

# Sharing the Cisco WebAttendant User Directory Database Information in Cisco CallManager 3.1

Document ID: 5270

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### Understanding Cisco WebAttendant Users, Devices and Accounts

### Task 1: Creating a New User on the Cisco CallManager Server

### Task 2: Sharing the Users Folder to Provide Access to the User Database

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

This document is part of a document set. For information on each of these documents, refer to the index for this set: *Installing and Configuring Cisco WebAttendant for CallManager 3.1*.

The Cisco WebAttendant client displays user and line information in the Directory section of its user interface. The Cisco TCD Database Path field in the Cisco WebAttendant client Settings dialog box controls where the Cisco WebAttendant client looks for its directory information.

By default, the Cisco WebAttendant client is configured to use cached user directory information directly from the Cisco CallManager server's user database. This is the preferred option. In this case, the Cisco WebAttendant client's path to the database is [\\<ip-address>\WAUSERS], where <ip-address> is the address of the Cisco CallManager server or [\\<dns-name>\WAUSERS], where <dns-name> is the name of the CallManager server.

There are other options for allowing Cisco WebAttendant clients to access the user database. The Cisco WebAttendant client PC can be configured to point to a local copy of the database on its own hard drive or on the hard drive of a remote server. If you decide to implement one of the alternative options, the database must be manually refreshed on a regular basis (copied from the Cisco CallManager server) to the location that you are using to provide access for the Cisco WebAttendant clients in order for the WebAttendant clients to have the most up-to-date database.

All of the options for making the user database available to the Cisco WebAttendant client require that the proper access permissions have been granted for the folder that the database resides in. Networks that use a Domain based security model might also require that the PC running the Cisco WebAttendant client application is granted access to the network. This is explained in more detail in the *Understanding Cisco WebAttendant Users, Devices and Accounts* section.

## Prerequisites

### Requirements

There are no specific requirements for this document.

## Components Used

This document is not restricted to specific software and hardware versions.

## Conventions

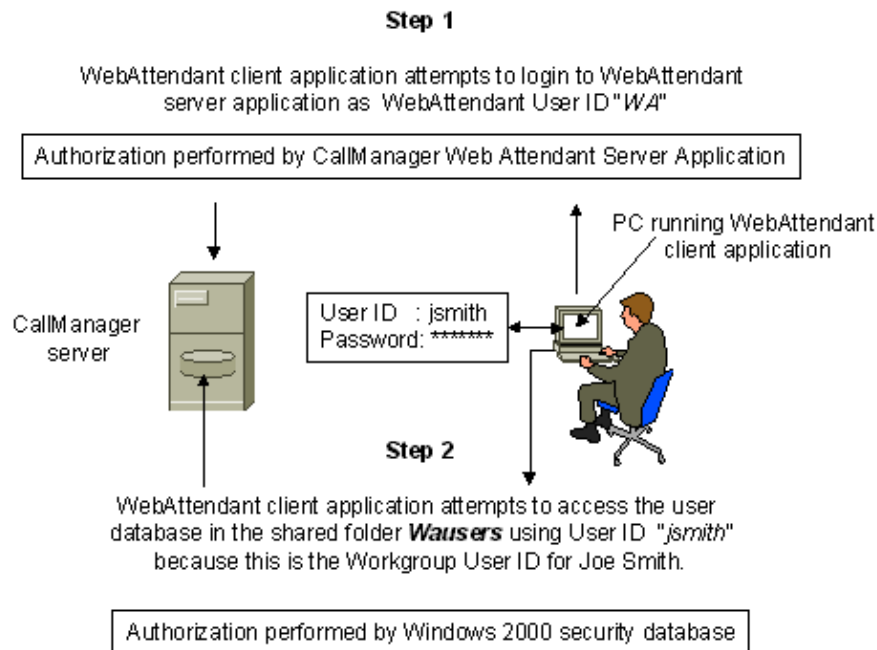
Refer to Cisco Technical Tips Conventions for more information on document conventions.

## Understanding Cisco WebAttendant Users, Devices and Accounts

This section explains some of the issues related to providing access to the Cisco CallManager user database for the WebAttendant user. It also explains the relationship between the Cisco CallManager WebAttendant users and the CallManager users that are stored in the DC Directory. If you already understand how to share folders and assign access rights, how to allow devices (PCs, servers) to access an NT or Windows 2000 environment, and the relationships between the different Cisco CallManager users, you can skip this section and proceed to the next section.

The creation of a functional Cisco WebAttendant environment involves several different user accounts, possibly device accounts and other security issues. The goal of this section is to expose the reader to these issues.

This figure shows the Workgroup model for allowing Cisco WebAttendant clients to access the user database.



In the next example, the network security is based on a Windows Workgroup model. The Cisco WebAttendant client application is accessing the user database on the Cisco CallManager server using the default method.

