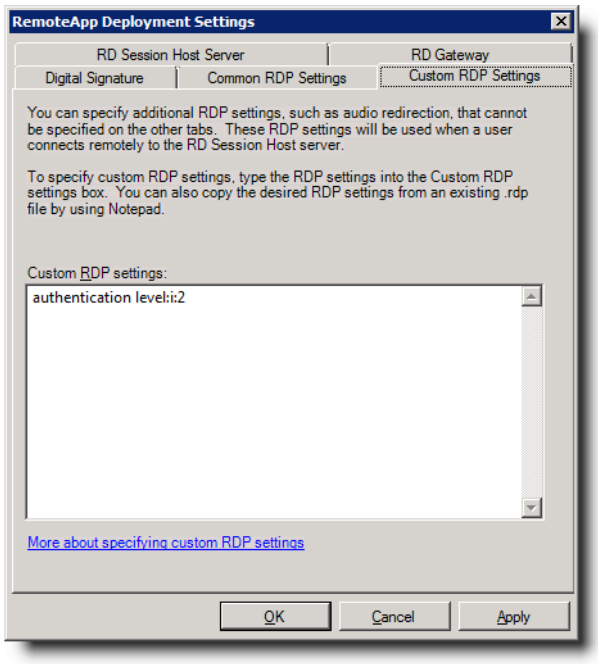
4. If you did not select SSL certification during the initial installation, it can be configured now:
   a. Select the Digital Signature tab.
   b. Check **Sign with a digital certificate**.
   c. In the Digital certificate details box, click **Change**.
   d. In the Select Certificate dialog box, select the appropriate certificate (i.e. - RDGateway.company.com).



5. Select the Common RDP Settings tab and make sure the options are set as shown in the figure to the right.



6. Select the Custom RDP Settings tab and make sure the custom RDP settings are set as shown in the figure to the right.



See link for more details: http://tehnet.microsoft.com/en-us/library/cc731249.aspx.

7. Click **OK**.

XBR Application Access

User Security Setup

- Each user connecting via Remote Desktop Services needs to be a domain user. Therefore, each user account that needs access to the Terminal Server must be added to the domain.
- Each new customer must have a new group created with the three letter customer OrgCode. This group will be used to handle security for all users of this customer.

In the US, the PTS customer code should be used for the OrgCode.

Add New Customers

1. Create a new local group on the server with the customer's OrgCode.
2. Request or create a new Domain user for that customer and assign the user(s) to the group created in step 1.
3. Create a new export folder for the customer as a sub-folder of:

   `C:\MICROS-Retail_Analytics_7.0\Analytics_export\Analytics_userfolders\XXX`

   where “XXX” is the customer OrgCode.

It is important that the name of the folder matches the customer OrgCode in the database and the `dtvanalytics.ini` file. In the US, this should be the PTS customer code.

4. Create a copy of the `dtvanalytics.ini` file and rename it using the customer OrgCode (i.e. - `dtvanalytics_xxx.ini`).
5. Modify/check the `dtvanalytics_xxx.ini` file for the following information:
   a. [XBR Database] section - make sure that the entries for Server Name and Database settings are pointing to the correct database/server for this customer
   b. [ORGANIZATION] section- modify the OrgCode parameter for this customer.

   ```
   [ORGANIZATION]
   OrgCode=XXX
   ```

   c. [TERMINAL] section- make sure that the Terminal setting is set to 'Y' and append the OrgCode to the Export path after Analytics_userfolders

   ```
   [TERMINAL]
   Terminal = Y
   Export = ..\Analytics_export\Analytics_userfolders\XXX
   ```

   d. [other] section- modify the setting for the Table Editor configuration file to a unique file for this customer.

   ```
   TableINI=dtvEditor_XXX.ini
   ```

6. Create a copy of the `dtveditor.ini` file and rename it using the customer OrgCode (i.e. `dtveditor_xxx.ini`).
7. Modify the `dtveditor_xxx.ini` file:

a. [ORGANIZATION] section- modify the OrgCode parameter for this customer:

```
[ORGANIZATION]
OrgCode=XXX
```

b. [TERMINAL] section- make sure the Terminal setting is set to 'Y' and append the OrgCode to the Export path after Analytics_userfolders:

```
[TERMINAL]
Terminal = Y
Export = ..\Analytics_export\Analytics_userfolders\XXX
```

c. [other] section- modify the setting for the XBR Analytics configuration file to a unique file for this customer.

```
XBRLPINI=dtvanalytics_xxx.ini
```

8. Create a new shortcut for the XBR application executable (`dtvanalytics.exe`) and name it appropriately with the customer's OrgCode. The shortcut should use the customer `dtvanalytics_xxx.ini` file as a passed parameter.

