

Tips for Accessing a Webcast

The following are tips on accessing an SCCM webcast utilizing the GoToWebinar Software

1. **Log on 15 – 20 minutes** prior to the actual webcast
2. Click on the link that was provided to you directly from the GoToWebinar email
3. Click on the Launch Software button to download the required files (depending on the speed of your internet this may take a few minutes up to 20 minutes).
4. GoToWebinar will download the required application. Please note this application is only stored in your temporary files and will be removed at the end of the program

System Requirements

PC-based attendees

Required: Windows® 7, Vista, XP or 2003 Server

Macintosh®-based attendees

Required: Mac OS® X 10.4.11 (Tiger®) or newer

Speakers or headset

Technical Assistance Questions: For technical assistance before or during the webcast please contact Go to Webinar at 1-800-263-6317.

Connection Help

Most connection-test difficulties are related to user-authentication issues. Please answer the question below to assist you with determining if this problem exists and which actions to take.

Did you see an Authentication Required dialog box containing three fields labeled Domain, User Name and Password?

Yes, I did see the dialog box and I believe I entered all the correct information but I am still having trouble.

The user name and password required here are the same as those that you use to log on to your Windows computer.

As when entering all user names and passwords, please make sure that:

- You are typing correctly, especially since you cannot see the password characters as you type them.
- Your Caps Lock key is off.
- You do not have any trailing white-space characters in the fields. Check this by deleting and retyping the entire contents of each field or by checking the end of each field for a blank space.

Yes, I did see the dialog box but the Domain field was empty or may be incorrect.

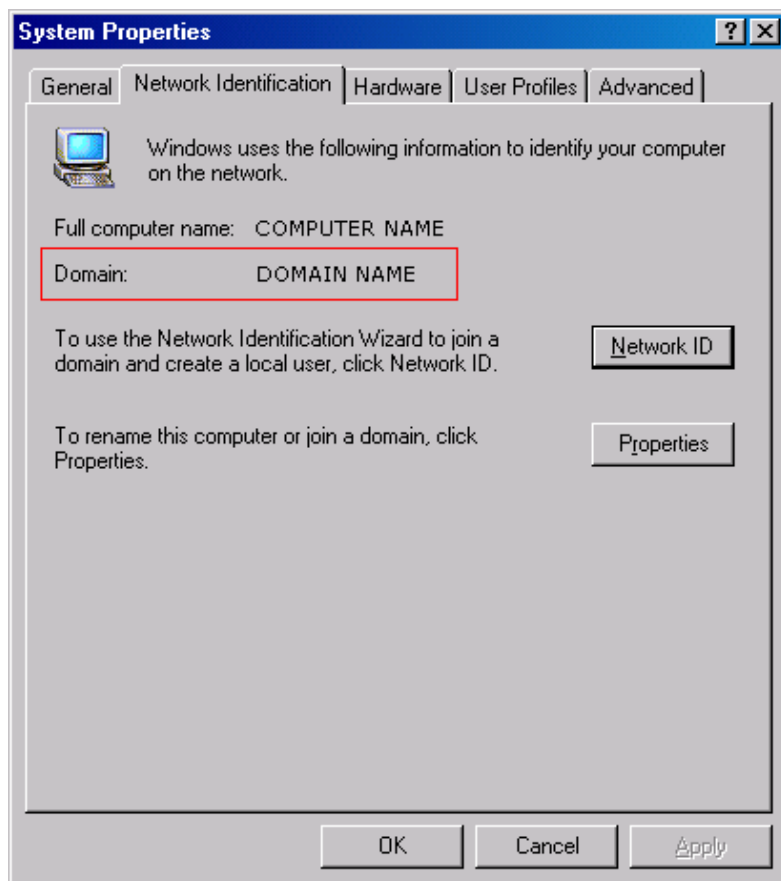
Our software will attempt to fill in the Domain field for you. In rare cases this may not work, and the Domain field will be blank or an incorrect Domain will be shown.

- You can easily determine and verify your correct Domain for the Domain field.

