

Sharing the Cisco WebAttendant User Directory Database Information in Cisco CallManager 3.0

Document ID: 7913

Introduction

Prerequisites

WebAttendant Users, Devices, and Accounts

Conventions

Windows Workgroup Model

Task 1: Create a New User on the CallManager Server

Task 2: Share the Users Folder to Provide Access to the User Database

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document is part four of a ten–document set. For information on each of these documents, consult the index for this set: Installing and Configuring Cisco WebAttendant for CallManager 3.0.

Note: Cisco WebAttendant has been superseded by Cisco Attendant Console (which is compatible with Cisco CallManager 3.1(2c)). Refer to the Installation and Administration Guide and the User Guide for information on installation, configuration, and the use of Cisco Attendant Console.

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

There are other options to allow WebAttendant clients to access the user database. The 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 CallManager server) to the location that you use to provide access for the WebAttendant clients in order for the WebAttendant clients to have the most up–to–date database.

All the options to make the user database available to the WebAttendant client require that the proper access permissions are granted for the folder in which the database resides. Networks that use a Domain–based security model can also require that the PC that runs the WebAttendant client application is granted access to the network.

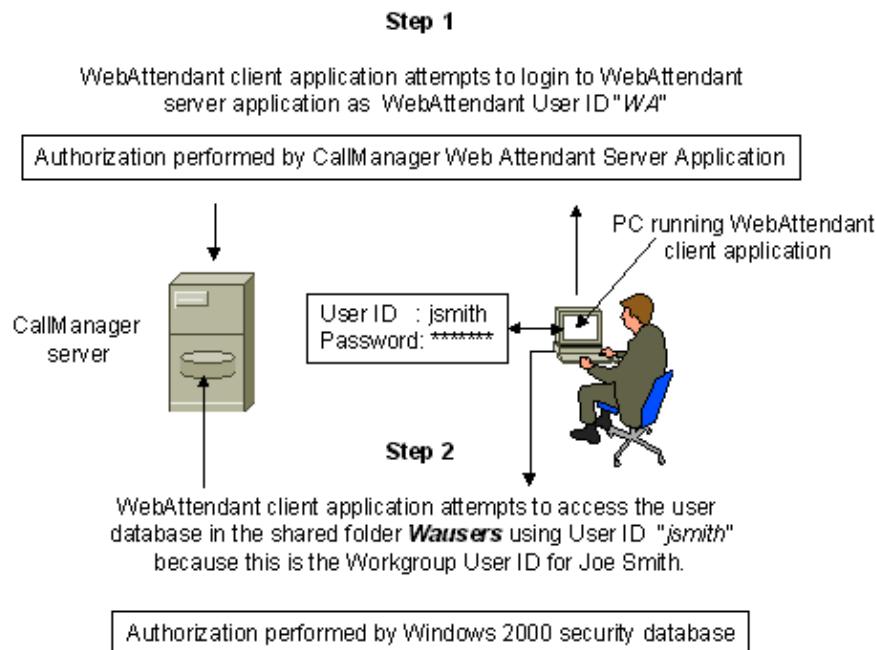
Prerequisites

WebAttendant Users, Devices, and Accounts

This section explains some of the issues related to the provision of access to the CallManager user database for the WebAttendant user. It also explains the relationship between the 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 CallManager users, you can skip this section and proceed to the next section.

The creation of a functional 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 that allows WebAttendant clients to access the user database.



Conventions

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

Windows Workgroup Model

The network security is based on a Windows Workgroup model. The WebAttendant client application accesses the user database on the CallManager server with the default method.

This table shows the steps involved.

Step	Explanation
The user logs onto the PC as jsmith.	In a Microsoft Workgroup based network in which users access resources on other systems, the user must log into their PC. This enables the other devices to identify the user (if required) when they initiate a

	<p>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 CallManager server to determine whether it allows or denies access to the user database in the Users folder.</p>
<p>The user starts the WebAttendant client application with the User ID "WA."</p>	<p>The WebAttendant client application logs on to the CallManager WebAttendant TCD application on the CallManager server with the WebAttendant User ID "WA."</p>
	<p>In this example, the WebAttendant client application logs on as "WA."</p>
	<p>Note: It is important to understand that in this case, the ID "WA" is authenticated by the CallManager WebAttendant server application, not the Windows 2000 server security database.</p>
<p>The WebAttendant client application takes over control of the IP phone for which it has been configured.</p>	<p>The WebAttendant client application has a field for the MAC address of the IP phone that it controls. This is how it knows which IP phone to use.</p>
	<p>The WebAttendant client application console displays the lines (DNs) that have been configured for the IP phone it controls.</p>
	<p>Note: If the user that runs the 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>The WebAttendant client displays the user database.</p>	<p>The WebAttendant client application attempts to access the user database in the shared users folder (WAUSERS) on the CallManager server. Access is granted or denied based on the User ID that the user used to log in to their PC, not the User ID of the WebAttendant client application.</p>
	<p>Note: Many customers use the same User ID for both purposes: to facilitate the management of the accounts and to troubleshoot problems.</p>
	<p>The WebAttendant client application uses the Line State Server (LSS) to track the status of the lines (DNs) assigned to phones.</p>

