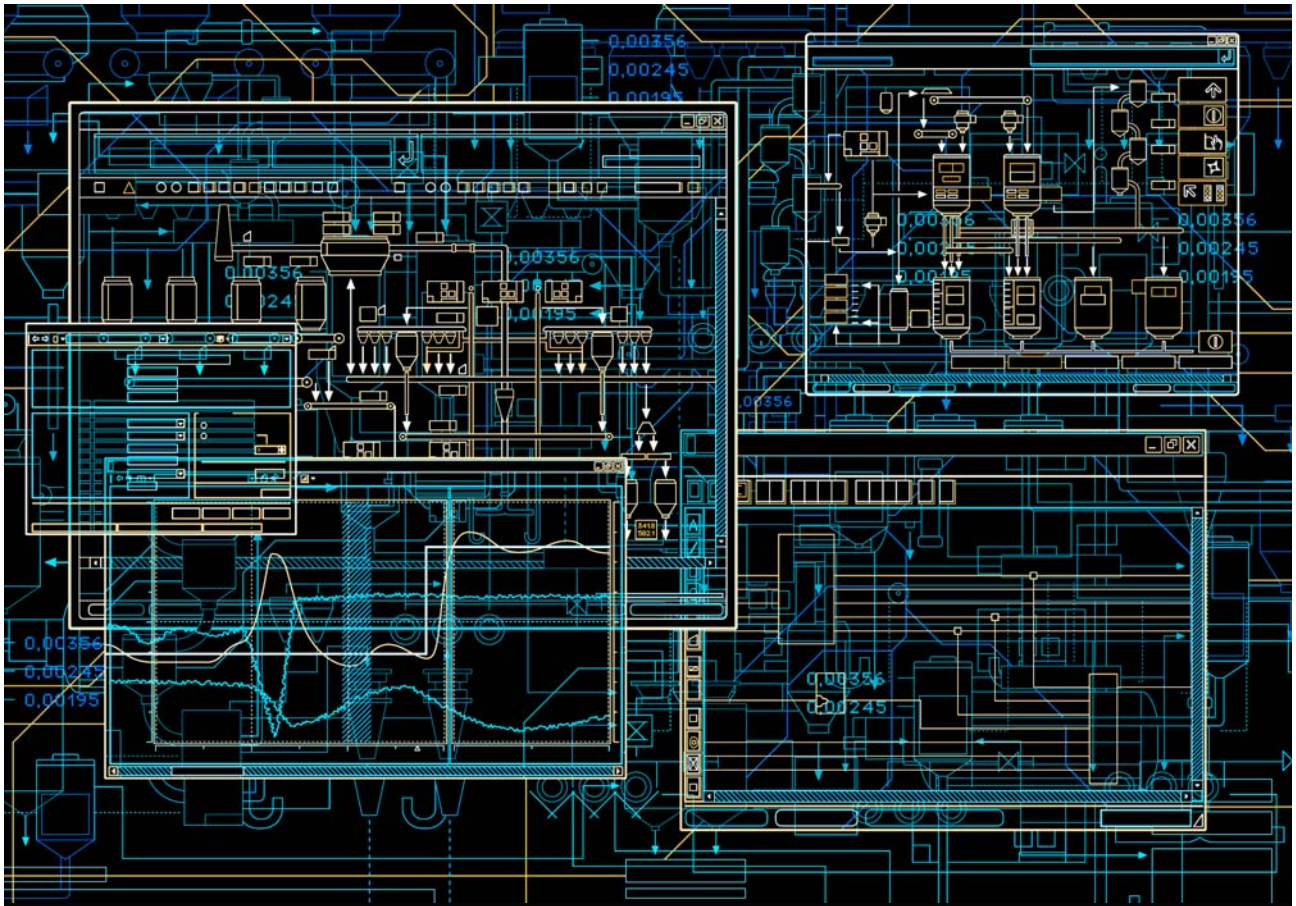

System 800xA Operations

Operator Workplace
Support for Mobile Devices

System Version 6.0

Power and productivity
for a better world™

System 800xA Operations

Operator Workplace
Support for Mobile Devices

System Version 6.0

NOTICE

This document contains information about one or more ABB products and may include a description of or a reference to one or more standards that may be generally relevant to the ABB products. The presence of any such description of a standard or reference to a standard is not a representation that all of the ABB products referenced in this document support all of the features of the described or referenced standard. In order to determine the specific features supported by a particular ABB product, the reader should consult the product specifications for the particular ABB product.

ABB may have one or more patents or pending patent applications protecting the intellectual property in the ABB products described in this document.

The information in this document is subject to change without notice and should not be construed as a commitment by ABB. ABB assumes no responsibility for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

This document and parts thereof must not be reproduced or copied without written permission from ABB, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

The software or hardware described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license. This product meets the requirements specified in EMC Directive 2004/108/EC and in Low Voltage Directive 2006/95/EC.

TRADEMARKS

All rights to copyrights, registered trademarks, and trademarks reside with their respective owners.

Release: August 2014
Document number: 2PAA110154-600

Table of Contents

Section 5 - Certificate Authority

Section 6 - Creating Certificates

Section 7 - Configuring NPS (RADIUS)

Section 8 - Remote Desktop Session Host Server Configuration

Section 9 - 800xA Customization for iPad®

Section 10 - Configuring BAT54

Section 11 - Remote Desktop Session Host Server Routing

Section 12 - Certificates for Mobile Devices

Section 13 - Remote Connection to 800xA

Section 14 - Lock iPad®

About This User Manual

General

Any security measures described in this User Manual, for example, for user access, password security, network security, firewalls, virus protection, etc., represent possible steps that a user of an 800xA System may want to consider based on a risk assessment for a particular application and installation. This risk assessment, as well as the proper implementation, configuration, installation, operation, administration, and maintenance of all relevant security related equipment, software, and procedures, are the responsibility of the user of the 800xA System.

System 800xA is used for monitoring and controlling a process plant. This user manual describes the configuration of an Operator Workplace.

Information in this user manual is intended for the engineers of a process plant.

User Manual Conventions

Microsoft Windows conventions are normally used for the standard presentation of material when entering text, key sequences, prompts, messages, menu items, screen elements, etc.

Feature Pack

The Feature Pack content (including text, tables, and figures) included in this User Manual is distinguished from the existing content using the following two separators:

Feature Pack Functionality

<Feature Pack Content>

Feature Pack functionality included in an existing table is indicated using a table footnote (*) :

*Feature Pack Functionality

Feature Pack functionality in an existing figure is indicated using callouts.

Unless noted, all other information in this User Manual applies to 800xA Systems with or without a Feature Pack installed.

Warning, Caution, Information, and Tip Icons

This User Manual includes Warning, Caution, and Information where appropriate to point out safety related or other important information. It also includes Tip to point out useful hints to the reader. The corresponding symbols should be interpreted as follows:

Electrical warning icon indicates the presence of a hazard which could result in *electrical shock.*

Warning icon indicates the presence of a hazard which could result in *personal injury.*

Caution icon indicates important information or warning related to the concept discussed in the text. It might indicate the presence of a hazard which could result in *corruption of software or damage to equipment/property.*

Information icon alerts the reader to pertinent facts and conditions.

Tip icon indicates advice on, for example, how to design your project or how to use a certain function

Although Warning hazards are related to personal injury, and Caution hazards are associated with equipment or property damage, it should be understood that operation of damaged equipment could, under certain operational conditions, result in degraded process performance leading to personal injury or death. Therefore, fully comply with all Warning and Caution notices.

Terminology

A complete and comprehensive list of terms is included in *System 800xA System Guide Functional Description (3BSE038018*)*. The listing includes terms and definitions that apply to the 800xA System where the usage is different from commonly accepted industry standard definitions and definitions given in standard dictionaries such as Webster's Dictionary of Computer Terms. Terms that uniquely apply to this User Manual are listed in the following table.

Term/Acronym	Description
802.11	IEEE Standard to encourage inter operability among wireless networking equipment
802.1x	IEEE Standard for an authentication framework for wireless LANs
ACL	Access Control List
AP	Access Point
CA	Certification Authority
EAP	Extensible Authentication Protocol
FW	Firewall
LAN	Local Area Network
MAC	Media Access Control
NPS	Network Policy Server
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial-In User Service
SSID	Service Set Identifier
SSL	Secure Socket Layer
TLS	Transport Level Security (equivalent to SSL)
WEP	Wired Equivalent Privacy (802.11 basic encryption)
Wi-Fi	Wireless Fidelity

Term/Acronym	Description
WLAN	Wireless Local Area Network
WPA	Wireless Protected Access

Released User Manuals and Release Notes

A complete list of all User Manuals and Release Notes applicable to System 800xA is provided in *System 800xA Released User Manuals and Release Notes (3BUA000263*)*.

System 800xA Released User Manuals and Release Notes (3BUA000263)* is updated each time a document is updated or a new document is released. It is in pdf format and is provided in the following ways:

- Included on the documentation media provided with the system and published to ABB SolutionsBank when released as part of a major or minor release, Service Pack, Feature Pack, or System Revision.
- Published to ABB SolutionsBank when a User Manual or Release Note is updated in between any of the release cycles listed in the first bullet.

A product bulletin is published each time *System 800xA Released User Manuals and Release Notes (3BUA000263*)* is updated and published to ABB SolutionsBank.

Section 1 Introduction

Integration of mobile technology in the automation and process control environment reduces cost, increases productivity of existing resources and improves operating efficiency. Utilizing standard technologies such as Microsoft's Remote Desktop Protocol (RDP), mobile devices can access the 800xA system over wireless networks. Application of Microsoft security patches should be applied to all nodes in the 800xA network.

It is highly recommended that ABB Qualified Security Updates are applied after they are available. Since the Remote Desktop Session servers will be exposed to the wireless networks, security patch updating is of higher importance.

In this guide, iPad® is used as the mobile device. This document provides a guideline that will assist in understanding the technologies used in WIFI deployment.

Mobile support for 800xA is not intended for remote over the internet operation of a production environment. It is intended for production environment mobility where operators and production staff can view the process. Any operation of the system without physical visual contact should be avoided. The iPad® should be dedicated to remote operation within the production environment and not be taken home or used in the office. There should also be no 3G/4G capabilities in the iPad®. Regulations should be in place which dictates that no usage of phone based hotspots is allowed in conjunction with the iPad®.

Due to the demanding requirements of industrial systems, it is highly recommended that specialists in WIFI industrial deployments are consulted for planning and implementation of the wireless solution.

Architecture

An overview of the concepts involved in providing wireless access from a mobile device such as an iPad® to the 800xA system is shown in Figure 1. As an iPad® does not have a native remote desktop client, a third party application (Pocket Cloud Pro) is required. Wireless connectivity is provided by multiple wireless access points that also implements firewall and intrusion detection systems.

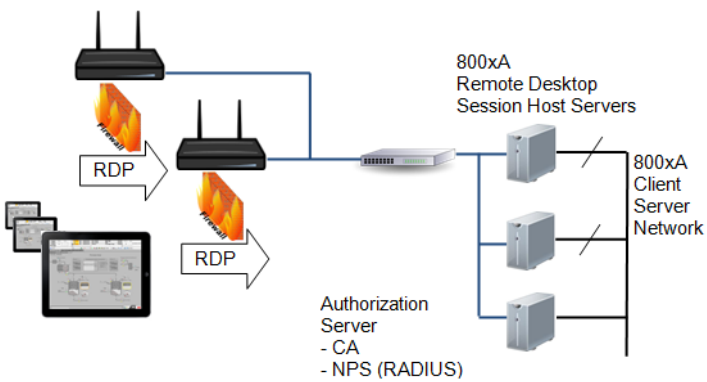

Figure 1. ABB 800xA Mobile Device Architectural Overview

The technology described in this guide is part of the IEEE 802.1X standard. Protected Extensible Authentication Protocol (PEAP), which uses certificates, is used to establish connection between wireless devices and wireless networks. This requires a Certificate Authority (CA) server to be present in the network. To provide security authorization, at least one Network Policy Server (NPS) server is used. This provides Remote Authentication Dial-In User Service (RADIUS) authorization functionality. A separate network is used for the server side of the wireless network to minimize exposed Windows services.

The wireless access points are connected to one or more 800xA Remote Desktop Session Hosts (previously called Terminal Servers) which provide the login sessions for the remote desktop connection.

Due to the limited screen size, graphic displays will need to be engineered accordingly.

Additional security measures must also be implemented to restrict who can log into the system, and that those users cannot operate equipment.

Server System Requirements

The expected functionality for the mobile access is that a user starts a remote session towards a Remote Desktop Session Host server. Only the 800xA workplace is to be presented with no desktop in the background when a remote desktop session has been established to a Remote Desktop Session Server through an iPad®.

To achieve this, the system must be Windows Server 2012 R2 with Remote Desktop Services and be a system with a domain controller.

The requirements:

- Windows Server 2012 R2
- Active Directory based system
- Remote Desktop Session Host with Remote Desktop Services role
- Remote Desktop Licensing

However, there are settings in the computer local user configuration which appears to provide the definition to run an application at logon, this does not work. The user settings must be defined in a domain.

The Remote Desktop Session Host (formally called Terminal Services) role must be installed before other applications could be installed. Addition and configuration of this role is described within this user guide.

Section 2 Concepts

This section describes the following:

- Factory Coverage
- Service Set Identifier
- Security

Factory Coverage

The coverage area is a major consideration for wireless implementation. Factory coverage is affected by structures, both moving and fixed, within the factory area.

Interference from any machine that has electrostatic discharge may require additional routers to be located in the vicinity to provide access to strong signals.

Manufacture specifications on range should be a guidance, but not the sole method for determining the layout of the wireless network. However, it is possible to place wireless routers at different locations to assess the coverage requirements. It is highly recommended to have a professional survey done for a comprehensive understanding of the coverage requirements. The survey should consider the changing conditions that may interfere with the wireless coverage in the factory. For example, when the production stock increases, during maintenance, or additional equipment entering the factory.

Access point placement best practices

The following provides a list of basic best practices when planning the access point coverage.

- Consider the coverage areas required.

- Consider the areas that should not have wireless access.
  For example, beyond the walls of the building
- Access points with overlapping signals should have different radio channels.
- Potential overlapping region should be considered in all directions, not just the current floor level.
- The physical potential signal blockages.
  For example, pillars, walls, steel beams, ventilation ducts, metal cabinets.
- Consider signals that has to go diagonally through a wall will experience a higher attenuation due to the thicker signal path.
- How will the environment change over time. Stock build up may interfere with signal strength.
- What are the potential electrical sources of interference.
  For example, arc welders, medical equipment, eclectic motors, wireless video cameras

Service Set Identifier

Service Set Identifier (SSID) is used to differentiate one wireless LAN (WLAN) from another. To enable a mobile device to connect to the same WLAN through different wireless routers, each wireless router is set up with the same SSID. The wireless routers are within the radio distance from each other. Each router should have a different channel configured.

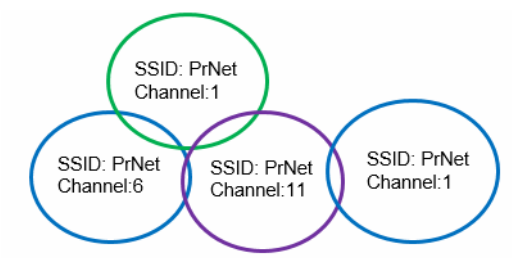

Figure 2. Wireless range and unique channel configuration example

Security

The security of a wireless system is dependent on the configuration of each of the components in the WLAN. This includes the physical configuration, the configuration of the devices and access points, and the subsequent monitoring of the system.

Understand the range of the wireless network. Considering that the wireless network is a potential attack point for hackers, it is important to understand where the wireless signals extend beyond the factory walls. These locations provide an opportunity for hackers to attempt to break into the network.

Use highest security available. The security level should be at least WPA2 or higher. WEP security is easier to hack. When selecting a secure key, do not use dictionary words, and use a mixture of letters, numbers, and characters such as "#%&". Many hacking techniques make initial attempts using a dictionary of common passwords as an easy entry into the system.

Ensure that all default passwords are changed.

Best practices are:

- Do not suppress SSID broadcast. This information can be obtained by more sophisticated hackers. Clients must probe for SSIDs which causes additional risks.
- Do not use MAC filtering. Hackers can easily modify the MAC address of their wireless devices to match allowed addresses.
- Use the strongest authentication possible. For example, WPA2

Section 3 Wireless Components

This section describes the following:

- Wireless Components
- Wireless Configuration

Wireless Components

Implementing a wireless solution should always have a strong focus on security. This guide describes a configuration that keeps the important nodes such as the domain controller from being on the physical network connected to the wireless access points. Hence, a separate server is used for the CA and NPS functionality. However, it is possible to have a primary and a backup NPS server, the initial support for mobile devices focuses on a single NPS server. There are many different methods for the implementation of security. The method described in this guide is based on a Certificate Authority and RADIUS server. These utilize existing Windows roles which reduces the requirements for additional third party systems.

Figure 3 presents these main components showing their communication dependency.

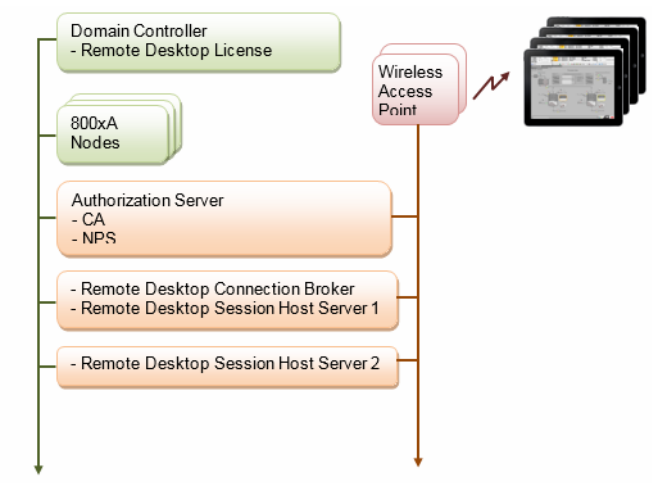

Figure 3. Overview of mobile network implementation

Establishing connection from the iPad® to the wireless access point is based WPA encryption and a certificate that has been generated in the Certificate Authority, and has previously been installed into the iPad®. Furthermore, RADIUS is used for the authentication where the user must provide domain credentials to establish connection. This provides a central method to remove the access to a lost iPad® by revoking the certificate or removing a user who should no longer have access to the system.

Multiple layers of defense should be used where possible. A separate network is used for the connection from the access points to the Remote Desktop Session Host servers. Both the access point and the Remote Desktop Session Host server have firewalls active. In the case of the BAT54 access point, this requires that the internal connection between wireless and physical network is in router mode. This intern requires that the DHCP is active in the access point, and that routing is setup in the Remote Desktop Session Host server.

Whilst the Remote Desktop Session Host server firewall will be setup using the 800xA System Installer, the access point is setup to only allow remote desktop protocol communication. In addition to the firewall, the BAT54 also contains an intrusion detection system. An intrusion attempt is typically scanning ports to determine potential vectors of attack. The intrusion detection system can be configured to detect the port scan, block the source address, and send an alert.

To provide remote authentication, a separate server is used for running the Certificate Authority (CA) and NPS (RADIUS - Remote Authentication Dial In Service). Whilst these functionalities could have been added to the domain controller, this would have exposed the domain controller to the wireless networks. This provides the link between the mobile device and the domain controller authentication. Having the CA and the NPS on the same server reduces complexity in maintenance of the certificates. In the access point, the RADIUS server address is added to enable its usage. Encryption will be set to WPA and use the Extension Authentication Protocol (EAP) - Protected EAP (PEAP). This allows the use of certificates and login using usernames and passwords defined in the Active Directory on the Windows Server to authenticate the mobile device onto the wireless network.

Wireless Configuration

To assist in understanding the configuration of the components that need to be installed and configured, the following diagram provides an example of an implementation that will be used for the subsequent descriptions in this user guide.

Practical implementations may see the requirement for utilizing VLANs to perform logical separation of network functionality.

The use of VLANs is not described in this document.

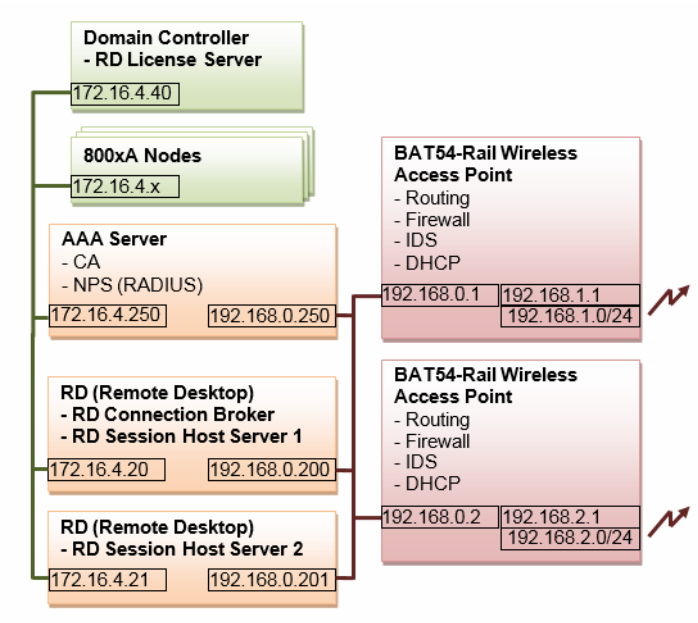

Figure 4. Example implementation of a mobile network

Section 4 Remote Desktop Sessions

This section describes the Remote Desktop Session (RDS) Server Licensing, RDS Server Licensing Configuration, RDS Server Role, and the RDS Server User Configuration.

RDS Host Server Licensing

By default, Windows Server allows to two administrative remote desktop session login. Beyond this, additional Remote Desktop CAL licenses are required. These are added to the Remote Desktop Session licensing server. In the example in this document, the Remote Desktop Licensing server is added to the domain controller.

Installation

Execute the following steps to add host server licensing role in the domain controller:

1. Logon to the Domain Controller and start the Server Manager.

2. Select **Roles > Add Roles and features**.

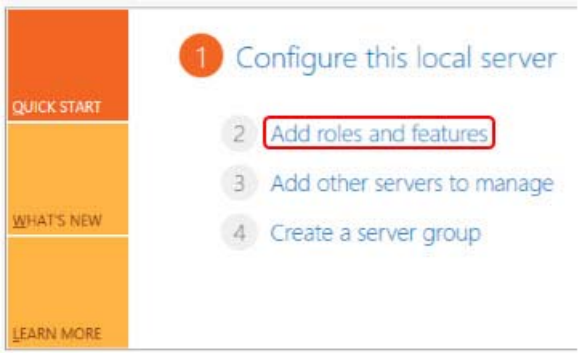

Figure 5. Accessing the Add Roles functionality

3. **Before You Begin** window appears. Click **Next**.

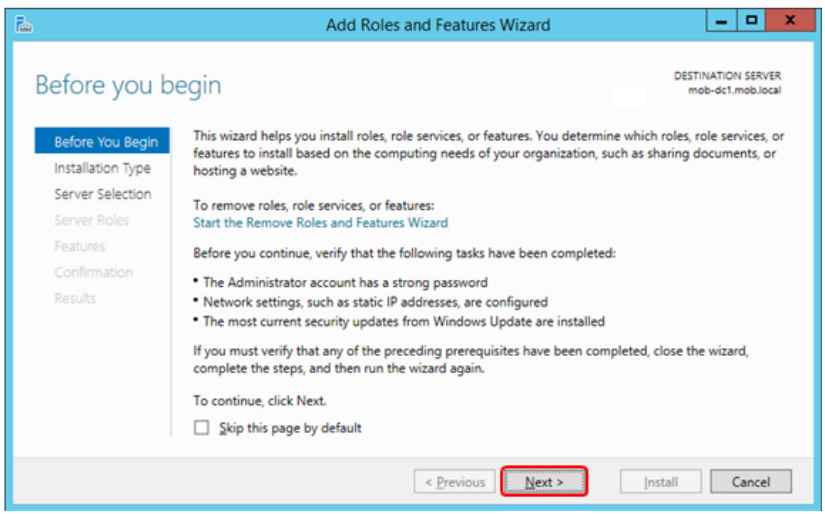

Figure 6. Before you begin information message

4. Select **Role-based** or **feature-based installation** and click **Next**.

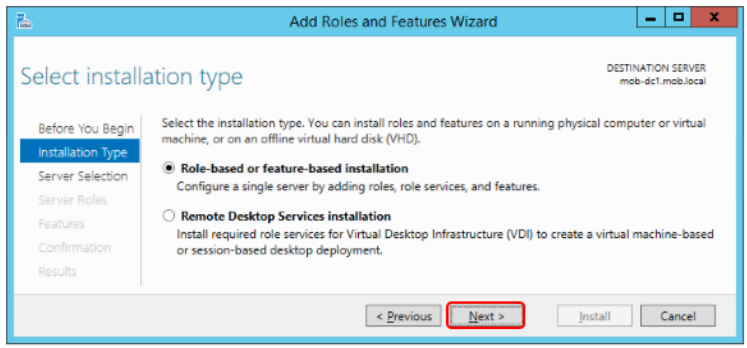

Figure 7. Selecting Installation Type

5. At the **Select destination server**, select the domain controller, and click **Next**.

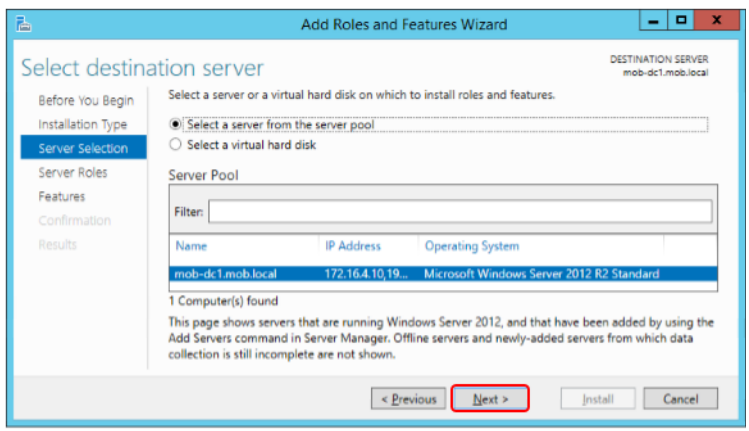

Figure 8. Selecting domain controller as the destination server for new roles

6. Select **Remote Desktop Services** as the additional role and click **Next**.

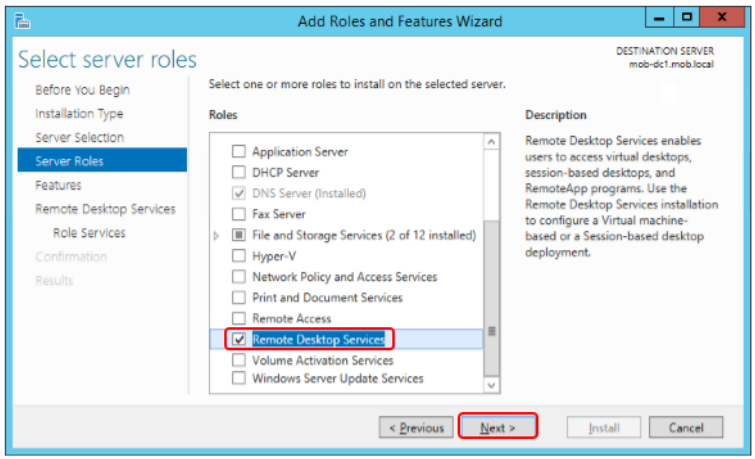

Figure 9. Adding the Remote Desktop Services role

7. Do not change the features. Click **Next.**

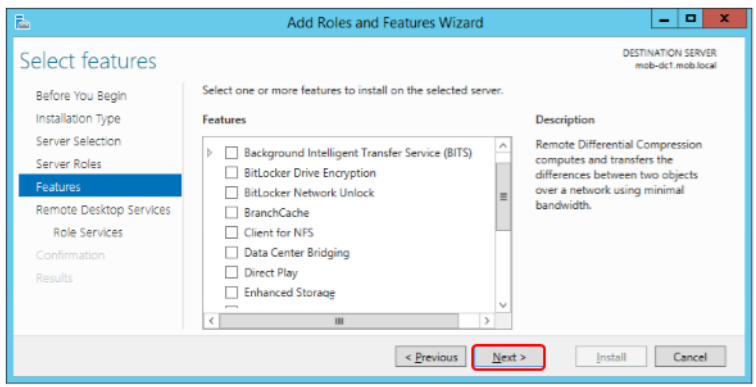

Figure 10. Leaving the additional features unchanged

8. **Remote Desktop Services** window appears. Click **Next**.

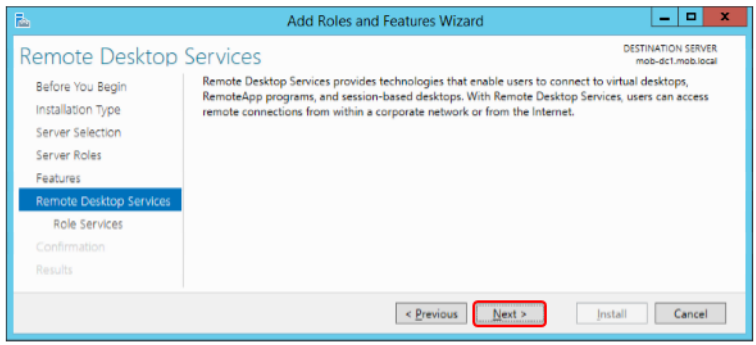

Figure 11. Introduction to Remote Desktop Services

9. Select **Remote Desktop Licensing** role, then the **Add Features** at the suggested additional features. Click **Next**.

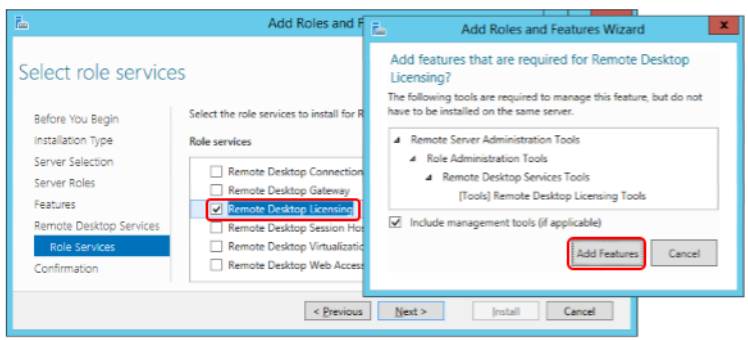

Figure 12. Adding the Remote Desktop Licensing role and additional features

10. Press **Install** in the **Confirmation Window**.

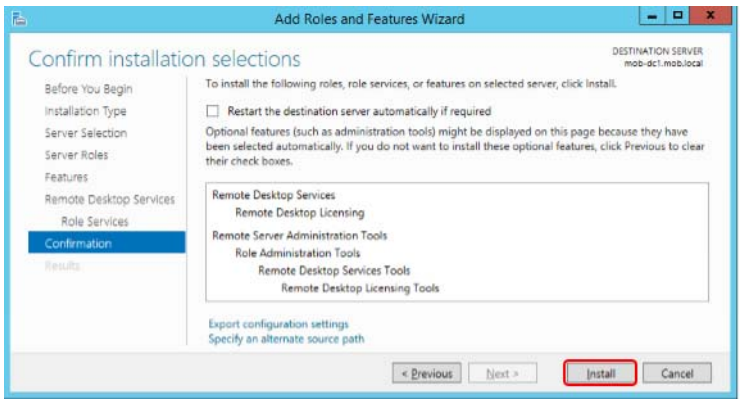

Figure 13. Confirmation to start adding additional roles and features

11. After the successful installation, click **Close** and restart the domain controller.

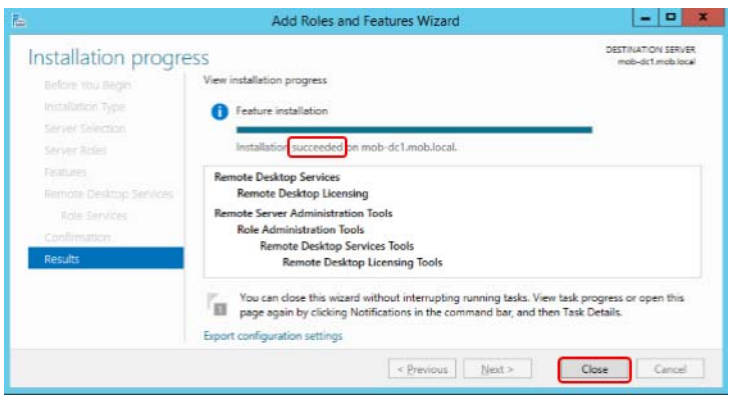

Figure 14. Completion of addition of new roles and features

Activating the Licensing Server and Adding Licenses

Perform the following tasks to configure the Terminal Server Licensing.

1. Activate the licensing server.
2. Add the purchased licenses.

The Remote Desktop Licensing Manager can be accessed through **Control Panel > Administrative Tools > Remote Desktop Services**.

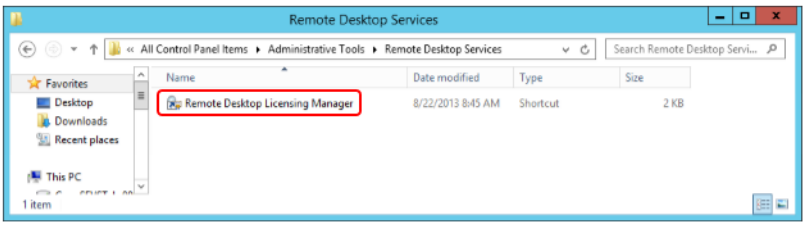

Figure 15. Accessing the Remote Desktop Licensing Manager

Activating the License Server

Execute the following steps to activate the license server:

1. Initially, the Remote Desktop Session Host Server Licensing has the status *Not activated*. Right-click the server and select **Activate Server**.

