RDS/Citrix Client Access Installation and User Guide

9.12.0 v1

Symmetry™ Security Management

9600-0404

RDS/Citrix Client Access Installation and User Guide
(9600-0404)

Issue 9.12.0v1 – 24th March 2025
Applies to version 9.12.0 or later of the Symmetry software, until superseded by a later issue of the manual.

Contents

Chapter 1: Introduction 1

About this Installation and User Guide 1

About the Symmetry RDS/Citrix Client Access Software 1

System Architecture 1

Microsoft Remote Desktop Services (RDS) Architecture 1
Citrix XenApp Architecture 2
Benefits of Thin-Client Technology 3
Communications Security 3

Summary of Key Features 3

Symmetry Licensing 4

"RDS/Citrix Client Access Licensing" (CAL) method 4
"Symmetry Concurrent User Licensing" method 4

Minimum System Requirements 5

Minimum Requirements when using Microsoft RDS 5
Minimum Requirements when using Citrix XenApp 6
Qualified Symmetry Peripherals 6

Upgrading to Symmetry v9.12 (or Later) 7

Chapter 2: Installation using Remote Desktop Services 8

Overview 8

Step 1 – Add Certificate Services 8

Step 2 – Set Permissions for the Web Server Template 10

Step 3 – Generate a Certificate 10

Step 4 – Install Remote Desktop Services (RDS) 14

Same-Server Installation Procedure 14
Separate-Server Installation Procedure 15

Step 5 – Configure Remote Desktop Services 17

Same-Server Installation Procedure 17
Separate-Server Installation Procedure 21

Step 6 – Test the RDS Connection 26

Step 7 – Install the Symmetry Client Software on the Web Server 27

Step 8 – Set up the RDS Group 27

Same-Server Installation Procedure 27
Separate-Server Installation Procedure 29

Step 9 – Assign Permissions 29

Step 10 – License RDS 30

Step 11 – Test that the Symmetry Client Software can start 30

Step 12 – Add Symmetry Licenses 31

Step 13 – Configure Alarm Routing 31

Step 14 – Connect to Symmetry from a Remote Machine 31
Optional Steps 33
Enabling Web Cameras 33
Installing a Fargo Badge Printer Driver 34

Chapter 3: Installation under Citrix XenApp 35
Step 1 – Install the Symmetry Client Software on the XenApp Server 35
Step 2 – Add Symmetry Licenses 35
Step 3 – Configure Alarm Routing 36
Step 4 – Configure Badge Printers (Optional) 36
Step 5 – Publish Symmetry 36
Step 6 – Prevent Uploading of Files from Browser Machines 37

Appendix A: Starting a Remote Desktop Connection 38
Connecting to a Computer Remotely 38

Chapter 1: Introduction

About this Installation and User Guide

This guide explains the purpose, operating concepts and benefits of the optional Symmetry RDS/Citrix Client Access software. This guide is intended to be used by:

- Managers deciding whether to use the software.
- Technical staff installing the software.
- Users who need to access the Symmetry software remotely though a web server.

About the Symmetry RDS/Citrix Client Access Software

The RDS/Citrix Client Access software uses "thin-client" technology to enable users to monitor, control and administer Symmetry remotely over the internet or through your company's intranet from a web browser. The Symmetry user interface at remote machines is the same as is displayed at a standard Symmetry client.

Users have the ability to perform a wide range of tasks, such as setting up card holders, producing badges, generating reports, monitoring alarms and registering visitor details. The Symmetry RDS/Citrix Client Access software is the ideal choice for remote users, or those who require casual access to the Symmetry software from any location. (To prevent excessive network loading, the use of digital video is not supported.)

The Symmetry RDS/Citrix Client Access software supports the leading thin-client technologies: Microsoft® Remote Desktop Services with Internet Information Services (IIS), or Citrix® XenApp.

Appendix A explains how to use the built in Microsoft Remote Desktop Connection tool to access a windows PC remotely (this is not part of the RDS/Citrix Client Access Software).

System Architecture

Microsoft Remote Desktop Services (RDS) Architecture

The architecture when using RDS is shown in Figure 1.

RDS requires only one web server machine to host all RDS services, IIS and the published web application (in this case, the Symmetry client software). However, for enhanced security, two separate machines can be used: a **Web Access Server** to host IIS, and a separate **RD App Server** to host the published application (Symmetry).

Note: The Symmetry server must not use the same machine(s) as used by Remote Desktop Services.

Remote machines require no specific client software. Users access the Symmetry user interface through a supported web browser (see page 5).

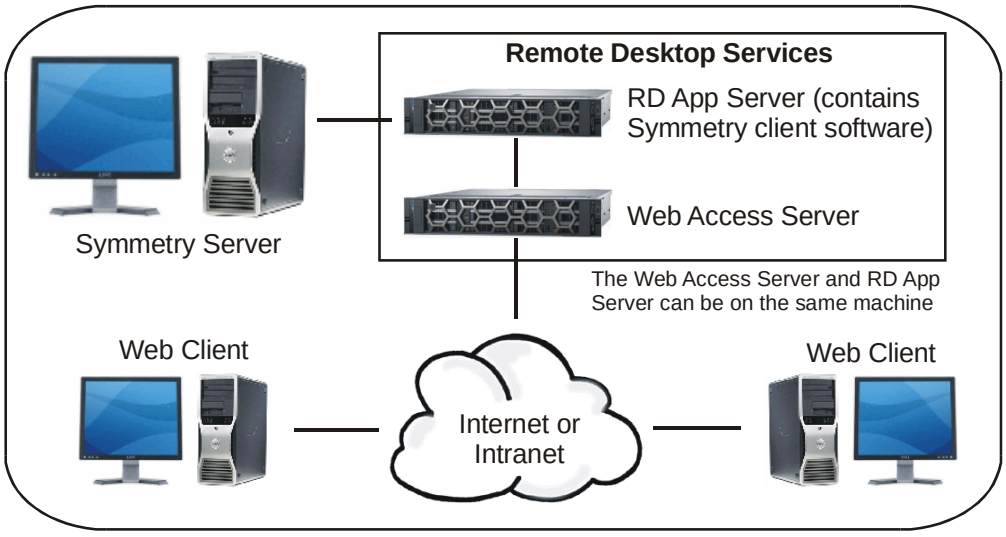


Figure 1: Example Architecture when using Remote Desktop Services

Citrix XenApp Architecture

The Citrix XenApp server hosts the Citrix XenApp web server software and the Symmetry web-access components. The Symmetry web-access components provide connectivity to Symmetry. Citrix XenApp and the Symmetry server must use different machines. See Figure 2.

Remote (client) machines require the Citrix XenApp Receiver software to be installed, and users access the Symmetry user interface through a supported web browser (see page 5).

Citrix XenApp is often a suitable solution when the security system has a large number of concurrent users at remote sites (e.g. 40, although this can be affected by a number of factors).

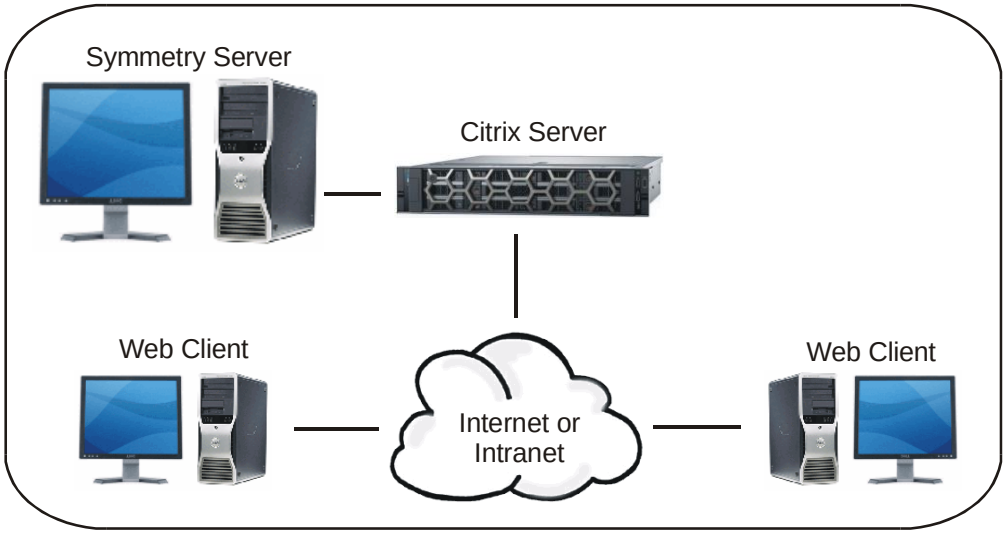


Figure 2: Example Architecture when using Citrix XenApp

Benefits of Thin-Client Technology

The use of thin-client technology avoids the need to download large amounts of data to and from the server, since only mouse and keyboard actions are transmitted, and screen updates received. Since all the software is stored on a web server, thin-client technology enables the software to be supported and upgraded more easily. In addition, since all processing is carried out on the web server, thin-client technology can offer quick response times from low-cost client PCs. Overall, these factors can significantly reduce cost.

For installations where network speed is fast and bandwidth is not an issue, a standard thick-client solution is recommended. When there are concerns about network speed or bandwidth, or there are many remote users, a thin-client implementation can provide significant advantages. For many installations, a hybrid implementation that combines both thick and thin clients gives the best overall solution.

The following summarizes the benefits can be achieved using thin-client technology:

- Centralized system administration
- Greater control of software
- Simplified installation and upgrade, particularly for remote or mobile users
- Reduced support costs
- Ability to use any applications across a WAN or VPN
- Low-cost client computers can give good application performance

Communications Security

The RDS/Citrix Client Access software can use the HTTPS protocol for communications security. This enables the server to authenticate itself to a client (using certificates), allows the client to authenticate itself to the server, and allows both machines to establish an encrypted connection.

Summary of Key Features

The key features of the RDS/Citrix Client Access software are as follows:

- Fully-integrated web browser solution.
- Enables tasks such as badge, card and report generation or visitor registration to be carried out remotely over the Internet or through company intranet.
- In most cases, Symmetry RDS/Citrix Clients require no special software (Citrix clients require some additional software to be installed if graphics devices such as webcams are used).
- Security maintained by user login.
- Provides an easy yet secure method for a user to monitor, control and administer a system from almost any location in the world.
- Uses thin-client technology, which can reduce hardware and IT support costs.

Symmetry Licensing

There are currently two alternative methods to license Symmetry when using the Symmetry RDS/Citrix Client Access Software. Each of these methods is described next.

Note: If you want to switch the licensing method, the Symmetry client software will need to be uninstalled and then reinstalled using the appropriate license number. The "RDS/Citrix Client Access Licensing" method also requires an "RDS/Citrix Client Users" and/or "RDS/Citrix Client Visitors" license number.

"RDS/Citrix Client Access Licensing" (CAL) method

With this method, an "RDS/Citrix Server License" number is entered when installing the Symmetry client software on the web server. The license number enables the Symmetry RDS/Citrix Client Access software. On an RDS/Citrix farm, each server requires its own Symmetry RDS/Citrix Client Access license.

After installation, an "RDS/Citrix Client Users" and/or an "RDS/Citrix Client Visitors" license number, as described below, must also be installed using the Symmetry "Maintenance/Licensing/Concurrent Client Licenses" screen. Doing so, creates a pool of one or more user licenses. When a Symmetry user logs in, a license is automatically allocated to that PC from the pool. When the user logs out, the license is automatically released to the pool and is available for use by a user from another PC.

"RDS/Citrix Client Users" license number

This gives Symmetry users access to all features supported at standard Symmetry clients (except video). If alarm routing is set up to route alarms to the web server, users who log in at an RDS/Citrix client can use the "Home/Monitoring/Alarms" screen to view all alarms that belong to a company in the user's company group.

"RDS/Citrix Client Visitors" license number

This is required if visitor management functionality is required. The license allows card holders who log in using the "Visitor Management" user role to pre-register visitors. Card holders who require the permission must have **Allow Visitor Management Login for this Cardholder** set in the "Home/Identity/Card Holders" screen.

Note: Symmetry gives access only to the visitor management options, as defined by the default "Visitor Management" user role. Changes to the Visitor Management role have no effect on the options provided at the client.

"Symmetry Concurrent User Licensing" method

With this method, you enter a "Symmetry Client Concurrent User License" number when installing the Symmetry client software on the web server. The license licenses a maximum number of users. For example, if a Symmetry 10-user license is purchased, up to ten users who access Symmetry through this licensing mechanism can use Symmetry simultaneously (concurrently) at any one time. A license is not fixed to any particular machine, and therefore when a user closes Symmetry, it allows another user to open Symmetry.

After installation, you can use the "Maintenance/Licensing/Concurrent Licenses" screen to see which users are currently using Symmetry and therefore one of the available concurrent licenses. The **Release** button in this screen allows a license to be returned to the pool manually, if required.

If at a later time, you want to increase the maximum number of concurrent users, you can install an additional "Symmetry Client Concurrent User License" number using the Symmetry "Maintenance/Licensing/System Licenses" screen.