	<p>In general, if the the WebAttendant client application has been able to log on to the CallManager server application, the connection to the LSS is successful.</p>
	<p>Note: The status bar for each of the lines displayed in the user area at the bottom of the WebAttendant client application console can 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 can transition from red to blue (status available). In some cases, the LSS can never be able to determine the status of a line. This does not prevent the user from the use of the WebAttendant client application console to make calls or to transfer calls.</p>

The network security is based on a Windows NT Domain. The WebAttendant client application accesses the user database on the CallManager server with the default method.

The table shows the steps involved.

Step	Explanation
The PC (Windows NT or Windows 2000) boots up and attempts to join the domain.	In a Microsoft NT/2000 domain based network, PCs that run 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 that runs Windows NT or Windows 2000 that has not been granted access to the domain to access resources on other devices, even though he or she can have a valid user account in the domain.
	Note: This does not apply to PCs that run Windows 95/98.
The user logs on to the PC and domain as "jsmith."	In a Microsoft domain based network in which users access resources on other systems, the user must log in to their PC and into the domain. This enables the other devices to identify the user when they initiate a request to access a resource owned by a different system.
	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

	<p>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 a reference 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 CallManager server to determine whether it allows or denies access to the user database in the Users folder.</p>
	<p>Note: In some cases, the password a user uses to log on to their PC is different from the password used to log on to the domain. If this happens, the user is prompted for a password twice. Most users do not know that they log on to their PC as well as on to the network because they have the same password for both actions.</p>
<p>The user starts the WebAttendant client application with the User ID "WA."</p>	<p>The WebAttendant client application logs on to the CallManager WebAttendant TCD application on the CallManager server with the WebAttendant User ID.</p>
	<p>In this example, the WebAttendant client application logs on as "WA."</p>
	<p>Note: It is important to understand that in this case the ID "WA" is authenticated by the 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 WebAttendant client application. The user's User ID can be "jsmith," and the WebAttendant client application User ID can be something like "jsmith-wa." In this case, access to the user database in the User's folder is configured for "jsmith", not "jsmith-wa."</p>
<p>The WebAttendant client application takes over control of the IP phone for which it has been configured.</p>	<p>The WebAttendant client application has a field for the MAC address of the IP phone that it controls. This is how it knows which IP phone to use.</p>
	<p>The WebAttendant client application console displays the lines (DNs) that have been configured for the IP phone it controls.</p>

	<p>Note: If the user who runs the WebAttendant client application has a primary extension (DN) that other people use to reach them, the IP phone controlled by the WebAttendant client application must be the one that has this DN associated with it.</p>
<p>The WebAttendant client application attempts to access the user database.</p>	<p>The WebAttendant client application attempts to access the user database in the shared users folder (WAUSERS) on the CallManager server. Access is granted or denied based on the User ID that the user used to log onto the domain, not the User ID of the WebAttendant client application.</p>
	<p>Note: Many customers use the same User ID for both purposes: to facilitate the management of the accounts and to troubleshoot problems.</p>
<p>The WebAttendant client application attempts to access the Line State Server (LSS).</p>	<p>The WebAttendant client application uses the LSS to track the status of the lines (DNs) assigned to phones.</p>
	<p>In general, if the the WebAttendant client application has been able to log in to the CallManager server application, the connection to the LSS is successful.</p>
	<p>Note: The status bar for each of the lines displayed in the user area at the bottom of the WebAttendant client application console can 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 can transition form red to blue (status available). In some cases, the LSS can never be able to determine the status of a line. This does not prevent the user from the use of the WebAttendant client application console to make calls or to transfer calls.</p>

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.

Refer to How to Enable Browsing Using NetBIOS Over IP for more information on this subject.