Windows 2000

▶ To find your domain in Windows 2000

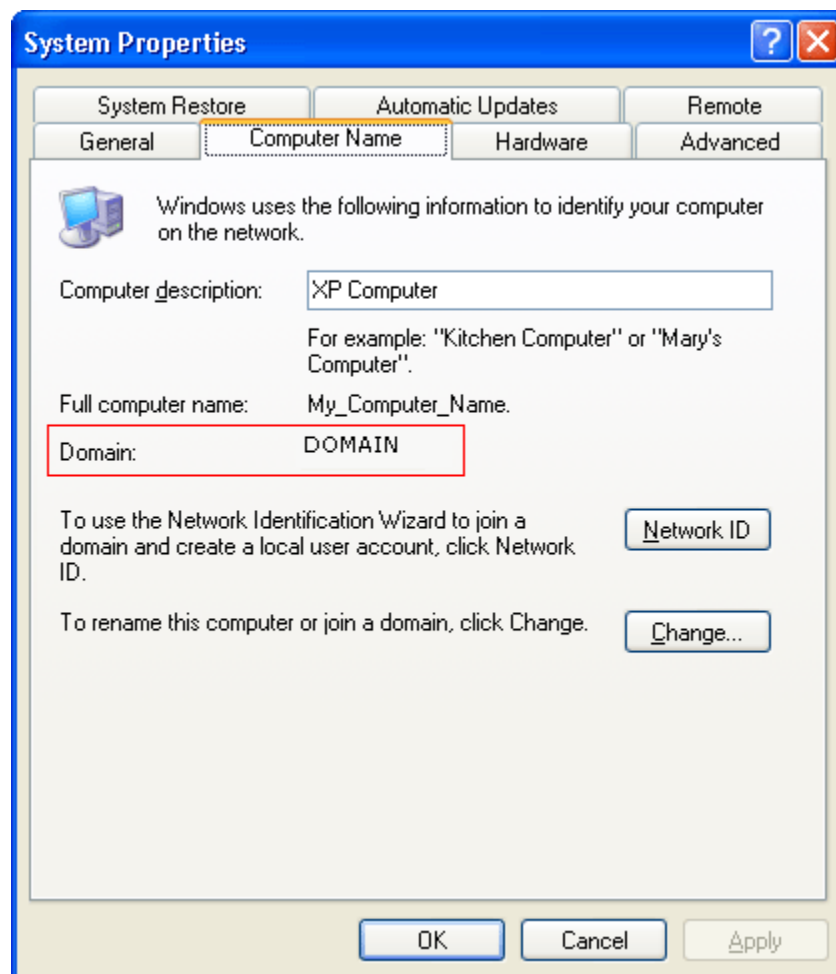
1. Right-click the My Computer icon on your desktop and select **Properties**.
2. Select the **Network Identification** tab.
3. The information shown for **Domain:** is the name of the Windows domain to which your computer belongs on your company network.
4. Please note your domain name so that you can enter it into the domain field of the Authentication Required dialog box.



Windows XP

► To find your domain in Windows XP

1. Click the **Start** button.
2. Right-click the My Computer icon and select **Properties**.
3. Select the **Computer Name** tab.
4. The information shown for **Domain:** is the name of the Windows domain to which your computer belongs on your company network.
5. Please note your domain name so that you can enter it into the domain field of the Authentication Required dialog box.



Yes, I did see the dialog box but the Domain field was missing.

This dialog box indicates that 'Basic Authentication' is in use on your Web proxy. The User Name and the Password required here might be the same as those you use to log on to your Windows computer.

However, your Web proxy may require different passwords than those you use to log on to your Windows computer. Your network administrator can confirm whether or not you have the correct information.

As when entering all user names and passwords, please make sure that:

- You are typing correctly, especially since you cannot see the password characters as you type them.
- Your Caps Lock key is off.
- You do not have any trailing white-space characters in the fields. Check this by deleting and retyping the entire contents of each field, or by checking the end of each field for a blank space.

No, I did not see the dialog box.

Please contact [Global Customer Support](#).