This table shows the steps involved:

Step	Explanation
------	-------------

<p>User logs onto his PC as <i>jsmith</i></p>	<p>In a Microsoft Workgroup based network in which users access resources on other systems, the user must log into his or her PC. This enables the other devices to identify the user (if required) when they initiate a request to access a resource owned by a different system.</p>
	<p>In this example the User ID "jsmith" is the one used by the Windows 2000 security system on the Cisco CallManager server to determine if it should allow or deny access to the user database in the Users folder.</p>
<p>User starts the Cisco WebAttendant client application using the User ID "WA"</p>	<p>The Cisco WebAttendant client application logs into the Cisco CallManager WebAttendant TCD application on the CallManager server using the WebAttendant User ID "WA".</p>
	<p>In this example Cisco WebAttendant client application logs in as "WA".</p>
	<p><b>Note:</b> It is important to understand that in this case, the ID "WA" is authenticated by the Cisco CallManager WebAttendant server application, not the Windows 2000 server security database.</p>
<p>Cisco WebAttendant client application takes over control of the IP Phone it has been configured for</p>	<p>The Cisco WebAttendant client application has a field for the MAC address of the IP Phone that will be controlled by it. This is how it knows which IP Phone to use.</p>
	<p>The Cisco WebAttendant client application console will display the lines (DNs) that have been configured for the IP Phone it controls.</p>
	<p><b>Note:</b> If the user running the Cisco WebAttendant client application has a primary extension (DN), the IP Phone controlled by the WebAttendant client application must be the one that has this DN associated with it.</p>
<p>Cisco WebAttendant client displays the user database</p>	<p>The Cisco WebAttendant client application attempts to access the user database in the shared users folder (WAUSERS) on the Cisco CallManager server. Access will be granted or denied based on the User ID that the user used to log in to his or her PC, not the User ID of the Cisco WebAttendant client application.</p>
	<p><b>Note:</b> Many customers use the same User ID for both purposes to facilitate managing the accounts and troubleshooting problems.</p>

Cisco WebAttendant client application displays the current status of the lines	The Cisco WebAttendant client application uses the Line State Server (LSS) to track the status of the lines (DNs) assigned to phones.
	In general, if the the Cisco WebAttendant client application has been able to log in to the Cisco CallManager server application, the connection to the LSS should also have been successful.
	<b>Note:</b> The status bar for each of the lines displayed in the user area at the bottom of the Cisco WebAttendant client application console might remain red (status unknown) until the line has been used. Once a user has made a call on a line the status bar for that line might transition from red to blue (status available). In some cases, however, the LSS may never be able to determine the status of a line. This doesn't prevent the user from using the Cisco WebAttendant client application console to make calls or to transfer calls.

In the following explanation, the network security is based on a Windows NT Domain. The Cisco WebAttendant client application is accessing the user database on the Cisco CallManager server using the default method.

This table shows the steps involved:

Step	Explanation
PC (Windows NT or Windows 2000) boots up and attempts to join the domain	In a Microsoft NT/2000 domain based network, PCs running either Windows NT or Windows 2000 must be granted access to the domain. This is in addition to the user level security that applies to both Workgroups and Domains.
	It is not possible for a user on a PC running Windows NT or Windows 2000 that has not been granted access to the domain to access resources on other devices, even though the user might have a valid user account in the domain.
	<b>Note:</b> This does not apply to PCs running Windows 95/98.
	In a Microsoft domain based network in which users access resources on other systems, the user must log in to his or her PC and into the domain. This enables the other devices to identify the user when they initiate a request to access a resource

	<p>owned by a different system.</p> <p>In an NT domain based environment one system (server) is used as the primary domain controller. Other systems can be secondary domain controllers. All devices (PCs, servers, printers) to which access is to be granted or denied based on information in the domain security database must be part of the domain.</p> <p>Access to resources in the domain that are not actually on a domain controller (or secondary domain controller) can be granted by either referring to the master user database on a domain controller or by the less specific method of local control.</p> <p>In this example the User ID "jsmith" is the one used by the domain controller system on the Cisco CallManager server to determine if it should allow or deny access to the user database in the Users folder.</p> <p><b>Note:</b> In some cases the password a user uses to log in to their PC will be different from the password used to log in to the domain. If this happens, the user will be prompted for a password twice. Most users do not know that they are logging into their PC as well as onto the network because they have the same password for both actions.</p>
<p>User starts the Cisco WebAttendant client application using the User ID "WA"</p>	<p>The Cisco WebAttendant client application logs into the Cisco CallManager WebAttendant TCD application on the CallManager server using the WebAttendant User ID.</p> <p>In this example Cisco WebAttendant client application logs in as "WA".</p> <p><b>Note:</b> It is important to understand that in this case the ID "WA" is authenticated by the Cisco CallManager WebAttendant server application, not the Windows 2000 server security database. It is possible to use a different User ID for the user and the Cisco WebAttendant client application. The user's User ID could be "jsmith" and the WebAttendant client application User ID could be something like "jsmith-wa". In this case, access to the user database in the User's folder would be configured for "jsmith", not "jsmith-wa".</p>

Cisco WebAttendant client application takes over control of the IP Phone it has been configured for	The Cisco WebAttendant client application has a field for the MAC address of the IP Phone that will be controlled by it. This is how it knows which IP Phone to use.
	The Cisco WebAttendant client application console will display the lines (DNs) that have been configured for the IP Phone it controls.
	<b>Note:</b> If the user running the Cisco WebAttendant client application has a primary extension (DN) that other people use to reach him or her, the IP Phone controlled by the Cisco WebAttendant client application must be the one that has this DN associated with it.
Cisco WebAttendant client application attempts to access the user database	The Cisco WebAttendant client application attempts to access the user database in the shared users folder (WAUSERS) on the Cisco CallManager server. Access will be granted or denied based on the User ID that the user used to log onto the domain, not the User ID of the Cisco WebAttendant client application.
	<b>Note:</b> Many customers use the same User ID for both purposes to facilitate managing the accounts and troubleshooting problems.
Cisco WebAttendant client application attempts to access the Line State Server (LSS)	The Cisco WebAttendant client application uses the LSS to track the status of the lines (DNs) assigned to phones.
	In general, if the Cisco WebAttendant client application has been able to log in to the Cisco CallManager server application, the connection to the LSS should also have been successful.
	<b>Note:</b> The status bar for each of the lines displayed in the user area at the bottom of the Cisco WebAttendant client application console might remain red (status unknown) until the line has been used. Once a user has made a call on a line, the status bar for that line might transition from red to blue (status available). However, in some cases, the LSS might never be able to determine the status of a line. This does not prevent the user from using the Cisco WebAttendant client application console to make calls or to transfer calls.