9. Assign group "XXX", created in step 1, the following permissions:

a. `C:\` - Read&execute; list; read permissions

b. `..\Micros_Retail_Analytics_7.0` directory - Read&execute; list; read permissions

c. `..\XBR` directory - Read&execute; list; read permissions

d. `..\Table_Editor` directory - Read&execute; list; read permissions

e. `..\Query_Viewer` directory - Read&execute; list; read permissions

f. `..\Analytics_export` directory - Read&execute; list; read permissions

g. `..\Analytics_userfolders` subdirectory - Read&execute; list; read permissions

h. `..\XXX` subdirectory (created in step 3) - Read&execute; list; read; write permissions

DISTRIBUTE WITH RD ACCESS

1. In the Action menu option of the RemoteApp Manager, select "Add RemoteApp Programs" in order to add the applications or their shortcuts to the RD Web Access. This will display the RemoteApp wizard. Click **Next**.

Figure 1-23: RemoteApp Wizard - Welcome

2. Select the appropriate XBR application shortcut to be published from the list or select its location using the **Browse** button.

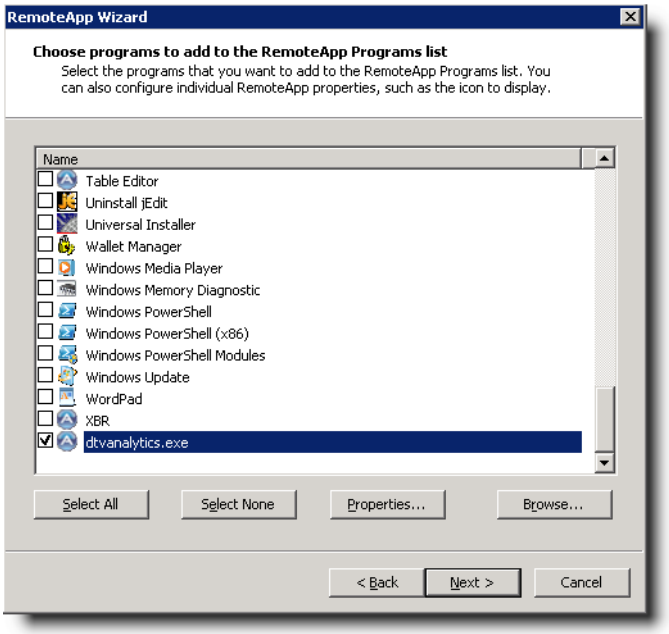


Figure 1-24: RemoteApps Program List

a. After selecting the XBR application shortcut, click the **Properties** button.

b. Make sure **RemoteApp is available through RD Web Access** box is checked.

c. Enter the Customer OrgCode (i.e. XXX) in the **Alias** field and click **OK**.