Benefits

Benefits of the "Symmetry concurrent user licensing" method include the following:

- If you have multiple web servers in an RDS/Citrix farm, you can use the same Symmetry license number when installing the Symmetry client software on each web server. This allows each server to be provisioned from the same image file. If, for example, there are three RDS/Citrix servers and 64 concurrent users are required, you could install all three servers with a image pre-installed using a "Symmetry Client Concurrent User License" for up to 64 users. As each server would have the same license number, the maximum number of concurrent users would be 64.

- The Symmetry concurrent user licensing method can also be used for Symmetry concurrent clients that access Symmetry outside of the RDS/Citrix environment (such as directly over the network or in a VMWare environment). Using the Symmetry concurrent user licensing method can simplify management of user licensing, as the licensing mechanism is not tied to a particular platform or environment.

Note that when using the "Symmetry concurrent user licensing" method, there is no Symmetry client definition for the web server in the "Install/System/Clients" screen, and therefore alarm routing can be configured only at the role and account levels (not at the client level).

Please refer to the *Symmetry Software Installation Manual* for further information about Symmetry concurrent user licensing.

Minimum System Requirements

Minimum Requirements when using Microsoft RDS

Symmetry software

- Symmetry Professional or Enterprise Edition.

Web server(s)

- A Web Access Server or RD App Server must have the same minimum hardware specification as a Symmetry Enterprise Edition server, as described in the *Symmetry Software Installation Manual*.

- The server on which Symmetry is installed requires a version of Windows Server supported for a Symmetry Enterprise Edition server, as documented in the *Symmetry Software Installation Manual*.

- A license to use Microsoft Remote Desktop Services is required (available separately).

Remote clients

- Google Chrome, Mozilla Firefox v55.0 or later, Microsoft Edge, or Internet Explorer 11 (or Microsoft Edge in Internet Explorer 11 Compatibility Mode).

  Note: AMAG support for any of the above browser versions ceases if the version is no longer supported by the browser manufacturer.

- Clients should have the same minimum specifications as standard Symmetry clients, as described in the *Symmetry Software Installation Manual*. However, machines with a lower minimum specification

or that use different operating systems may operate correctly. If such machines are used, they must be tested thoroughly to ensure correct operation.

Symmetry licensing – Please refer to "*Symmetry Licensing*" on page 4.

Minimum Requirements when using Citrix XenApp

Symmetry software

- Symmetry Professional or Enterprise Edition.

Citrix XenApp hardware

- The hardware must have the same minimum specification as a Symmetry Enterprise Edition server, as described in the *Symmetry Software Installation Manual*. The machine must not be the same machine as the Symmetry server or any separate Symmetry database server.

Citrix XenApp software

- XenApp Server. For details of the version number of XenApp to use, please refer to the Symmetry Technical Bulletin for the version of Symmetry being used, or contact your technical support representative.
- Windows Server - the versions supported are the same as for a Symmetry Enterprise Edition server, as documented in the *Symmetry Software Installation Manual*.
- License to use Citrix XenApp (available separately).

Remote clients

- Google Chrome, Microsoft Edge or Internet Explorer 11.

  Note: AMAG support for any of the above browser versions ceases if the version is no longer supported by the browser manufacturer.

- Clients should have the same minimum specifications as a standard Symmetry clients, as described in the *Symmetry Software Installation Manual*. However, machines with a lower minimum specification or that use different operating systems may operate correctly. If such machines are used, they must be tested thoroughly to ensure correct operation.

Symmetry licensing – Please refer to "*Symmetry Licensing*" below.

Qualified Symmetry Peripherals

Card printers can be used for printing and magstripe encoding (only).

USB plug-and-play web cameras supported by the local client operating system can be used for image capture.

It is not possible to associate a Symmetry client port with a Symmetry web client. Therefore, the use of peripherals (or integrations) that require a client port is not supported.

Upgrading to Symmetry v9.12 (or Later)

In previous versions of Symmetry, a **VDI-Server** option was available in the **To Client** menu of the "Operation/Alarms/Routing" screen, which was used to route alarms to all clients using Symmetry concurrent user licensing. This mechanism meant that all concurrent users were restricted to use the same alarm routing.

Symmetry v9.12 (or later) does not include a **VDI-Server** option. Instead, concurrent clients can take advantage of alarm routing at the user-account and user-roll levels. This enables different users to see different alarms at different times, as described in *Overview of Alarm Routing* in the *Symmetry Online Help*.

If you upgrade a version of Symmetry that is earlier than v9.12 to Symmetry v9.12 (or later), any alarm routing to **VDI-Server** is converted to the new mechanism, as described in the *Symmetry Software Installation Manual* (see the chapter titled *Upgrading Symmetry*).

When using the "RDS/Citrix Client Access Licensing" method, there is a Symmetry client definition for the RDS/Citrix web server, and therefore alarm routing configured for the web server is retained. After the upgrade, you may want to change alarm routing to use alarm routing at the user-role or user levels instead.

Chapter 2: Installation using Remote Desktop Services

Overview

This chapter explains the installation process when using Microsoft Remote Desktop Services. This chapter assumes a domain installation of the software.

Note: The process documented in this chapter assumes Windows Server 2019. The process may be different for later versions of Windows Server.

Note: You must log in as an administrator to carry out the installation and setup. A preconfigured Symmetry server must reside elsewhere on the same domain.

As part of the installation procedure, a web-site certificate needs to be issued by a trusted certification authority. It may be preferred for the certificate to be purchased from a third-party certification authority. Alternatively, the certificate can be issued on site by installing a Microsoft Certificate Authority.

Web Servers that are internet facing and accessible over a public network are required to be secured with a certificate purchased from an online trusted certificate authority.

Step 1 – Add Certificate Services

This section describes how to add roles for Certificate Services. Certificates are the most common way to protect information that is being transmitted between browsers and the Web Access Server.

At the Web Access Server:

1. Install the Windows operating system and make sure you set the computer name as desired. Preferably, choose a reasonably straightforward name, since you and web users will need to enter it several times.

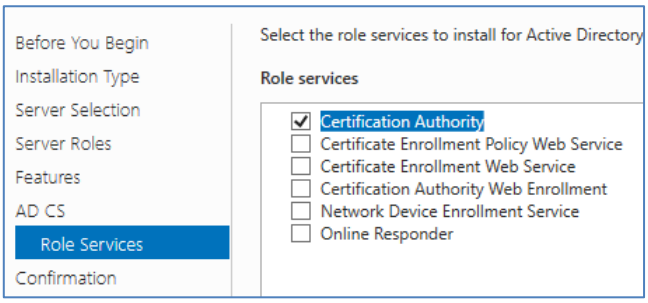
2. Select **Programs and Features** in the Windows Control Panel.

3. Select **Turn Windows features on and off**.

4. Choose the following in the Add Roles and Features Wizard (leave all other options at their default settings).

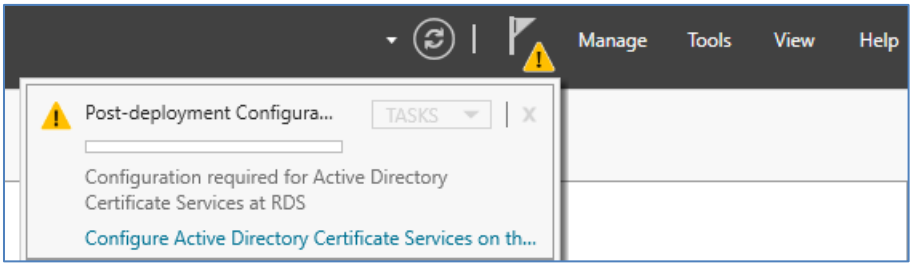
   Note: After selecting a setting, click **Add Features**, if prompted.

Screen Name	Settings
Installation Type	Select **Role-based or feature-based installation**.
Server Selection	Select the Web Access Server.

Server Roles	Select **Active Directory Certificate Services**.
AD CS, Role Services	Select **Certification Authority**: 

5. Click **Next** repeatedly until the **Install** button is displayed, and click **Install**.

6. On completion, click **Close**, then select **Configure Active Directory Certificate Services on the destination server** in the Add Roles and Features Wizard, or in the notifications in the Server Manager:



7. When prompted by AD CS Configuration, choose the following settings (leave all other options at their default settings).

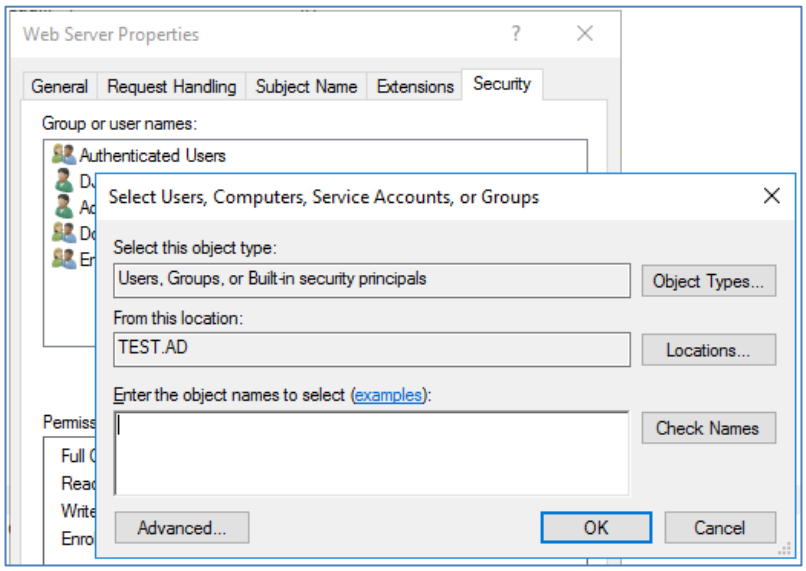
Screen Name	Settings
Role Services	Select **Certification Authority**.
Setup Type	Select **Enterprise CA**.
CA Type	Select **Root CA**.
Private Key	Select **Create a new private key**.
Private Key, Cryptography	Select **SHA256** unless advised otherwise by the IT administrator.

8. Click **Next** repeatedly until the **Configure** button is displayed, and click **Configure**.

9. On completion, click **Close**.

Step 2 – Set Permissions for the Web Server Template

1. In the Microsoft Management Console (MMC), open **Certificate Templates**.
2. Right-click **Web Server Template** (or equivalent) and select **Properties**.
3. In the Security tab, click **Add**.



4. Click **Object Types**.
5. Select **Computers**, then click **OK**.
6. In the **Enter object names to select** box (as shown above), add the computer name of the RDS server the certificate request is generated from, then click **OK**.
7. Make sure that **Read** and **Enroll** are set to **Allow**, and click **OK**.

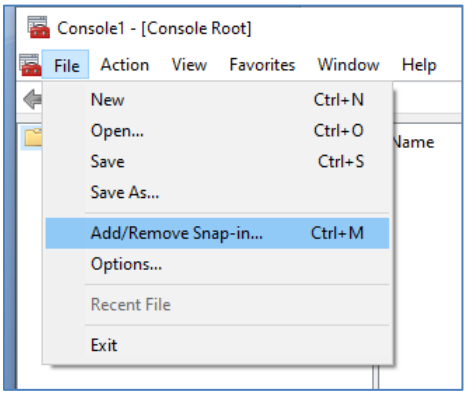
Step 3 – Generate a Certificate

A certificate can be purchased from a third-party certification authority and the .pfx file copied to the Web Access Server (as detailed on pages 18 and 23). Alternatively, if Microsoft Certificate Authority is installed, you can generate a certificate yourself, as described in this step.

Note: The certificate authority Web Server template is used (see substep 10 below). You may need to give the RDS Web Server permission to access the template before proceeding.

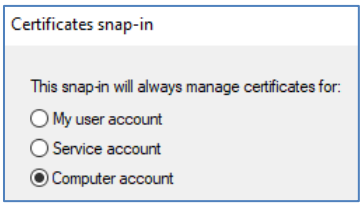
To generate a certificate yourself:

1. In the Windows Search box at the RDS Web Server, enter **mmc** to open the Microsoft Management Console.
2. Select **File, Add/Remove Snap-in**, as shown next.



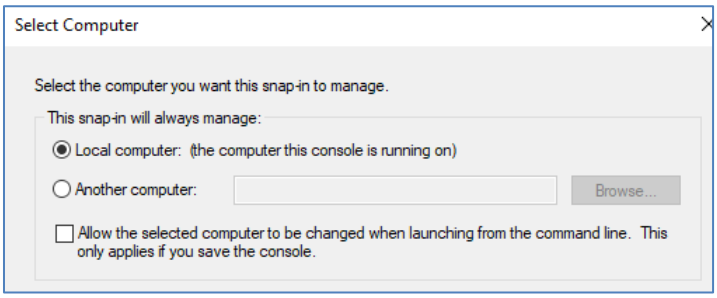
3. Select **Certificates** and click **Add>**.