**Note:** A thorough explanation of the issues related to security and other network related issues in a Microsoft Windows environment is beyond the scope of this document. There are many third party books available that

explain these issues in detail.

For information from Cisco on these subjects, refer to the Windows Networking Design Implementation Guide and How to Enable Browsing Using NetBIOS Over IP for more information.

## Task 1: Creating a New User on the Cisco CallManager Server

If your network uses the Workgroup authentication model, you will need to create a new user account on the Cisco CallManager server for each Cisco WebAttendant client. This task explains how to do this.

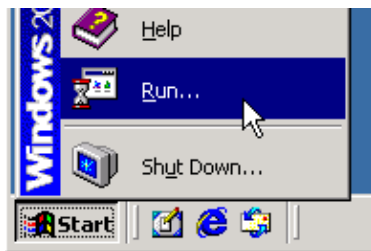
If your network is using the Domain authentication model, you will need to create the new accounts on the primary domain controller or master database server. The process is very similar to steps 7 and 8 below.

The default configuration for Windows 2000 on the Cisco CallManager server does not have the User and Group management application installed on the menus. In addition to explaining how to add a new user, this task also explains how to add the application to the menu system.

**Note:** Windows 2000 has very good context sensitive help that is accessible by selecting **F1**. Press **F1** during any step in this task to see the help that is available.

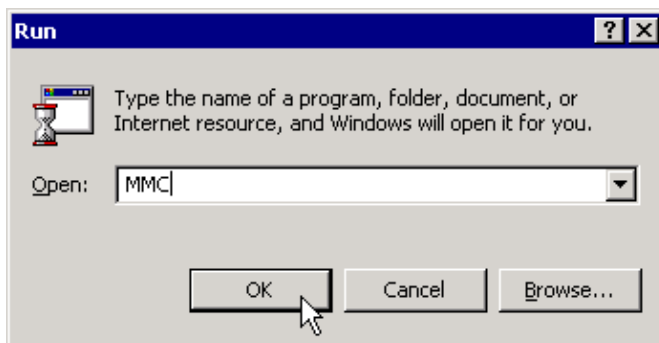
Complete these steps:

1. Go to the Start menu on the Cisco CallManager server and select **Run**.

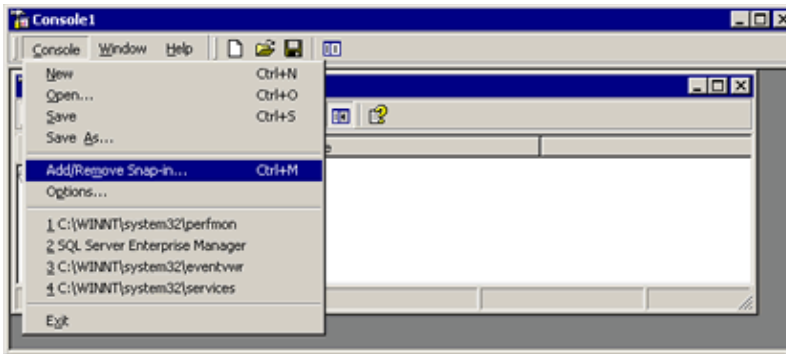


2. Enter **MMC** and press **OK**.

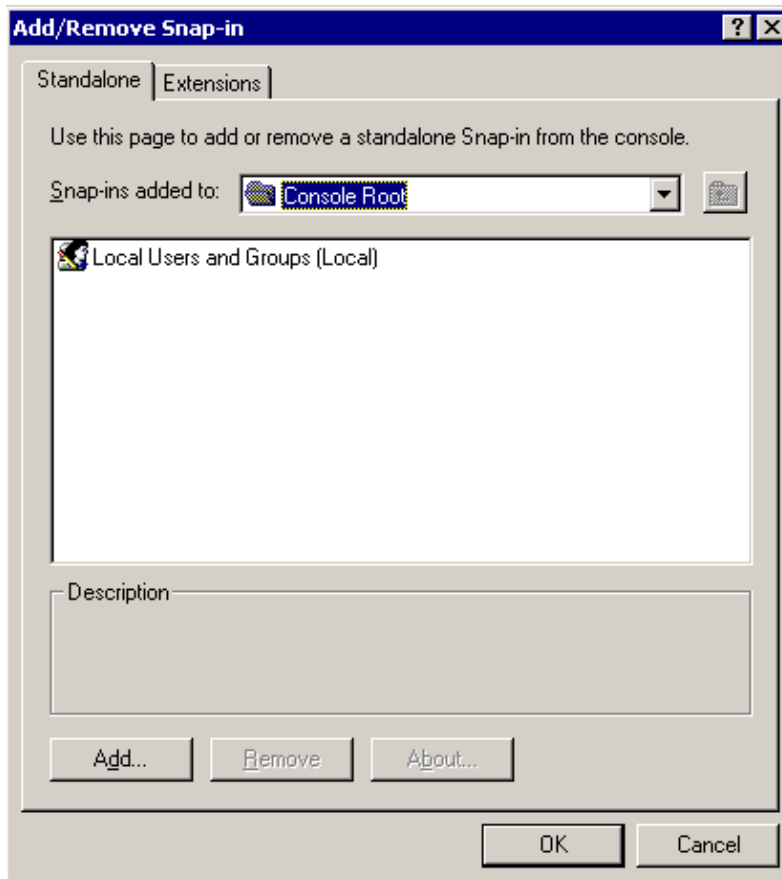
This starts an instance of the Console application.