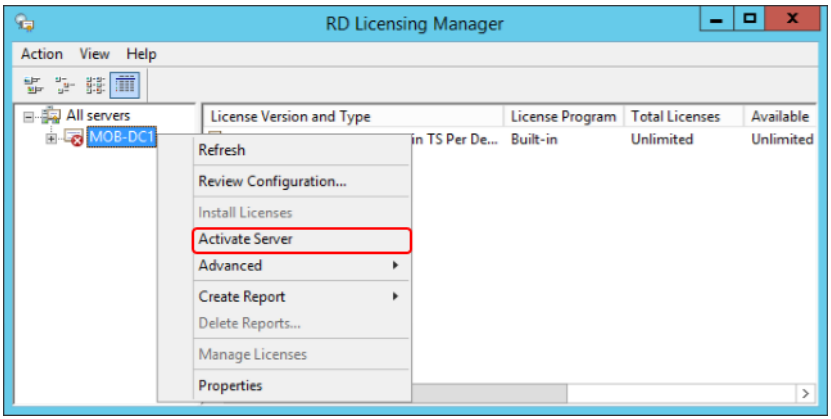

Figure 16. Activating the RD license server

2. **Welcome to the Activate Server Wizard** window appears. Click **Next**.

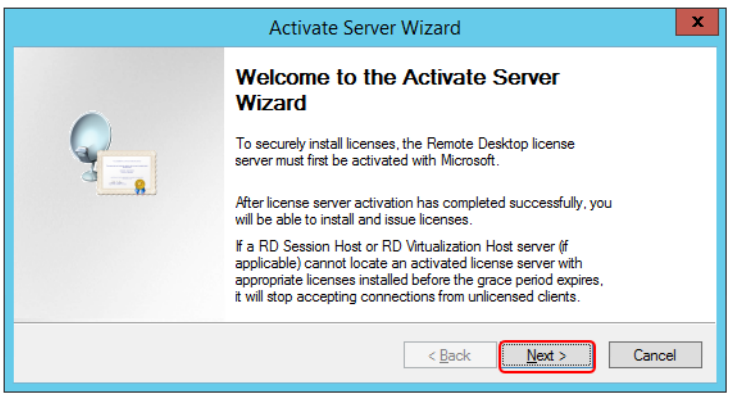

Figure 17. Welcome message to activate the RD licensing server

3. The following example uses **Automatic connection** since internet connection was available. Where this is not practicable, there is an option for activation over the telephone. Click **Next**.

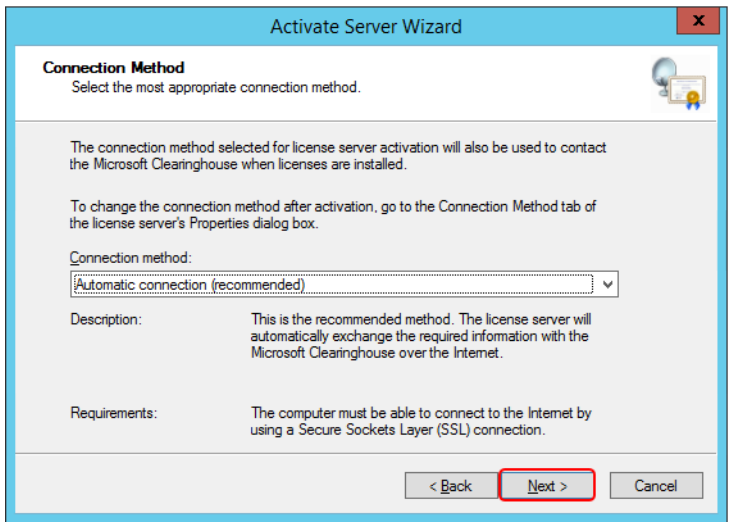

Figure 18. Selecting Automatic connection (usually via internet) to activate the server

4. Enter name, company, and country details for the administrator of the system and click **Next**.

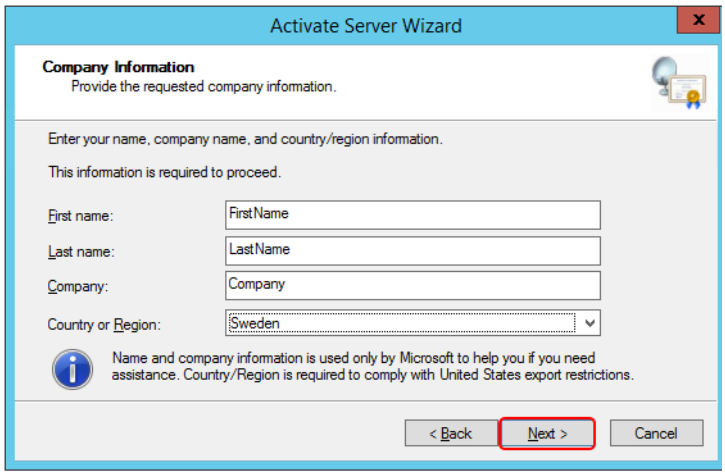

Figure 19. Providing identification details for the activation of the RD licensing server

5. Enter optional information, if required, and click **Next**.

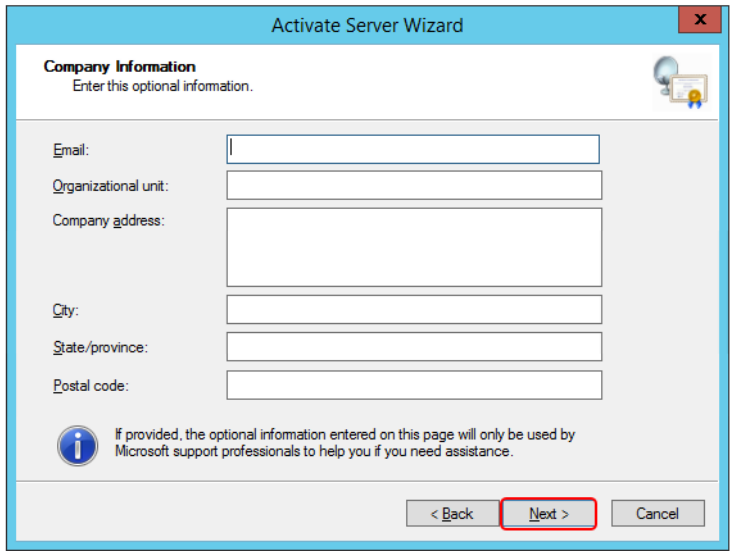

Figure 20. Providing optional information for the activation of the RD licensing server

6. In the **Completing the Activate Server Wizard** window, remove the selection of **Start Install Licenses Wizard now**, and click **Finish**.

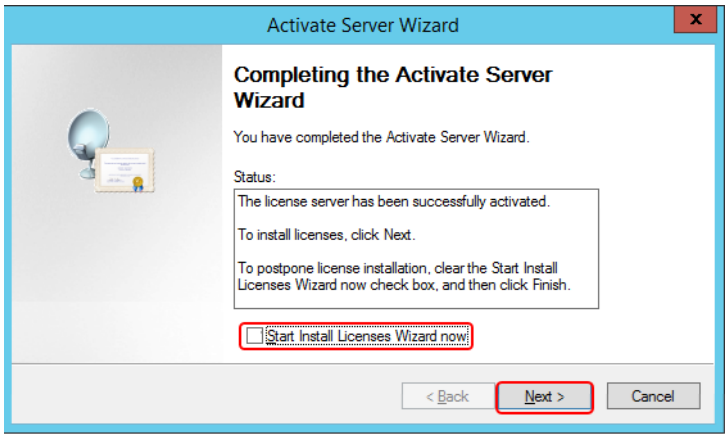

Figure 21. Completion of the activation of the RD licensing server

Reviewing Configuration

Execute the following steps:

1. After activating the licensing service, right-click the server and select **Review Configuration** to review the configuration.

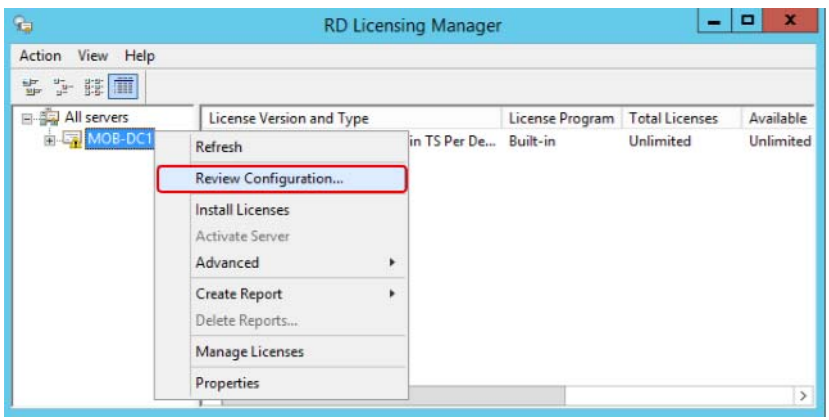

Figure 22. Reviewing the RD licensing server Configuration

If there is any issue with membership of the license server, click **Add to Group**.

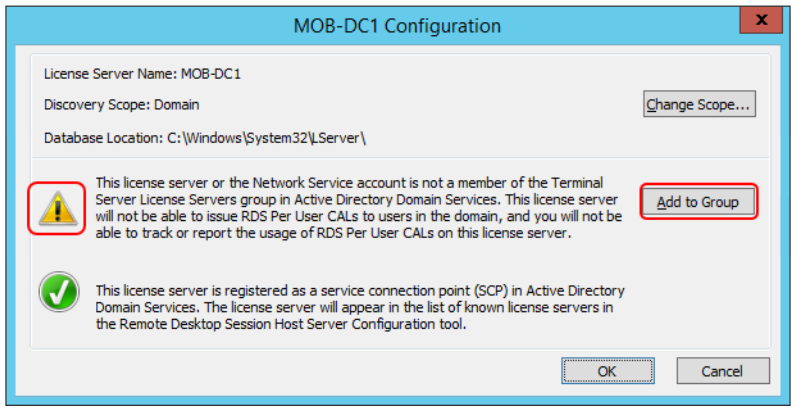

Figure 23. Reviewing issues with the RD license server

2. At the request to add the computer account for the license server, click **Continue**.

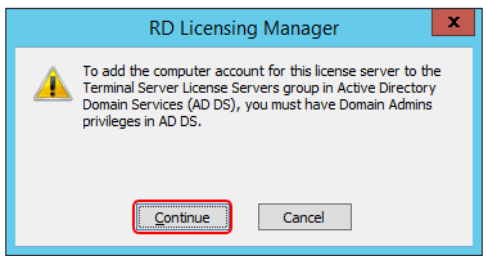

Figure 24. Adding the computer account to the Terminal Server License Server group

3. Click **OK** in the Confirmation window.

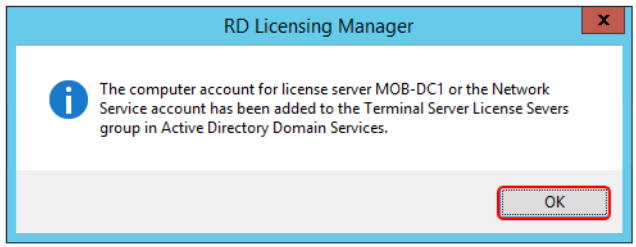

Figure 25. Confirmation that the computer account is added to the Terminal Server License Server group

4. Restart the RD Licensing Service to update the RD License Service status.

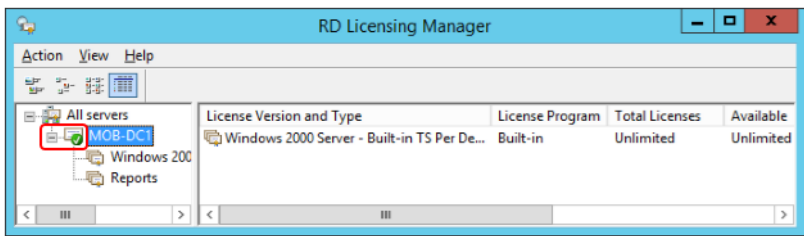

Figure 26. Confirmation that the RD License Server is now healthy

Adding RDS Server License

Execute the following steps to add the Remote Desktop Session Host Server license:

1. In the **RD Licensing Manager**, right-click the licensing server, and select **Install Licenses** from the context menu.

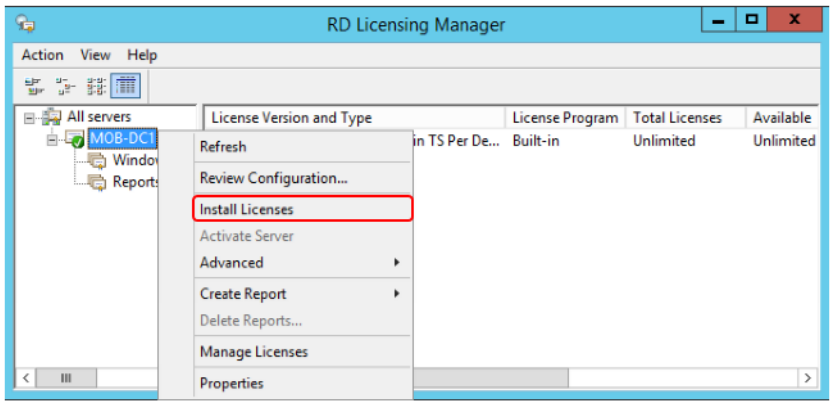

Figure 27. Installing licenses into the RD licensing server

2. **Welcome to the Install Licenses Wizard** window appears. Click **Next**.

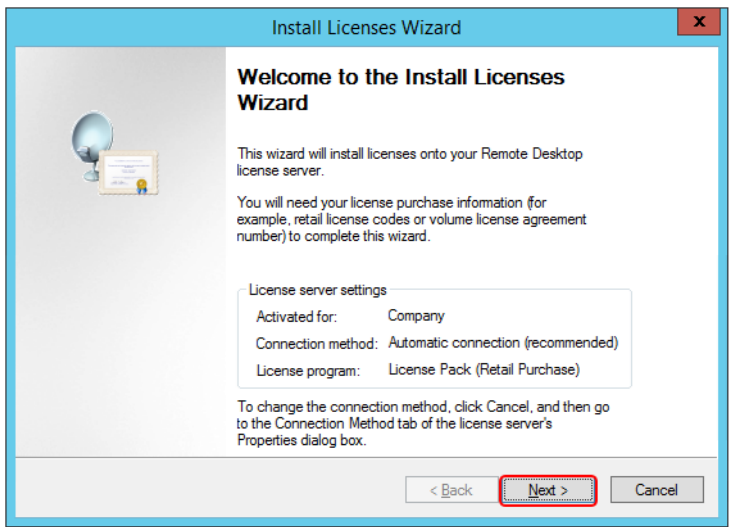

Figure 28. Welcome message for the installation of RD licenses

3. Select the appropriate license program and click **Next**.

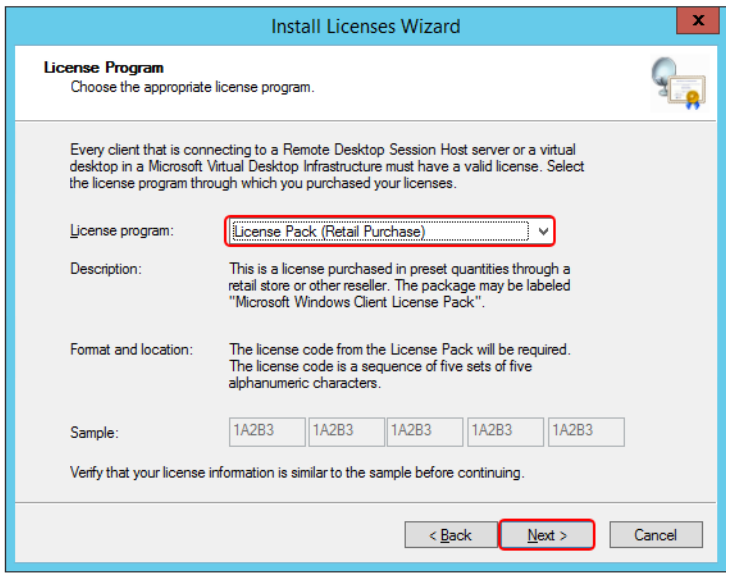

Figure 29. Selecting the licensing program for the RD licenses

4. Add the purchased licenses and click **Next** to install the licenses.

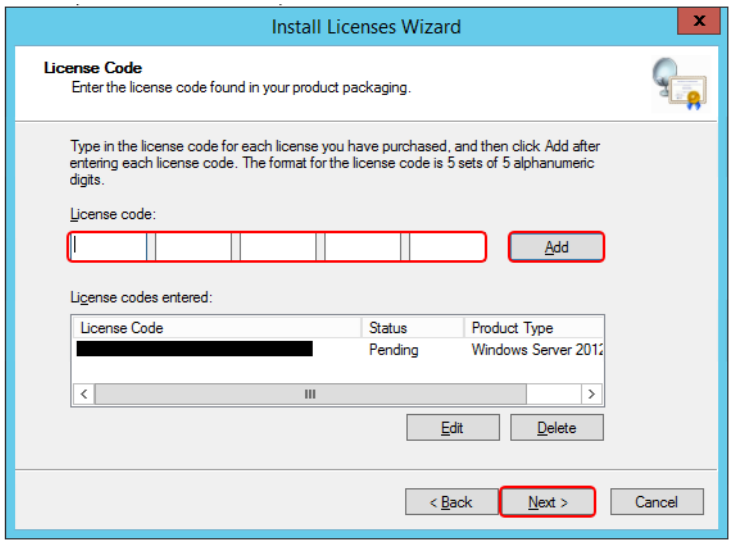

Figure 30. Entering the purchased RD license keys

5. **Competing the Install Licenses Wizard** window appears. Click **Finish**.

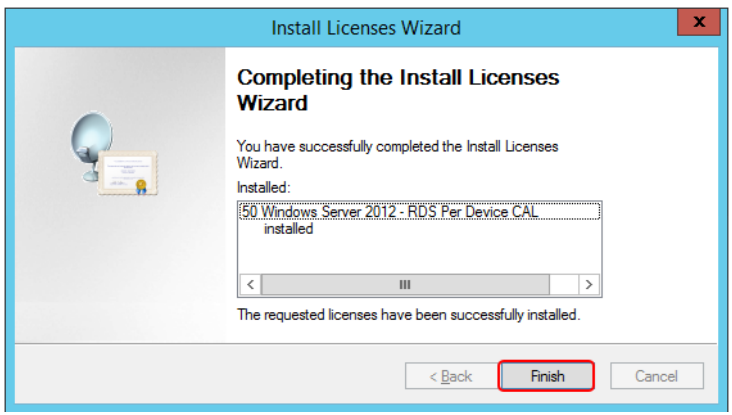

Figure 31. Successful installation of purchased RD licenses

The additional licenses should now be present in the RD Licensing Manager.

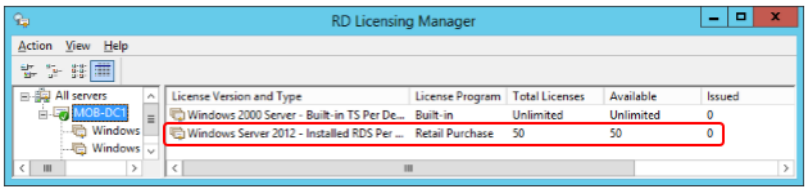

Figure 32. Additional licenses in the RD Licensing Manager

RDS Host Server Role

The Remote Desktop Session role supports remote desktop sessions. Initially, it is installed in the first Remote Desktop Session Host. Additional Remote Desktop Session servers are then added to make a collection of Remote Desktop Session Hosts.

Adding the Remote Desktop Session Host Server Role

Execute the following steps to add the Remote Desktop Session Host Server Role:

1. Logon to the server that will be the Remote Desktop Session Host Server. Start the **Server Manager** and select **Roles - Add Roles and features**.

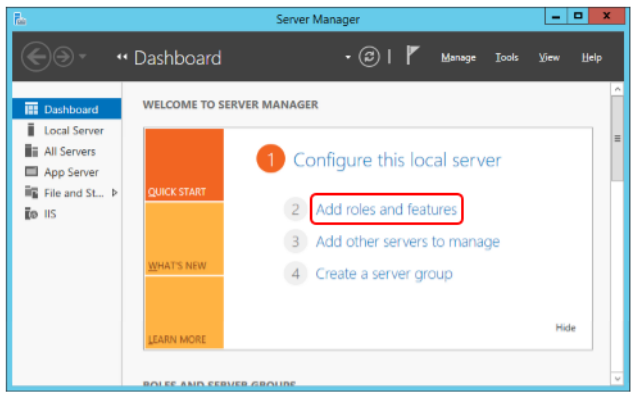

Figure 33. Accessing the addition of roles to the server

2. **Before You Begin** window appears. Click **Next**.

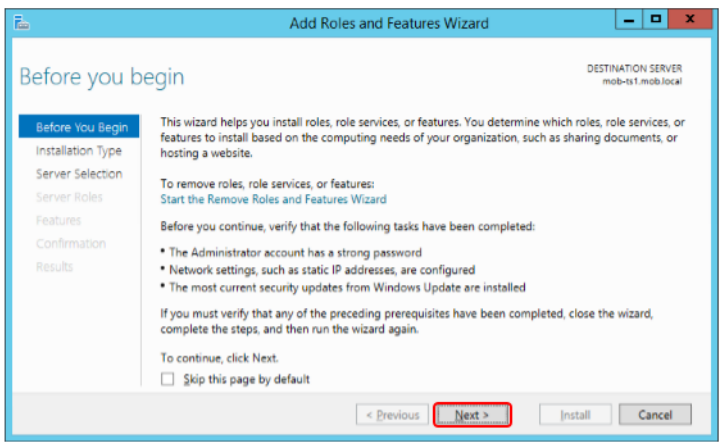

Figure 34. Before you begin adding roles information message

3. At the **Select Installation Type**, select **Remote Desktop Services Installation** and click **Next**.

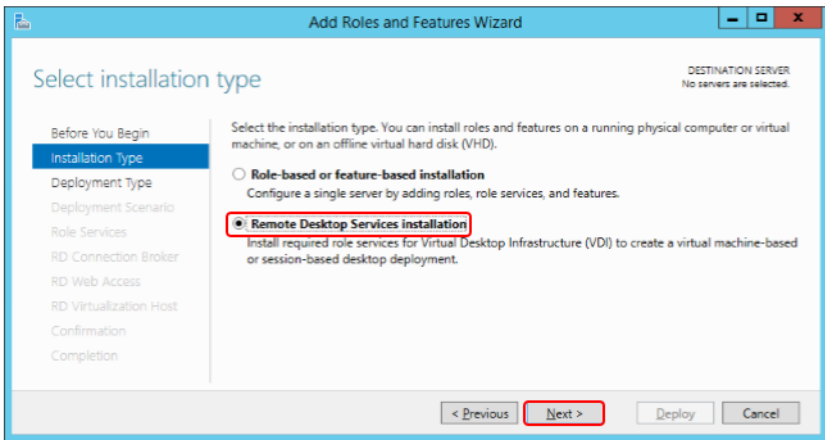

Figure 35. Selecting the Installation Type

4. At the **Select Deployment Type**, select **Standard Deployment** and click **Next**.

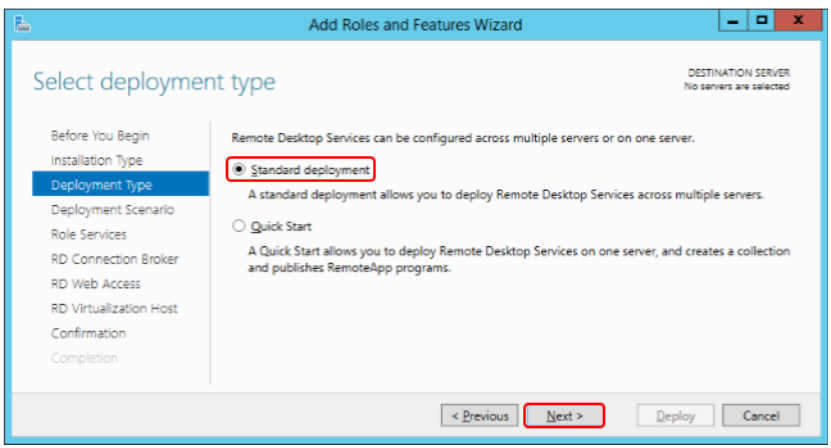

Figure 36. Selecting the Deployment Type

5. At the **Select Deployment Scenario**, select **Session-based desktop deployment** and click **Next**.

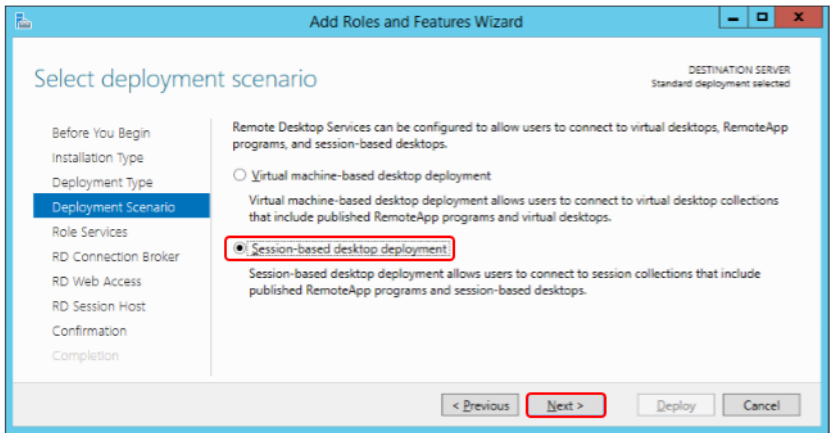

Figure 37. Selecting the Deployment Scenario

6. Review the changes to be done and click **Next**.

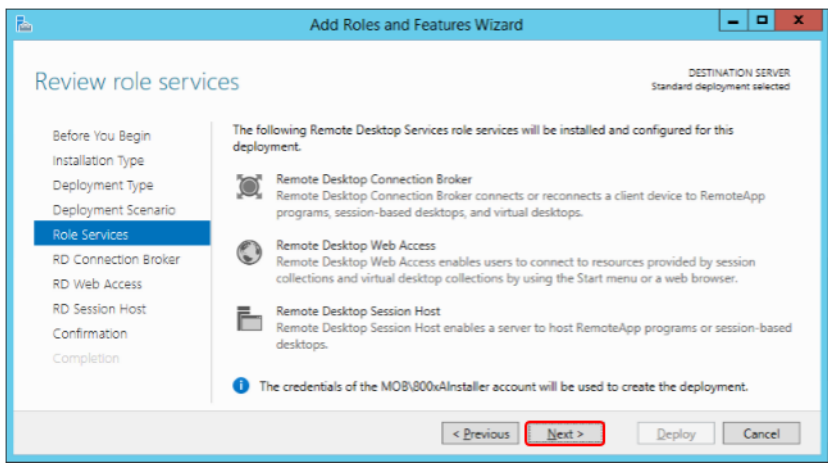

Figure 38. Reviewing the changes to be done

7. At least one node must be the RD Connection Broker server. In this example, the first Remote Desktop Session host will be configured to be the RD

Connection Broker server. Add the server to be **RD Connection Broker** server and click **Next**.

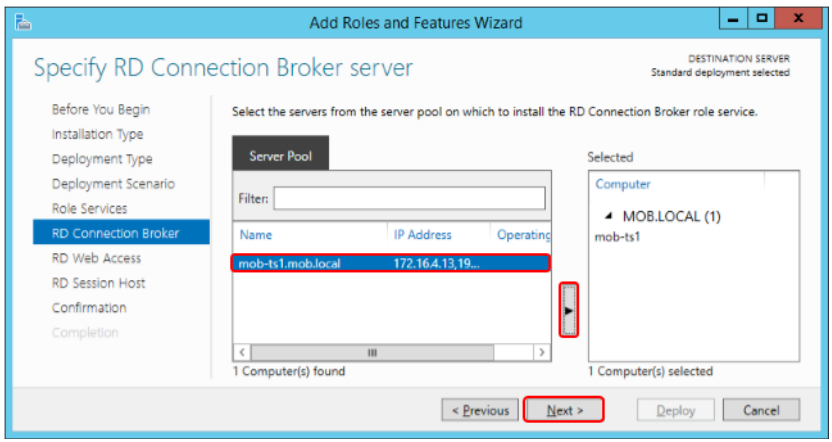

Figure 39. Specifying the RD Connection Broker Server

8. At least one node needs to be the RD Web Access server. In this example, the first Remote Desktop Session host will be configured to be the RD Web Access server. Add the server to be **RD Web Access server** and click **Next**.

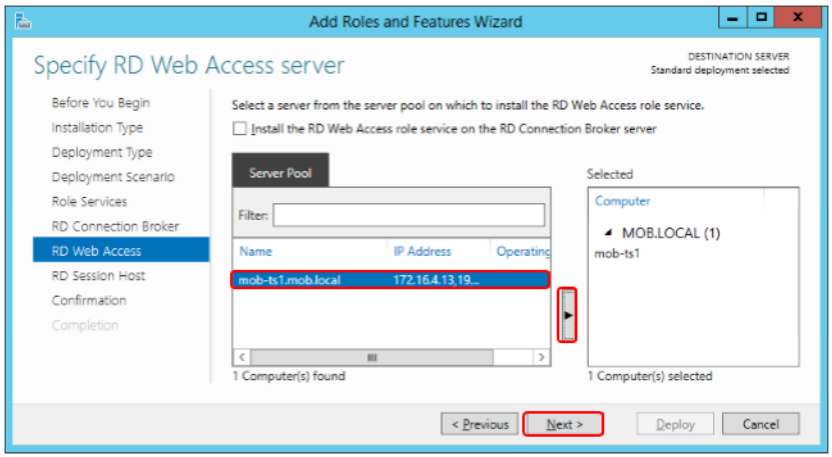

Figure 40. Specifying the RD Web Access Server

9. Add the server to be RD Session Host server and click **Next**.

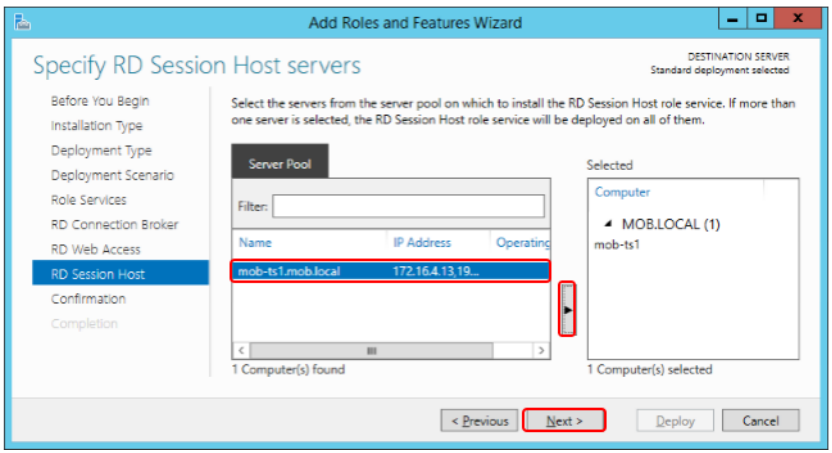

Figure 41. Specifying the RD Session Host Server

10. Select the **Restart the destination server automatically if required** check box and click **Deploy**.

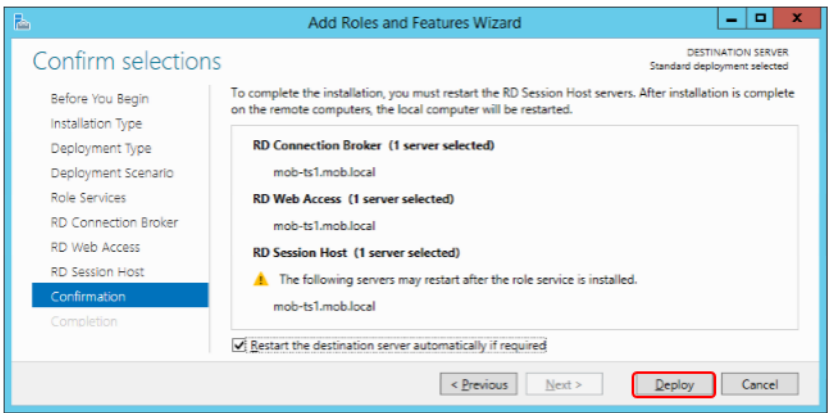

Figure 42. Deploying the Configuration

11. After restarting the computer, start the Server Manager to view the progress. Click **Close**.

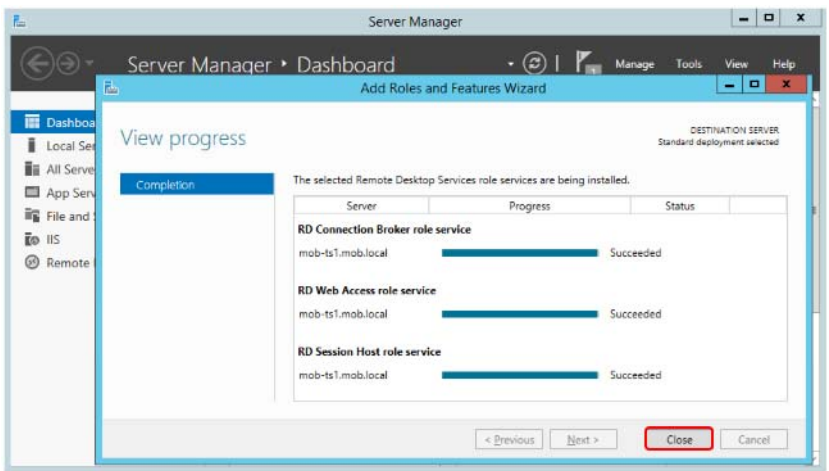

Figure 43. Checking the Deployment Completion

Adding Additional Remote Desktop Session Hosts

Additional Remote Desktop Session Hosts can be added from the first Remote Desktop Session Host. This is done in two stages:

1. The additional Remote Desktop Server is added to the servers to manage,
2. The additional Remote Desktop Server is added as an additional Remote Desktop Session Host.

Execute the following steps:

1. Add the additional server to be the additional Remote Desktop Session Host by starting the Server Manager, and selecting Add other servers to manage.