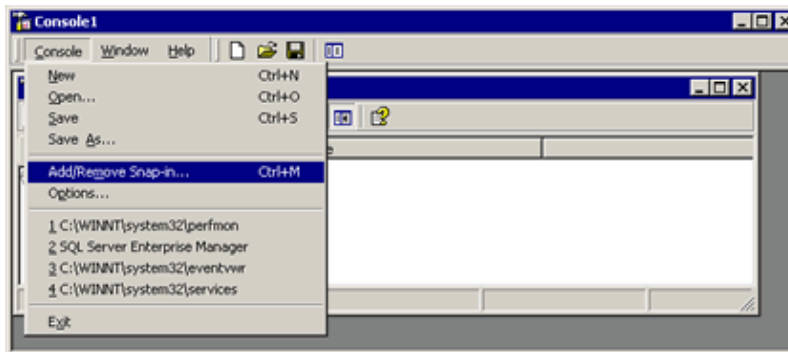
Task 1: Create a New User on the CallManager Server

If your network uses the Domain authentication model, you 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.

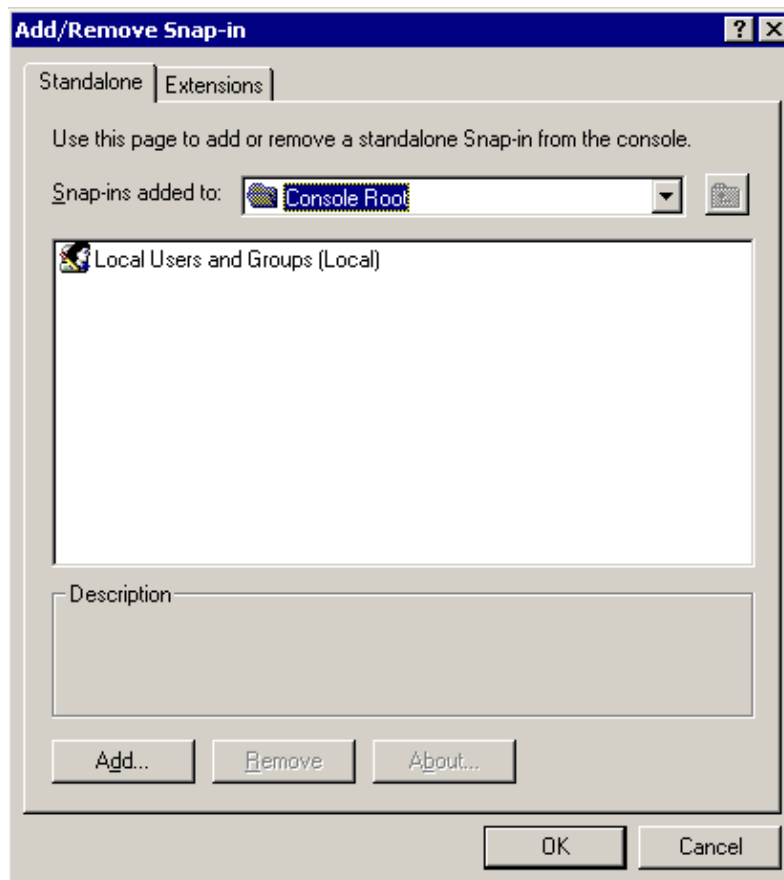
The default configuration for Windows 2000 on the CallManager server does not have the User and Group management application installed on the menus. In addition to the explanation of how to add a new user, this task also explains how to add the application to the menu system.

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

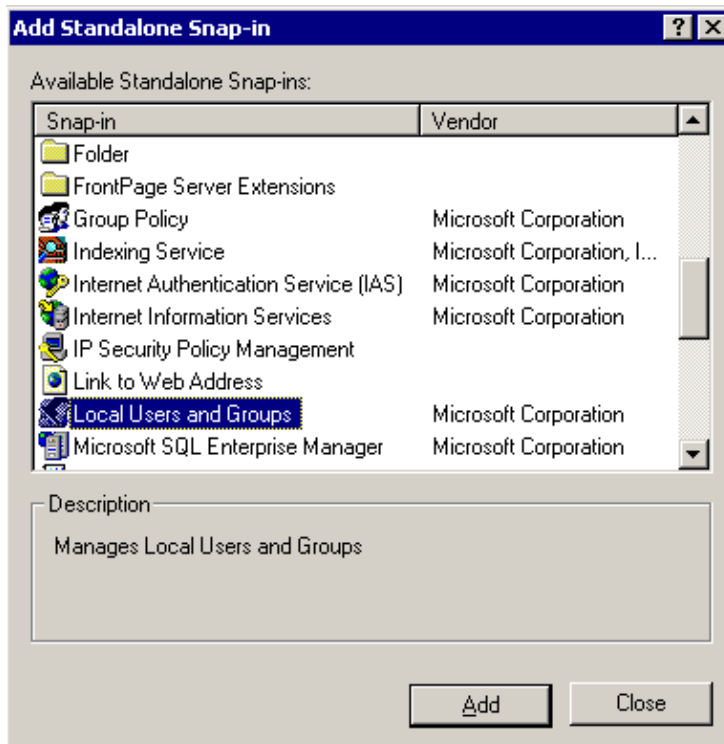
1. Go to the **Start** menu on the CallManager server and choose **Run**. Type **MMC** and press **OK**. This starts an instance of the Console application.
2. From the **Console** menu, choose **Add/Remove Snap-in**.