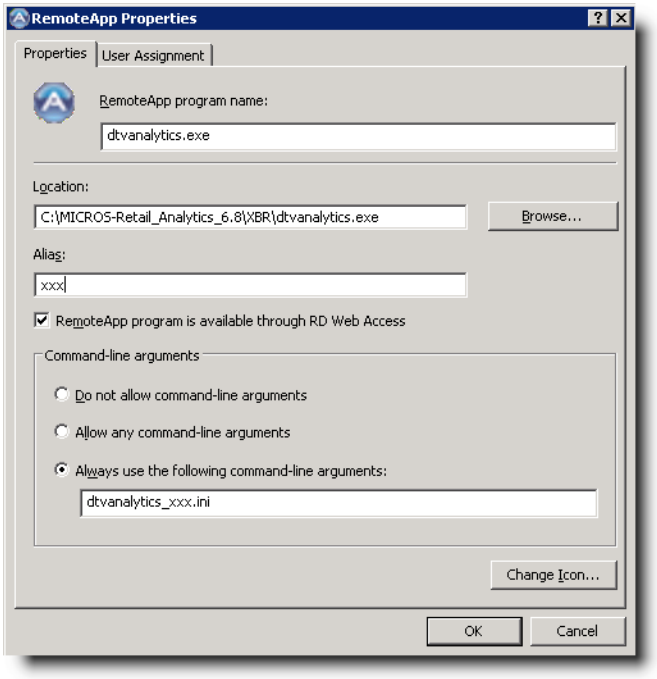


Figure 1-25: RemoteApps Program List - Properties

3. Click **Finish** to complete the configuration.

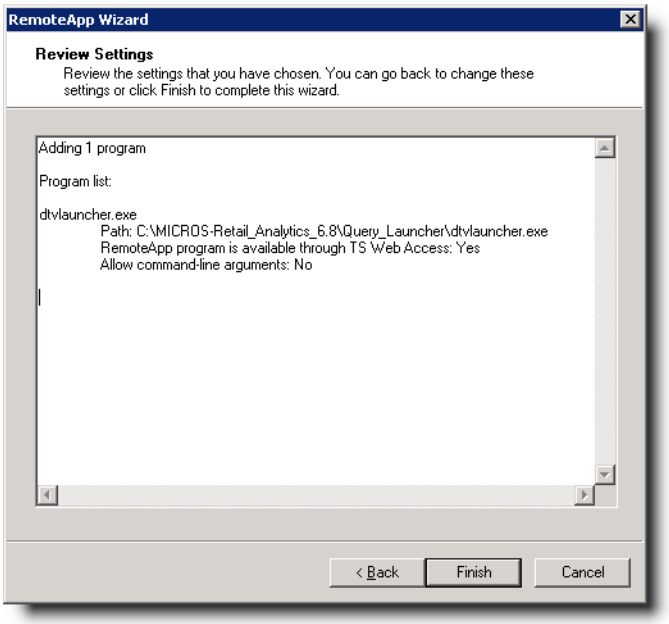


Figure 1-26: Review Settings

The application properties can be modified by right-clicking on the application in **RemoteApp Programs** and selecting **Properties**".

4. After finishing the configuration of publishing the application, right-click on the newly added shortcut under **RemoteApp Programs** and select **Show in RD Web Access**. This will publish the application on the web.

Similarly, the **Hide in RD Web Access** option can be selected to remove the application from the web.

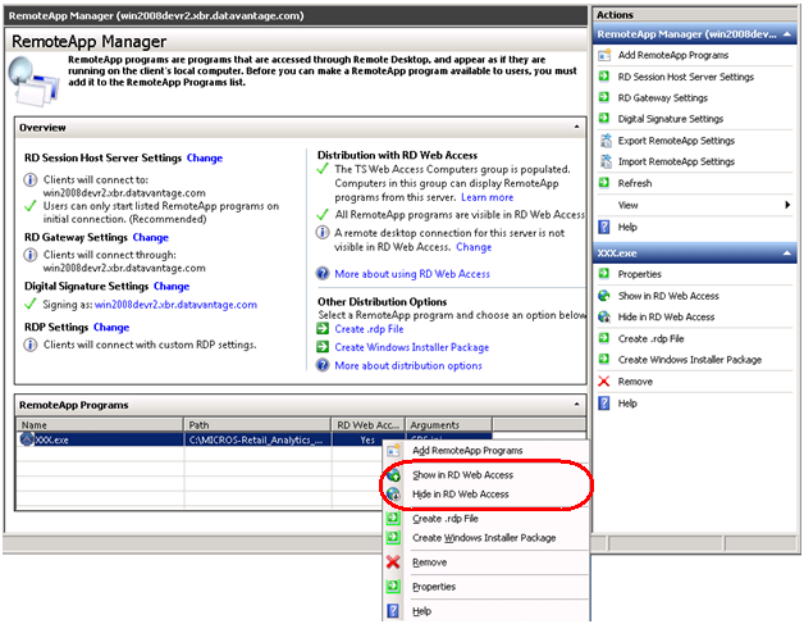


Figure 1-27: RemoteApp Manager - Publish

User Access to Specific Application

1. In the application **Properties** window, under the *User Assignment* tab, users can be added to access a specific application, thus securing the application from unauthorized access.
2. Select the specific domain users and/or domain groups and click **OK.**

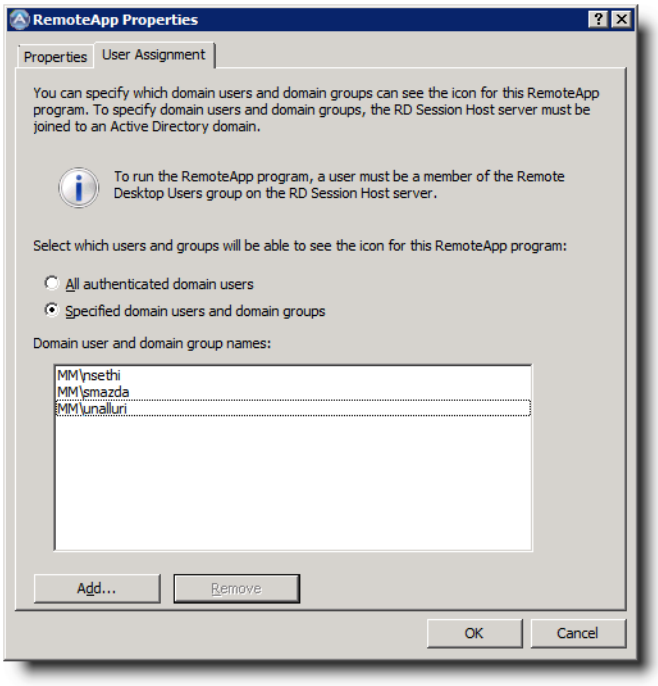


Figure 1-28: User Assignment for Application

Users and groups can be added by clicking the **Add** button.