Help, I followed the steps but I am still having trouble.

Please contact [Global Customer Support](#).

Firewall interference

Using GoToWebinar with personal firewalls

If you can't connect and have a personal firewall (ZoneAlarm®, Norton Personal Firewall™, etc.) installed, make sure that GoToWebinar is not being blocked. If so, unblock GoToWebinar and try again.

Additionally, you can configure your personal firewall to enable GoToWebinar to access the Internet anytime you need it to.

Enabling GoToMeeting/GoToWebinar to access the Internet

The first time you run GoToWebinar on a PC that has a firewall installed, you will set off the firewall and be prompted to allow GoToWebinar to access the Internet.

1. Select the check box to *Remember the answer each time I use this program*.
2. Click **Yes** to enable /GoToWebinar to access the Internet.

Using GoToMeeting/GoToWebinar within a corporate Environment

If you do not have a personal firewall but are in a corporate environment, you may have a hardware firewall. Please provide the following document to your IT department so that they may allow GoToWebinar to connect.

Optimal Firewall Configuration

Covers GoToAssist®, GoToMeeting®, GoToWebinar®, GoToMyPC® and future product deployments involving our servers as of May 2010.

1. Citrix Online products are configured to work outbound through ports 8200, or 80 or 443. In a restricted environment port 8200 can be set up for outbound connections. Our products do not listen for, nor do they require, any inbound connections. Connections outbound via port 8200 are optimal, although connections through ports 80 and 443 can also be used.
2. If your firewall includes a content or application data scanning filter, this may cause blocking or latency, which would be indicated in the log files for the filter. To address this problem, verify the below IP ranges will not be scanned or filtered by content or application data scanning filters by specifying exception IP ranges that will not be filtered.
3. If your security policy requires you to specify explicit IP ranges, then configure your firewall to limit port 8200 or 80 or 443 destination IP addresses to only the Citrix Online ranges listed below.

Important Note: Steps 2 and 3 are discouraged unless absolutely necessary because such IP ranges need to be periodically audited and modified, creating additional maintenance to your network. These changes are rare, but they may be necessary to continue to provide the maximum performance for the Citrix Online family of applications. Maintenance and failover events may cause you to connect to servers within any of the ranges.

Citrix Online server / Datacenter IP addresses for use in firewall configurations Equivalent specifications in 3 common formats			
Citrix Online Assigned Range by Block	Numeric IP Address Range	Netmask Notation	CIDR Notation
Block 1	216.115.208.0 - 216.115.223.255	216.115.208.0 255.255.240.0	216.115.208.0 / 20
Block 2	216.219.112.0 - 216.219.127.255	216.219.112.0 255.255.240.0	216.219.112.0 / 20
Block 3	66.151.158.0 - 66.151.158.255	66.151.158.0 255.255.255.0	66.151.158.0 / 24
Block 4	66.151.150.160 - 66.151.150.191	66.151.150.160 255.255.255.224	66.151.150.160 / 27
Block 5	66.151.115.128 - 66.151.115.191	66.151.115.128 255.255.255.192	66.151.115.128 / 26
Block 6	64.74.80.0 - 64.74.80.255	64.74.80.0 255.255.255.0	64.74.80.0 / 24
Block 7	202.173.24.0 - 202.173.31.255	202.173.24.0 255.255.248.0	202.173.24.0 / 21
Block 8	67.217.64.0 - 67.217.95.255	67.217.64.0 255.255.224.0	67.217.64.0 / 19
Block 9	78.108.112.0 - 78.108.127.255	78.108.112.0 255.255.240.0	78.108.112.0 / 20
Block 10	68.64.0.0 - 68.64.31.255	68.64.0.0 255.255.224.0	68.64.0.0 / 19
Block 11	206.183.100.0 - 206.183.103.255	206.183.100.0 255.255.252.0	206.183.100.0 / 22
Block 12	173.199.0.0 - 173.199.63.255	173.199.0.0 255.255.192.0	173.199.0.0/18

If a connection still cannot be established, please contact [Global Customer Support](#).