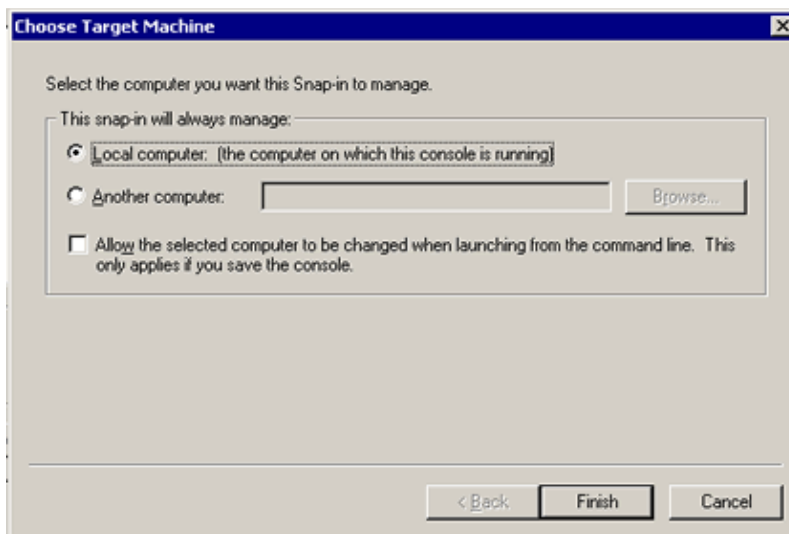
3. Click **Add** from the window that appears.



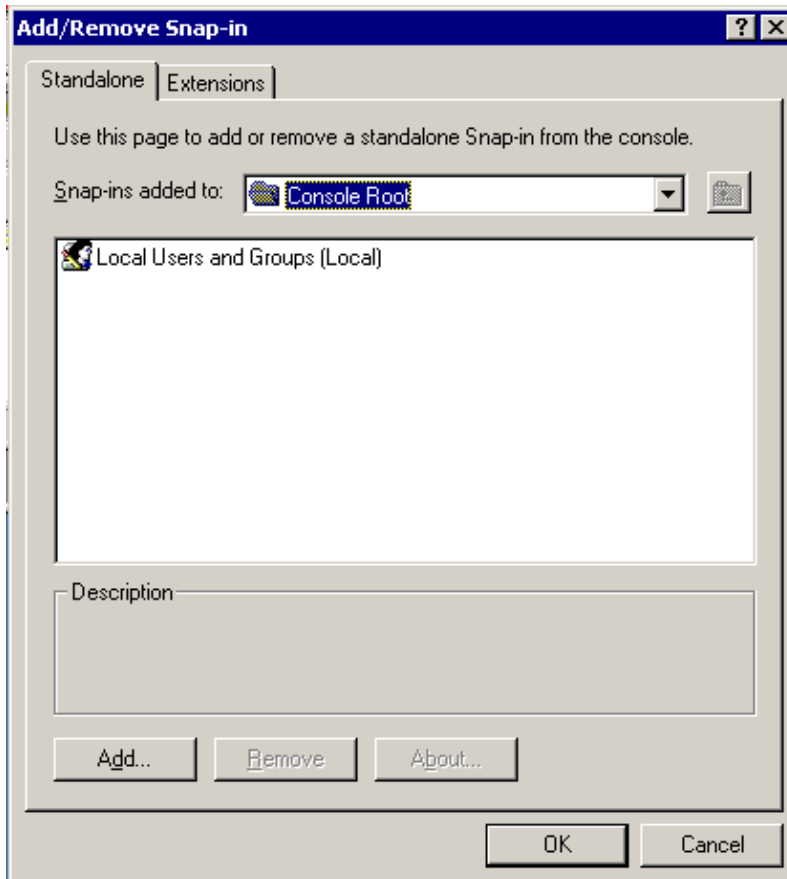
4. Scroll down the menu, locate the **Local Users and Groups** snap-in, and click **Add**.



