



IT Administrators Guide

Skype™ for Windows® version 4.2

Version 2.0

Copyright © Skype Limited 2010



Overview

Skype lets your business work the way you want to, whatever the message, wherever people are. This guide shows you how to implement and manage Skype's business tools so that your business can save time, save money and stay ahead.

Every business can start saving by downloading Skype. There are numerous benefits to your business:

- **Calling:** use free Skype-to-Skype calls, anywhere in the world.
- **Video:** have face-to-face meetings without leaving your desk.
- **Conferencing:** conduct multi-person meetings without any difficult set-up.
- **Screen sharing:** easily show others all or part of your screen.
- **Instant Messaging (IM):** chat with colleagues and business contacts.
- **File transfer:** send and receive large files easily.

With Skype Manager™, you can take full benefit of Skype by centrally managing your entire workforce's Skype usage. You can:

- **Create accounts:** easily set up business accounts for every employee.
- **Allocate Skype Credit:** centrally manage balances and automatic top-up.
- **Assign features:** allocate features, including Online Numbers, Call forwarding, Subscriptions and Voicemail, to individual business accounts.
- **Monitor usage:** view real-time reporting about Skype usage and costs.

If your business uses a SIP-enabled PBX system, Skype for SIP is also available via Skype Manager. Skype for SIP lets Skype users call your business directly from Skype or via a Skype button at no cost to them and Skype's global calling rates offer potential cost savings when calling landlines and mobile phones.

The aim of this guide

This guide will help you understand:

- How you can use Skype within your business
- Skype's architecture model
- How we address security and privacy issues

It also provides instructions on installing and configuring Skype for your business. We've created best practice guidance based on our experience in deploying our software across a wide range of organizations.

This guide replaces previous versions of the Network Administrator's Guide, which should no longer be used.

Who should read this guide?

This guide is for system and network administrators responsible for determining networking guidelines and for software on the Microsoft® Windows® platform. It assumes you're familiar with:

- Enterprise deployment issues
- Editing the Windows registry
- Windows Group Policy administration
- Basic XML syntax
- Other topics related to computer networking, network security and operating system environments

Important legal information

Before using Skype or the Skype Application Programming Interface (API), please ensure you understand and agree with all the appropriate Skype legal terms, depending on the Skype products you want to use:

- You must accept our End User License Agreements:
End User License Agreement: skype.com/legal/eula
Business End User License Agreement: skype.com/legal/business/eula
- If you use any paid-for internet communication products provided by Skype Communications S.a.r.l, you must accept our Terms of Service:
Terms of Service: skype.com/intl/en/legal/terms/voip
Terms of Service - Business: skype.com/legal/business/terms
- Skype Etiquette gives guidelines for dealing with the other members of our community:
skype.com/intl/en/legal/terms/etiquette
- To use the Skype API, you must accept our API Terms:
skype.com/intl/en/legal/terms/api

Copyright

The content contained in this document is the property of Skype Limited (“Skype”) and is protected by international copyright laws. Skype makes no representation or warranty as to the accuracy, completeness, condition, suitability, or performance of the document or related documents or their content, and shall have no liability whatsoever to any party resulting from the use of any of such documents.

By using this document and any related documents, the recipient acknowledges Skype’s intellectual property rights therein and agrees to the terms above, and shall be liable to Skype for any breach thereof.

Trade Marks

Skype, the Skype logo, Skyper Manager, SILK are all trade marks of Skype Limited. Microsoft and Windows are registered trade marks of Microsoft Corporation in the United States and/or other countries. Linux is a registered trade mark of Linus Torvalds in the United States and other countries. Apple and Mac OS X are trade marks of Apple, Inc., registered in the United States and other countries. Asterisk is a registered trade mark of Digium, Inc. All other names or brands may be trade marks or registered trade marks belonging to their respective owners.

Disclaimer

This document describes products offered by Skype Software Sarl, Skype Communications Sarl or their affiliates. Skype products may be modified or terminated at any time according to the current version of the Skype Business End User License Agreement and Business Terms of Service available on 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.

Access to a broadband internet connection is required. Skype is not a replacement for traditional telephone services and cannot be used for emergency calling. Skype for SIP is meant to complement existing traditional telephone services used with a corporate SIP-enabled PBX, it is not a stand-alone solution. Skype for SIP users need to ensure all calls to emergency services are terminated through traditional fixed line telephone services, connected to the local exchange, or through other emergency calling capable telephone services.