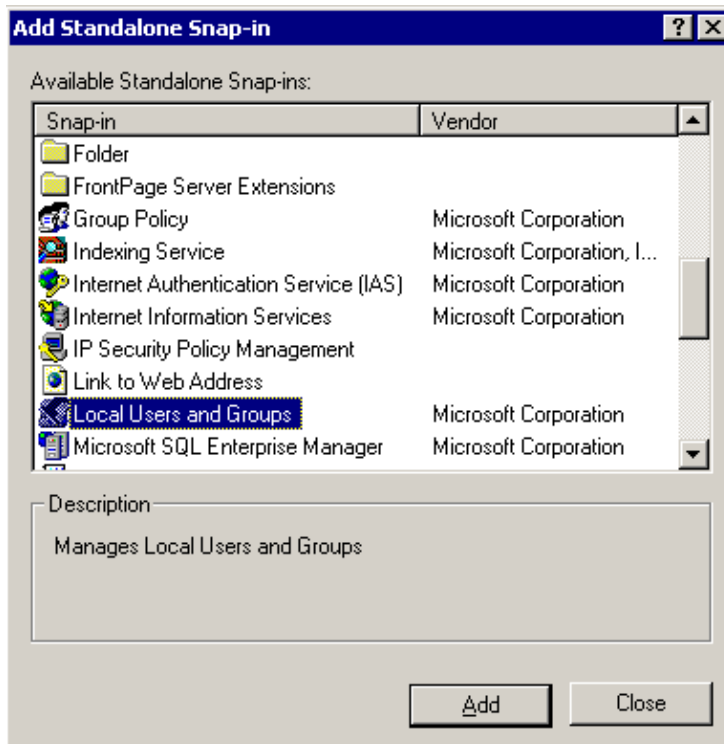
3. From the Console menu, select **Add/Remove Snap-in**.



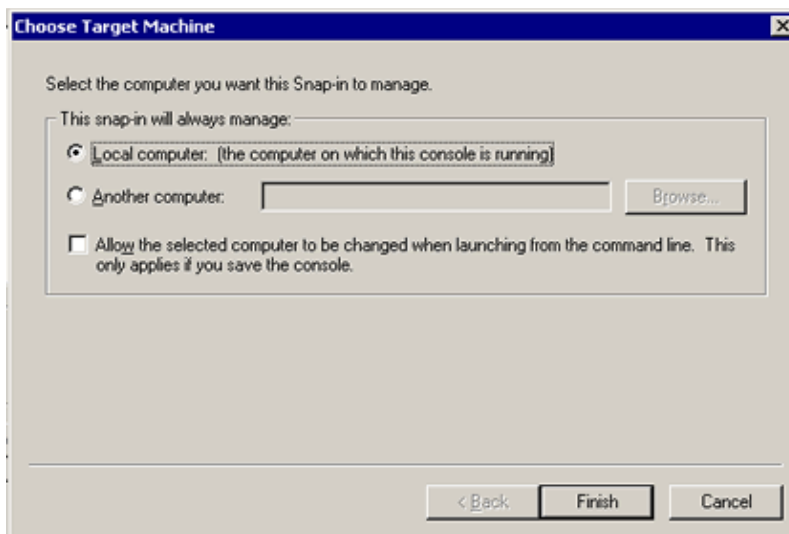
4. Click **Add** from the screen that appears.