4. Select **Computer account** and click **Next**:



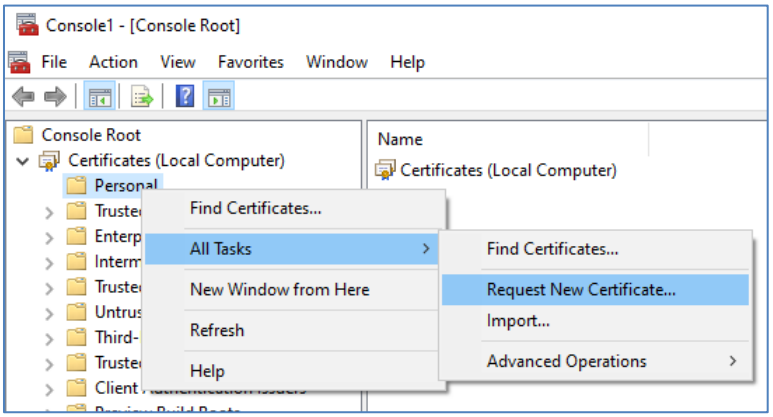
5. Click **Next**.

6. Select **Local computer**:



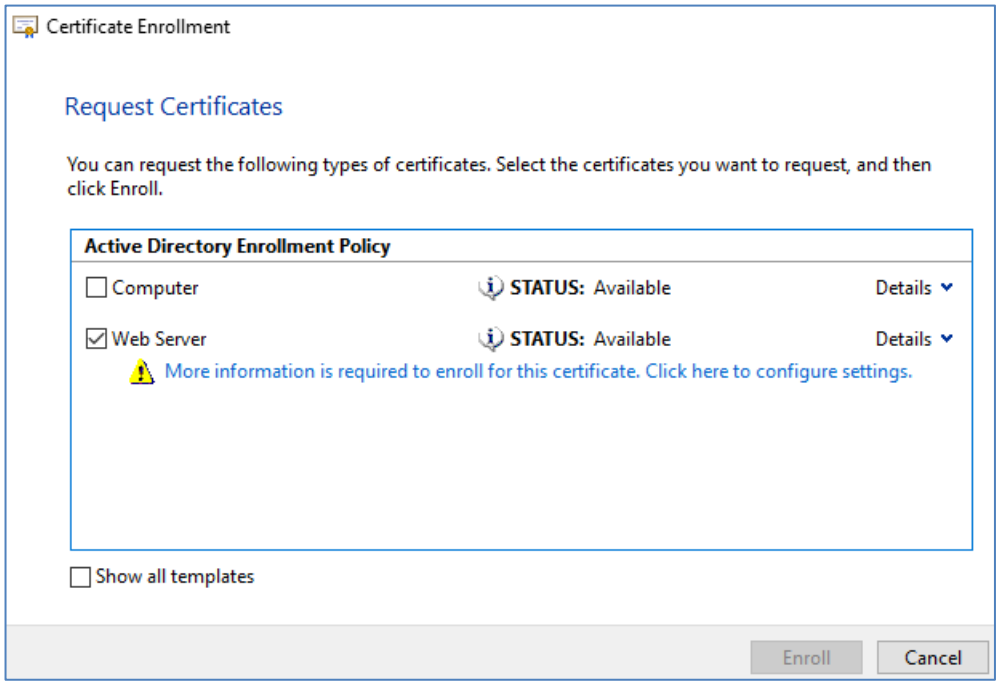
7. Click **Finish**, then **OK**.

8. Right-click the **Certificates, Personal** folder and select **All Tasks, Request New Certificate**:



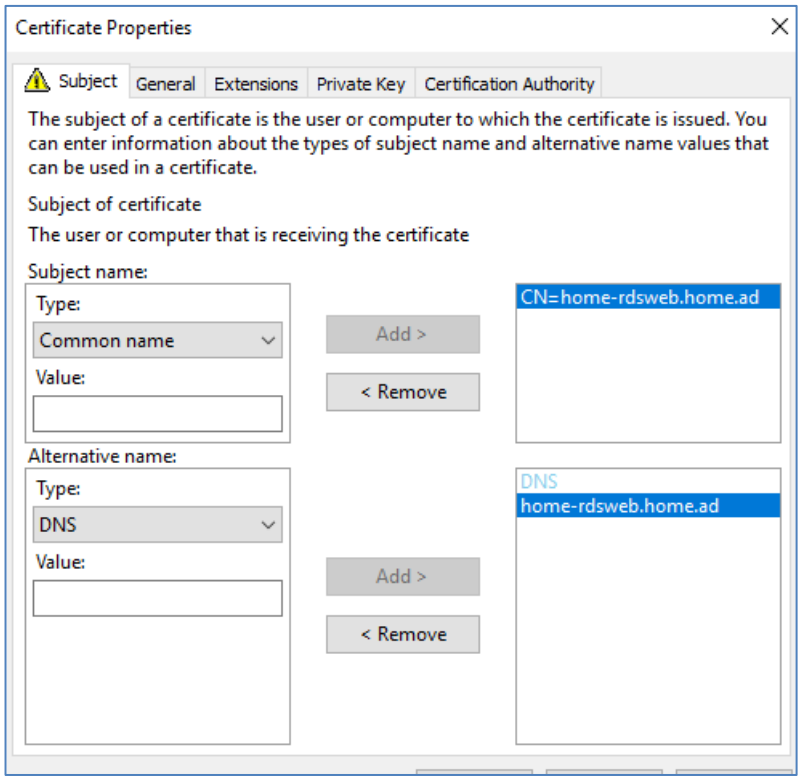
9. Click **Next** twice.

10. In the Request Certificates page, select **Web Server** and click **More information is required to enroll for this certificate**:

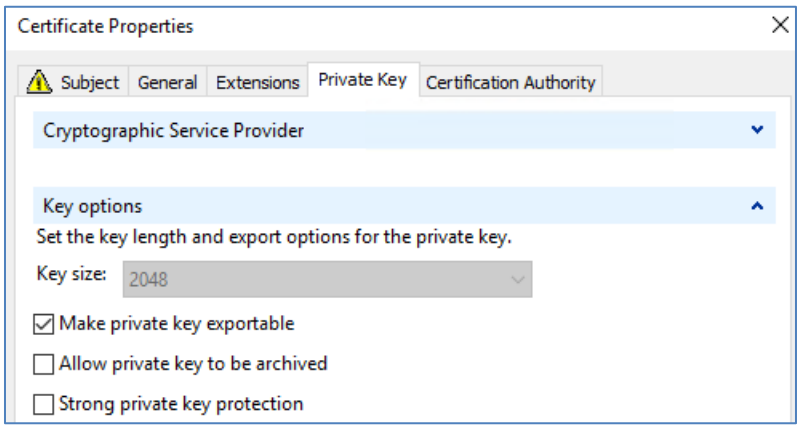


Note: You may need to give the RDS Web Server permission to access the Web Server template.

The following window is displayed:

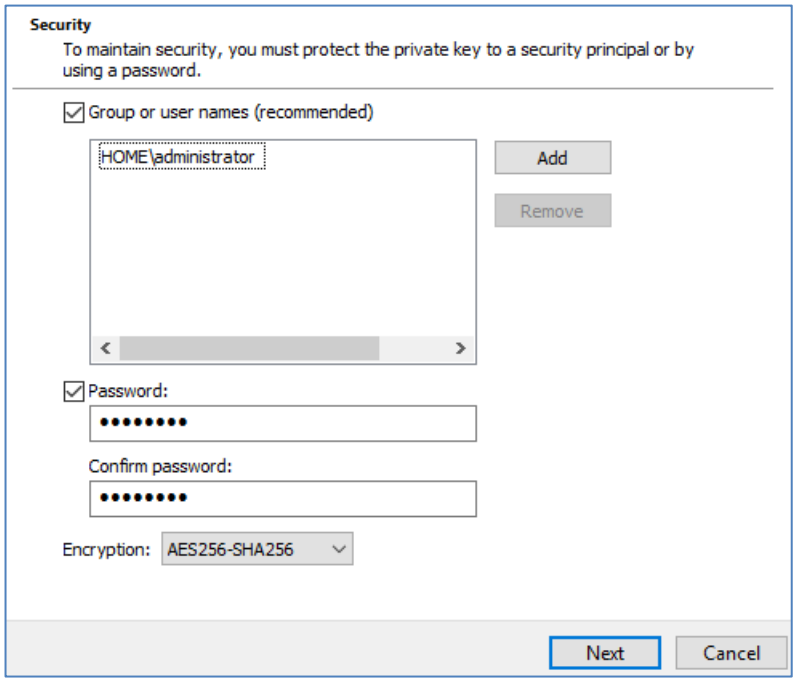


11. In the Subject tab, set:
    - **Subject Name, Type** to **Common Name**.
    - **Subject Name, Value** to the fully-qualified domain name of the RDS Web Access server.
    - **Alternate Name, Type** to **DNS**.
    - **Alternate Name, Value** to the fully-qualified domain name of the RDS Web Access server.
12. In the Private Key tab, select **Make private key exportable**:



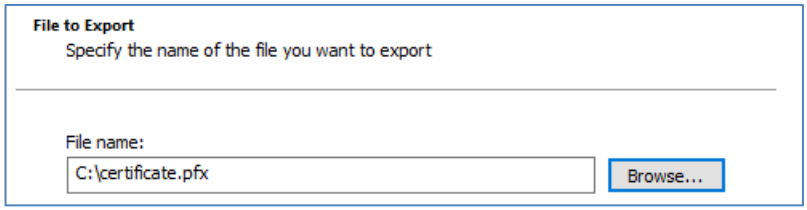
13. Click **OK**, then **Enroll**, then **Finish**.
14. In the Microsoft Management Console, right-click the certificate you have generated and select **All Tasks, Export**.
15. Click **Next**.
16. Select **Yes, export the private key**:

18. Click **Next**, and **Next** again.
19. In the security details, specify a password for the private key and (optionally) the name of the user or group that you want to be able to import the exported certificate, as shown next.



20. Select **AES256-SHA256** from the **Encryption** menu, then click **Next**.

21. Specify a filename:



22. Click **Next**, then **Finish**.

23. Check that the certificate file is present in the specified location.

Step 4 – Install Remote Desktop Services (RDS)

Same-Server Installation Procedure

Use this procedure if your selected architecture requires the Web Access Server and RD App Server to use the same machine.

At the Web Access Server:

1. In **Server Manager**, select **Local Server**.

2. Click **Add Roles and Features** from the **Manage** menu.

3. In the Add Roles and Features Wizard, set the following (leave all other options at their default settings).

Note: After selecting a setting, click **Add Features**, if prompted.

Screen Name	Settings
Installation Type	Select **Role-based or feature-based installation**.
Server Selection	Select the web server.
Server Roles	Select **Remote Desktop Services**.
Remote Desktop Services, Role Services	Select **Remote Desktop Session Host** and **Remote Desktop Web Access**.

4. Click **Next**, then **Install**.

5. On completion, click **Close** and restart the server.

Separate-Server Installation Procedure

Use this procedure if your selected architecture requires the Web Access Server and RD App Server to use separate machines.