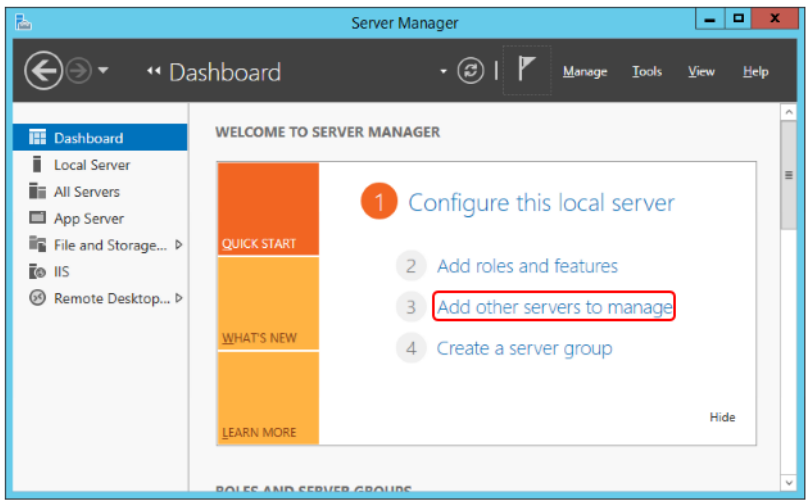

Figure 44. Adding additional servers to manage

2. Add the computers that are to become additional Remote Desktop Session Hosts, and click **OK**.

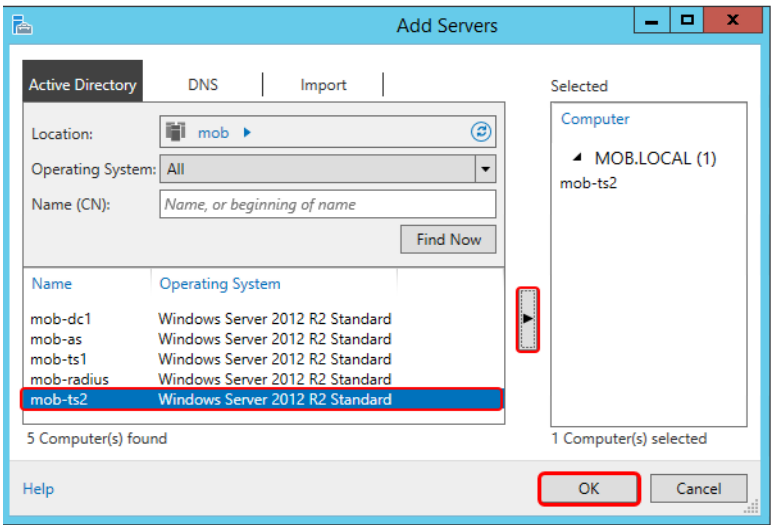

Figure 45. Adding additional servers to manage

3. Add the other server to the RD Session Host.

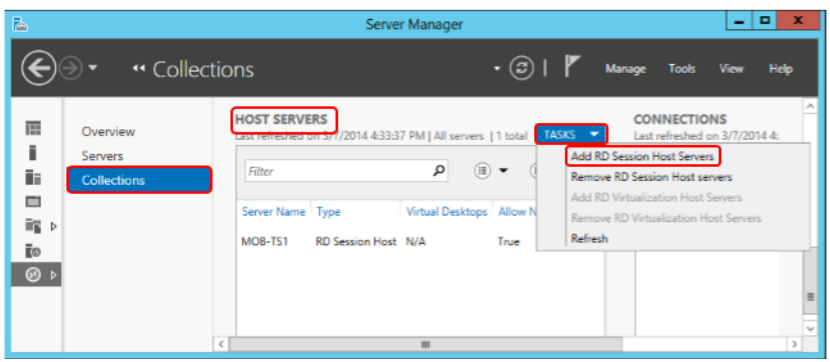

Figure 46. Adding additional RD Session Host Servers

4. Select the additional servers that are to become Remote Desktop Session Host Servers, and click **Next**.

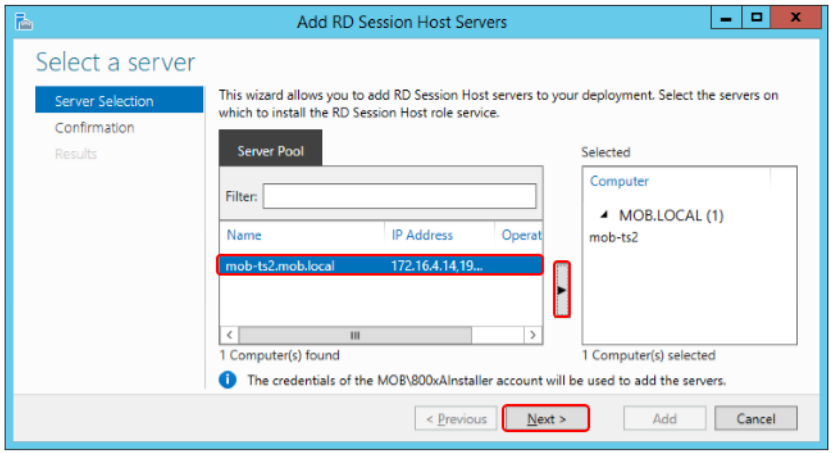

Figure 47. Selecting servers to become additional RD Session Host Servers

5. Click **Add** to confirm the addition of the server.

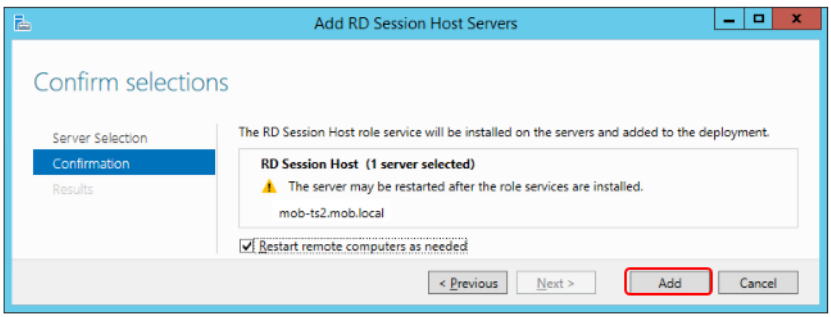

Figure 48. Confirmation to add additional server

6. When the operation is succeeded, click **Close**.

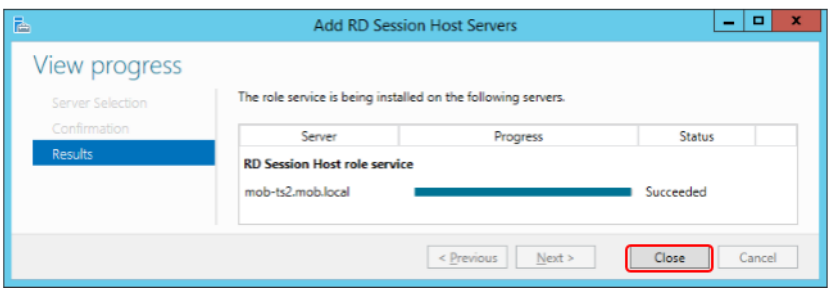

Figure 49. Addition of the Server is successfully completed

Setting up the License Server

The RD License Server must be defined in the configuration to access licenses for remote desktop sessions.

Execute the following steps to setup the license server:

1. In the **Server Manager - Remote Desktop Services**, edit the deployment properties.

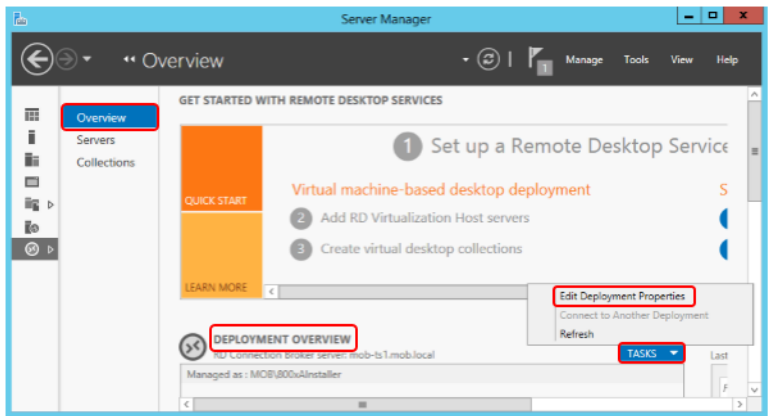

Figure 50. Editing the Remote Desktop Services Deployment Properties

2. Select RD Licensing and specify the licensing according to the type of RD License CALs purchased. Type in the computer name of the RD license server, click **Add** and then click **Apply** and **OK**.

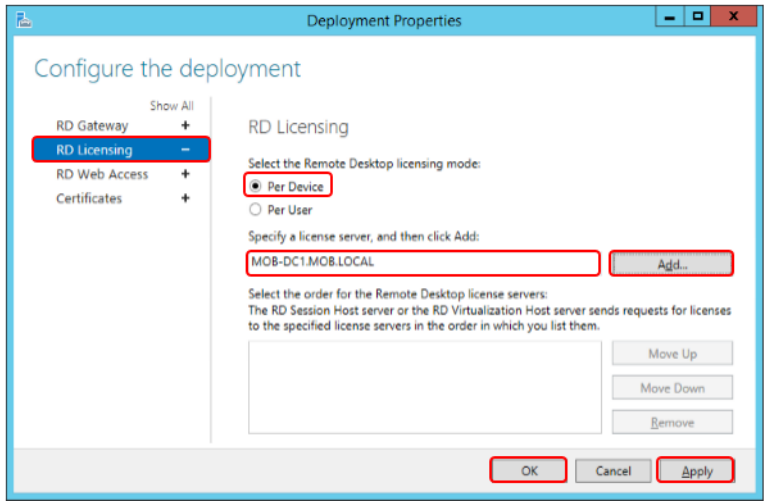

Figure 51. Specifying the RD Licensing for the Remote Desktop Server

Creating a Remote Desktop User Group

While there are Remote Desktop Users in the active directory configuration it may be preferred not to use this as it will grant remote logon to other servers.

In the domain controller, use the Active Directory Users and Computers interface to create a new security group for the purpose of assigning remote operator privileges.

In the domain controller, create a new group for remote access.

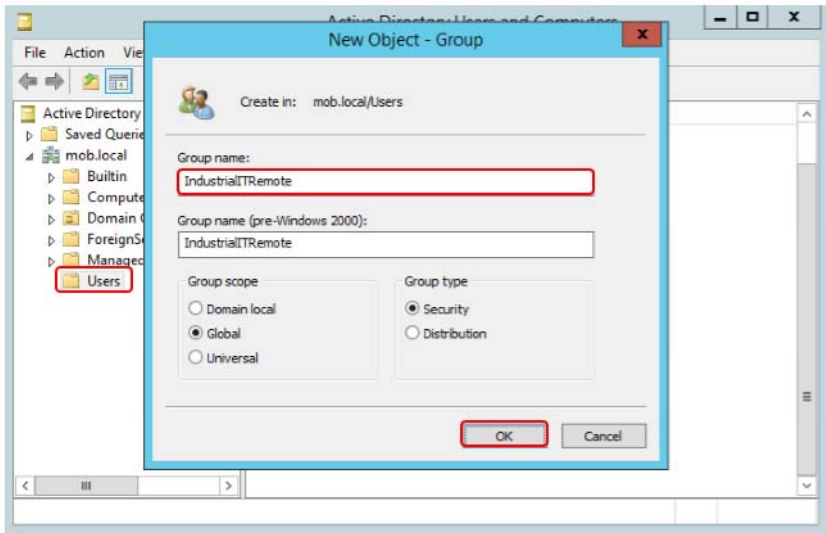

Figure 52. Creating a user group for remote desktop access

Creating a Remote User

Execute the following steps to set up the first remote user:

1. In the domain controller, use the Active Directory Users and Computers interface to create a new user.

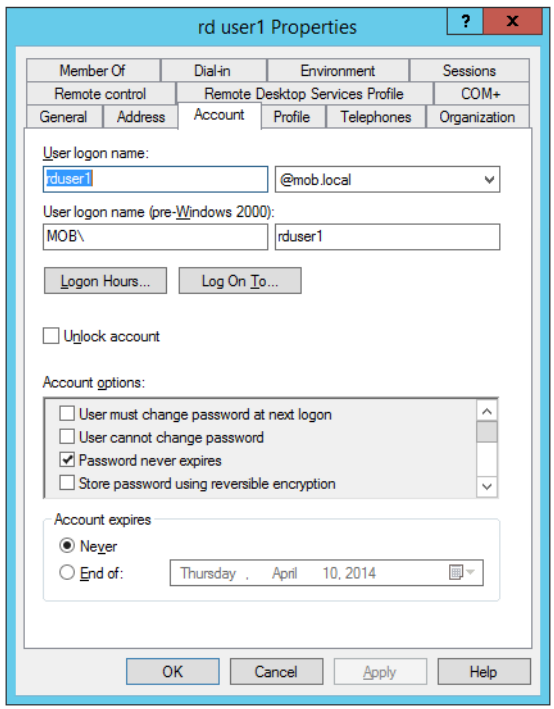

Figure 53. New User for Remote Desktop access

2. To provide security access for remote desktop login, make the user a member of the remote desktop security group. The user is also added to the IndustrialITUser group for access to 800xA and to the Users group to allow local login.

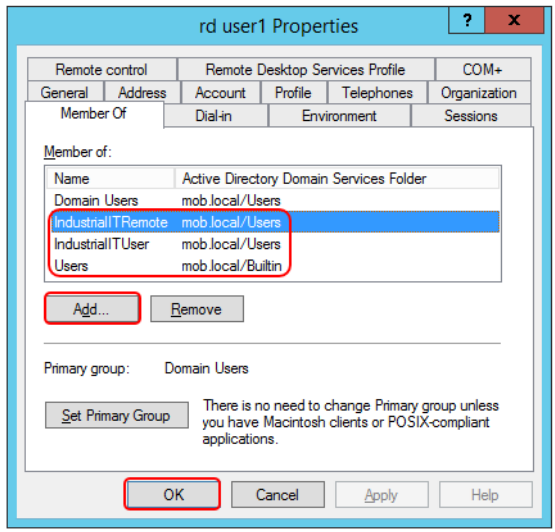

Figure 54. Remote Desktop Security Group Membership

Creating a New Collection

A collection is one or more Remote Desktop Session Hosts and provides control over the remote desktop sessions such as user group access control and load balancing.

To create a new collection:

1. Select the **Collections** in the Server Manager and select **Create Session Collection** from the **Tasks**.

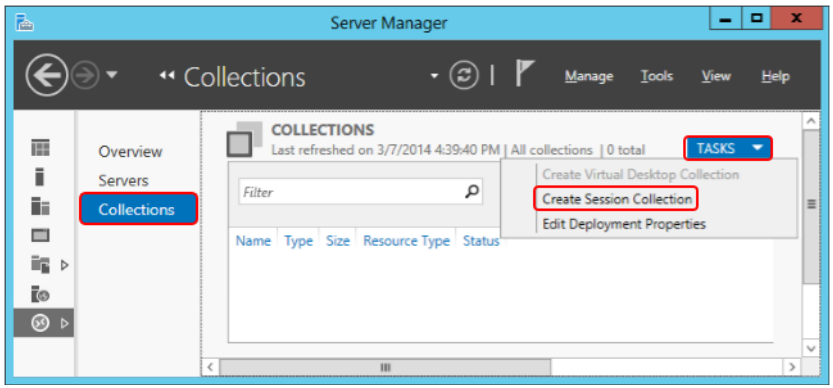

Figure 55. Creating a new Remote Desktop Session Collection

2. At the **Before you begin** window, click **Next**.

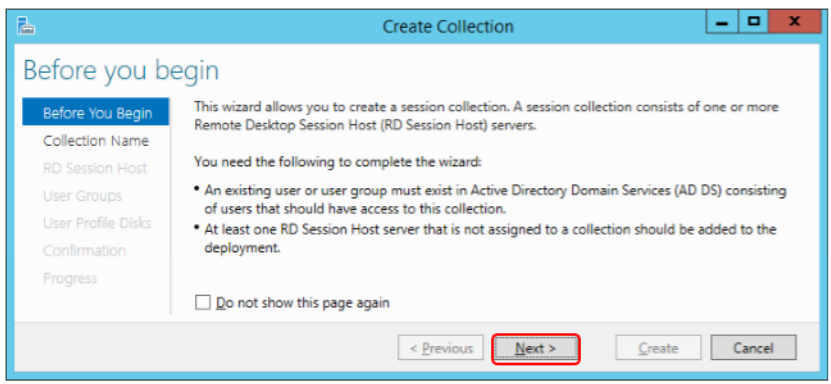

Figure 56. Creating a Collection Information

3. Provide a name and description for the new collection and click **Next**.

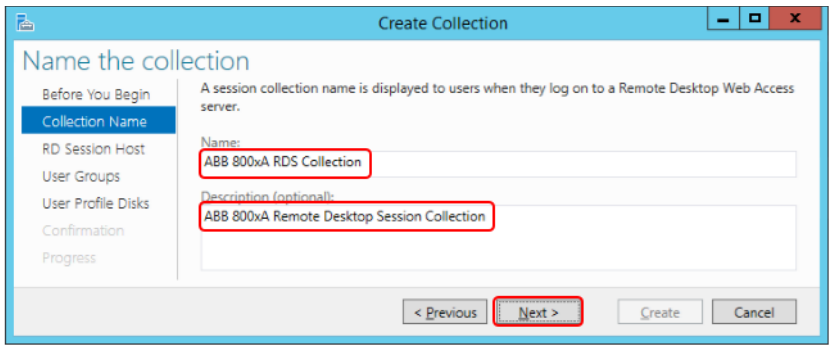

Figure 57. Providing a name and description for the Collection

4. Add the Remote Desktop Session Hosts to the new collection and click **Next**.

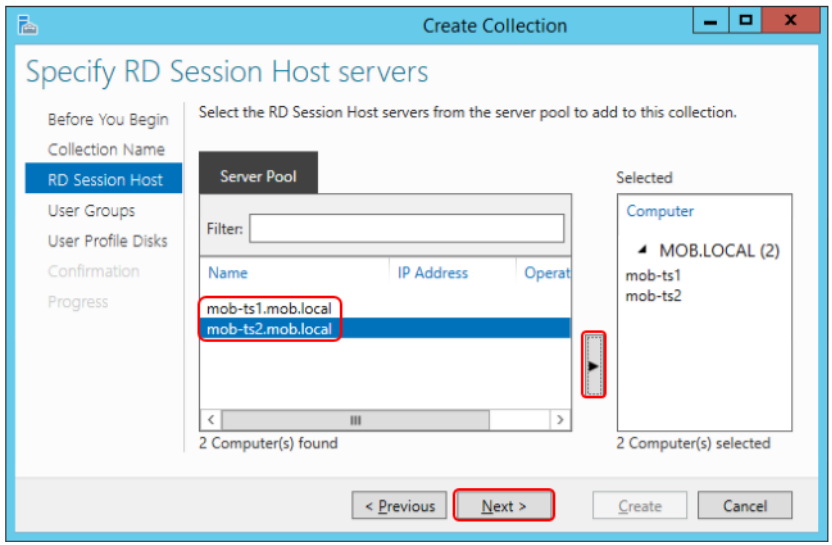

Figure 58. Adding Remote Desktop Session host servers to the new collection

5. Specify the user groups which are allowed to connect to the collection. In the Default Wizard configuration, Domain Users is added. To have a tighter limit on user access, use the group created specifically for remote access. In this example, the IndustrialITRemote user group.

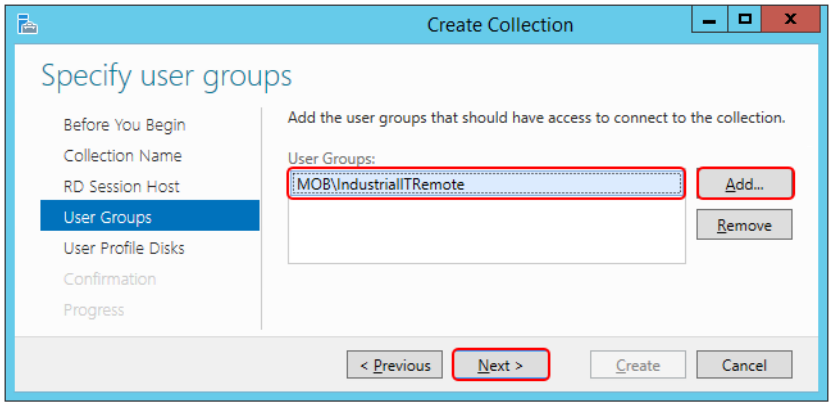

Figure 59. Specifying the user groups to have access to the remote desktop session collection

6. Remove the selection of **Enable user profile disks** check box and click **Next**.

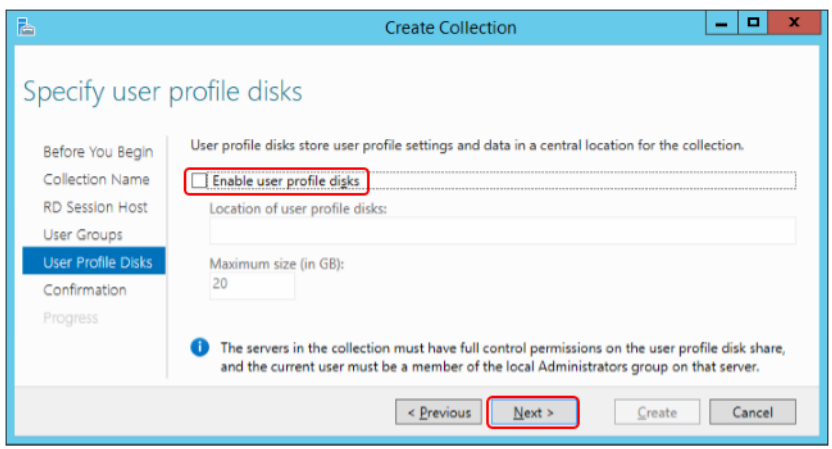

Figure 60. Specifying the user profile disks option

7. At the **Confirm Selections** window, review the configuration and click **Create**.

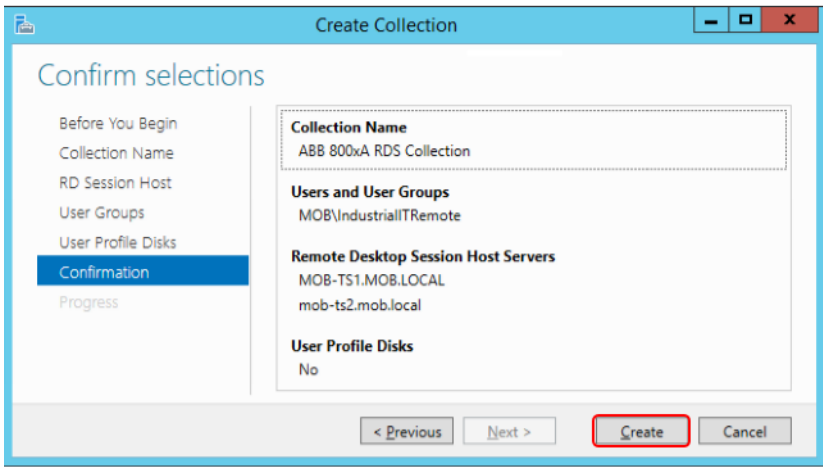

Figure 61. Confirmation of changes to be done

8. Click **Close** after the changes are successfully completed.

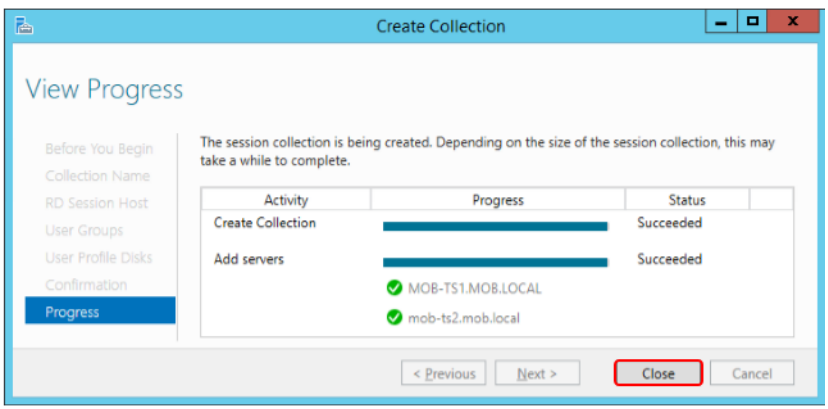

Figure 62. Completed creation of new collection

Limiting loading of Remote Desktop Session - Load balancing

Load balancing is a function of the Remote Desktop Session Collection that enables the control of the maximum number of sessions that can be running on a Remote Desktop Session Host.

To access the Remote Desktop Session load balancing:

1. Select the collection and select **Edit Properties** from **Tasks**.

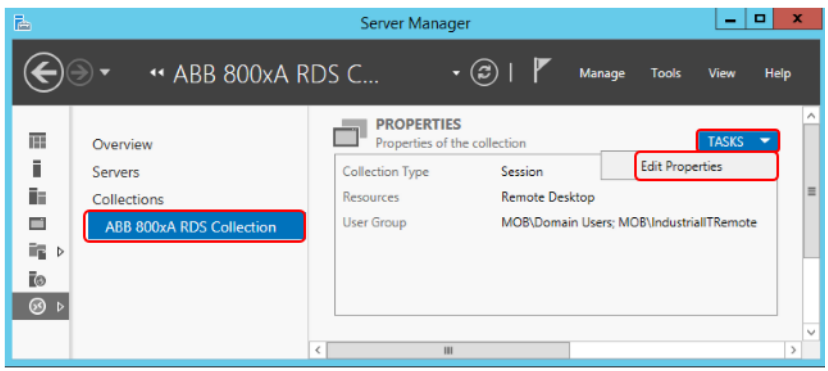

Figure 63. Editing the collection properties to access the load balancing settings

2. Select the Load Balancing option and specify the Session Limit. In the example below, each Remote Desktop Session Host has been limited to 2 sessions. If a user is logged into the server (that is, not in a remote session), this is still counted as a session. This value should be set to the corresponding maximum users for each RD Session Host Server.

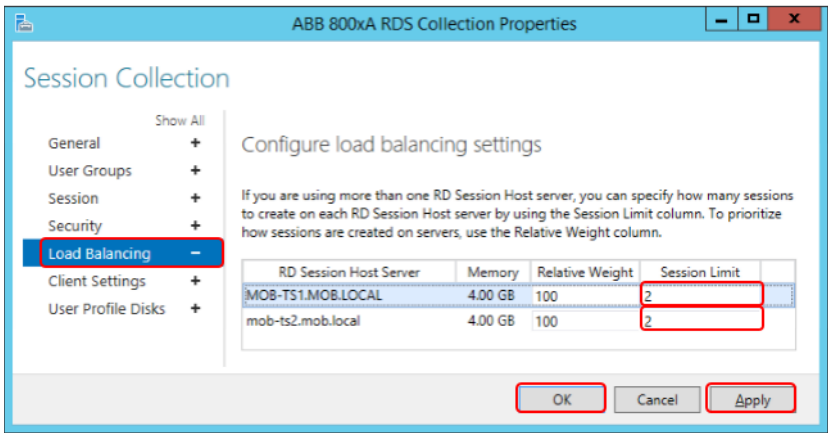

Figure 64. Configuring load balancing for the Remote Desktop Session Collection

Any of the Remote Desktop Session Host server IP addresses can be used to make a connection. If the designated server session limit is reached, another available server in the collection will be used. If there are no more sessions available, an error message will be presented.

Testing Load Balancing

It is essential to confirm that the load balancing is working as intended. This is done by setting an initial low maximum user count on the Remote Desktop Session Servers and attempting to connect more users than the maximum. This can be done by making multiple remote desktop sessions from a client to the Remote Desktop Session servers using different users for each session.

The user logged into the console is counted as one user. In the following example, the maximum user count is set to 2, there is a user logged into the console (800xAInstaller) and a remote desktop session has been started using the rduser1 user.

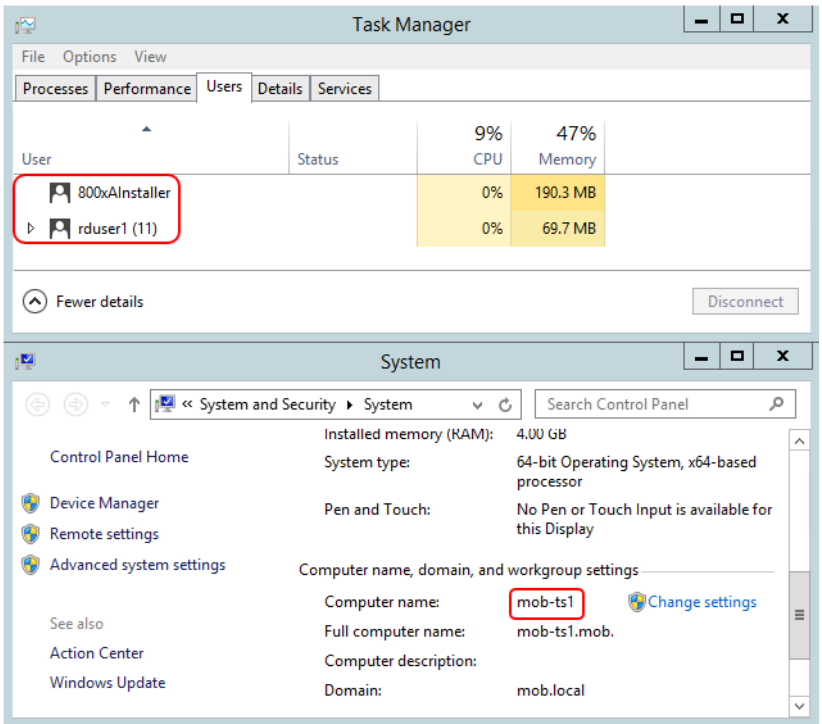

Figure 65. One remote desktop session user in addition to the locally logged in user in Remote Desktop Session Host Server 1

When an additional user is logged in (rduser2), this user is redirected to another remote desktop session host in the same collection. In the example below, mob-ts2.

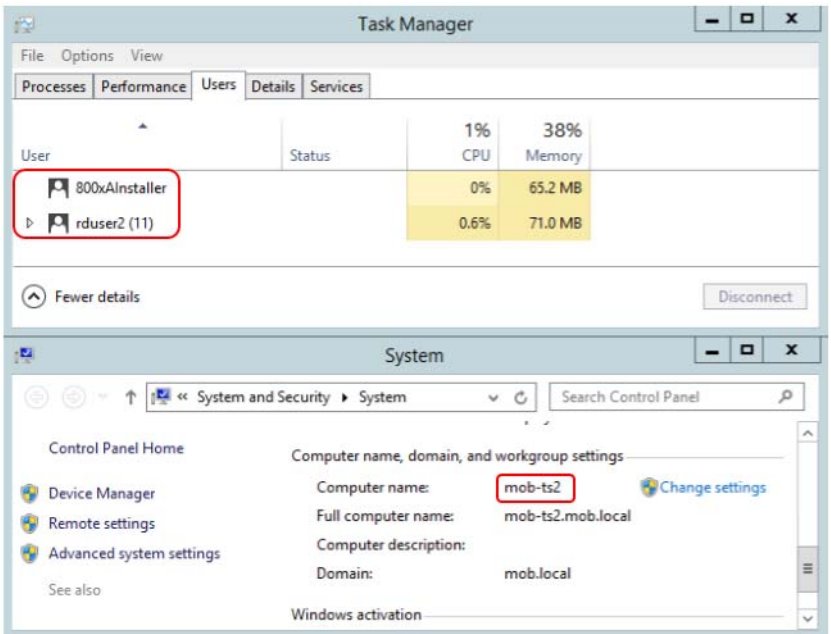

Figure 66. A second remote desktop session user is redirected to an available remote desktop session host server

If there are no available Remote Desktop Session Host Servers, that is, all the session limits are reached, an error box will be presented indicating that was a problem connecting to the remote computer:

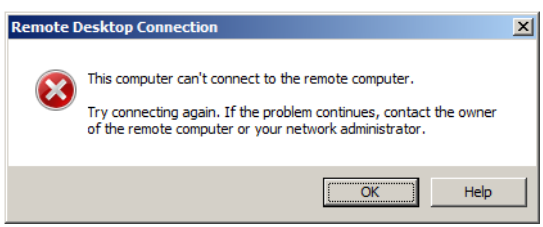

Figure 67. Attempting to establish a remote desktop session where session limits have been reached

Enabling Audio

The default installation of Windows Server 2012 R2 does not enable audio. Audio is required for Remote Desktop Sessions for audible alarms. The system tray in the Remote Desktop Session server shows the current state of the audio support. In Figure 68, audio has not been enabled yet:

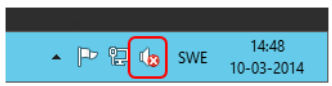

Figure 68. Audio not enabled in Window Server 2012R2

To enable audio, select **Services** from the Computer Manager. Right-click the Windows Audio service and select **Properties**.

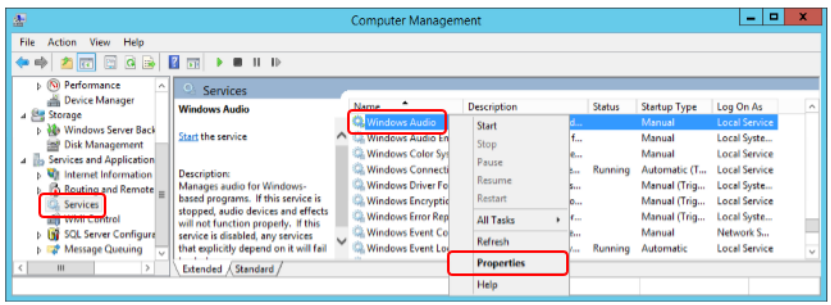

Figure 69. Accessing the Windows Audio service properties

Set the Startup type to **Automatic**, click **Start** and then click **OK**.

