6UCSCG0008-29A
February 2013

Configuration Guide

Installing and Configuring a NetVanta UC Server Version 5.3 Business Continuity Solution

This configuration guide provides instructions for installing and configuring a NetVanta Unified Communications (UC) Server version 5.3 Business Continuity solution. It describes the function of business continuity, the limitations of a business continuity system during failover, and provides installation and configuration instructions for business continuity solutions. Additionally, this guide provides special considerations for NetVanta Enterprise Communications Server (ECS), and instructions for recovering from an extended failure of the primary server.

This guide consists of the following sections:

Overview

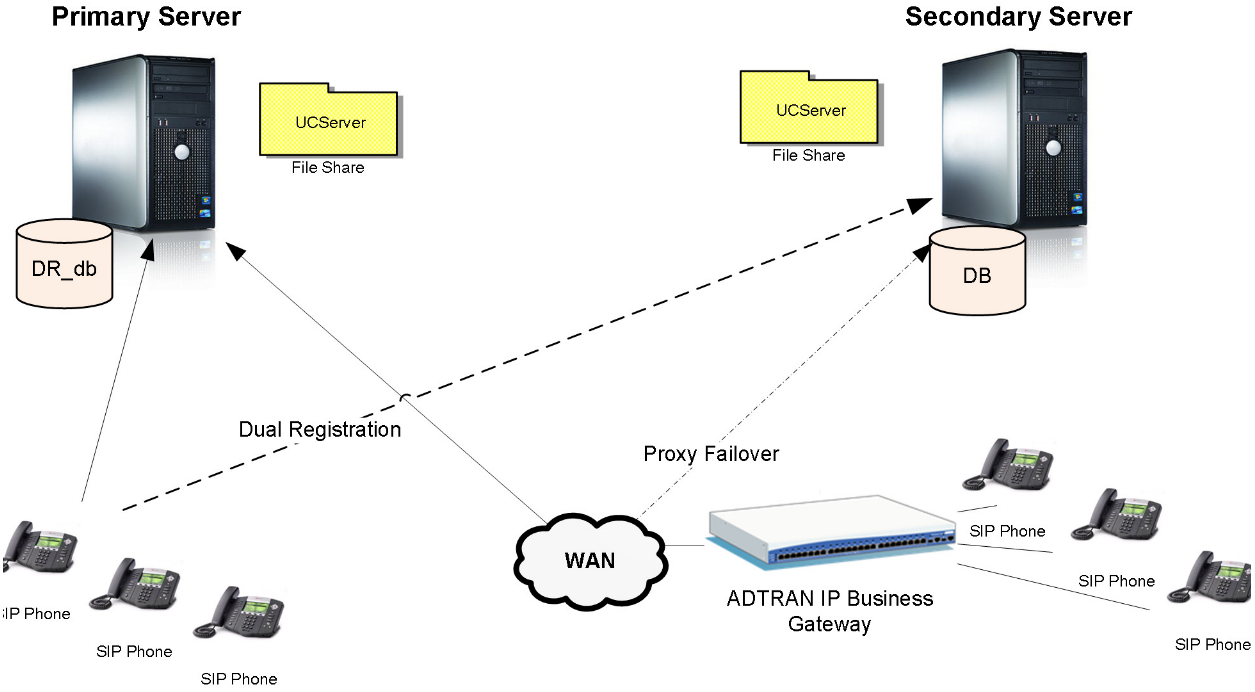
The ADTRAN NetVanta UC Server Business Continuity solution is implemented using two servers: the primary server and the secondary server.

The solution provides resiliency in the event of a permanent network, hardware, or software failure of the primary NetVanta UC Server. The secondary server will provide core UC features and capabilities until the primary server is restored to operation. The secondary NetVanta UC Server is not intended to be used permanently; when a failure occurs with the primary NetVanta UC Server, the secondary NetVanta UC Server will temporarily provide services while the issues with the primary NetVanta UC Server are being resolved.

Business continuity requires a solutions approach, whereby all SIP endpoints, including phones, gateways, and external private branch exchanges (PBXs) must be configured to support a primary and failover SIP connection to the primary and secondary NetVanta UC Servers, respectively. In some cases the SIP endpoints will register with both the primary and secondary servers. In other cases where the phones are being managed through a survivable gateway, or register/connect to an external PBX, the gateway will manage the transition between primary and secondary NetVanta UC Servers.

> NOTE *This failover solution is typically installed by ADTRAN ACES. Please ensure that you have the required knowledge and training before attempting this without assistance. The solution requires additional software to be installed and configured on both the primary and secondary servers.*

The following diagram provides an example of a typical business continuity deployment:



Business Continuity Service

Every instance of NetVanta UC Server contains a component called the Business Continuity Sync Service (Business Continuity Service) which is responsible for synchronizing the state of the primary and secondary servers. This service is only active on the server if your product license enables the Business Continuity feature and NetVanta UC Server is configured as either a primary or secondary server.

Synchronization is controlled by a number of parameters which are described in a later section (*Appendix D - Handling an Extended Failure of the Primary Server on page 66*). The Business Continuity Sync Service is enabled by configuring the business continuity role of a NetVanta UC Server as either a primary or secondary server within a business continuity solution. This configuration is described in *Installing a New NetVanta UC Server version 5.3 Business Continuity Solution on page 8*.

Operational Algorithm

NOTE *The bolded parameters mentioned in this section are configured during business continuity configuration. Please refer to Step 6: Configure Business Continuity on the Secondary Server on page 20 and Step 7: Configure Business Continuity on the Primary Server on page 25 for details on the parameters mentioned in this section.*

The Business Continuity Service on the primary and secondary servers activates at intervals determined by the **Synchronization service polling interval** parameter configured on each server during business continuity configuration. The services on the primary and secondary servers operate asynchronously, meaning the services on each of the servers can have different Synchronization service polling interval intervals and can activate independently. When the Business Continuity Service is activated at the Synchronization service polling interval, the service will perform the synchronization actions described below.

When the Business Continuity Service activates on the primary server, it will determine whether there has been any message activity on the secondary server. If there has been message activity on the secondary server, the service on the primary server will perform the following actions:

- The service will send an email to the configured **Email recipient** (configured in the **Business Continuity Server Configuration** menu) address if an email has not been sent within the interval specified by the **Time between emails** setting. For more information on the emails sent, refer to *Email Notifications on page 4*.
- The service will synchronize the local message store voicemails from the secondary server to the primary server if a synchronization has not occurred within the interval specified by the **Minimum time between voicemail synchronizations**.

When the Business Continuity Service activates on the secondary server, the service will perform the following actions:

- At the **Daily full synchronization time**, the service will perform a full backup of the primary server to the secondary server.
- If a full backup is not performed (i.e., it is not the **Daily full synchronization time**), and if a synchronization has not occurred within the interval specified by the **Minimum time between voicemail synchronizations**, the service will synchronize the local message store voicemails from the primary server to the secondary server. Also, if a full backup is not performed, the service will synchronize the SIP registration records from the primary server to the secondary server.

Email Notifications

The Business Continuity Service sends email notifications when the following critical events occur:

- An email notification is sent to the **Email recipient** specified on the primary server if voicemail activity from the Local Message Store, Exchange server, or Internet Message Protocol (IMAP) server is detected on the secondary server. If the voice message was stored in Local Message Store, the mail will include the user names of people who had activity on the secondary server.
- An email notification is sent to the **Email recipient** specified on either the primary or secondary server if any serious errors are detected. The email recipient to whom the email is sent depends on where the error occurred (for example, if the secondary server is unable to access the MessageAction database table on the primary server, a message will be sent to the **Email recipient** specified on the secondary server). Serious error checking is performed every time the Business Continuity Service activates. Serious errors include:
  - The MessageAction database table that tracks voice message activity on the other server cannot be accessed.
  - The synchronization process returns an error on the secondary server and error logs that indicate the code has an internal problem.

The frequency with which emails are sent is based on the **Time between emails** value. Only one email is sent for the **Time between emails** time irrespective of the amount of voicemail activity or serious error detections. The email will contain the events of the last activity within the **Time between emails** period.

Example Voicemail Activity Email Content

When voicemail activity is detected on the secondary server, an email notification is sent to the **Email recipient** specified on the primary server. An example of the notification is provided below.

> The NetVanta UC Server has encountered voicemail activity on the secondary server. In most situations, this condition will automatically correct itself. If you are performing any kind of server or network related maintenance, or if you are experiencing any network outages or issues, this may be a temporary consequence of the maintenance. If these errors continue after you have completed your maintenance tasks, or network problems have been resolved, further investigation is recommended.
>
> Below are the users who have had voicemail activity on their account in the secondary server:
>
> *User a*
>
> *User b*

The user information paragraph only applies when the voicemail is stored in Local Message Store.

Example Serious Error Email Content

When serious errors are detected, an email notification is generated. An example is provided below.

> Serious errors have been detected on your system. Please check your system as soon as possible.
>
> The NetVanta UC Server has encountered a problem. Your system is most likely operating in DR mode, with limited functionality. If you are performing any kind of server or network related maintenance, or if you are experiencing any network outages or issues, this may be a temporary consequence of the maintenance. If these errors continue after you have completed your maintenance tasks, or network problems have been resolved, further investigation is recommended.
>
> If this email is older than 60 minutes, and you have not received another email since, normal operation might have been restored.

Types of Failures

In general, there are two types of failure modes: transient server failure and complete server failure.

A transient failure may result in a more complicated situation. If, for example, there is a routing problem where some users are routed to the primary and others to the secondary server, the users routed to the secondary server will experience feature limitations whereas those routed to the primary server will not. It is important that immediate action be taken to restore users on the primary server when an email notification is received indicating that there is activity on the secondary server.

In complete failure mode (for example, hard drive failure on the primary server), the primary server will be down for an extended period of time. During that time, the secondary server will provide all users of the system with the capabilities described in *Supported Features on page 6*. Similarly, the features described in *Exceptions on page 6* will not be provided.

Hardware and Software Requirements and Limitations

The primary and secondary servers must be running identical software versions with identical build numbers and must be installed and configured using the instructions provided in this document.

Some host computers may require additional software be installed for the proper operation of the business continuity. For more information on prerequisite software, refer to *Prerequisites on page 7*.

Peripheral devices such as telephones and gateways must be configured so that, if service is not provided by the primary server, they will use the secondary server instead:

- Telephones must either be dual registered or use a SIP proxy which is aware of both servers and sends SIP packets to one or the other depending on which is operational.
- SIP gateways must have routing entries so that if they do not receive a response from one server they will use the other server. The gateways must also accept outgoing calls from either server.

Business continuity is supported on NetVanta Enterprise Communication Server (ECS), NetVanta UC Server, and NetVanta Business Communications Server (BCS). In NetVanta BCS systems, a business continuity solution will only provide failover for the NetVanta UC Server capabilities. Because the PBX features are provided by the NetVanta 7100, failover for all PBX capabilities must be provided by the NetVanta 7100. Similarly, for a NetVanta UCS system, business continuity provides failover for the voicemail functionality; however, failover for the external PBX must be provided by the PBX or gateway.

Only Polycom phones are supported for business continuity solutions.

Federated NetVanta UC Servers (trusted UC servers) are not supported in business continuity solutions.

Supported Features and Exceptions

The following sections provide information on the supported features and exceptions of the current business continuity release.

Supported Features

All features of a standard ECS system operate normally when the primary server is operational. During failover, when service is being provided by the secondary server, only the following features are supported:

- Origination and termination of calls
- Receipt of new voicemails
- Basic call features
  - Call transfers (Assisted and Blind)
  - Call park
  - Hold (with music on hold (MOH))
- If Exchange or IMAP integration is used, because the server maintains synchronization, users will see no impact.
- Telephone User Interface (TUI)

> NOTE *Some phone features and types of information synchronization are not supported during failover. For more information, refer to the Exceptions section below.*

Exceptions

The following NetVanta UC Server services and capabilities are not supported or have limited functionality during failover:

- ADTRAN IP 706 and IP 712 phones will not operate because they do not support dual registration.
- Administrative changes are not supported during failover. This includes phone configuration and all NetVanta UC Client or GUI-based changes.
- The following clients, GUIs, and applications are not supported: ucCompanion, NetVanta UC Client, Live Attendant, and NetVanta Unified Communications Notification Server (UCNS).
- Click-to-Dial and Print-to-Fax features are not supported.
- Message waiting indicators (MWI) are not supported to prevent issues with phones that are dual registered.

- Busy Lamp Fields (BLFs) are not supported.
- Local message store messages received since the last synchronization may not be accessible to users.
- Local message store messages deleted since the last synchronization will be displayed again to users.
- External databases that reside on the primary server are not automatically updated on the secondary server. Services that rely on databases may not function when the server fails.
- Modifications made directly on the secondary server to the existing users or identities may not be overwritten by the primary server's configuration parameter. However, any users that are deleted from the secondary server will be recreated with the correct parameters from the primary server if the user still exists on the primary server.
- Phones that are rebooted during the failover will take longer to become operational since they will first try to download their configuration from the primary server. After timing out they will operate with the previously downloaded configuration.
- Users may experience a delay when initiating calls.

Prerequisites

This section describes prerequisite software that is required for the NetVanta UC Business Continuity services.

Windows Server Resource Kit

If the host computer's operating system is Windows 2003 Server you must install the Windows Server 2003 Resource Kit Tools. The Resource Kit includes additional utilities, such as Robocopy.exe and bcp.exe, which are required for the business continuity software.

The Windows Server 2003 Resource Kit Tools can be obtained from the following link:

http://www.microsoft.com/downloads/details.aspx?FamilyID=9D467A69-57FF-4AE7-96EE-B18C4790CFFD&displaylang=en

SQL Server Management Studio Express

Although other SQL management tools can be used, it is recommended that SQL Server Management Studio Express (2005 or 2008) be installed. This application can be used to configure the database that is used to coordinate synchronization states between the primary and secondary NetVanta UC Servers.

The application can be obtained from the following links:

SQL Server Management Studio Express 2005
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=c243a5ae-4bd1-4e3d-94b8-5a0f62bf7796

or

SQL Server Management Studio Express 2008
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=08e52ac2-1d62-45f6-9a4a-4b76a8564a2b

Installing a New NetVanta UC Server version 5.3 Business Continuity Solution

The following section describes the steps required to install and configure a business continuity solution when no previous versions of NetVanta UC Server has been installed.

If a previous version of NetVanta UC Server has been installed (including disaster recovery software), the steps are slightly different. Installation in these scenarios is described later in this document.

In this scenario, a NetVanta UC Server 5.3 Business Continuity solution is being installed where no previous NetVanta UC Server system existed. Before beginning, acquire two separate server computers. One will be used as the primary server while the second will be used as the secondary server.

Use the following procedure to install and configure the systems.

Preparation

Select a domain account that will be used as the NetVanta UC Server service account on both the primary and secondary servers. If Exchange Server will be used, this account must have special Exchange Server permissions. For more information on configuring the permissions for the service account, refer to *Configuring Microsoft Exchange 2007 and 2010 Permissions for Integration with NetVanta UC Server* available from the ADTRAN Support Community (https://supportforums.adtran.com).

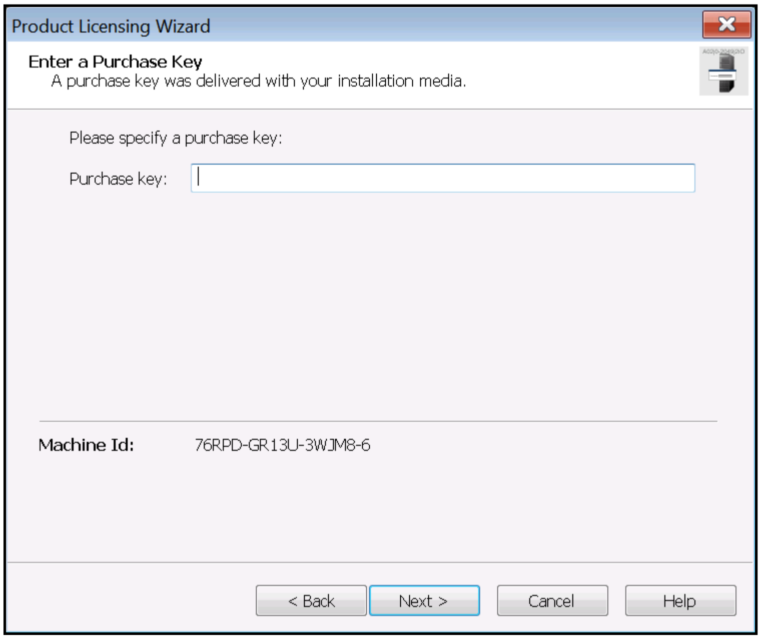
Ensure that the chosen account is a member of the local Administrators group on both systems. You can do this from the **Local users and Groups** section of the **Computer Managemen**t console. The selected account will be called the service account in the rest of this section.

Step 1: Install NetVanta UC Server on the secondary server and Retrieve the Secondary Server Machine ID

This section describes how to install NetVanta UC Server 5.3 on the secondary server and determine the machine identity of the secondary server (used for product licensing).

1. Login to secondary server using the service account.
2. Install NetVanta UC Server version 5.3 on the secondary server. For more information on installing NetVanta UC Server, refer to the *NetVanta Unified Communications Software Installation Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com).
3. In the Windows Start menu, navigate to **Programs > ADTRAN > NetVanta UC Server** > **NetVanta UC Server Configuration Wizard**. The **NetVanta UC Server Configuration Wizard** main menu appears.
4. On the main menu, select **Product Licensing** to open the **Product Licensing Wizard**. The **Product Licensing Wizard** menu appears.
5. Select **Next**. The **Enter a Purchase Key** menu appears.

6. The **Enter a Purchase Key** menu displays the **Machine Id** of the secondary server as shown below. Record the **Machine Id**. It will be used later to request a business continuity license key from ADTRAN.



Product Licensing Wizard

Enter a Purchase Key

A purchase key was delivered with your installation media.

Please specify a purchase key:

Purchase key:

Machine Id: 76RPD-GR13U-3WJM8-6

7. Do not go any further in this wizard at this time. Select **Cancel** and then exit the **NetVanta UC Server Configuration Wizard**.

Step 2: Install NetVanta UC Server on the Primary Server and Begin Configuring the Primary Server

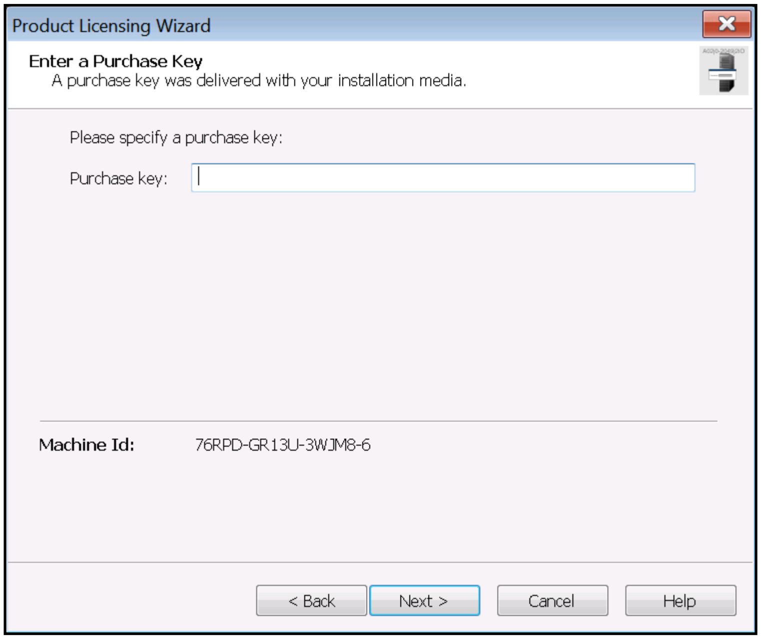
This section describes how to enter the product license key, configure the service account, and temporarily specify the server role as standalone on the primary server.

The business continuity role of the primary server is specified later in the business continuity configuration.

1. Log in to the primary server using the service account.
2. Install the same version of NetVanta UC Server software on the primary server as was previously installed on the secondary server. For more information on installing NetVanta UC Server, refer to the *NetVanta Unified Communications Software Installation Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com).

    The build numbers of the versions of NetVanta UC Server installed on the primary and secondary servers must be identical for server synchronization

3. In the Windows Start menu, navigate to **Programs > ADTRAN > NetVanta UC Server** > **NetVanta UC Server Configuration Wizard**. The **NetVanta UC Server Configuration Wizard** main menu appears.
4. On the main menu, select **Product Licensing** to open the **Product Licensing Wizard**. The **Product Licensing Wizard** main menu appears.
5. Select **Next**. The **Enter a Purchase Key** menu appears.
6. In the **Purchase key** field, enter the purchase key for the NetVanta UC Server software. Also, record the **Machine Id** of the primary server displayed in this menu. It will be used later to request a business continuity license key from ADTRAN. Then, select **Next**. The **Enter a License Key** menu appears.



Product Licensing Wizard

Enter a Purchase Key

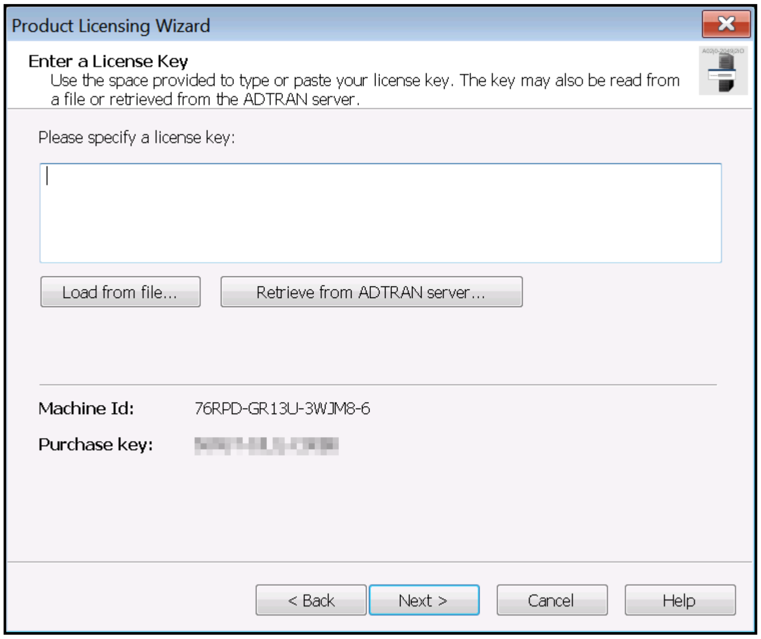
A purchase key was delivered with your installation media.

Please specify a purchase key:

Purchase key:

Machine Id: 76RPD-GR13U-3WJM8-6

7. In the **Enter a License Key** menu, you will enter the business continuity license key; however, you must first request the license key from ADTRAN. To request a license key, use the License Key Request tool available from http://www.adtran.com/uctools. You will be asked for the machine IDs of the primary and secondary servers. Once you have the business continuity license key, enter the license key in the **Please specify a license key** field. Then, select **Next**. The **Summary of License Options** menu appears.



Product Licensing Wizard

Enter a License Key

Use the space provided to type or paste your license key. The key may also be read from a file or retrieved from the ADTRAN server.

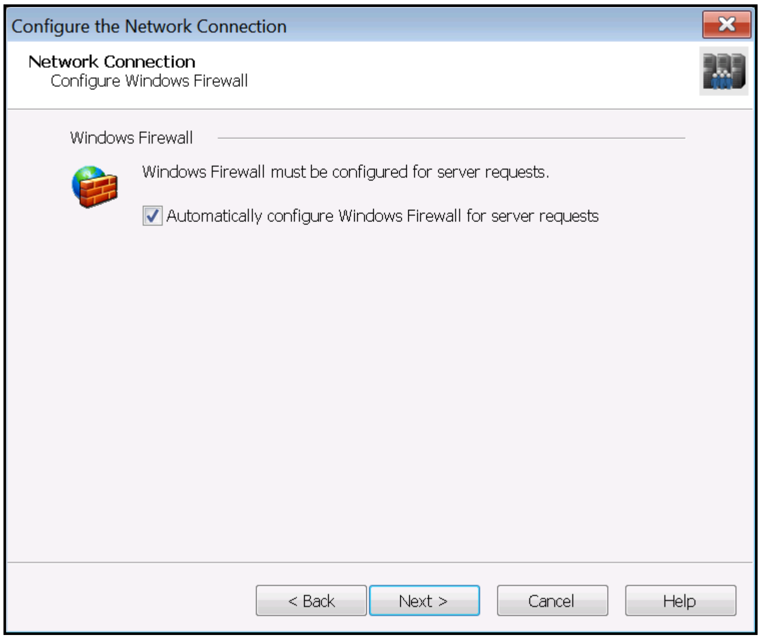
Please specify a license key:

Machine Id: 76RPD-GR13U-3WJM8-6

Purchase key: [redacted]

8. In the **Summary of License Options** menu, review the details of the licensed features. Then, select **Next**.
9. The purchase key and license key will be registered with the ADTRAN server. Select **Next** once these tasks have been completed. Then, select Next again to exit the **Product Licensing Wizard**.
10. In the **NetVanta UC Server Configuration Wizard** main menu, select **Windows Network Integration** to open the **Windows NetWork Integration Wizard**. The **Windows Network Integration Wizard** menu appears.
11. Select **Next**. The **Network Connection** menu appears.

12. In the **Network Connection** menu, ensure that the checkbox next to **Automatically configure Windows Firewall for server requests** is checked. Then, select **Next**. The **Configure the Windows Integration** menu appears.