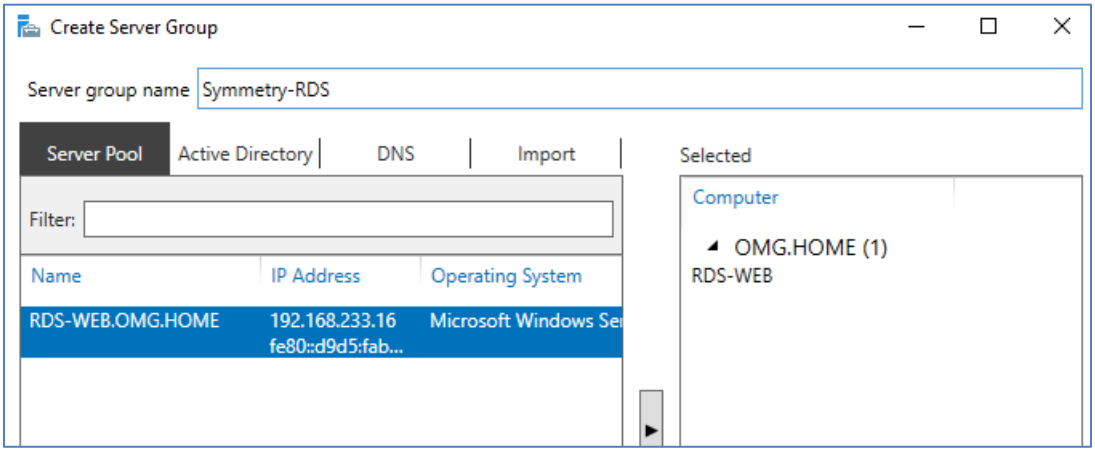
At the Web Access Server:

1. In **Server Manager**, select **All Servers**.

2. Click **Create Server Group** from the **Manage** menu.

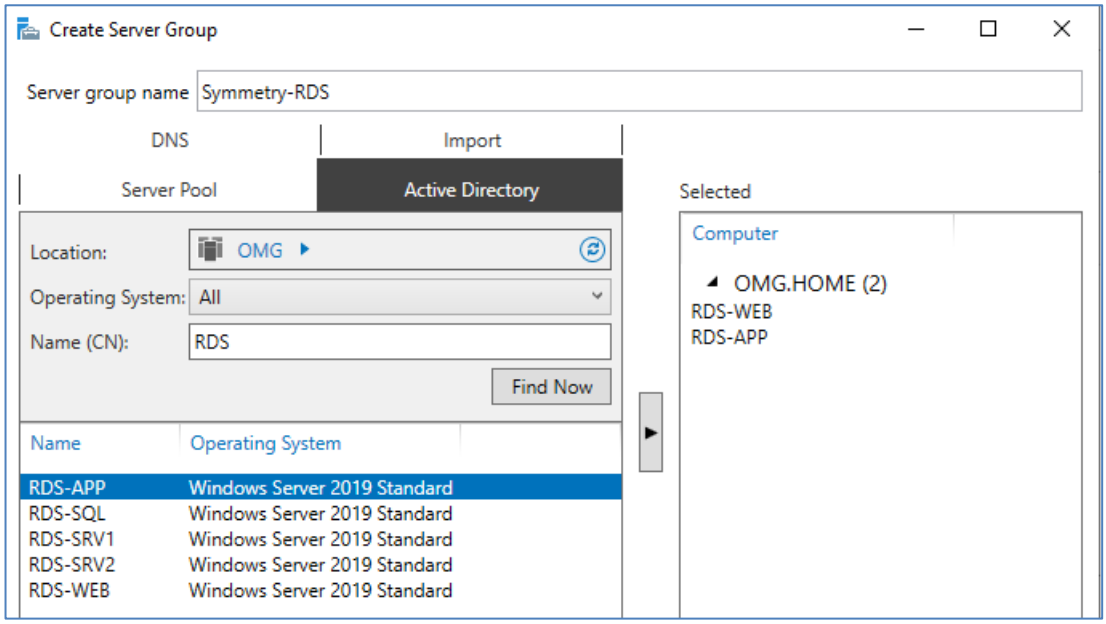
3. Give the server group a name, e.g. "Symmetry-RDS".

4. Move the local (Web Access Server) machine to the **Selected** pane:



5. Click the **Active Directory** tab and search for the RD App Server.

6. Move the RD App Server to the **Selected** pane and click **OK**:



7. Click **Add Roles and Features** from the **Manage** menu.

8. In the Add Roles and Features Wizard, set the following (leave all other options at their default settings).

Screen Name	Settings
Installation Type	Select **Role-based or feature-based installation**.
Server Selection	Select the Web Access Server and click **Next**.
Server Roles	Select **Remote Desktop Services**.
Remote Desktop Services, Role Services	Select **Remote Desktop Session Host** and **Remote Desktop Web Access**.

9. Click **Next**, then **Install**.

10. On completion, click **Close**.

11. Restart the Web Access Server.

Step 5 – Configure Remote Desktop Services

Same-Server Installation Procedure

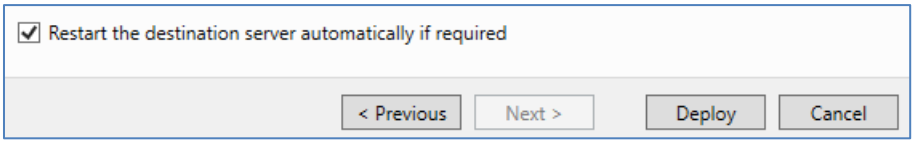
Use this procedure if the Web Access Server and RD App Server use the same machine.

At the Web Access Server:

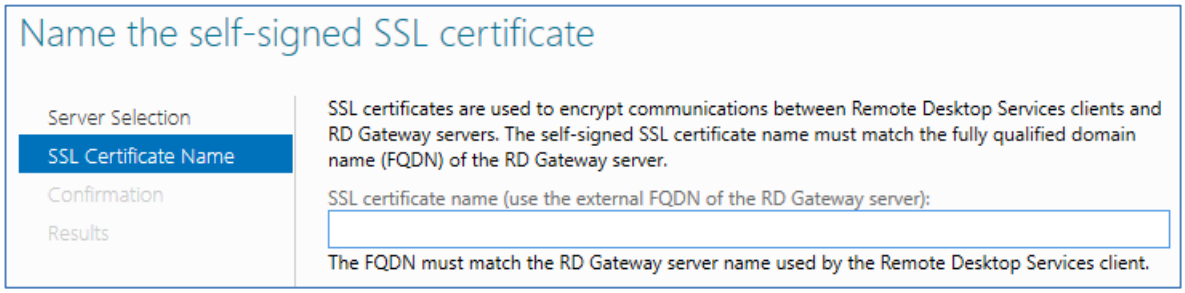
1. In **Server Manager**, select **Local Server**.
2. Click **Add Roles and Features** from the **Manage** menu.
3. In the Add Roles and Features Wizard, apply the settings shown in the following table (leave all other options at their default settings).

Screen Name	Settings
Installation Type	Select **Remote Desktop Services installation**.
Deployment Type	Select **Quick Start**.
Deployment Scenario	Select **Session-based desktop deployment**.
Server Selection	Ensure that the local machine is in the **Selected** pane.

4. Click **Next**.
5. Near the bottom of the **Confirmation** page, select **Restart the destination server automatically if required** and click **Deploy**:

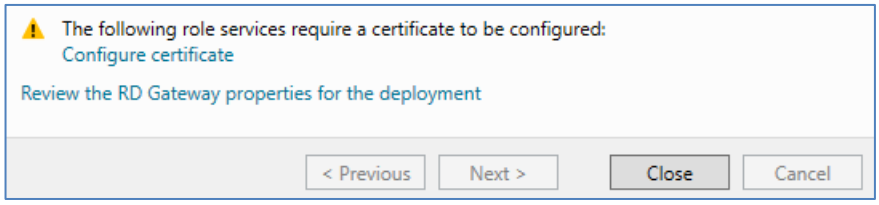


6. On completion, click **Close** and reboot the server.
7. In **Server Manager**, select **Remote Desktop Services**.
8. Select **RD Gateway**.
9. In the **Server Selection** page, move the local machine to the **Selected** pane.
10. In the **SSL Certificate Name** page, enter the Fully Qualified Domain Name (FQDN) of the server into the **SSL certificate name** field, as shown next.

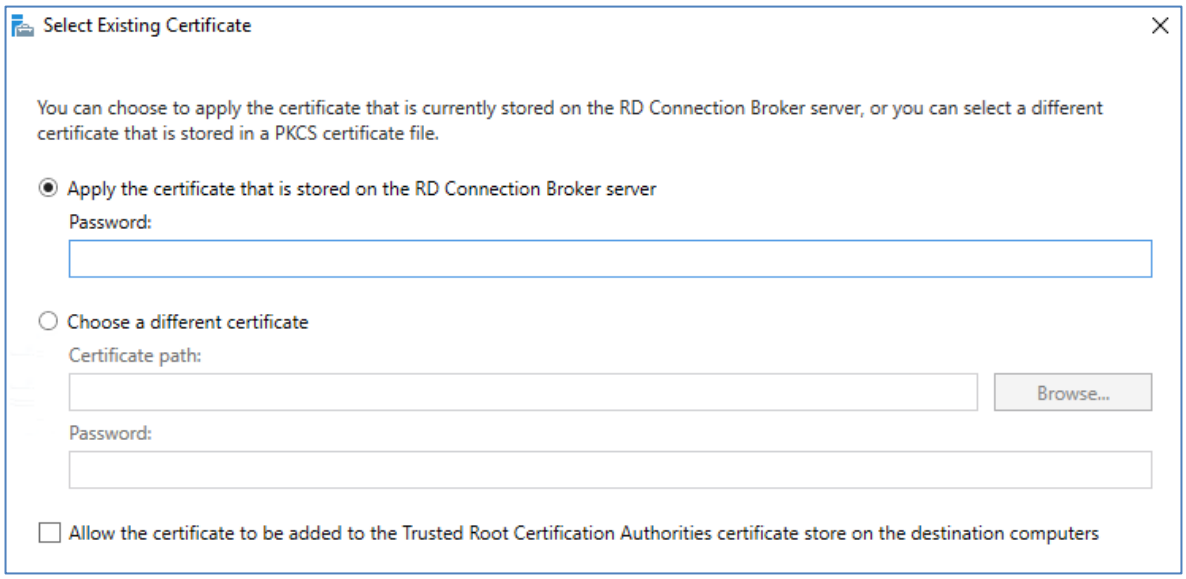


11. Click **Next**, then **Add** and wait for the installation to finish.

12. Once the installation is complete, click **Configure certificate** near the bottom of the window:



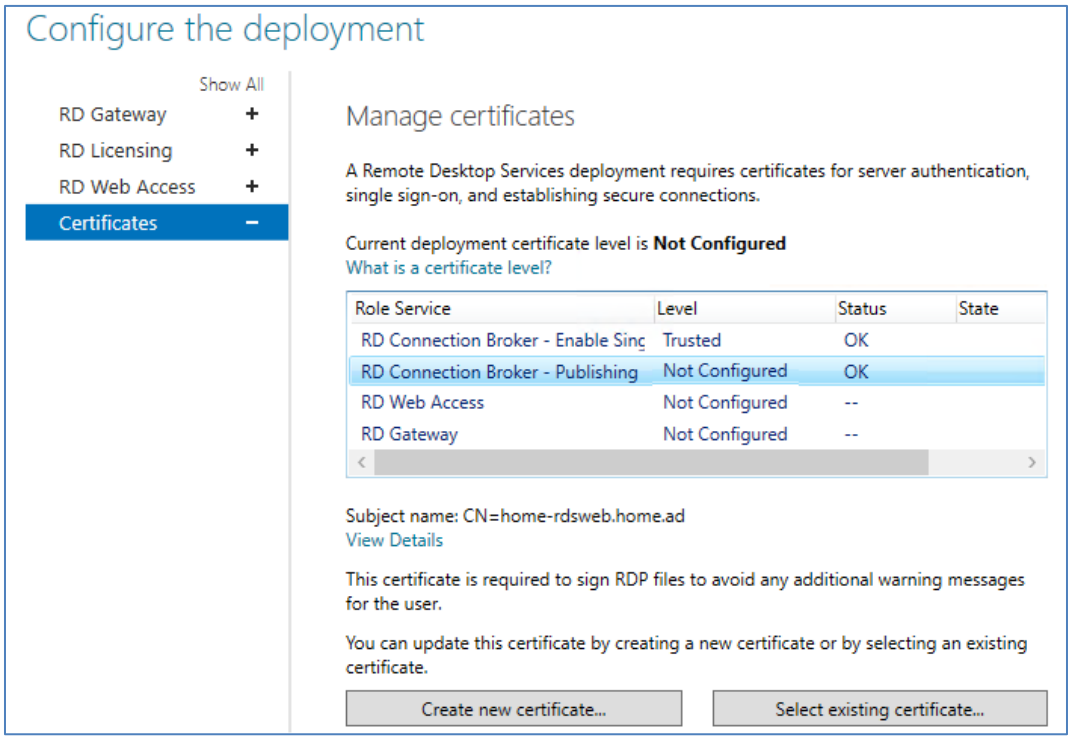
13. Click **Select existing certificate**. The window shown next is displayed.



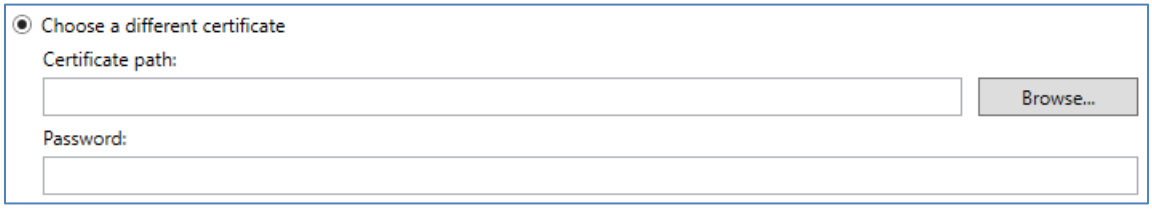
14. In the Select Existing Certificate window:
    a) Browse to the .pfx file.
    b) Specify the password in the **Password** field.
    c) Select **Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on the destination computers**.
    d) Click **OK**.