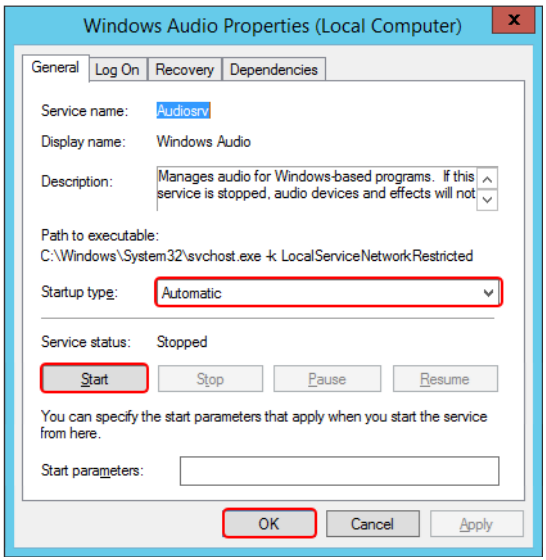

Figure 70. Setting the Windows Audio service to Automatic and starting the service

Now, the speaker in the system tray indicates that the audio is enabled.

Figure 71. Audio enabled in the Remote Desktop Session Host server

Section 5 Certificate Authority

The certificate authority is responsible for providing certificates which are used in the authentication of the wireless device to the wireless access point. As it is expected to have limited number of mobile devices used in conjunction with the 800xA system, it is preferable to have one certificate per device. This provides a more concise control over device access to the wireless networks.

Installing the Certificate Authority

Execute the following steps:

1. To add the certificate authority role, login to the radius server and start the **Server Manager.** Select **Add Roles and Features**. .

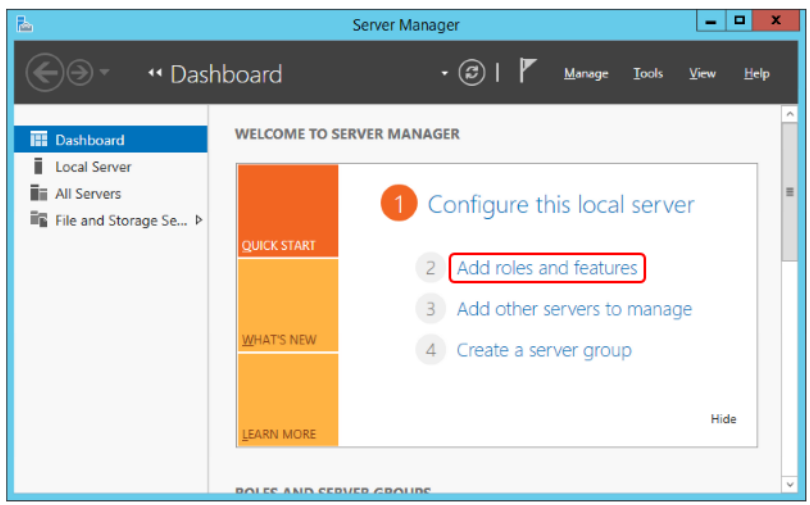

Figure 72. Selecting the Add Roles and features to add the certificate authority role

2. **Before You Begin** window appears. Click **Next**.

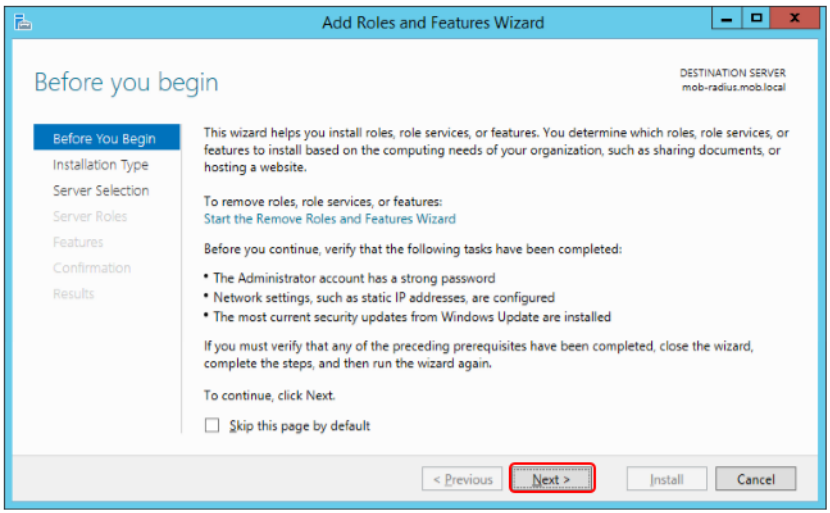

Figure 73. Before you begin information message

3. Select **Role-based** or **feature-based installation** and click **Next**.

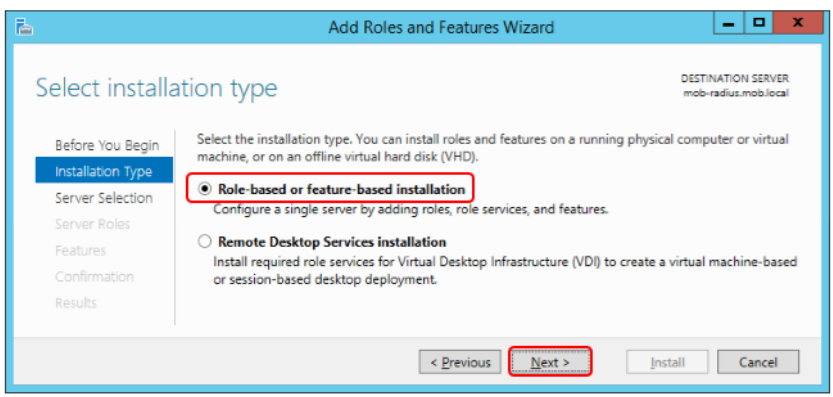

Figure 74. Selecting Installation Type

4. Select the radius server and click **Next**.

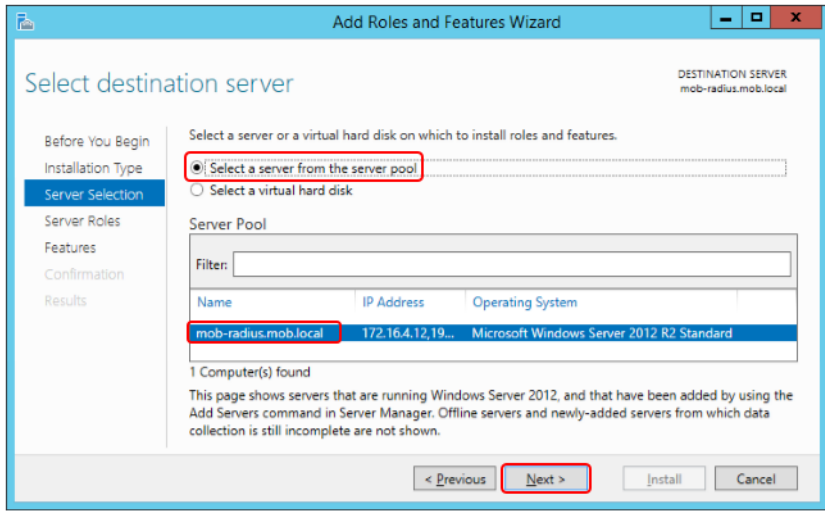

Figure 75. Selecting radius server for installation of the new role

5. At the **Select Server Roles** window, select the **Active Directory Certificate Services** role. This will call a prompt to add additional features. Select the **Include management tools** check box and click **Add Features**.

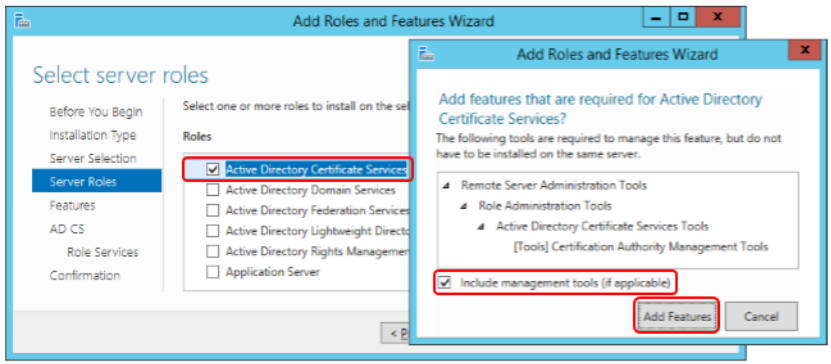

Figure 76. Selecting to add the Active Directory Certificate Services role and required features

6. In the **Select Features** window, click **Next**.

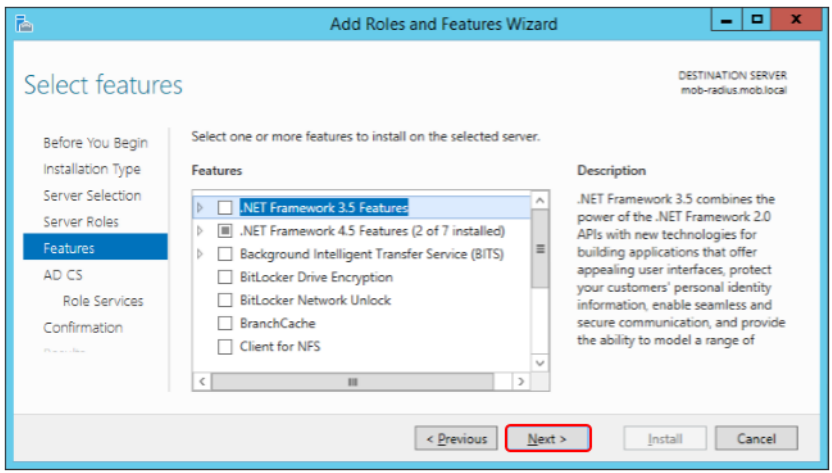

Figure 77. Selecting the features

7. Click **Next** at the information window.

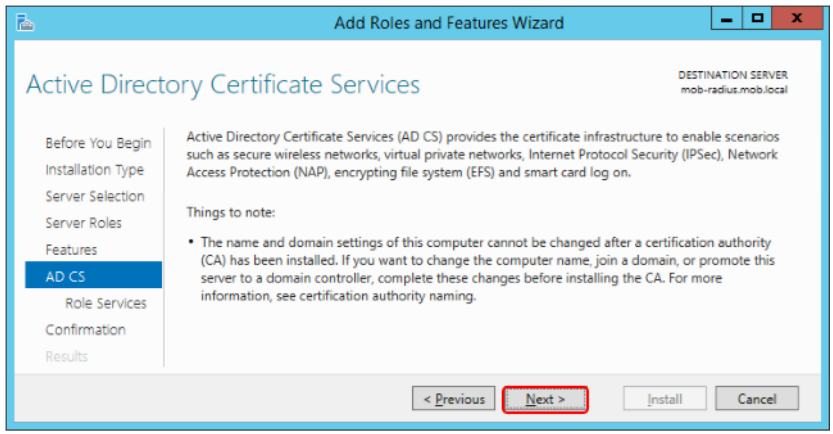

Figure 78. Information window on Active Directory Certificate Services

8. At the **Select role services** window, select the **Certification Authority** role and click **Next**.

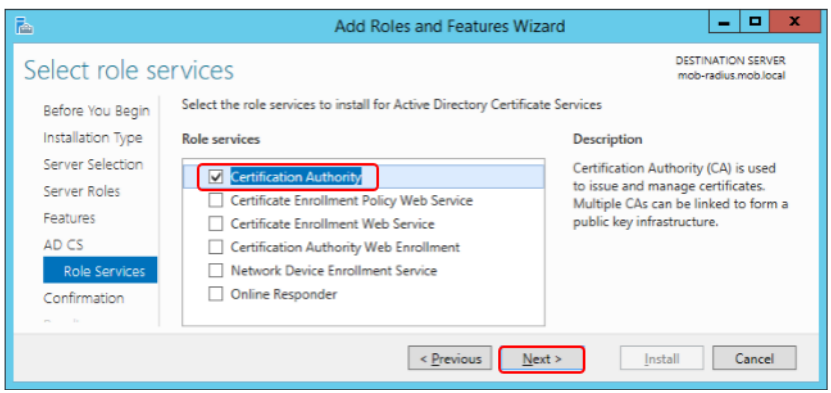

Figure 79. Adding Certification Authority Role

9. Review the configuration changes to be done and click **Install**.

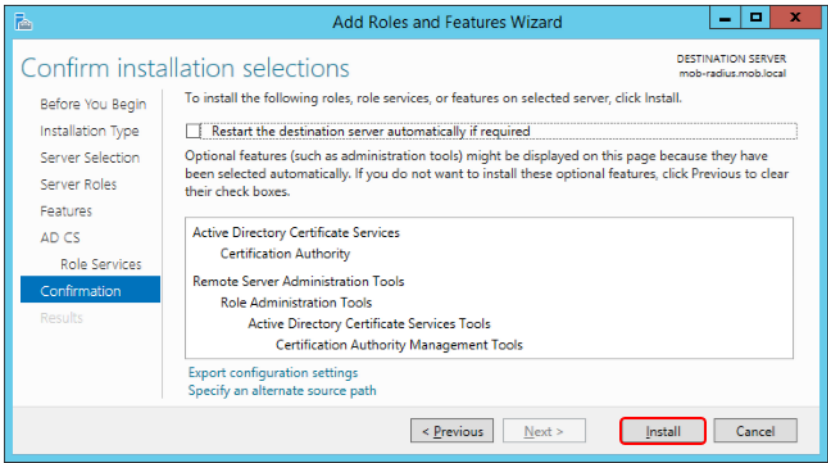

Figure 80. Reviewing configuration changes before installation

10. Click **Close** after completing the installation.

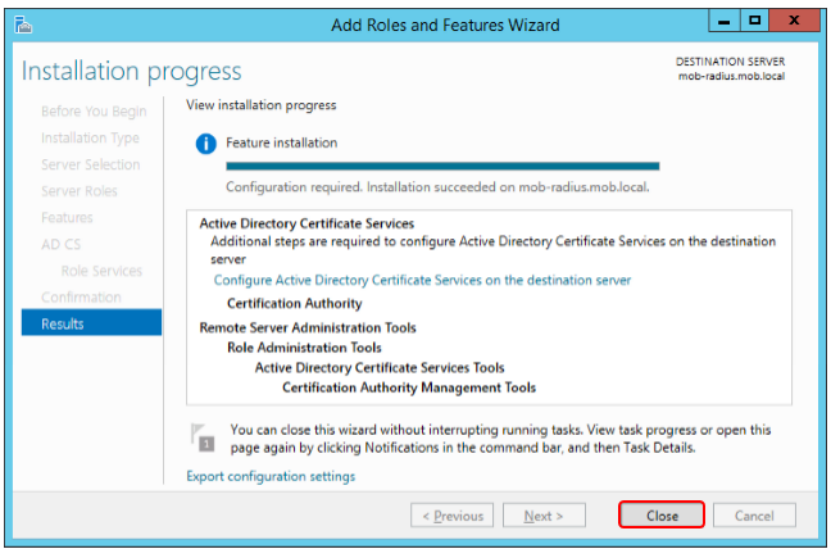

Figure 81. Successful completion of the role addition

Configuring the Certificate Authority

After installing the Certificate Authority, it must be configured to setup the base mode of operation. This requirement will be highlighted in the alert in the Server Manage.

Click the alert in the Server Manager, and select the Configure Active Directory Certificate Services on this node.

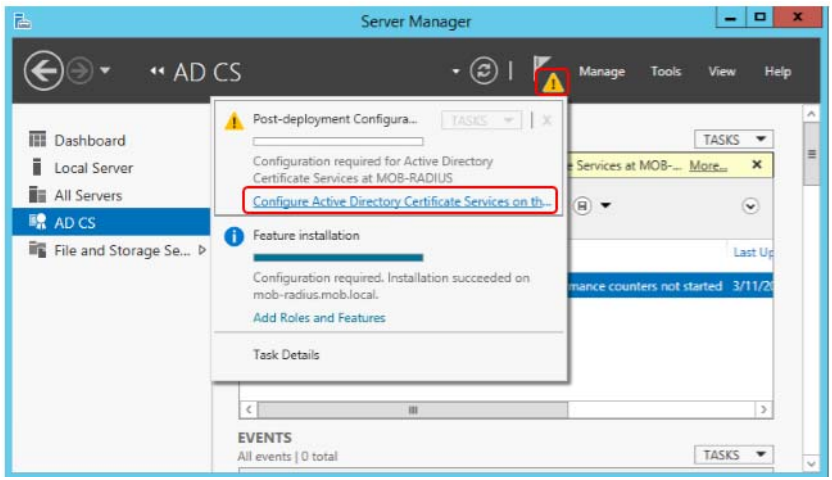

Figure 82. Initiating Certificate Authority post installation configuration

11. Provide the required administrative credentials to configure the node and click **Next**.

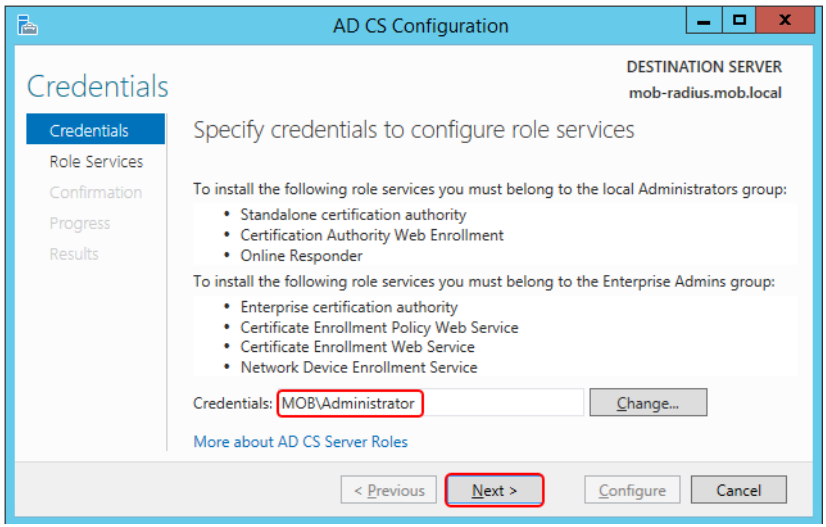

Figure 83. Supplying the required administrative credentials to configure the role

12. Select Certification Authority role to configure and click **Next**.

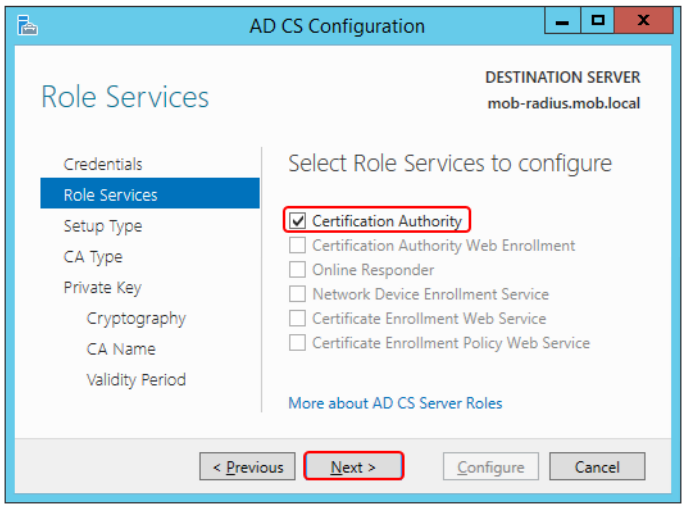

Figure 84. Selecting the Certification Authority to configure

13. At the **Setup Type** window, keep the setting as **Enterprise CA** and click **Next**.

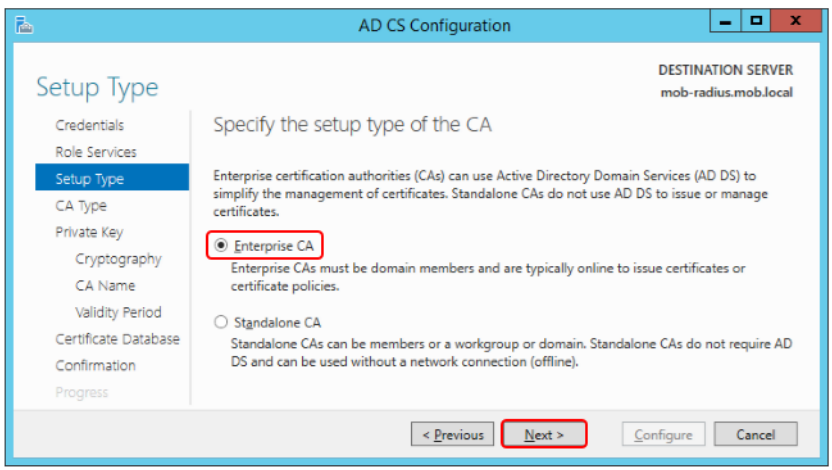

Figure 85. Selecting the CA setup type as Enterprise

14. **Specify CA Type** window appears. Leave the setting as **Root CA** and click **Next**.

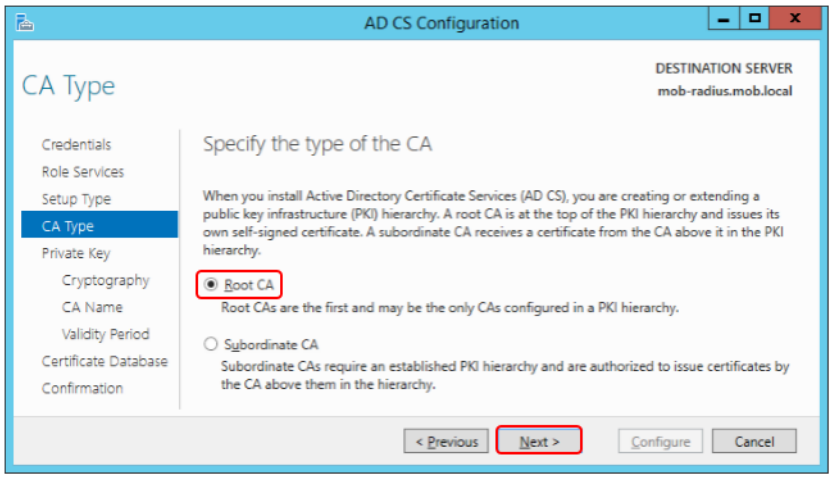

Figure 86. Specifying the Root CA option

15. Select **Create a new private key** when requested to set up a private key and click **Next**.

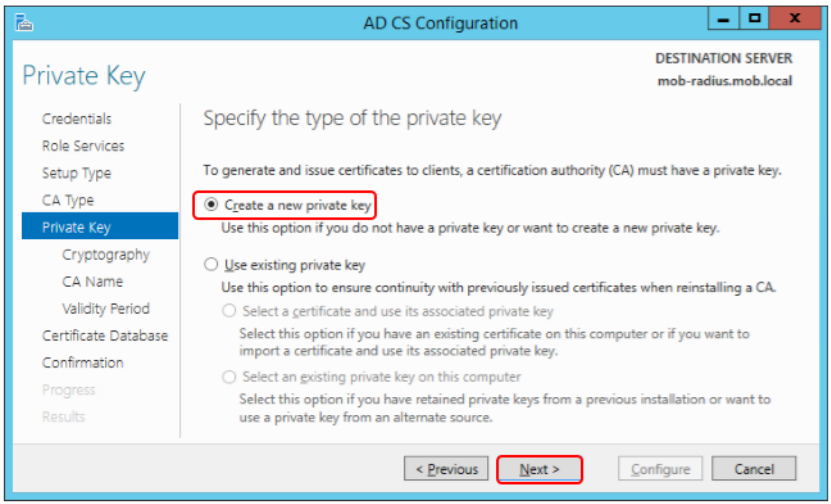

Figure 87. Specifying that a new private key should be produced

16. Leave the defaults when configuring the cryptography for CA, and click **Next**.

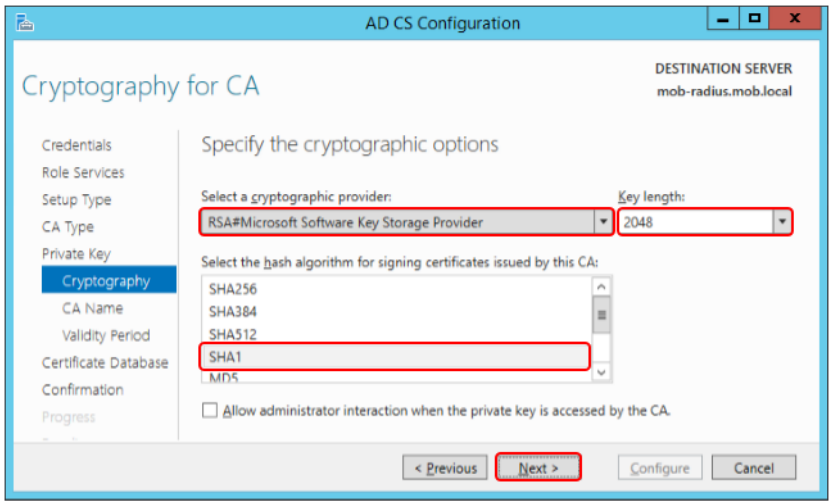

Figure 88. Using default cryptography configuration

17. Leave the default suggestion for the common name for the CA and click **Next**.

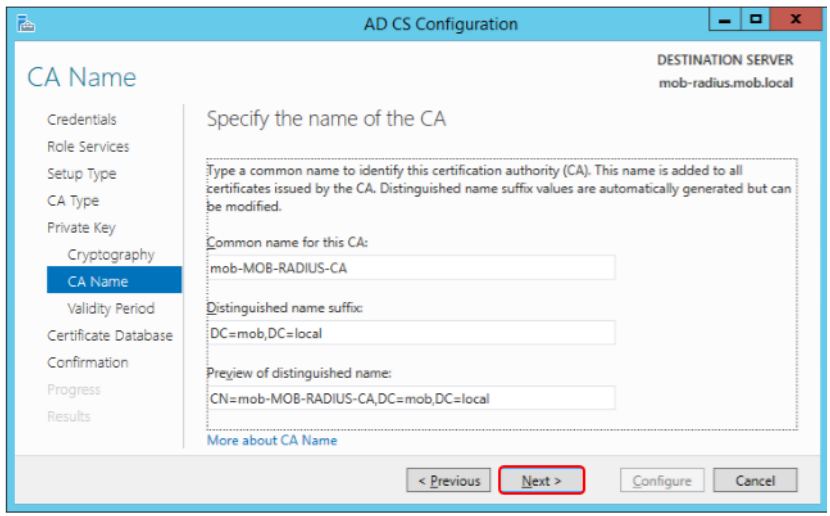

Figure 89. Providing a common name for the CA

18. Enter a validity period for the certificate generated by the CA and click **Next**.

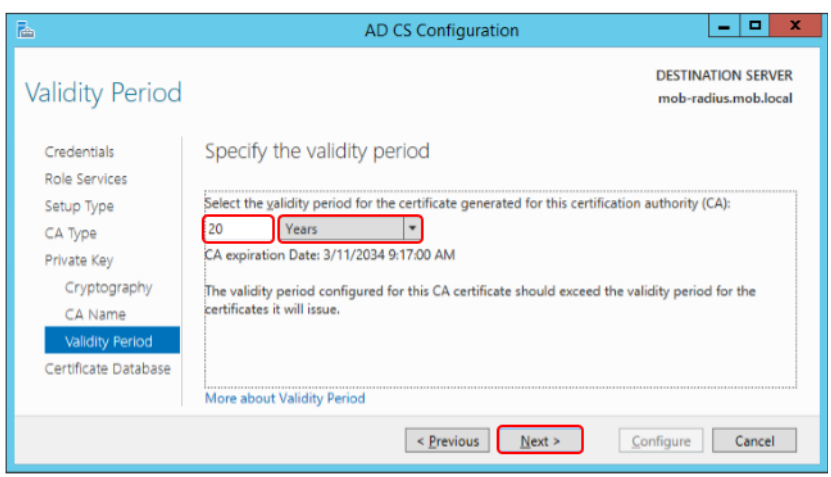

Figure 90. Specifying the certificate validity period

19. Leave the certificate database settings as default and click **Next**.

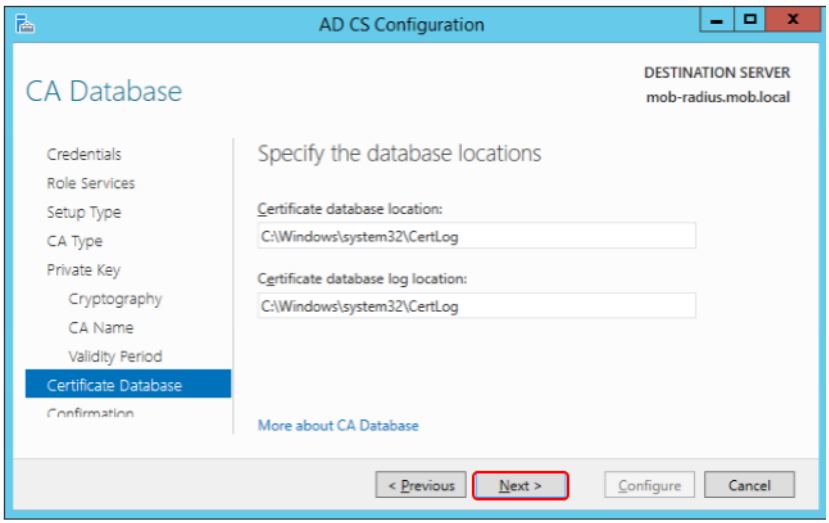

Figure 91. Default configuration for the certificate database

20. At the confirmation window, click **Configure**.

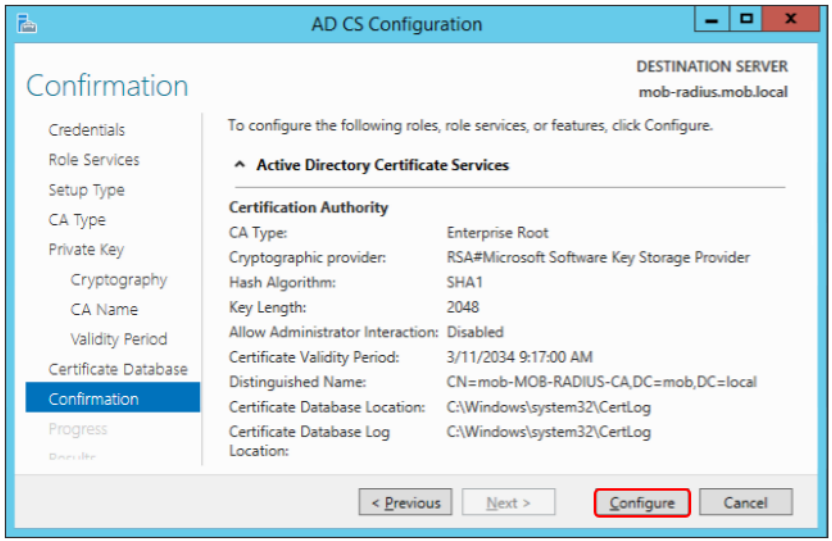

Figure 92. Confirmation to commit the configuration changes

21. After successful completion of configuration changes, click **Close**.

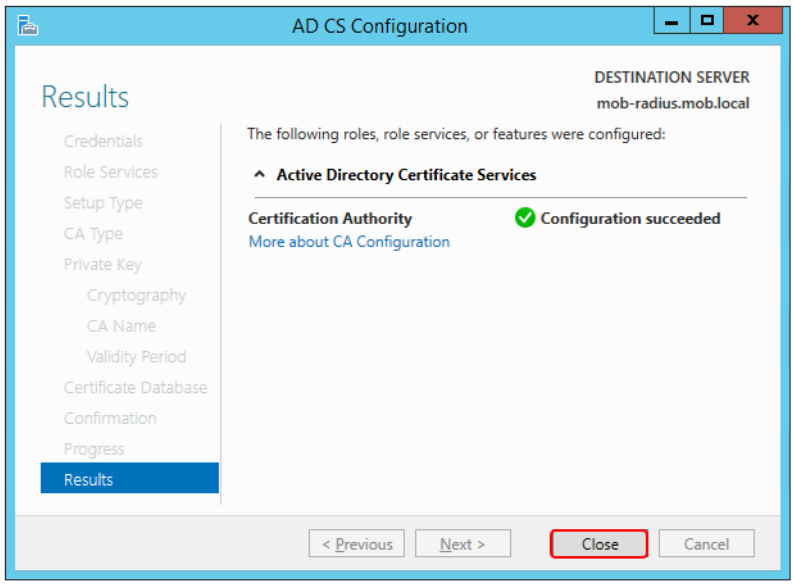

Figure 93. Completion of configuration changes

Section 6 Creating Certificates

Each device should have its own certificate. When the NPS server configuration is created, one certificate is used for the first client access.