5. You see a window similar to this. Choose the **Local Computer** option.

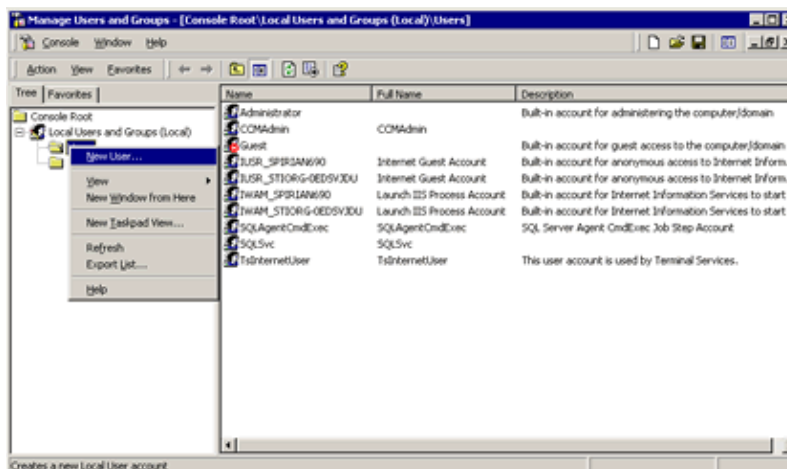


Click **Finish** and then **Close**.
6. You see a window similar to this.



Click **OK**.

7. Right click on **Users** and choose **New User**.



8. In this example, **wa** is used as the User name and **cisco** as the password. Choose 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 User name and password combination is not the same as the User ID and password used by the CallManager WebAttendant user configuration task. Many customers use the same values, but the values are held in separate databases and must be managed separately.

- When you close the MMC Console1 window, you can see a message that asks if you want to save the configuration to make it available from the menu system of the CallManager server. It is recommended that you choose **Save** from this window to ensure that 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 appears 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.

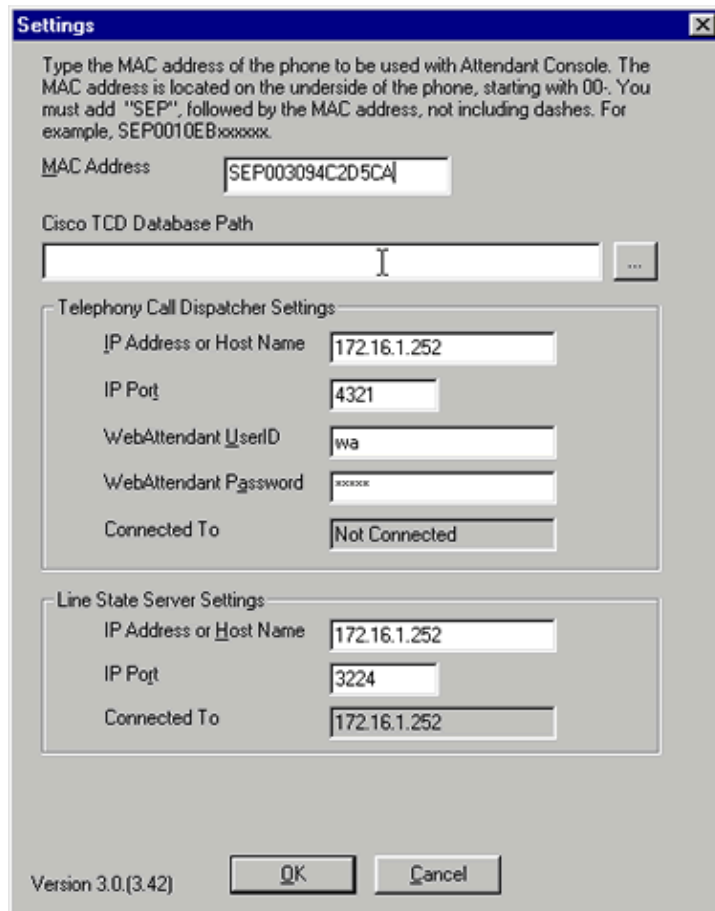
Task 2: Share the Users Folder to Provide Access to the User Database

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

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

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

This window shows that the Cisco TCD Database Path is currently blank, so it uses 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 desktop of the CallManager server to begin navigation to the Users folder, then the Cisco folder.