Configure the Network Connection

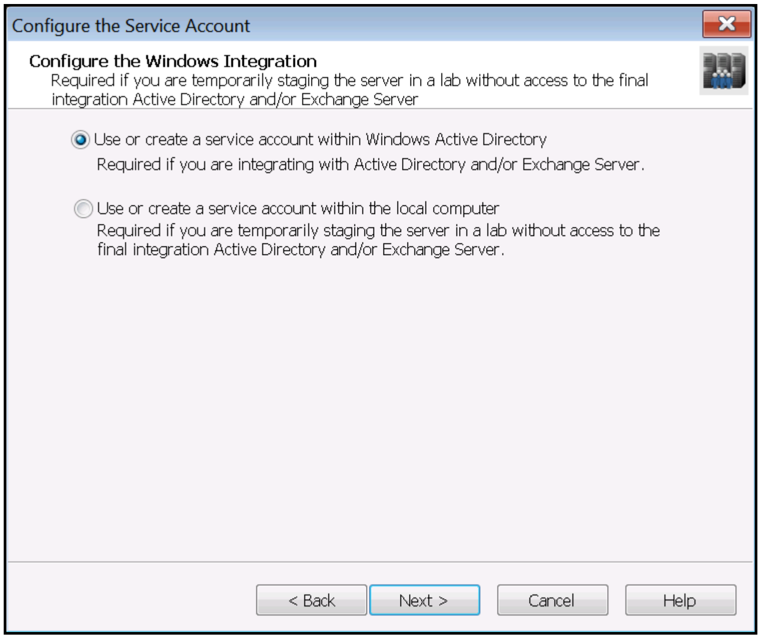
Network Connection
Configure Windows Firewall

Windows Firewall

Windows Firewall must be configured for server requests.

☑ Automatically configure Windows Firewall for server requests

13. In the **Configure the Windows Integration** menu, select the **Use or create a service account within Windows Active Directory** radio button. Then, select **Next**. The **Windows Domain Service Account** menu appears.



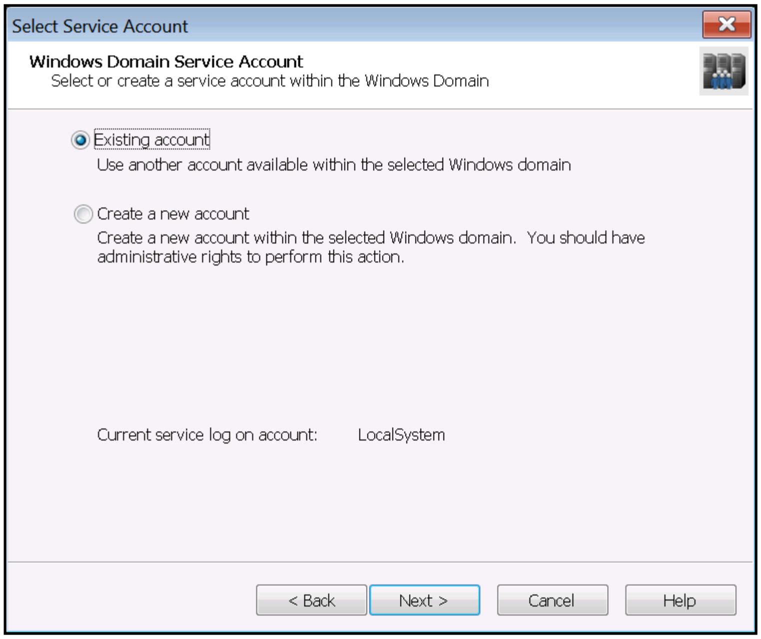
Configure the Service Account

Configure the Windows Integration
Required if you are temporarily staging the server in a lab without access to the final integration Active Directory and/or Exchange Server

● Use or create a service account within Windows Active Directory
Required if you are integrating with Active Directory and/or Exchange Server.

○ Use or create a service account within the local computer
Required if you are temporarily staging the server in a lab without access to the final integration Active Directory and/or Exchange Server.

14. In the **Select Service Account**, select the **Existing account** radio button. Then, select **Next**. The **Service Account Settings** menu appears.



Select Service Account

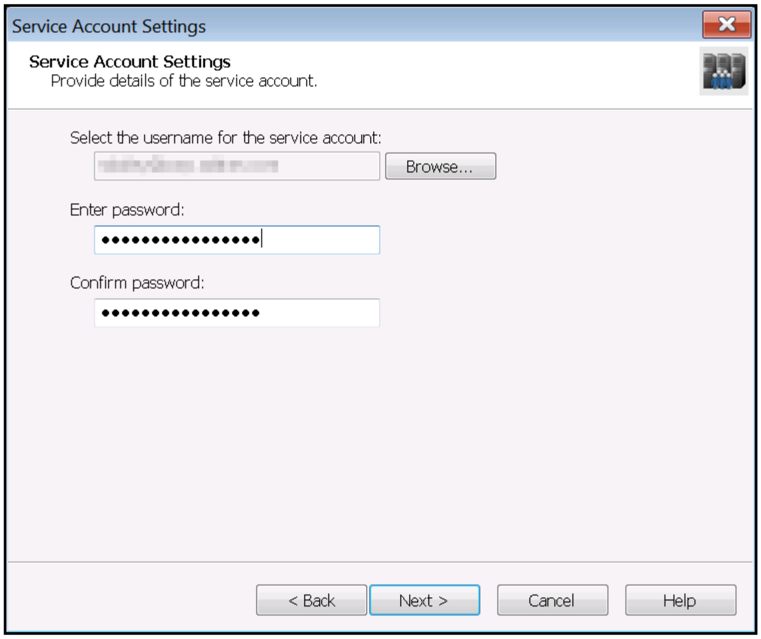
Windows Domain Service Account
Select or create a service account within the Windows Domain

● Existing account
Use another account available within the selected Windows domain

○ Create a new account
Create a new account within the selected Windows domain. You should have administrative rights to perform this action.

Current service log on account: LocalSystem

15. In the **Service Account Settings** menu, select the **Browse** button to browse for the service account you created during *Preparation on page 8*. Once you have chosen the service account, enter the password for the service account in the **Enter password** field, then re-enter the password in the **Confirm password** field. Then, select **Next**.



Service Account Settings

Service Account Settings
Provide details of the service account.

Select the username for the service account:
[redacted]

Enter password:
••••••••••••••••

Confirm password:
••••••••••••••••

16. On the summary page that appears, review the options you selected, then select **Submit**.

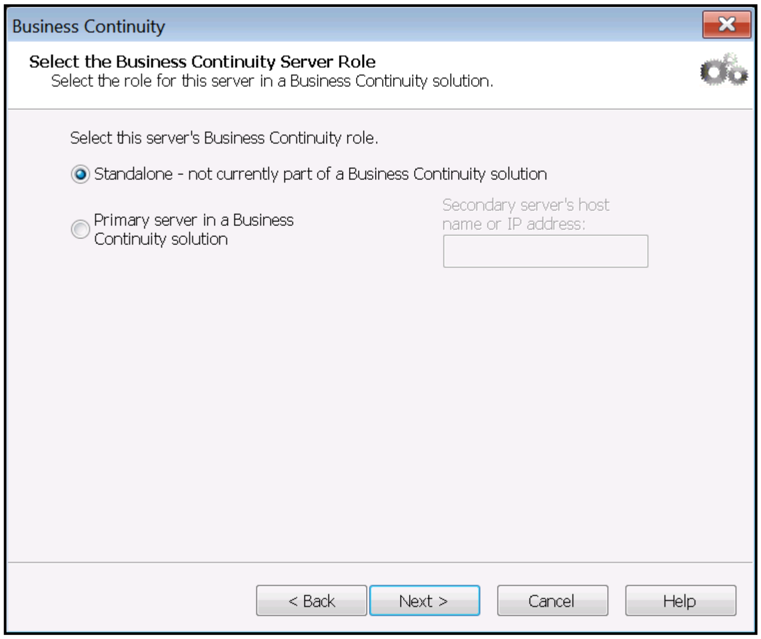
17. The wizard will configure the Windows Firewall and service account. Select **Next** once these tasks have been completed. Then, select **Next** again to exit the **Windows Network Integration Wizard**.

18. Use the **Communication Systems** and **Phone Types** wizards in the **NetVanta UC Server Configuration Wizard** to configure the communication systems and phone types that will be used with NetVanta UC Server. For more information on using the wizards available in the **NetVanta UC Server Configuration Wizard**, refer to the *NetVanta Unified Communications Server Configuration Guide* for your version of NetVanta UC Server available from the ADTRAN Support Community (https://supportforums.adtran.com).

19. Once you are able to access it, select **Business Continuity** in the **NetVanta UC Server Configuration Wizard** main menu to open the **Business Continuity Wizard**. The **Business Continuity Wizard** menu appears.

20. Select **Next**. The **Select the Business Continuity Server Role** menu appears.

21. In the **Select the Business Continuity Server Role** menu, select **Standalone** (because the secondary server has not yet been configured). Then, select **Next**.



Business Continuity

Select the Business Continuity Server Role

Select the role for this server in a Business Continuity solution.

Select this server's Business Continuity role.

● Standalone - not currently part of a Business Continuity solution

○ Primary server in a Business Continuity solution

Secondary server's host name or IP address:

22. On the summary page that appears, review the options you selected, then select **Submit**.

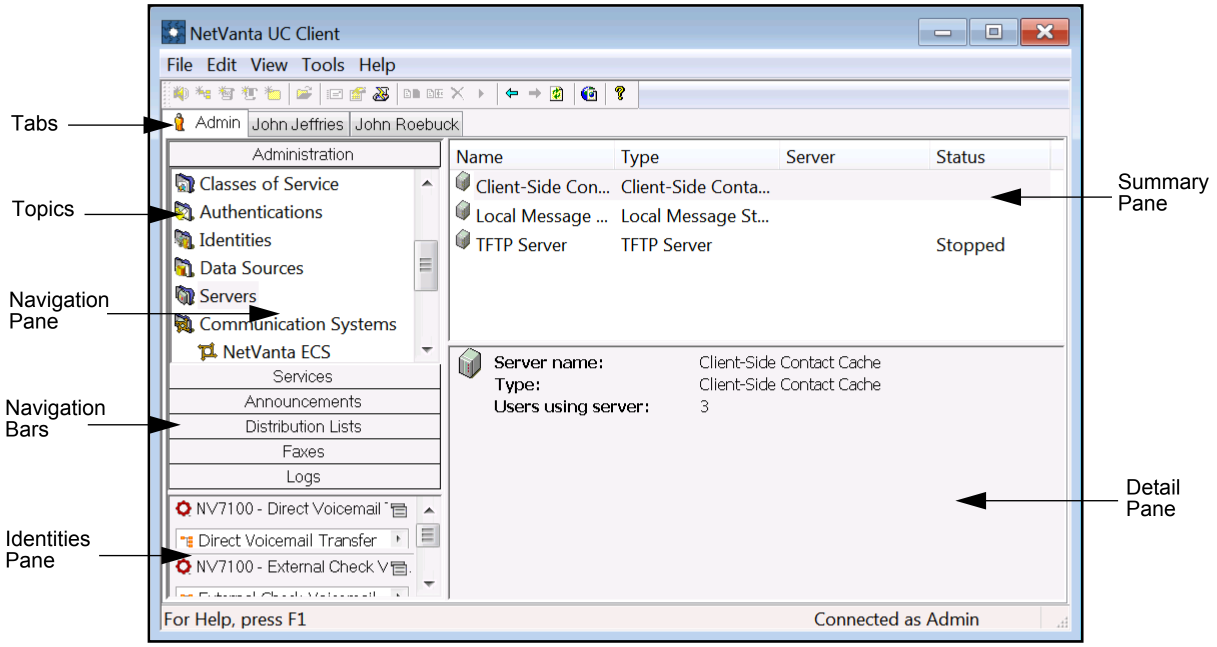
23. The wizard will configure the server's business continuity role. Select **Next** once the task has been completed. Then, select **Next** again to exit the **Business Continuity Wizard**.

24. Continue to use the NetVanta UC Server Configuration Wizard to configure the primary NetVanta UC Server. For more information on using the wizards available in the **NetVanta UC Server Configuration Wizard**, refer to the *NetVanta Unified Communications Server Configuration Guide* for your version of NetVanta UC Server available from the ADTRAN Support Community (https://supportforums.adtran.com).

25. After you have completed all of the wizards available in the **NetVanta UC Server Configuration Wizard**, log in to NetVanta UC Client as an administrator.

26. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.

27. Select the **Servers** topic from the **Administration** navigation pane.



Name	Type	Server	Status
Client-Side Con...	Client-Side Conta...		
Local Message ...	Local Message St...		
TFTP Server	TFTP Server		Stopped

Server name: Client-Side Contact Cache
Type: Client-Side Contact Cache
Users using server: 3

28. In the **Servers** summary pane, right-click each server object, and select **Track message actions** (if it is available).

Step 3: Create a Network Share on the Primary and Secondary Servers for Copying NetVanta UC Server Data

In order for the Business Continuity Service to copy NetVanta UC Server data from one NetVanta UC Server computer to the other during synchronization, the root directory of the NetVanta UC server installation must be shared on the network. Typically, this directory will be **C:\Program Files (x86)\ADTRAN\NetVanta UC Server**. The share must be created on both the primary and secondary servers. This document uses the share name **UCServerSync**.

NOTE *The shares created on the primary and secondary servers are not required to have the same name, because the name of the share is specified during business continuity configuration.*

The NetVanta UC Server service account must have at least **Change** and **Read** permissions for this network share. For more information on sharing a folder and setting user permissions for shared folders, refer to the following Microsoft TechNet article http://technet.microsoft.com/en-us/library/cc770406.aspx.

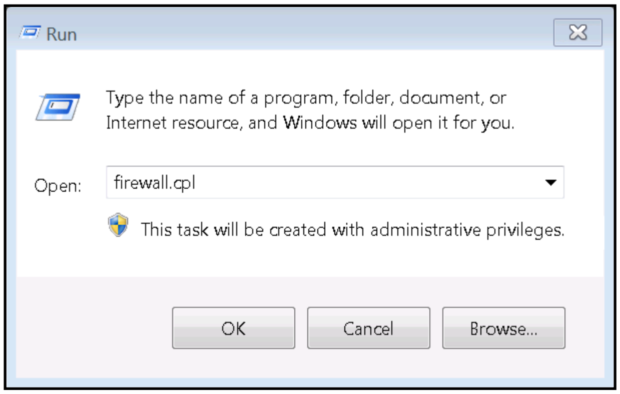
NetVanta UC Server automatically creates a backup folder for storing interim NetVanta UC Server system files, database schema, and database content during synchronization. For NetVanta UC Server upgrades from 5.2.x, the backup folder is **C:\backup**. For new installations of NetVanta UC Server version 5.3.0, the backup folder is **C:\ADTRAN\Backup**.

Step 4: Configure the Windows Firewall for SQL Server Access on the Primary and Secondary Servers

The Business Continuity Service accesses the SQL Server databases used by NetVanta UC Server. In particular, the service on the secondary server accesses the databases on the primary server and vice versa. This section outlines how to configure the Windows Firewall to allow this remote access. These steps must be performed on both the primary and secondary servers. If the firewall is disabled, it is not necessary to configure exceptions to permit remote connections to SQL Server.

This topic is discussed in detail in the following Microsoft Developer Network article: http://msdn.microsoft.com/en-us/library/cc646023.aspx. The basic steps are as follows:

1. In the **Start** menu, open **Run**.
2. In the **Open** field, enter **firewall.cpl**, and select **OK**. The control panel's **Windows Firewall** menu will open.



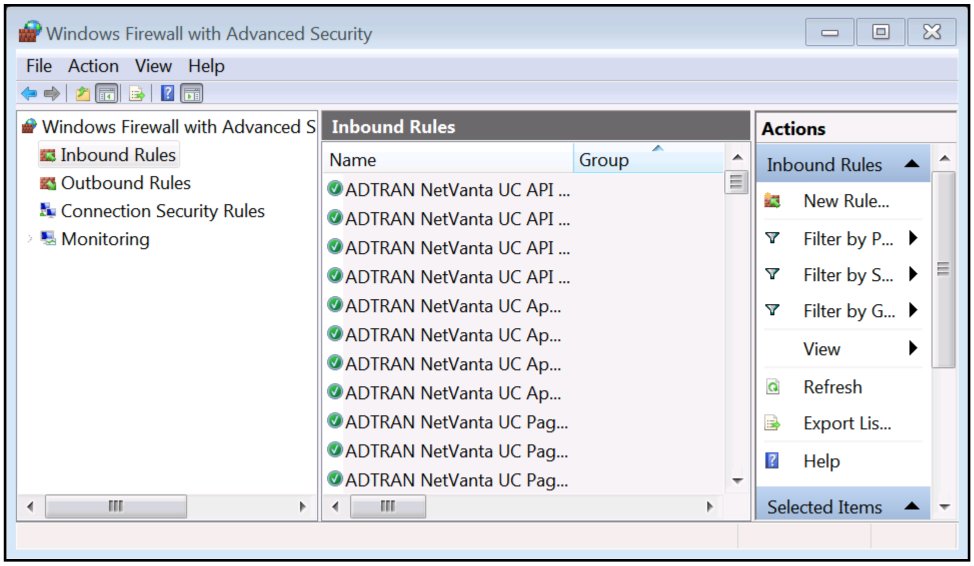
Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: firewall.cpl

This task will be created with administrative privileges.

3. On the left side of the **Windows Firewall** menu, select A**dvanced settings** to open the **Windows Firewall with Advanced Security** menu.
4. In the **Windows Firewall with Advanced Security** menu, select **Inbound Rules**.



Windows Firewall with Advanced Security

ADTRAN NetVanta UC API ...
ADTRAN NetVanta UC API ...
ADTRAN NetVanta UC API ...
ADTRAN NetVanta UC API ...
ADTRAN NetVanta UC Ap...
ADTRAN NetVanta UC Ap...
ADTRAN NetVanta UC Ap...
ADTRAN NetVanta UC Ap...
ADTRAN NetVanta UC Pag...
ADTRAN NetVanta UC Pag...
ADTRAN NetVanta UC Pag...

5. Scroll through the list of **Inbound Rules** to determine if access to **SQL Server** is already permitted. Look in the **Program** column for the following entry on a 32-bit system:
C:\Program Files\Microsoft SQL Server\MSSQL10.NETVANTAUC\MSSQL\Binn\sqlservr.exe
Look in the **Program** column for the following entry on a 64-bit system:
C:\Program Files (x86)\Microsoft SQL Server\MSSQL10.NETVANTAUC\MSSQL\Binn\sqlservr.exe
If an entry is found and the corresponding **Action** column contains **Allow**, then the firewall is likely already properly configured.
6. If no such entry is found, select **New Rule** under the **Actions** section. The **Rule Type** menu of the **New Inbound Rule Wizard** appears.
7. In the **Rule Type** menu, select the **Program** radio button. Then, select **Next**. The **Program** menu appears.
8. In the **Program** menu, select the **This program path** radio button. Then select the **Browse** button.
9. In the menu that opens, browse to the following directory on a 32-bit system:
C:\Program Files\Microsoft SQL Server\MSSQL10.NETVANTAUC\MSSQL\Binn
On a 64-bit system, browse to the following directory:
C:\Program Files (x86)\Microsoft SQL Server\MSSQL10.NETVANTAUC\MSSQL\Binn
Once you have browsed to the appropriate directory, select **sqlservr.exe**, then select **Open**.
10. Once you have selected the program path of **sqlservr.exe**, select **Next**. The **Action** menu appears.
11. In the **Action** menu, select **Allow the connection**. Then, select **Next**. The **Profile** menu appears.
12. In the **Profile** menu, select **Next**. The **Name** menu appears.
13. In the **Name** menu, use the provided fields to specify a name and optional description for the rule. Then, select **Next**. The inbound rule will be created and you will be returned to the **Windows Firewall with Advanced Security** menu.
14. Scroll through the list of **Inbound Rules** to determine if access to **SQL Server Browser** is already permitted. Look in the **Program** column for the following entry on a 32-bit system:
C:\Program Files\Microsoft SQL Server\90\Shared\sqlbrowser.exe
Look in the **Program** column for the following entry on a 64-bit system:
C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe
If an entry is found and the corresponding **Action** column contains **Allow**, then the firewall is likely already properly configured.
15. If no such entry is found, select **New Rule** under the **Actions** section. The **Rule Type** menu of the **New Inbound Rule Wizard** appears.
16. In the **Rule Type** menu, select the **Program** radio button. Then, select **Next**. The **Program** menu appears.
17. In the **Program** menu, select the **This program path** radio button. Then select the **Browse** button.
18. In the menu that opens, browse to the following directory on a 32-bit system:
C:\Program Files\Microsoft SQL Server\90\Shared\
Browse to the following directory on a 64-bit system:
C:\Program Files (x86)\Microsoft SQL Server\90\Shared\
Once you have browsed to the appropriate directory, select **sqlbrowser.exe**, then select **Open**.
19. Once you have selected the program path of **sqlbrowser.exe**, select **Next**. The **Action** menu appears.
20. In the **Action** menu, select **Allow the connection**. Then, select **Next**. The **Profile** menu appears.
21. In the **Profile** menu, select **Next**. The **Name** menu appears.

22. In the **Name** menu, use the provided fields to specify a name and optional description for the rule. Then, select **Next**. The inbound rule will be created and you will be returned to the **Windows Firewall with Advanced Security** menu.

Step 5: Enter the Product License Key on the Secondary Server and Begin Configuring the Secondary Server

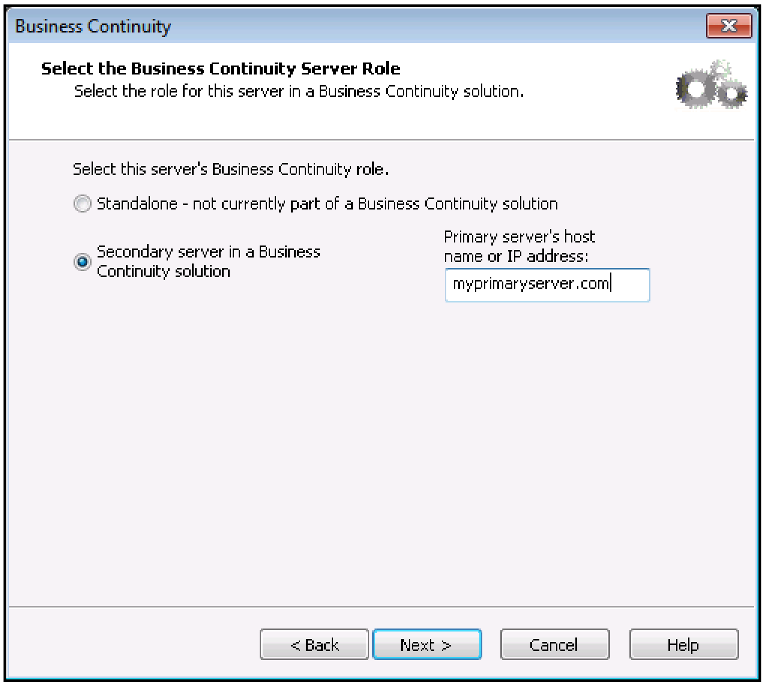
To enter the business continuity license key and begin configuring the secondary server using the Server Configuration Wizard, follow these steps:

1. Log in to the secondary server using the service account.
2. In the Windows Start menu, navigate to **Programs > ADTRAN > NetVanta UC Server** > **NetVanta UC Server Configuration Wizard**. The **NetVanta UC Server Configuration Wizard** main menu appears.
3. On the main menu, select **Product Licensing** to open the **Product Licensing Wizard**. The **Product Licensing Wizard** welcome menu appears.
4. Select **Next**. The **Enter a Purchase Key** menu appears.
5. In the **Purchase key** field, enter the purchase key for the NetVanta UC Server software. Then, select **Next**. The **Enter a License Key** menu appears.
6. In the **Please specify a license key** field of the **Enter a License Key** menu, enter the license key you obtained from ADTRAN (this is the same license key you entered in the primary server earlier in the configuration). Then, select **Next**. The **Summary of License Options** menu appears.
7. In the **Summary of License Options** menu, review the details of the licensed features. Then, select **Next**.
8. The purchase key and license key will be registered with the ADTRAN server. Select **Next** once these tasks have been completed. Then, select **Next** again to exit the **Product Licensing Wizard**.
9. In the NetVanta UC Server Configuration Wizard main menu, select **Windows Network Integration** to open the **Windows Network Integration Wizard**. The **Windows Network Integration Wizard** welcome menu appears.
10. Select **Next**. The **Network Connection** menu appears.
11. In the **Network Connection** menu, ensure that the checkbox next to **Automatically configure Windows Firewall for server requests** is checked. Then, select **Next**. The **Configure the Windows Integration** menu appears.
12. In the **Configure the Windows Integration** menu, select the **Use or create a service account within Windows Active Directory** radio button. Then, select **Next**. The **Windows Domain Service Account** menu appears.
13. In the **Select Service Account** menu, select the **Existing account** radio button. Then, select **Next**. The **Service Account Settings** menu appears.
14. In the **Service Account Settings** menu, select the **Browse** button to browse for the service account you created during *Preparation on page 8*. This must be the same service account as the one used on the primary server. Once you have chosen the service account, enter the password for the service account in the **Enter password** field, then re-enter the password in the **Confirm password** field. Once you have finished selecting the service account and entering the password, select **Next**.