Creating a new certificate for the device

Execute the following to create a certificate for a device:

1. Logon to the node where the Certificate Authority has been installed and run the mmc command.

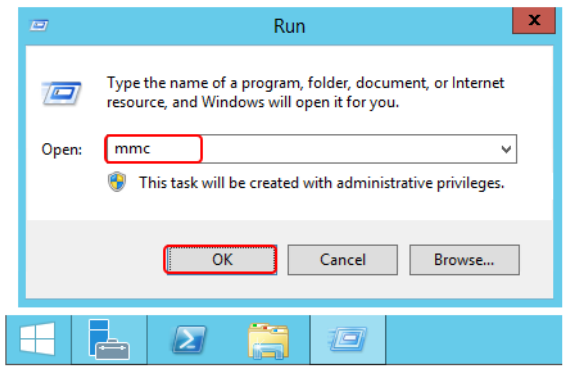

Figure 94. Starting mmc on the Certificate Authority node

2. Handling certificates is done through a Snap-in. Select **File > Add/Remove Snap-in**.

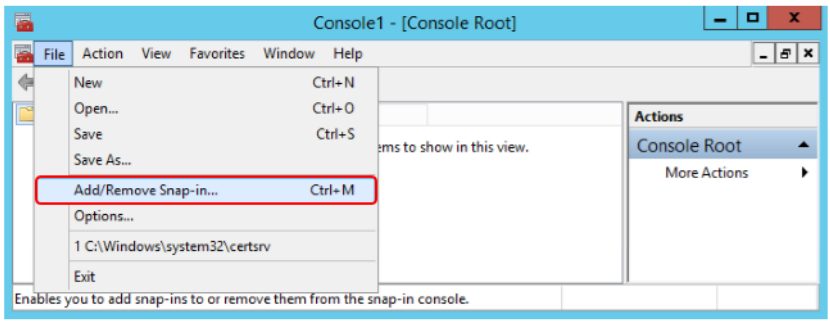

Figure 95. Adding the Certificates snap-in

3. From the available snap-ins, select the Certificates snap-in and then click **Add**.

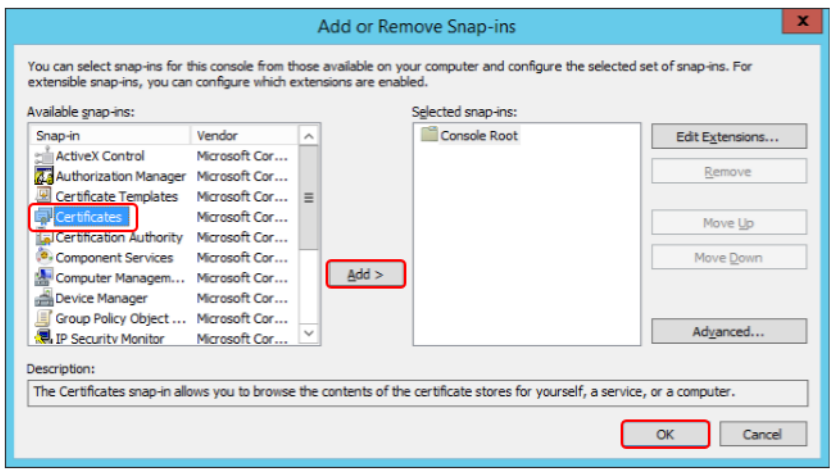

Figure 96. Selecting the Certificates snap-in

4. Select to manage certificates for the computer and click **Next**.

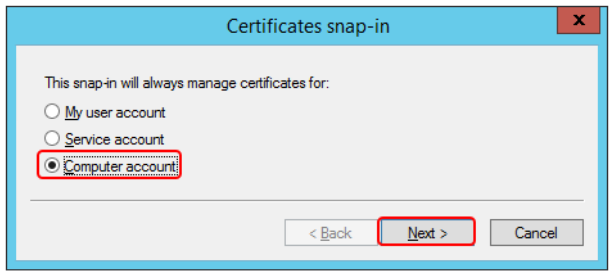

Figure 97. Selecting to manage certificates for the Computer Account

5. Select to manage certificates for the local computer and click **Finish**.

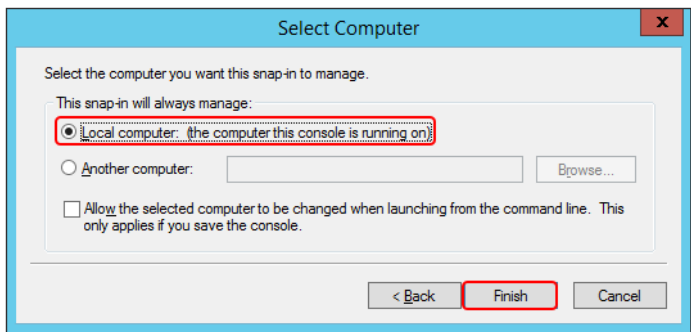

Figure 98. Selecting to manage certificates for the local computer

6. Click **OK**.

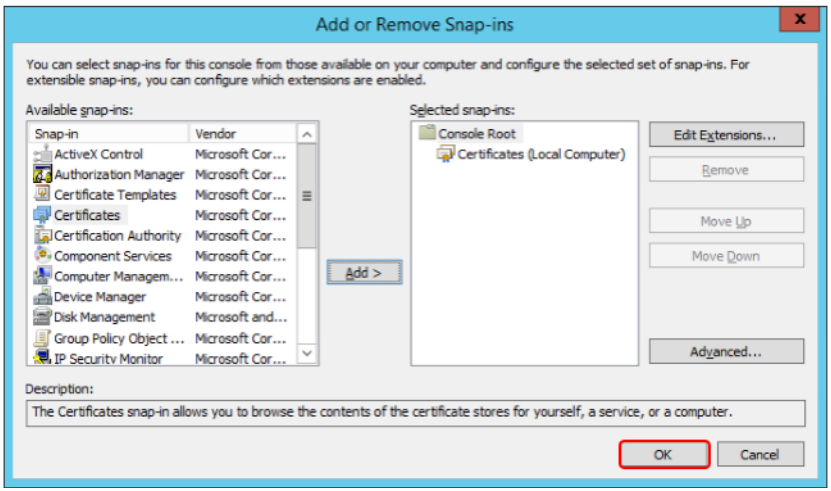

Figure 99. Certificates snap-in added to mcc

7. To create a new certificate, navigate to the **Console Root > Certificates > Personal > Certificates**, right-click the Certificates item and select **All Tasks > Request New Certificate**.

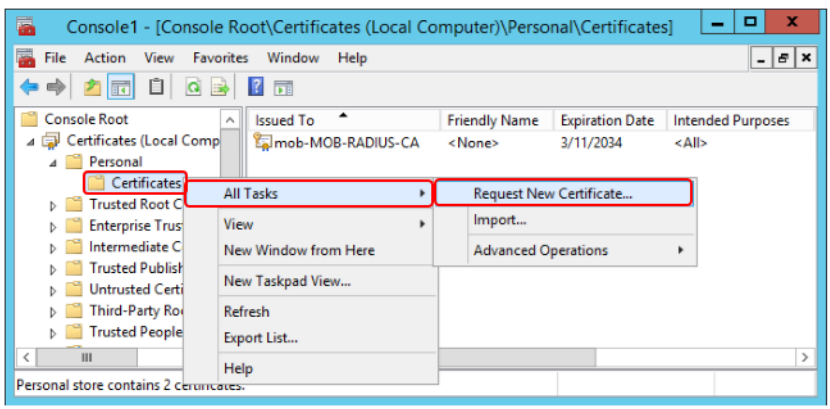

Figure 100. Creating a new certificate for a device

8. At the **Before you begin** window, click **Next**.

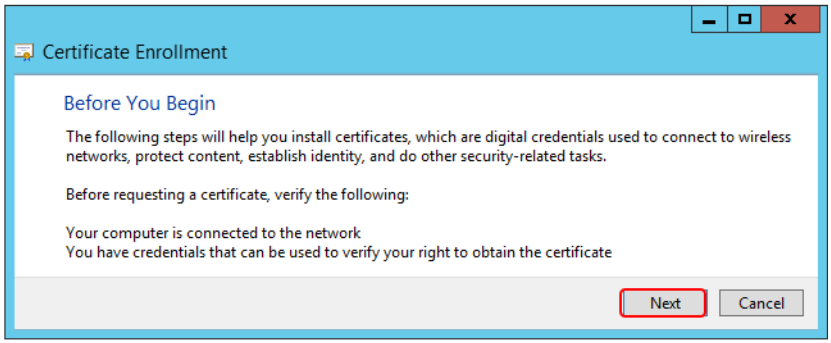

Figure 101. Before you create a certificate window

9. At the **Select Certificate Enrollment Policy** window, click **Next**.

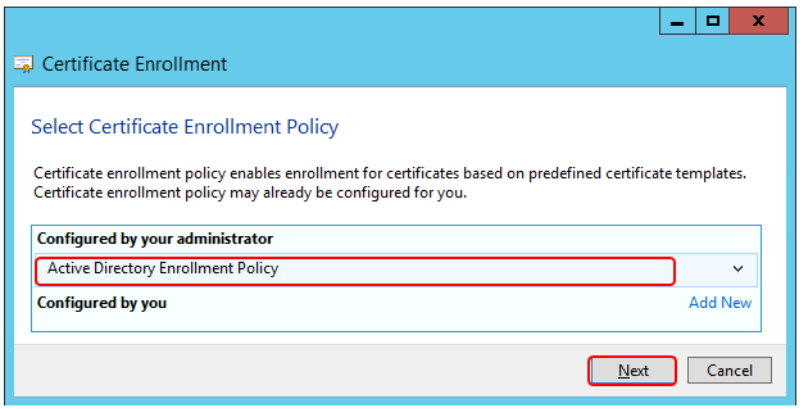

Figure 102. Selecting the certificate enrollment policy

10. Select **Computer** at the **Request Certificates** window and click **Enroll**.

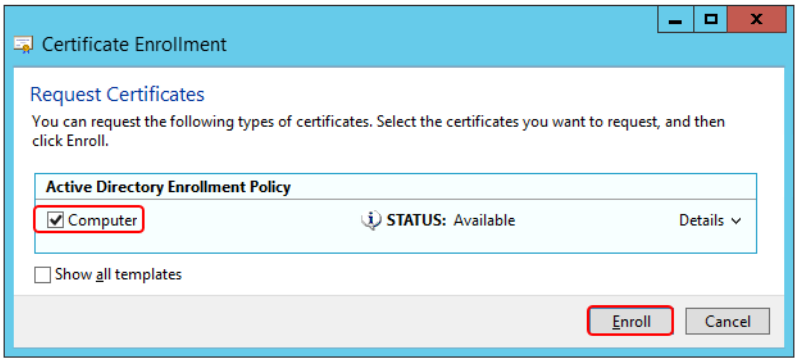

Figure 103. Enroll the new certificate

11. At the confirmation that the new certificate has been produced, click **Finish**.

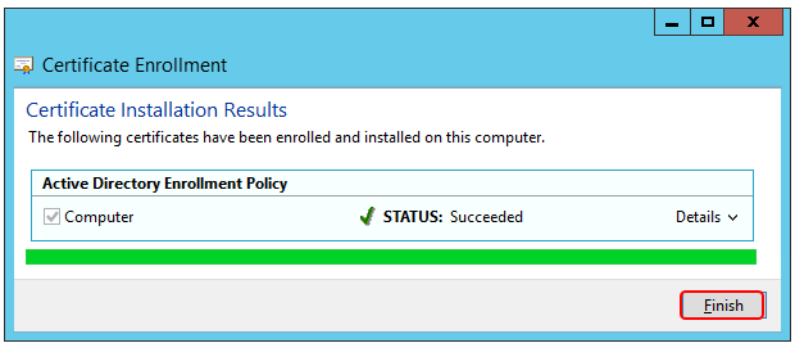

Figure 104. Certificate request completed

12. Use the Properties on the new certificate to change the friendly name to identify the intended device.

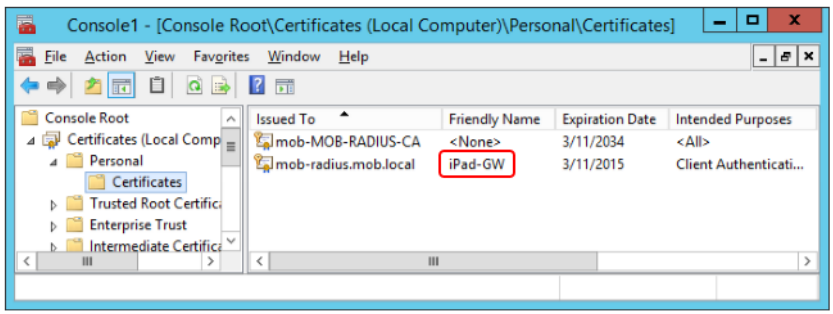

Figure 105. Certificate for device with friendly name

Export Certificates

To export the certificate:

1. Login to the authorization server and access the certificates through the mmc. Navigate to the **Console Root > Certificates > Personal > Certificates**, and right-click the device. Note that the previously defined friendly name assists in selecting the correct device. From the context menu, select **All Tasks > Export**.

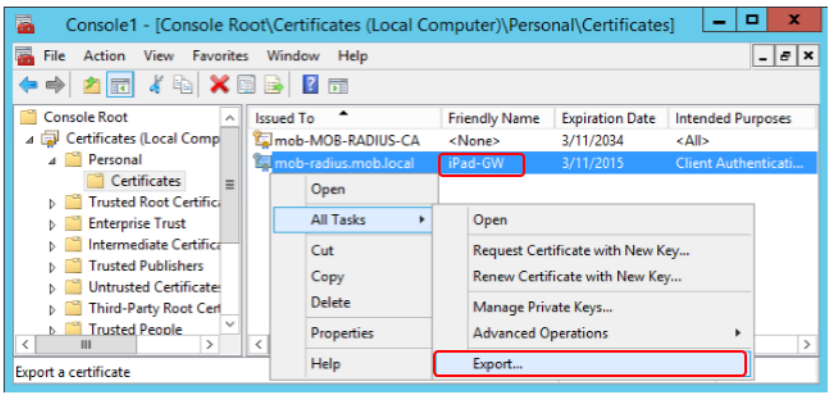

Figure 106. Exporting the Certificate for a device

2. In the **Certificate Export Wizard**, click **Next**.

Figure 107. Certificate Export Wizard

3. Click **Next** at the **Export Private Key** window.

Figure 108. Exporting the private key options

4. Use the default export file format and click **Next**.

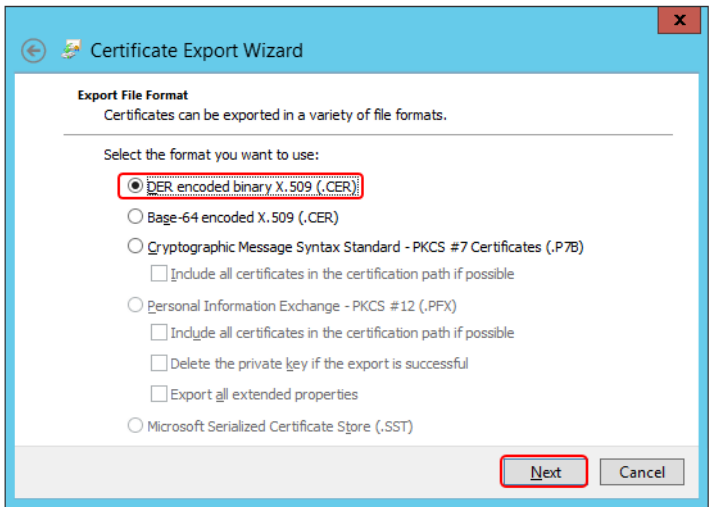

Figure 109. Setting the export file format

5. Provide a file name for the certificate and click **Next**.

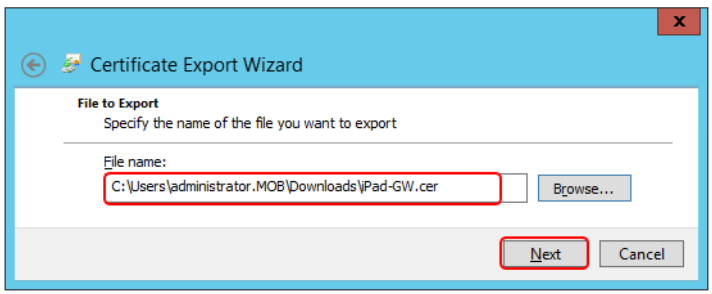

Figure 110. Providing a file name for the exported certificate

6. Click **Finish** to complete the export operation.

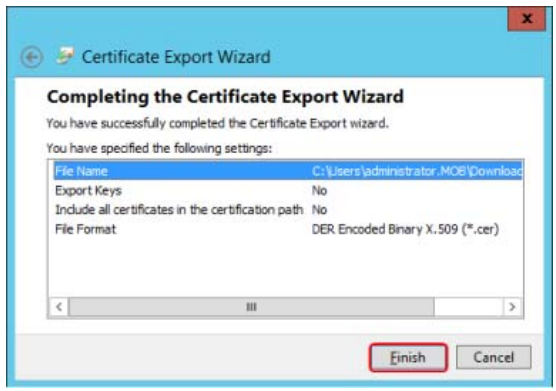

Figure 111. Completing the certificate export wizard

7. Click **OK** to acknowledge the successful completion.

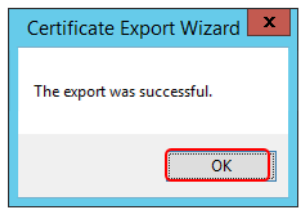

Figure 112. Completion of exporting the certificate for a device

Section 7 Configuring NPS (RADIUS)

This section describes the procedure to add and configure the NPS (RADIUS).

Adding NPS (RADIUS)

In Windows Server 2012 R2, the RADIUS functionality is included in the Network Policy and Access Services role. This must be added to the authorization servers.

Execute the following steps to add the NPS (RADIUS):

1. Logon to the authorization server and start the **Server Manager**.

   Select **Add roles and features**.

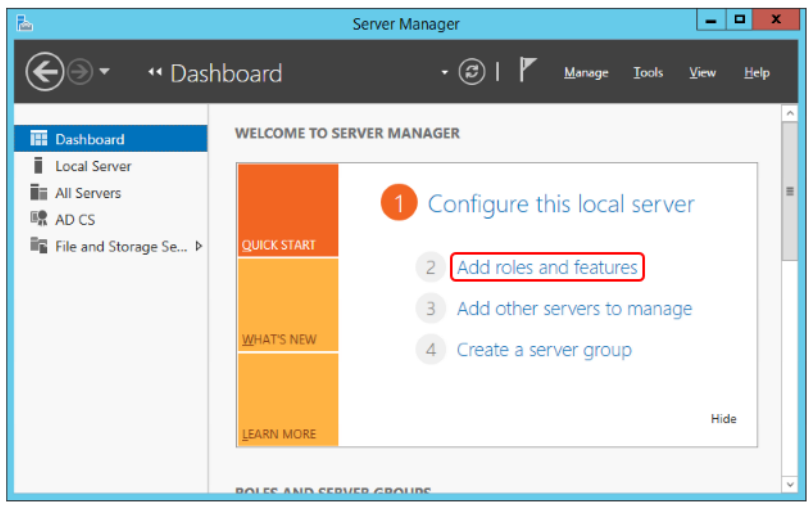

Figure 113. Starting the Server Manager in the authorization server

2. In **Before You Begin** wizard, click **Next**.

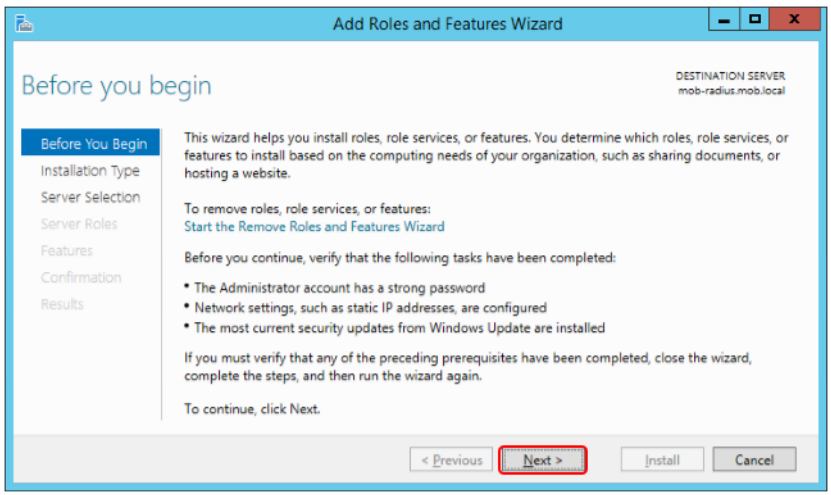

Figure 114. Before you add the roles information

3. Select **Role-based** or **feature-based installation** and click **Next**.

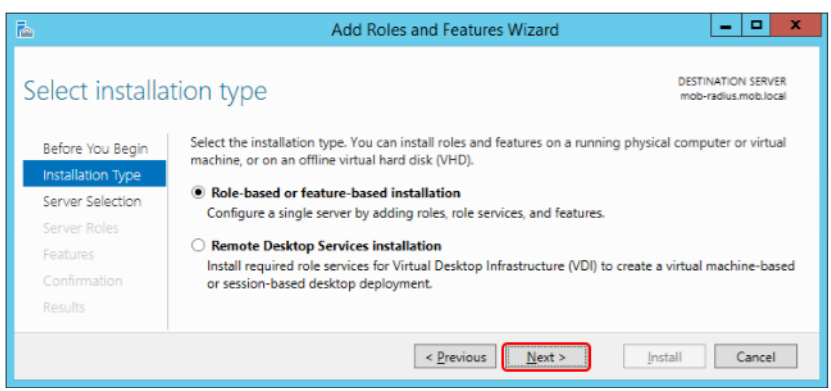

Figure 115. Selecting Installation Type

4. Select the authorization server and click **Next**.

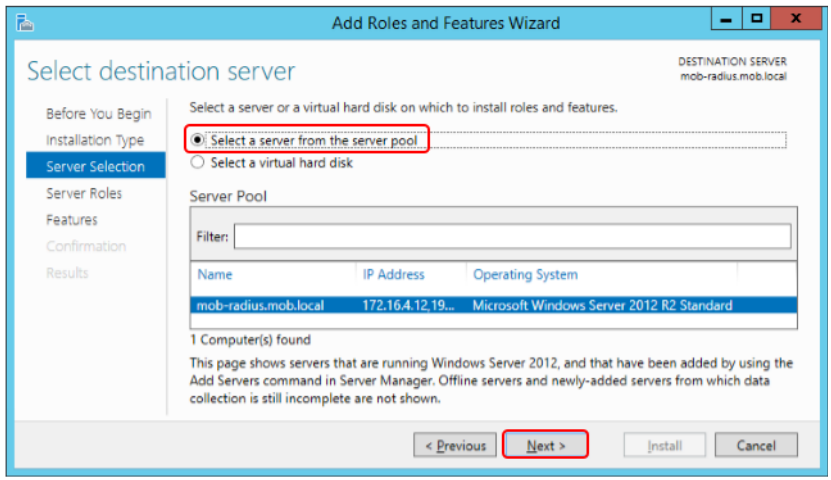

Figure 116. Selecting authorization server for the NPS (RADIUS) role

5. **In Select Server Roles** wizard, select the **Network Policy and Access Services** check box and click **Next**.

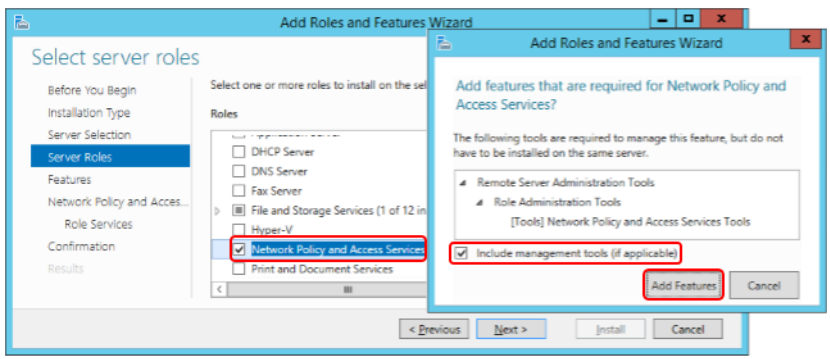

Figure 117. Adding the Network Policy and Access Services role

6. In the **Select Features** window, click **Next**.

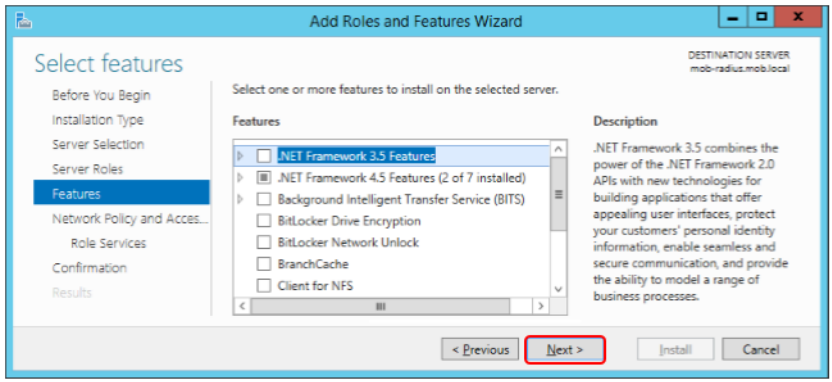

Figure 118. Selecting features

7. In **Network Policy and Access Services** wizard, review the information on the policy and click **Next**.

Figure 119. Information regarding Network Policy and Access Services

8. In **Select Role Services** wizard, select the **Network Policy Server** check box to access the Remote Desktop Session Host servers. Click **Next**.

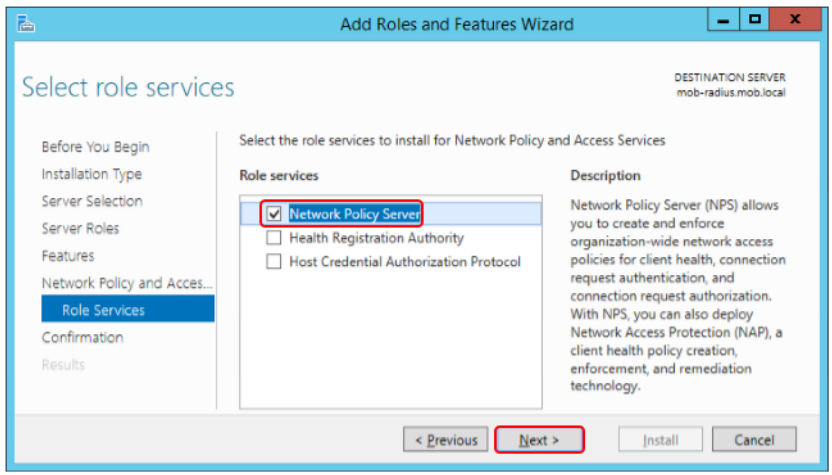

Figure 120. Required option for the Network Policy Server

9. In **Confirm Installation Selections** wizard, click **Install** to begin the installation of the NPS role.

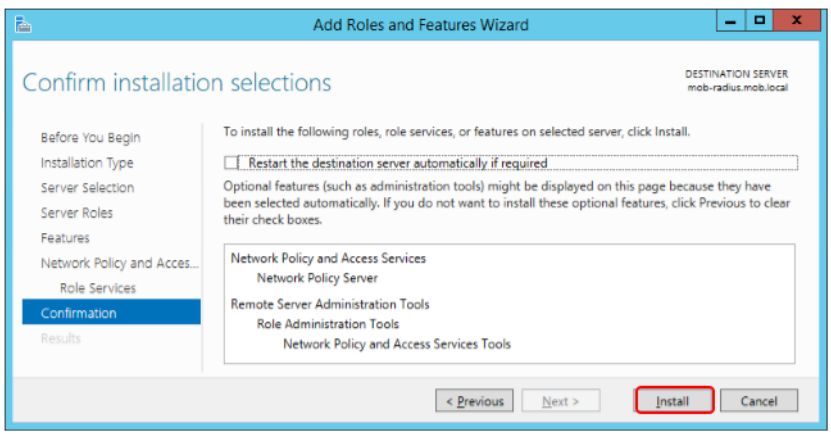

Figure 121. Initiate installation of NPS server

10. In the **Installation Results** wizard, click **Close**.

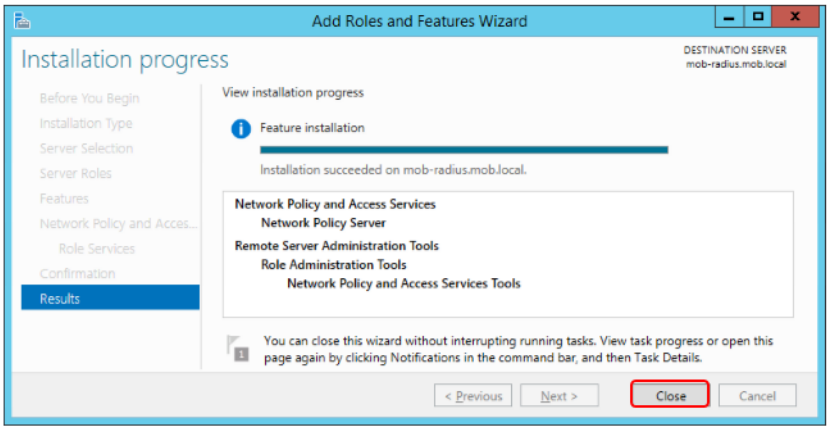

Figure 122. Successful addition of the NPS server

Registering the server with Active Directory

Initially the NPS server has to be registered with the Active Directory.

Execute the following steps to register the NPS Server.

1. In **Server Manager > NAP**, right-click the NPS Server and select Network Policy Server.

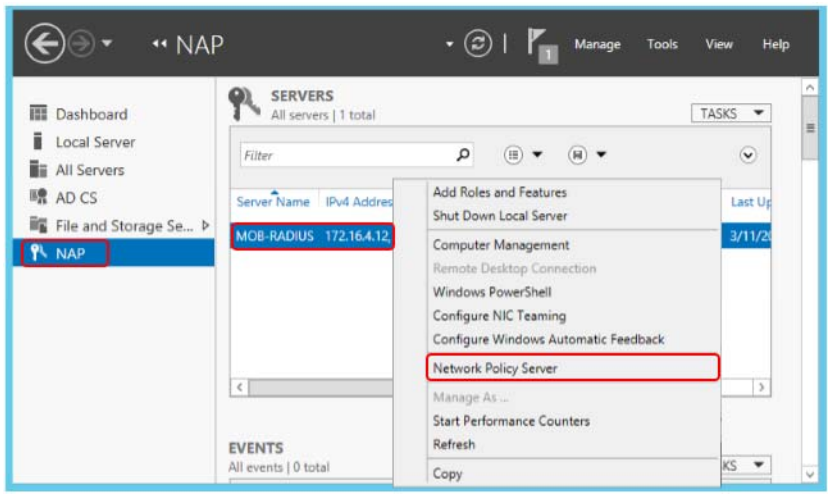

Figure 123. Accessing the Network Policy Server interface

2. Right-click the NPS object and select **Register server in Active Directory** from the context menu.

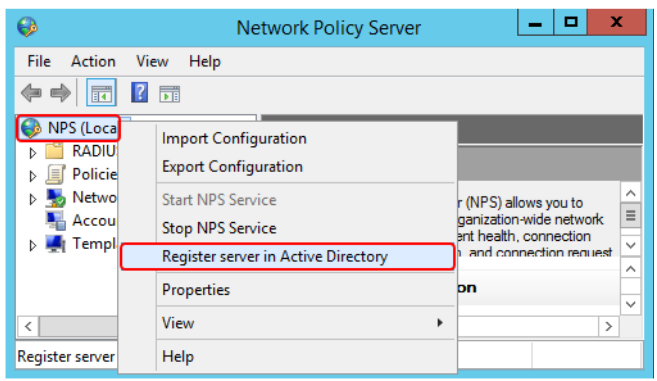

Figure 124. Registering the NPS server in Active Directory

3. Click **OK** to confirm that the changes to read users dial-in properties are to be done.

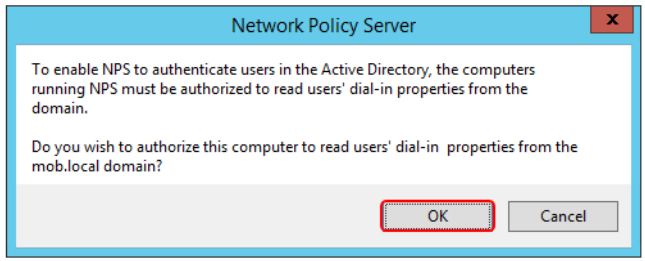

Figure 125. Request to authorize the computer to read users' dial-in properties

This prompts for a confirmation. Click **OK** to proceed.

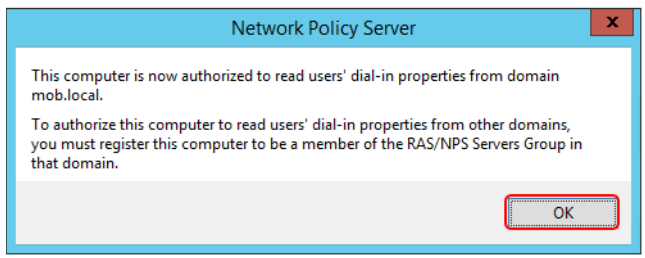

Figure 126. Confirmation that the computer is authorized to read users' dial-in properties

Configuring NPS (RADIUS)

After the installation of the NPS, the NPS server must be configured as a RADIUS server.

This will, for example specify the type of encryption to use. The initial configuration is in the form of a getting started guide. Once completed, the resulting configuration can be reviewed and modified as required.

Execute the following steps to configure the NPS (RADIUS):

1. Access the NPS configuration (see Step 1). The **Getting Started** dialog appears where the **Standard Configuration** should be set to *RADIUS server for 802.1X Wireless* or *Wired Connection*. Then select **Configure 802.1X**.

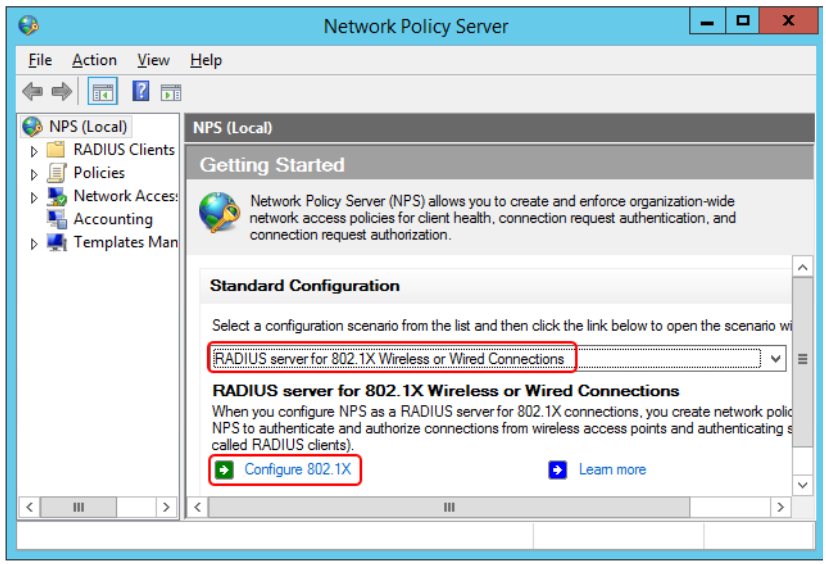

Figure 127. Specifying the standard configuration

2. In the **Configure 802.1X** dialog, select **Secure Wireless Connections**. Enter the name of the policy and click **Next**.