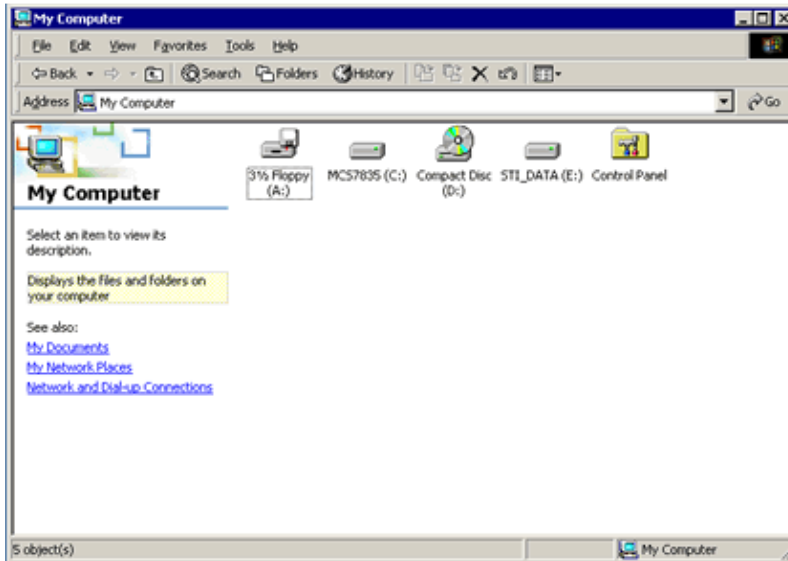


Note: If you see a message similar to this one, you need to choose the **Show Files** option in order to complete the navigation process to the Users folder.

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

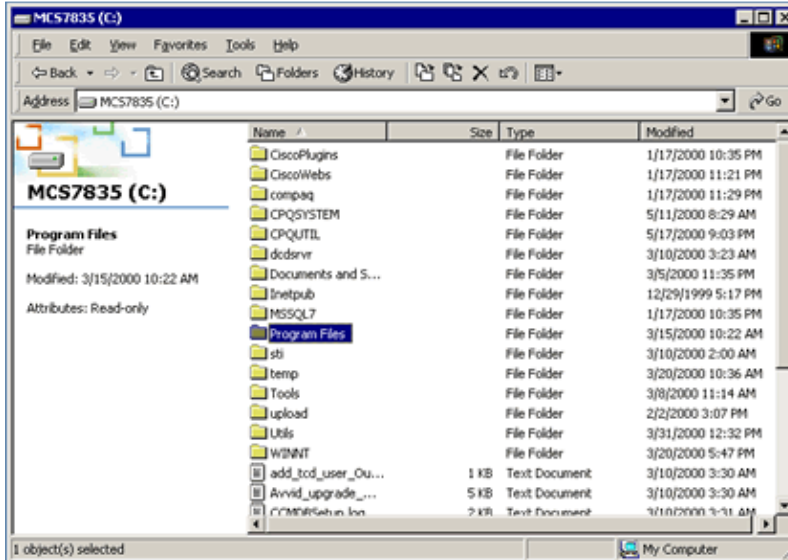
To view the contents of this folder, click: [Show Files](#)

2. You see a window similar to this.



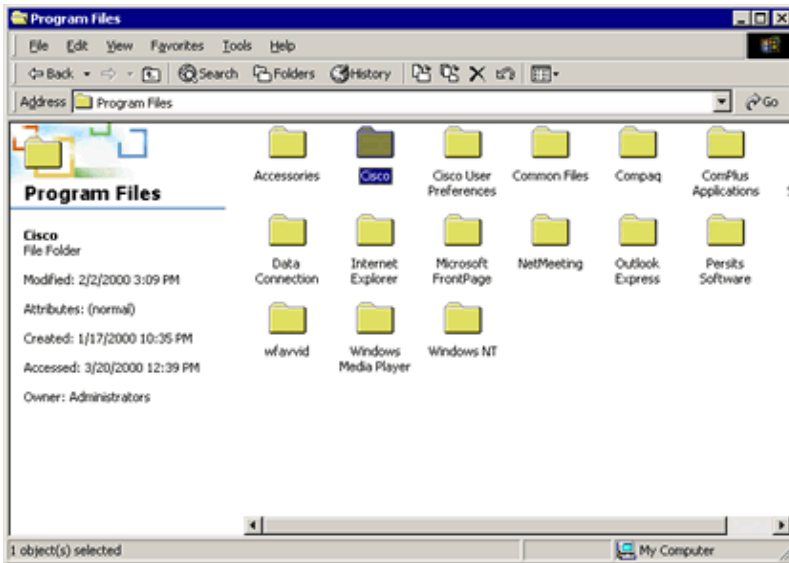
Double click on the **C:** drive.