5. Scroll down the menu, locate the Local Users and Groups snap-in and click **Add**.

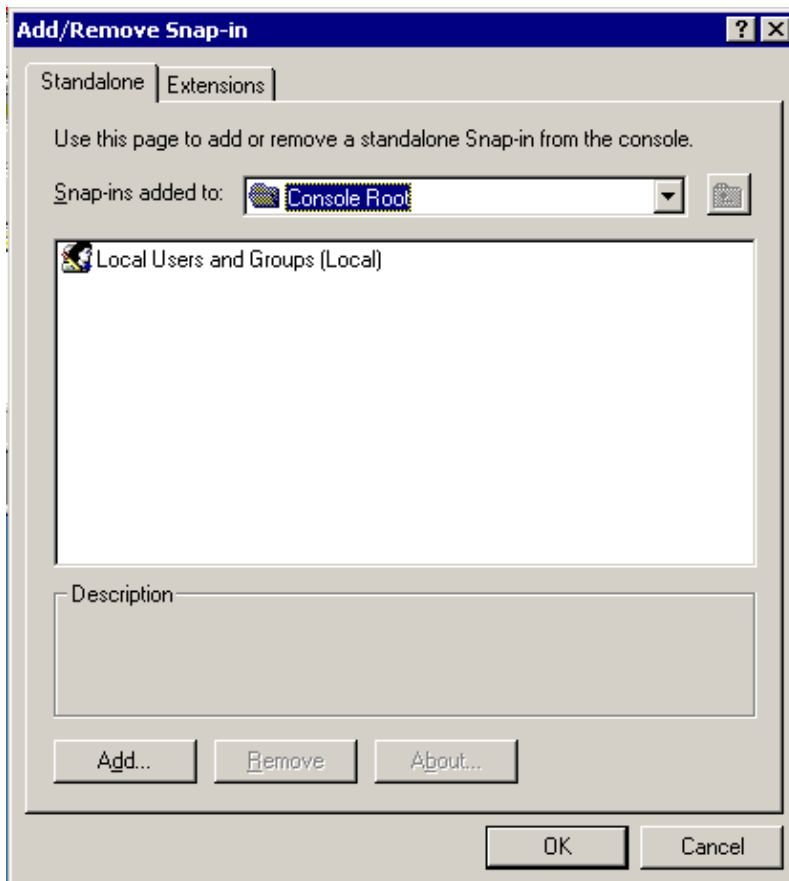


6. You should see a screen similar to this. Choose the **Local Computer** option.

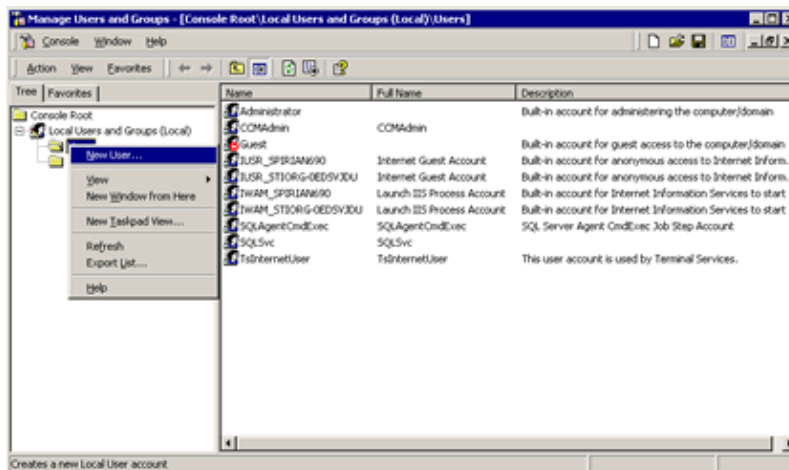


7. Click **Finish**, then **Close**.

You should see a screen similar to this:



8. Click **OK**.
9. Right click **Users** and select **New User**.



In this example, **wa** is used as the username and **cisco** as the password. Select the password options as appropriate for your security guidelines.

**New User** [?] [X]

User name: wa

Full name: webattendant

Description:

---

Password: xxxxxx

Confirm password: xxxxxx

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

[Create] [Close]

**Note:** This username and password combination is not the same as the User ID and password used by the Cisco CallManager WebAttendant user configuration task. Many customers use the same values. The values, however, are held in separate databases and must be managed separately.

- When you close the MMC Console1 screen, you might see a message asking if you would like to save the configuration to make it available from the Cisco CallManager server's menu system. It is recommended that you select **Save** from this screen to ensure the Users and Group management application is easily accessible in the future.

**Save As** [?] [X]

Save in: Administrative Tools

File name: Manage Users and Groups

Save as type: Microsoft Management Console Files (\*.msc)

[Save] [Cancel]

In this case, the new console is saved as Manage Users and Groups. It will appear on the Start > Programs > Administrative Tools menu list. This completes this task. Proceed to the next task to share the folder for the new user.

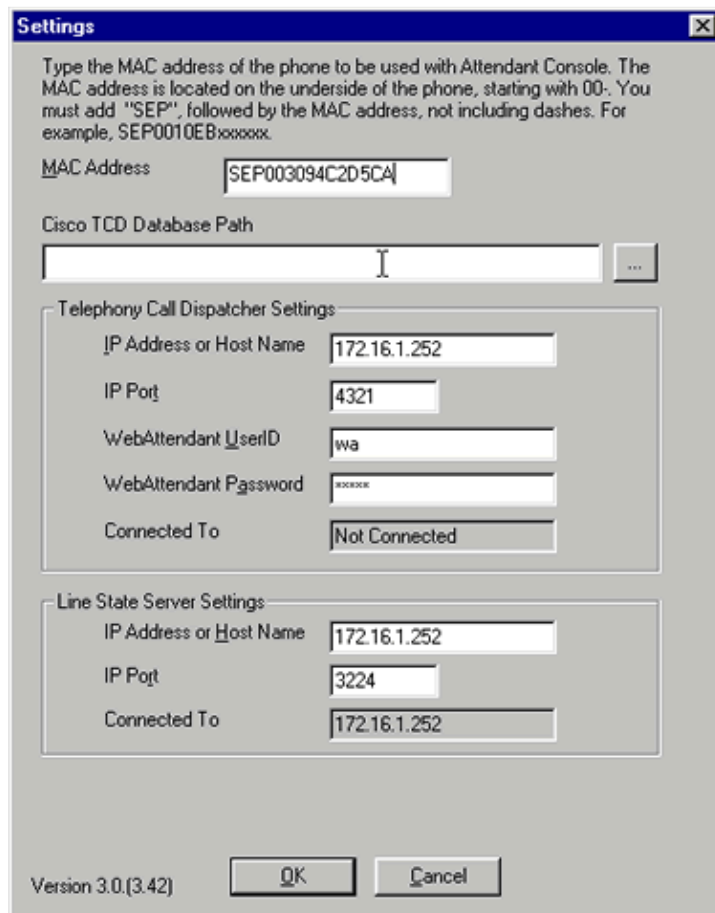
## Task 2: Sharing the Users Folder to Provide Access to the User Database

This task explains how to share a folder on a server and assign the correct permissions so that the Cisco WebAttendant client application users can access the user database on the Cisco CallManager server.