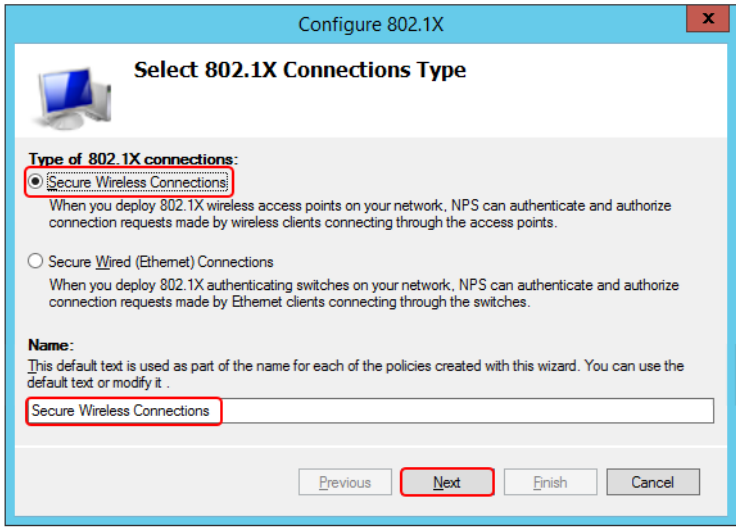

Figure 128. Selecting the connection type

3. The next window provides the ability to add wireless access points. In this guide, the clients will be added at a later stage. Click **Next** to continue.

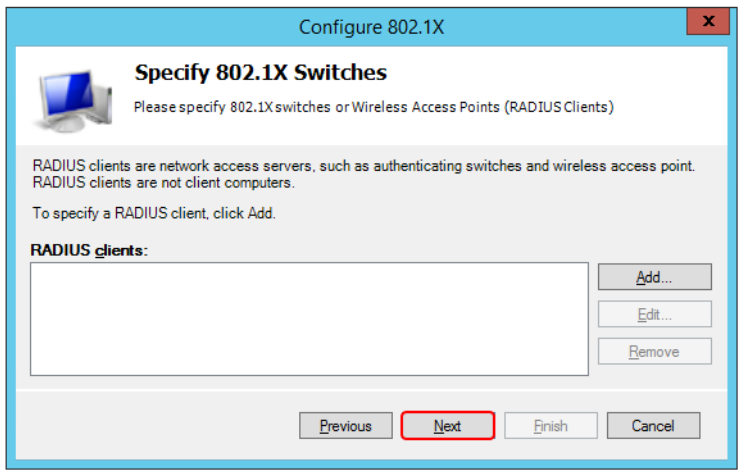

Figure 129. Configuration window for adding clients such as wireless access points

4. In **Type**, select **Microsoft Protected EAP (PEAP)** and click **Configure**. It helps to confirm the authentication method. The certificates will be setup at a later stage.

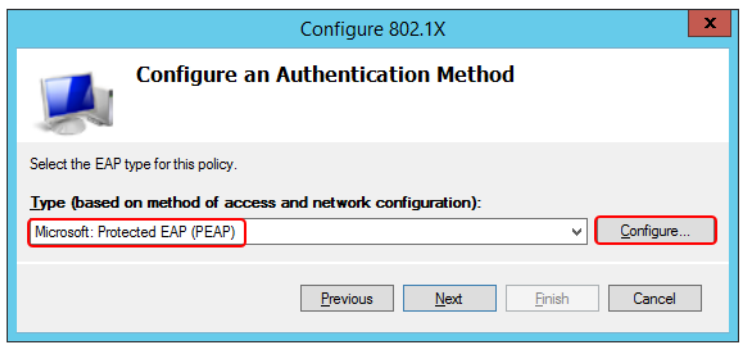

Figure 130. Specifying the authentication method

5. With the certificate in place, the **Edit Protected EAP Properties** dialog appears.

If a warning appears with a message that there is no available certificate, either a CA Authority has been installed on another node or it has not been installed on the Domain Controller. Multi-node CA, NPS, DC are not in the scope of this user guide.

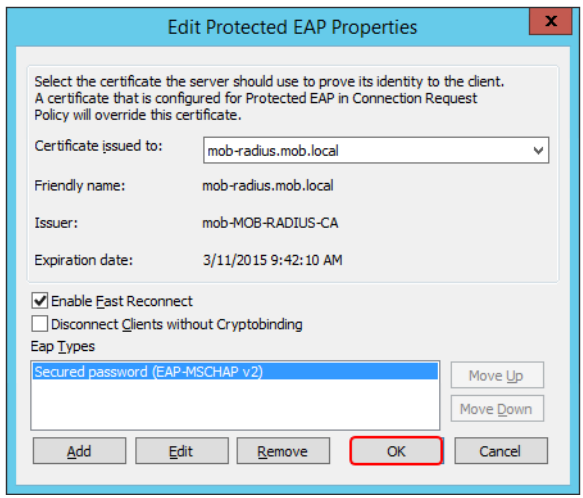

Figure 131. Editing the Protected EAP properties

Click **OK** to return to **Configure an Authentication Method** window (see Figure 130). Click **Next**.

6. The **Specify User Groups** wizard is used to restrict the authentication to specific User Groups. It is recommended to restrict the users to non-administrative user groups. In the following example, the **Groups** will be left blank. Click **Next**.

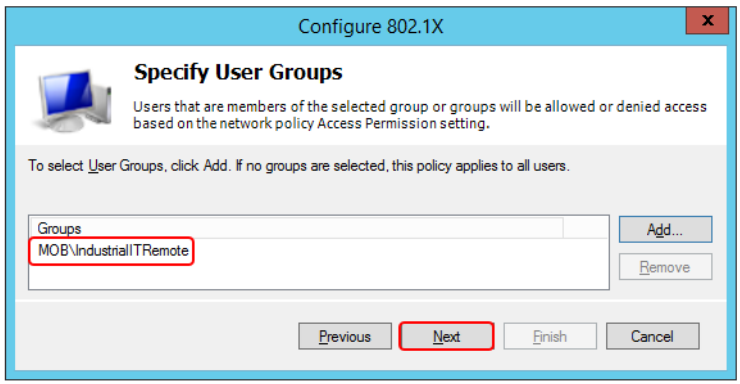

Figure 132. Restriction of access based on User Groups

7. The **Configure Traffic Controls** wizard appears. This is used to configure the traffic control attributes. In this example, no adjustments are made. Click **Next**.

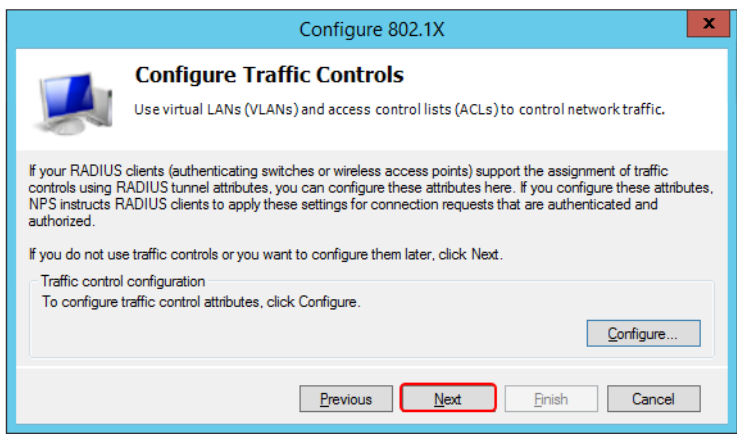

Figure 133. Option to implement traffic control

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

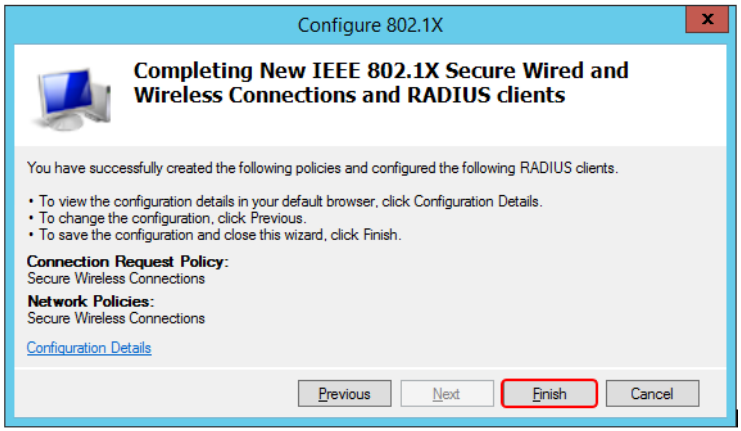

Figure 134. Completing the getting started configuration

Starting and Stopping the NPS Service

After completing the configuration, stop and start the NPS Service to ensure that the configuration is applied to the NPS Server.

To stop the NPS Service, right-click the NPS object and select **Stop NPS Service** from the context menu.

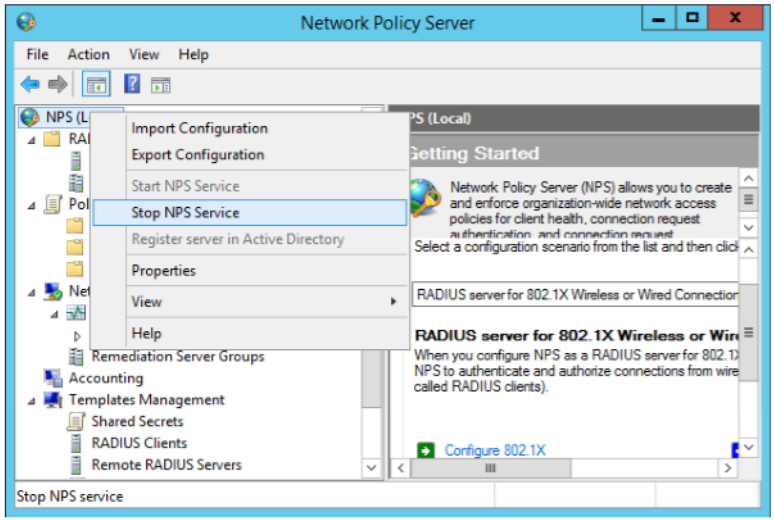

Figure 135. Stopping the NPS Service

To start the NPS Service, right-click the NPS object and select **Start NPS Service** from the context menu.

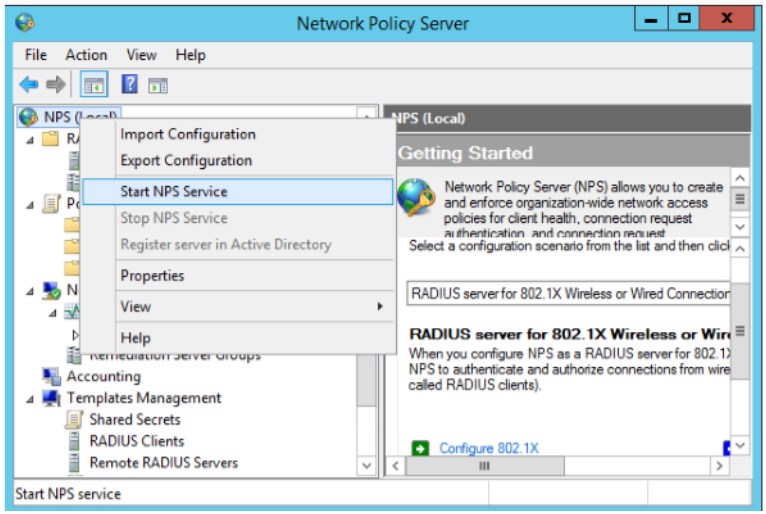

Figure 136. Starting the NPS Service

Section 8 Remote Desktop Session Host Server Configuration

The goal for the Remote User Configuration is to provide a configuration where the remote operator logs on to the 800xA system and is presented only with an 800xA workplace. When the workplace is closed, the remote desktop session is automatically closed.

If the remote operator disconnects from the session, reconnecting to the system presents the same remote desktop session.

Note that automatic closing of remote desktop session can be configured in the Remote Desktop Session Host server. It may be desirable to set this to a time that allows movement between production areas without closing the session.

Whilst remote desktop log on may be granted to an existing user, the configuration described here assumes that a separate user is created for remote logon to enable the remote user privileges to be more restrictive, that is, monitor the process, but not to operate it.

Following is the procedure to set up the first remote user:

1. Create a remote user.
2. Create a Remote Operators security group.
3. Add the remote operator to the Remote Operators and IndustrialITUser group.
4. Add the remote operator to the 800xA system.
5. Add the Remote Operators group to the Remote Desktop Session Host Server Remote Desktop Host Configuration security.
6. Add the Remote Operators group to the local policy of the Remote Desktop Session Host Server for the Allow log on locally, and Allow log on through Remote Desktop Services.

7. Restart the Remote Desktop Session Host server.
8. Test log on to the remote operator through the Windows remote desktop client.
9. Create a desktop shortcut to the iPad® Workplace.
10. Use the startup program definition from the shortcut to setup the environment startup program for the remote user.
11. Configure the 800xA User profile for the remote user to use the iPad® Operator workplace in Operator workplace mode.
12. Configure remote operator privileges for non-operation.
13. Test that remote desktop log on of the remote operator provides a full screen operator workplace with no desktop.

Adding the remote operator to 800xA

Log on to the Aspect Server, and use the 800xA Configuration Wizard to add the remote operator account to the 800xA system. Make this account a member of Everyone, and Operators.

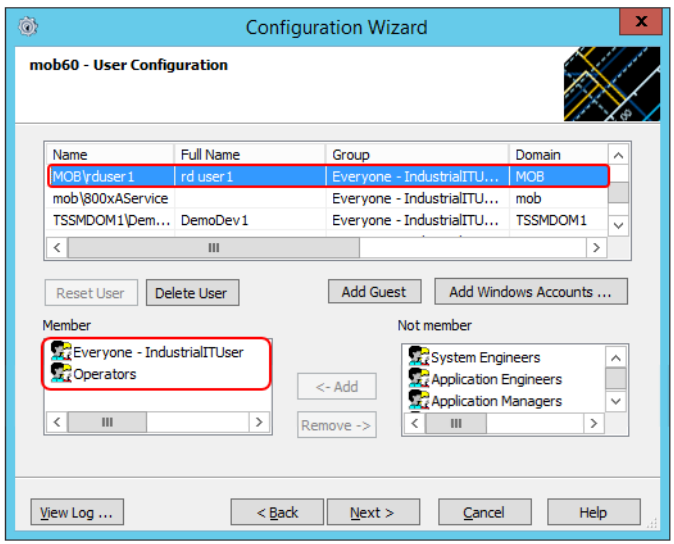

Figure 137. Configuring the remote operator in 800xA

Testing Remote Log on

At this stage it should be possible to use a Windows workstation or server to start a remote desktop session to the Remote Desktop Session Host server using the remote operator account.

Create a desktop shortcut to the iPad® Workplace

After opening the remote desktop session, it is beneficial for the user configuration to place a shortcut to the iPad® Workplace (assuming that this is required workplace for the remote operator) in the desktop.

Start the 800xA Workplace application, select the workplace required, and click **Create Desktop Shortcut**.

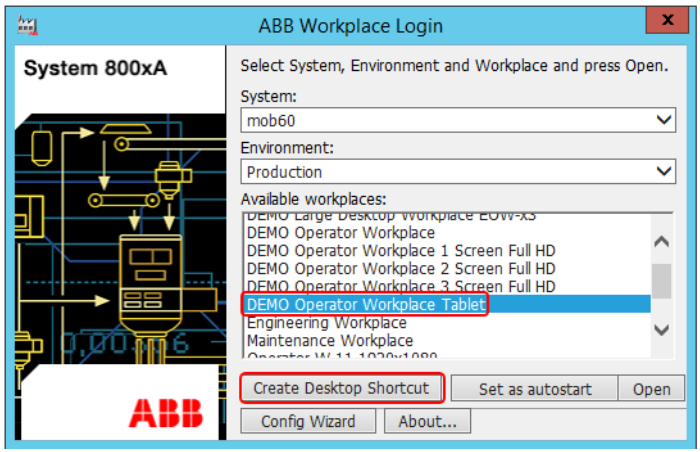

Figure 138. Using the 800xA Workplace application to create a desktop icon

This creates a shortcut on the desktop.

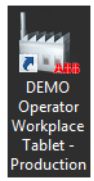

Figure 139. The 800xA iPad® Operator Workplace desktop icon

Setting the remote operator startup application

To ensure that the remote operator has access only to the workplace, the workplace should be defined in the environment settings of the remote user.

To determine the command line for the workplace, right-click the workplace desktop icon and select Properties.

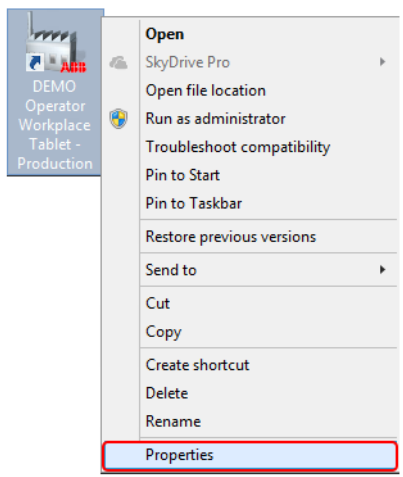

Figure 140. Accessing Properties of the iPad® Operator Workplace

Copy the Application Target line. As this must be entered in the Domain Controller, the target definition can be copied into a text file that will then be copied to the Domain Controller.

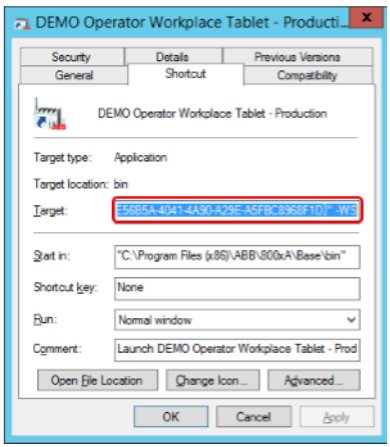

Figure 141. Retrieving the target for the iPad® Operator Workplace

Log on to the domain controller, start the Active Directory Users and Computers program, double-click the remote operator account, select the Environment tab, select the **Start the following program at logon** check box, and paste in the target obtained through the desktop shortcut as in Figure 141.

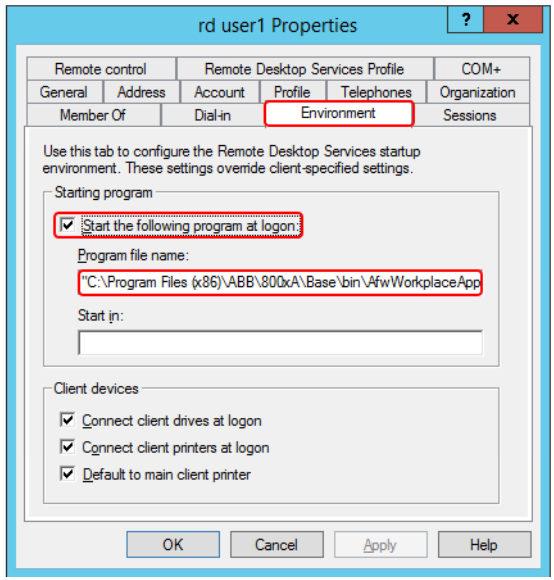

Figure 142. Updating the remote operator user to only start the iPad® Operator Workplace at log on

Configuring the 800xA user profile for the remote

The remote user should be configured in 800xA for the correct workplace, and that the workplace should be in Operator mode.

Log on to the aspect server, start the engineering, and access the Workplace Profile Values for the remote operator. Set the Default Workplace to the iPad® Operator Workplace.

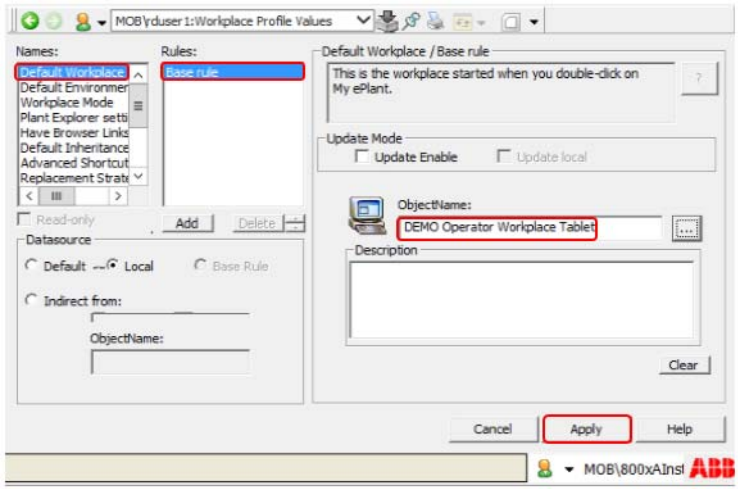

Figure 143. Setting the remote operator Default Workplace

Configure the Workplace Mode to be in Operator Workplace Mode.

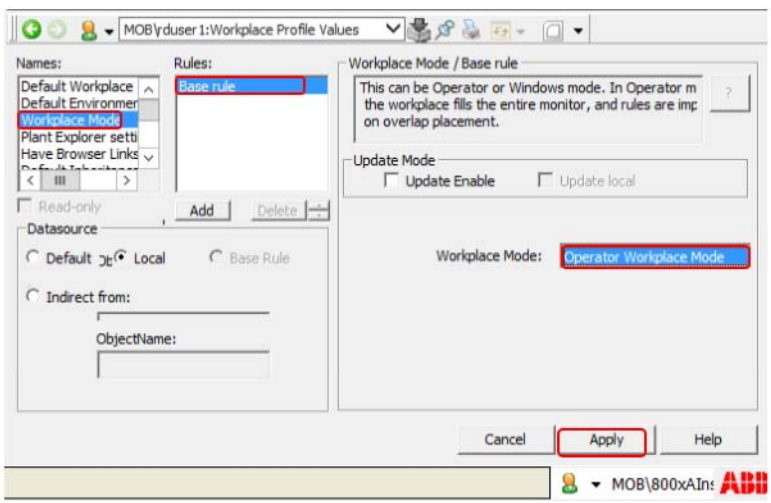

Figure 144. Setting the remote operator Workplace Mode

Configure remote operator privileges for non-operation

While mobile access to the production system provides many benefits, the risk to accidental operation of the system must be minimized. Mobile devices such as iPads, are easy to pick up in one hand and perform unintended actions. To minimize this risk, the security definitions in 800xA should be defined to prevent operation of the system by the remote operator.

One example of security restriction, is to place a **Security Definition** aspect on the Control Network base and configure it to deny access to the remote operator:

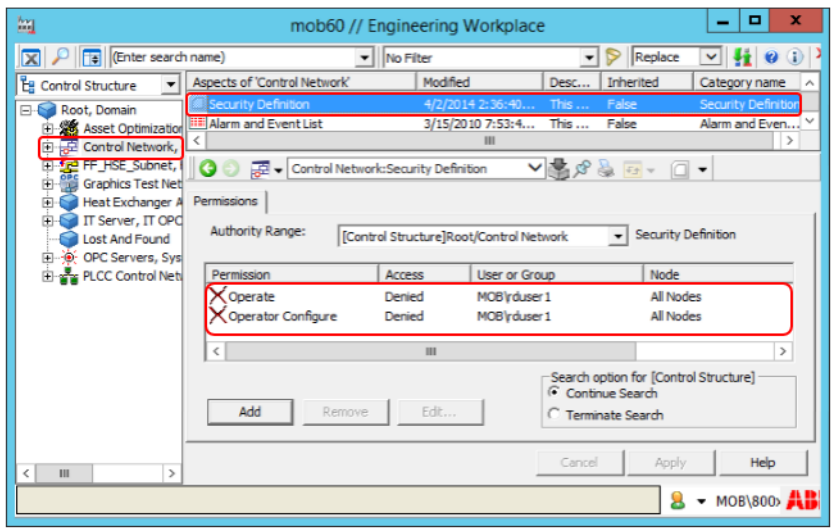

Figure 145. Placing a Security Definition on the Control Network to restrict operations

While this allows the remote operator to view graphic displays and faceplates, the buttons on the faceplate will be disabled.

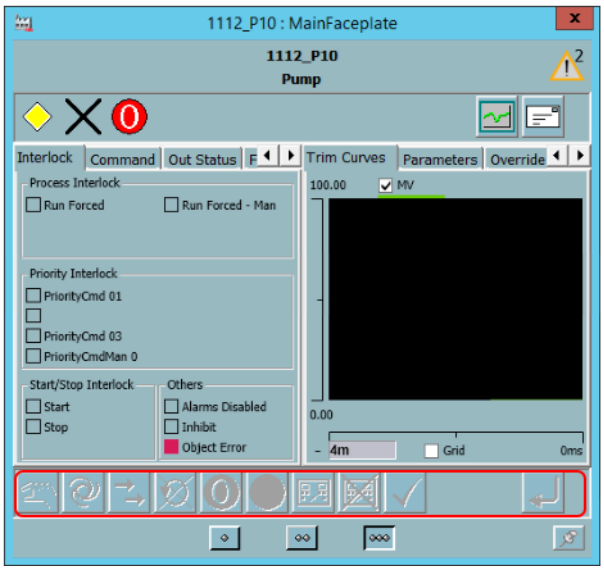

Figure 146. Confirmation that the remote operator cannot control production

Test the remote desktop log on of the remote operator

To test the configuration, use a Windows workstation or server and the remote desktop client to open a session to the Remote Desktop Session Host Server. When logged on, only the 800xA workplace should be present:

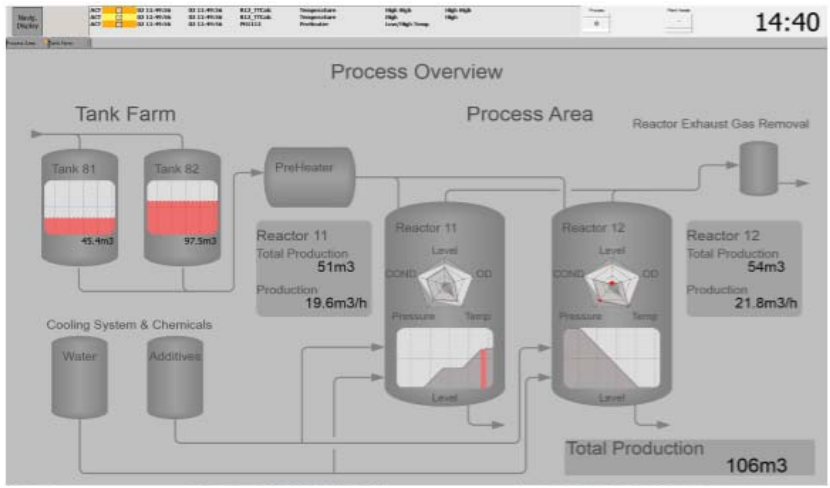

Figure 147. Full screen remote logon to the production environment

Closing the workplace should end the remote desktop session.

Section 9 800xA Customization for iPad®

Due to the smaller screen area of iPad®, there may be difficulties interfacing with items on the screen. This may be due to the small size such as the close window button on the top right of the window, or the requirement to scroll across a number of columns in an alarm band.

There are two main areas of customization for iPad® Workplace. The first customization includes 800xA objects to assist in setting up a workplace in a smaller screen area, and the second is to configure Windows to enlarge certain Windows elements.

800xA iPad® Workplace

The customized 800xA iPad® operator workplace, available via the ABB Library, provides a starting point for developing a workplace which is more suited to the smaller screen size of the iPad®. The customized workplace is in the form of an .afw file which can be imported into the 800xA system. It comprises the following:

- iPad® Operator Workplace object
  - The date and time application bar item has been removed
  - The tool bar time item used instead of the application bar
- iPad® Operator Workplace panel object
  - This defines the startup display for the iPad® Operator Workplace
- iPad® Alarm & Event List Configurations object
  - This contains the 3 line alarm list which has been defined for a smaller screen to eliminate the horizontal scroll bar from occurring

The following is the resultant iPad® Operator Workplace.

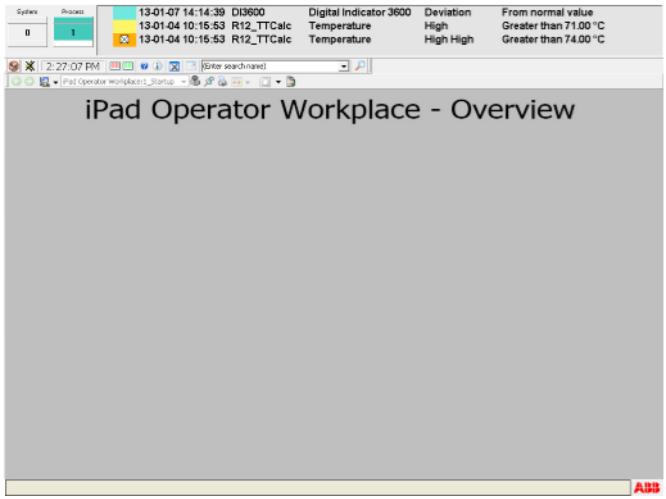

Figure 148. Initial iPad® Operator Workplace

Windows Configuration on Small Screens

Configuring the Windows environment for smaller screens enables easier operation. This must be performed on a per user basis. Since access is required to the Windows environment, the startup to the 800xA workplace needs to be temporarily disabled.

Since this configuration removes the target information, a copy should be placed into a text file for easy restoration of the setting.

Changing the Title Bar Size

One of the difficulties in a smaller screen area is closing windows as the close button in the title bar is so small.

Execute the following steps to change the title bar size:

1. Log on to the Remote Desktop Session Host server with the remote operator user account. Right-click on the desktop and select **Personalize** from the context menu.

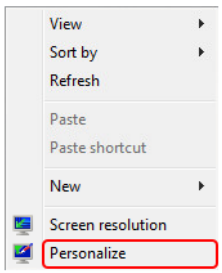

Figure 149. Accessing the windows personal configuration

2. Select the current windows color configuration.

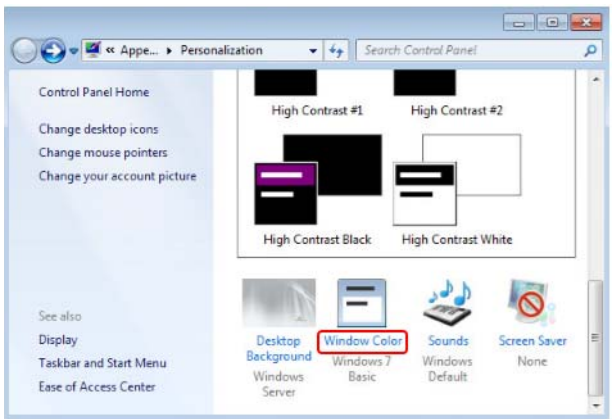

Figure 150. Accessing the Windows Color and Appearance configuration

3. Select the Title Bars and change the Font. Click **Apply** to commit the changes.

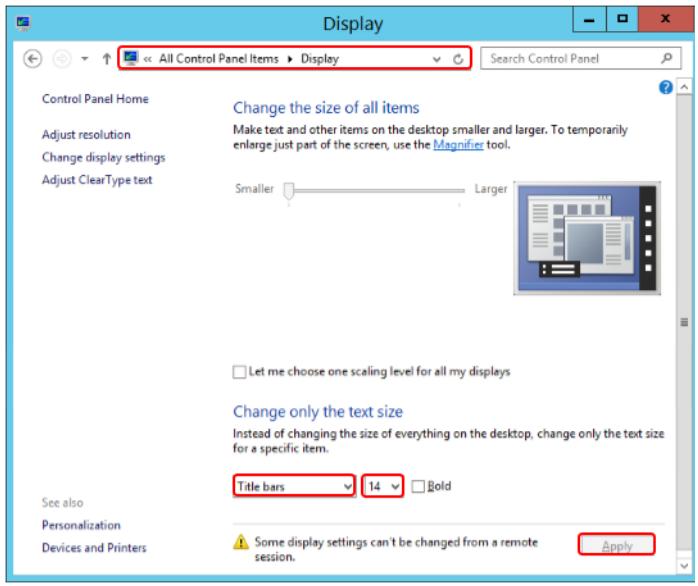

Figure 151. Modifying the title bar for a larger close button

4. The original workplace had the following title bar.

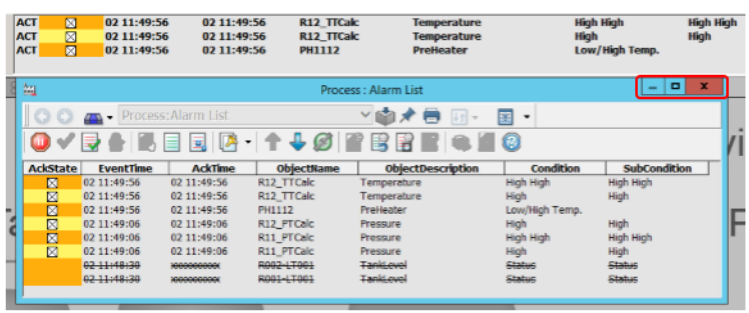

Figure 152. Original windows title bar

5. The following is the modified workplace. This minor modification results in easier closing of windows in the workplace.

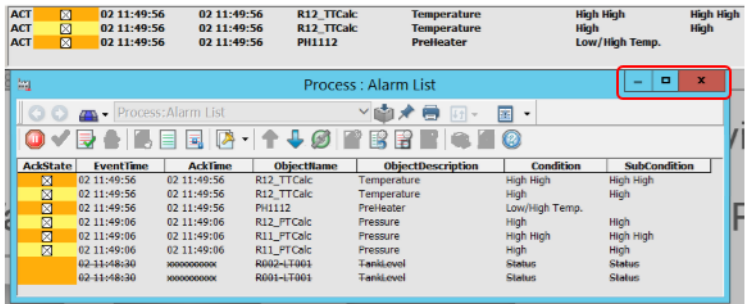

Figure 153. Enlarged windows title bar

Section 10 Configuring BAT54

This section describes the procedure to configure the BAT54 wireless access points, configure tool installation, configure BAT54 rail devices, and to add access points to RADIUS.