15. On the summary page that appears, review the options you selected, then select **Submit**.
16. The wizard will configure the Windows Firewall and service account. Select **Next** once these tasks have been completed. Then, select **Next** again to exit the **Windows Network Integration Wizard**.
17. Use the **Communication Systems** and **Phone Types** wizards in the **NetVanta UC Server Configuration Wizard** to configure the communication systems and phone types that will be used with NetVanta UC Server. The communication systems and phone types defined on the secondary server must match those defined earlier on the primary server in Step 18 of *Step 2:Install NetVanta UC Server on the Primary Server and Begin Configuring the Primary Server*. They must also be installed in the same order as they were on the primary server. For more information on using the wizards available in the **NetVanta UC Server Configuration Wizard**, refer to the *NetVanta Unified Communications Server Configuration Guide* for your version of NetVanta UC Server available from the ADTRAN Support Community (https://supportforums.adtran.com).

> NOTE
>
> *If a NetVanta ECS communication system was defined on the primary server using the Communication Systems wizard, a matching NetVanta ECS communication system also must be configured on the secondary server. For more information on managing NetVanta ECS communication systems, refer to Appendix C – NetVanta ECS Communication System Considerations on page 63.*

18. Once you are able to access it, select **Business Continuity** in the **NetVanta UC Server Configuration Wizard** main menu to open the **Business Continuity Wizard**.
19. Select **Next**. The **Select the Business Continuity Server Role** menu appears.
20. In the **Select the Business Continuity Server Role** menu, select **secondary server in a Business Continuity Solution**, and enter the fully qualified domain name (FQDN) or IP address of the primary server in the **Primary server's host name or IP address field**. Then, select **Next**.



Business Continuity

Select the Business Continuity Server Role

Select the role for this server in a Business Continuity solution.

Select this server's Business Continuity role.

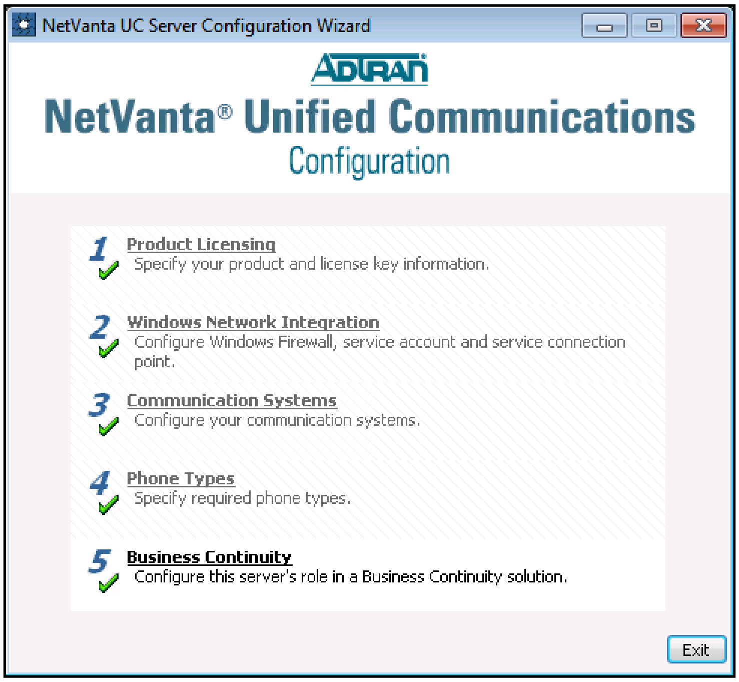
○ Standalone - not currently part of a Business Continuity solution

● Secondary server in a Business Continuity solution

Primary server's host name or IP address: myprimaryserver.com

21. On the summary page that appears, review the options you selected, then select **Submit**.

22. The wizard will configure the server's business continuity role and the FQDN or IP address of the primary server. Select **Next** once the task has been completed. Then, select **Next** again to exit the **Business Continuity Wizard**.
23. After exiting the **Business Continuity** wizard, the remaining wizards will be removed from the list of available wizards in the **NetVanta UC Server Configuration Wizard**, because they no longer apply to the secondary server. The **NetVanta UC Server Configuration Wizard** main menu appears as follows:


NetVanta UC Server Configuration Wizard
ADTRAN
NetVanta® Unified Communications
Configuration
Exit

1 Product Licensing
Specify your product and license key information.

2 Windows Network Integration
Configure Windows Firewall, service account and service connection point.

3 Communication Systems
Configure your communication systems.

4 Phone Types
Specify required phone types.

5 Business Continuity
Configure this server's role in a Business Continuity solution.

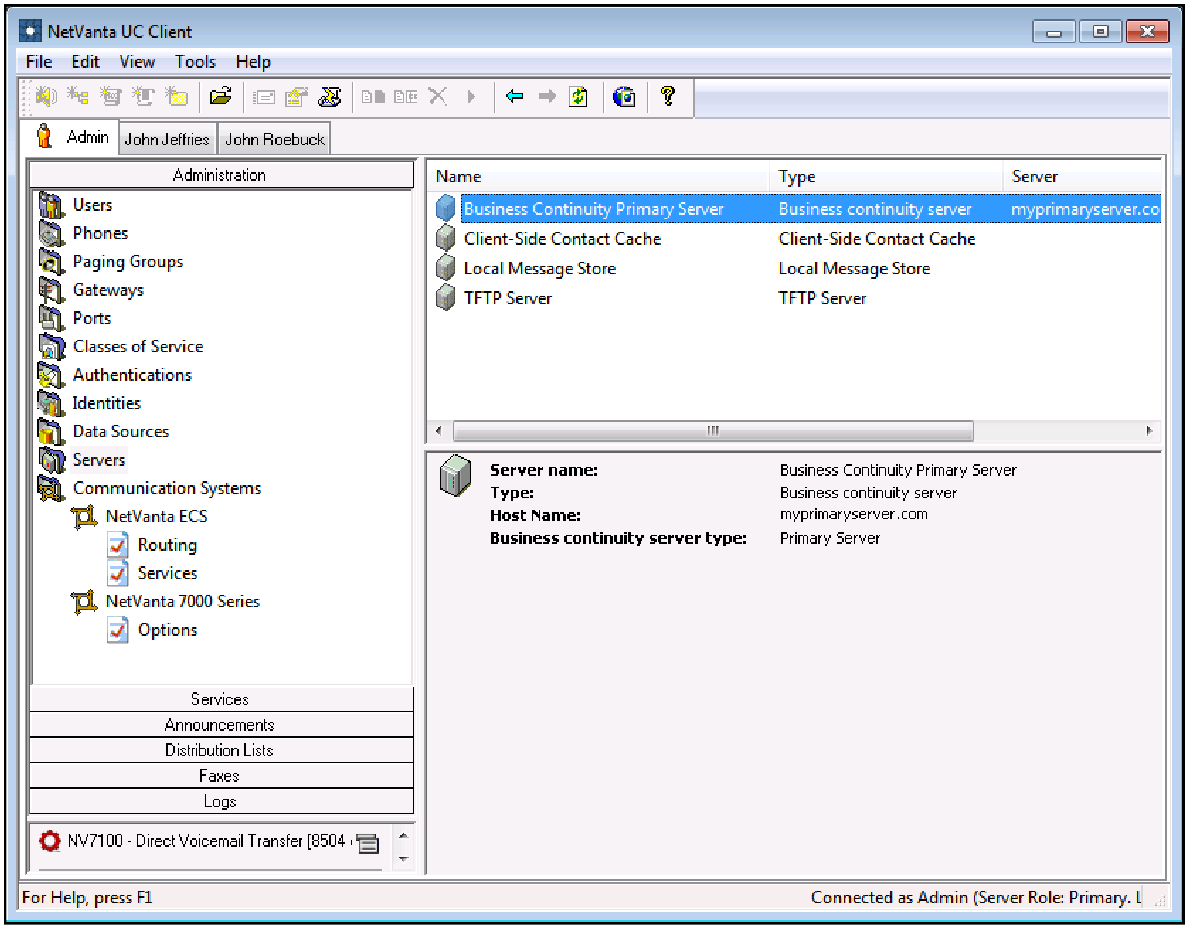
24. Exit the **NetVanta UC Server Configuration Wizard**.

Step 6: Configure Business Continuity on the Secondary Server

To complete the business continuity configuration for the secondary server, follow these steps:

1. Log in to the secondary server using the service account.
2. Log in to the NetVanta UC Client as an administrator.
3. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.
4. Select the **Servers** topic from the **Administration** navigation pane.
5. In the **Servers** summary pane, right-click each server object, and select **Track message actions** (if it is available).

6. In the **Servers** summary pane, double-click the **Business Continuity primary Server** object. The **Business Continuity Server Configuration** menu appears.

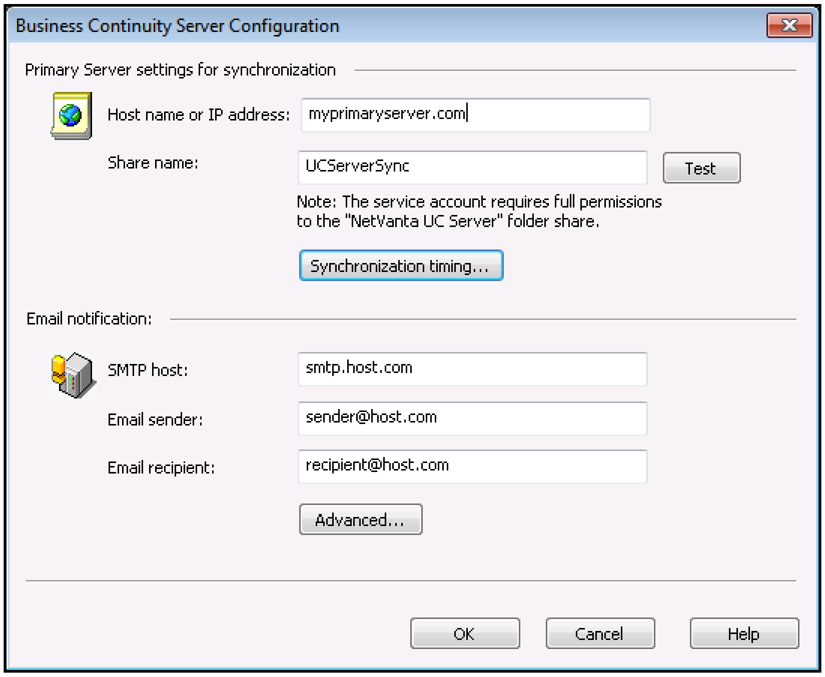


Name	Type	Server
Business Continuity Primary Server	Business continuity server	myprimaryserver.co
Client-Side Contact Cache	Client-Side Contact Cache	
Local Message Store	Local Message Store	
TFTP Server	TFTP Server	

Server name: Business Continuity Primary Server
Type: Business continuity server
Host Name: myprimaryserver.com
Business continuity server type: Primary Server

For Help, press F1 Connected as Admin (Server Role: Primary. L

7. The **Business Continuity Server Configuration** menu is used to configure the hostname or IP address of the partner server and network share used on the partner server to copy NetVanta UC Server data from one server to the other during synchronization. Also, email notification information for the server is configured in this menu.


Business Continuity Server Configuration
Primary Server settings for synchronization
Test
Synchronization timing...
Email notification:
Advanced...
OK
Cancel
Help

Host name or IP address: myprimaryserver.com

Share name: UCServerSync

Note: The service account requires full permissions to the "NetVanta UC Server" folder share.

SMTP host: smtp.host.com

Email sender: sender@host.com

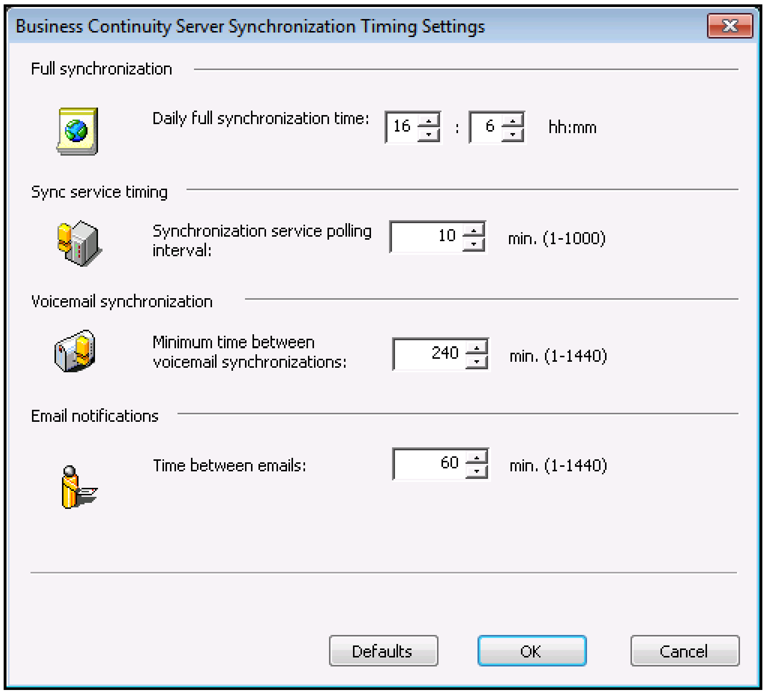
Email recipient: recipient@host.com

The following table describes the settings that can be configured in this menu:

Settings	Description
Host name or IP address	This field specifies the hostname or IP address of the partner server in the business continuity solution. For example, if you are configuring the secondary server, the hostname or IP address of the primary server should be entered in this field.
Share name	This field specifies the network share configured on the partner server in the business continuity solution that was created during business continuity installation. For example, if you are configuring the secondary server, the name of the network share created on the primary server should be entered in this field. This folder is used to copy NetVanta UC Server data from one server to the other during synchronization. The NetVanta UC Server service account must have full permissions to this network share.
Test	This button validates the network share specified in the **Share name** field.
Synchronization timing	This button opens the **Business Continuity Server Synchronization Timing Settings** menu.
SMTP host	This field specifies the IP address of the Simple Mail Transfer Protocol (SMTP) host used to send business continuity email notifications and error reports.
Email sender	This field specifies the sender email address of business continuity email notifications and error reports.
Email recipient	This field specifies an email recipient to receive business continuity email notifications and error reports.

Settings *(Continued)*	Description *(Continued)*
Advanced	This button opens the **Business Continuity Advanced SMTP Security Settings** menu.

8. In the **Business Continuity Server Configuration** menu, select the **Synchronization timing** button to access the **Business Continuity Server Synchronization Timing Settings** menu.


Business Continuity Server Synchronization Timing Settings
Full synchronization
Sync service timing
Voicemail synchronization
Email notifications
Defaults
OK
Cancel

Daily full synchronization time: 16 : 6 hh:mm

Synchronization service polling interval: 10 min. (1-1000)

Minimum time between voicemail synchronizations: 240 min. (1-1440)

Time between emails: 60 min. (1-1440)

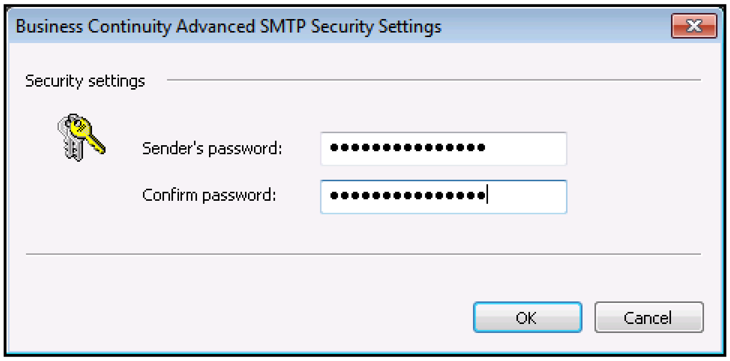
In this menu, you can configure the synchronization timing settings for the Business Continuity Service on the secondary server. The following table describes the settings that can be configured in this menu:

Settings	Description
Daily full synchronization time	This setting specifies the time of day (in 24-hour format) at which a full backup is performed of the primary server to the secondary server. This time should be scheduled during a maintenance window.
Synchronization service polling interval	This setting specifies the interval (in minutes) at which the Business Continuity Service on the secondary server will wake up and perform its synchronization actions. When the Business Continuity Service on the secondary server wakes up, it will perform the following actions: • At the Daily full synchronization time, the service will perform a full backup of the primary server to the secondary server. • If a full backup is not performed (i.e., it is not the Daily full synchronization time) and if a synchronization has not occurred within the interval specified by the Minimum time between voicemail synchronizations, the service will synchronize the local message store voicemails from the primary server to the secondary server. Also, if a full backup is not performed, the service will synchronize the SIP registration records from the primary server to the secondary server. The default value for this setting is **10** minutes. The value range for this setting is **1** to **1000** minutes.

Settings *(Continued)*	Description *(Continued)*
Minimum time between voicemail synchronizations	This setting specifies the minimum interval (in minutes) at which the Business Continuity Service on the secondary server will synchronize local message store voicemail from the primary server to the secondary server. If during its wake-up synchronization routine the Business Continuity Service on the secondary server detects voicemail activity on the primary server and a synchronization has not been performed in this interval, the local message store voicemails will be synchronized from the primary server to the secondary server. The default value for this setting is **240** minutes. This interval provides a balance between the bandwidth required for copying voicemails and the time window within which voicemails will be out of sync. The value range for this setting is **1** to **1440** minutes.
Time between emails	This setting specifies the interval (in minutes) at which the primary server will send notification emails to the **Email recipient** (configured in the **Business Continuity Server Configuration** menu). The default value for this setting is **60** minutes. The value range for this setting is **1** to **1440** minutes.

9. After you have finished configuring the business continuity server synchronization timing settings for the secondary server, select **OK** to save the settings and return to the **Business Continuity Server Configuration** menu.

10. In the **Business Continuity Server Configuration** menu, select the **Advanced** button to access the **Business Continuity Advanced SMTP Security Settings** menu. This menu is used to configure the password for the **Email sender** address used to send business continuity email notifications. Enter the password for the **Email sender** in the **Sender's password** field, then re-enter the password in the **Confirm password** field. Select **OK** to save the password and return to the **Business Continuity Server Configuration** menu.


Business Continuity Advanced SMTP Security Settings
Security settings
Sender's password: ••••••••••••••••
Confirm password: ••••••••••••••••
OK
Cancel

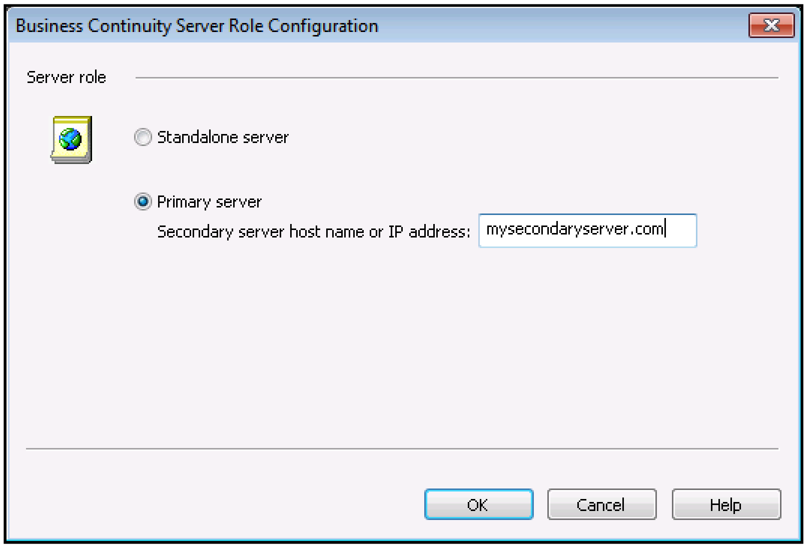
11. Now that you have configured all of the settings available in the **Business Continuity Server Configuration** menu, select **OK** to save the configuration.

Step 7: Configure Business Continuity on the Primary Server

Now that the secondary server is configured, business continuity configuration can be completed on the primary server. To complete the business continuity configuration on the primary server, follow these steps:

> *As soon as the primary server's role is set to primary, synchronization from the primary to the secondary server will occur at the default time (12:30 AM). It is important that all the following steps be accomplished before automatic synchronization occurs.*

1. Log in to the primary server using the service account.
2. Log in to the NetVanta UC Client as an administrator.
3. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.
4. Select the **Servers** topic from the **Administration** navigation pane.
5. Right-click in the **Servers** summary pane, and select **UC Server Role**. The **Business Continuity Server Role Configuration** menu appears.
6. In the **Business Continuity Server Role Configuration** menu, select the **Primary server** radio button, and enter the host name or IP address of the secondary server in the provided field. Then, select **OK**



○ Standalone server

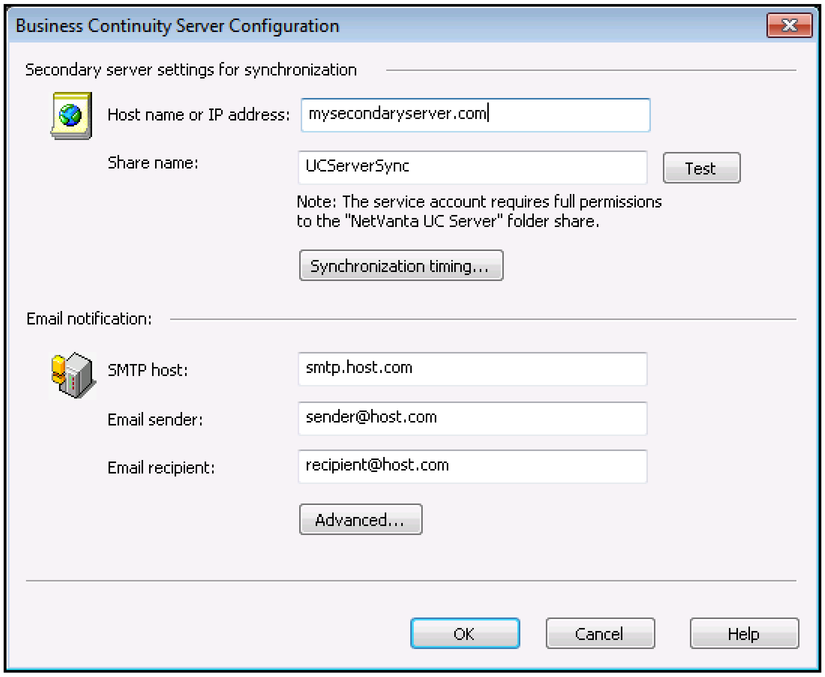
● Primary server

Secondary server host name or IP address: mysecondaryserver.com

> *Any phones that are configured to dual register will now be reprogrammed to register with both the primary and secondary servers.*

7. In the Servers summary pane, double-click the **Business Continuity secondary server** object. The **Business Continuity Server Configuration** menu appears.

8. The **Business Continuity Server Configuration** menu is used to configure the hostname or IP address of the partner server and network share used on the partner server to copy NetVanta UC Server data from one server to the other during synchronization. Also, email notification information for the server is configured in this menu.



Business Continuity Server Configuration

Secondary server settings for synchronization

Host name or IP address: mysecondaryserver.com

Share name: UCServerSync

Note: The service account requires full permissions to the "NetVanta UC Server" folder share.

Email notification:

SMTP host: smtp.host.com

Email sender: sender@host.com

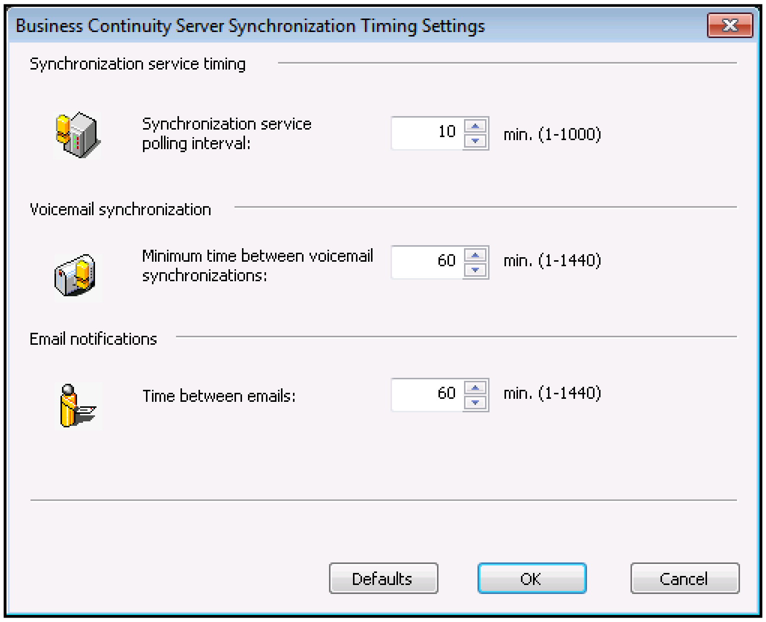
Email recipient: recipient@host.com

The following table describes the settings that can be configured in this menu:

Settings	**Description**
Host name or IP address	This field specifies the hostname or IP address of the partner server in the business continuity solution. For example, if you are configuring the primary server, the hostname or IP address of the secondary server should be entered in this field.
Share name	This field specifies the network share configured on the partner server in the business continuity solution that was created during business continuity installation. For example, if you are configuring the primary server, the name of the network share created on the secondary server should be entered in this field. This folder is used to copy NetVanta UC Server data from one server to the other during synchronization. The NetVanta UC Server service account must have full permissions to this network share.
Test	This button validates the network share specified in the **Share name** field.
Synchronization timing	This button opens the **Business Continuity Server Synchronization Timing Settings** menu.
SMTP host	This field specifies the IP address of the SMTP host used to send business continuity email notifications and error reports.
Email sender	This field specifies the sender email address of business continuity email notifications and error reports.
Email recipient	This field specifies an email recipient to receive business continuity email notifications and error reports.

Settings *(Continued)*	Description *(Continued)*
Advanced	This button opens the **Business Continuity Advanced SMTP Security Settings** menu.

9. In the **Business Continuity Server Configuration** menu, select the **Synchronization timing** button to access the **Business Continuity Server Synchronization Timing Settings** menu.