**Note:** The steps in this task are similar for both Workgroup and Domain based networks.

By default, the Cisco WebAttendant client is configured to use cached user directory information directly from the Cisco CallManager server's user database. This is the preferred option. In this case, the CiscoWebAttendant client's path to the database is [\\<ip-address>\WAUSERS], where <ip-address> is the address of the Cisco CallManager server or [\\<dns-name>\WAUSERS], where <dns-name> is the name of the CiscoCallManager server.

The next screen shows that the Cisco TCD Database Path is currently blank. Therefore, it will use the default method to access the user database.



In order to ensure that this default setting works properly, the Cisco CallManager administrator must share the C:\Program Files\Cisco\Users folder as WAUSERS and set permissions so that all Cisco WebAttendant client users have read and write access. This must be done on all Cisco CallManagers in the cluster.

This task explains how to configure this.

1. Double click the **My Computer** icon on the Cisco CallManager server's desktop to begin navigating to the Users folder, then the Cisco folder.

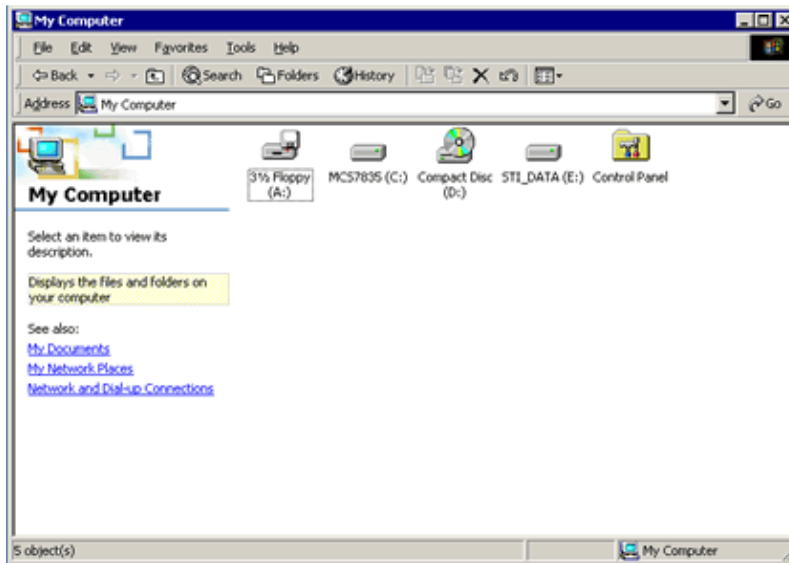


**Note:** If you see a message similar to this next one, you need to select the **Show Files** option in order to complete the process of navigating to the Users folder.

This folder contains files that keep your system working properly. There is no need to modify its contents.

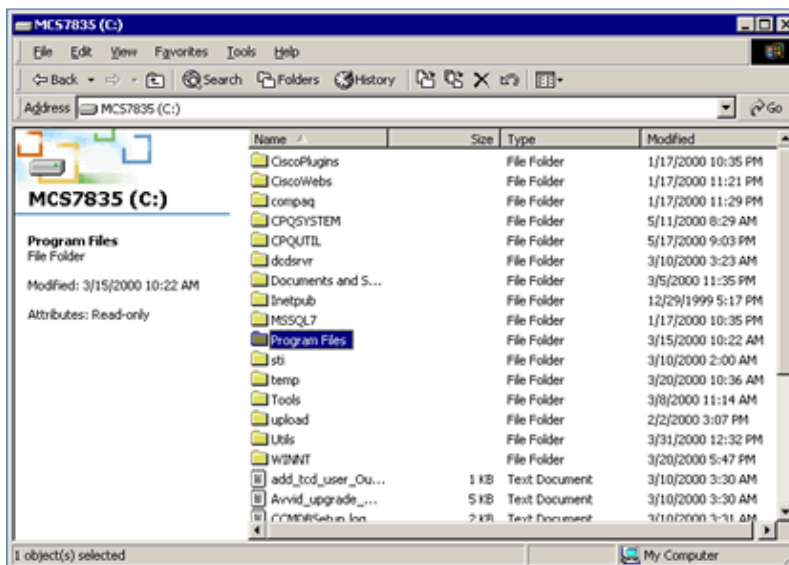
To view the contents of this folder, click: [Show Files](#)

You should see a screen similar to this:



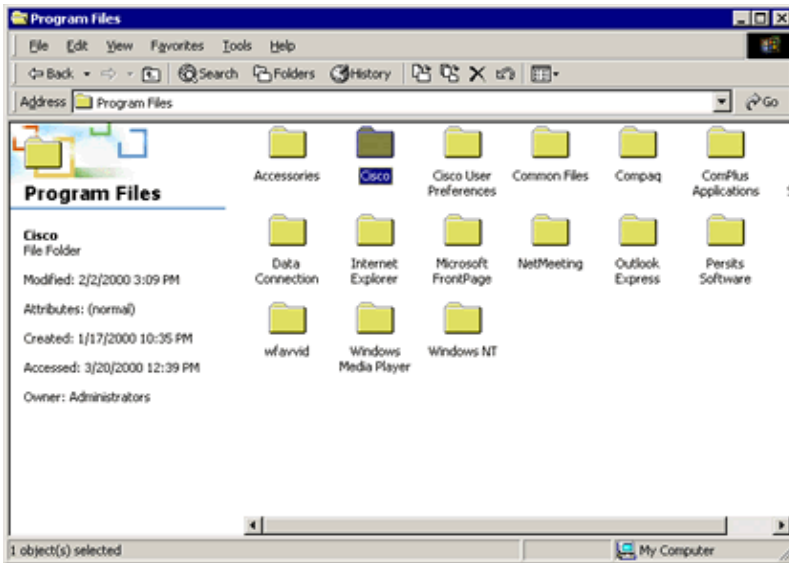
2. Double click the **C:** drive.