Configuring BAT54 Wireless Access Points

This section is described based on wireless access points that are not previously configured, or reset to the default settings.

To enable easy identification of each device, it is recommended to have only one new device on the network at a time. After assigning an IP address to the device, the next device is attached to the network and configured.

Configuring Tool Installation

Execute the following steps to configure tool installation:

1. The BAT54 is configured through a dedicated utility from Hirschmann. Execute the *HAC-LANconfig.exe* files to install the utility.

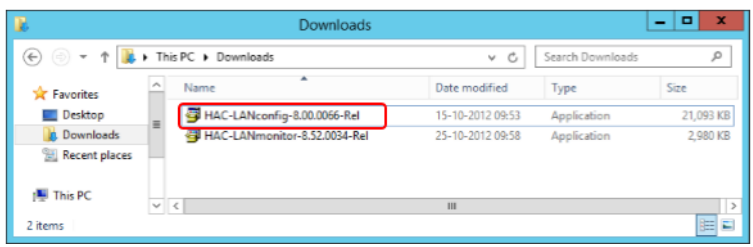

Figure 154. Hirschmann configuration installation utility

2. The **Hirschmann Software Setup** dialog appears. Click **Next**.

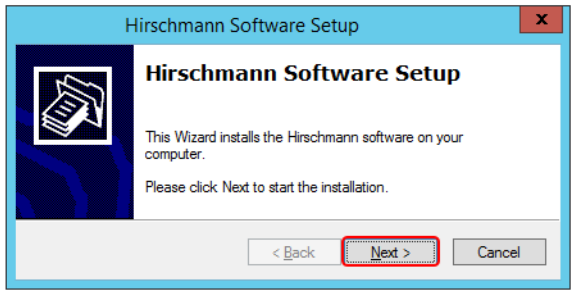

Figure 155. Hirschmann installation program

3. The **Software Components** wizard appears. Click **Next**.

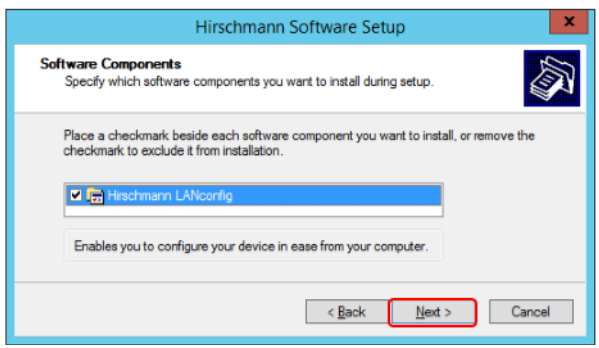

Figure 156. Selection of software components

4. The **Target Directory** wizard appears. Click **Browse** to select the location to install the software. Click **Next.**

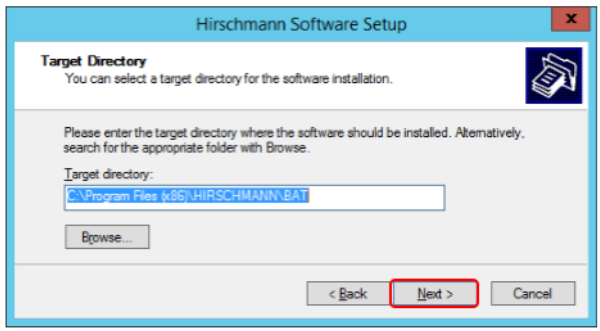

Figure 157. Selecting the target directory

5. The **Desktop Links** wizard appears. Click **Next**.

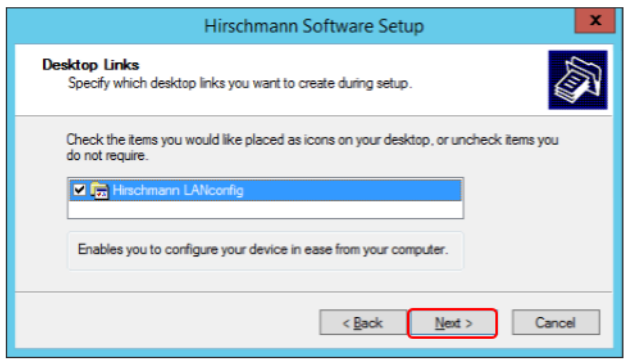

Figure 158. Selection of Desktop Links

6. The **Setup complete** wizard appears. Click **Finish** to complete the installation.

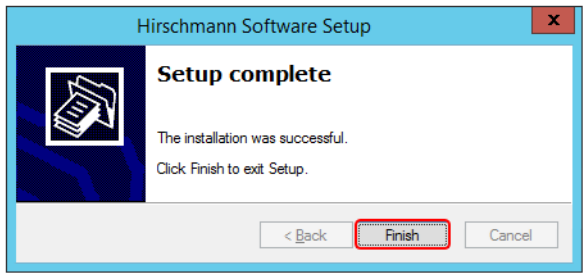

Figure 159. Setup Complete window

Configuring BAT54 Wireless Access Points

Execute the following steps to configure BAT54 wireless access points:

1. Execute the configuration utility from the desktop.

Figure 160. Hirschmann configuration utility desktop icon

2. The **Firmware update** dialog appears. Click **OK** to notify that there are no firmware files in the archive directory.

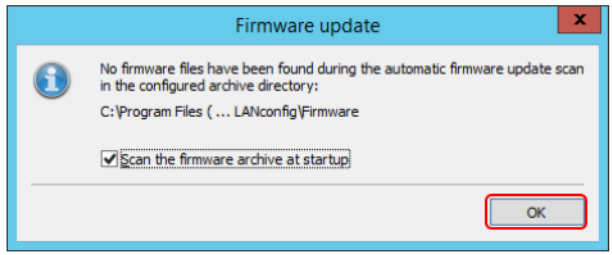

Figure 161. Notification that there are no firmware files in the archive directory

3. To add devices, select the **Hirschmann LANconfig** folder.

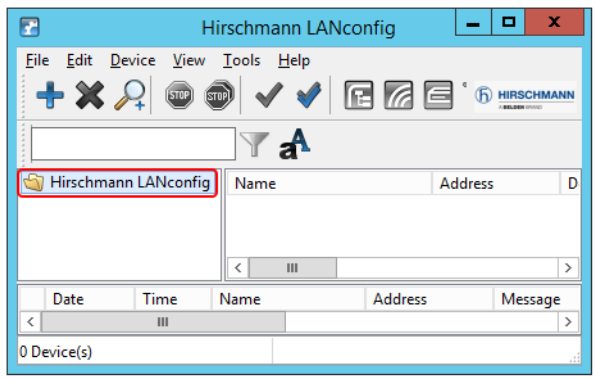

Figure 162. Selecting the Hirschmann LANconfig folder

Group configuration of access points has been found to set up one of the wireless networks. Hence, group configuration of access points should be avoided unless full functionality can be established.

4. Select **File** > **Find Devices** option.

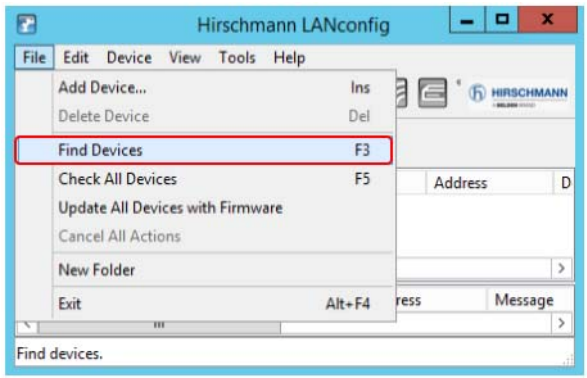

Figure 163. Initiating a scan for new wireless devices

5. Click **OK** in the **Find Devices** dialog.

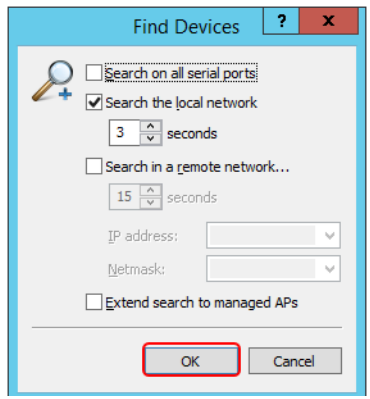

Figure 164. Find devices option window

If there is difficulty in finding a device that has just been added to the network, it may require that only the new device is on the network. i.e. temporarily, disconnect the other BAT54 wireless access points. The other access points need to remain disconnected until the initial configuration has been written to the newly attached access point. This procedure is applicable to the initial setup of the device, and not after the wireless network is in use.

6. The default IP address of new devices will be 192.168.0.254.

Click **Yes** to begin the initial device configuration.

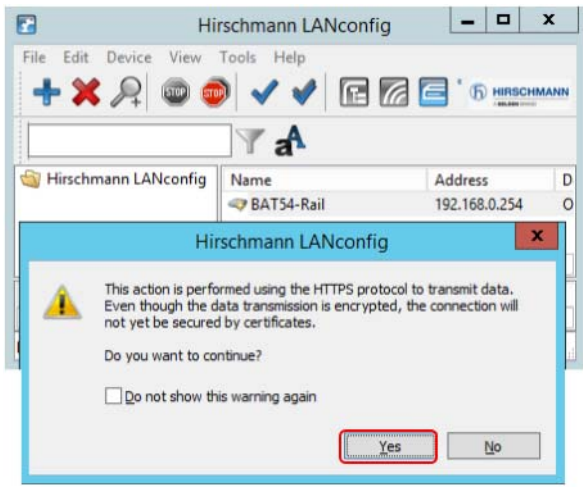

Figure 165. Newly discovered device

7. The **Setup Wizard for BAT54 Rail** dialog appears. Click **Next**.

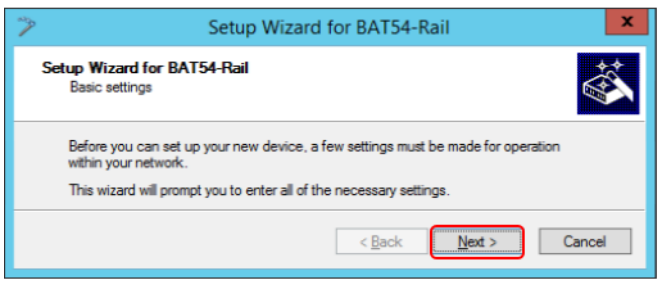

Figure 166. Setup wizard for BAT54-Rail

8. In **Device Name**, enter a name for the device and click **Next**.

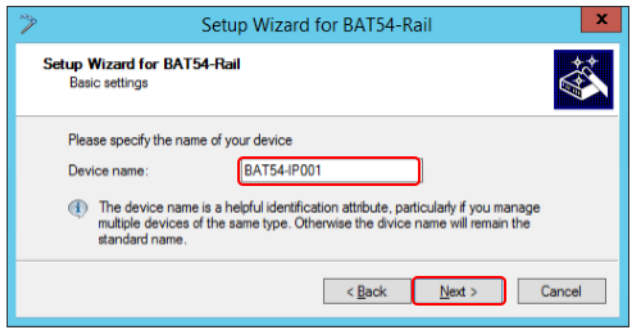

Figure 167. Providing a name for the access point

9. To restrict administration access, it is required to define a password. This should be a complex password and kept under strict control. Enter the password twice and click **Next**.

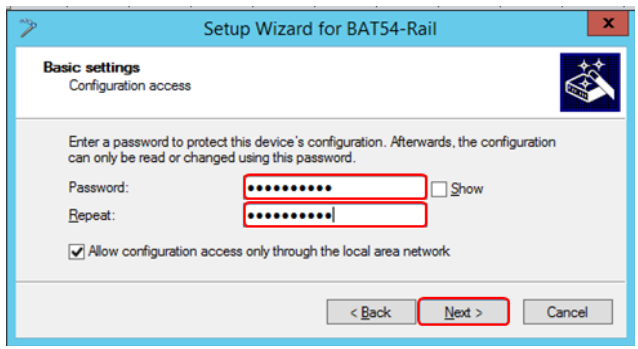

Figure 168. Providing an administrative password for the device

10. The next window provides the option to define how the device should get its IP address. For this configuration, a static address is defined by first setting the DHCP mode to **Off**.

    Click **Next**.

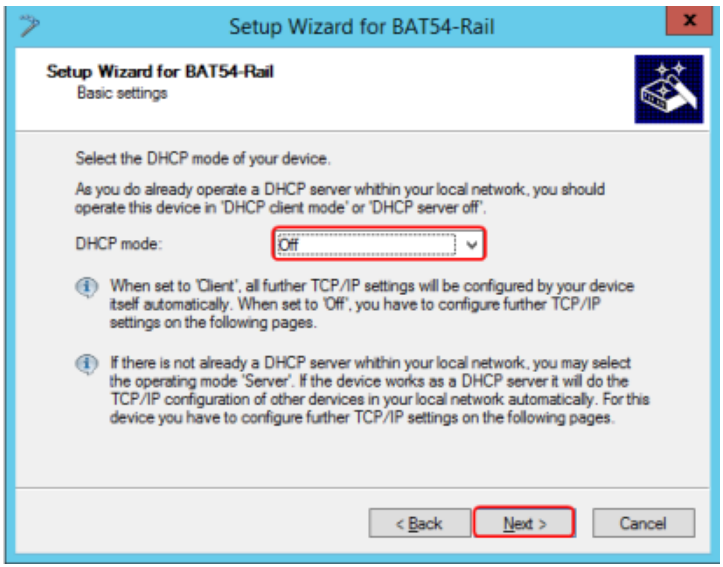

Figure 169. Defining that a static IP address will be assigned to the device

11. The first access point in the example will be set to 192.168.0.1. As the device only needs to communicate to the Remote Desktop Session Host servers, no gateway or DNS server addresses are required.

    Enter the IP address and click **Next**.

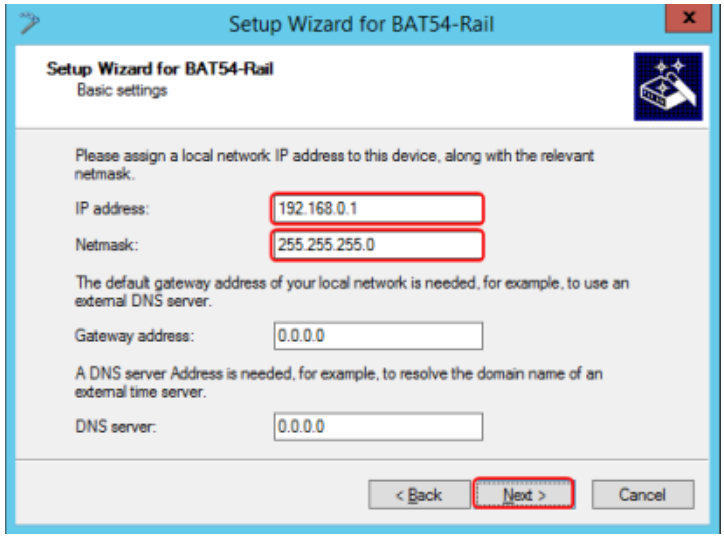

Figure 170. Providing the IP address for the access point

12. Enter the relevant information in **Location**, **Administrator**, and **Comments**. This information will be used for the general maintenance of the wireless network. Click **Next**.

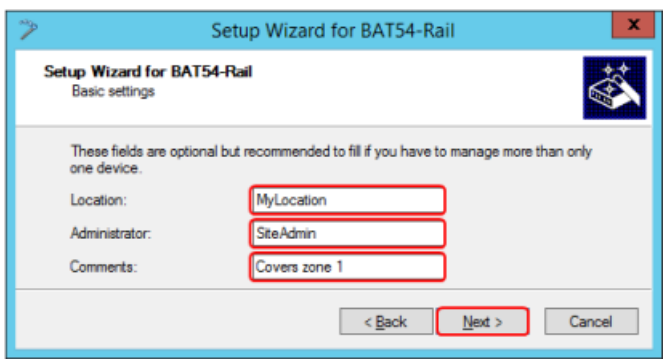

Figure 171. Providing optional additional information to assist in maintenance of the system

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

Figure 172. Completion of the setup wizard

14. The **Password Entry for BAT54 Rail** dialog appears.

    Enter the administrative password and click **Accept**. The Administrator name is not required.

Figure 173. Entering the administrative password

15. After a period of checking the device, the setup wizard for the device will be presented. To enable an understanding of the configuration, each required item will be configured separately. Click **Cancel**.

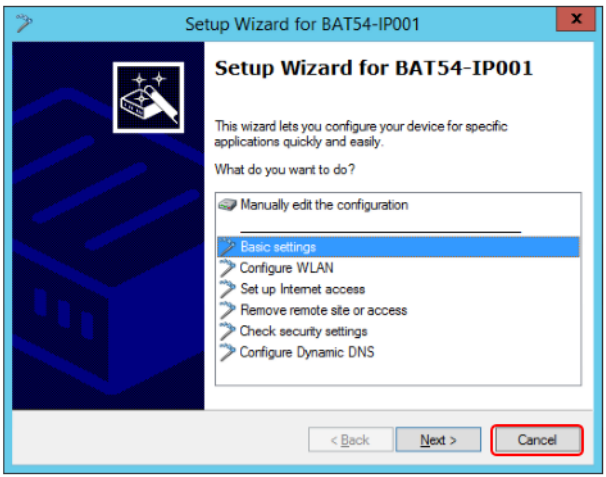

Figure 174. Setup wizard which starts after initial setup of device

Configuring BAT54-Rail Devices

Execute the procedure mentioned in this section to configure the BAT54-Rail Devices.

Entering the configuration mode of the device

To enter the configuration mode of the device, right-click a device entry, and select **Configure** from the context menu.

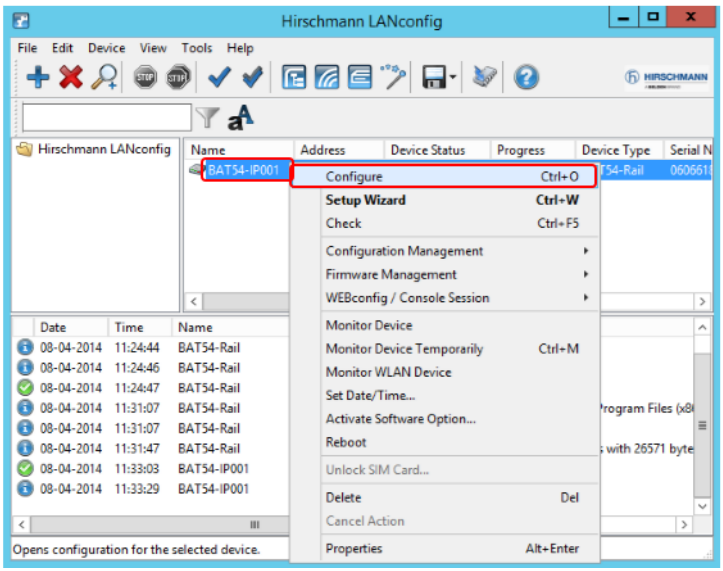

Figure 175. Accessing the configuration mode

Specifying the Country

Select **Configuration > Wireless LAN > General** and set the Country to the correct value..

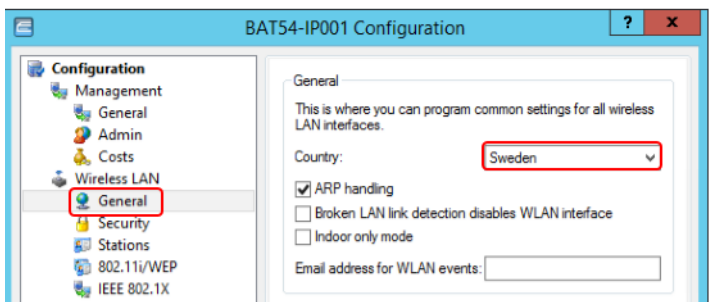

Figure 176. Specifying the country

Specifying Radio Channels

Setting up radio channels is essential to provide a wireless network over an area. Each wireless access points must have different radio channels applied. To manage this, a clear floor plan should be maintained which documents the location of the access points, measured signal radius and radio channel.

It is imperative not to forget that areas above and below the access points should be taken into account. The access point signal should be considered as a sphere, not a circle.

Radio channels must be in the range of 1 - 11.

Execute the following steps for the two wireless interfaces (if both are present). The wireless interfaces must be assigned different channels, and the channels must not interfere with adjacent wires access points.

1. Select **Configuration > Wireless LAN > General**. In **Interfaces**, select *WLAN interface 1 (On)* from drop-down.

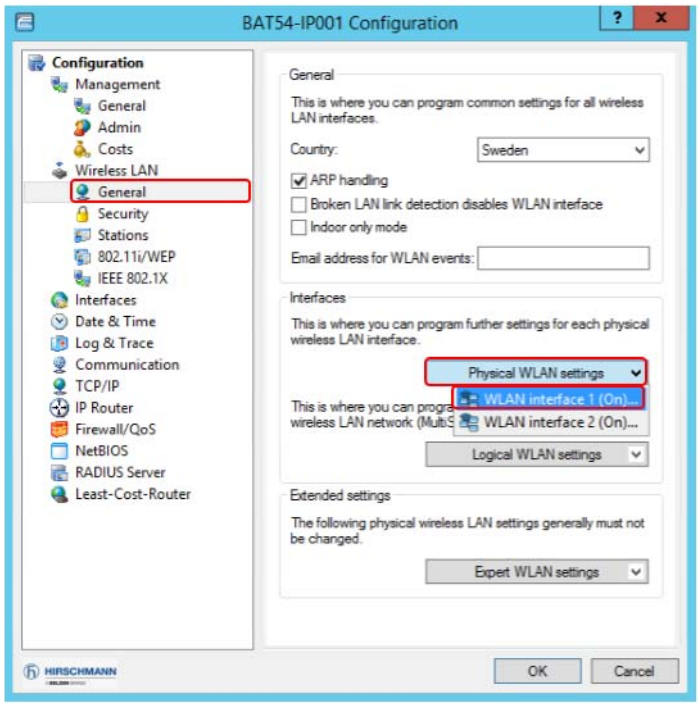

Figure 177. Accessing the WLAN interface 1 parameters to change the radio channel

2. In **Channel Number**, select the channel from the drop-down. Click **OK**.

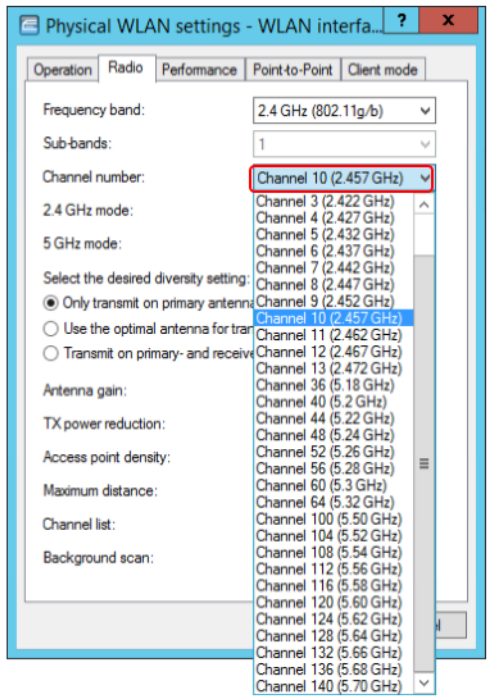

Figure 178. Selection of radio channels

Specifying Encryption

Select the **Configuration > Wireless LAN > 802.11i/WEP** and then click **WPA** or **Private WEP settings** in 802.11i(WPA/AES)/Wired Equivalent Privacy.

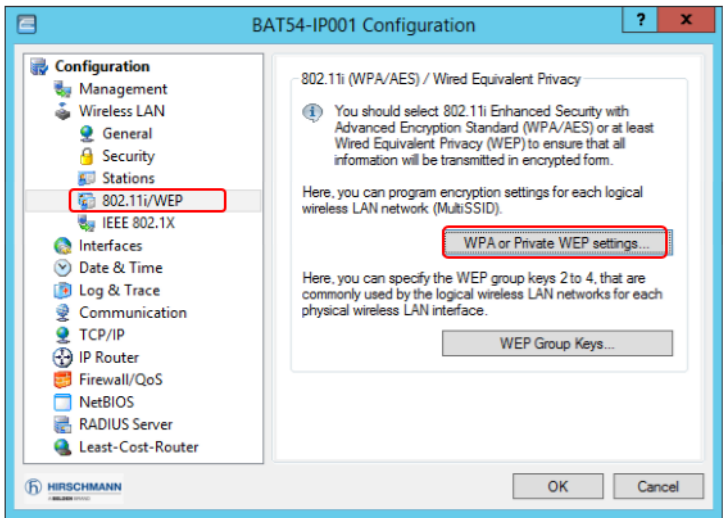

Figure 179. Access the wireless security settings

By default, all of the interfaces have the default settings.

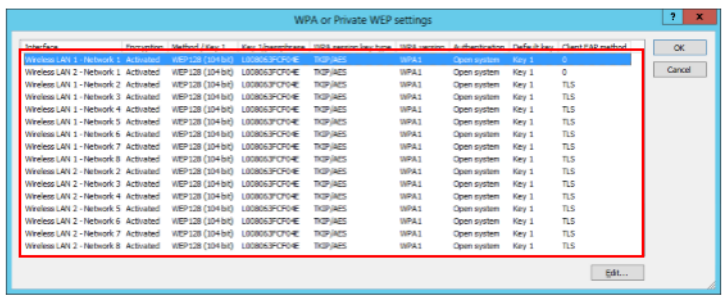

Figure 180. Default encryption definition

Double-click each interface and set the parameters (see Figure 181).

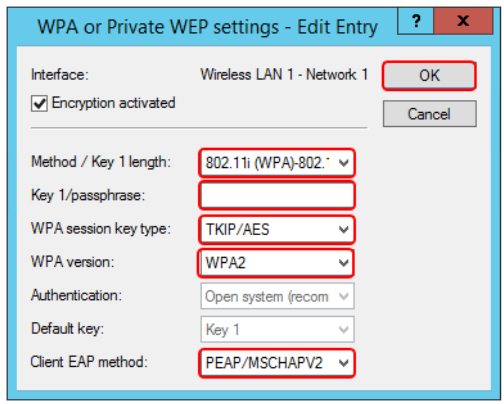

Figure 181. Security setting required for each interface

Ensure that all interfaces are setup correctly and click **OK**.

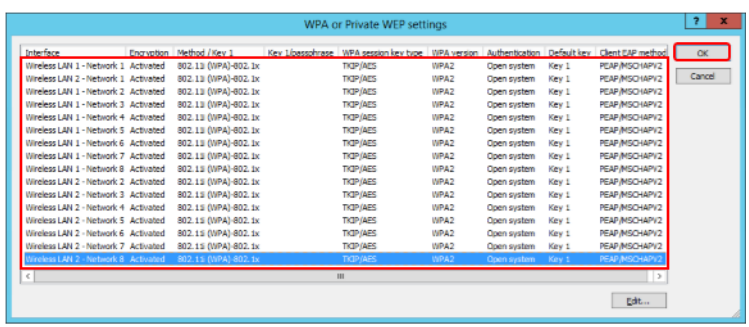

Figure 182. Interfaces configured for encryption

Authentication via RADIUS Configuration

1. Select the **Configuration > Wireless LAN > IEEE 802.1X** and click **RADIUS server** in Authentication via RADIUS.

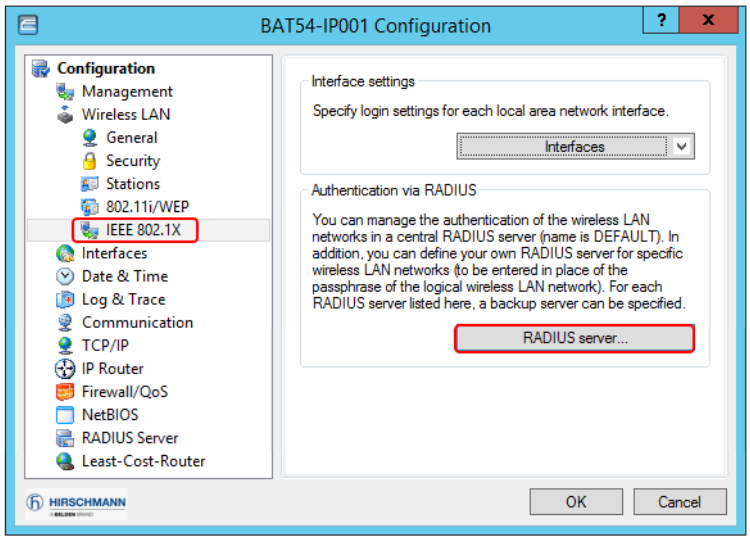

Figure 183. Access the RADIUS server configuration

2. Enter the name, IP address and shared secret for the RADIUS server.

   The shared secret must be same as the shared secret used when defining the access point as a client in the RADIUS server. Click **OK**.

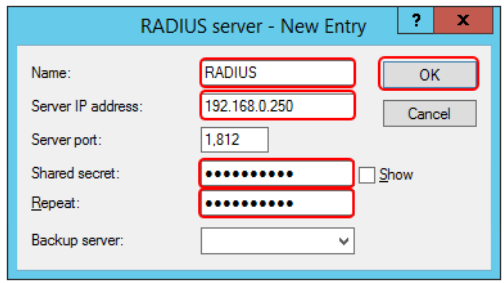

Figure 184. Defining a RADIUS server

After adding the RADIUS servers, it will be possible to define backup servers. This functionality must be tested before the system is placed into production.

Setting the BAT54-Rail to router mode

The device must be in router mode because the BAT54-Rail utilizes the firewall functionality.

1. Select the **Configuration > Interfaces > LAN item** and select **Connect by using the router (isolated mode)** in the LAN bridge settings.

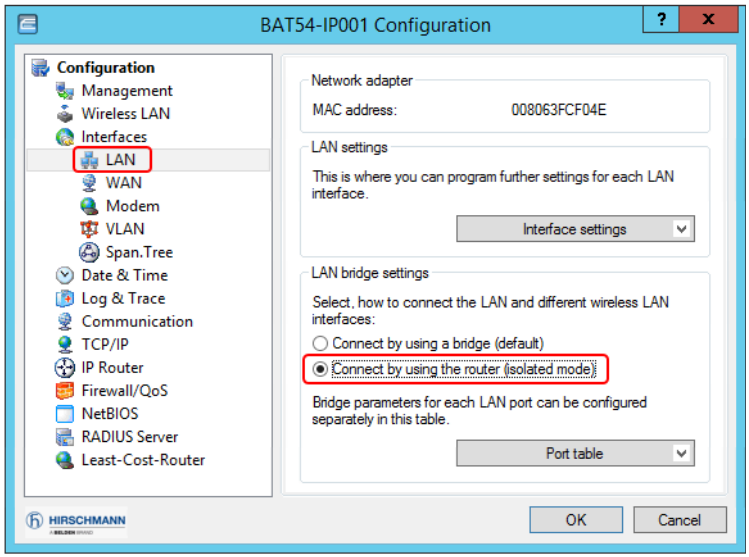

Figure 185. Setting the LAN bridge to router to enable the firewall to be used

Create WLAN1 Network Definition

Each wireless access point must have an IP address defined in the wireless network as a gateway to the Remote Desktop Session Host server.

1. Select **Configuration > TCP/IP > General** and click **IP Networks** in **Own addresses** to create a network.

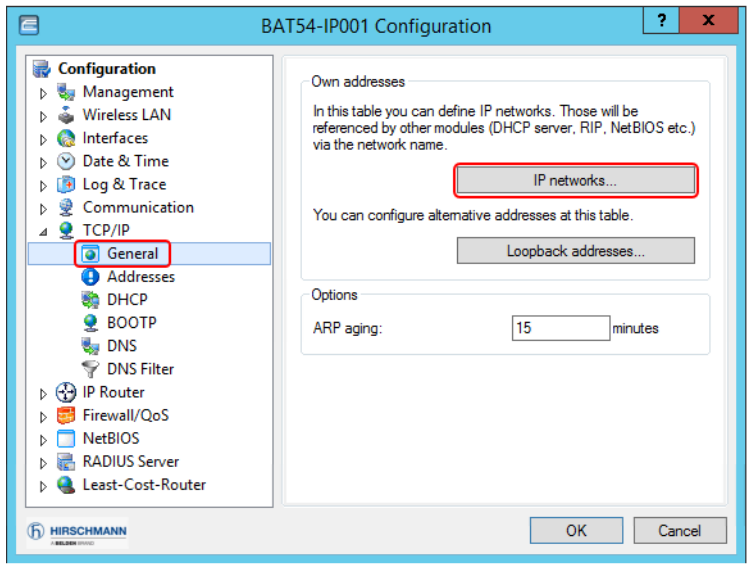

Figure 186. Accessing the IP networks interface

2. Click **Add** to add a new network.

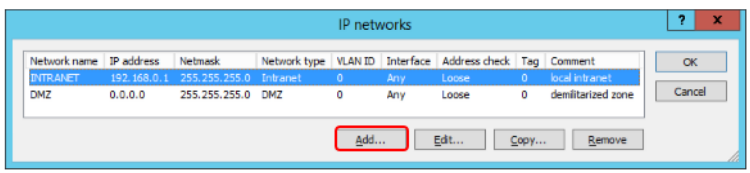

Figure 187. Adding a new network

3. Enter a name and IP address for the network and click **OK**.

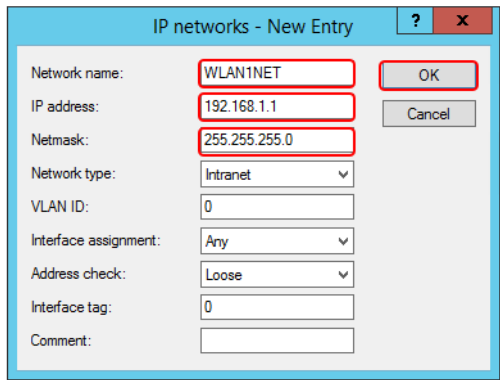

Figure 188. Defining the new network

4. The details of the network will be displayed in the **IP Networks** dialog. Click **OK**.

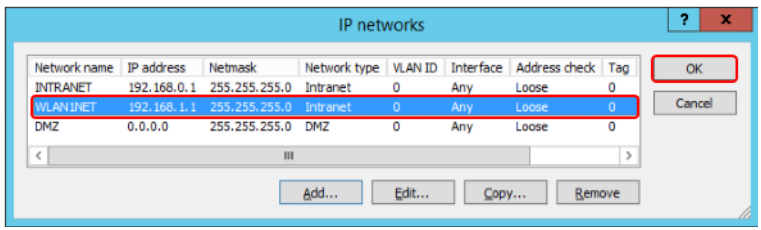

Figure 189. IP networks with newly added network

Creating DHCP Network

After creating the IP network, the DHCP service on the network can be defined.

