

Responding to Sygate Messages

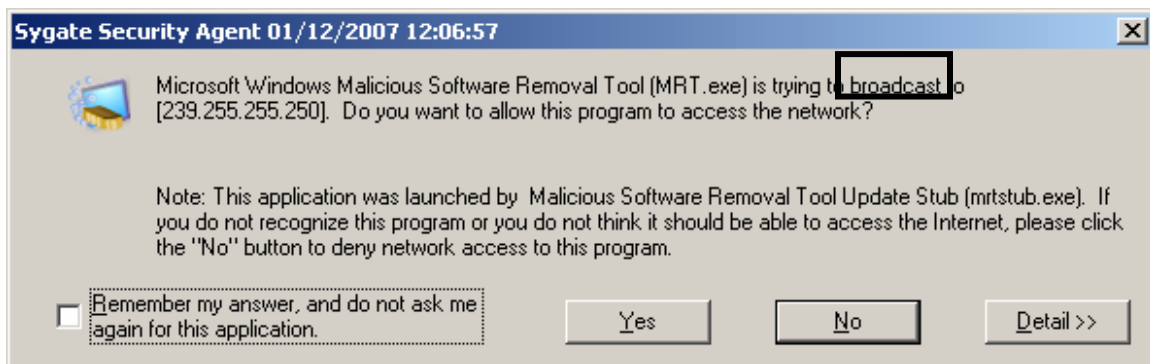
Sygate is a managed firewall program for your PC. A firewall program has the ability to prevent certain types of network activity in order to protect your computer. Although Sygate is managed by Technology Services, and rules are already set about some types of network activity, sometimes a program on your PC will attempt to perform a type of network activity which Sygate is unsure about. In these cases Sygate will prompt you with a dialog box asking you, the computer user, if you want to allow that particular network activity. How should you answer?

General rules of thumb:

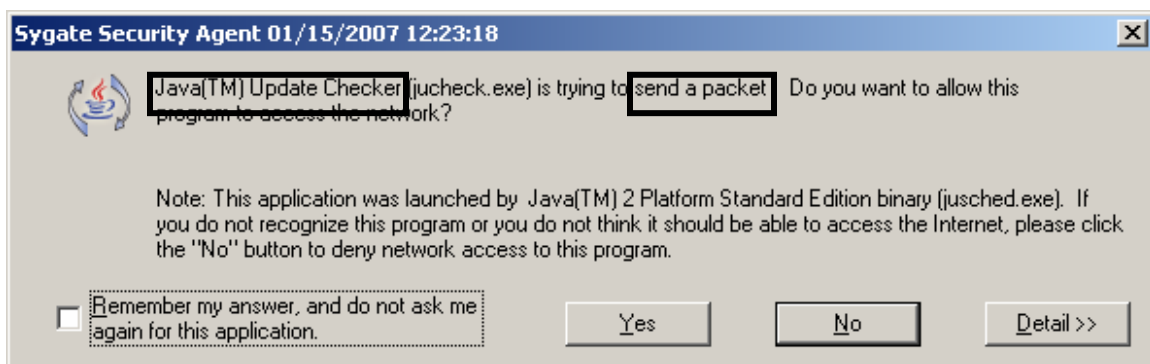
- If a request is about a program that have open and running, click YES.
- If the request is about a program that you trust and consider legitimate (one that you know is installed on your computer by you or by Hartwick College), click YES.
- If the program is unknown to you, or you think it has no legitimate reason to contact the network, click NO.
- If you have any questions, contact the Technology Resource Center at x-4357.

Examples of Sygate prompts and how to respond:

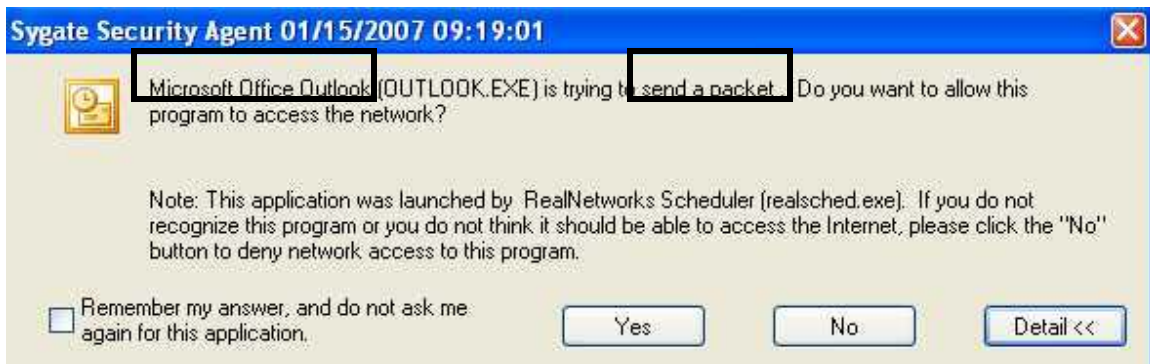
1. **Broadcasts:** If Sygate says that any program is trying to **BROADCAST**, you should click **NO**. In the case of a broadcast, you may wish to check the box for “remember my answer” before clicking no.



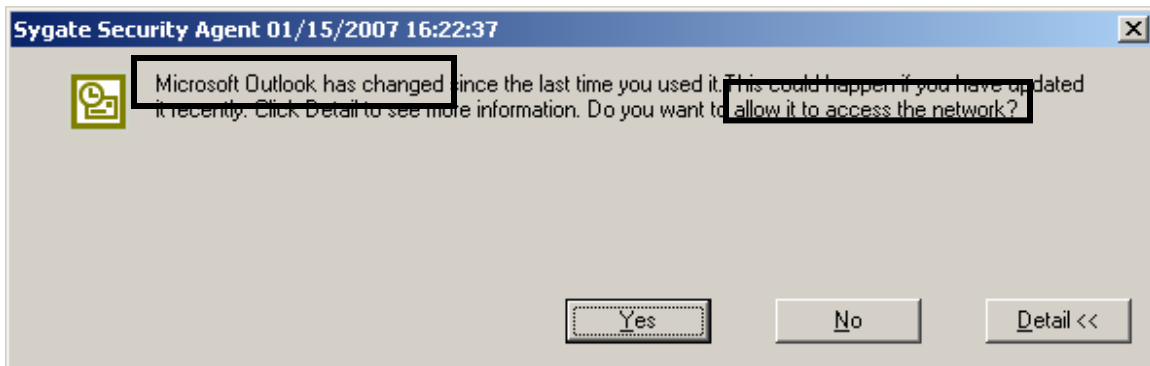
2. **Updates:** Sygate may prompt you when a program’s update checker is trying to send a packet or to check for **UPDATES**. This might be Java, Adobe, a Microsoft product, Symantec or some other program. If it is a program that you know you run on your computer, and that you trust, click **YES**. You may also wish to check the checkbox for “remember my answer”.



3. **Legitimate program sending a packet:** If you see a legitimate program (one that you recognize and know is running on your computer) trying to send a packet, click **YES**. In the window below, Outlook is trying to contact a Hartwick server. If you click no, you will have trouble sending and receiving e-mail. If you wish more info about where the packet is going, you can click the details button, or you can call the TRC at x-4357.



4. **Program that has changed accessing the network:** After updates to a program have been installed, including Windows updates, you may be asked if this "changed" program can access the network. If it is a legitimate program, click **YES**. If you aren't sure, contact the TRC at x-4357.



5. **Remote computer contacting your computer:** Click **NO**