Business Continuity Server Synchronization Timing Settings

Synchronization service timing

Synchronization service polling interval: 10 min. (1-1000)

Voicemail synchronization

Minimum time between voicemail synchronizations: 60 min. (1-1440)

Email notifications

Time between emails: 60 min. (1-1440)

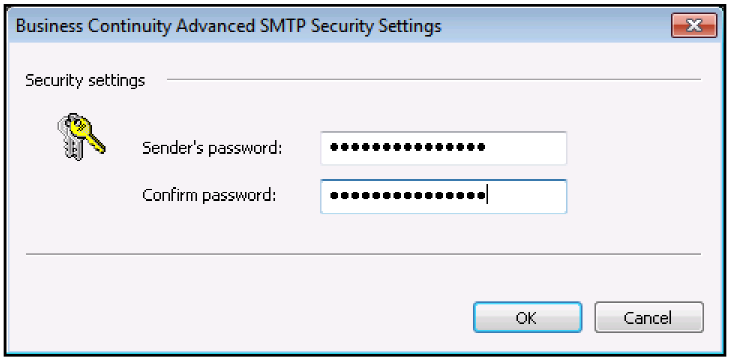
In this menu, you can configure the synchronization timing settings for the Business Continuity Service on the primary server. The following table describes the settings that can be configured in this menu:

Settings	Description
Synchronization service polling interval	This setting specifies the interval (in minutes) at which the Business Continuity Service on the primary server will wake up and perform its synchronization actions. When the Business Continuity Service on the primary server wakes up, it will determine if any voicemail activity has occurred on the secondary server. If there has been activity on the secondary server, the Business Continuity Service on the primary server will perform the following actions: • The service will send an email to the Email recipient (configured in the **Business Continuity Server Configuration** menu) if an email has not been sent within the interval specified by the **Time between emails** setting. • The service will synchronize the local message store voicemails from the secondary server to the primary server if a synchronization has not occurred within the interval specified by the **Minimum time between voicemail synchronizations**. The default value for this setting is **10** minutes. The value range for this setting is **1** to **1000** minutes.

Settings	Description *(Continued)*
Minimum time between voicemail synchronizations	This setting specifies the minimum interval (in minutes) at which the Business Continuity Service on the primary server will synchronize the local message store voicemail from the secondary server to the primary server. If during its wake-up synchronization routine the Business Continuity Service on the primary server detects voicemail activity on the secondary server and a synchronization has not been performed in this interval, the local message store voicemails will be synchronized from the secondary server to the primary server. The default value for this setting is **60** minutes. This interval provides a balance between the bandwidth required for copying voicemails and the time window within which voicemails will be out of sync. The value range for this setting is **1** to **1440** minutes.
Time between emails	This setting specifies the interval (in minutes) at which the primary server will send notification emails to the Email recipient (configured in the **Business Continuity Server Configuration** menu). The default value for this setting is **60** minutes. The value range for this setting is **1** to **1440** minutes.

10. After you have finished configuring the business continuity server synchronization timing settings for the secondary server, select **OK** to save the settings and return to the **Business Continuity Server Configuration** menu.

11. In the **Business Continuity Server Configuration** menu, select the **Advanced** button to access the **Business Continuity Advanced SMTP Security Settings** menu. This menu is used to configure the password for the **Email sender** address used to send business continuity email notifications. Enter the password for the **Email sender** in the **Sender's password** field, then re-enter the password in the **Confirm password** field. Select **OK** to save the password and return to the **Business Continuity Server Configuration** menu.



Sender's password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

12. Now that you have configured all of the settings available in the **Business Continuity Server Configuration** menu, select **OK** to save the configuration. The business continuity solution is now operational.

Step 8: Manually Synchronize the Secondary Server with the Primary Server

To perform an initial, manual synchronization of the secondary server with the primary server, follow these steps:

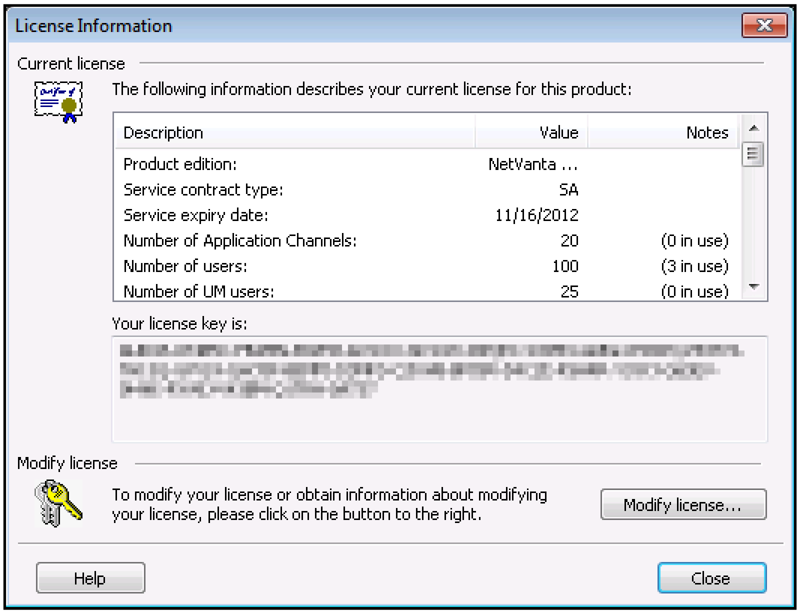
1. In the Windows Start menu on the secondary server, right-click **Command Prompt** entry, and select **Run as administrator**. This will run Windows **Command Prompt** as an Administrator.
2. Use the CD command to change directories to the **NetVanta UC Server\Bin** folder. On 32-bit systems, the default for this directory is **C:\Program Files\ADTRAN\NetVanta UC Server\Bin**. On 64-bit systems, the default for this directory is **C:\Program Files (x86)\ADTRAN\NetVanta UC Server\Bin**, for example:
   >**CD C:\Program Files (x86)\ADTRAN\NetVanta UC Server\Bin**
3. Once you have changed directories, execute the following command:
   >**cscript DataSync.vbs RunFirst**
   The NetVanta UC Server objects on the primary server will be copied to the secondary server.

If the Secondary Server Is Not Initially Available

The steps described above assume that the secondary server is immediately available. If this is not the case, it is possible to modify the previous installation steps so that the primary server can be configured without knowing the machine ID of the secondary server. The required changes to the installation process are:

1. Skip the steps in *Step 1: Install NetVanta UC Server on the secondary server and Retrieve the Secondary Server Machine ID on page 8* since the secondary server is not initially available.
2. In *Step 2: Install NetVanta UC Server on the Primary Server and Begin Configuring the Primary Server on page 9*, request a license key from ADTRAN using only the machine ID of the primary server. This license key will indicate that the Business Continuity feature is enabled but it cannot be used to license the secondary server. This key will be replaced with a key that contains both machine IDs once the secondary server is available.
3. Create a network share on the primary server using the directions in *Step 3: Create a Network Share on the Primary and Secondary Servers for Copying NetVanta UC Server Data on page 15*. Then, configure the Windows firewall for SQL server access on the primary server using the directions in *Step 4: Configure the Windows Firewall for SQL Server Access on the Primary and Secondary Servers on page 16*.
4. Once the secondary server is available, install NetVanta UC Server using the directions in *Step 1: Install NetVanta UC Server on the secondary server and Retrieve the Secondary Server Machine ID on page 8*. Then, request a new product license key using the primary and secondary server machine IDs, as outlined in *Step 2: Install NetVanta UC Server on the Primary Server and Begin Configuring the Primary Server on page 9*.
5. Complete *Step 3: Create a Network Share on the Primary and Secondary Servers for Copying NetVanta UC Server Data on page 15* and *Step 4: Configure the Windows Firewall for SQL Server Access on the Primary and Secondary Servers on page 16* on the secondary server.
6. During *Step 5: Enter the Product License Key on the Secondary Server and Begin Configuring the Secondary Server on page 18*, use the new product license key that you requested using the primary and secondary server machine IDs.

7. Complete the remaining steps provided above to configure business continuity on the secondary server. Omit any steps pertaining to the primary server, as these are already complete.
8. After configuring business continuity on the secondary server, log in to the primary server using the service account. Then, log in to the NetVanta UC Client as an administrator.
9. In the menu bar, select **Help**, then select **License Information** from the drop-down menu. The **License Information** menu will appear.
10. In the **License Information** menu, select **Modify license**. The **Modify License** menu will appear.



License Information

Current license

The following information describes your current license for this product:

Description	Value	Notes
Product edition:	NetVanta ...	
Service contract type:	SA	
Service expiry date:	11/16/2012	
Number of Application Channels:	20	(0 in use)
Number of users:	100	(3 in use)
Number of UM users:	25	(0 in use)

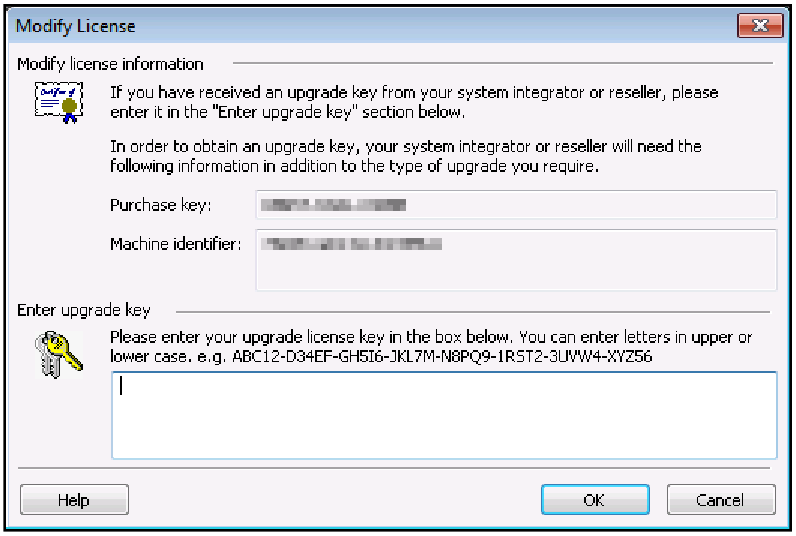
Your license key is:

[redacted]

Modify license

To modify your license or obtain information about modifying your license, please click on the button to the right.

11. In the **Enter upgrade key** field of the **Modify License** menu, enter the new product license key that you requested using the primary and secondary server machine IDs. Then, select **OK**.



Modify License

Modify license information

If you have received an upgrade key from your system integrator or reseller, please enter it in the "Enter upgrade key" section below.

In order to obtain an upgrade key, your system integrator or reseller will need the following information in addition to the type of upgrade you require.

Purchase key: [redacted]

Machine identifier: [redacted]

Enter upgrade key

Please enter your upgrade license key in the box below. You can enter letters in upper or lower case. e.g. ABC12-D34EF-GH5I6-JKL7M-N8PQ9-1RST2-3UVW4-XYZ56

Installing a NetVanta UC Server Version 5.3 Business Continuity Solution as an Upgrade

This section provides steps for installing a NetVanta UC Server version 5.3 Business Continuity solution as an upgrade for a previous version of NetVanta UC Server. This section cannot be used for systems on which a disaster recovery solution is installed. For instructions on upgrading a previous NetVanta UC Server Disaster Recovery solution installation, see *Upgrading From a NetVanta UC Server Disaster Recovery Solution on page 39*.

Preparation

Select a domain account that will be used as the NetVanta UC Server service account on both the primary and secondary servers. If Exchange Server will be used, this account must have special Exchange Server permissions. For more information on configuring the permissions for the service account, refer to *Configuring Microsoft Exchange 2007 and 2010 Permissions for Integration with NetVanta UC Server* available from the ADTRAN Support Community (https://supportforums.adtran.com)

Ensure that the chosen account is a member of the local Administrators group on both systems. You can do this from the **Local users and Groups** section of the **Computer Managemen**t console. The selected account will be called the service account in the rest of this section.

Step 1: Install NetVanta UC Server on the Secondary Server and Retrieve the Secondary Server Machine ID

For more information on installing NetVanta UC Server 5.3 on the secondary server and determining the machine ID of the secondary server (used for product licensing), refer to *Step 1: Install NetVanta UC Server on the secondary server and Retrieve the Secondary Server Machine ID on page 8*.

Step 2: Upgrade NetVanta UC Server on the Primary Server and Begin Configuring the Primary Server

To enter the product license key, configure the service account, and temporarily specify server role as standalone on the primary server, follow these steps:

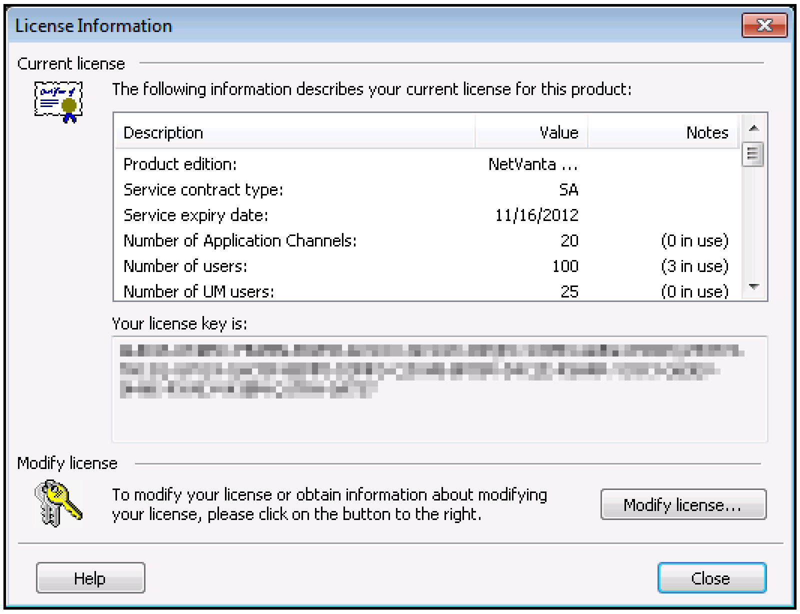
> NOTE *The business continuity role of the primary server is specified later in the business continuity configuration.*

1. Log in to the primary server using the service account.

2. Install the same version of NetVanta UC Server software on the primary server as was previously installed on the secondary server. The current version of NetVanta UC Server software will be upgraded. For more information on installing NetVanta UC Server, refer to the *NetVanta Unified Communications Software Installation Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com). **Do not run the NetVanta UC Server Configuration Wizard.**

> NOTE *The build numbers of the versions of NetVanta UC Server installed on the primary and secondary servers must be identical for server synchronization*

3. Log in to the NetVanta UC Client as an administrator.
4. In the menu bar, select **Help**, then select **License Information** from the drop-down menu. The **License Information** menu will appear.
5. In the **License Information** menu, select **Modify license**. The **Modify License** menu will appear.



License Information

Current license

The following information describes your current license for this product:

Description	Value	Notes
Product edition:	NetVanta ...	
Service contract type:	SA	
Service expiry date:	11/16/2012	
Number of Application Channels:	20	(0 in use)
Number of users:	100	(3 in use)
Number of UM users:	25	(0 in use)

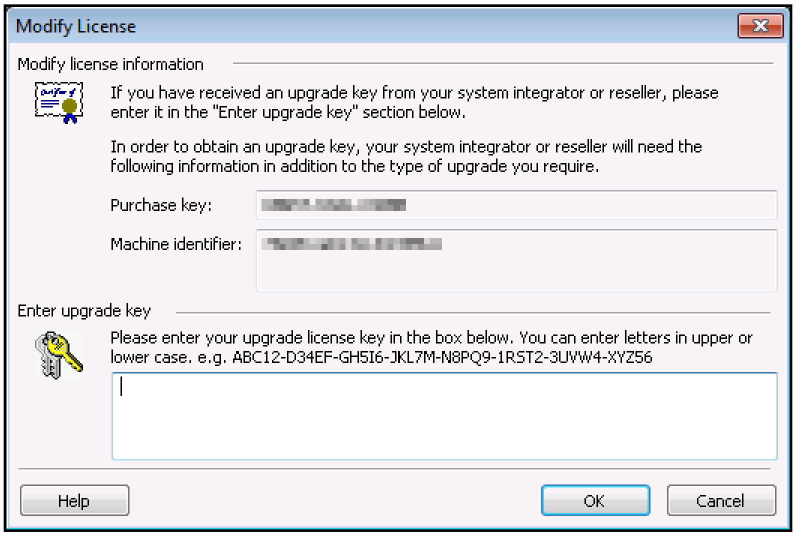
Your license key is:

[redacted]

Modify license

To modify your license or obtain information about modifying your license, please click on the button to the right.

6. In the **Modify License** menu, the machine ID for the primary server will appear in the **Machine identifier** field. Use this machine ID along with the one recorded for the secondary server to request a business continuity license key. Contact ADTRAN technical support to request a business continuity license key. You will be asked for the machine IDs of the primary and secondary servers. Once you have the business continuity license key, enter the license key in the **Enter upgrade key field** of the **Modify License** menu. Then, select **OK**.


Modify License

Modify license information

If you have received an upgrade key from your system integrator or reseller, please enter it in the "Enter upgrade key" section below.

In order to obtain an upgrade key, your system integrator or reseller will need the following information in addition to the type of upgrade you require.

Purchase key: [redacted]

Machine identifier: [redacted]

Enter upgrade key

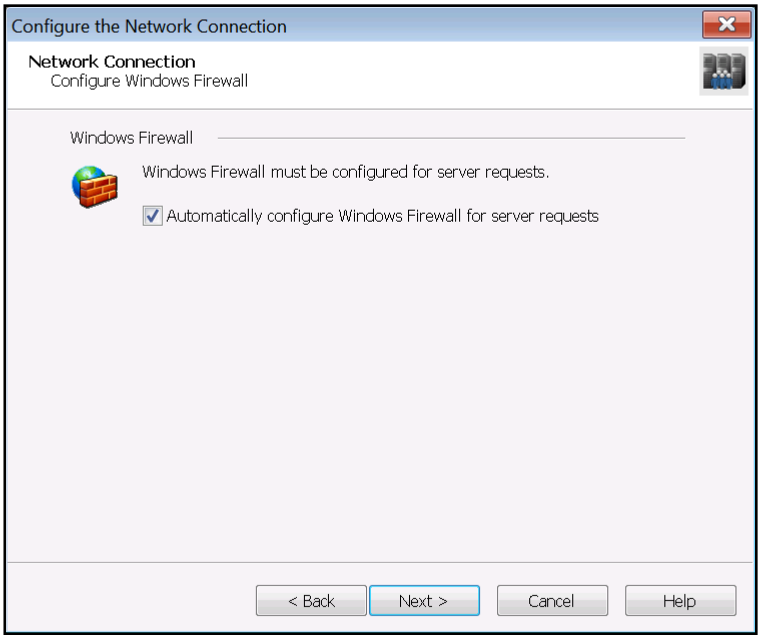
Please enter your upgrade license key in the box below. You can enter letters in upper or lower case. e.g. ABC12-D34EF-GH5I6-JKL7M-N8PQ9-1RST2-3UVW4-XYZ56

7. In the Windows Start menu on the primary server, navigate to **Programs > ADTRAN > NetVanta UC Server** > **NetVanta UC Server Configuration Wizard**. The **NetVanta UC Server Configuration Wizard** main menu appears.

8. In the **NetVanta UC Server Configuration Wizard** main menu, select **Change Server Account** to open the **Windows NetWork Integration Wizard**.

9. Select **Next**. The **Network Connection** menu appears.

10. In the **Network Connection** menu, ensure that the checkbox next to **Automatically configure Windows Firewall for server requests** is checked. Then, select **Next**. The **Configure the Windows Integration** menu appears.



Configure the Network Connection

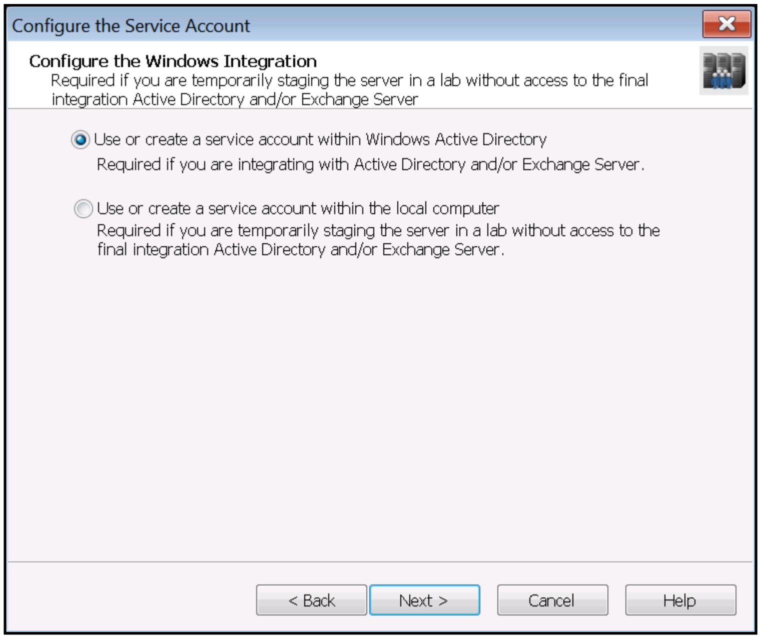
Network Connection
Configure Windows Firewall

Windows Firewall

Windows Firewall must be configured for server requests.

☑ Automatically configure Windows Firewall for server requests

11. In the **Configure the Windows Integration** menu, select the **Use or create a service account within Windows Active Directory** radio button. Then, select **Next**. The **Windows Domain Service Account** menu appears.



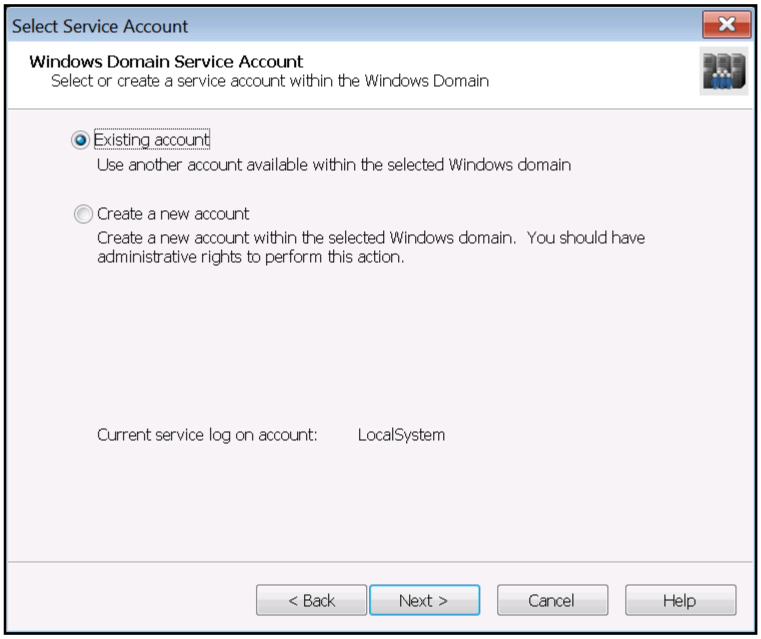
Configure the Service Account

Configure the Windows Integration
Required if you are temporarily staging the server in a lab without access to the final integration Active Directory and/or Exchange Server

● Use or create a service account within Windows Active Directory
Required if you are integrating with Active Directory and/or Exchange Server.

○ Use or create a service account within the local computer
Required if you are temporarily staging the server in a lab without access to the final integration Active Directory and/or Exchange Server.

12. In the **Select Service Account**, select the **Existing account** radio button. Then, select **Next**. The **Service Account Settings** menu appears.



Select Service Account

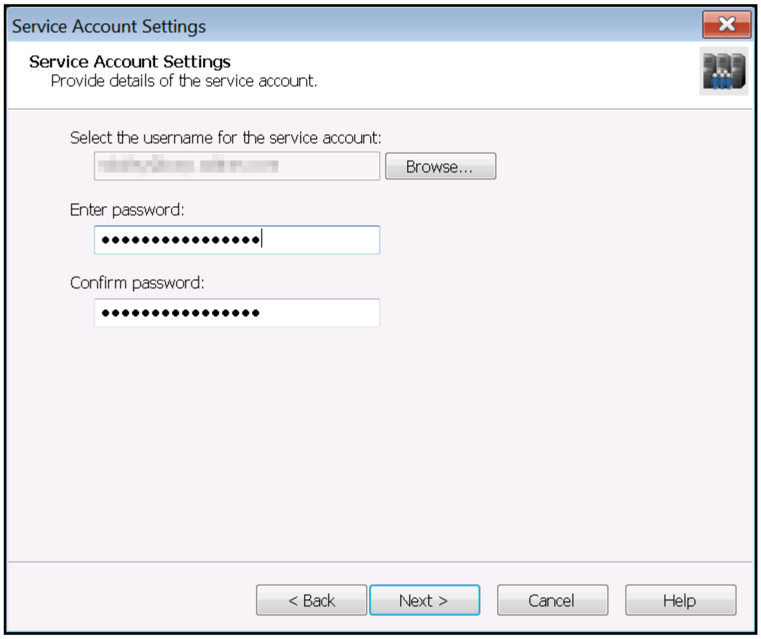
Windows Domain Service Account
Select or create a service account within the Windows Domain

● Existing account
Use another account available within the selected Windows domain

○ Create a new account
Create a new account within the selected Windows domain. You should have administrative rights to perform this action.

Current service log on account: LocalSystem

13. In the **Service Account Settings** menu, select the **Browse** button to browse for the service account you created during *Preparation on page 31*. Once you have chosen the service account, enter the password for the service account in the **Enter password** field, then re-enter the password in the **Confirm password** field. Then, select **Next**.