Remote Desktop Services Web Access - Client Access

Launch RD Web Access

1. Launch Internet Explorer and go to a fully qualified domain name that points to the server IP address (e.g. https://xbrdc-micros-retail.com/RDWEB).
2. Login using Username (domain\user) and Password (network password).

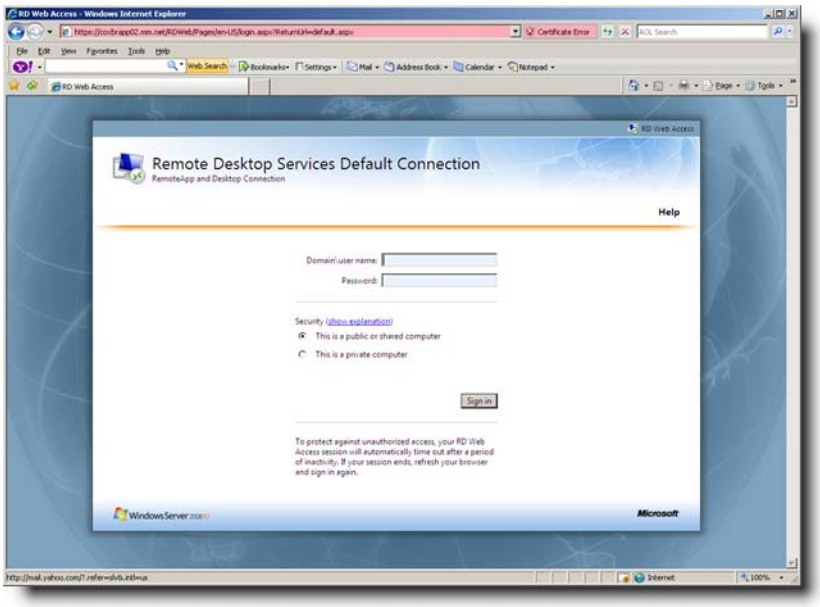


Figure 1-29: Remote Desktop Services Default Connection

Install Active X Client Control

3. If you are prompted to run the **Remote Desktop Services ActiveX Client control** from your browser when you access RD Web Access, do either of the following, depending on your operating system:
   - **a.** If you are running Windows Server 2003 or Windows XP:
     - **1)** Right-click on the message line in the browser.
     - **2)** Click **Run ActiveX Control**.
     - **3)** Click **Run**. After you have enabled the control, refresh the Web page.
   - **b.** If you are running Windows Server 2008 or Windows Vista:
     - **1)** Click the warning message on the Internet Explorer Information bar.
     - **2)** Point to Add-on Disabled and click **Run ActiveX Control**.
     - **3)** When you do this, you may see a security warning. Make sure that the publisher for the ActiveX control is "Microsoft Corporation" before you click **Run**.
   - **c.** If the Internet Explorer Information bar does not appear, you can enable the ActiveX control by using the Manage Add-ons tool on the Tools menu of Internet Explorer.

4. After logging into the browser, you will see the published application shortcut. Double-click on the icon.

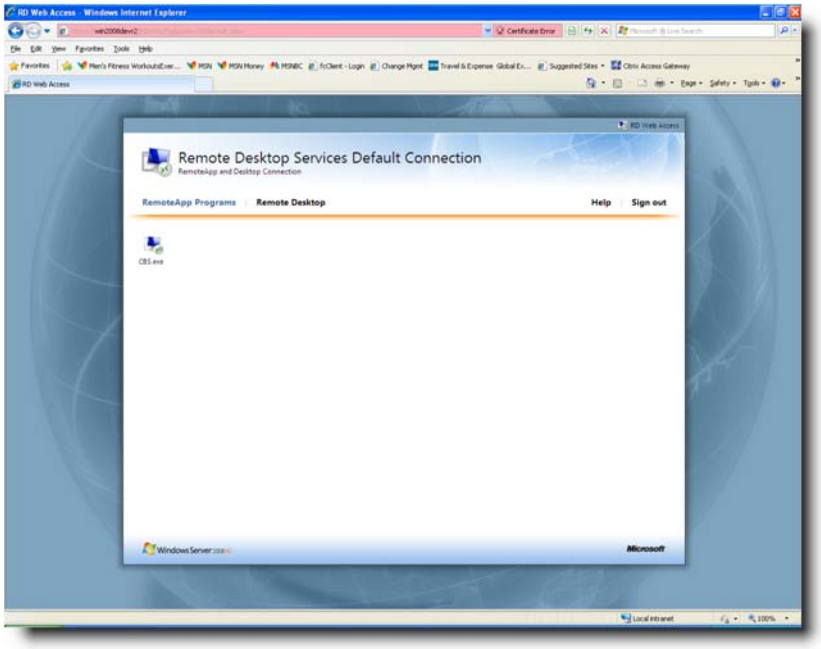


Figure 1-30: Application Shortcut

5. In order to access your local resources from the terminal server, make sure that **Drives**, **Clipboard**, and **Printers** are all selected.