15. Click **Apply**.

16. In the **Certificates** page, select **RD Connection Broker – Publishing** and click **Select existing certificate…**:



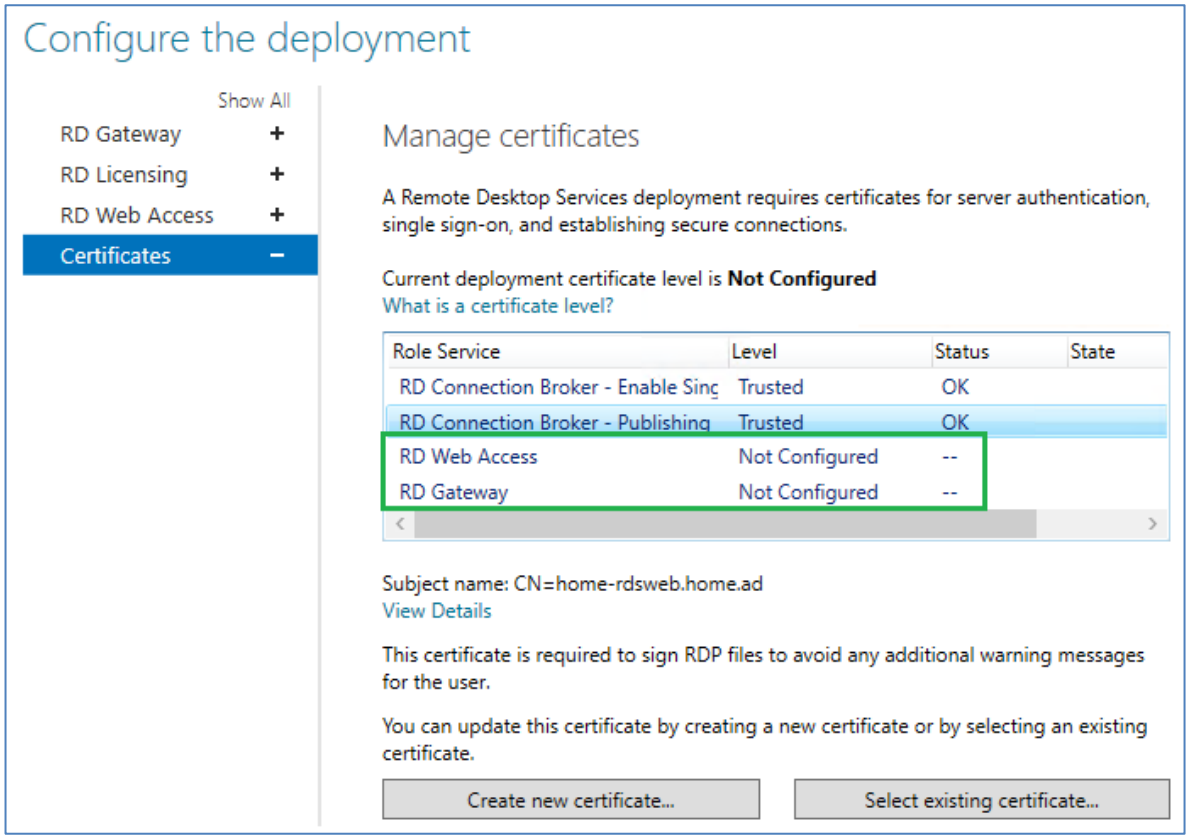
17. Browse to the certificate pfx file:



18. Enter the password and select **Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on the destination computers**.

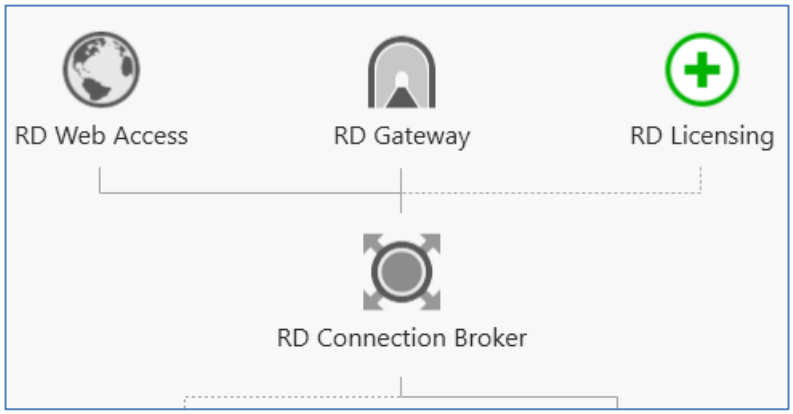
19. Click **OK**, then **Apply**.

20. Repeat steps 16 – 19 for both **RD Gateway** and **RD Web Access**:



21. Click **OK**, then **Close**.

22. Select **RD Licensing**:



23. In the **Server Selection** page, move the local machine to the **Selected** pane.

24. Click **Next, Add** and wait for the installation to finish.

25. On completion, click **Close**.

Separate-Server Installation Procedure

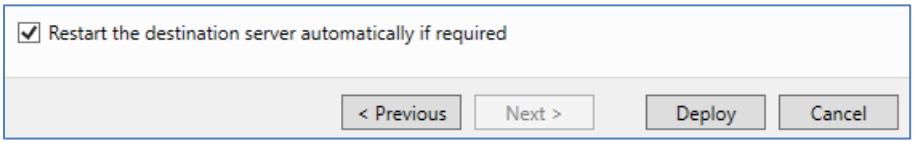
Use this procedure if the Web Access Server and RD App Server use separate machines.

At the Web Access Server:

1. In **Server Manager**, select **Local Server**.
2. Click **Add Roles and Features** from the **Manage** menu.
3. In the Add Roles and Features Wizard, apply the settings shown in the following table (leave all other options at their default settings).

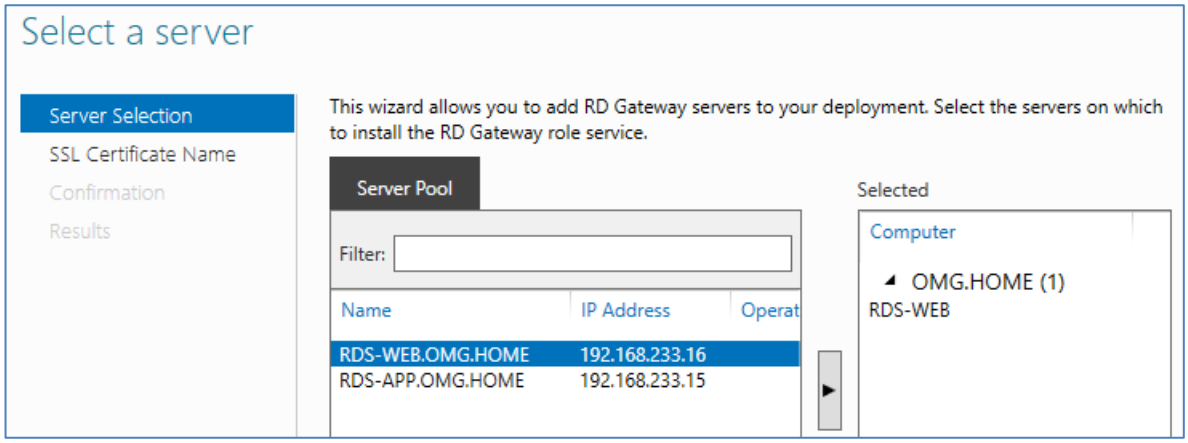
Screen Name	Settings
Installation Type	Select **Remote Desktop Services installation**.
Deployment Type	Select **Standard deployment** and click **Next**.
Deployment Scenario	Select **Session-based desktop deployment**.
Role Services	Click **Next**.
RD Connection Broker	Move the RD App Server to the **Selected** pane.
RD Web Access	Move the Web Access Server to the **Selected** pane.
RD Session Host	Move the RD App Server to the **Selected** pane.

4. Click **Next**.
5. Near the bottom of the **Confirmation** page, select **Restart the destination server automatically if required** and click **Deploy**:

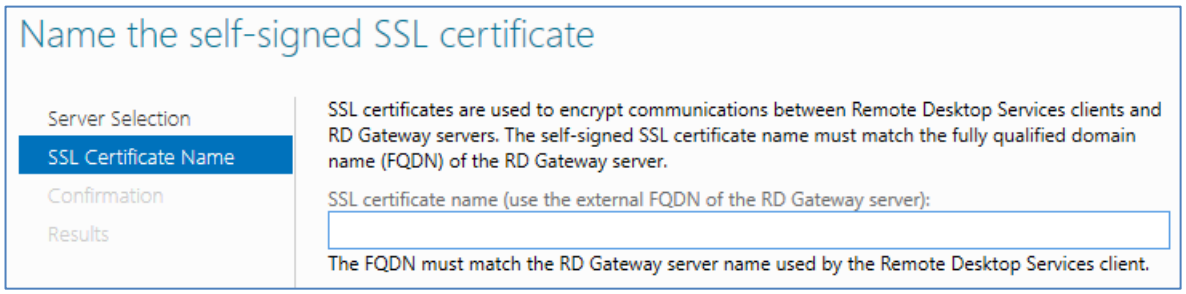


6. On completion, click **Close** and reboot the server.
7. In **Server Manager**, select **Remote Desktop Services**.
8. Select **RD Gateway**.

9. In the Server Selection page, move the Web Access Server to the **Selected** pane:

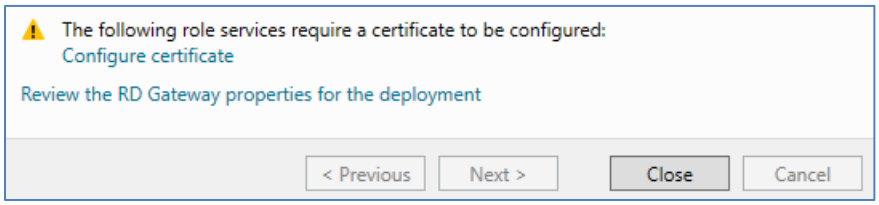


10. In the **SSL Certificate Name** page, enter the Fully Qualified Domain Name (FQDN) of the Web Access Server into the **SSL certificate name** field:

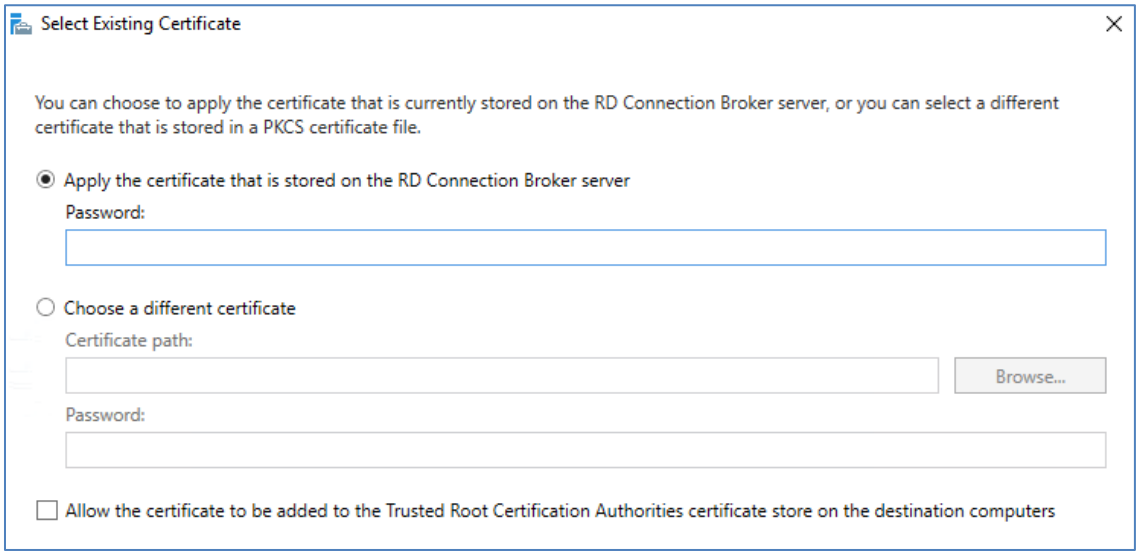


11. Click **Next**, then **Add** and wait for the installation to finish.

12. Once the installation is complete, click **Configure certificate** near the bottom of the window:



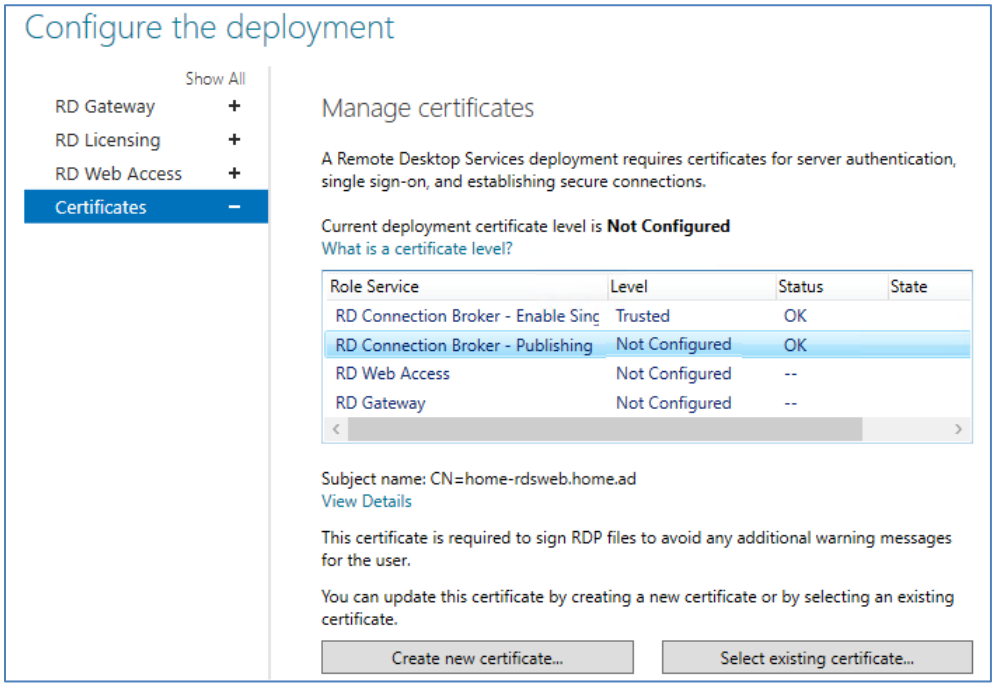
13. Click **Select existing certificate**. The following window is displayed:



14. In the Select Existing Certificate window:
    a) Browse to the .pfx file.
    b) Specify the password in the **Password** field.
    c) Select **Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on the destination computers**.
    d) Click **OK**.