Service Account Settings

Service Account Settings
Provide details of the service account.

Select the username for the service account: [redacted]

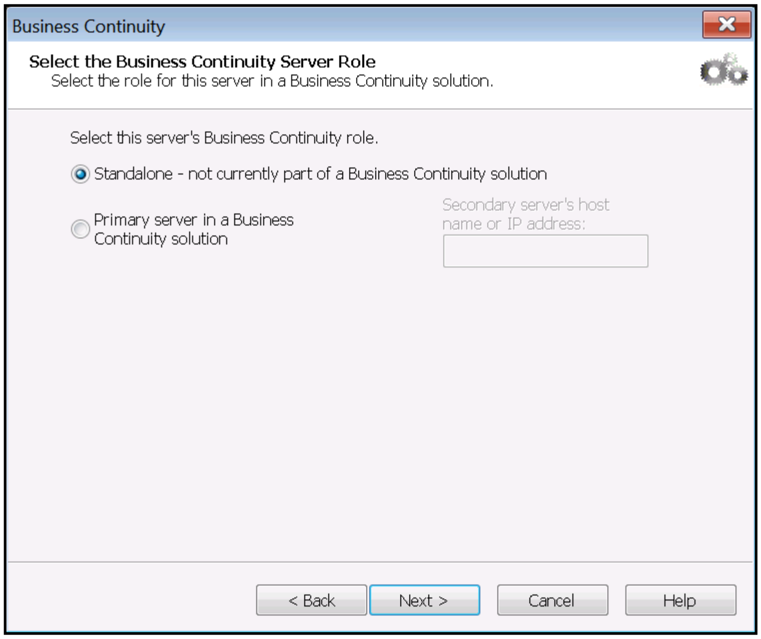
Enter password: ••••••••••••••••

Confirm password: ••••••••••••••••

14. On the summary page that appears, review the options you selected, then select **Submit**.

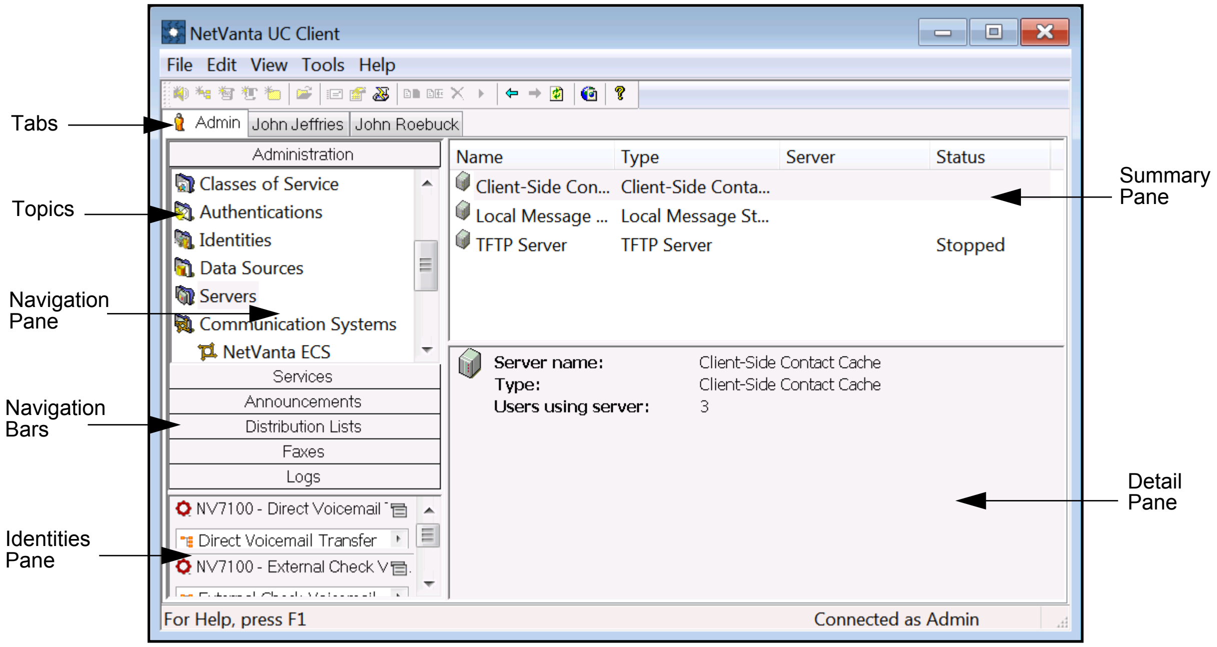
15. The wizard will configure the Windows Firewall and service account. Select **Next** once these tasks have been completed. Then, select **Next** again to exit the **Windows Network Integration Wizard**.

16. Select **Business Continuity** in the **NetVanta UC Server Configuration Wizard** main menu to open the **Business Continuity Wizard**. The **Business Continuity Wizard** menu appears.
17. Select **Next**. The **Select the Business Continuity Server Role** menu appears.
18. In the **Select the Business Continuity Server Role** menu, select **Standalone**. Then, select **Next**.


Business Continuity
Select the Business Continuity Server Role
Select the role for this server in a Business Continuity solution.
Select this server's Business Continuity role.
● Standalone - not currently part of a Business Continuity solution
○ Primary server in a Business Continuity solution
Secondary server's host name or IP address:
< Back
Next >
Cancel
Help

19. On the summary page that appears, review the options you selected, then select **Submit**.
20. The wizard will configure the server's business continuity role. Select **Next** once the task has been completed. Then, select **Next** again to exit the **Business Continuity Wizard**.
21. Exit the **NetVanta UC Server Configuration Wizard**.
22. Log in to the NetVanta UC Client on the primary server as an administrator.
23. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.

24. Select the **Servers** topic from the **Administration** navigation pane.



Name	Type	Server	Status
Client-Side Con...	Client-Side Conta...		
Local Message ...	Local Message St...		
TFTP Server	TFTP Server		Stopped

Server name: Client-Side Contact Cache
Type: Client-Side Contact Cache
Users using server: 3

25. In the **Servers** summary pane, right-click each server object, and select **Track message actions** (if it is available).

Step 3: Create a Network Share on the Primary and Secondary Servers for Copying NetVanta UC Server Data

In order for the Business Continuity Service to copy NetVanta UC Server data from one NetVanta UC Server computer to the other during synchronization, the root directory of the NetVanta UC server installation must be shared on the network. Typically, this directory will be **C:\Program Files (x86)\ADTRAN\NetVanta UC Server**. The share must be created on both the primary and secondary servers. This document uses the share name **UCServerSync**.

> NOTE *The shares created on the primary and secondary servers are not required to have the same name, because the name of the share is specified during business continuity configuration.*

The NetVanta UC Server service account must have at least **Change** and **Read** permissions for this network share. For more information on sharing a folder and setting user permissions for shared folders, refer to the following Microsoft TechNet article http://technet.microsoft.com/en-us/library/cc770406.aspx.

NetVanta UC Server automatically creates a backup folder for storing interim NetVanta UC Server system files, database schema, and database content during synchronization. For NetVanta UC Server upgrades from 5.2.x, the backup folder is **C:\backup**. For new installations of NetVanta UC Server version 5.3.0, the backup folder is **C:\ADTRAN\Backup**.

Step 4: Configure the Windows Firewall for SQL Server Access on the Primary and Secondary Servers

The Business Continuity Service accesses the SQL Server databases used by NetVanta UC Server. In particular, the service on the secondary server accesses the databases on the primary server and vice versa. The Windows Firewall must be configured on each server to allow remote access to SQL server. For more information on configuration the Windows Firewall to allow SQL Server access, refer to *Step 4: Configure the Windows Firewall for SQL Server Access on the Primary and Secondary Servers on page 16*. This section outlines how to configure the Windows Firewall to allow this remote access. These steps must be performed on both the primary and secondary servers. If the firewall is disabled, it is not necessary to configure exceptions to permit remote connections to SQL Server.

Step 5: Enter the Product License Key on the Secondary Server and Begin Configuring the Secondary Server

For instructions on entering the business continuity license key and configuring the secondary server using the **Server Configuration Wizard**, refer to *Step 5: Enter the Product License Key on the Secondary Server and Begin Configuring the Secondary Server on page 18*.

Step 6: Configure Business Continuity on the Primary Server

After configuring the primary and secondary servers using the **Server Configuration Wizard**, you must configure business continuity on the primary server using the NetVanta UC Client. Refer to *Step 7: Configure Business Continuity on the Primary Server on page 25* for instructions on how to configure business continuity on the primary server.

Step 7: Configure Business Continuity on the Secondary Server

After configuring business continuity on the primary server, you must configure business continuity on the secondary server using the NetVanta UC Client. Refer to *Step 6: Configure Business Continuity on the Secondary Server on page 20* for instructions on how to configure business continuity on the secondary server.

Step 8: Manually Synchronize the Secondary Server with the Primary Server

After configuring business continuity on both the primary and secondary servers, an initial, manual synchronization of the secondary server with the primary server must be performed. Refer to *Step 8: Manually Synchronize the Secondary Server with the Primary Server on page 29* for instructions on how to perform the manual synchronization.

Upgrading From a NetVanta UC Server Disaster Recovery Solution

This section provide steps for installing a NetVanta UC Server version 5.3 Business Continuity solution on a system where a NetVanta UC Server Disaster Recovery solution is installed. In this case, NetVanta UC Server is already installed on both the primary and secondary servers. In this procedure, the existing primary server license key is first upgraded to a version 5.3 non-business continuity license key. Then, the primary server NetVanta UC Server software is upgraded to version 5.3 on both the primary and secondary servers. After upgrading the software, the license key is modified on the primary and secondary servers to a business continuity license key. Finally, business continuity is configured on both the primary and secondary servers. The following procedure assumes that the primary and secondary servers have been synchronizing properly.

> NOTE *This upgrade must be performed during a maintenance window.*

Preparation

Select a domain account that will be used as the NetVanta UC Server service account on both the primary and secondary servers. If Exchange Server will be used, this account must have special Exchange Server permissions. For more information on configuring the permissions for the service account, refer to *Configuring Microsoft Exchange 2007 and 2010 Permissions for Integration with NetVanta UC Server* available from the ADTRAN Support Community (https://supportforums.adtran.com).

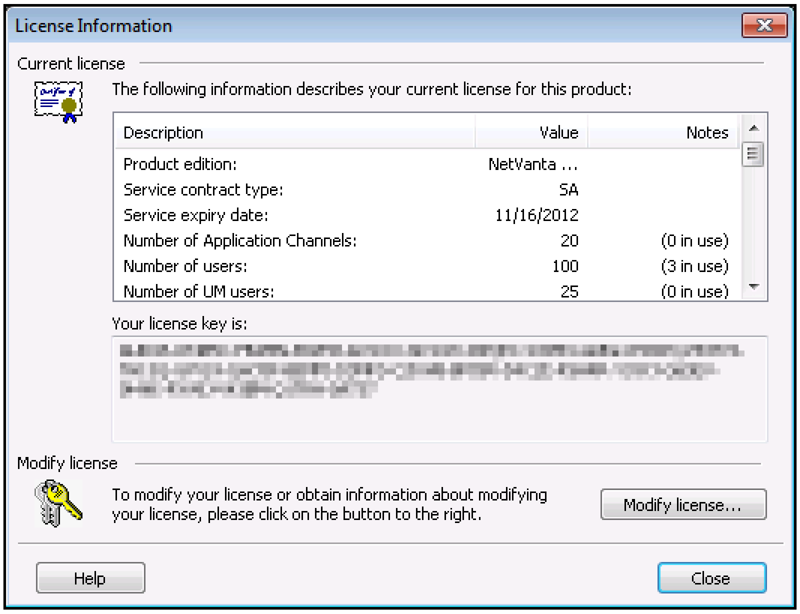
Ensure that the chosen account is a member of the local Administrators group on both systems. You can do this from the **Local users and Groups** section of the **Computer Managemen**t console. The selected account will be called the service accountin the rest of this section.

Step 1: Modify the License Key of the Primary Server

To modify the license key on the primary server to NetVanta UC Server version 5.3, follow these steps:

1. Log in to the NetVanta UC Client on the primary server as an administrator.
2. In the menu bar, select **Help**, then select **License Information** from the drop-down menu. The **License Information** menu will appear.

3. In the **License Information** menu, select **Modify license**. The **Modify License** menu will appear.



The following information describes your current license for this product:

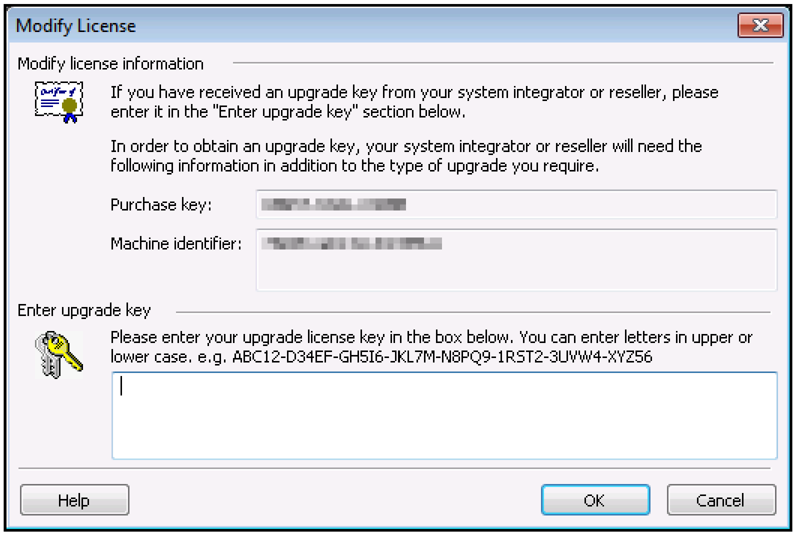
Description	Value	Notes
Product edition:	NetVanta ...	
Service contract type:	SA	
Service expiry date:	11/16/2012	
Number of Application Channels:	20	(0 in use)
Number of users:	100	(3 in use)
Number of UM users:	25	(0 in use)

Your license key is:

[redacted]

To modify your license or obtain information about modifying your license, please click on the button to the right.

4. In the **Modify License** menu, the machine ID for the primary server will appear in the **Machine identifier** field. Use this machine ID to request a NetVanta UC Server version 5.3 license key. Contact ADTRAN technical support to request the license key. You will be asked for the machine ID of the primary server. **Do not request a business continuity license key.** Once you have the license key, enter it in the **Enter upgrade key field** of the **Modify License** menu. Then, select **OK**.



If you have received an upgrade key from your system integrator or reseller, please enter it in the "Enter upgrade key" section below.

In order to obtain an upgrade key, your system integrator or reseller will need the following information in addition to the type of upgrade you require.

Purchase key: [redacted]

Machine identifier: [redacted]

Please enter your upgrade license key in the box below. You can enter letters in upper or lower case. e.g. ABC12-D34EF-GH5I6-JKL7M-N8PQ9-1RST2-3UVW4-XYZ56

Step 2: Upgrade NetVanta UC Server on the Primary and Secondary Servers

To upgrade NetVanta UC Server on the primary and secondary servers to version 5.3, follow these steps:

1. Login to primary server using the service account.

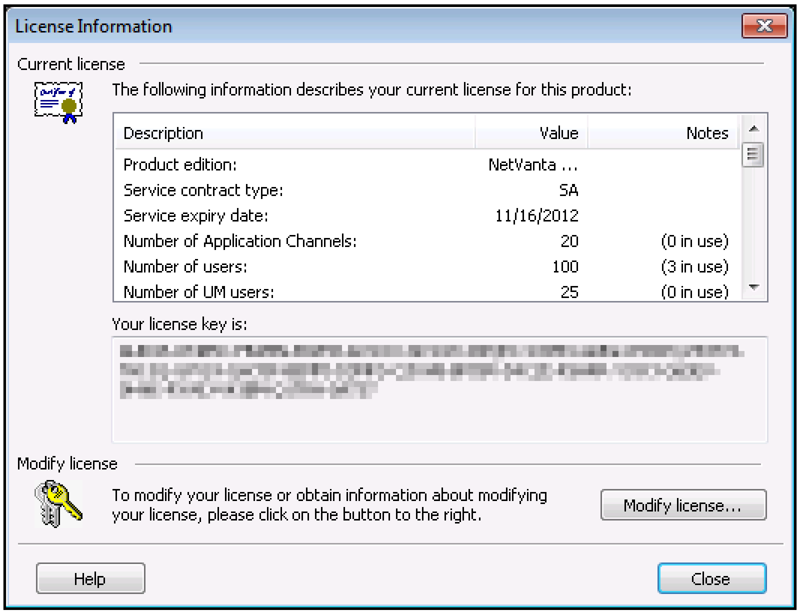
2. Install NetVanta UC Server version 5.3 on the primary server. The current version of NetVanta UC Server software will be upgraded. For more information on installing NetVanta UC Server, refer to the *NetVanta Unified Communications Software Installation Guide* available from the ADTRAN Support Community (https://supportforums.adtran.com). **Do not run the NetVanta UC Server Configuration Wizard.**
3. Log in to the secondary server using the service account.
4. Install the same version of NetVanta UC Server software on the secondary server as was previously installed on the primary server. The current version of NetVanta UC Server software will be upgraded. **Do not run the NetVanta UC Server Configuration Wizard.**

> *The build numbers of the versions of NetVanta UC Server installed on the primary and secondary servers must be identical for server synchronization,*

Step 3: Obtain the Machine ID of the Secondary Server

To obtain the machine IDs of the secondary server, follow these steps:

1. Log in to the NetVanta UC Client on the secondary server as an administrator.
2. In the menu bar, select **Help**, then select **License Information** from the drop-down menu. The **License Information** menu will appear.
3. In the **License Information** menu, select **Modify license**. The **Modify License** menu will appear.



Current license

The following information describes your current license for this product:

Description	Value	Notes
Product edition:	NetVanta ...	
Service contract type:	SA	
Service expiry date:	11/16/2012	
Number of Application Channels:	20	(0 in use)
Number of users:	100	(3 in use)
Number of UM users:	25	(0 in use)

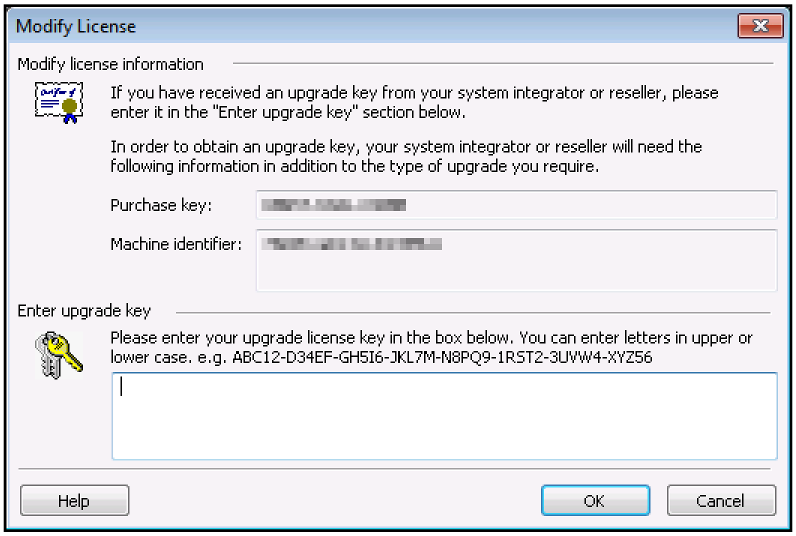
Your license key is:

[redacted]

Modify license

To modify your license or obtain information about modifying your license, please click on the button to the right.

4. In the **Modify License** menu, the machine ID for the secondary server will appear in the **Machine identifier** field. Record this machine ID. It will be used with the primary server machine ID to request a business continuity license key.



Modify License

Modify license information

If you have received an upgrade key from your system integrator or reseller, please enter it in the "Enter upgrade key" section below.

In order to obtain an upgrade key, your system integrator or reseller will need the following information in addition to the type of upgrade you require.

Purchase key: [redacted]

Machine identifier: [redacted]

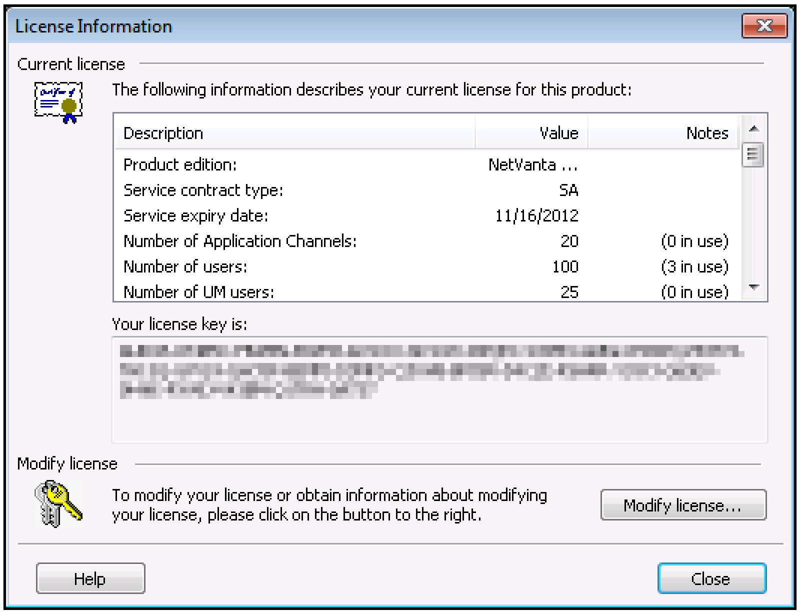
Enter upgrade key

Please enter your upgrade license key in the box below. You can enter letters in upper or lower case. e.g. ABC12-D34EF-GH5I6-JKL7M-N8PQ9-1RST2-3UVW4-XYZ56

Step 4: Modify the Primary Server License Key for Business Continuity

To modify the license key for business continuity on the primary server, follow these steps:

1. Log in to the NetVanta UC Client on the primary server as an administrator.
2. In the menu bar, select **Help**, then select **License Information** from the drop-down menu. The **License Information** menu will appear.
3. In the **License Information** menu, select **Modify license**. The **Modify License** menu will appear.



License Information

Current license

The following information describes your current license for this product:

Description	Value	Notes
Product edition:	NetVanta ...	
Service contract type:	SA	
Service expiry date:	11/16/2012	
Number of Application Channels:	20	(0 in use)
Number of users:	100	(3 in use)
Number of UM users:	25	(0 in use)

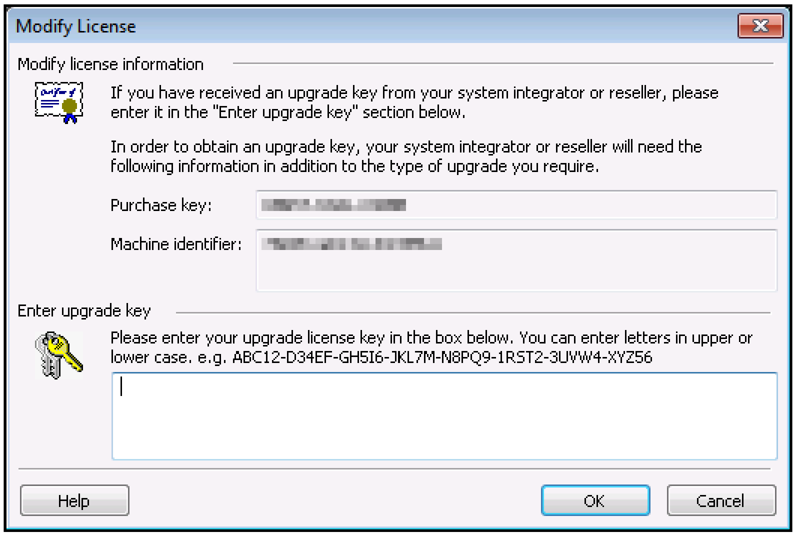
Your license key is:

[redacted]

Modify license

To modify your license or obtain information about modifying your license, please click on the button to the right.

4. In the **Modify License** menu, the machine ID for the primary server will appear in the **Machine identifier** field. Use this machine ID along with the one recorded for the secondary server to request a business continuity license key. Contact ADTRAN technical support to request a business continuity license key. You will be asked for the machine IDs of the primary and secondary servers. Once you have the business continuity license key, enter the license key in the **Enter upgrade key field** of the **Modify License** menu. Then, select **OK**.



Modify license information

If you have received an upgrade key from your system integrator or reseller, please enter it in the "Enter upgrade key" section below.

In order to obtain an upgrade key, your system integrator or reseller will need the following information in addition to the type of upgrade you require.