6. Click **Connect** and re-authenticate against the network.

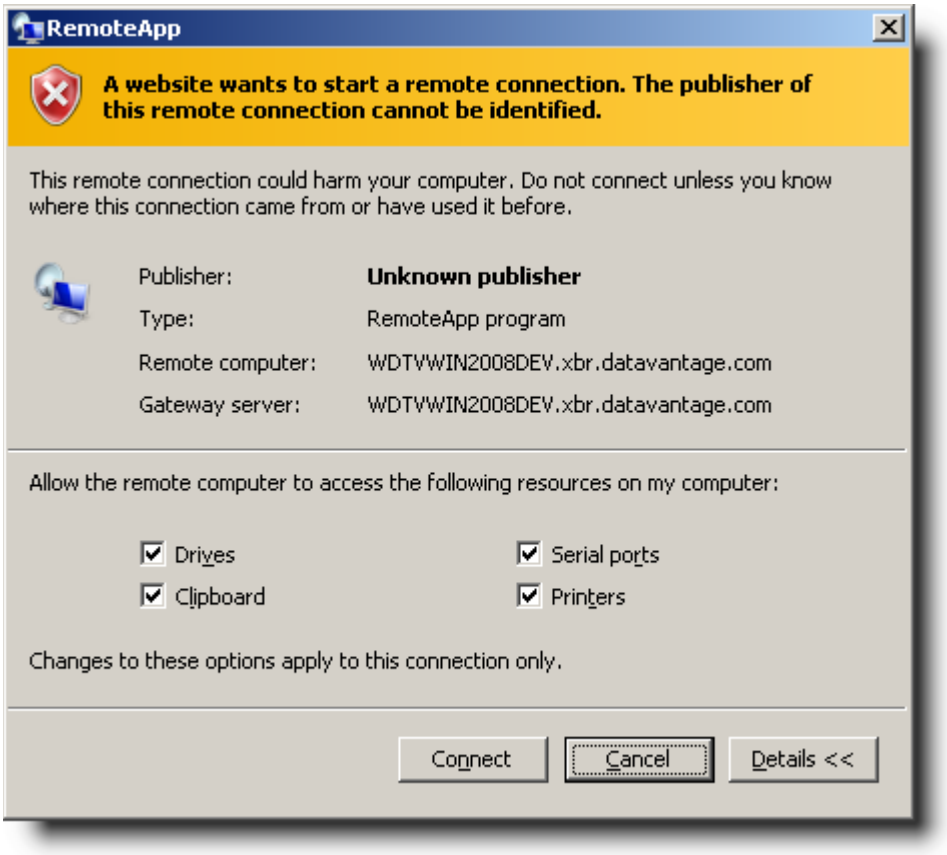


Figure 1-31: Start Remote Connection

7. Enter your XBR user credentials on the Application login screen that appears.

Figure 1-32: XBR Log In Screen

VIDEO VIA REMOTE DESKTOP SERVICES

> *In order for remote users to be able to access the video through XBR, the video source (DVR) should accessible to the terminal server machine either via an external IP for remote networks or internal IP in a WAN/MAN setup.*

The path to the video player executable must be specified in the appropriate `dtvanlytics.ini` file on the Remote Desktop Server.

If the video player executable is installed on the server, the path in the `dtvanalytics.ini` file would look similar to:

```
c:\videoplayer\vidplayer.exe
```

If the video player executable will be accessed from the client machine, the path in the dtvanalytics.ini file would look similar to:

`\\tsclient\C\videoplayer\vidplayer.exe` where “C\videoplayer\vidplayer.exe” is the path on the client machine.