15. Click **Apply**.

16. In the **Certificates** page, select **RD Connection Broker – Publishing** and click **Select existing certificate…**:

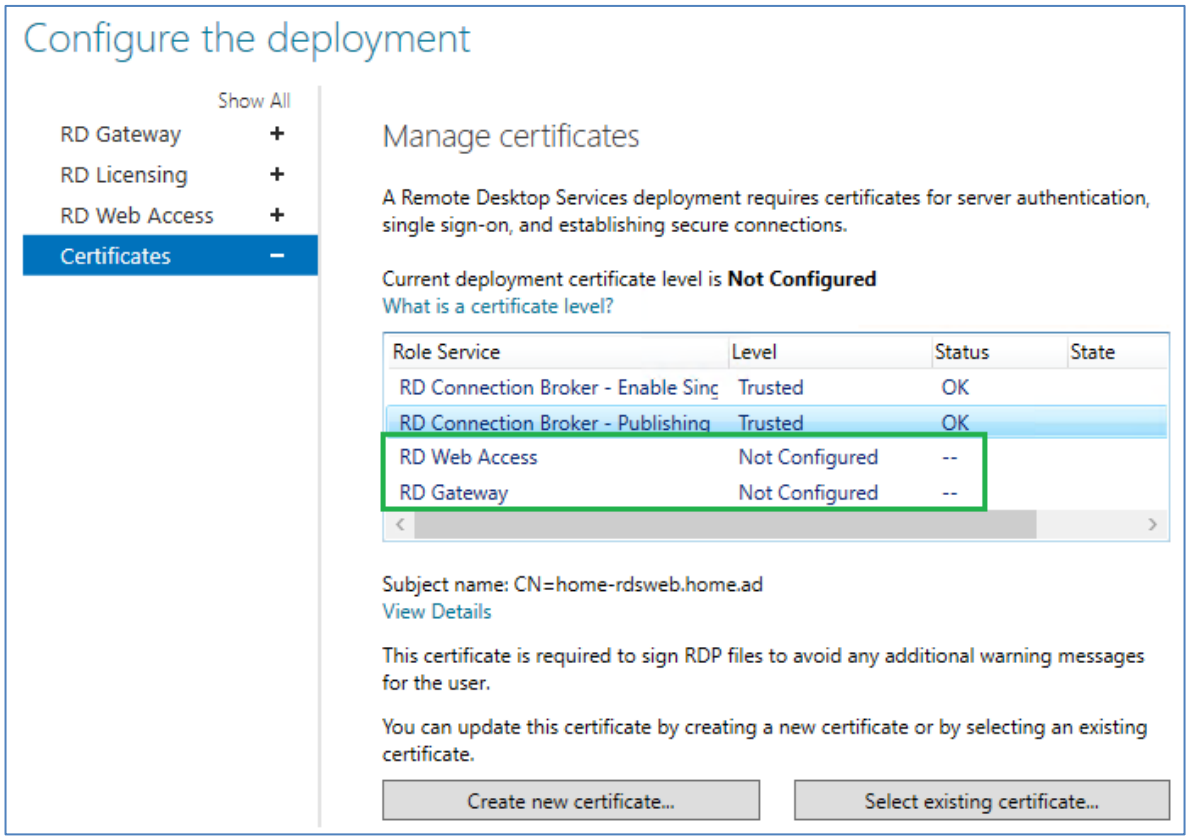


17. Browse to the certificate pfx file:

18. Enter the password and select **Allow the certificate to be added to the Trusted Root Certification Authorities certificate store on the destination computers**.

19. Click **OK**, then **Apply**.

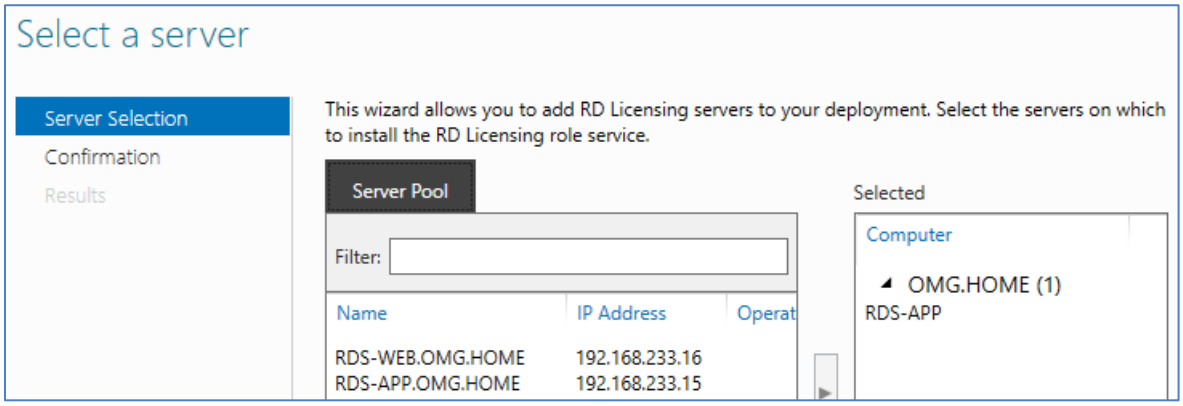
20. Repeat steps 16 – 19 for both **RD Gateway** and **RD Web Access**:



21. Click **OK**, then **Close**.

22. Select **RD Licensing**:

23. In the **Server Selection** page, move the RD App Server to the **Selected** pane:

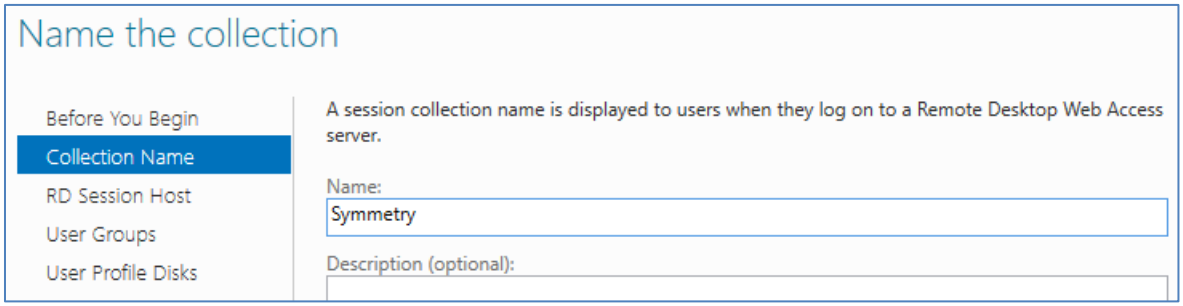


24. Click **Next, Add** and wait for the installation to finish.

25. On completion, click **Close**.

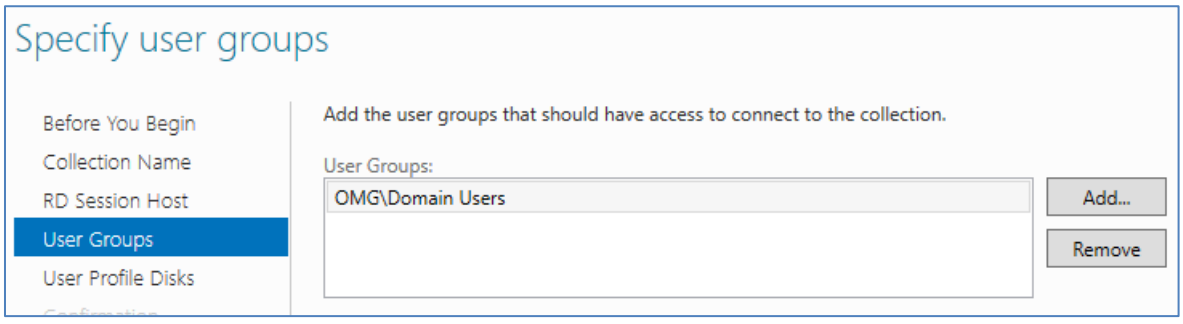
26. Click **Create Session Collections**.

27. In the **Collection Name** page, give the collection a name (e.g. "Symmetry"):

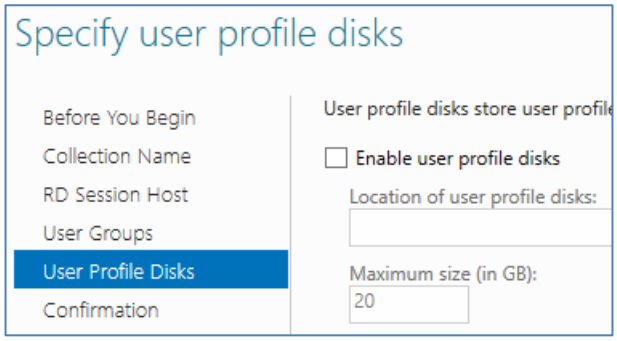


28. Move the RD App Server to the **Selected** pane and click **Next**.

29. In the **User Groups** page, specify the user group that will have access to the RDS connection:



30. In the **User Profile Disks** page, deselect **Enable user profile disks**:



31. Click **Next**, then **Create**.

32. On completion, click **Close**.

33. In the collection, click **publish RemoteApp programs**.

34. Select the **Calculator** and click **Next**.

35. Click **Publish**, then **Close**.

Step 6 – Test the RDS Connection

You should test that the main RDS setup has been successful before installing the Symmetry web-access components.

On a machine that is not the Web Access Server or RD App Server:

1. Open a web browser.

2. Go to https://< WebServer>/rdweb (where WebServer is replaced by the name of the Web Access Server).

3. Log in using your domain credentials.

4. Select **Calculator**.

5. Open the downloaded RDP file.

6. Input your domain credentials and click **OK**. The calculator should open via RDS.

Step 7 – Install the Symmetry Client Software on the Web Server

At the RD App Server:

1. Run Symmetry setup.exe on the installation media and when prompted, enter the Symmetry "RDS/Citrix Server License" or "Symmetry Client Concurrent User License" number. Please refer to page 4 for information about Symmetry licensing.

2. Select the Symmetry server and follow the prompts to install Symmetry. Please refer to the *Symmetry Software Installation Manual* if you need assistance with any prompts displayed.

Step 8 – Set up the RDS Group

You now need to modify the RDS group details and add Symmetry to the group.

Same-Server Installation Procedure

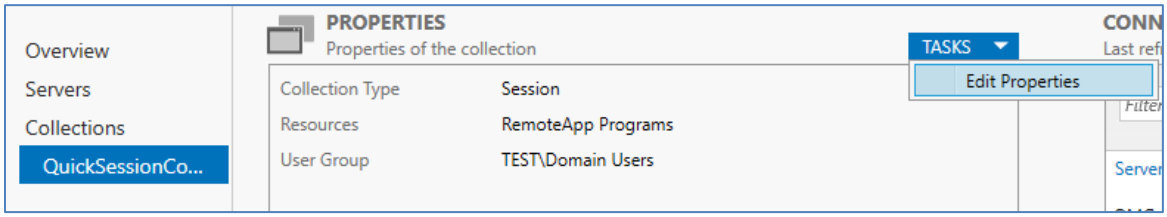
Use this procedure if the Web Access Server and RD App Server use the same machine.