3. You see a window similar to this.

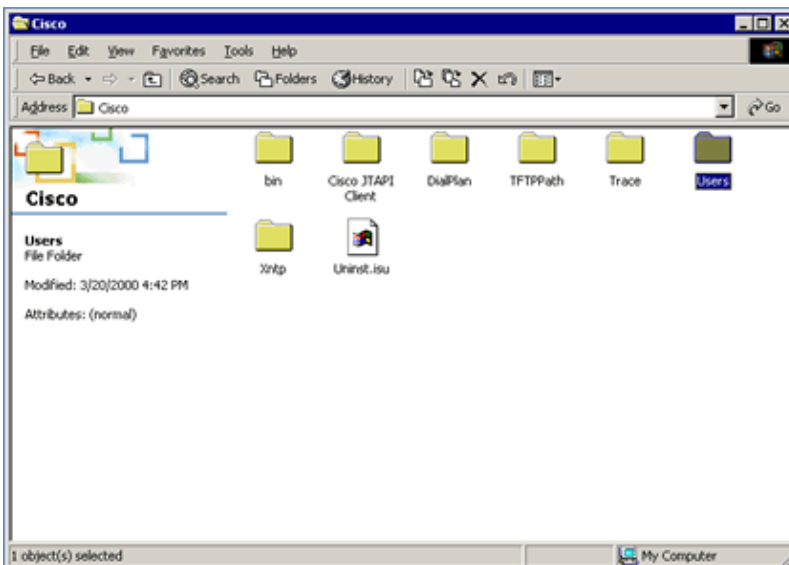


Double click on the **Program Files** folder.

4. You see a window similar to this.



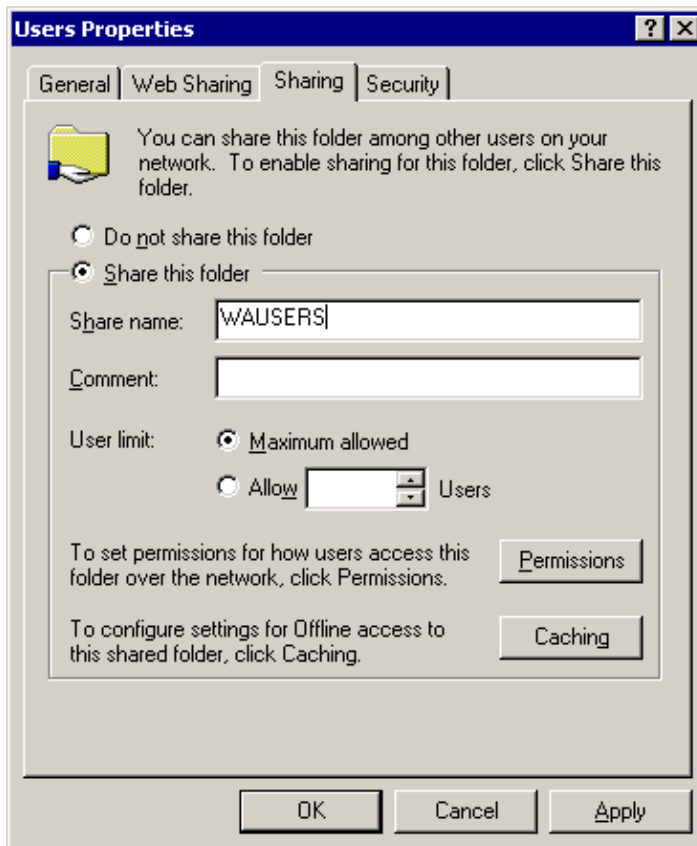
- Double click on the **Cisco** folder.
5. This window shows the location of the Users folder.



- Right click on it and choose **Permissions**.
6. You see a window similar to this.

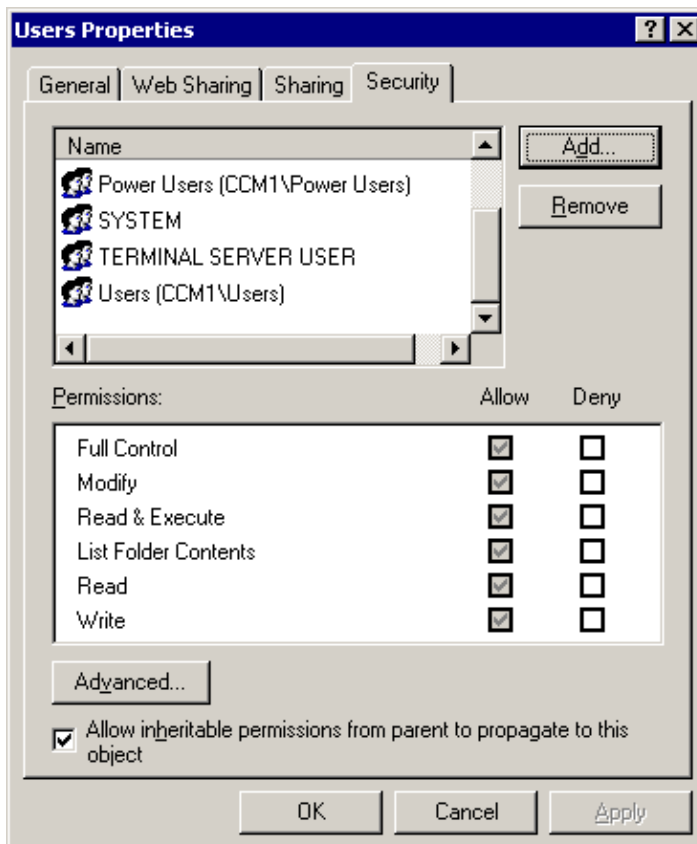
The Sharing tab has been chosen, and the name **WAUSERS** has been entered.