Purchase key: [redacted]

Machine identifier: [redacted]

Enter upgrade key

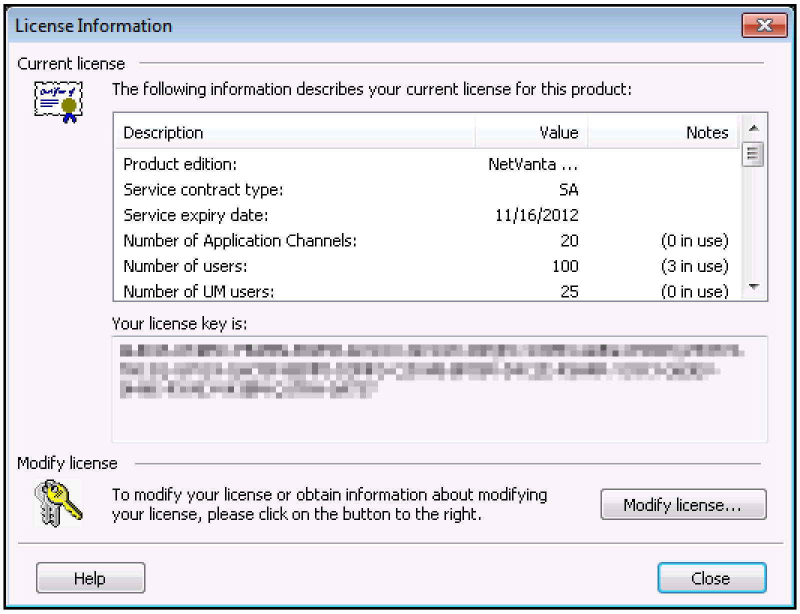
Please enter your upgrade license key in the box below. You can enter letters in upper or lower case. e.g. ABC12-D34EF-GH5I6-JKL7M-N8PQ9-1RST2-3UVW4-XYZ56

Step 5: Modify the Secondary Server License Key for Business Continuity

To modify the license key for business continuity on the secondary server, follow these steps:

1. Log in to the NetVanta UC Client on the secondary server as an administrator.
2. In the menu bar, select **Help**, then select **License Information** from the drop-down menu. The **License Information** menu will appear.

3. In the **License Information** menu, select **Modify license**. The **Modify License** menu will appear.



License Information

Current license

The following information describes your current license for this product:

Description	Value	Notes
Product edition:	NetVanta ...	
Service contract type:	SA	
Service expiry date:	11/16/2012	
Number of Application Channels:	20	(0 in use)
Number of users:	100	(3 in use)
Number of UM users:	25	(0 in use)

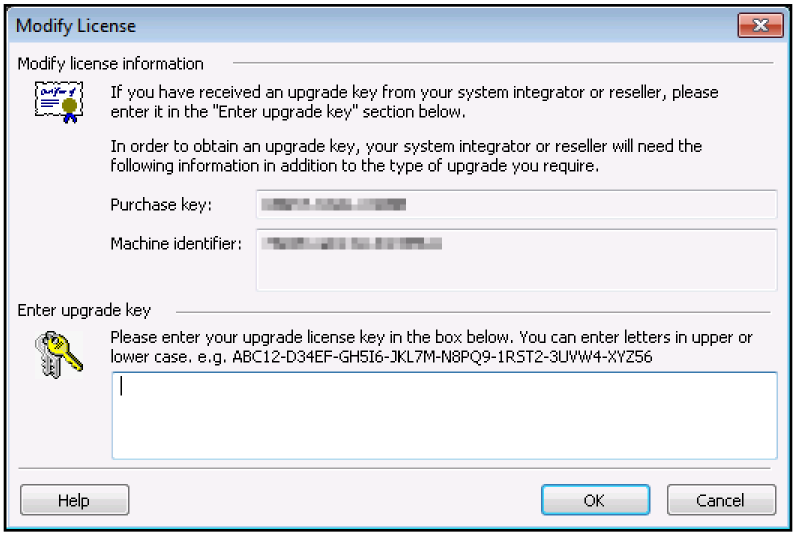
Your license key is:

[redacted]

Modify license

To modify your license or obtain information about modifying your license, please click on the button to the right.

4. In the **Modify License** menu, enter the business continuity license key in the **Enter upgrade key field** of the **Modify License** menu. Then, select **OK**.



Modify License

Modify license information

If you have received an upgrade key from your system integrator or reseller, please enter it in the "Enter upgrade key" section below.

In order to obtain an upgrade key, your system integrator or reseller will need the following information in addition to the type of upgrade you require.

Purchase key: [redacted]

Machine identifier: [redacted]

Enter upgrade key

Please enter your upgrade license key in the box below. You can enter letters in upper or lower case. e.g. ABC12-D34EF-GH5I6-JKL7M-N8PQ9-1RST2-3UVW4-XYZ56

Step 6: Create a Network Share on the Primary and Secondary Servers for Copying NetVanta UC Server Data

> NOTE
>
> *A network share at the root directory of the NetVanta UC Server installation should have been created on both the primary and secondary servers as a part of the Disaster Recovery solution installation. If this network share is present, it can be reused for business continuity. However, you must ensure that the NetVanta UC Server service account has* ***Change*** *and* ***Read*** *permissions for the network shares. If appropriate network shares do not exist on the servers, they must be created. This section provides instructions for creating network shares for business continuity synchronization.*

In order for the Business Continuity Service to copy NetVanta UC Server data from one NetVanta UC Server computer to the other during synchronization, the root directory of the NetVanta UC server installation must be shared on the network. Typically, this directory will be **C:\Program Files (x86)\ADTRAN\NetVanta UC Server**. The share must be created on both the primary and secondary servers. This document uses the share name **UCServerSync**.

> NOTE
>
> *The shares created on the primary and secondary servers are not required to have the same name, because the name of the share is specified during business continuity configuration.*

The NetVanta UC Server service account must have at least **Change** and **Read** permissions for this network share. For more information on sharing a folder and setting user permissions for shared folders, refer to the following Microsoft TechNet article http://technet.microsoft.com/en-us/library/cc770406.aspx.

NetVanta UC Server automatically creates a backup folder for storing interim NetVanta UC Server system files, database schema, and database content during synchronization. For NetVanta UC Server upgrades from 5.2.x, the backup folder is **C:\backup**. For new installations of NetVanta UC Server version 5.3.0, the backup folder is **C:\ADTRAN\Backup**.

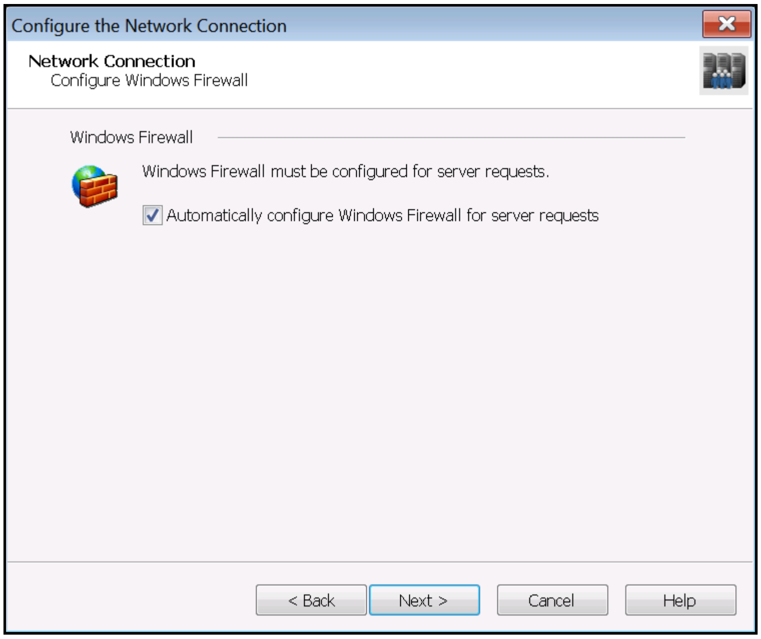
Step 7: Configure the Windows Firewall for SQL Server Access on the Primary and Secondary Servers

The Business Continuity Service accesses the SQL Server databases used by NetVanta UC Server. In particular, the service on the secondary server accesses the databases on the primary server and vice versa. The Windows Firewall must be configured on each server to allow remote access to SQL server. For more information on configuration the Windows Firewall to allow SQL Server access, refer to *Step 4: Configure the Windows Firewall for SQL Server Access on the Primary and Secondary Servers on page 16*. This section outlines how to configure the Windows Firewall to allow this remote access. These steps must be performed on both the primary and secondary servers. If the firewall is disabled, it is not necessary to configure exceptions to permit remote connections to SQL Server.

Step 8: Configure the Primary Server using the Server Configuration Wizard

To configure the primary server using the Server Configuration Wizard, follow these steps:

1. Log in to the primary server using the service account.
2. In the Windows Start menu, navigate to **Programs > ADTRAN > NetVanta UC Server** > **NetVanta UC Server Configuration Wizard**. The **NetVanta UC Server Configuration Wizard** main menu appears.
3. On the main menu, select **Product Licensing** to open the **Product Licensing Wizard**. All of the licensing information for the primary server was configured earlier in *Step 4: Modify the Primary Server License Key for Business Continuity on page 42*, and should already be entered in the appropriate fields. Select **Next**.
4. In the NetVanta UC Server Configuration Wizard main menu, select **Windows Network Integration** to open the **Windows NetWork Integration Wizard**. The **Windows Network Integration Wizard** menu appears.
5. Select **Next**. The **Network Connection** menu appears.
6. In the **Network Connection** menu, ensure that the checkbox next to **Automatically configure Windows Firewall for server requests** is checked. Then, select **Next**. The **Configure the Windows Integration** menu appears.


Configure the Network Connection

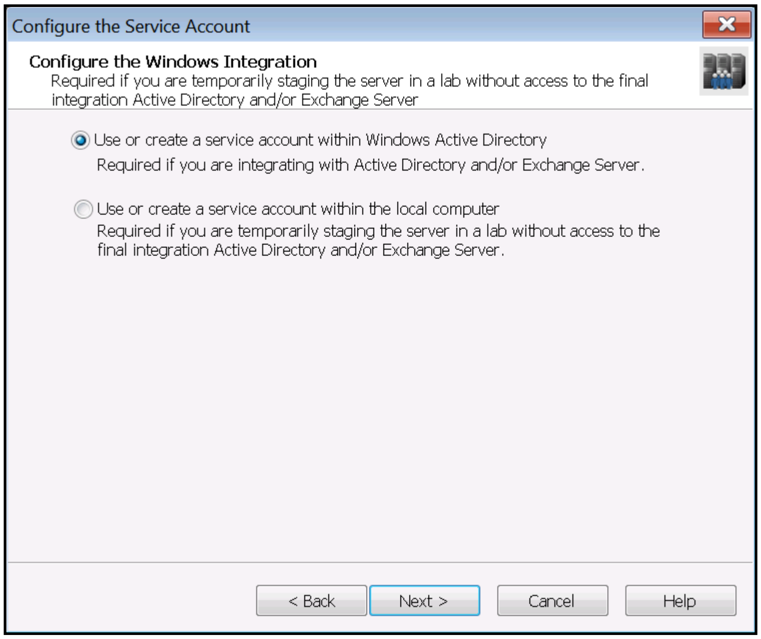
Network Connection
Configure Windows Firewall

Windows Firewall

Windows Firewall must be configured for server requests.

☑ Automatically configure Windows Firewall for server requests

7. In the **Configure the Windows Integration** menu, select the **Use or create a service account within Windows Active Directory** radio button. Then, select **Next**. The **Windows Domain Service Account** menu appears.



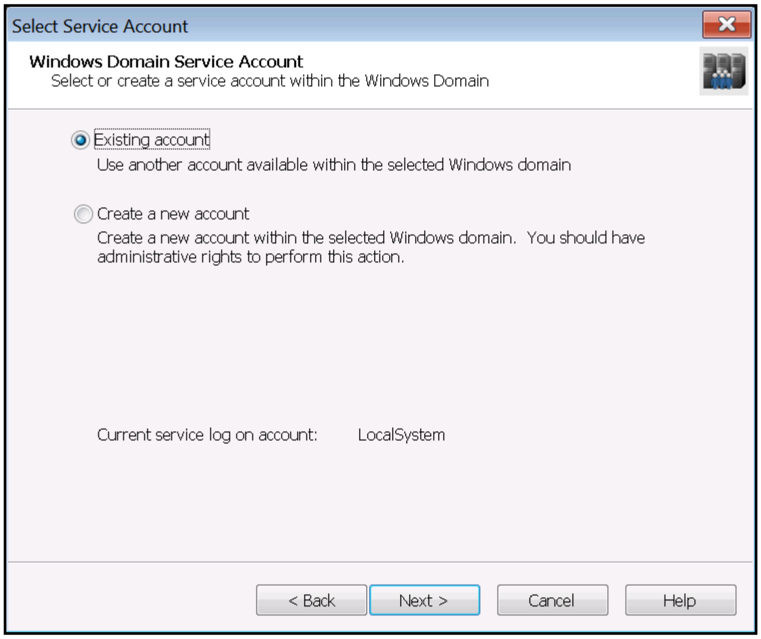
Configure the Service Account

Configure the Windows Integration
Required if you are temporarily staging the server in a lab without access to the final integration Active Directory and/or Exchange Server

● Use or create a service account within Windows Active Directory
Required if you are integrating with Active Directory and/or Exchange Server.

○ Use or create a service account within the local computer
Required if you are temporarily staging the server in a lab without access to the final integration Active Directory and/or Exchange Server.

8. In the **Select Service Account**, select the **Existing account** radio button. Then, select **Next**. The **Service Account Settings** menu appears.



Select Service Account

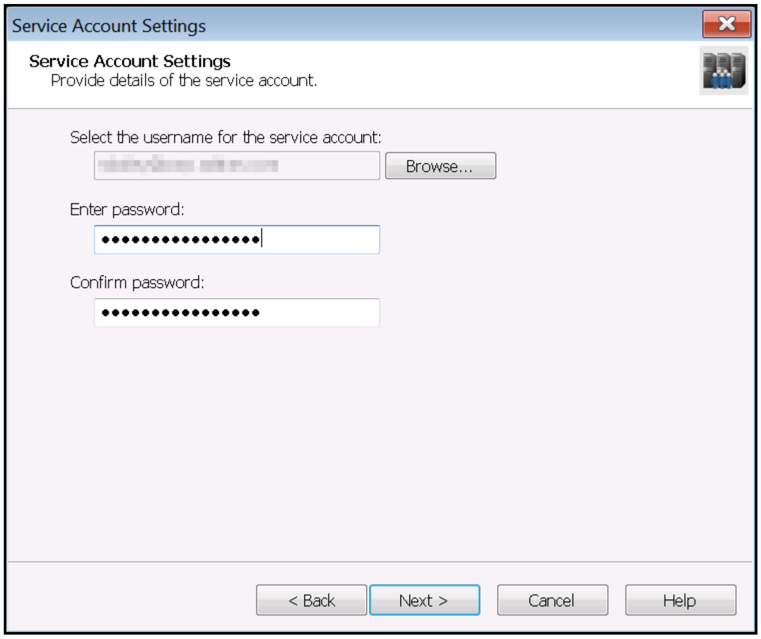
Windows Domain Service Account
Select or create a service account within the Windows Domain

● Existing account
Use another account available within the selected Windows domain

○ Create a new account
Create a new account within the selected Windows domain. You should have administrative rights to perform this action.

Current service log on account: LocalSystem

9. In the **Service Account Settings** menu, select the **Browse** button to browse for the service account you created during *Preparation on page 39*. Once you have chosen the service account, enter the password for the service account in the **Enter password** field, then re-enter the password in the **Confirm password** field. Then, select **Next**.



Service Account Settings

Service Account Settings
Provide details of the service account.

Select the username for the service account: [redacted]

Enter password: ••••••••••••••••

Confirm password: ••••••••••••••••

10. On the summary page that appears, review the options you selected, then select **Submit**.

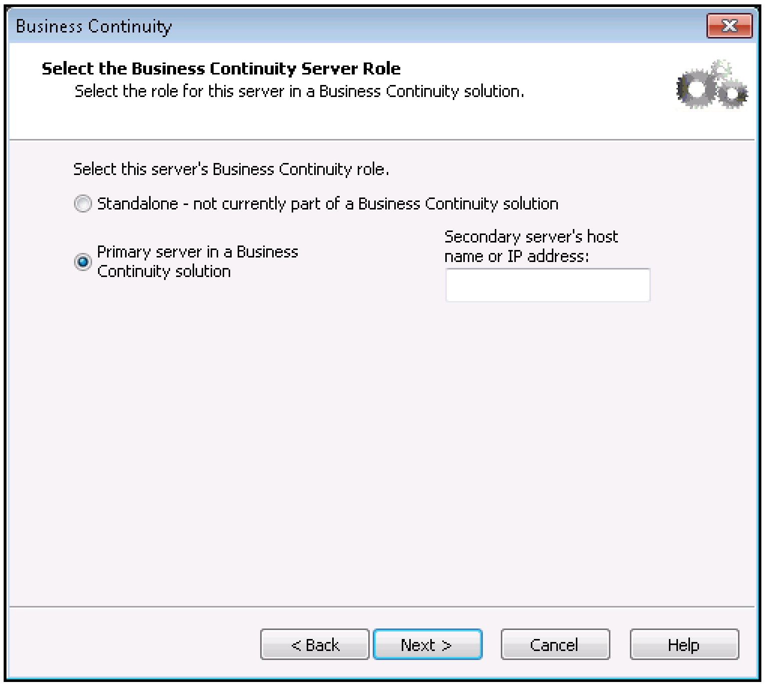
11. The wizard will configure the Windows Firewall and service account. Select **Next** once these tasks have been completed. Then, select **Next** again to exit the **Windows Network Integration Wizard**.

12. Use the **Communication Systems** and **Phone Types** wizards in the **NetVanta UC Server Configuration Wizard** to configure the communication systems and phone types that will be used with NetVanta UC Server. For more information on using the wizards available in the **NetVanta UC Server Configuration Wizard**, refer to the *NetVanta Unified Communications Server Configuration Guide* for your version of NetVanta UC Server available from the ADTRAN Support Community (https://supportforums.adtran.com).

13. Once you are able to access it, select **Business Continuity** in the **NetVanta UC Server Configuration Wizard** main menu to open the **Business Continuity Wizard**. The **Business Continuity Wizard** menu appears.

14. Select **Next**. The **Select the Business Continuity Server Role** menu appears.

15. In the **Select the Business Continuity Server Role** menu, select **primary server in a Business Continuity Solution**, and enter the fully qualified domain name (FQDN) or IP address of the primary server in the **Primary server's host name or IP address field**. Then, select **Next**.


Business Continuity

Select the Business Continuity Server Role

Select the role for this server in a Business Continuity solution.

Select this server's Business Continuity role.

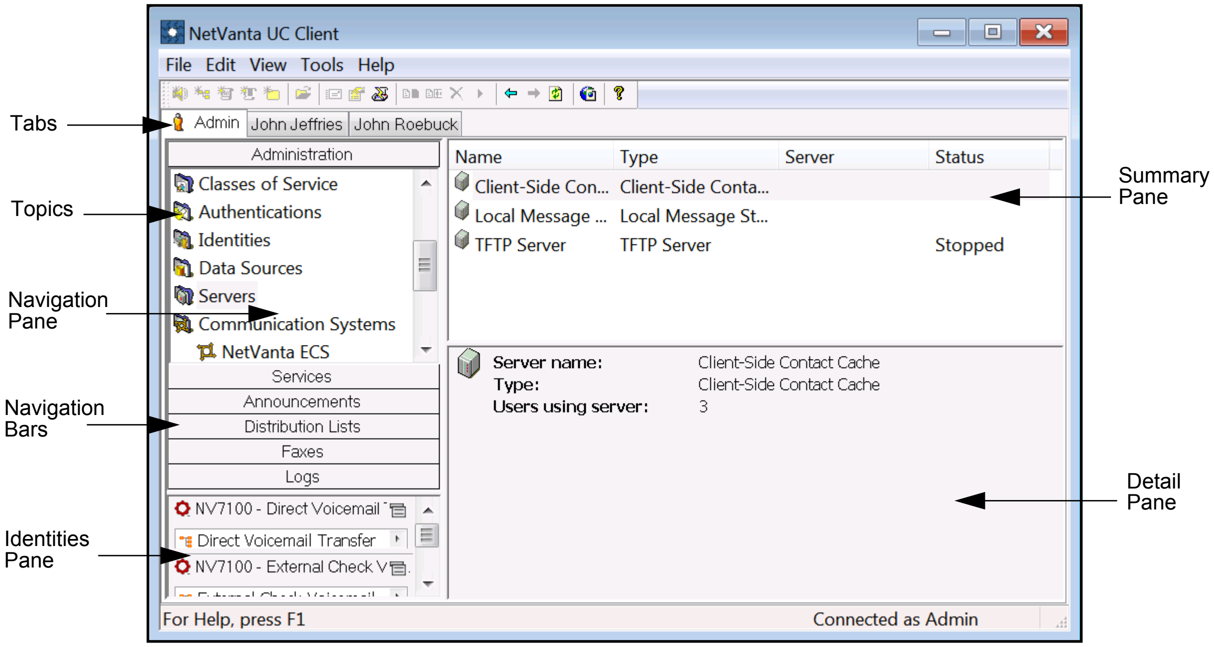
○ Standalone - not currently part of a Business Continuity solution

● Primary server in a Business Continuity solution

Secondary server's host name or IP address:

16. On the summary page that appears, review the options you selected, then select **Submit**.
17. The wizard will configure the server's business continuity role. Select **Next** once the task has been completed. Then, select **Next** again to exit the **Business Continuity Wizard**.
18. Continue to use the NetVanta UC Server Configuration Wizard to configure the primary NetVanta UC Server. For more information on using the wizards available in the **NetVanta UC Server Configuration Wizard**, refer to the *NetVanta Unified Communications Server Configuration Guide* for your version of NetVanta UC Server available from the ADTRAN Support Community (https://supportforums.adtran.com).
19. After you have completed all of the wizards available in the **NetVanta UC Server Configuration Wizard**, log in to the NetVanta UC Client as an administrator.
20. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.

21. Select the **Servers** topic from the **Administration** navigation pane.



Name	Type	Server	Status
Client-Side Con...	Client-Side Conta...		
Local Message ...	Local Message St...		
TFTP Server	TFTP Server		Stopped

Server name: Client-Side Contact Cache
Type: Client-Side Contact Cache
Users using server: 3

22. In the **Servers** summary pane, right-click each server object, and select **Track message actions** (if it is available).

Step 9: Configure the Secondary Server using the Server Configuration Wizard

To configure the secondary server using the Server Configuration Wizard, follow these steps:

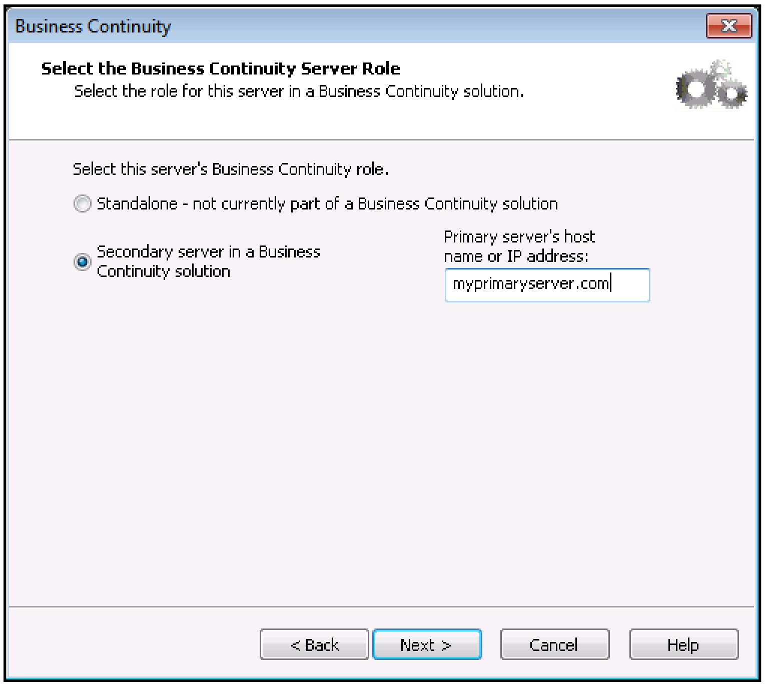
1. Log in to the secondary server using the service account.
2. In the Windows Start menu, navigate to **Programs > ADTRAN > NetVanta UC Server** > **NetVanta UC Server Configuration Wizard**. The **NetVanta UC Server Configuration Wizard** main menu appears.
3. In the **NetVanta UC Server Configuration Wizard** main menu, select **Product Licensing** to open the **Product Licensing Wizard**. All of the licensing information for the primary server was configured earlier in *Step 4: Modify the Primary Server License Key for Business Continuity on page 42*, and should already be entered in the appropriate fields. Select **Next**.
4. In the **NetVanta UC Server Configuration Wizard** main menu, select Windows Network Integration to open the **Windows NetWork Integration Wizard**. The **Windows Network Integration Wizard** menu appears.
5. Select **Next**. The **Network Connection** menu appears.
6. In the **Network Connection** menu, ensure that the checkbox next to **Automatically configure Windows Firewall for server requests** is checked. Then, select **Next**. The **Configure the Windows Integration** menu appears.
7. In the **Configure the Windows Integration** menu, select the **Use or create a service account within Windows Active Directory** radio button. Then, select **Next**. The **Windows Domain Service Account** menu appears.

8. In the **Select Service Account**, select the **Existing account** radio button. Then, select **Next**. The **Service Account Settings** menu appears.
9. In the **Service Account Settings** menu, select the **Browse** button to browse for the service account you created during *Preparation on page 8*. This must be the same service account as the one used on the primary server. Once you have chosen the service account, enter the password for the service account in the **Enter password** field, then re-enter the password in the **Confirm password** field. Once you have finished selecting the service account and entering the password, select **Next**.
10. On the summary page that appears, review the options you selected, then select **Submit**.
11. The wizard will configure the Windows Firewall and service account. Select **Next** once these tasks have been completed. Then, select **Next** again to exit the **Windows Network Integration Wizard**.
12. Use the **Communication Systems** and **Phone Types** wizards in the **NetVanta UC Server Configuration Wizard** to configure the communication systems and phone types that will be used with NetVanta UC Server. The communication systems and phone types defined on the secondary server must match those defined earlier on the primary server in *Step 8:Configure the Primary Server using the Server Configuration Wizard*. For more information on using the wizards available in the **NetVanta UC Server Configuration Wizard**, refer to the *NetVanta Unified Communications Server Configuration Guide* for your version of NetVanta UC Server available from the ADTRAN Support Community (https://supportforums.adtran.com).