At the Web Access Server:

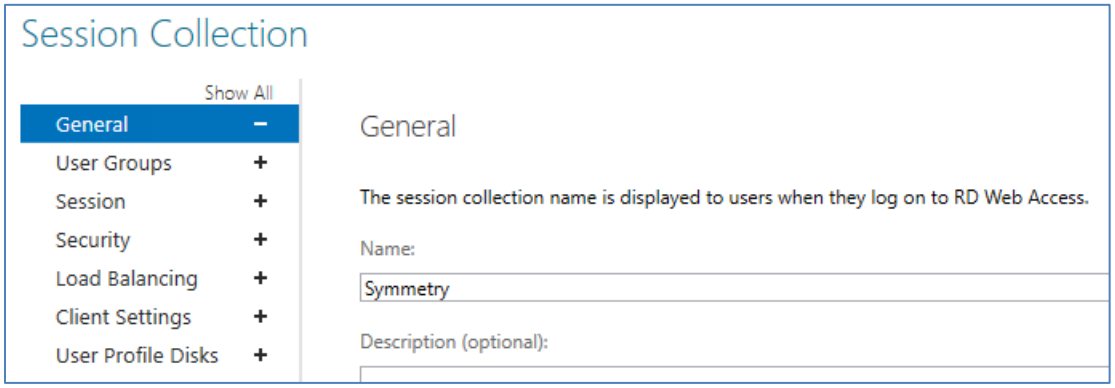
1. In **Server Manager**, select **Remote Desktop Services**.

2. Under **Collections**, select **QuickSessionCollection**.

3. To the right of the **PROPERTIES** box, click **TASKS** and select **Edit Properties**:



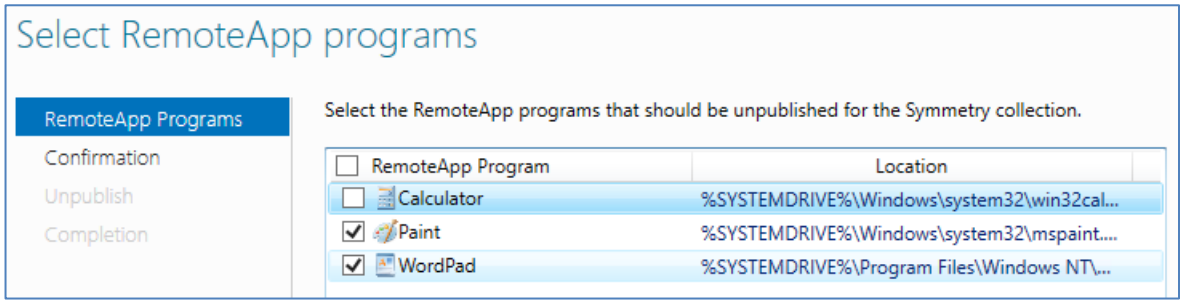
4. Change the name to “Symmetry”:



5. Click **OK**.

6. To the right of the **REMOTEAPP PROGRAMS** box, click **TASKS** and select **Unpublish RemoteApp Programs**.

7. Select **Paint** and **WordPad**:

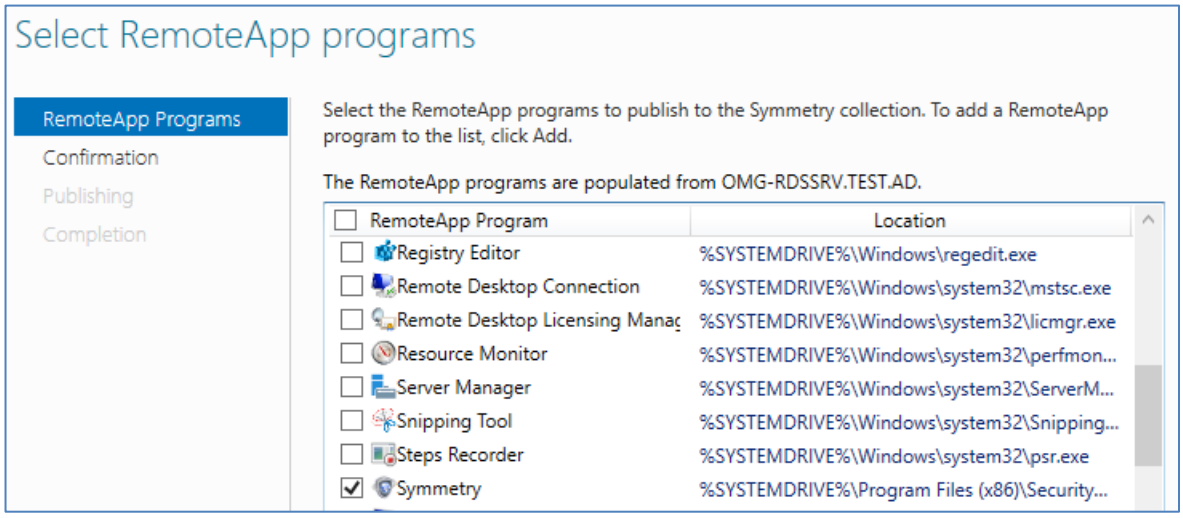


8. Click **Next**, check that Paint and Wordpad are listed in the Confirmation page, and click **Unpublish**.

9. Once the unpublishing is complete, click **Close**.

10. To the right of the **REMOTEAPP PROGRAMS** box, click **TASKS** and select **Publish RemoteApp Programs**.

11. Select **Symmetry** from the list of applications:



12. Click **Next**, check that Symmetry is listed in the Confirmation page and click **Publish**.

13. Once publishing is complete, click **Close**.

Separate-Server Installation Procedure

Use this procedure if the Web Access Server and RD App Server use separate machines.

At the Web Access Server:

1. In **Server Manager**, select **Remote Desktop Services**.
2. Select the **Symmetry** collection.
3. To the right of the **REMOTEAPP PROGRAMS** box, click **TASKS** and select **Publish RemoteApp Programs**.
4. Select **Symmetry** from the list of applications and click **Next**.
5. Check that Symmetry is listed in the Confirmation page and click **Publish**.
6. Click **Close**.

Step 9 – Assign Permissions

At the RD App Server:

1. In **Server Manager**, click **Tools, Computer Management**.
2. Under **System Tools** in the tree, select **Local Users and Groups** (available only if you are not using the primary domain controller).
3. Click **Groups**.
4. Right-click **Remote Desktop Users** and select **Add to Group**.
5. Add **Domain Users**, if it is not already included.

On the primary domain controller:

1. In **Server Manager**, click **Tools, Active Directory User and Computers**.
2. Make sure that any user who is going to use Symmetry through RDS is a member of the following groups:

   Remote Desktop Users

   ACSUsers. The name of the group may be "ACSUsers", or a different group name may have been selected for use as ACSUsers during the installation of the Symmetry software (as described in the *Symmetry Software Installation Manual*).

Step 10 – License RDS

In this step, you will license RDS (an RDS license is required separately from the Symmetry software).

At the licensing server:

1. In **Server Manager**, Click **Remote Desktop Services**.
2. In the Overview page, choose **Edit Deployment Properties** from the **TASKS** menu.
3. Display the RD Licensing page and choose the licensing mode (**Per Device** or **Per User**), then click **OK**.
4. In the Servers page, right-click the server that was configured as the RDS License Server and choose **RD Licensing Manager**.
5. In the RD Licensing Manager window, right-click the server, choose **Activate Server** and follow the steps to install and activate the purchased license.
6. Make sure that the license server is a member of the Terminal Server License Servers group in Active Directory Domain Services.

Step 11 – Test that the Symmetry Client Software can start

Note: The following procedure must not be actioned through a Remote Desktop session, otherwise Symmetry will fail to detect the web server.

At the RD App Server:

1. Start the Symmetry software using the desktop icon. The following is displayed:

Note: If you are unable to display the above, log into Windows as the user who is assigned to run the Symmetry services and try again.

2. Log in as a Symmetry user who has installer-level permissions assigned.

The Symmetry Installation Wizard is not displayed; the Symmetry client is automatically defined in the "Install/System/Clients" screen.

Step 12 – Add Symmetry Licenses

Carry out this step only if you are using the "RDS/Citrix Client Access Licensing" (CAL) method (see page 4).

In the Symmetry software:

1. Check that the Symmetry "RDS/Citrix Server" license has been registered:
   a) Display the "Maintenance/Licensing/System Licenses screen.
   b) If not already done, register the Symmetry "RDS/Citrix Server" license (and the main Symmetry license, if that has also not been registered).
2. Add a license to enable remote clients to use Symmetry:
   a) Display the "Maintenance/Licensing/Concurrent Licenses" screen.
   b) Install an "RDS/Citrix Client Users" license and/or an "RDS/Citrix Client Visitors" license, as required.

Step 13 – Configure Alarm Routing

If you require alarms to be displayed to users at the RDS clients, select the routing profiles set up for the alarms (as configured in the "Operation/Alarms/Routing Profiles" screen) in one or more of the following screens:

- "Maintenance/User & Preferences/Roles"
- "Maintenance/User & Preferences/Accounts"
- "Install/System/Clients" (by selecting the Symmetry client defined for the web server). This is applicable only if you are using the "RDS/Citrix Client Access Licensing" method, as the "Symmetry Concurrent User Licensing" method does not include a Symmetry client to represent the web server.

  As is normally the case, if routing profiles are assigned to a client, any routing profiles assigned to roles or accounts are not used.

For further information, please refer to *Overview of Alarm Routing* in the *Symmetry Online Help*.

To monitor alarms at an RDS web client, a Symmetry user must be logged into the Symmetry software and have permission to view the "Home/Monitoring/Alarms" screen.

Step 14 – Connect to Symmetry from a Remote Machine

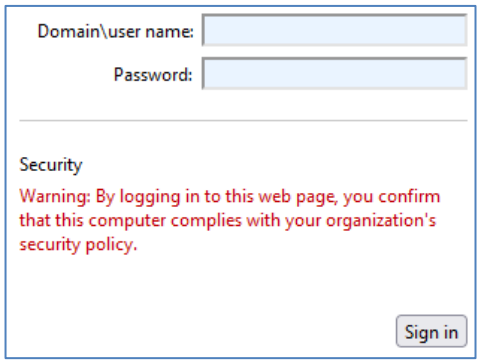
Installation is now complete. This step explains how to connect to Symmetry remotely from a web browser. It is important to test this process.

At a remote machine:

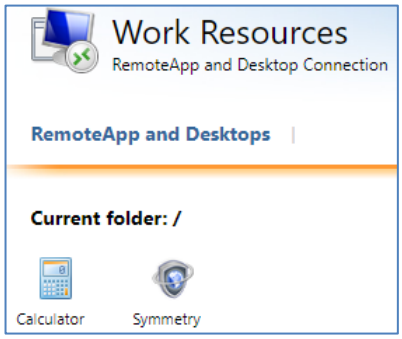
1. Open the web browser.
2. Enter https://<RDAppServerName>/RDWeb

Where <RDWebAccessServerName> is the name of the Web Access Server.

3. On the login page, enter your domain login details, as shown next.



4. Click the **Symmetry** icon:



5. A file will download.

If you are using **Microsoft Edge**:

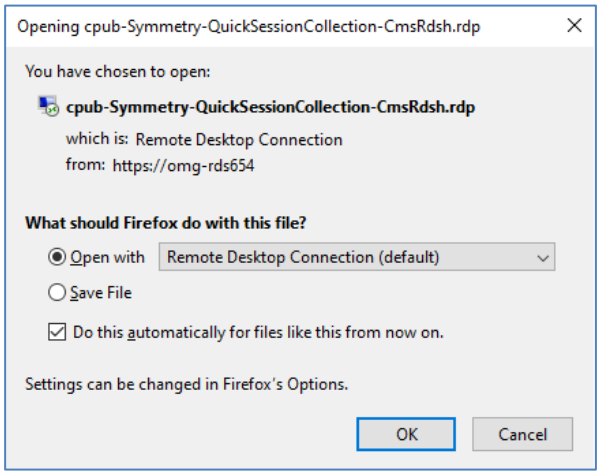
Optionally, right-click the downloaded file and select **Always open files of this type**.

If you are using **Google Chrome**:

Optionally, click the up-arrow on the download and select **Always open files of this type**.

If you are using **Mozilla Firefox**:

In the pop-up window, select **Open with – Remote Desktop Connection** and, optionally, **Do this automatically for files like this from now on**:



6. Click the file and log into Windows using your domain login details.

7. Click **Symmetry** and log into Symmetry.

Optional Steps

The following are optional steps that you may need to follow depending on site requirements.

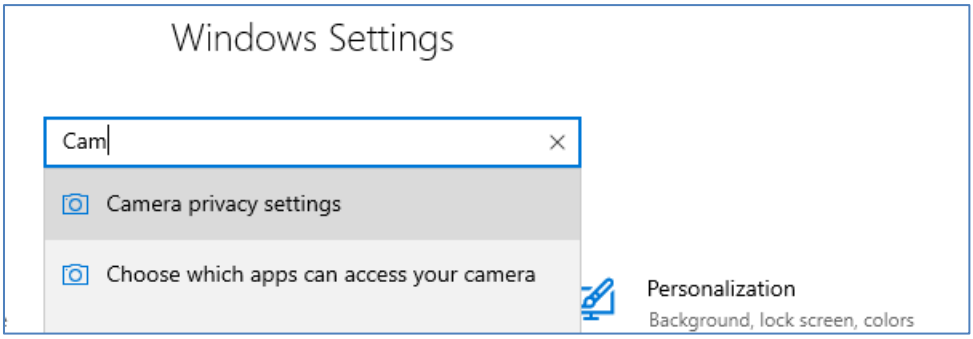
Enabling Web Cameras

Use the following procedure if remote Symmetry users need to be able to use web cameras to capture live images of people in the "Home/Identity/Card Holders" or "Home/Identity/Visitors" screen. When an image is captured, it is stored with the card details and can be printed on the badge.