You should see a screen similar to this:



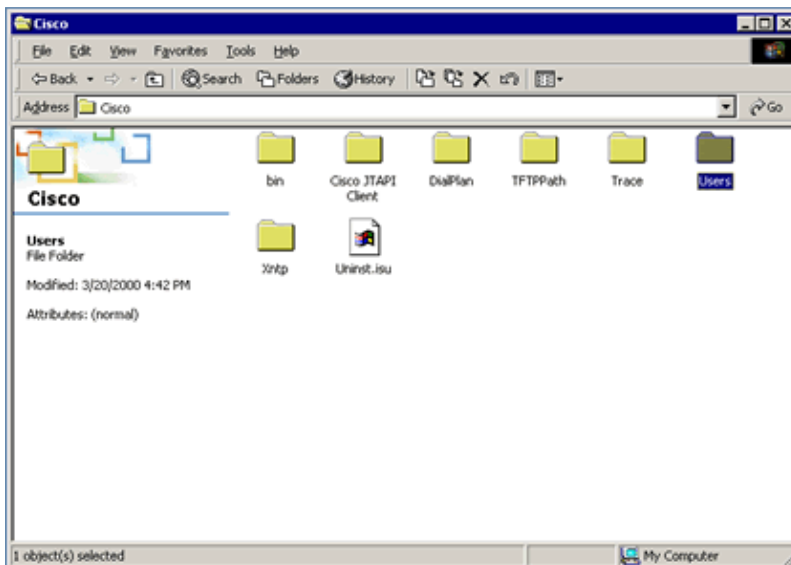
3. Double click the **Program Files** folder.

You should see a screen similar to this:



4. Double click the **Cisco** folder.

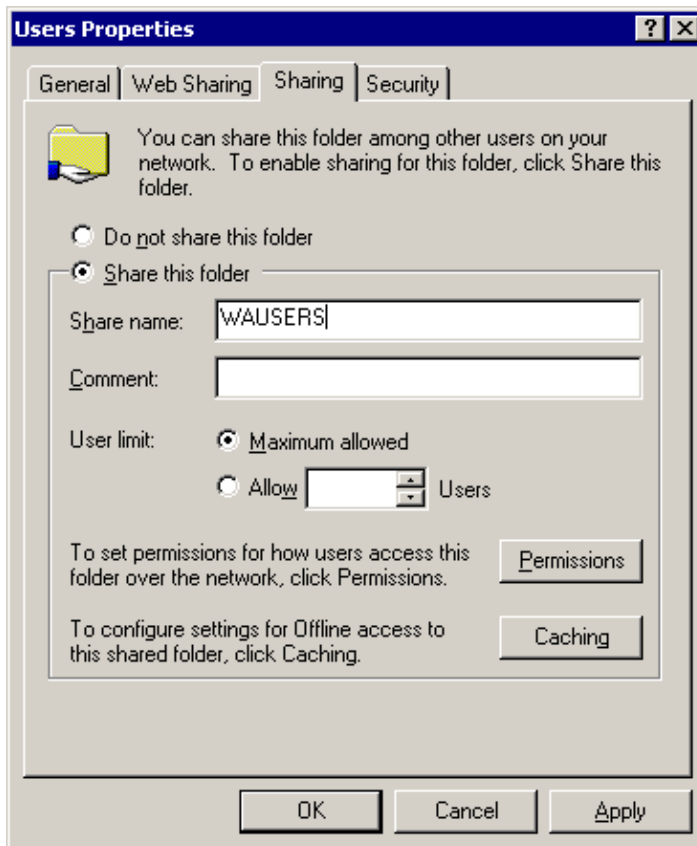
This screen shows the location of the Users folder.



5. Right click it and select **Properties**.

You should see a screen similar to the following. The Sharing tab has been selected and the name WAUSERS has been entered.

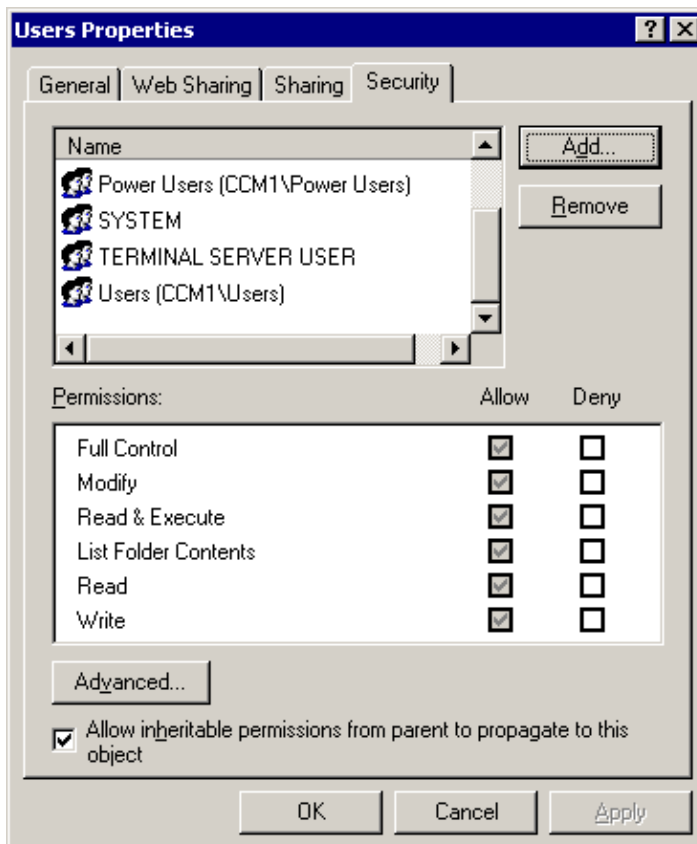
**Note:** When you are using the default method for providing access to the database, as explained in this task, you must use the name WAUSERS. The use of any other name will prevent the WebAttendant client application from being able to access the user database.