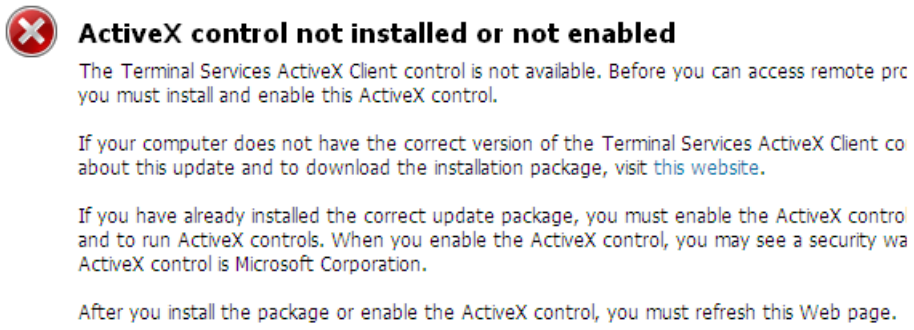
> ***All*** remote users must have the executable installed using the same path on their local client.

More information on video configuration settings can be found in the *XBR Implementation Guide*.

ISSUE RESOLUTION

Active X Fix

Sometimes machines are not enabling or not downloading the application, the issue:



ActiveX control not installed or not enabled. The Remote Desktop ServicesActiveX Client control is not available. Before you can access remote programs and connect to remote desktops through RD Web Access, you must install and enable this ActiveX control.

The recommended fix:

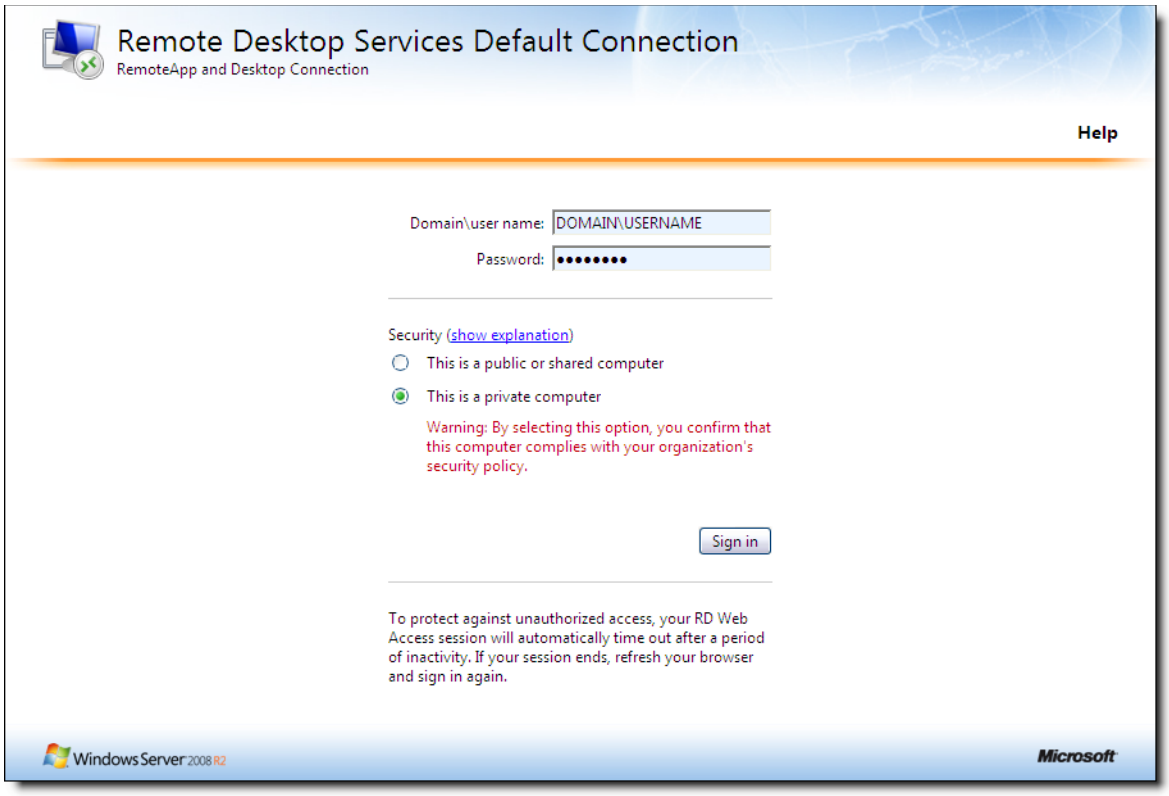
Select **Internet Explorer -> Tools -> Internet Options -> Advanced Tab -> Reset**