1. Select **Configuration > TCP/IP > DHCP** and click **DHCP networks**.

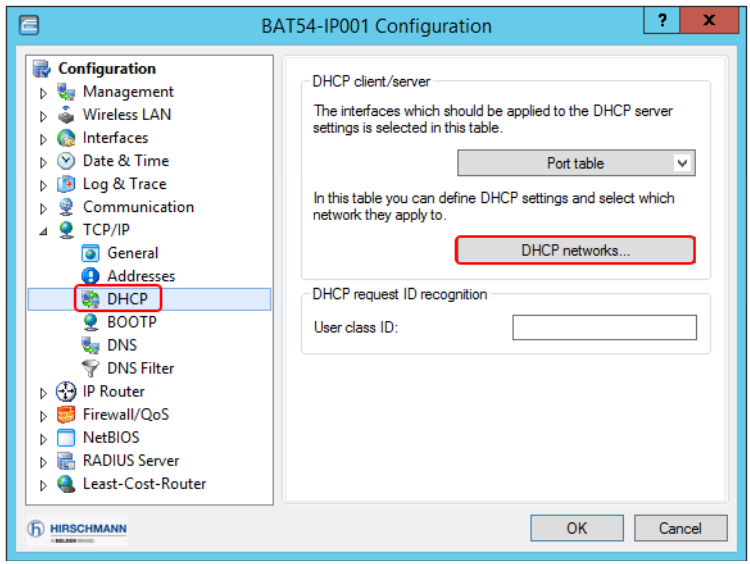

Figure 190. Accessing the DHCP networks interface

2. Click **Add** to create a new DHCP definition.

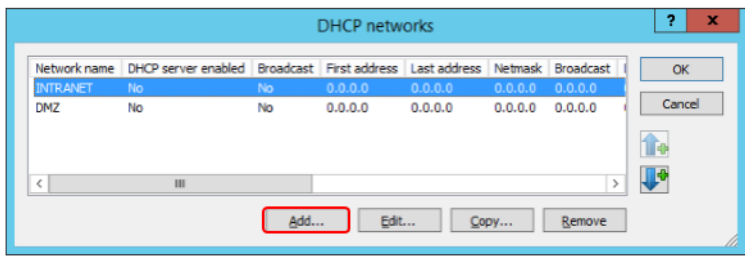

Figure 191. Adding a new DHCP definition

3. In **Network name**, select the IP network. Enter the IP address range, the broadcast and default gateway values. Click **OK**.

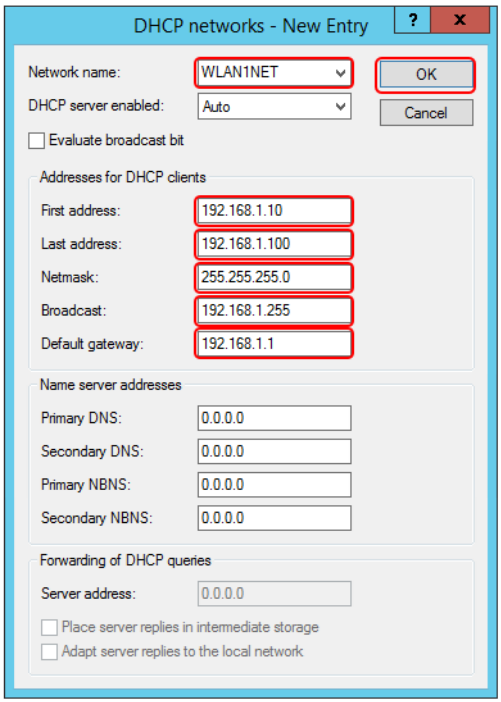

Figure 192. Defining the DHCP configuration

The address range must be within the subnet range and must exclude the IP address of the gateway. The gateway is the IP address of the defined network.

Creating Firewall Service Object for RDP

The firewall service object that defines the RDP service may not be defined in the access point.

1. Select **Configuration > Firewall/QoS > Rules** and click **Service objects**.

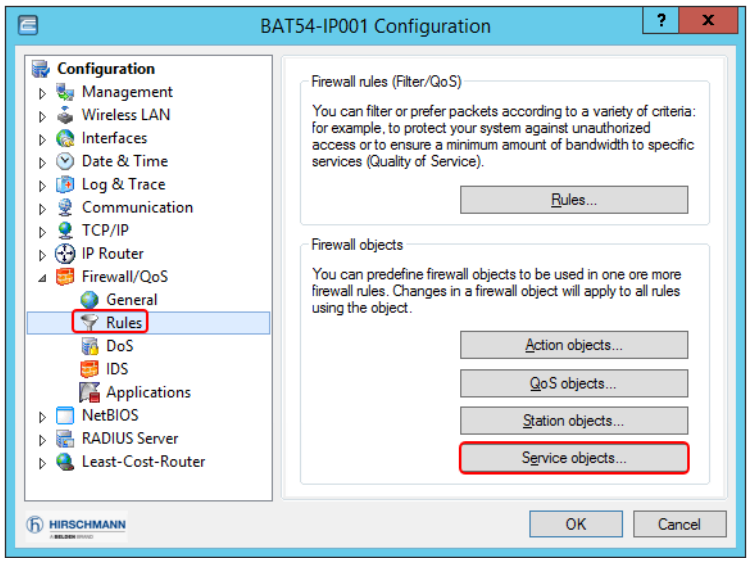

Figure 193. Accessing the firewall Service objects

2. Click **Yes** in the **Default objects missing!** window. In the list, the RDP object that is present is required for Remote Desktop Session Host server access. If the RDP object is not present, a new object that allows TCP communication on port 3389 needs to be created.

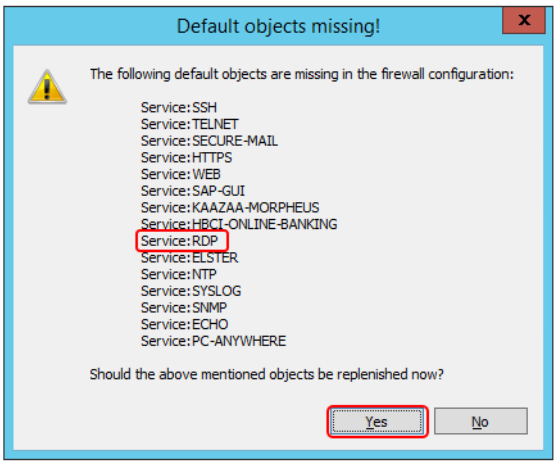

Figure 194. Adding in predefined service object definitions

3. Click **Yes** to correct any incorrect firewall definitions.

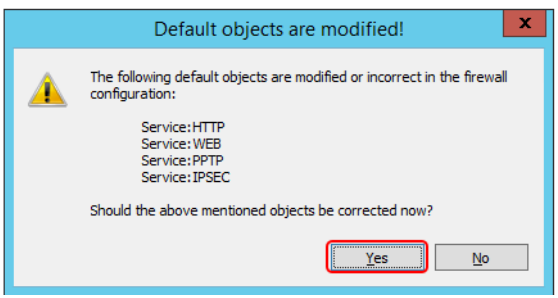

Figure 195. Correcting incorrect firewall definitions

4. Verify that RDP definition appears in the list and click **OK**.

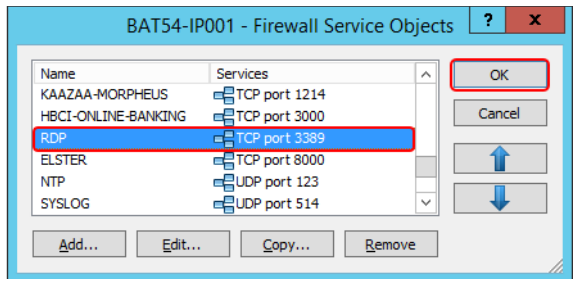

Figure 196. RDP definition required for setting up firewall

Setting up the Firewall

In the example in this user guide, only the remote desktop session is to be allowed access to the Remote Desktop Session Host server. This definition is setup in the firewall rules configuration.

Select **Configuration > Firewall/QoS > Rules** and click **Rules** in **Firewall rules (Filter/QoS)** to configure the firewall rules.

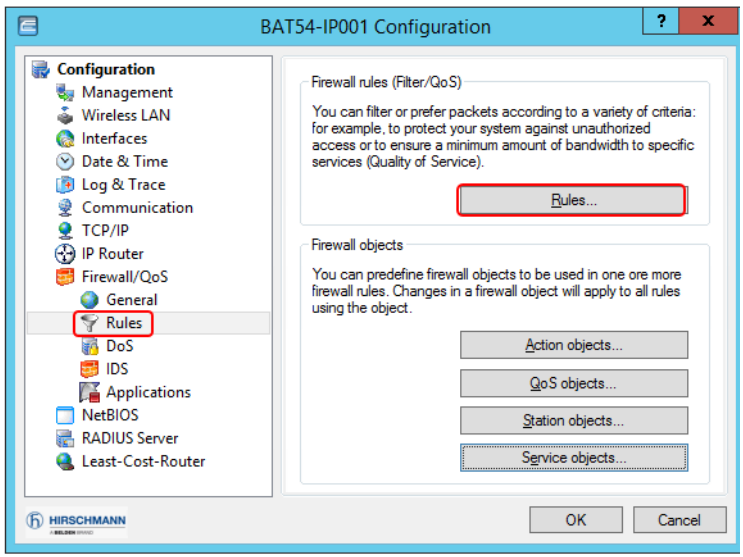

Figure 197. Accessing the firewall rules definition

Remove the existing firewall definition and add the definitions (see Figure 198). Click **OK**.

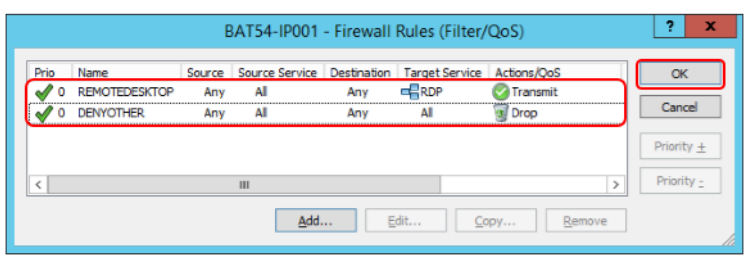

Figure 198. Required firewall definition

The first entry allows RDP traffic and the second ensures that all other traffic is dropped.

Applying Configuration Changes

After completing the configuration, click **OK** in the **BAT54-IP001 Configuration** dialog to update the configuration information to the access point.

Adding Access Points to RADIUS

The access point must be defined in the RADIUS server configuration for the RADIUS server to communicate with the access point. Execute the following steps to add access points to RADIUS:

1. Start the **Server Manager** and select NAP. Right-click the RADIUS Server and select Network Policy Server.

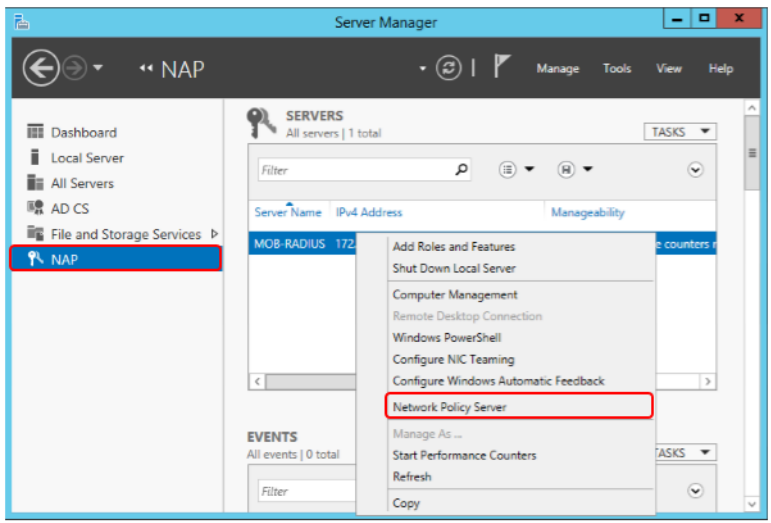

Figure 199. Accessing the Network Policy Server configuration interface

2. Right-click RADIUS Clients and click **New**.

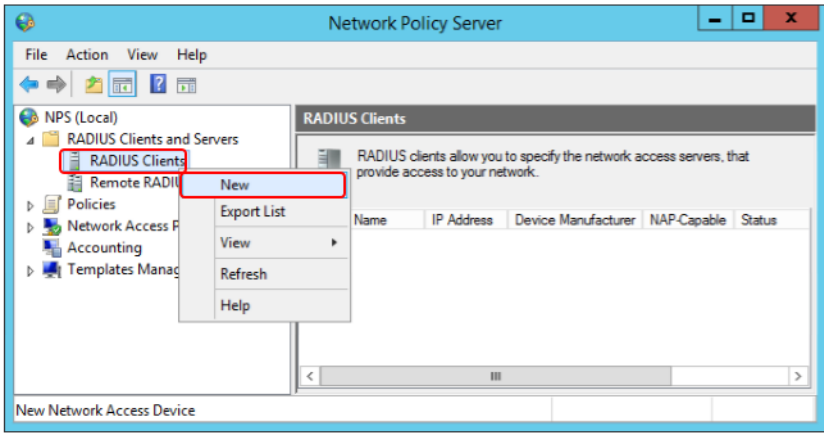

Figure 200. Adding a new client to the RADIUS configuration

3. In **Friendly name**, enter a name for the device. Enter the IP address and enter the Shared secret that was used while setting the RADIUS server in the access point. Click **OK**.

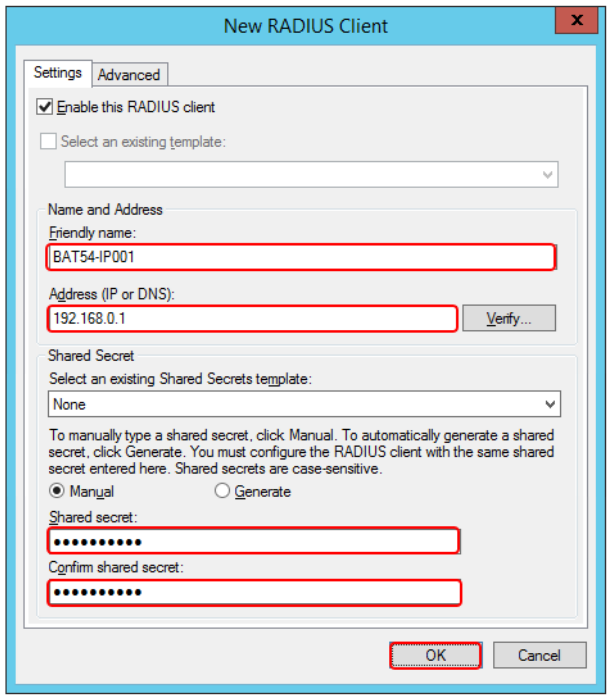

Figure 201. Adding the access point to the RADIUS server as a client

Section 11 Remote Desktop Session Host Server Routing

Each Remote Desktop Session Host Server must be setup with a route that defines the gateway IP address that is responsible for forwarding traffic to the correct destination. With multiple wireless access points in the network, this would require one route to be setup for each access point. The route command has an option for making the definition persistent when restarting the computer.

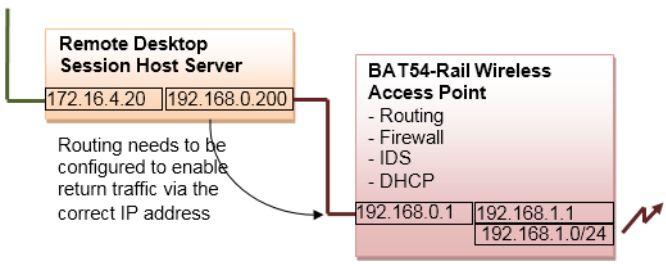

Figure 202. Routing between the Remote Desktop Session Host server and the wireless networks

To create the required routing for the configuration in Figure 202, execute the following windows command in each terminal server:

route-p add 192.168.1.0 mask 255.255.255.0 192.168.0.1

route-p add 192.168.2.0 mask 255.255.255.0 192.168.0.2

The command needs to be executed using the administrative account. The *-p* option makes the route persistent, which will survive a restart of the Remote Desktop Session Host server.

Section 12 Certificates for Mobile Devices

To enable the mobile device to connect to the access point, the certificate for the device must be exported, sent to the device through an email and installed. Take precautions when using emails to deliver certificates. The email must not remain accessible after delivering the certificate because the certificate can be installed on other devices.

Transferring the Certificate to the iPad®

The initial configuration of the iPad® must be done and an email account must be setup for the initial transfer of the certificate.

Execute the following steps to transfer the certificate to an iPad®.

1. The certificate is typically transferred to the iPad® through email. Send the certificate to the email account that is setup on the iPad®. Then touch the attached file.

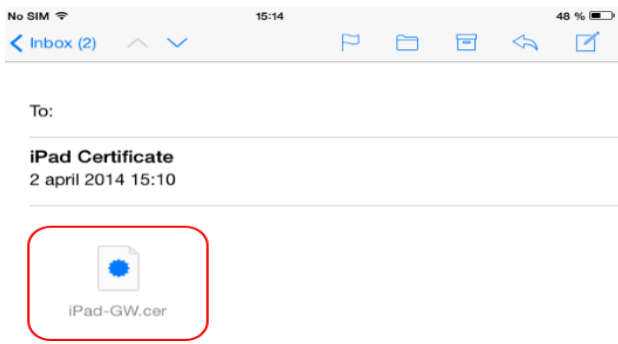

Figure 203. Email sent to iPad® with required certificate

2. In the example, a self-signed authority is used, that will show up as **Not Trusted**. Click **Install**.

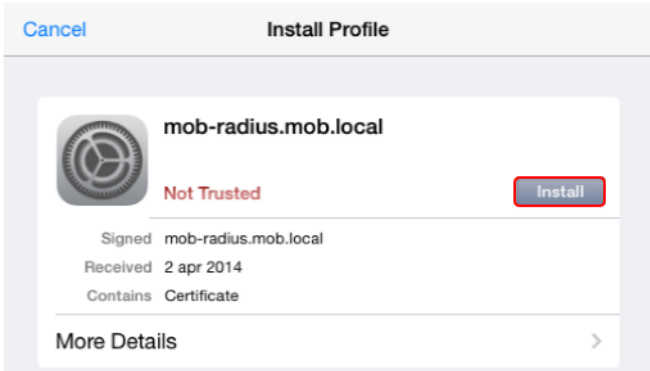

Figure 204. Installing the new certificate

3. Click **Install Now** in the **Unverified Profile** dialog.

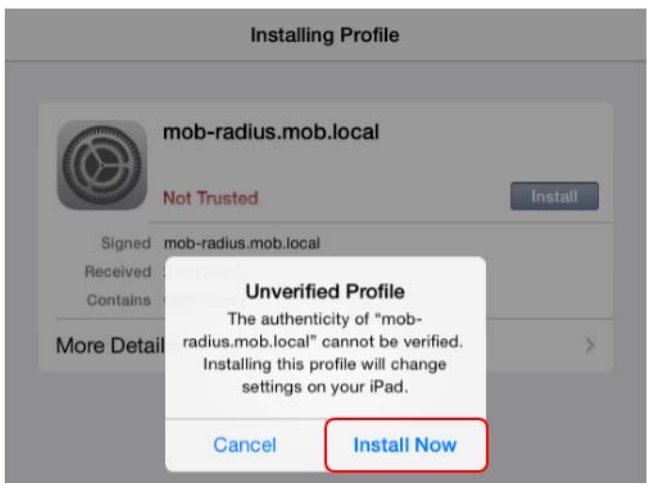

Figure 205. Installing the new profile

4. Click **Done** in the **Profile Installed** dialog.

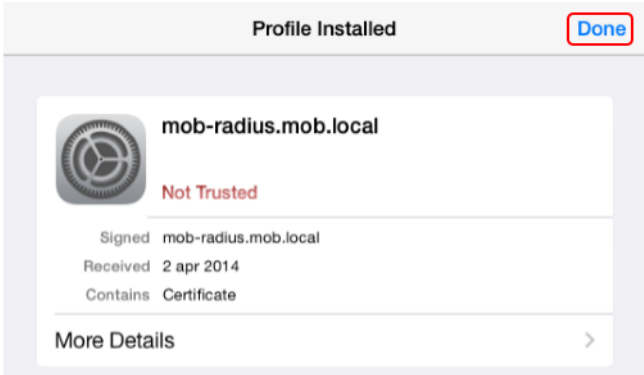

Figure 206. Completed profile installation

5. To view the current list of profiles, enter the settings app in the iPad®, and select **Settings > General** profile.

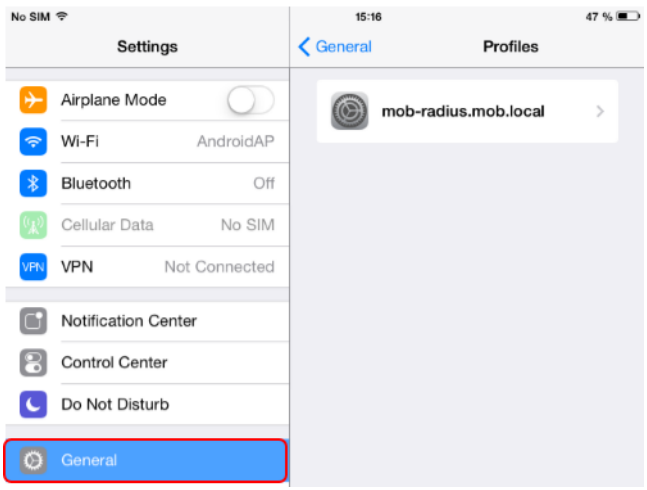

Figure 207. Installed profiles in iPad®

6. Select the wireless network from the list of available wireless networks.

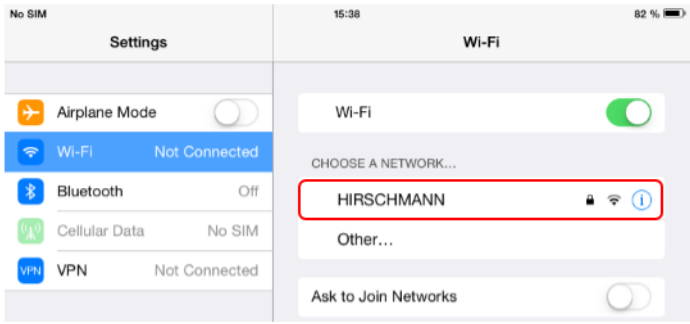

Figure 208. Selecting the wireless network

7. Enter the windows user name and password in **Username** and **Password** respectively and click **Join**.

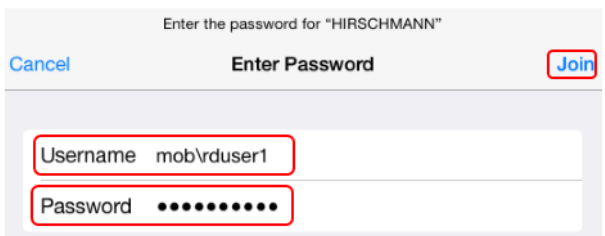

Figure 209. Entering Windows domain credentials to establish the wireless connection

8. Click **Accept** for the certificate request.

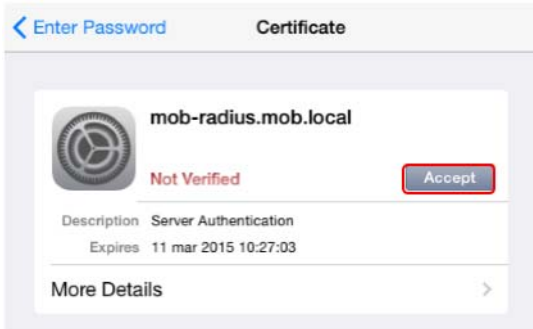

Figure 210. Accepting the certificate

9. After establishing the connection, a check mark and a change in color will indicate that the wireless network connection is established.

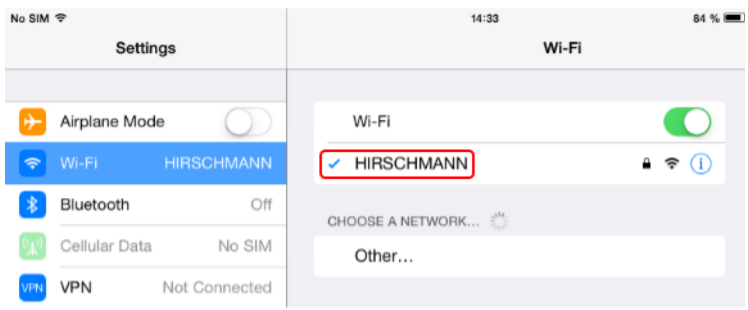

Figure 211. Established wireless network connection

Section 13 Remote Connection to 800xA

Remote connection to the 800xA system is through a remote desktop session. A third party application is required because the iPad® does not have a remote desktop client.

Installing the iPad® remote desktop application

Execute the following steps:

1. Start the iPad® and click icon (see Figure 212) to access the app store.

Figure 212. iPad® App Store icon

2. Search for and purchase **Pocket Cloud Pro.** Figure 213 shows a Pocket Cloud Pro app icon.

Figure 213. Pocket Cloud Pro app icon

Connecting 800xA Remote Desktop Session Host Server

Execute the following steps:

1. Start the Pocket Cloud Pro app and click **Advanced users**.

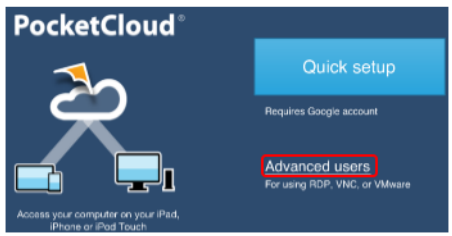

Figure 214. Creating a remote desktop session via the Advanced users option

2. Click **No** at the request to provide anonymous usage statistics.

Figure 215. Anonymous usage statistics request

3. Click the **+** icon and click **Manual Connection** to create a new connection.

Figure 216. Creating a new connection

4. Click **RDP** for the connection type.

Figure 217. Creating a new RDP connection

5. Enter a name for the Remote Desktop Session Host Server, the IP address, the username, and domain. The password should not be saved in the configuration of the session. Click **Save**.

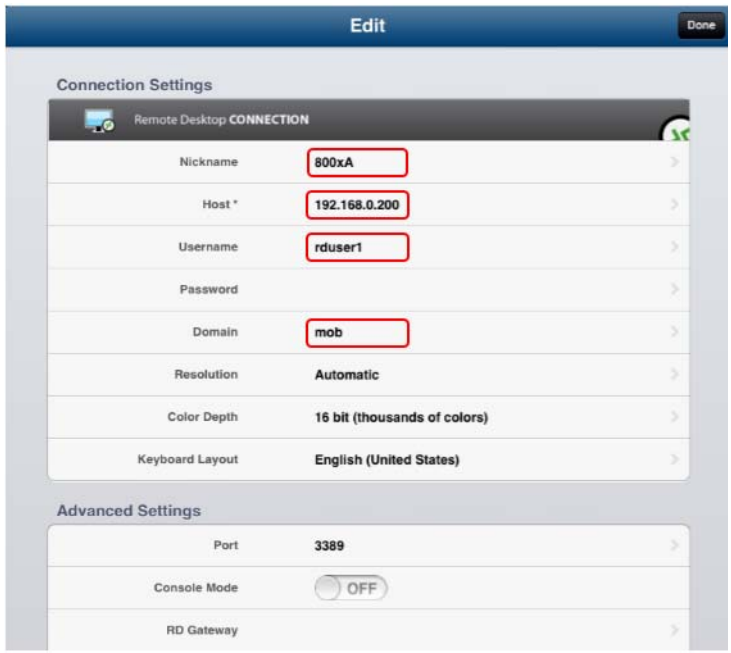

Figure 218. Providing the parameters for establishing a Remote Desktop Session Host server session

6. To establish the connection, select the session and click **Connect**.

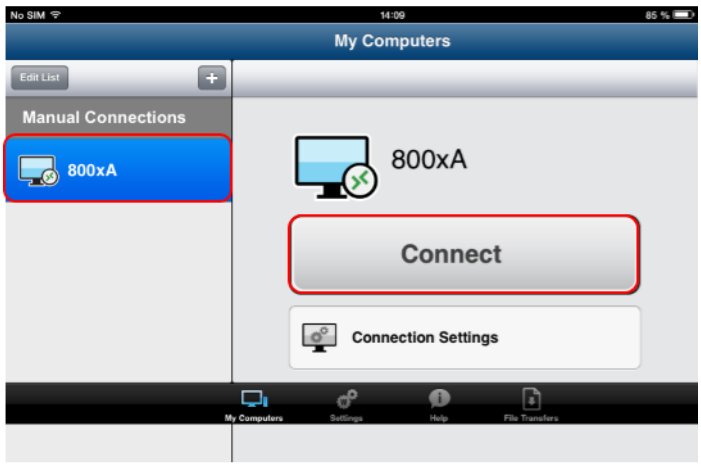

Figure 219. Initiating a remote connection

7. The remote connection must display a full screen 800xA Operator Workplace.

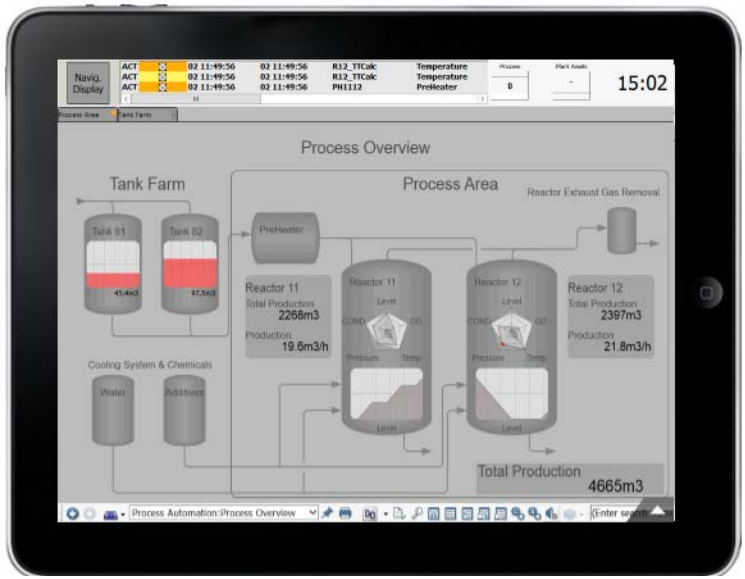

Figure 220. 800xA Workplace via an iPad®

Section 14 Lock iPad®

To prevent unauthorized usage of the iPad®, the in-built functionality of the iPad® to restrict usage must be enabled.

Consider the following to lock an iPad®:

- Restrictions are accessed through the **Settings > General > Restrictions**. By default, the restrictions are turned off.

Figure 221. Accessing the Restrictions functionality of the iPad®

- By default, the restrictions are set to **Allow**. To enable the restrictions, click **Enable Restrictions**.

Figure 222. Enabling iPad® restrictions

- To control future access to the restrictions options, the iPad® will request for a 4 digit passcode be set. The passcode information should be restricted to administrator of the network.

Enter a 4 digit passcode. A confirmation of the passcode will be requested.

Figure 223. Entering a passcode to restrict future access to the restrictions functionality

- The list in **Allows** should be changed to **Off**.

Figure 224. Disallowing iPad® functionalities

- In addition to the controlling of apps, the allowed content should be set to as shown in Figure 225.

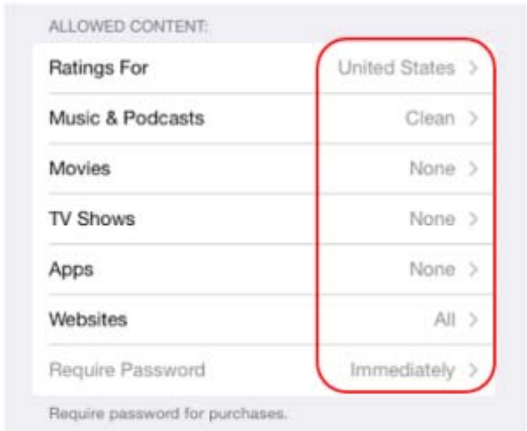

Figure 225. Restricting Allowed Content

- Changing of accounts should be disabled, and the Game Center options should also be set to **OFF**.

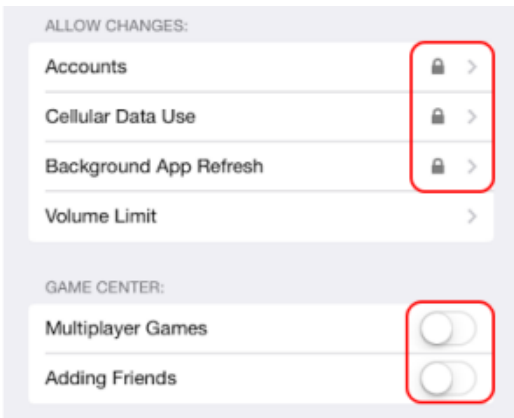

Figure 226. Restricting changes of iPad® accounts and access to the Games Center

Index

Contact us

www.abb.com/800xA
www.abb.com/controlsystems

2PAA110154-600

Power and productivity
for a better world™