6. Choose **Share this folder**.

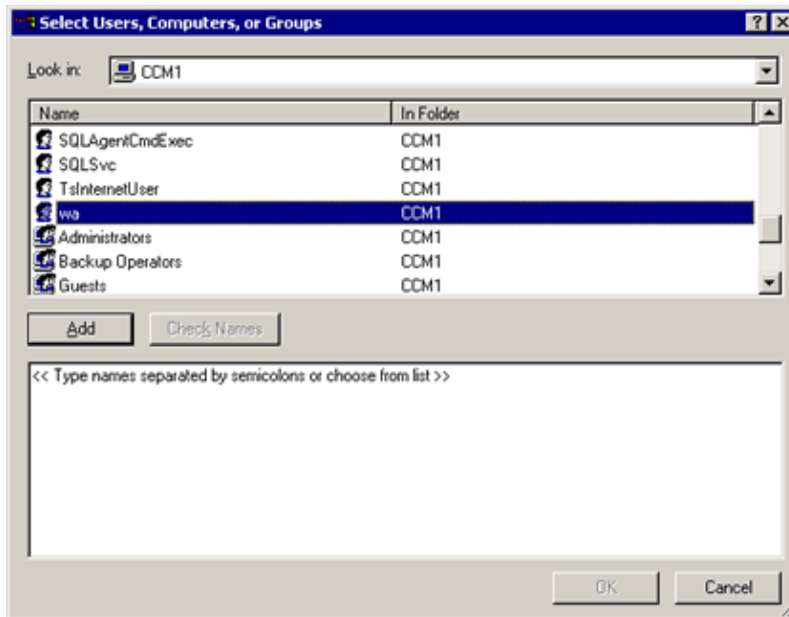
7. The new user (wa) must have Read and Write access permissions on C:\Program Files\Cisco\Users\ folder. In order to assign these permissions, click the **Security** tab.

The other permissions shown here will be assigned in step 10 of this task.



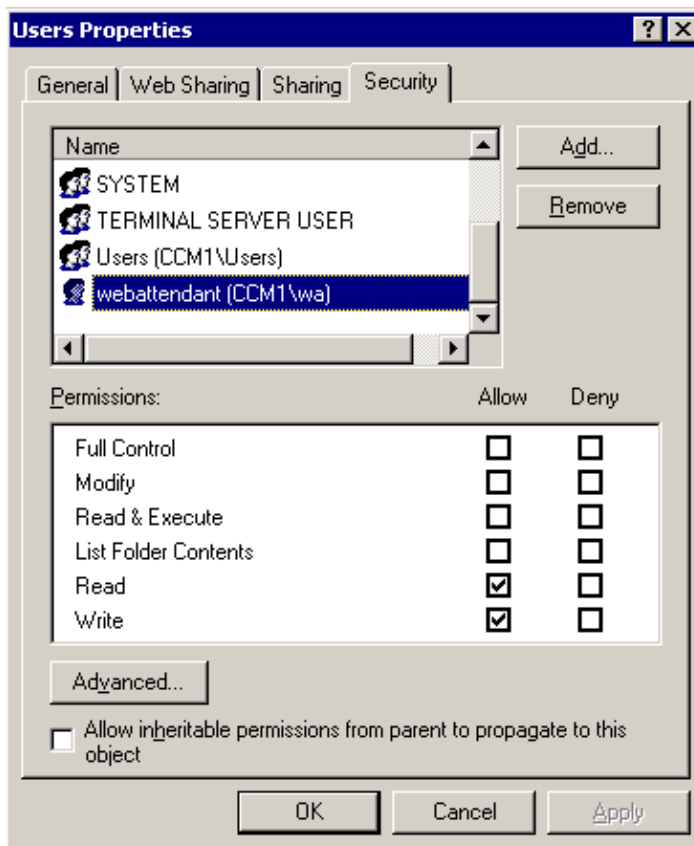
8. Click **Add**.

You should see a screen similar to this:



9. Scroll down to the wa user name, then click **Add** and **OK**.

10. You should see a screen similar to the following. Select the **Read** and **Write** options, and uncheck the **Allow inheritable permissions from parent to propagate to this object** box.



11. Click **OK**.

This completes this task.

[Return to the index page.](#)

## NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Voice
Service Providers: Voice over IP
Voice & Video: Voice over IP
Voice & Video: IP Telephony
Voice & Video: IP Phone Services for End Users
Voice & Video: Unified Communications
Voice & Video: IP Phone Services for Developers
Voice & Video: General

### Related Information

- [Voice Technology Support](#)
- [Voice and Unified Communications Product Support](#)
- [Recommended Reading: Troubleshooting Cisco IP Telephony](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: Feb 02, 2006

Document ID: 5270

---