Multiple Login Prompt Issue

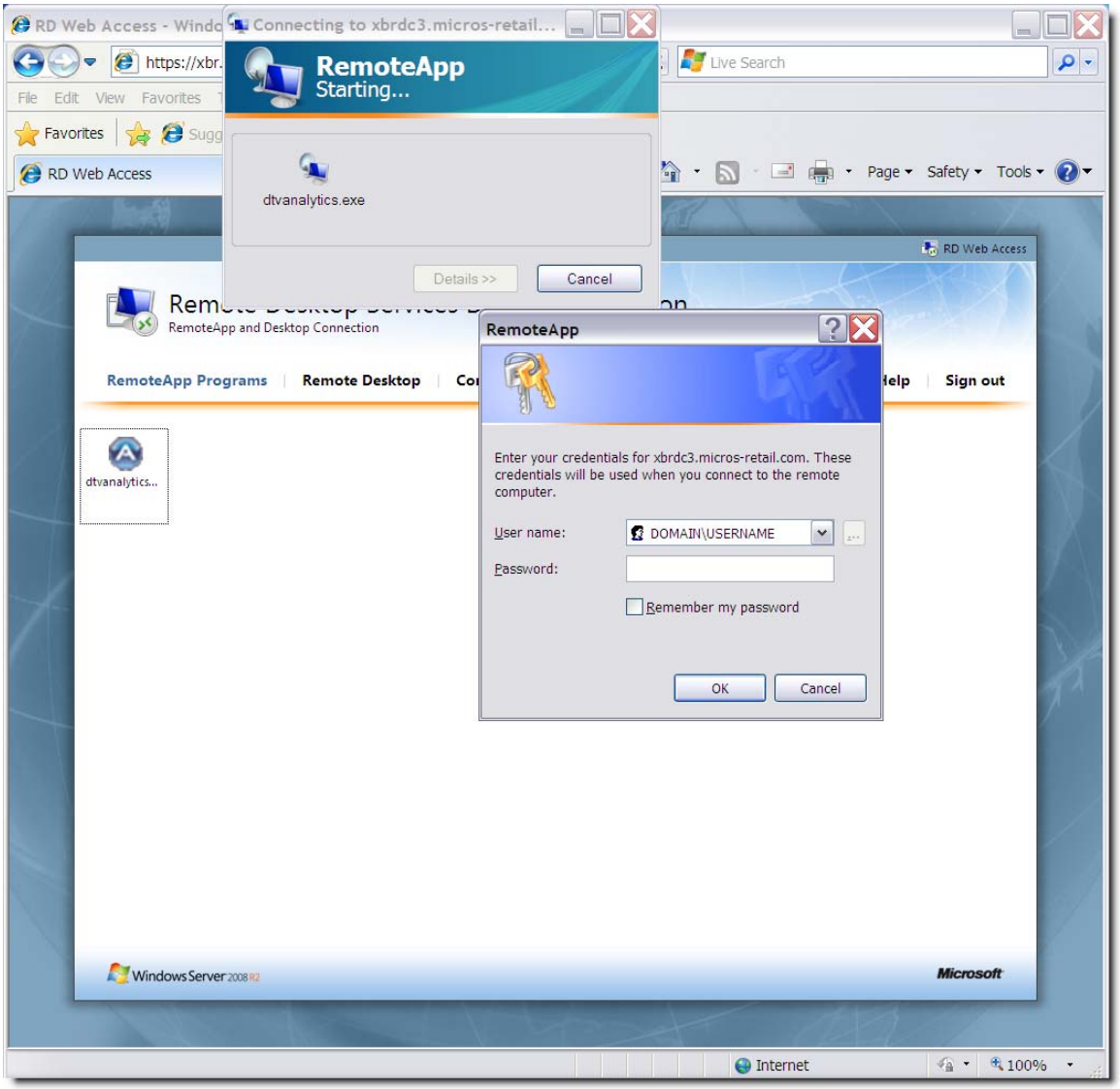
Issue Description

When accessing XBR through Remote Desktop Web Access on Windows 2008 R2 Server the user may experience two domain logon prompts. This issue has been observed on PCs running Windows XP SP3 OS and older versions of the Remote Desktop Connection client.

This first Prompt is expected:



This second prompt should not be appearing:



Resolution - Part 1: Install Hotfix

Install Remote Desktop Connection 7.0 client update for Remote Desktop Services (RDS) for Windows XP SP3. It may be necessary to restart the computer after applying this update. Security policies in effect on the local PC may restrict the ability to perform some of the required actions.

The Microsoft Knowledge base article and 7.0 client update can be found at:

http://support.microsoft.com/?kbid=969084

Use the following steps to install the client update:

1. Launch the executable.

2. Click **Run**.

3. Click **Next** to start the Installation process.

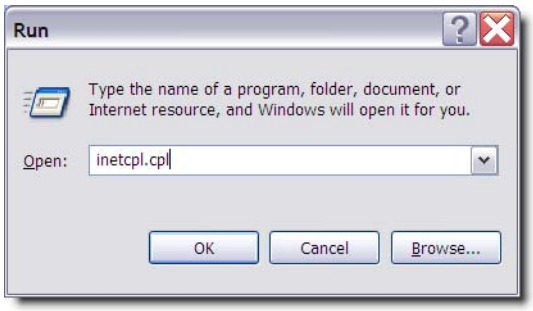
4. When Installation is complete, click **Finish**.