Note: When you use the default method to provide access to the database, as explained in this task, you must use the name **WAUSERS**. The use of any other name does not allow the WebAttendant client application to access the user database.



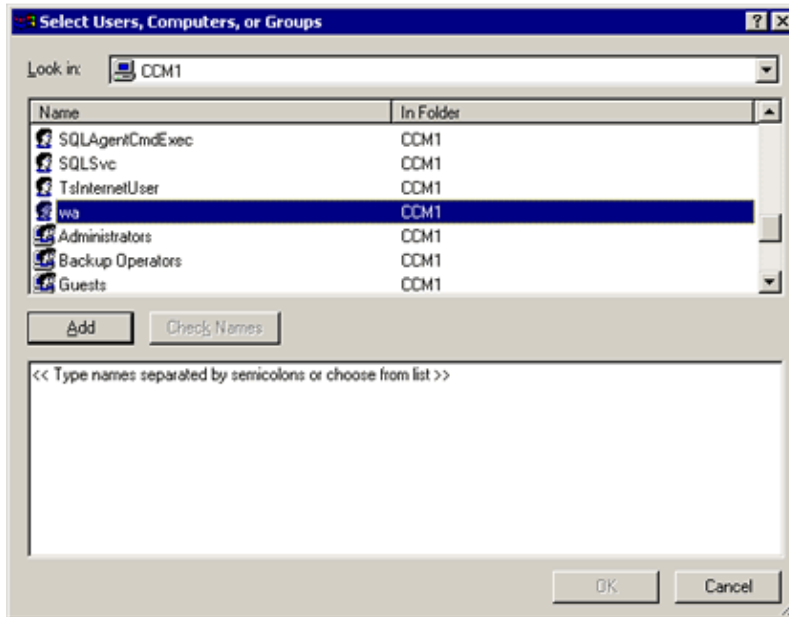
Choose **Share this folder**.

- 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 are assigned in step 9 of this task.



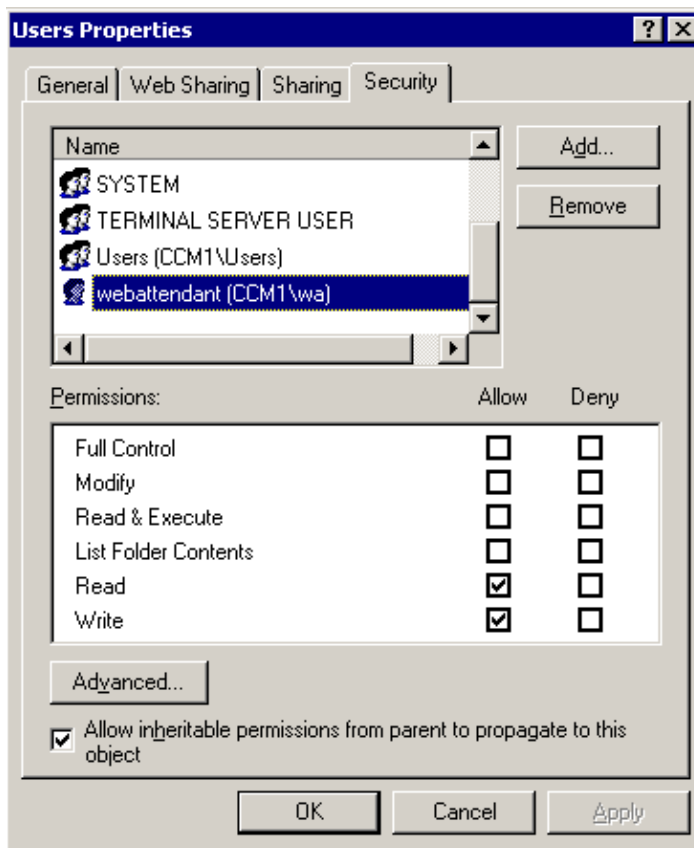
Click **Add**.

8. You see a window similar to this.



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

9. You see a window similar to this. Choose the **Read** and **Write** options.



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

- **Field Notices**
- **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: 7913