> NOTE *If a NetVanta ECS communication system was defined on the primary server using the Communication Systems wizard, a matching NetVanta ECS communication system also must be configured on the secondary server. For more information on managing NetVanta ECS communication systems, refer to Appendix C – NetVanta ECS Communication System Considerations on page 63.*

13. Once you are able to access it, select **Business Continuity** in the **NetVanta UC Server Configuration Wizard** main menu to open the **Business Continuity Wizard**. The **Business Continuity Wizard** menu appears.
14. Select **Next**. The **Select the Business Continuity Server Role** menu appears.

15. In the **Select the Business Continuity Server Role** menu, select **secondary server in a Business Continuity Solution**, and enter the fully qualified domain name (FQDN) or IP address of the primary server in the **Primary server's host name or IP address field**. Then, select **Next**.



Business Continuity

Select the Business Continuity Server Role

Select the role for this server in a Business Continuity solution.

Select this server's Business Continuity role.

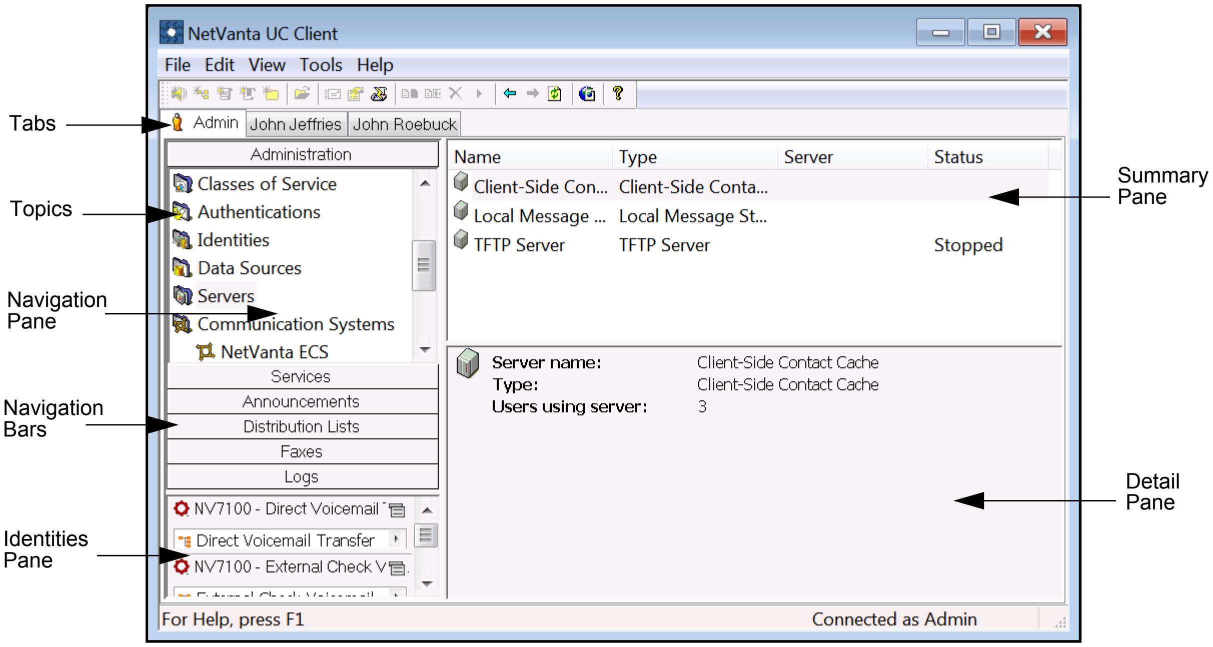
○ Standalone - not currently part of a Business Continuity solution

● Secondary server in a Business Continuity solution

Primary server's host name or IP address: myprimaryserver.com

16. On the summary page that appears, review the options you selected, then select **Submit**.
17. The wizard will configure the server's business continuity role and the FQDN or IP address of the primary server. Select **Next** once the task has been completed. Then, select **Next** again to exit the **Business Continuity Wizard**.
18. After you have completed all of the wizards available in the **NetVanta UC Server Configuration Wizard**, log in to the NetVanta UC Client as an administrator.
19. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.

20. Select the **Servers** topic from the **Administration** navigation pane.



Name	Type	Server	Status
Client-Side Con...	Client-Side Conta...		
Local Message ...	Local Message St...		
TFTP Server	TFTP Server		Stopped

Server name: Client-Side Contact Cache
Type: Client-Side Contact Cache
Users using server: 3

21. In the **Servers** summary pane, right-click each server object, and select **Track message actions** (if it is available).

Step 10: Configure Business Continuity on the Primary Server

After configuring the primary and secondary servers using the **Server Configuration Wizard**, you must configure business continuity on the primary server using the NetVanta UC Client. Refer to *Step 7: Configure Business Continuity on the Primary Server on page 25* for instructions on how to configure business continuity on the primary server.

Step 11: Configure Business Continuity on the Secondary Server

After configuring business continuity on the primary server, you must configure business continuity on the secondary server using the NetVanta UC Client. Refer to *Step 6: Configure Business Continuity on the Secondary Server on page 20* for instructions on how to configure business continuity on the secondary server.

Step 12: Manually Synchronize the Secondary Server with the Primary Server

After configuring business continuity on both the primary and secondary servers, an initial, manual synchronization of the secondary server with the primary server must be performed. Refer to *Step 8: Manually Synchronize the Secondary Server with the Primary Server on page 29* for instructions on how to perform the manual synchronization.

Appendix A - Using NetVanta UC Client on the Secondary Server

After configuring business continuity, the secondary server will be licensed as a secondary server. Consequently, the NetVanta UC Client on the secondary server can only be used to access the administrator's profile, and most updates to the secondary server from the NetVanta UC Client are not allowed. Configuration of the system should always be performed on the primary server. The Business Continuity Service will ensure that updates made on the primary server are synchronized to the secondary server.

Administrator's are still able to perform some tasks from the secondary server. For example, it is possible to log in as an administrator and view the objects (users, phones, servers, etc.) that exist on the secondary NetVanta UC Server and their attributes.

Although most updates are not permitted, three kinds of updates can be performed by administrators in the NetVanta UC Client on the secondary server:

- The server role of the secondary server can be changed.
- The license key can be modified.
- The configuration of the Business Continuity Service on the secondary server can be changed.

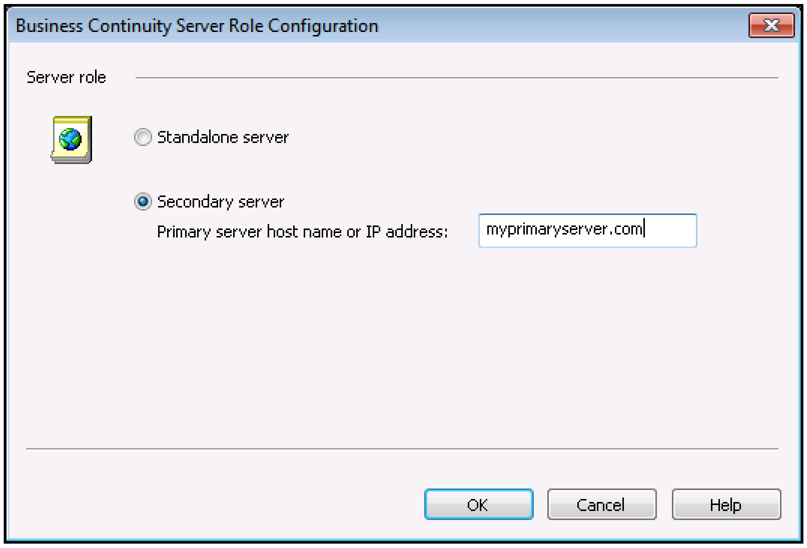
The first two actions are used when there is an extended failure of the primary server (see *Appendix D - Handling an Extended Failure of the Primary Server on page 66*). The third action permits ongoing configuration of the Business Continuity Service.

Changing the Role of the Secondary Server

To change the role of the secondary server, follow these steps:

1. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.
2. Select the **Servers** topic from the **Administration** navigation pane.
3. Right-click in the **Servers** summary pane, and select **UC Server Role**. The **Business Continuity Server Role Configuration** menu appears.

4. Use the available radio buttons to change the business continuity server role of the secondary server. Then, select **OK**.



○ Standalone server

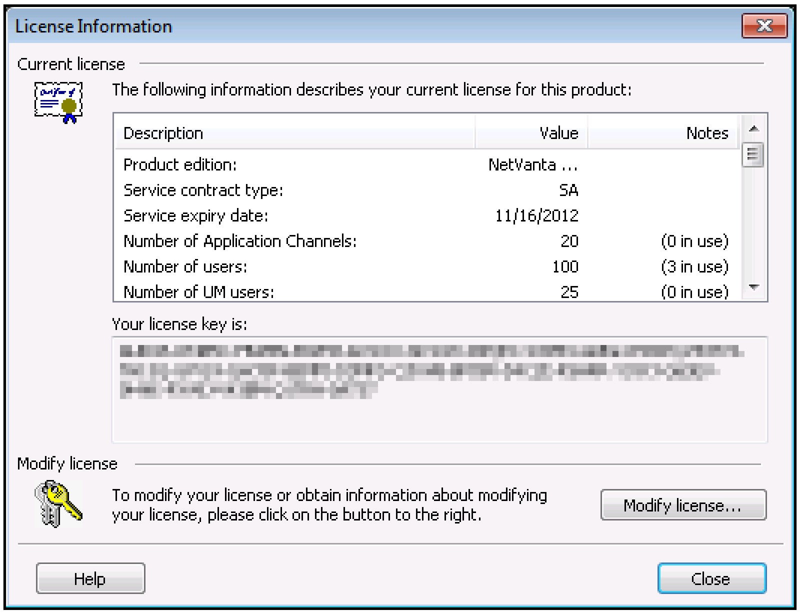
● Secondary server

Primary server host name or IP address: myprimaryserver.com

Modifying the License Key of the Secondary Server

To modify the license key of the secondary server, follow these steps:

1. Log in to the NetVanta UC Client as an administration.
2. Select the **Admin** tab in the NetVanta UC Client.
3. Select **Help** in the menu bar, then select **License Information** from the drop-down menu. The **License Information** menu will appear.
4. In the **License Information** menu, select **Modify license**. The **Modify License** menu will appear.



The following information describes your current license for this product:

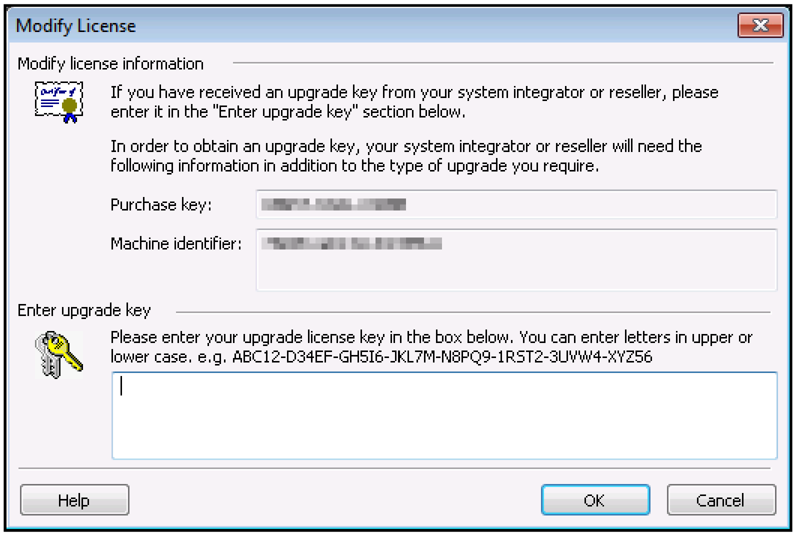
Description	Value	Notes
Product edition:	NetVanta ...	
Service contract type:	SA	
Service expiry date:	11/16/2012	
Number of Application Channels:	20	(0 in use)
Number of users:	100	(3 in use)
Number of UM users:	25	(0 in use)

Your license key is:

[redacted]

To modify your license or obtain information about modifying your license, please click on the button to the right.

5. In the **Enter upgrade key** field of the **Modify License** menu, enter the new product license key that you requested using the primary and secondary server machine IDs. Then, select **OK**.



If you have received an upgrade key from your system integrator or reseller, please enter it in the "Enter upgrade key" section below.

In order to obtain an upgrade key, your system integrator or reseller will need the following information in addition to the type of upgrade you require.

Purchase key: [redacted]

Machine identifier: [redacted]

Please enter your upgrade license key in the box below. You can enter letters in upper or lower case. e.g. ABC12-D34EF-GH5I6-JKL7M-N8PQ9-1RST2-3UVW4-XYZ56

Changing the Business Continuity Service Configuration on the Secondary Server

For more information on changing the configuration of the Business Continuity Service on the secondary server, refer to *Step 6: Configure Business Continuity on the Secondary Server on page 20*.

Appendix B - Simplifying Phone Management

To provide failover for phone service in a business continuity solution, phones that are capable of dual registration should be registered with both the primary and secondary servers, and all other phones should be placed behind an outbound proxy. The phone class of service (CoS) feature available in NetVanta UC Server version 5.3 can be used to quickly configure multiple phones to register appropriately for failover support. To simplify phone failover management, a phone CoS should be created for phones capable of dual registration. Additionally, a phone CoS should be created for each SIP proxy server used for phones that are not capable of dual registration.

Configuring a Phone CoS

The phone CoS feature is used to quickly apply common attributes to one or more phones. For example, it can be used to configure multiple phones to register with a secondary NetVanta UC Server or a SIP proxy server to allow failover support in business continuity installations.

NOTE

Only phones that support dual registration can register with a secondary NetVanta UC Server.

The phone CoS features can be applied to multiple phones, or each feature can be configured individually on a per-phone basis without using the CoS. However, a CoS and an individual configuration cannot be applied to a single phone at the same time. If a CoS is applied to the phone, individual settings cannot be applied to override specific aspects of the CoS. If a different variation of settings is necessary, the phone either must be individually configured, or a new CoS with the desired settings must be created and applied to that phone.

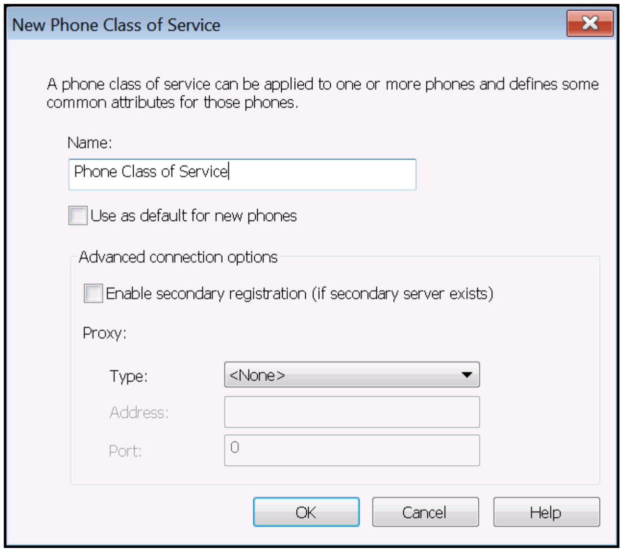
When adding a new phone to the NetVanta UC Server system, the default CoS is available to all phones. The **Standard Phones** CoS is available as the phone's CoS default during a new installation or a system upgrade of the NetVanta UC Server. If another CoS has been configured, it is also available during a new installation or system upgrade. If another CoS is set as the default, then it will be available as the default CoS to all new phones. If the default CoS does not exist, then the **None** CoS is available for all phones.

Creating a Phone CoS

To create a new phone CoS, follow these steps:

1. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.

2. Right-click on the **Classes of Service** topic in the **Administration** navigation pane and select **New Phone Class of Service** from the drop-down menu. You can also create a new phone CoS by selecting the **Classes of Service** topic in the **Administration** navigation pane and right-clicking on the summary pane. Select **New Phone Class of Service** from the drop-down menu. The **New Phone Class of Service** menu appears.



New Phone Class of Service

A phone class of service can be applied to one or more phones and defines some common attributes for those phones.

Name: Phone Class of Service

□ Use as default for new phones

Advanced connection options

□ Enable secondary registration (if secondary server exists)

Proxy:

Type: <None>

Address:

Port: 0

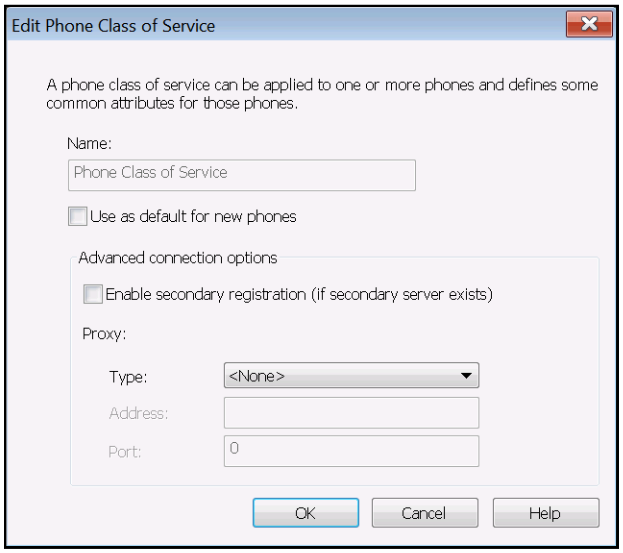
3. Specify the name for the CoS in the **Name** field of the **New Phone Class of Service** menu. The name should be a unique identifier specifically for this CoS.
4. Select the check box next to **Use as default for new phones** if you want this phone CoS to be the default CoS for all new phones added to the system.
5. You can select **OK** to save the phone CoS with the default settings, or you can continue to edit the **Advanced connection options**. For more information on configuring the **Advanced connection options**, refer to *Configuring the Advanced Connection Options on page 59*
6. After you have finished configuring the phone CoS settings, select **OK** to save the phone CoS.

Editing an Existing Phone CoS

If you would like to make changes to an existing phone CoS, follow these steps:

1. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.
2. Select the **Classes of Service** topic from the list.

3. In the summary pane, double-click on the phone CoS that you would like to edit. The **Edit Phone Class of Service** menu appears.



Edit Phone Class of Service

A phone class of service can be applied to one or more phones and defines some common attributes for those phones.

Name: Phone Class of Service

□ Use as default for new phones

Advanced connection options

□ Enable secondary registration (if secondary server exists)

Proxy:

Type: <None>

Address:

Port: 0

4. You can select **OK** to save the phone CoS with the default settings, or you can continue to edit the **Advanced connection options**. For more information on configuring the Advance connection options, refer to *Configuring the Advanced Connection Options on page 59*.
5. After you have finished configuring the phone CoS settings, select **OK** to save the phone CoS.

Configuring the Advanced Connection Options

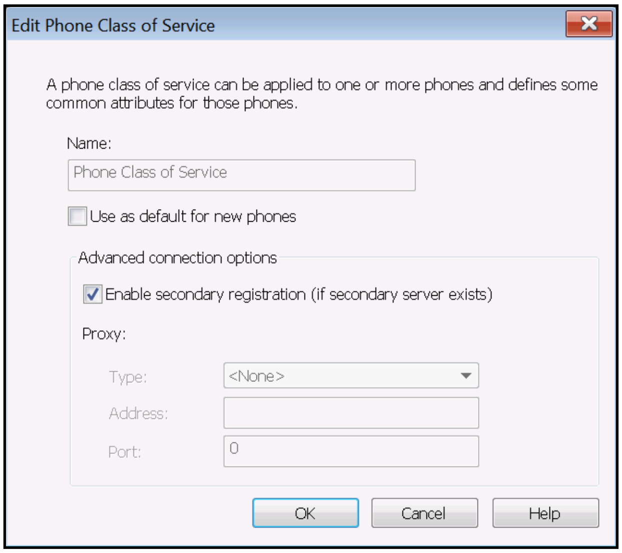
In order to provide business continuity failover support, phones must be able to redirect to the secondary NetVanta UC Server in the event the primary NetVanta UC Server fails. This is accomplished using the advanced connection options. When configuring the CoS advanced connection options, you can specify whether phones register with a secondary NetVanta UC Server or a SIP proxy server. If a SIP proxy server is used, the SIP proxy will forward the SIP packets to the secondary server in case the primary server fails.

NOTE *If you are using a SIP proxy, it must be aware of both the primary and secondary NetVanta UC Servers, and it must be configured to reroute the SIP packets from the phones based on which NetVanta UC Server is operational.*

Enabling Secondary Registration

To enable registration to the secondary NetVanta UC Server for phones in this CoS, select the **Enable secondary registration (if secondary server exists)** check box. The phones with this CoS applied will dual register with both the primary and secondary NetVanta UC Servers.

NOTE *Only phones that support dual registration can register with a secondary NetVanta UC Server.*



Edit Phone Class of Service

A phone class of service can be applied to one or more phones and defines some common attributes for those phones.

Name: Phone Class of Service

□ Use as default for new phones

Advanced connection options

☑ Enable secondary registration (if secondary server exists)

Proxy:

Type: <None>

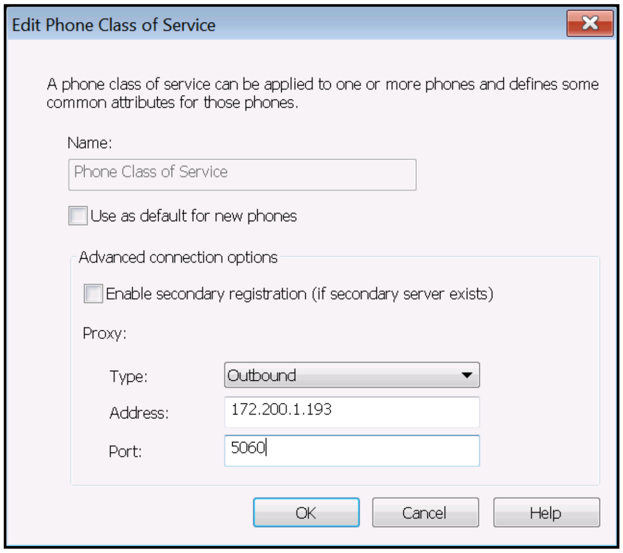
Address:

Port: 0

Configuring SIP Proxy Registration

To configure the phones in this CoS to register to a SIP proxy server, follow these steps:

1. Use the **Type** drop-down menu to select either **Stateful** or **Outbound** for the SIP proxy type. This is the type of SIP proxy server to which the phones will register.



Edit Phone Class of Service

A phone class of service can be applied to one or more phones and defines some common attributes for those phones.

Name: Phone Class of Service

□ Use as default for new phones

Advanced connection options

□ Enable secondary registration (if secondary server exists)

Proxy:

Type: Outbound

Address: 172.200.1.193

Port: 5060

> NOTE *In business continuity solutions, a stateful SIP proxy should be used, as outbound SIP proxies only provide local failover support.*

2. In the **Address** field, enter one of the following:
   - For **Outbound** proxy server types, enter the IP address of the outbound SIP proxy server.
   - For **Stateful** proxy server types, enter the host name of the stateful SIP proxy server.
3. In the **Port** field, enter the port on the SIP proxy server to which the phones will register.
4. Select **OK** to apply the settings and save the changes to the CoS.

Apply the CoS to Phones

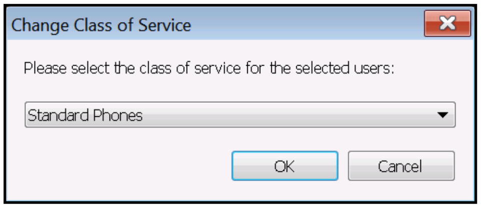
Once the phone CoS is created, it can be applied to phones in a number of ways. You can apply the CoS to multiple or individual phones already configured on the system or to phones as they are added to the system. The following sections outline the different methods of applying a phone CoS.

Applying the CoS to Phones Already in the System

To apply a configured phone CoS to existing phones, follow these steps:

1. Select the **Phones** topic from the list in the **Administration** navigation pane.

2. In the **Phone** summary pane, select the phone to which you want to apply the CoS. To select multiple phones, hold down the Shift key while making your selection. Once you have selected the phones to which you want to apply the CoS, right-click in the highlighted area and select **Change Class of Service** from the drop-down menu. The **Change Class of Service** menu appears.



Change Class of Service

Please select the class of service for the selected users:

Standard Phones

3. From the **Change Class of Service** menu, select the desired CoS from the drop-down menu.

4. Select **OK**. The **Class of service** field in the **Phones** summary pane displays each phone's assigned CoS.

NOTE *You can also change a phone's CoS assignment in the **Phone** menu. To access this menu, right-click on a phone in the **Phones** summary pane and select **Open**. In the **Phone** menu, select the desired CoS from the **Phone class of service** drop-down menu. When you have finished, select **OK** to apply the new CoS to the phone.*

Applying the CoS to a New Phone

If you are manually adding a new phone to the NetVanta UC Server system, you can apply a phone CoS to the phone during the configuration process. Use the **Phone class of service** drop-down menu in the **Phone** menu to apply a CoS when adding a phone.

Appendix C – NetVanta ECS Communication System Considerations

If an installation of NetVanta UC Server includes a NetVanta ECS communication system, it must be defined identically on both the primary and secondary servers. The Business Continuity Service does not synchronize the NetVanta ECS definitions because the definitions contain a combination of system specific (for example, the selected network adapter) and common (for example, a group name) information. Use the following guidelines in managing the definition of a NetVanta ECS communication system.