   In most cases this will resolve the issue. If multiple logon prompts are still being experienced the problem may be resolved by closing Internet Explorer and resetting all IE options to their default values. Refer to the next section for more information.

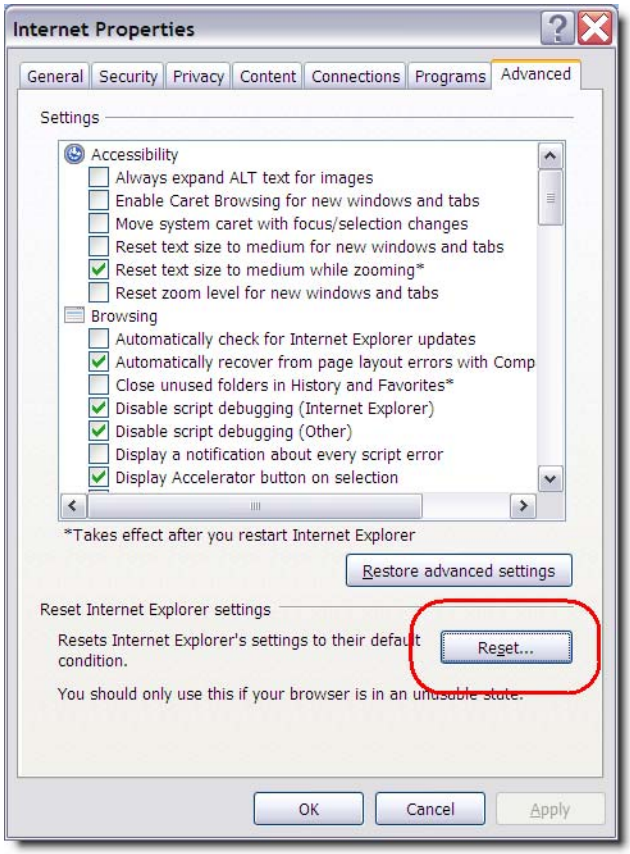
Resolution - Part 2: Reset Internet Explorer Options

> ***!*** *Proceeding with this procedure will reset all Internet Explorer options to their default settings and delete all logon IDs and passwords saved in Internet Explorer.*

1. Make sure all Internet Explorer 8 sessions are closed.
2. From the Windows Taskbar click **Start → Run**.



3. Type “inetcpl.cpl” in the **Open** text box and click **OK**. The Internet Options Control Panel will open.
4. Click the Advanced tab.



5. Click **Reset**.

6. Check **Delete Personal Settings** and click **Reset**.

7. When complete click **Close**.

Local Group Policy Settings for Printing

In order for remote services clients to have their local printers available and retain their default printer in the remote XBR session, it is suggested that the following Group Policy settings be configured as shown below.

On the Windows 2008r2 Server using the Local Group Policy Editor Management Console (gpedit.msc) go to this folder:

`Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Printer Redirection`

Configure the following settings as indicated:

Do not allow client printer redirection	Disable
Do not set default client printer to be default printer in a session	Disable
Redirect only the default client printer	Disable
Specify RD Session Host fallback printer driver behavior	Not configured
Use Remote Desktop Easy Print printer driver first	Enable

Printing Blank Pages

When printing from a PowerBuilder application that is accessed through Remote Desktop Web Access on Windows 2008 R2 Server, the user may get blank pages. This issue has been observed on PCs running Windows XP, Windows Vista SP1, and Windows Server 2008.

Microsoft Hotfix 959554 must be applied to win2008r2 RDS server to fix the problem of printing blank pages from PowerBuilder applications.

The Microsoft Knowledge base article and Hotfix can be found at:

http://support.microsoft.com/kb/959554

Following successful application of the Hotfix, the line "`PRINTWIN2008=Y`" or "`PRINTWIN2008=N`" should be removed, if present, from any `dtvanalytics.ini` file currently in use on the server.

If the server is not rebooted after installation of the Hotfix, the Print Spooler service must be restarted.

Contact Information

www.micros-retail.com

30500 Bruce Industrial Parkway
Cleveland, OH 44139 USA
Toll Free: 888.328.2826
Tel: 440.498.4414
Fax: 440.542.3043

1800 West Park Drive
Westboro, MA 01581
Tel:508.655.7500
Fax:508.647.9495

MICROS Systems, Inc.
www.MICROS.com
7031 Columbia Gateway Drive
Columbia, MD 21046-2289
Tel: 443.285.6000