



Security Considerations

1. Windows
2. Default Configuration
3. Unused Services
4. Incoming Connections
5. Default Port Numbers
6. IP Address Filtering
7. Secure Sockets Layer
8. User Account and OS Integration
9. IP Address Lockout
10. The Human Factor
11. Summary

RemotelyAnywhere has additional security features that add to the built-in security features of Microsoft Windows XP/2000/NT. Configured properly, you can minimize serious security risks.

This document has been prepared with a single Windows web server in mind. There may be steps that do not apply to your configuration.

1. WINDOWS

A Windows XP/2000/NT computer sitting unprotected on the Internet is quite easy to access. For this reason it is advisable to take security precautions. This guide was written with a security-conscious system administrator in mind, so we're not going to go into details about securing a Windows machine for the Internet, but here are a few key points:

- Disable NetBIOS on the network adapter that provides Internet access.
- Rename any built-in accounts that are in use.
- Disable any built-in accounts that are not in use.
- Apply the latest patches to the operating system and its components.

2. DEFAULT CONFIGURATION

Having configured the computer to be as safe as possible, you can now turn to securing RemotelyAnywhere. The default RemotelyAnywhere configuration is as follows:

- Accepts Web and Console connections on port 2000 on all network adapters.
- Accepts Telnet connections on port 23 on all network adapters.
- Accepts SSH connections on port 22 on all network adapters.
- All above connections must be authenticated with a username/password pair that identifies a user who's a member of the Administrators group.
- Connections are accepted from any internet address.

3. UNUSED SERVICES

Decide which RemotelyAnywhere services you want to use on the computer, and disable the rest. We recommend disabling Telnet and SSH if you do not need access to a command prompt - if you do, disable Telnet and leave SSH running.

4. INCOMING CONNECTIONS

The IP address on which RemotelyAnywhere listens can also be changed. Assume you have a web server placed on the Internet named **www.MyWebServer.com** and RemotelyAnywhere is installed on your web server on port 2000. The web server can now be remotely managed by typing "**http://www.mywebserver.com:2000**" in any web browser. However, by adding another IP address to the server for remote administration purposes and restricting RemotelyAnywhere to listen only to that particular address the server can only be accessed from this address. For example, if you add the address **177.246.27.91**, the server can only be accessed by typing **http://177.246.27.91:2000**. Any attempt to access RemotelyAnywhere on the original address (**http://www.mywebserver.com:**

2000) will result in refused connections on the protocol level.

If possible, try to use an IP address that's on a different subnet than the addresses in use by the website or websites hosted on the computer. Most attacks begin with a port scan on the target computer. If the attacker sees that port 2000 is open on www.MyWebServer.com they will know that RemotelyAnywhere is installed on the computer. Using a different administrative IP address will hide this fact.

5. DEFAULT PORT NUMBERS

Unlike the default Windows XP/2000/NT services, such as file sharing, the port providing access to RemotelyAnywhere can be changed to be something the potential intruder cannot detect or is not known. You should, however, pick numbers that are easy to remember.

6. IP ADDRESS FILTERING

Another way to strengthen security is IP Address Filtering. RemotelyAnywhere can be told the IP addresses, or ranges of IP addresses, from which to accept connections. With this technique employed, even if someone took the time to find out what IP address and port to connect to, they could not connect if they were not on the "trusted" list. Any number of IP addresses and networks can be listed as "trusted".

Conversely, a list of IP addresses and networks from which RemotelyAnywhere will refuse to accept a connection may be designated.

If you'll only be connecting to the computer from a number of known networks, you can tell RemotelyAnywhere to ignore incoming connections from anywhere else.

Suppose that the computer is in a datacenter. You will want to access it from the office, from home, and from your wireless PDA. In this case, create an IP address filtering rule that allows connections from these three networks but denies connections from any other computer. You will need to know the Internet IP address blocks and subnet addresses for the three networks you wish to enable. If you have dialup accounts in any of these locations, contact the ISP's customer service to find out the range of IP addresses that they can assign to you.

You will not "trust" everyone who's on your ISP, of course - but even if they have a whole class A subnet it's better to grant access to it as opposed to not setting up IP address filtering at all. Granting access to a huge class A subnet and denying connections from anywhere else locks out about 99.6% of possible intruders.

7. SECURE SOCKETS LAYER

Set up Secure Sockets Layer on the computer using the "SSL Setup" menu option under Security in RemotelyAnywhere's menu. You can also disable unsecured connections under Preferences > Network. This way, all traffic between the host and the remote computers will be encrypted using industry-strength 128-bit ciphers, protecting your passwords and data.

8. USER ACCOUNTS AND OS INTEGRATION

The above methods are effective for dealing with unwanted visitors. However, they only prevent possible intruders from getting to the login screen where they must authenticate themselves with a username and a password. A valid Windows XP/2000/NT username and password must be supplied to RemotelyAnywhere in order for the user to be granted access. Initially, this must be any user who has administrative credentials. After configuring RemotelyAnywhere, any user or group can be granted access to the remote administration interface. Not all administrators

must be given access, and access is not necessarily limited to administrators. It is up to the administrator to configure RemotelyAnywhere to best suit their needs. There is simply no way around being authenticated by RemotelyAnywhere. If it fails, the user will be denied access. Once the user has been authenticated RemotelyAnywhere impersonates them towards the operating system when servicing requests. This ensures that the user is only able to perform actions that their Windows credentials allow.

There is always the chance that someone will gain access to the password by a brute-force method or by simply guessing until access is granted. There are two very effective measures against this.

The first is common sense! The System Administrator must always remember to use a password that is difficult to guess and set a password policy that enforces this on ordinary users as well. Passwords should be long, and preferably contain numbers and special characters, such as punctuation.

The second is a feature provided by RemotelyAnywhere and is discussed below.

9. IP ADDRESS LOCKOUT

RemotelyAnywhere can be set to lock out IP addresses after a user specified number of failed login attempts. The System Administrator determines how many failed login attempts are allowed within a certain number of seconds, and for how long the offending IP address should be locked out. It will then be put on the “distrusted” list and all future connection attempts will fail. For example, a typical configuration might be: 5 unsuccessful login attempts in a 30-minute time window would result in the IP address being locked out for 30 minutes. The lockout period, as well as the amount of time the user initially has to successfully log in, can be as long as 4 billion seconds. This is fundamentally different from Windows’ own lockout mechanism. When Windows detects a certain number of failed login attempts, it disables logins to that account from all network locations as opposed to disabling the offending network address only. The two lockout methods complement each other.

10. THE HUMAN FACTOR

Any chain is as strong as its weakest link. Always remember to use long, hard to guess (but easy to remember) passwords. Always use encrypted connections to RemotelyAnywhere, such as SSL or SSH. Always log off when you’ve finished working. Set up the additional security measures detailed above if they apply.

11. SUMMARY

Reducing or eliminating security threats is a fairly simple, yet vitally important, process. A System Administrator is able to conceal the fact that RemotelyAnywhere is installed on a machine. RemotelyAnywhere can be configured to accept connections only from “friendly” computers. A valid Windows XP/2000/NT username and password must authenticate the user attempting to connect to RemotelyAnywhere. This password can be made very difficult to guess. Finally, System Administrators are able to use the state-of-the-art encryption found in RemotelyAnywhere to protect the data sent and received by the browser, so no unauthorized users can gain access to sensitive information.