Initially Configuring NetVanta ECS on the Primary and Secondary Servers

During installation, the NetVanta ECS communication system should be defined identically on both servers (same answering group number, same group name, same priority, etc.). The selected network adapter will be specific to the primary or secondary server.

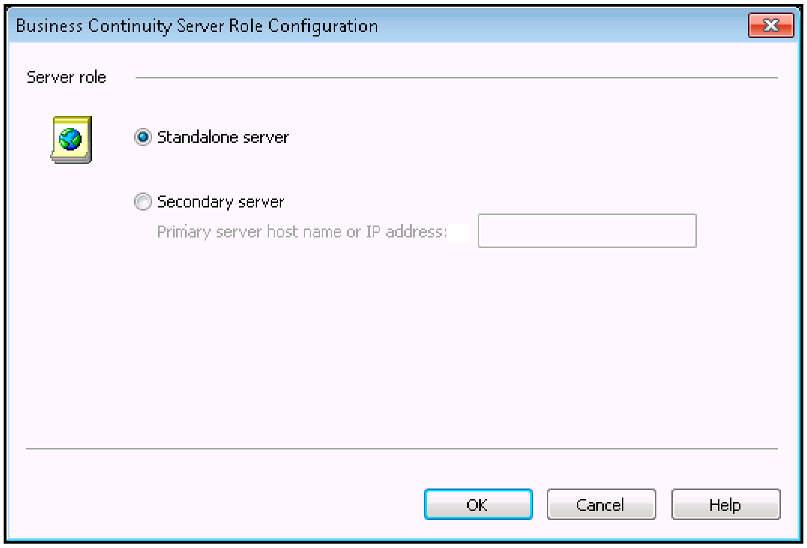
Making Changes to NetVanta ECS

After the installation and setup of NetVanta ECS communication system is complete, it is possible to use the NetVanta UC Client on the primary server to edit the NetVanta ECS communication system. If changes are made to the group name or priority of NetVanta ECS, the same changes must be made manually on the secondary server because the definition is not automatically synchronized. Since such updates are normally not allowed on the secondary server, special steps are required to make the corresponding changes on the secondary server. To make changes to NetVanta ECS on the secondary server, follow these steps:

NOTE *These steps should be performed during a maintenance window.*

1. Log in to the secondary server using the service account.
2. Log in to the NetVanta UC Client as an administrator.
3. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.
4. Select the **Servers** topic from the **Administration** navigation pane.
5. Right-click in the **Servers** summary pane, and select **UC Server Role**. The **Business Continuity Server Role Configuration** menu appears.

6. Select the **Standalone server** radio button to change the business continuity server role of the secondary server to standalone. Then, select **OK**. You will now be able to update the NetVanta ECS communication system.



Business Continuity Server Role Configuration

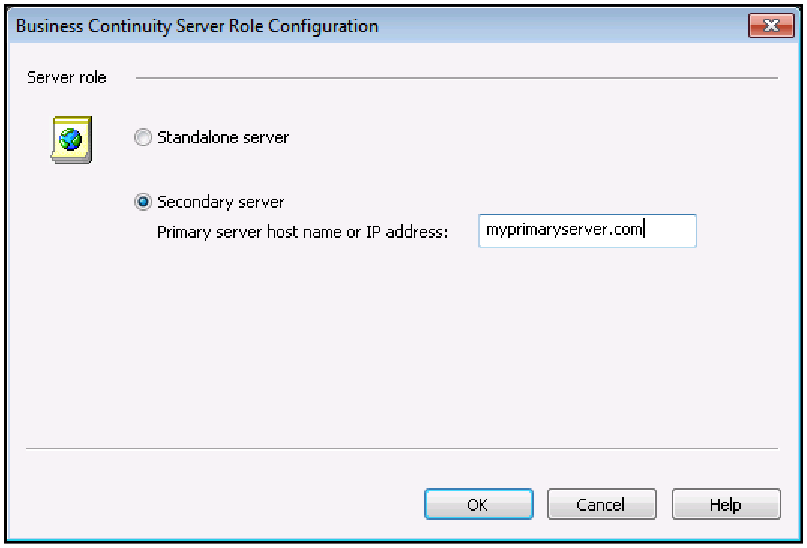
Server role

● Standalone server

○ Secondary server

Primary server host name or IP address:

7. Make the same changes to the group name and/or priority of the NetVanta ECS communication system that were made on the primary server.
8. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.
9. Select the **Servers** topic from the **Administration** navigation pane.
10. Right-click in the **Servers** summary pane, and select **UC Server Role**. The **Business Continuity Server Role Configuration** menu appears.
11. Select the **Secondary server** radio button, and in the **Primary server host name or IP address** field, enter the FQDN or IP address of the primary server. Then, select **OK**.



Business Continuity Server Role Configuration

Server role

○ Standalone server

● Secondary server

Primary server host name or IP address: myprimaryserver.com

12. In the **Primary server host name or IP address** field, enter the FQDN or IP address of the primary server.
13. You will now need to reconfigure the **Business Continuity primary Server** object parameters. Refer to *Step 6: Configure Business Continuity on the Secondary Server on page 20* for more information on configuring the **Business Continuity primary Server** object on the secondary server.

Making Changes to the NetVanta ECS .cfg File

In rare cases, it may be necessary to use a text editor to modify the .cfg file associated with the NetVanta ECS communication system. If changes are made to this file on the primary server, the file should be copied to the corresponding location on the secondary server and the NetVanta UC Server service should be restarted.

Appendix D - Handling an Extended Failure of the Primary Server

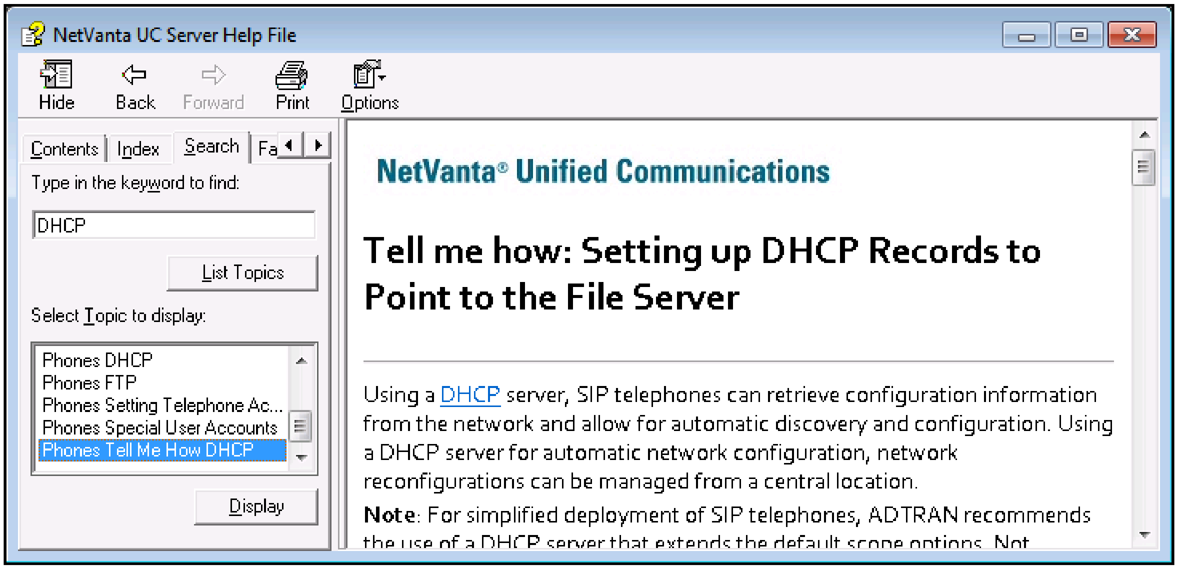
When the primary server is unavailable for an extended period of time (for example, some server hardware fails and must be replaced), telephony and related functionality will still be provided by the secondary server. However, steps must be taken to permit the ongoing administration of the NetVanta UC Server system (i.e., activities normally done on the primary server).

Transitioning the Secondary Server to Standalone Mode

In the case of a primary server failure, the secondary server should be placed in the Standalone server role to restore full Unified Communications and Administrative functionality. To transition the secondary server to Standalone server mode, perform the following steps:

1. Ensure that the primary server cannot come back online by turning off the server or removing it from the network.
2. On the secondary server, the system should be placed into standalone mode. Use the steps provided in *Changing the Role of the Secondary Server on page 54* to access the **Business Continuity Server Roll Configuration** menu, and change the server role to **Standalone**. The secondary server will continue to support telephony and related functionality. In addition, the NetVanta UC Client on the secondary server can now be used to make changes. However, NetVanta UC Client will display a warning after each login.
3. The secondary server can now operate with the full functionality of a standalone system. Of course, there is no longer a backup to the system in case of problems with the secondary server.

4. If the Dynamic Host Configuration Protocol (DHCP) server was manually configured to allow phones to retrieve their configuration on the primary server, the DHCP server should be updated so that phones will retrieve their configurations from the secondary server. Information on this task can be found in the Server Configuration Wizard help file. To access this help file, navigate to the **Bin** folder in the NetVanta UC Server installation directory (the default directories are **C:\Program Files (x86)\ADTRAN\NetVanta UC Server\Bin** on a 64-bit system and **C:\Program Files\ADTRAN\NetVanta UC Server\Bin** on a 32-bit system). Double-click **ServerConfigWizard.chm** to open the Server Configuration Wizard help file. In the **Search** tab, search for **DHCP**. The help topic titled **Phones Tell Me How DHCP** provides information for manually configuring DHCP servers for phones.


NetVanta UC Server Help File
Hide
Back
Forward
Print
Options
Contents
Index
Search
Fa
Type in the keyword to find:
DHCP
List Topics
Select Topic to display:
Phones DHCP
Phones FTP
Phones Setting Telephone Ac...
Phones Special User Accounts
Phones Tell Me How DHCP
Display
NetVanta® Unified Communications

Tell me how: Setting up DHCP Records to Point to the File Server

Using a DHCP server, SIP telephones can retrieve configuration information from the network and allow for automatic discovery and configuration. Using a DHCP server for automatic network configuration, network reconfigurations can be managed from a central location.

Note: For simplified deployment of SIP telephones, ADTRAN recommends the use of a DHCP server that extends the default scope options. Not

Restoring the Primary Server to Service

The following section describes how the overall system can be restored so that the primary server takes on primary responsibility for telephony and related functionality and the secondary server reverts to providing backup functionality in the event of primary server failure.

Installing and Configuring NetVanta UC Server on the Primary Server

This section provides an outline of the tasks that are required to install and configure NetVanta UC Server on the restored primary server. The process is similar to installing a new business continuity solution. To install and configure NetVanta UC Server on the restored primary server, follow these steps:

1. Log in to the primary server using the service account.
2. Install the same version of NetVanta UC Server 5.3 on the primary server as is installed on the secondary server.

> *The build numbers of the versions of NetVanta UC Server installed on the primary and secondary servers must be identical for server synchronization.*

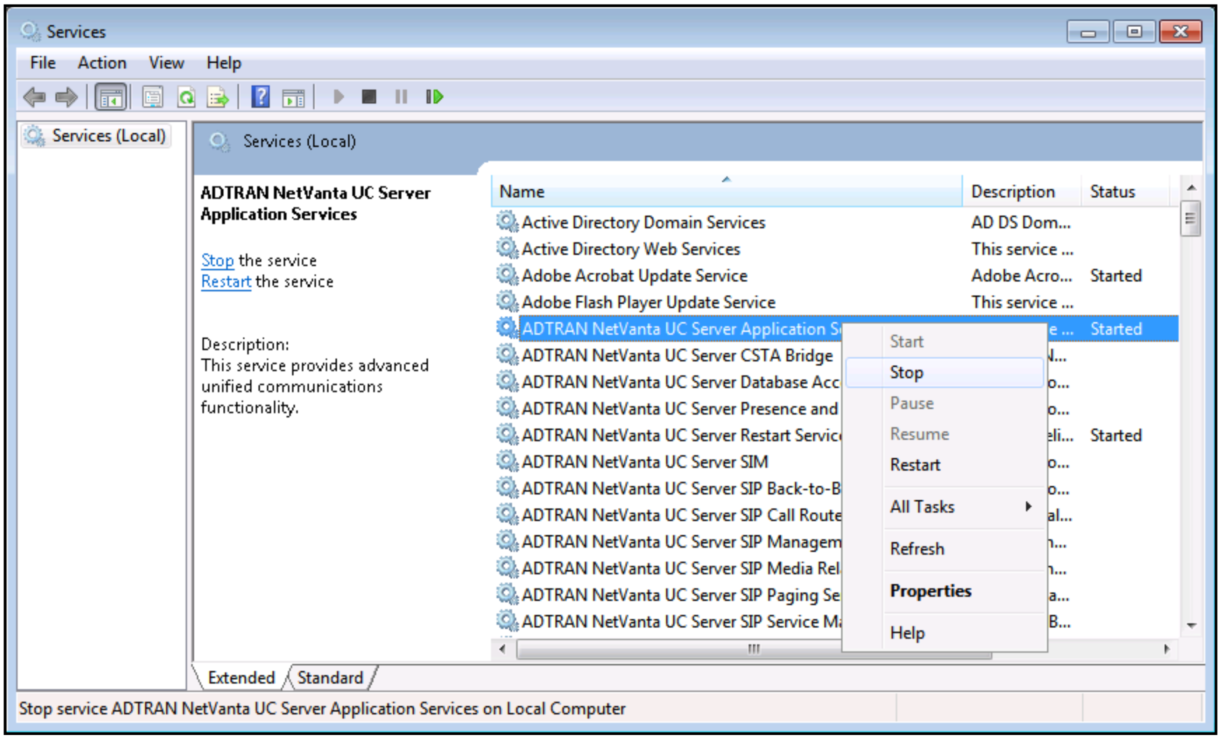
3. Run the Server Configuration Wizard on the primary server. Enter the **Product Licensing** wizard.
    - If the machine ID of the new primary server is the same as it was before the primary server failure (i.e., the same hardware is being used), enter the license key that is currently in use on the secondary server. In this case, no change is required to the license key on the secondary server.
    - If the machine ID has changed (i.e., the hardware has changed), request a new license key from ADTRAN specifying the new machine ID as the primary ID and the machine ID of the secondary server as the secondary ID. Use this license key in the **Product Licensing** wizard.
4. In the **Windows Network Integration** wizard, ensure the same service account and password that was used on the secondary server is specified.
5. In the **Communication Systems** wizard, if a **NetVanta Enterprise Communications Server** was defined on the secondary server, it must be defined here as well.
6. In the **Phone Types** wizard, enable the same phone types that were enabled on the secondary server.
7. **Do not run any other wizards in the Server Configuration Wizard**. The NetVanta UC Server on the primary server will still be in the Standalone role at this point. Exit the Server Configuration Wizard.

Synchronize the Primary Server and Go Live

The steps in the previous section can be done while the secondary server is still operational. **The remaining steps in this section must be performed during a maintenance window (i.e., when users do not expect the system to be operational).**

Stopping both the primary and secondary NetVanta UC Servers

On both the primary and secondary servers, open the Service Control Manager and stop all **ADTRAN NetVanta UC Server** services. Right-click each service with a **Started** status and select **Stop** from the drop-down menu.



ADTRAN NetVanta UC Server Application Services

Stop the service
Restart the service

Description:
This service provides advanced unified communications functionality.

Name	Description	Status
Active Directory Domain Services	AD DS Dom...	
Active Directory Web Services	This service ...	
Adobe Acrobat Update Service	Adobe Acro...	Started
Adobe Flash Player Update Service	This service ...	
ADTRAN NetVanta UC Server Application S	e ...	Started
ADTRAN NetVanta UC Server CSTA Bridge	N...	
ADTRAN NetVanta UC Server Database Acc	o...	
ADTRAN NetVanta UC Server Presence and	o...	
ADTRAN NetVanta UC Server Restart Servic	eli...	Started
ADTRAN NetVanta UC Server SIM	o...	
ADTRAN NetVanta UC Server SIP Back-to-B	o...	
ADTRAN NetVanta UC Server SIP Call Route	al...	
ADTRAN NetVanta UC Server SIP Managem	n...	
ADTRAN NetVanta UC Server SIP Media Rel	n...	
ADTRAN NetVanta UC Server SIP Paging Se	a...	
ADTRAN NetVanta UC Server SIP Service M	B...	

Stop service ADTRAN NetVanta UC Server Application Services on Local Computer

Copying NetVanta UC Server data from the secondary server to the primary server

To copy the NetVanta UC Server data from the secondary server to the primary server, perform the following steps on the secondary server:

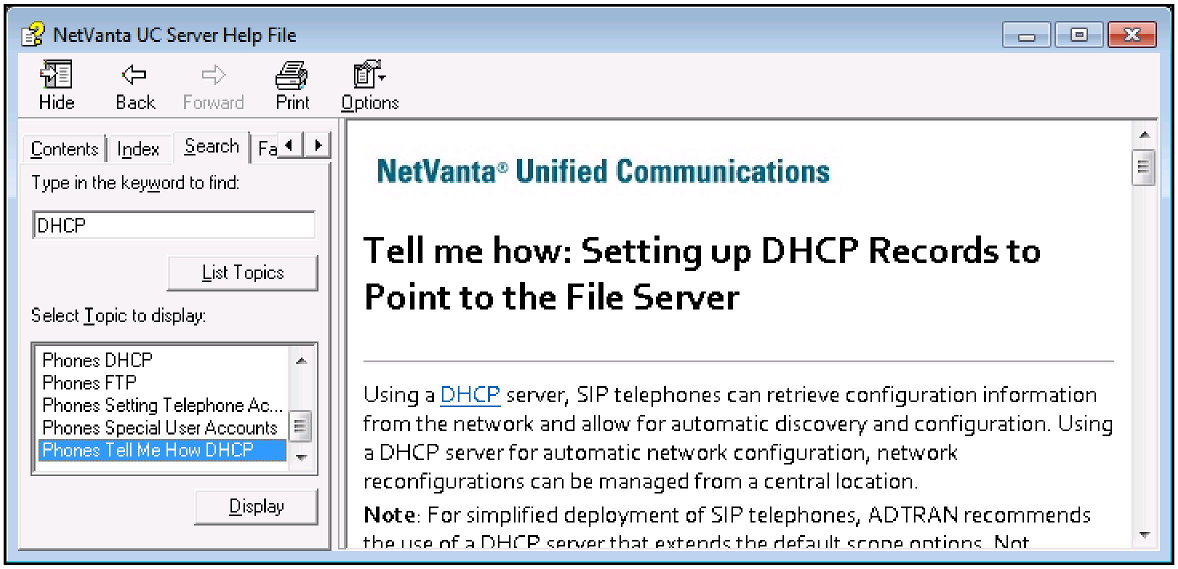
1. Log in to the secondary server using the service account.
2. In the Windows Start menu, right-click **Command Prompt** entry, and select **Run as administrator**. This will run Windows **Command Prompt** as an Administrator.
3. Use the CD command to change directories to the **NetVanta UC Server\Bin** folder. On 32-bit systems, the default for this directory is **C:\Program Files\ADTRAN\NetVanta UC Server\Bin**. On 64-bit systems, the default for this directory is **C:\Program Files (x86)\ADTRAN\NetVanta UC Server\Bin**, for example:
   >**CD C:\Program Files (x86)\ADTRAN\NetVanta UC Server\Bin**
4. Once you have changed directories, execute the following command:
   >**cscript DataSync.vbs Reverse**
   The NetVanta UC Server objects on the secondary server will be copied to the primary server.

Configuring DHCP and the business continuity role of the primary server

To configure the DHCP server and the business continuity role of the primary server, perform the following steps on the primary server:

It is important that the steps in this section be completed after the NetVanta UC Server data is copied from the secondary server to the primary server. This ensures that all phones that should be dual registered are rebooted.

1. If after the primary server failure the DHCP server was manually configured to allow phones to retrieve their configuration on the secondary server (refer to *Transitioning the Secondary Server to Standalone Mode on page 66*), the DHCP server should be updated so that phones will retrieve their configurations from the primary server. Information on this task can be found in the Server Configuration Wizard help file. To access this help file, navigate to the **Bin** folder in the NetVanta UC Server installation directory (the default directories are **C:\Program Files (x86)\ADTRAN\NetVanta UC Server\Bin** on a 64-bit system and **C:\Program Files\ADTRAN\NetVanta UC Server\Bin** on a 32-bit system). Double-click **ServerConfigWizard.chm** to open the Server Configuration Wizard help file. In the **Search** tab, search for **DHCP**. The help topic titled **Phones Tell Me How DHCP** provides information for manually configuring DHCP servers for phones.



Type in the keyword to find: DHCP

Select Topic to display:
Phones DHCP
Phones FTP
Phones Setting Telephone Ac...
Phones Special User Accounts
Phones Tell Me How DHCP

NetVanta® Unified Communications

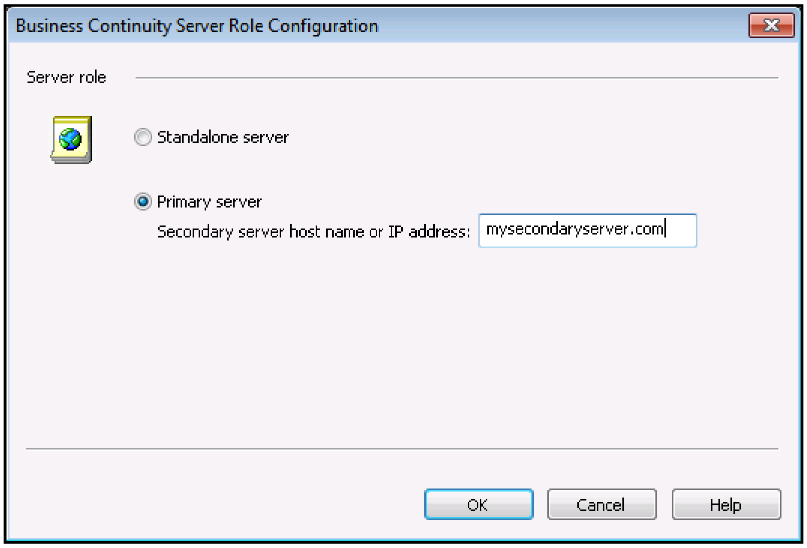
Tell me how: Setting up DHCP Records to Point to the File Server

Using a DHCP server, SIP telephones can retrieve configuration information from the network and allow for automatic discovery and configuration. Using a DHCP server for automatic network configuration, network reconfigurations can be managed from a central location.

Note: For simplified deployment of SIP telephones, ADTRAN recommends the use of a DHCP server that extends the default scope options. Not

2. Log in to NetVanta UC Client as an administrator.
3. From the **Admin** tab, select the **Administration** navigation bar to access the **Administration** navigation pane.
4. Select the **Servers** topic from the **Administration** navigation pane.
5. Right-click in the **Servers** summary pane, and select **UC Server Role**. The **Business Continuity Server Role Configuration** menu appears.

6. In the **Business Continuity Server Role Configuration** menu, select the **Primary server** radio button, and enter the host name or IP address of the secondary server in the provided field. Then, select **OK**.



Secondary server host name or IP address: mysecondaryserver.com

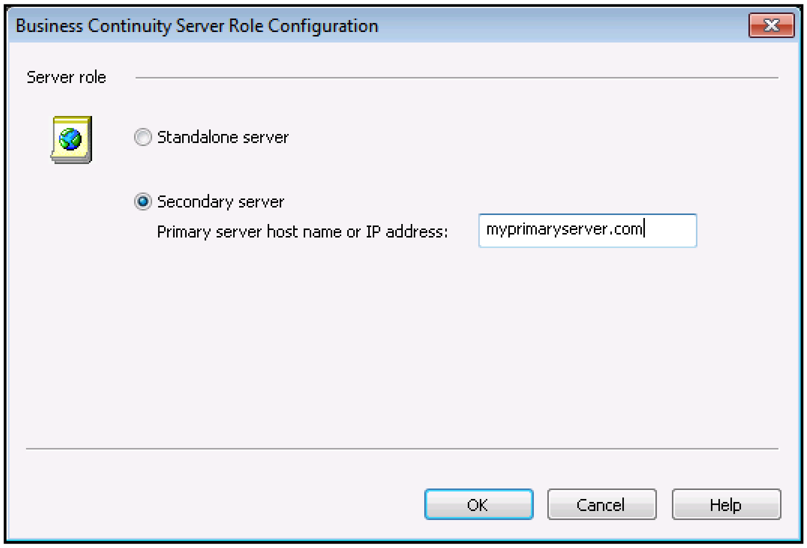
> NOTE *Any phones that are configured to dual register will now be reprogrammed to register with both the primary and secondary servers.*

Configuring the business continuity role of the secondary server

After configuring the business continuity role of the primary server, you must configure the role of the secondary server and specify the address of the primary server. To configure the business continuity role of the secondary server, follow these steps:

1. From the **Admin** tab of the NetVanta UC Client on the secondary server, select the **Administration** navigation bar to access the **Administration** navigation pane.
2. Select the **Servers** topic from the **Administration** navigation pane.
3. Right-click in the **Servers** summary pane, and select **UC Server Role**. The **Business Continuity Server Role Configuration** menu appears.

4. In the **Business Continuity Server Role Configuration** menu, select the **Secondary server** radio button to change the server role to secondary server. Then, in the **Primary server host name or IP address** field, enter the FQDN or IP address of the primary server. Select **OK**.



Server role

○ Standalone server

● Secondary server

Primary server host name or IP address: myprimaryserver.com

Applying the new license key to the secondary server (Optional)

If a new license key was required when the primary server software was installed (because the primary server is using different hardware), the new license key must now be applied to the secondary server. For more information on changing the license key of the secondary server, refer to *Modifying the License Key of the Secondary Server on page 55*.