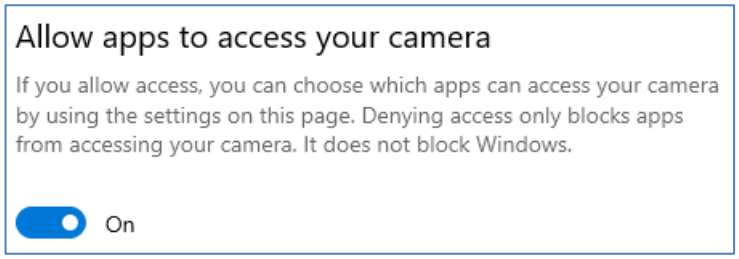
On the RD App Server:

1. Select **Start, Settings**.

2. Search for "camera" and select **Camera privacy settings**:



3. Switch on **Allow apps to access your camera**:



On the domain controller:

1. Open **Group Policy Management**.
2. Right-click **Forest, Domains, Domain Name, Group Policy Objects**, and select **New**.
3. Give the object a name (e.g. "RDS-WebCam") and click **OK**.
4. Right-click the policy and select **Edit**.
5. Open **Computer Configuration, Policies, Administrative Template, Windows components, Remote Desktop Services, Remote Desktop Session Host, Device and Resource Redirection**.
6. Select **Allow audio and video playback redirection**.
7. Click **Edit policy setting**. and set to enabled.
8. Close the window.
9. Under **Security Filtering**, click **Add…**.
10. Specify the domain user group of the users that will be operating Symmetry.
11. Click **OK**.

Installing a Fargo Badge Printer Driver

To encode a card on a supported Fargo badge printer (see page 6), the latest Fargo driver must be installed and configured on the Symmetry server, on the RD App Server and on any remote machines where Symmetry is accessed through a web browser.

On the RD App Server, **Use Remote Desktop Easy Print printer driver first** must be set to **disabled**. This setting is located in Group Policy Object, Local Computer Policy, Computer Configuration, Administrative Templates, Windows Components, Remote Desktop Services, Remote Desktop Session Host, Printer Redirection.

Chapter 3: Installation under Citrix XenApp

This chapter describes how to install and publish Symmetry on a Citrix XenApp server. This chapter assumes that the Citrix software has already been installed and configured ready for use.

Step 1 – Install the Symmetry Client Software on the XenApp Server

Note: Before following this step, make sure that Symmetry is already installed on the Symmetry server.

Note: If you are using an Active Directory account, please make sure that your user profile does not have an associated Home Folder, otherwise installation will fail.

Note: The following procedure must not be actioned through a Remote Desktop session, otherwise Symmetry will fail to detect the web server.

At the Citrix server where you want to install the Symmetry client software:

1. Run Symmetry setup.exe on the installation media and when prompted, enter the Symmetry "RDS/Citrix Server License" or "Symmetry Client Concurrent User License" number. Please refer to page 4 for information about Symmetry licensing.

2. Select the Symmetry server and follow the prompts to install Symmetry. Please refer to the *Symmetry Software Installation Manual* if you need assistance with any prompts displayed.

Step 2 – Add Symmetry Licenses

Carry out this step only if you are using the "RDS/Citrix Client Access Licensing" (CAL) method (see page 4).

In the Symmetry software:

1. Check that the Symmetry "RDS/Citrix Server" license has been registered:
   a) Display the "Maintenance/Licensing/System Licenses screen.
   b) If not already done, register the Symmetry "RDS/Citrix Server" license (and the main Symmetry license, if that has also not been registered).

2. Add a license to enable remote clients to use Symmetry:
   a) Display the "Maintenance/Licensing/Concurrent Licenses" screen.
   b) Install an "RDS/Citrix Client Users" license and/or an "RDS/Citrix Client Visitors" license, as required.

Step 3 – Configure Alarm Routing

If you require alarms to be displayed to users at the Citrix clients, select the routing profiles set up for the alarms (as configured in the "Operation/Alarms/Routing Profiles" screen) in one or more of the following screens:

- "Maintenance/User & Preferences/Roles"
- "Maintenance/User & Preferences/Accounts"
- "Install/System/Clients" (by selecting the Symmetry client defined for the web server). This is applicable only if you are using the "RDS/Citrix Client Access Licensing" method, as the "Symmetry Concurrent User Licensing" method does not include a Symmetry client to represent the web server.

  As is normally the case, if routing profiles are assigned to a client, any routing profiles assigned to roles or accounts are not used.

For further information, please refer to *Overview of Alarm Routing* in the *Symmetry Online Help*.

To monitor alarms at a Citrix web client, a Symmetry user must be logged into the Symmetry software and have permission to view the "Home/Monitoring/Alarms" screen.

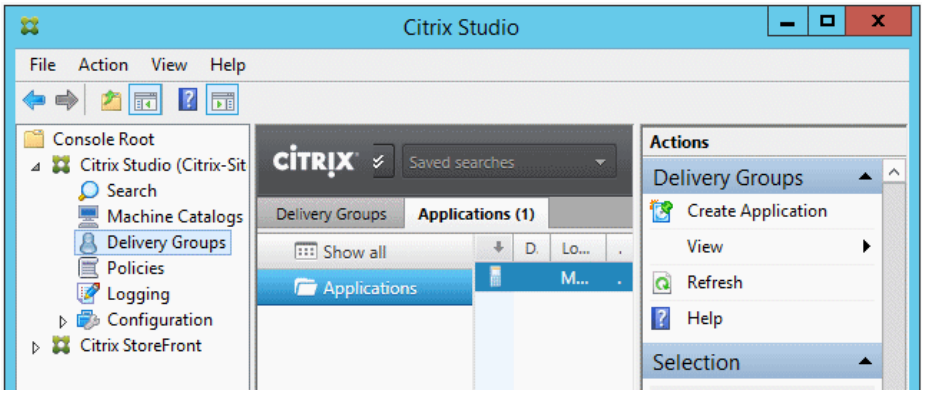
Step 4 – Configure Badge Printers (Optional)

Encoding and printing on Fargo printers is possible using a printer attached to a Citrix client PC. The printer drivers need to be installed at every Citrix client that needs to use it. The printer can be shared over the network to allow other Citrix clients to print to it, but they require the printer driver to be installed.

Step 5 – Publish Symmetry

On the Citrix server:

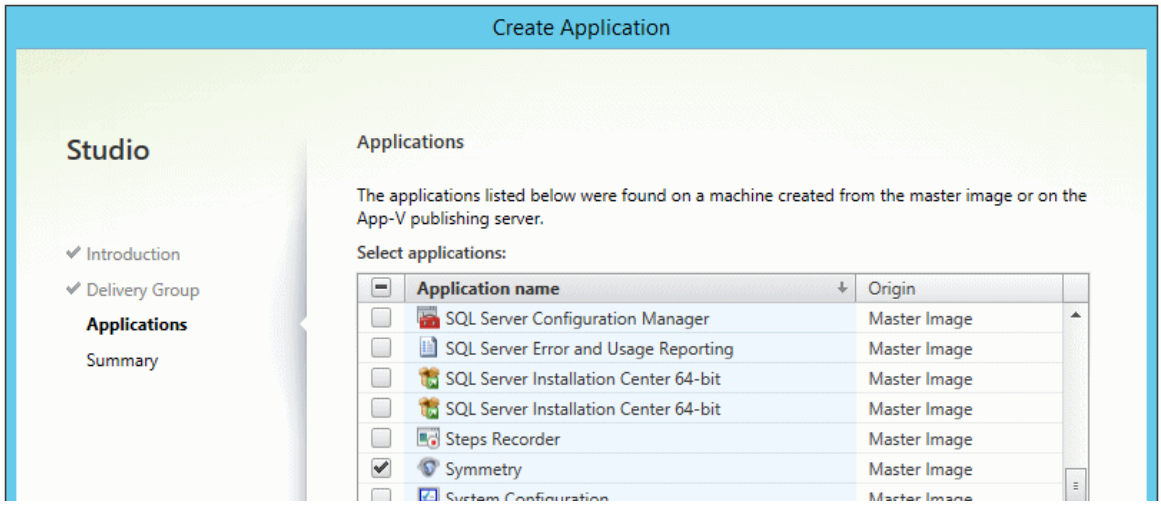
1. Launch Citrix Studio.
2. Select **Delivery Groups**, and in **Actions**, click **Create Application**:



The Create Application wizard is displayed.

3. In the Delivery Group page, select the delivery group where the Symmetry Citrix Client Access software has been installed.

4. In the Applications page, select **Symmetry**:



5. Click **Finish**.

You should now be able to connect to Symmetry from a remote web browser by entering the web address of the Citrix Store Front.

Step 6 – Prevent Uploading of Files from Browser Machines

You may want to prevent end users from being able to use options within Symmetry to browse to files (such as card holder images) located on the local browser machine, since the local machine may not be located within a secure environment. Instead, you may want browsing to be constrained to permitted locations on the Citrix web server machine.

To limit browsing to the Citrix web server, set the Citrix **Auto Connect Client Drives** profile setting to DISABLED.

Appendix A: Starting a Remote Desktop Connection

This appendix describes how to connect a computer remotely using Microsoft Remote Desktop Connection.

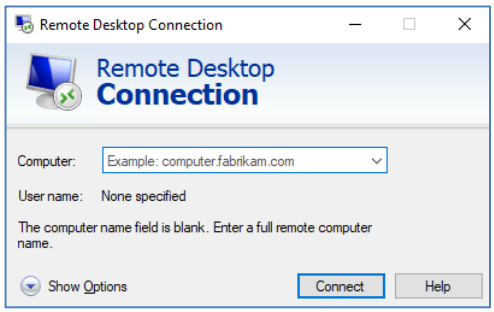
The Remote Desktop Connection tool is a built-in part of Windows that operates standalone without the need for web server components.

Connecting to a Computer Remotely

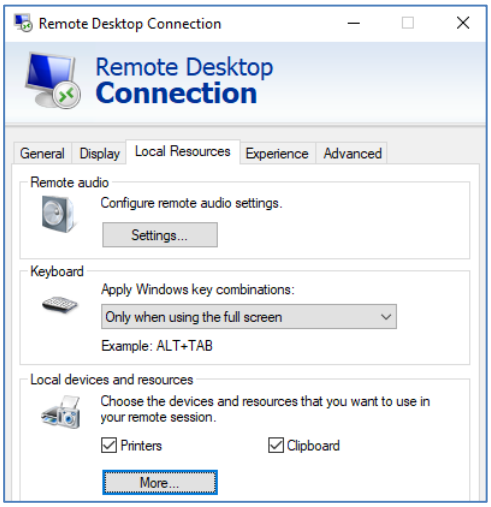
Note: The computer you want to connect to must allow remote connections, as configured in the Windows Settings (Control Panel).

To connect to a computer remotely:

1. Open the Remote Desktop Connection application (e.g. by entering **Remote Desktop** in the Windows Search box). The following is displayed:

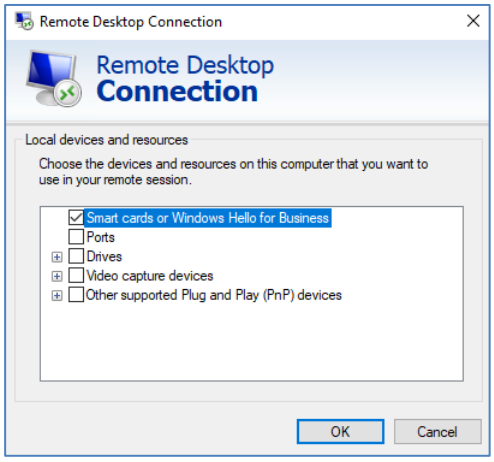


2. Optionally, if you want to use a local USB device during the Remote Desktop session:
   a) Click **Show Options** near the bottom-left corner of the window.
   b) Display the Local Resources tab, as shown next.

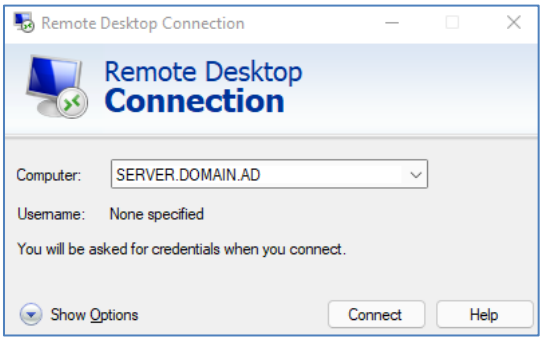


c) Under **Local devices and resources**, click **More...**.

d) Select the required device(s) and click **OK**:



3. Enter the server name (e.g. Servername.domain) and click **Connect**:



4. Enter your domain credentials and click **OK**: