Guide for Network Administrators

Guide for Network Administrators

How to optimize & tune networks and computers for Skype

Version 1.0.1, April 2005

Skype Technologies S.A.

Trademark acknowledgments

Skype is a trademark of Skype Technologies S.A. in Luxembourg and other countries. Windows is a registered trademark of Microsoft Corporation in the United States and other countries. Linux is a registered trademark of Linus Torvalds. Apple and Macintosh are registered trademarks of Apple Computer, Inc. in the United States and other countries. UPnP is a trademark of the UPnP Implementers Corporation.

Other names and brands may be trademarks or registered trademarks of others.

Disclaimer

This document describes services offered by Skype Technologies S.A., its subsidiaries or affiliates as of the time of writing. Skype services may be modified or terminated at any time according to the current Skype Terms of Service available at the official Skype website. The internal design of Skype software and networking techniques are subject to change without prior notice.

Skype is not responsible for the content of any third-party websites or documents that may be referenced in this document. Any such references are provided purely for the convenience of Skype's customers, who are advised that Skype has not verified that such references are accurate or fit for any particular purpose.

Big Points for Network Administrators

skype™

Big Points for IT Managers

1

Skype works with antivirus tools

Inbound and outbound Skype file transfers are scanned by the major antivirus products
Page 21

2

Skype protects your privacy

Skype's encryption and authentication may help you meet national privacy mandates
Page 5

3

Firewalls stay secure

Skype doesn't require any inbound openings in your firewall — often no change is needed at all
Pages 7 and 17

4

Users are protected from spam

Skype technology stops Skype-based spam and gives users full control over their contacts
Pages 23 and 27

5

Skype preserves your IT budget

With zero per-client costs and favorable outbound call pricing, Skype can slash your costs

1 Understanding how Skype works

"The initial ARPA network working group met at SRI on October 25-26, 1968. It was generally agreed beforehand that the running of interactive programs across the network was the first problem that would be faced."

–JEFF RULIFSON, RFC NUMBER 5

Overview

The Skype software and services provide individuals with a new, secure and innovative way to communicate with other people using the Internet as the medium of transport for messages, whether they're voice calls, text messages or other forms of communication. Skype is the world's first decentralized telephony network, but it provides far more services than just voice calling that's carried over the public Internet.

By using a compact client program, which is available in versions for several popular computer platforms, a Skype user is able to send or receive text messages, hold voice calls and exchange data files with other persons. Communications with other on-line Skype users are provided free of charge, while certain premium services, such as the placing of voice calls to standard telephone numbers, are available for a modest fee.

Skype communications rely largely on peer-to-peer communications techniques in order to improve the quality of voice calls and to reduce the latency of data transfers between users. The term "peer-to-peer", frequently written as "P2P", is a class of software applications that rely on resources located at the network edge, such as the large number of individual personal computers that are always connected to the Internet, rather than relying on large and costly centralized computer servers. It's this aspect of Skype networking that makes it incredibly robust and tolerant of network failures: Skype has no single "critical node" upon which the service relies for its operation.

Description of Skype services

The utility of Skype services are found in the voice calling, file transfer and instant messaging facilities that are built into every user Skype software client. Underlying these services are Skype's directory, presence management and network traversal technologies.

Skype provides its users with a variety of communications and related services, including the following:

- Voice calling to another Skype user
- Voice conference calling
- Voice calling to traditional telephone lines (SkypeOut)
- Voice calling from traditional telephone lines (SkypeIn)

- Chat, providing instant messaging for groups of up to 48 participants
- Cross-platform file transfer
- Directory and presence management

Skype user programs have been built for use on several popular computing platforms, including personal computers running Windows XP, Windows 2000 or Linux, Apple Macintosh computers running Mac OS X and Pocket PCs running Windows Mobile 2003.

Skype is safe and trustworthy

In many circles, people confuse the term “P2P” with file sharing, but what Skype P2P means is that we have a lower cost structures because we have less infrastructure to deploy and manage. Those cost savings are passed directly along to you, the user. Skype is committed to producing high-quality software products and services that are best-in-class and that help our users in the most reliable and cost-effective manner.

No adware and no spyware

What is adware? Adware is software, often installed without the user’s consent or with consent that’s buried in the middle of a complex end-user licensing agreement, that displays advertising to a user, often even while the host application is not running. Some adware even takes such action as changing a web browser’s home page or popping banners up while no other programs are running.

What is spyware? Spyware is software, normally installed without the user’s consent, or mislabelled to appear to be a useful utility, that secretly reports on the habits of a user. Some spyware even captures keystrokes or copies entire web pages and clandestinely sends this information for commercial exploitation.

Does Skype include adware or spyware? **NO!** Skype does not, and never has, included adware or spyware in the Skype application or in the Skype installer. Skype is adware-free and spyware-free.

In order to operate its service, Skype does collect and process data about your calls. For instance, if you maintain SkypeOut calling credit, we collect information about SkypeOut calls you place so that we can maintain your account balance. Skype explains how this data are used in the Skype Terms of Service, which are posted on Skype’s web site at `http://www.skype.com/company/legal/terms/tos_voip.html`

How Skype works

To provide the most robust and scalable service possible, Skype uses a design called a “supernode P2P architecture”, over which all Skype communications are handled. Rather than rely on a single big central server to complete calls, Skype software clients directly interact with each other to ensure that the network directory is up to date and that calls are quickly completed. Put another way, Skype users not only use the network as a way to complete calls, their participation in the network helps make the Skype network work.

Compare this to the traditional telephone network, in which all users are connected to each other through a hierarchical set of expensive switches that are set up in several tiers in order to allow the completion of local, regional and long-distance calls. The supernode P2P architecture used by Skype avoids the physical connections needed by the traditional phone network. The Skype network makes this work because of its proprietary Global Index distributed directory, though which users can find out about each other, place calls, send messages and communicate, all without using any central servers.

Supernode P2P architectures have been successfully used by a number of earlier peer-to-peer software applications. A supernode is a regular Skype client that provides a bit of assistance to the Skype network by handling contact lists and helping out with call routing. This service, called the Global Index function of Skype, allows Skype to build a reliable suite of services atop a constellation of unreliable peers. Skype's network can scale to at least tens of millions of simultaneous users without foreseeable performance or reliability issues.

When a Skype client becomes a supernode, it accepts network connections from a small number of other Skype users for the purpose of maintaining the accuracy of the Global Index. Although the supernode activity is entirely transparent to the user, a Skype client that is unable to receive inbound network connections (such as a user behind a NAT or firewall) will never become eligible to become a supernode nor will it ever be asked to relay a third party's traffic.

Firewalls and network address translation

Most Voice over Internet Protocol (VoIP) solutions are designed for enterprise environments. Many residential broadband users would be unable to make VoIP calls without complex reconfiguration of their routers and firewalls, often because the customer's network includes a restrictive firewall or a network address translation (NAT) gateway, neither of which are easily capable of carrying VoIP calls directly.

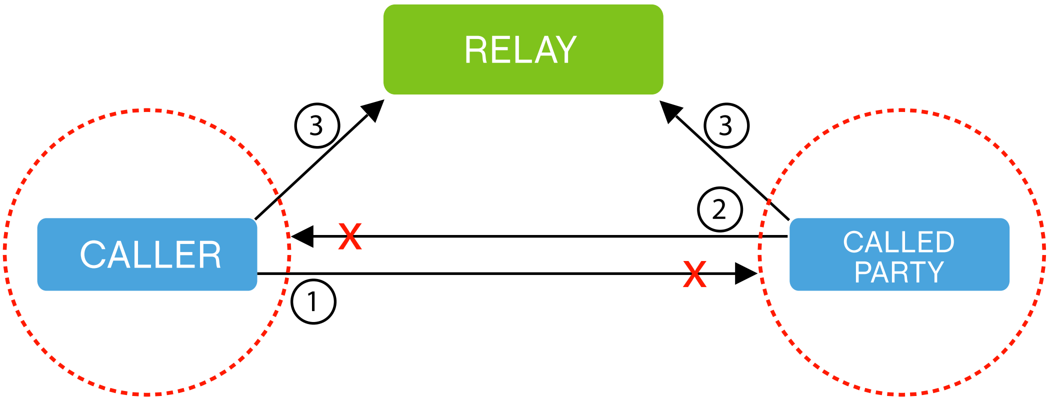


Figure 1-1 Two firewalled Skype users establishing communication

Skype's P2P architecture solves this, allowing calls from users located behind a firewall or a NAT gateway to be transparently routed through the help of a peer that is unfirewalled. This means that anyone can use Skype to make VoIP calls without the need to reconfigure routers or firewalls. In business environments, there is no need for a user to demand specialized deployment or operations support for the user client. There is no need to configure ports, gateway names or proxies. In the vast majority of cases, administrators need make no changes to firewall or network configurations.

As shown in Step 1 of Figure 1-1, when two Skype users wish to communicate with one another, the caller first simply tries to contact the called party directly. However, if the called party is protected by a firewall, then the called party's computer is asked by the Global Index to connect in the reverse direction back to the caller's computer, as shown in Step 2 of Figure 1-1. If either of these connections succeeds, then the call is established using a direct connection, providing the most reliable and lowest-latency connection possible between the two parties.

However, if both parties to the call are behind restrictive firewalls, then neither party will be able to reach the other directly. This requires the call to be relayed by a third parties who are reachable by both parties to the call. To do this, a small number of Skype users are selected as relay hosts by the Global Index.

In this case, both the caller's and the called party's computers establish a direct link to these relay computers, as shown in Step 3 of Figure 1-1. Once these connections are established, the caller and called party can communicate because the relay computer will pass data packets between the two parties. One important factor to consider is that even when calls are relayed by third parties, the entire contents of the call, including any voice conversations, text messages or file transfers, are encrypted between the caller and the called party.

Reaching outside networks

One of the difficulties that plagues many VoIP solution is that the call is unable to pass across network boundaries. This problem may arise due to the presence of network address translation (NAT) equipment at the network's boundary or due to restrictive rules put in place on a firewall at the network edge.

To allow users the greatest possible flexibility, Skype has implemented a robust set of NAT traversal techniques in its software, allowing Skype to frequently be able to operate in situations where traditional VoIP telephony would fail. We discuss optimization and tuning parameters for networks in Chapter 2.

Most networks in use today in homes and offices use NAT to allow easier administration of the network without requiring each network to obtain its own block of scarce network addresses. An effective way to set up P2P communications between two computers hosted on private networks — ones behind NAT devices — is to use a technique called "hole punching". This technique is widely used by application software communicating using UDP packets and can also be used to establish connections using the more reliable TCP protocol.

Although the name "hole punching" might suggest otherwise, this technique does not compromise the security of private networks but instead seeks to establish communications by working within the policy framework of most NATs. These techniques signal to the NAT devices in the path of a communication that the P2P sessions have been solicited and should therefore be passed.

Skype security

The security properties of Skype services are intended to meet the following objectives:

Confidentiality. The contents of user communications must be accessible only to the intended parties and the identity of participants to a communication must be verifiable. In addition, details of user accounts and specific user activity must be accessible to users as well as to Skype staff, vendors and partners, but only to the extent necessary to provide Skype services.

Integrity. User communications must be verifiably authentic; by corollary, communications must not be corrupted or modified while in transit. Communications purporting to be from a particular Skype user must be verifiable as such.

Availability. Skype services must be available and accessible to legitimate Skype users when needed.

These aspects of security are paramount for IT managers and Chief Information Officers who are ensuring that their organisations are in compliance with national and international privacy regulations such as HIPAA (an American health privacy directive), the European Union Privacy Directive, or similar national legislation.

Authentication of user identities

Skype's notion of identity (a "Skype user") is based upon the Skype username. Conceptually, a Skype username represents an autonomous individual, despite the fact that Skype does not itself have any limitation preventing a single individual from possessing more than one Skype username.

Skype users authenticate their identity by using a passphrase that is initially set at the point when a user account is created. Users may change their passphrase at any time through the Skype user account management system. This password is used both to log in to the Skype software and to log into Skype's web-based account manager. Users should never use their Skype password for any other program or service. A user may choose to allow for automatic logins to Skype by saving their password, but this option should never be used on shared or public use computers.

Once a user has authenticated his identity by presenting the correct passphrase, a user is given a limited-duration electronic credential that is digitally signed by Skype, using the private portion of Skype's 1536-bit (2048-bit for paid services) RSA signing key. This signed credential is sent by a Skype user who is identifying himself to another Skype user. The presence of a valid signature on this credential can be used to validate the identity of the Skype user without any need to contact a central server.

Encryption of Skype communications

All message contents sent between any pair of Skype users is strongly encrypted from end to end. Because Skype communications are sometimes relayed through third parties as part of the NAT traversal process, it's important that all communications be encrypted from source to destination.

All communications between any pair of Skype users—consisting of any combination of voice, video, text chat or file transfer—are carried over an encrypted Skype “session layer” that is established between the communicating users before messaging begins. At the point of call set-up, the two communicating parties simultaneously exchange signed identification credentials and agree upon a 256-bit encryption key that is used to encrypt the session layer between the parties. Each session is encrypted using the Advanced Encryption Standard (AES) in its AES-256 mode.

The key established for each Skype session is unique for that session and is neither retained by the user after session termination nor escrowed by Skype or any other party. If a Skype user has multiple concurrent open sessions—such as the operation of two or more simultaneous chat sessions—the keys used to encrypt each session will be unrelated to one another.

Because all communications between any pair of users is sent simultaneously over a single session, using a technique called multiplexing, the contents of voice calls, text chats and any other form of Skype communication is sent with an equal degree of security. By contrast, once a text message, file or audio stream is received by the intended receiver, Skype does not prevent the copying, archiving or redistribution of the received message. In other words, Skype protects the confidentiality of user communications while in transit, whether the connection is made directly between two communicating users or is relayed through a third party. Naturally, users themselves are responsible for protecting the security of their communications prior to sending and, similarly, following receipt, just as they would with e-mail attachments.

System requirements

In order to run Skype software on a supported platform, Skype recommends that users ensure that the computer on which the Skype software is to be installed meets the minimum system requirements described on the download page of Skype’s website at `http://www.skype.com/download/`.

For all platform editions, Skype requires an Internet connection with a minimum speed of 56 Kbps—Skype recommends the user of a broadband Internet connection for optimal quality.

2 Make your network Skype-friendly

"If you deny to dance, let's hold more chat."

–KING FERDINAND
LOVE'S LABOUR'S LOST
ACT V, SCENE II

Tuning at the network edge

In this section, we will look at how networks can be configured to be Skype-friendly, meaning not only that Skype will work on these networks but also that Skype will work well. While this section discusses firewalls, the treatment of software firewalls, also known as "personal firewalls", will be covered in the section on Skype installation. If you don't manage a network with a separate hardware firewall, you may wish to read this section for background, but may skip ahead to the section on Installation.

Like all peer-to-peer (P2P) applications, Skype relies on the Internet in order to function properly. While Skype provides a robust capability to communicate across many firewalls and network address translation (NAT) configurations, different network configurations may yield different call quality for users served by these networks. The ideal situation for Skype or most any P2P application would be to be directly connected to the Internet, but the reality is that most computers are separated from the Internet by some kind of firewall.

Skype will work in a very large number of firewalled networks, but some configurations afford better Skype quality than others. This is because as one's network strays further from an ideal configuration, the more likely that the workaround employed by Skype to connect to the Internet will affect factors such as network speed and latency which, in turn, can affect sound quality.

It should be pointed out that the Skype application will not provide full functionality unless it can find a way to reach the public Internet. When connectivity to the Internet is unavailable or terminated, the user client will change its state to "offline" and continue to search for a path to the Internet. If Internet connectivity is terminated while a call is in progress, Skype will attempt to continue the call until its conclusion, but the user will not be able to add parties to the call or make further calls. Once Internet connectivity is restored, the client will automatically resume its previous online status.

Configuring the local area network

Network administrators can positively impact the quality of Skype communications conducted by their network's users by tuning the network's handling of transmission control protocl (TCP) and user datagram protocol (UDP) packets for best Skype performance. By this we mean that network administrators can exercise a great deal of control over their users' networking experience by adjusting control parameters on networking appliances such as routers, firewalls and network address translation devices. In the broadest possible terms, Skype considers an ideal network configuration to be one that's set up according to the rules shown in Table 1-1, below.

1. Outgoing TCP connections should be allowed to remote ports 1024 and higher.

2. Outgoing TCP connections should be allowed to remote ports 80 and 443.

3. Outgoing UDP packets should be allowed to remote ports 1024 and higher. For UDP to be useful to Skype, the NAT must allow for replies to be returned to sent UDP datagrams. (The state of UDP "connections" must be kept for at least 30 seconds, and Skype recommends that these translations be maintained for as long as an hour, if possible.)

4. The NAT translation should provide consistent translation, meaning that outgoing address translation is usually the same for consecutive outgoing UDP packets.

Table 1-1 Ideal network configuration for Skype

Many peer-to-peer applications, including Skype, rely heavily on UDP packets to help maintain the best possible quality of connection among peers because UDP packets can be transmitted quickly and require very little overhead to manage. However, for UDP communications to work properly for Skype through NAT, the translation rules for UDP packets must be consistently handled, meaning that UDP packets set from one external network address and port number must be consistently translated to an internal network address and port number without varying either the network address or port number.

Although the use of UDP is optional—meaning Skype will work fine without the ability to transmit UDP messages—the call quality experienced by Skype users will be much better, on average, if the caller is able to send UDP packets to the called party and receive UDP answers in reply.

Tip: Checking your network for P2P friendliness

Many of our customers have told us that they use a freeware program called "NAT Check", written by Bryan Ford, to see if their network's UDP translation is compatible with P2P protocols including Skype. The NAT Check program is available for free download from the program's website at `http://midcom-p2p.sourceforge.net` and is available in a precompiled form for platforms running Microsoft Windows, Mac OS X and Linux. (NAT Check is not Skype software.)

```
UDP RESULTS:
UDP consistent translation:         YES (GOOD for peer-to-peer)
UDP loopback translation:           YES (GOOD for peer-to-peer)
UDP unsolicited messages filtered:  YES (GOOD for security)
```

Table 1-2 A Skype-friendly partial result from NAT Check

In the result of NAT Check shown above, we see that the network's UDP translation is applied consistently ("consistent translation"), that the input and output ports are identical except in the event of a conflict ("loopback translation") and that unsolicited UDP packets sent to the network are discarded ("unsolicited messages filtered").

Although not strictly necessary, it is preferable for the network's firewall or NAT gateway to support IP packet fragmentation and reassembly. In addition, the firewall must not block an attempt to send parallel UDP packets or TCP connection attempts to multiple ports at the destination address. Some firewalls misclassify such behavior as port scanning and therefore block the host altogether. Such behavior could not only impact the ability of Skype to run but would likely impact other legitimate network applications running on the same host computer.

Skype and proxies

Skype fully supports SOCKS5 and HTTPS/SSL proxles, including optional authentication. For SOCKS5, the proxy must allow, at a minimum, unrestricted TCP connections to at least port 80, or port 443, or high-numbered ports, meaning those numbered 1024 and higher. For HTTPS/SSL proxies, the proxy must allow unrestricted TCP connections to port 443.

On Microsoft Windows platforms, Skype uses the proxy settings in Microsoft Internet Explorer to determine what proxy settings, if any, to use. However, the Skype user can set the SOCKS5 or HTTPS/SSL proxy manually, including any needed username and password for proxy authentication.

3 Configure the Skype software

"Even when change is elective, it will disorient you."

–HARVEY MACKAY

Install Skype

Skype's goal is to allow users to use the Skype application from as wide a variety of networks as possible, without requiring the user to understand or configure complex options such as relay hosts or preferred network ports. In this sense, Skype is generally "hands-off."

The most up-to-date version of Skype is always available directly from Skype's own download server at `http://www.skype.net/download/`. While we recommend that you obtain Skype directly from our servers, third parties are permitted to host downloads of Skype's application, provided they follow the terms in Skype's End User License Agreement (EULA) concerning redistribution of Skype software.

Once it's installed, the Skype application checks every so often to see if there is a software update available. Skype software never updates itself but instead provides a visual indication to users that an upgrade is available. It's up to the user to decide whether to upgrade to a new Skype release. Users may decide not to check for upgrades by setting the corresponding option in the user client. In this case, users will be informed of the availability of an upgrade only if Skype releases a critical software change.

Verifying the authenticity of the installer package

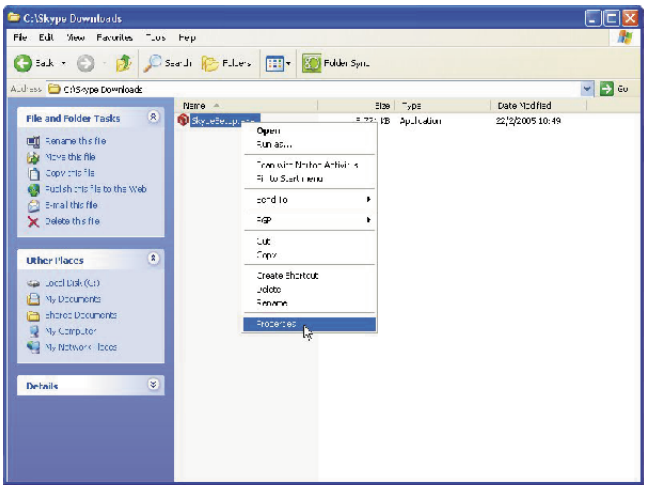
The Skype software is developed and packaged for installation solely by us at Skype. Although third parties are permitted, under terms specified in Skype's EULA, to redistribute our Software, the Skype software may not be repackaged or "wrapped" in any other software. To best protect your installation, you should download the Skype application only from the Skype website at `http://www.skype.com/download/` and verify the software installer's digital signature.

Our software installers for Microsoft Windows XP, Windows 2000 and Windows Pocket PC 2003, as well as the Skype application itself, are digitally signed. For optimal protection against the installation of malware or spyware, you should manually verify the Skype installer's digital signature prior to running it.

Copies of Skype built for the Mandrake distribution of Linux are packaged in RPM format and are signed using Skype's signing key, which is available for download from Skype's web site at `http://www.skype.com/products/skype/linux/`.

Steps to take for verifying the authenticity of the Skype installer for Windows

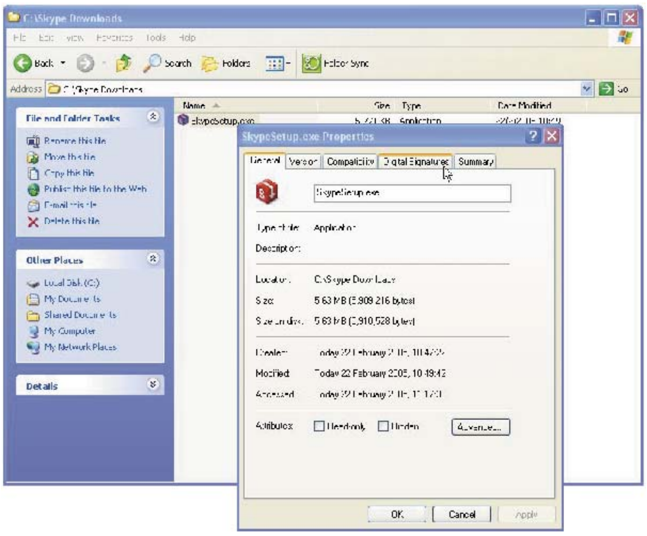
Step 1. Open Windows File Explorer and locate the Skype installer program



Name: SkypeSetup.exe — Type: Application — Date Modified: 22/2/2005 10:49

Step 2. Right-click on the Skype installer program and select Properties from the pop-up menu. The Properties dialogue box for the Skype installer should now be displayed.

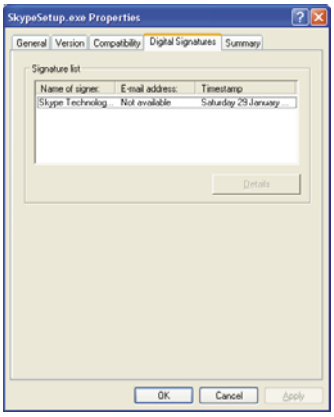
Step 3. At the top of the Properties box are several tabs. One of these tabs should be labeled “Digital Signatures.” Select the Digital Signatures tab.


SkypeSetup.exe Properties
General Version Compatibility Digital Signatures Summary
OK Cancel Apply

SkypeSetup.exe
Type of file: Application
Location: C:\Skype Downloads
Size: 5.63 MB (5,909,216 bytes)
Size on disk: 5.63 MB (5,910,528 bytes)
Modified: Today 22 February 2005, 10:49:43
Attributes: □ Read-only □ Hidden

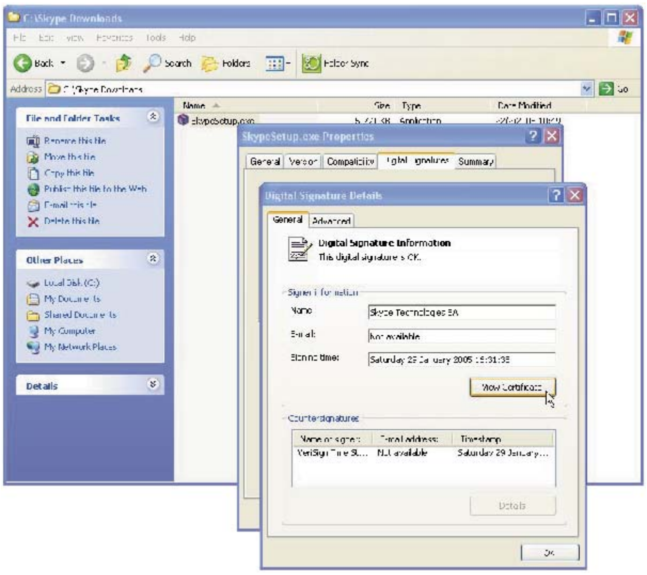
If there is no Digital Signatures tab, **DO NOT CONTINUE.** There is a problem with the installer’s digital signature. In this case, you should skip ahead directly to the section entitled “What if there’s a problem with the digital signature?”

Step 4. In the Properties box, you now should see a list of digital signatures applied to this installer package. There should be only one signer of the installer package, “Skype Technologies SA”.


SkypeSetup.exe Properties
General Version Compatibility Digital Signatures Summary
Details
OK Cancel Apply

Signature list

Name of signer	E-mail address	Timestamp
Skype Technolog...	Not available	Saturday 29 January...



Digital Signature Information
This digital signature is OK.

Signer information
Name: Skype Technologies SA
E-mail: Not available
Signing time: Saturday 29 January 2005 15:31:35

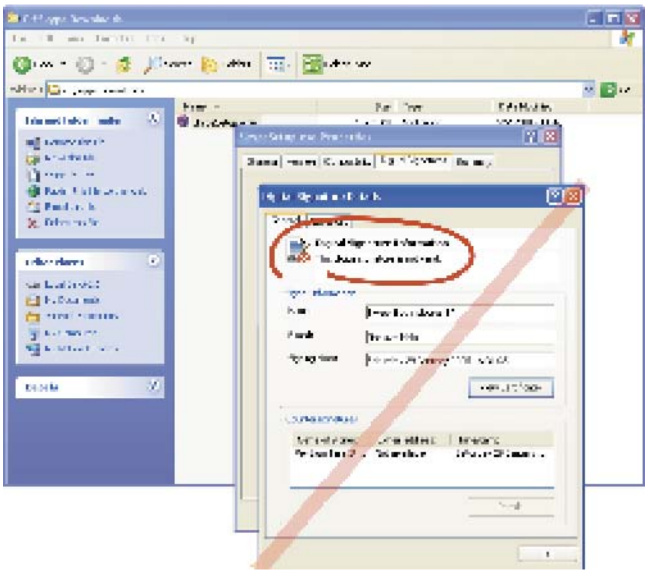
Countersignatures

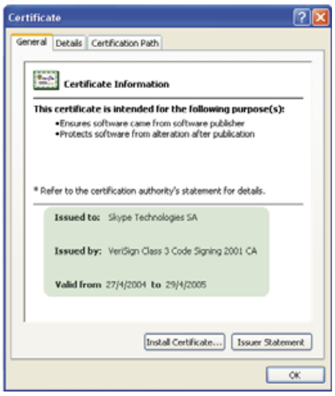
Name of signer	E-mail address	Timestamp
VeriSign Time St...	Not available	Saturday 29 January...

Step 5. Double-click on the line containing “Skype Technologies SA”, which will raise a window containing the details of Skype’s digital signature.

Step 6. Look at the pop-up window labeled "Digital Signature Details". It should say "This digital signature is OK".

If the pop-up instead says that "This digital signature is not valid", **DO NOT CONTINUE.** There is a problem with the installer's digital signature. In this case, you should skip ahead directly to the section entitled "What if there's a problem with the digital signature?"





Certificate Information

This certificate is intended for the following purpose(s):

- Ensures software came from software publisher
- Protects software from alteration after publication

* Refer to the certification authority's statement for details.

Issued to: Skype Technologies SA

Issued by: VeriSign Class 3 Code Signing 2001 CA

Valid from 27/4/2004 **to** 29/4/2005

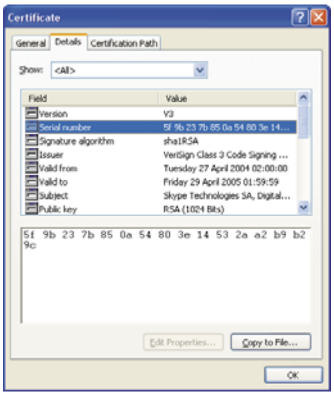
Step 7. Click on the button labeled "View Certificate" to display the details of the digital certificate used to sign the installer software. The pop-up window labeled "Certificate" should display the following details:

Issued to: Skype Technologies SA
Issued by: VeriSign Class 3 Code Signing 2001 CA

If either the Issued To or Issued By fields is varies from what is shown above, **DO NOT CONTINUE.** There is a problem with the installer's digital signature. In this case, you should skip ahead directly to the section entitled "What if there's a problem with the digital signature?"

Step 8. Click on the Details tab to display the serial number of the signing certificate. The serial number will change once a year, so the information shown below will be updated as new signing certificates are issued.

If the certificate serial number for this copy of the Skype installer does not match precisely the one shown in Table 3-1 below, **DO NOT CONTINUE.** There is a problem with the installer's digital signature. In this case, you should skip ahead directly to the section entitled "What if there's a problem with the digital signature?"



Field	Value
Version	V3
Serial number	5f 9b 23 7b 85 0a 54 80 3e 14...
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Code Signing ...
Valid from	Tuesday 27 April 2004 02:00:00
Valid to	Friday 29 April 2005 01:59:59
Subject	Skype Technologies SA, Digital...
Public key	RSA (1024 Bits)

```
5f 9b 23 7b 85 0a 54 80 3e 14 53 2a a2 b9 b2
9c
```

	a. For Skype released during this period:	*b. The certificate serial number should be:*
1.	27 April 2004-29 April 2005	`5f 9b 23 7b 85 0a 54 80 3e 14 53 2a a2 b9 b2 9c`

Table 3-1 Digital certificate serial numbers for Skype software

This signature verification test can be performed on an installed Skype executable program file once the Skype installer has been run, but it is most important that these signature checks be made prior to running the Skype software installer for an initial installation or for any upgrade.

If you had no problems with the digital signature verification, you should skip ahead to Installation Procedure, which is immediately after the following section.

What if there's a problem with the digital signature?

Invalid digital signatures can appear on downloaded files for a number of reasons. For instance, it could mean that the installer was corrupted inadvertently while being downloaded or that Skype was improperly bundled with someone else's software without Skype's permission. It could also mean that someone has tried to tamper with Skype's software in order to add malware or spyware, a practice that is strictly prohibited by Skype's license agreement.

If you notice any problem with a Skype digital signature, we stronly recommend that you follow these steps:

1. DO NOT use or run any copy of the Skype installer that failed verification checks.

2. Contact Skype security to advise us of the problem by sending e-mail to `security@skype.net`. Be sure to indicate the kind of problem you have experienced and the place where you obtained the copy of Skype that failed verification.

3. Download a fresh copy of the Skype installer from `http://www.skype.net/download/` and reverify the digital signatures by following the steps in the previous section.

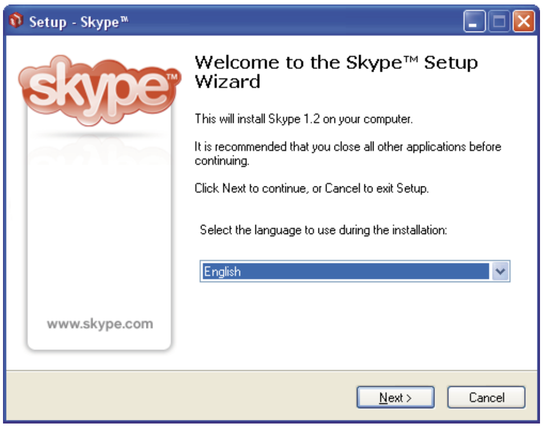
Installation procedure

On Microsoft Windows platforms, Skype is installed using a custom application installer. Although Skype's installer is not currently based upon Windows Installer, Skype is able to be installed by users without possessing any special authorizations because Skype relies on no special privileges to operate, other than the same Internet access available to any program.

To install Skype, simply download the Skype setup utility from the Skype download website and, after verifying its authenticity as described in the previous section, run the installer.

Step 1. Run the installer by double-clicking on the Skype setup program's icon or by typing the name into a command window.

The Skype installer is localized in several languages. Before continuing, select the language to be used during the installation. Select Next to continue.



Welcome to the Skype™ Setup Wizard

This will install Skype 1.2 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Select the language to use during the installation:

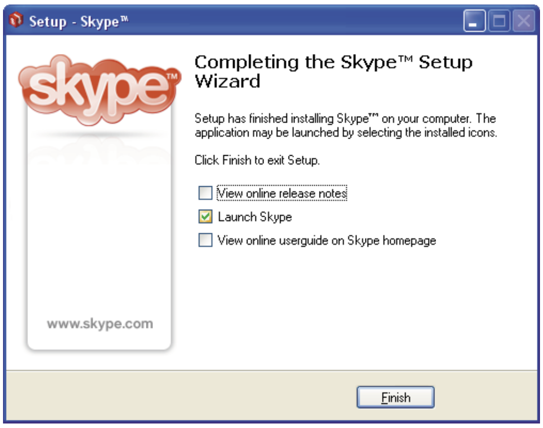
English

Step 2. The second installation screen displays a copy of Skype's End-User License Agrement (EULA). Read the EULA carefully.

If you agree to the EULA, select "I accept the agreement" and click on Next to continue. If you do not agree to the EULA agreement, select Cancel, which will terminate the installation process.

If you accepted the EULA terms, the installer will begin the process of installing Skype. The setup program will display a running display of the progress of the installation process. A description of the files and directories created by the installer is provided in the following section.

Step 3. The Skype installer verifies that Skype has been correctly installed by providing a dialogue box that says "Setup has finished installing Skype on your computer."



Completing the Skype™ Setup Wizard

Setup has finished installing Skype™ on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

- □ View online release notes
- ☑ Launch Skype
- □ View online userguide on Skype homepage

If the installation encountered any errors, the error message will be displayed in a pop-up dialogue box containing a message detailing the problem that was encountered during installation.

Files, directories and Windows registry keys created by Skype

When the Skype setup application installs Skype, it writes a copy of the Skype application as well as a small number of support files to the system's hard disk. In addition, some persistent information is maintained in the Windows registry on the Skype for Windows edition.

On the Microsoft Windows XP or Windows 2000 platform, the following files and directories are created (this is not an exhaustive list):

	a. When this process runs:	b. The following directory, file or registry key is created:
1.	Skype Installer (SkypeSetup.exe)	1. If the installing account has Administrator privileges, the Skype shared program is written to the `%programfiles%` directory, which is usually C:\Program Files\Skype\Phone\ 2. If the installing account has limited privileges, the Skype program is written in the `%homedrive%:\%homepath%` directory, which is usually C:\Documents and Settings\<username>\Application Data\Skype\ 3. A folder named My Skype Pictures is created in the `%allusersprofile%` directory, which is usually C:\Documents and Settings\All Users\Documents\Skype\My Skype Pictures\. This folder contains common icons used by Skype during the running of the application. 4. A temporary folder is created in the user's `%temp%` directory for the purpose of expanding the installation executables during the setup process. This directory and its contents are deleted after the setup process concludes. 5. Several default file locations are stored in a persistent way in the Windows registry under the following registry key: `HKLM\SOFTWARE\Skype` 6. Some other registry keys may be created by other Windows subsystems as a consequence of Skype registering its installation on the platform, for instance: - Registration of the callto:// URL handler - Obtaining Windows Firewall inbound connection approval
2.	Skype application	1. A Skype folder is created for the individual user which may be used to store user-specific information. This folder is usually C:\Documents and Settings\<username>\Documents\Skype\. 2. A folder named My Skype Pictures may be created in the user's Skype folder, which is usually C:\Documents and Settings\<username>\Documents\Skype\My Skype Pictures\. This folder contains any icons which may be created or used by an individual and which is not common to all users on the platform. 3. If not created during the installation process, a folder named Skype may be created in the user's Application Data directory. This directory stores ephemeral information pertaining to a user's Skype sessions. This folder is usually C:\Documents and Settings\<username>\Local Settings\Application Data\Skype\.

Table 3-2 Files and directories created during a Windows installation of Skype

Make sure that your copy of Skype is the most current one

The Skype application includes a provision to let users know when a new version of Skype is available. However, a user may elect to disregard these upgrade notices or may opt to turn off upgrade notifications by deselecting the default “Check for updates automatically” option in the Tools->Options...->Advanced panel.

Users may check whether their installed version of Skype is up-to-date in two ways:

1. A user may select Help->Check for Update from the main Skype window, which will launch the default web browser which indicates if the installed version of the application is up-to-date; or

2. To determine if the currently installed copy of Skype is up-to-date without running Skype, open the Windows Control Panel and double-click on Add or Remove Programs. Find the entry in the Add or Remove Programs panel for Skype and click on the entry labeled “Click here for support information”. Follow the web link on the line entitled “Product Updates,” which will launch the default browser and indicate if the installed version of the application is up-to-date.

Personal firewalls and Skype

As Internet security has increased, so has the use of software firewalls on end-user computers. The so-called “personal firewall” works very much like a traditional enterprise firewall — allowing certain communications to pass and denying the passage of other types of communication — with one big difference: Unlike enterprise firewalls, personal firewalls know the actual program that is the source of (or destination for) the traffic it is screening.

For this reason, setting up personal firewalls to work with Skype is usually straightforward because instead of having to devise complex tables of “allow” and “deny” rules for specific types of network traffic, most users or system administrators can admit or deny network connections based on the application itself.

The following sections describe how to configure different commonly used personal firewalls to work with Skype:

Windows Firewall for Microsoft Windows XP with Service Pack 2

> You can find more details on managing Windows Firewall from Microsoft TechNet: `http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/mangxpsp2/mngwfw.mspx`

The Windows Firewall is a firewall product bundled with every copy of Microsoft Windows XP with Service Pack 2, replacing an earlier firewall feature known as the Internet Connection Firewall. The Windows Firewall is a stateful host-based firewall that drops all unsolicited incoming network traffic unless it a message sent in response to a request sent by the protected computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic). With some minor exceptions that do not impact Skype, the Windows Firewall does not drop any outgoing traffic.

Skype depends on the Internet to run, so when Skype is installed and each time it runs, Skype ensures that it can communicate in the best way possible with the outside world by including itself in the Windows Firewall exceptions table. This allows Skype to listen on specific ports for incoming connections to Skype in order to complete calls.

However, sometimes this setting can't be made by the installer or by the Skype application. For instance, if you are using Group Policy to configure Windows Firewall, the settings in the Group Policy might not permit any local configuration. In this case, even though Skype won't be able to obtain authorization to listen for incoming connections, Skype will continue to function normally. However, in this case the user might find that the call quality provided by Skype in such a situation is lower than would be the case if the firewall were set to allow Skype to receive incoming network connections.

The reason for this is that Skype tries to make the most efficient connection between any pair of users. As outlined in the first section of this Guide, when one user attempts to call another, the caller tries to send the call directly to the called party. However, if the Windows Firewall blocks the incoming connection, a series of alternative connections and relaying arrangements are set up and tried in order to allow the call to go through.

By including Skype in the Windows Firewall application exception list, the Skype program can accept these call requests directly, provided that they're not blocked by some other network component, such as a restrictive enterprise firewall or certain types of NAT appliances.

If you are managing a Group Policy object for Windows clients on a managed network or in an enterprise environment, you can make your network policy more Skype-friendly by applying a simple exception in the Group Policy snap-in by adding an exception rule to your existing policy settings:

Group Policy Setting Profile:

```
Computer Configuration/Administrative Templates/Network/Network Connections/Windows Firewall/Standard Profile
```

Policy Setting:

```
Windows Firewall: Define program exceptions (Enabled)
```

Program exception definition to add:

```
%PROGRAMFILES%\skype\phone\skype.exe:*:enabled:Skype
```

Table 3-3 Windows Firewall Group Policy settings for Skype

If you are a home user manage your own computer running Microsoft Windows with Service Pack 2, you can provide Skype with the same authorization as the Group Policy setting above by manually adding Skype to the Windows Firewall exceptions list. Note that in most cases, Skype will accomplish these steps automatically upon installation.

To manually add Skype to the Windows Firewall exceptions list, follow these steps:

1. Click Start and select Control panel.

2. Open the Windows Security Center.

3. In the Security Center panel, under "Manage security settings", select Windows Firewall.

4. On the "General" tab of the Windows Firewall control panel, check to see if the firewall is on or off by looking for whether the "On" or the "Off" entry is ticked. It might have been switched off intentionally if a third-party firewall is installed on your computer; in this case you should close the Windows Firewall control panel and ensure your third-party firewall is configured to allow Skype communications.

   Skype recommends that the Windows Firewall be enabled on any Microsoft Windows device connected to a network unless another firewall has been installed to take its place.

5. If the firewall is on, ensure that the box marked "Don't allow exceptions" is NOT ticked (the box should NOT be filled with a check mark).

6. Select the "Exceptions" tab.

7. If Skype is available in the Programs and Services list, make sure that the checkbox next to Skype is ticked (the box should be checked).

8. If Skype is NOT in the Programs and Services list, click the Add Program... button and add Skype to the list. To complete this task, locate Skype from the list of installed programs and then click the button labeled "OK".

9. Close the Windows Firewall box by clicking the button labeled "OK" to confirm any changes. Close the Windows Security Center and the Windows Control Panel.

Norton Internet Security

Graphical step-by-step instructions for configuring Norton Internet Security for use with Skype are available on Skype's website at `http://web.skype.com/help_firewalls.html`

To configure Norton Internet Security to allow you to use Skype:

1. Open Norton Internet Security. Click on "Personal Firewall" and then on "Configure".

2. Click on the Programs tab near the top of the configuration popup panel.

3. Locate the Programs section and find Skype in the list of programs.

4. Highlight Skype and click on the menu selection under the heading "Internet Access". Set the access level to "Permit All".

5. Click "OK". You should be able to use Skype now.

Zone Alarm Pro

Graphical step-by-step instructions for configuring Norton Internet Security for use with Skype are available on Skype's website at `http://web.skype.com/help_firewalls.html`

To configure Zone Alarm Pro to allow you use Skype:

1. Open Zone Alarm Pro. Click on "Program Control".

2. Select the "Programs" tab, if it wasn't selected already, and find the line listing Skype.

3. Select the line containing Skype and then right-click under Server:Trusted to open the options menu. Set the option to "Allow".

4. On the same line, right click under "Send Mail" and set the option to "Block". There should be four green checkmarks displayed on the left and one red "X" displayed on the right.

5. Close the Zone Alarm configuration window. You should be able to use Skype now.

McAfee Firewall Pro

Graphical step-by-step instructions for configuring McAfee Firewall Pro for use with Skype are available on Skype's website at `http://web.skype.com/help_firewalls.html`

To configure McAfee Firewall Pro to allow you use Skype:

1. Open McAfee Firewall Pro. Click on the "Personal Firewall" tab.

2. Locate the button marked "View the Internet Applications List" and click on it.

3. A new window will appear, displaying a list of Internet applications. Find the line containing Skype and select it.

4. In the Change Permissions To... column, select the "Allow Full Access" option to allow Skype to contact the Internet.

5. Close the McAfee Firewall Pro windows. You should be able to use Skype now.

Mac OS X firewall

Skype will work out-of-the-box with Mac OS X firewall without additional configuraiton. However, call quality can be improved by optimizing OS X's firewall settings:

1. Open Skype preferences by launching Skype and selecting Skype->Preferences...

2. On the Preferences panel, select Advanced. Make a note of the Port number listed underneath the label "Connection: Port" at the bottom of the panel. This number is different for each installation of Skype.

3. Open System Preferences and select Sharing.

4. On the Sharing Panel, select Firewall.

5. To the right of the Allow list, select New...

6. On the pop-up menu that appears, click on the drop-down list and select “Other”.

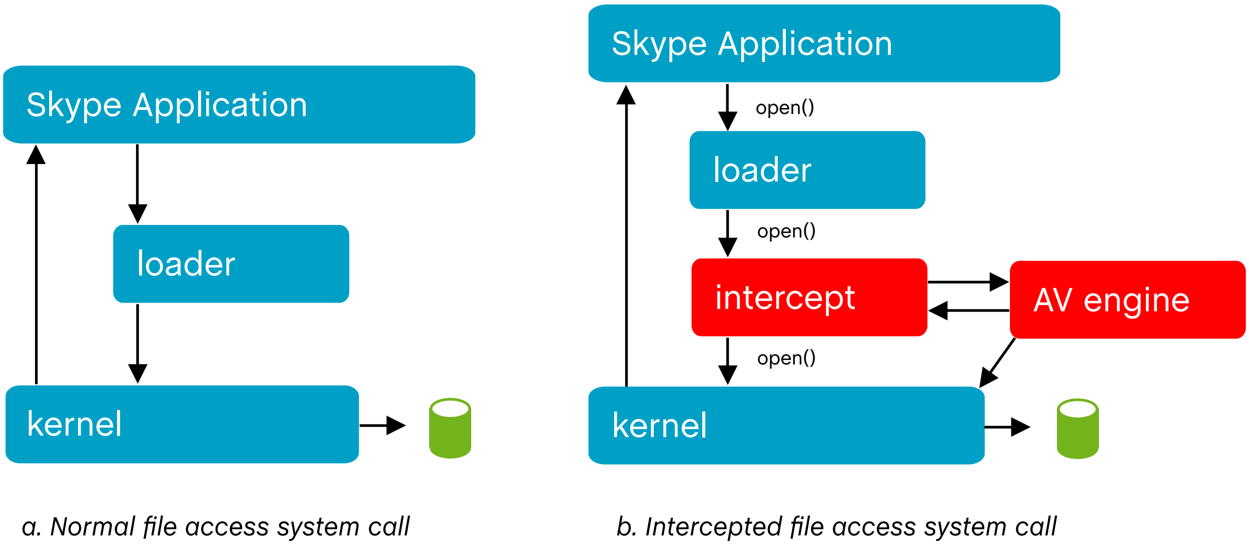
7. In the blank labeled “Port number, range or series”, enter the port number you recorded in Step 2. For “Description” enter Skype.

8. Close the Sharing window. You should be able to use Skype now.

Anti-virus scanners and Skype

Provided you have installed an anti-virus product and keep the virus definitions updated, **Skype introduces no more risk of allowing the spread of viruses** than through e-mail or other file transfer services.

Skype’s file transfer service is fully compatible with all major antivirus vendors’ “shield” AV scanning products. Although Skype does not integrate antivirus scanning functionality into its messaging product, it uses industry-standard techniques for creating files, reading from them and writing to them, thus allowing for standard scanning by antivirus products during either the sending or the receiving of files through the Skype application.



a. Normal file access system call

b. Intercepted file access system call

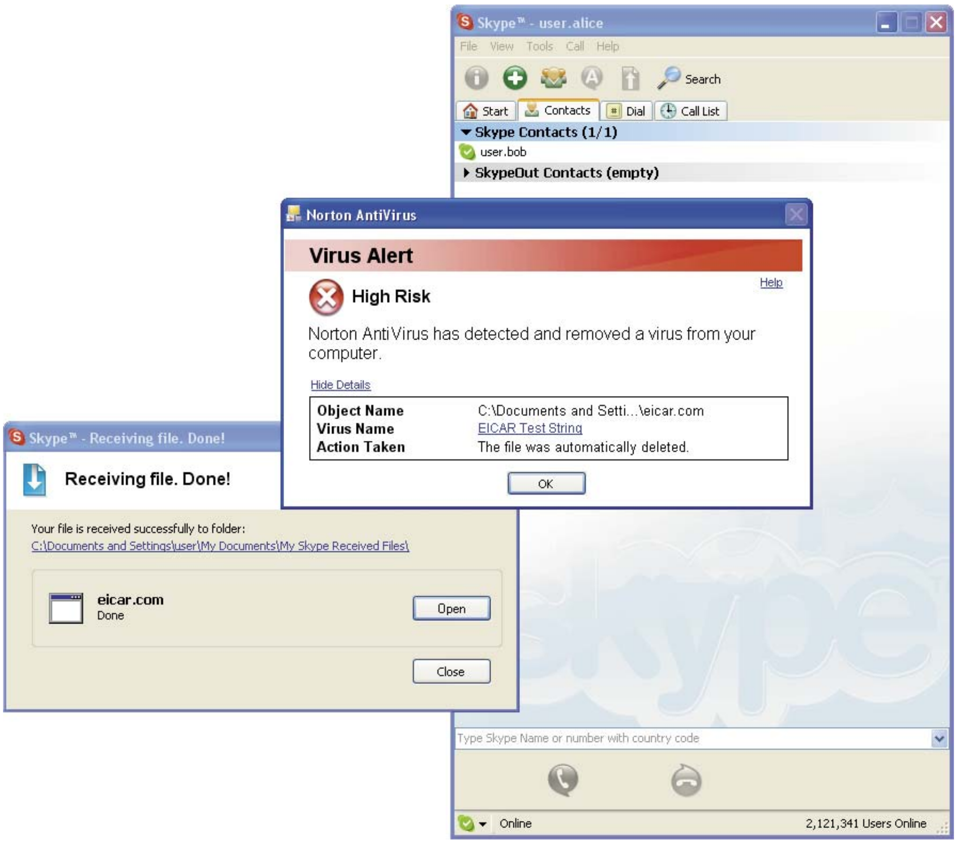
Figure 3-1 System call interception by antivirus scanner

When a program wishes to read from or write to a file on disk, the application wishing to access the file calls the `open()` primitive from the kernel to attempt the appropriate access, as is shown in the left panel of Figure 3-1. When Skype, for instance, reads a file the user wishes to transmit, or when Skype writes the file on the receiving end, Skype requests to create, open, read from or write to the file as appropriate.

Antivirus tools make use of the fact that all file access is done through a small number of kernel primitives by employing one of several techniques, depending on the type of operating system in use, to “shim”, wrap or intercept all calls to all file access kernel functions. Therefore, if a user attempts to use Skype to send or receive a file, the antivirus program will detect the attempt to read or write a file containing and deny Skype the permission to continue writing.

As is shown in the right panel of Figure 3-1, the antivirus program inserts itself in the file access chain, which gives it the opportunity to watch for file contents which match known virus signatures. To illustrate this, we sent an industry-standard virus scanner test file, called the EICAR test file, from an unprotected computer to a Skype user on a Microsoft Windows XP computer protected with a retail copy of Norton AntiVirus Professional.

Although Skype would have otherwise allowed the file transfer, the file was immediately caught and deleted by Norton AntiVirus, while the user was alerted by the Norton pop-up dialogue box shown in Figure 3-2, below.



Norton AntiVirus has detected and removed a virus from your computer.

Object Name	C:\Documents and Setti...\eicar.com
Virus Name	EICAR Test String
Action Taken	The file was automatically deleted.

Your file is received successfully to folder:
C:\Documents and Settings\user\My Documents\My Skype Received Files\

Figure 3-2 Norton AntiVirus stopping reception of the EICAR antivirus test file over Skype

4 Use Skype safely and securely

"The trouble with learning from experience is that you never graduate."

DOUG LARSON

Managing your Skype identity

Skype users are uniquely identified by a Skype username, which is normally chosen upon running Skype for the first time after the software is installed. Skype usernames may also be created at any time by selecting "Log In As Another User..." and then requesting to create a new account. A Skype user may hold one or more accounts, although currently only a single Skype user may be logged in at a time on any instance of Skype.

When we speak of a "Skype user" we typically mean a human user of the Skype software, while a "Skype username" refers to a username that, along with the correct password, allows login to the Skype software. Therefore a single Skype user could have one or more than one Skype username.

What's in a username?

The choice of your username is up to you. Provided the name hasn't been taken by someone else already, you're free to choose whatever username you wish. Skype usernames are public names, so you wouldn't want to include something you consider private within your Skype username.

You can describe yourself in your Skype profile in enough detail that other users can find you using the Skype program's search tool. It's natural that users would want to put as little information as possible in their Skype profile until they feel comfortable with the software and how the information will be used. Skype believes that the more information is available in the directory, the better, as we explain in a subsequent section on the Skype directory (see below).

What's in a password?

It's very important that you protect your account by selecting a good password for your Skype account. Don't use a password that's in use somewhere else. And be sure to use a password that includes both upper- and lower-case characters, symbols and digits.

Remember, your password is the key to your Skype account. **Never give your Skype account password to anyone.** No one from Skype will ever ask you for your password. (If anyone ever asks you to divulge your Skype password, you should decline to do so and then notify Skype about the attempt by e-mail to `abuse@skype.net`. Please include details of the contact or the URL of the web page.)

If you lose your password, you can request a replacement to be issued by e-mail to the mail account associated with your Skype account. Because your password is encrypted before it's ever sent to Skype, no one at Skype ever has access to your password. If you didn't specify an e-mail account to use with Skype or if you have lost access to your e-mail account, Skype will be unable to help you obtain access to your account. In this case, you'll need to create a new Skype account.

Skype strongly recommends that you print out a copy of your account details when you create your account and that you write your password down and store it in a safe place.

A word about passwords

All too often, computer users are "hacked" because they use easily-guessed passwords or ones that are written down and left out for others to find. The best protection is to use a strong password that you don't have to write down at all. A strong password is one that's at least eight characters long and includes a combination of letters, digits and punctuation; the password should be easy to remember but hard to guess.

Although completely random passwords are the most "secure", because they're the hardest to guess, they're not very useful because they are also very hard to remember. You'd likely write the password down and leave it where others might find it.

An easy way to create a memorable strong password is to develop a "passphrase", which is a sentence that you can remember, like "Our house is three doors away from my friend Jean-Luc". By using the first character of each word, you could develop the password "`ohitdafmfjl`". You can make this even stronger by mixing upper- and lower-case letters as well as digits and symbols. For instance, the same phrase could become "`Oh13d@fmfJ-L`".

The Skype directory

Skype maintains an online directory of all users who are logged in to Skype as well as those who have been logged in at some point in the last couple of weeks or so. In order to find another user, a Skype user can search against any or all of the fields listed in the online directory.

The Skype directory is global, which means that common names, like Pierre DuPont or Robert Smith, will provide a large list of possible matches. Therefore, it's important that you provide enough information to identify you uniquely so that persons who want to reach you are able to find you.

It's best if you include your e-mail address in your Skype profile, because doing so will let your friends and associates most easily find you. Although users can search the online directory using your e-mail, Skype won't give out e-mail addresses as a result of searching. This protects Skype users from spammers who would like to compile lists of valid e-mail addresses. As an anti-spam measure, Skype doesn't even store your e-mail address in the Skype directory. Instead, a mathematical representation of your address, called a hash, is stored. This means that only people knowing your full and exact e-mail address can search for you. Users not able to develop lists of employees in companies by doing "partial match" searches such as "`*@skype.net`" or "`bob@*`".

You can change your Skype profile at any time. Some people who travel a lot add notes next to their name indicating their current timezone. Others add comments in the description field that describe how or when to reach them. If you put a telephone number in one of the telephone number blanks, Skype users can click on those links to reach you via SkypeOut if you aren't on-line at the time.

Telephone numbers should be entered in international format, which starts with the plus symbol ("+") followed by the country code, city or area code, prefix and line number. For instance, the New York City directory service number would be written +1 212 555 1212.

Presence status indicators

Skype users can indicate their presence on the Skype network by selecting from among six status indicators. Status indicators are a way for users to tell their contacts whether they're available, busy or not available. In addition, a special status, called "Skype Me", signals that you're open for contact by people who are not one of your contacts.

✓	Online	A user whose status is Online is active at the computer and is available for contact with other Skype users. However, a user may set a privacy setting which restricts incoming voice calls or chats either to persons on the user's own contacts list or to persons who have been previously authorized by the user.
✓☺	Skype Me	The "Skype Me" status is just like Online, except that anyone may initiate contact with the user, regardless of the privacy settings the user may have previously established. This is an excellent way for Skype users in a local area to find one another, because the Skype search tool has a special search for people who are in Skype Me mode. The user's normal privacy preferences are reapplied as soon as the user changes into any other Skype presence status.
✓🕒	Away	The Away status indicates that a user has recently been active at the computer but may be away from the keyboard for a brief period. This status can be manually set by the user or will be automatically set by the Skype program after the computer has been idle for five minutes (this delay interval is configurable by the user).
✓☾	Not Available	Not Available status indicates that a user plans to be away from the keyboard for an extended period or that the computer has been idle for at least 20 minutes (this delay period is user configurable).
✓⛔	Do Not Disturb	When a user is in Do Not Disturb status, the user does not wish to be disturbed. In this case, chat sessions will no longer pop up on the user's screen but instead will be stored for later viewing. At any point, the user can go to the Start tab on the main Skype window and click on the corresponding chat session to see its contents.
✓	Invisible	The Invisible status is identical to the Online status, except that the user appears to authorized contacts to be offline. A user who is set to Invisible status will remain in this status until manually changed by the user.

Table 4-1 Skype presence status indicators

Understanding Skype authorizations

Skype was founded on the idea that people want to communicate with one another and that there is value in sharing presence information with one's colleagues, associates and friends. However, Skype also realizes that users have a right to keep information about themselves private if they wish. Authorizations are one of the mechanisms Skype uses to help users control access to themselves and their personal information.

Broadly speaking, a Skype authorization is an approval certificate that is issued by you to a specifically named third party to whom you give permission to see your presence status and, depending on the user's privacy preferences, to call or chat with you when others might be restricted from doing so.

A request for an authorization is generated each time one user adds another user to his contact list. Let's say that user Bob wishes to add user Alice to his contact list. In this case, Bob would select Tools->Add a Contact… and enter Alice as the Skype username to add to his contact list.

At this point, Bob will be presented with a window labeled "Request Authorization from Alice", which includes a blank that allows Bob to explain to Alice who he is and why he is requesting Alice to grant an authorization. (This is partiuclarly important if Alice was not expecting Bob's authorization request.)

When Bob completes the message text and clicks OK to dismiss the Request Authorization window, the request will be sent from Bob directly to Alice, as is shown in arrow 1 in Figure 4-1. Because Bob has not, at this point, been authorized by Alice, Bob is unaware of Alice's presence status. If Alice is not logged in to Skype when Bob makes his authorization request, it will be sent the next time when both Bob and Alice are logged on at the same time.

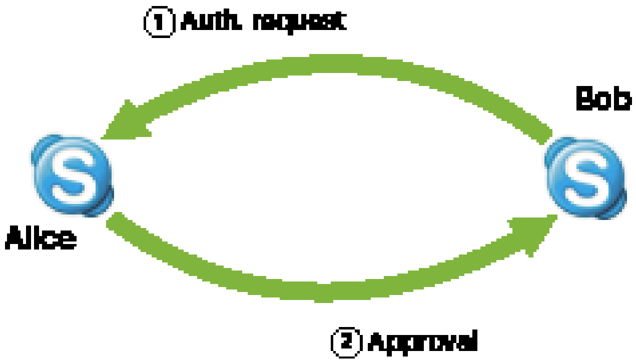


Figure 4-1 Successful authorization

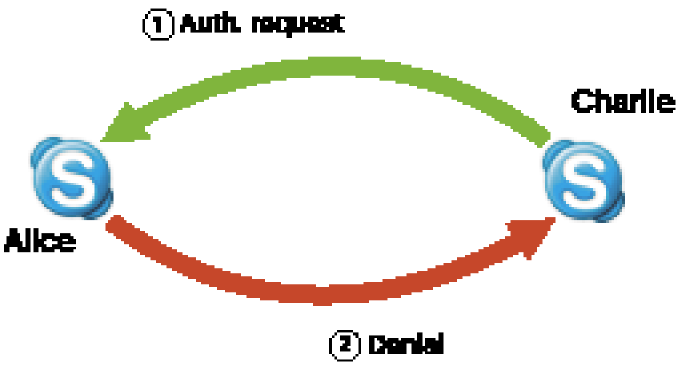


Figure 4-2 Rejected authorization request

Alice will receive Bob's authorization message in a special window that is clearly labeled as an incoming authorization request. Alice can either accept or reject the authorization request. If she accepts the authorization request, she would select the "allow this user to see when I'm online" button and click OK to accept the authorization. If, on the other hand, she rejects the authorization request, she would select the "do not allow this user to see when I'm online" button.

In either case, once Alice's decision on the authorization request has been entered, the answer is returned to Bob's Skype client. In the case of an approved authorization, as shown in Figure 4-1, the approval message is sent to Bob following the path of arrow 2, at which point Bob's Skype client would immediately begin to show Alice's presence.

In Figure 4-2 we show an unwanted authorization request sent by Skype user Charlie to user Alice. As usual, Charlie created the authorization request by adding Alice to his contact list. But, in this case, Alice decided not to disclose her presence information to Charlie and therefore rejected Charlie's authorization request. Although a denial message is returned to Charlie's Skype program to close out the request, Charlie is not informed of the rejection. To Charlie, Alice's status simply remains a question mark.

User blocking

Authorizations are forever: Once you send a Skype authorization to another user, there's no taking it back. This is becuase it's like a signed document you give to someone which, once signed, is signed forever.

However, there's a parallel service in Skype, called Skype blocking, that lets you change your mind and nullify an authorization. In addition, if you just don't want to receive contact from someone -- even someone whom you've never authorized -- you can block that user from ever contacting you through Skype by using Skype blocking.

Each user can create a list by selecting Tools->Manage Blocked Users... and entering the Skype usernames to block. Until it's removed from this list, a Skype user who is blocked will be unable to see the status of or communicate with the user who blocked. Users who have been blocked may be unblocked at any time by the user who put the block in place, simply by removing the blocked user's name from the blocking list.

Countering "spam" and "spit"

Spam is the scourge of today's internet: unsolicited commercial e-mail is an unwanted reality of e-mail communications today. Skype has taken steps to prevent the use of Skype as a tool to help spammers or those who spam over intenet telephony ("spit").

You can take an active role in countering spam and spit by authorizing only users whose identity you've confirmed. You can set your privacy settings to that you can be called only by persons who you know. You can include a note in your Skype Profile asking potential callers to send you an chat message before calling.

In addition, Skype has taken steps to ensure that your e-mail address is not available to those who would use the Skype on-line directory to find potential advertising targets. Even though you may include your e-mail address in your Skype profile, it won't be made available to others.

Just as is the case with e-mail and web communications, you should know to whom you are communicating before you divulge any private information. As we describe in this document, Skype uses advanced technology to ensure that no one can counterfeit a user identity or masquerade as someone else. But it's up to the user to ensure that the Skype user account is indeed being used by the intended person on the other end of the call, not someone who might be sharing the same computer.

Abusive situations should be referred to Skype Abuse by e-mail at `abuse@skype.net`.

Countering phishing

As is the case in other e-commerce sectors of the Internet, Skype users might receive false e-mails or encounter third-party web pages designed to look like e-mails or web pages created by Skype and intended to con users into giving up their username and password. This kind of attempt to collect user's credentials has been given the name "phishing", and it is rapidly becoming the #1 threat to individual users on the Internet.

Skype will never, under any circumstances, ask a user to divulge his or her password. You should use your Skype user password only for logging into the Skype program itself or when managing your Skype account on the web at `https://secure.skype.com/store/member/login.html`.

If you believe you have been the victim of phishing, you should change your password immediately and refer the situation to Skype Abuse by e-mail at `abuse@skype.net`. Please describe the problem in detail and include the phishing e-mail or the URL of the phisher's web page.

Securing your computer

Skype wants its customers to have a safe and enjoyable experience using Skype to enable their communications. However, Skype would like to underscore the importance of keeping your computer safe and secure while doing so.

Skype has published its recommendations for general computer security on its main web site at `http://www.skype.com/help/guides/staysecure.html`. In addition, we would like to underscore some main points from this guide:

1. Before you deploy Skype in an organization or redistribute it to others, be sure it is an authentic copy. Check the digital signature of the installer and be sure to follow the limitations in Skype's Terms of Service before redistributing Skype software.

2. Keep your computer up-to-date with relevant patches. Most of the computer security problems on the Internet today can be traced back to improperly patched computers. Don't fall into this category.

3. Use anti-virus protection, even on non-Microsoft computers such as the Apple Macintosh, and keep the virus signatures constantly updated.

4. When you use Skype, know who you're authorizing and don't hesitate to block users who are making unwanted contact with you. Keep your user profile up-to-date, but also know that everything in your profile (except your e-mail address) is viewable to others whose search matches your information.

5. Always authenticate the other party before beginning to discuss any confidential business or personal information. Remember that although Skype takes care to protect your communications from unwanted disclosure, it is possible that your computer or that of the person with whom you are communicating has been "hacked" or compromised by person with ill intent.

6. Select good passwords for Skype and change them regularly. Importantly, you should never check “remember my password” when using Skype on a shared computer (such as a computer at an Internet café or on someone else’s computer).