Table of Contents

1.0 Introduction to Skype : Page 6	3.4.5 Adware and spyware : Page 23
1.1 How Skype can help your business : Page 6	3.4.6 Security and Skype for SIP : Page 24
1.1.1 Skype : Page 6	3.4.7 Security summary : Page 24
1.1.2 Skype Manager : Page 7	4.0 Appendix 1: Configurable policies : Page 26
1.1.3 Skype for SIP : Page 8	5.0 Appendix 2: File locations : Page 29
2.0 Architecture overview : Page 9	6.0 Appendix 3: Additional information : Page 30
2.1 The P2P architecture : Page 9	
2.1.1 Nodes : Page 9	
2.1.2 Operation : Page 10	
2.2 Network configuration considerations : Page 11	
2.2.1 Firewall and NAT traversal : Page 11	
2.2.2 NAT configuration : Page 12	
2.2.3 HTTPS/SOCKS5 proxies : Page 13	
2.2.4 Relays : Page 13	
2.2.5 Network impact : Page 14	
2.3 Software distribution, upgrades and version control : Page 15	
2.4 Skype client configuration and policies : Page 15	
2.4.1 Windows registry : Page 16	
2.4.2 Group policies : Page 16	
2.4.3 XML configuration files : Page 17	
2.4.4 Client-side settings : Page 17	
2.5 Managing accounts and cost : Page 17	
2.6 Compliance : Page 18	
3.0 Security and privacy : Page 19	
3.1 Transport-level security : Page 19	
3.2 Security limitations : Page 19	
3.3 Privacy : Page 20	
3.3.1 Sharing contact details : Page 20	
3.3.2 Controlling communication : Page 20	
3.3.3 Location of personal information : Page 21	
3.4 Security best practice : Page 21	
3.4.1 Password security : Page 22	
3.4.2 Viruses and Trojans : Page 22	
3.4.3 Falsifying user identity : Page 23	
3.4.4 Spam and SPIT : Page 23	

1.0 Introduction to Skype

Skype brings business people together, helping your business overcome the barriers of cost, distance and technology and allowing you to do more anywhere in the world.

You can set up and start using Skype in no time. Reach colleagues and customers for less, improve meetings with face-to-face video calls and keep in touch with Instant Messenger (IM). You'll discover more flexible ways of working together with Skype.

1.1 How Skype can help your business

Skype provides real-time solutions for your business:

- **Communicate with your employees**

Free Skype-to-Skype calls or IM mean you can get an immediate response when you need it.

- **Communicate with your customers**

Use Skype buttons placed on your website and emails so that customers can contact you for free via Skype or buy Online Numbers so that your customers can reach you from landlines and mobiles.

- **Communicate with PSTN users**

If you have a SIP-enabled PBX, use Skype for SIP to take advantage of Skype's competitive global calling rates to landline and mobile phones. You can also choose to receive customer calls by purchasing Online Numbers.

- **Communicate on the move**

Add Skype Credit to call phones worldwide, have face-to-face meetings using video calls and conduct multi-person meetings easily, ensuring that your employees are involved, wherever they are in the world.

- **Communicate effectively**

Use Skype Manager to get the most out of Skype in your business. Manage Skype business accounts, purchase and allocate Skype Credit, assign features, and view real-time reports on expenditure. This ensures you have control over your business communications over Skype.

1.1.1 Skype

Skype has great functionality that can be used to help drive your business communications.

With Skype, you can:

- **See the selected online status of others and call them for free**

You can view the selected online status of colleagues on Skype and contact them immediately via free Skype-to-Skype calls or IM.

- **Have face-to-face meetings**

You can have face-to-face meetings at your desk with colleagues anywhere in the world using Skype-to-Skype video calls.

- **Contact groups of people at the same time**

You can use multi-person video conferencing that's easy to set up, or create group IMs to use as discussion spaces or to share important information instantly over Skype.

- **Share knowledge**

You can share your screen with colleagues to conduct presentations remotely or to just let them see what you're seeing.

- **Transfer files**

You can send and receive large files via Skype, ensuring that business information gets to your colleagues when it is needed.

1.1.2 Skype Manager

Skype Manager is a multi-functional, web-based tool that lets you control and manage Skype in your company. With Skype Manager you can:

- **Create Skype business accounts**

These accounts are owned and managed by your company rather than the individual employee which means that you can control how these accounts are used. You can also logically group accounts into business functions or departments, such as Sales or Marketing.

- **Buy and allocate Skype Credit**

This lets you centrally manage the use of Skype Credit within your business. Skype Credit can be bought and then allocated to each employee or SIP Profile, as required.

- **Assign features**

You can use the Skype Credit within Skype Manager to purchase and assign features such as calling subscriptions and Online Numbers to your employees.

- **View reports**

Skype Manager allows you to keep all your Skype calling costs under control. You can view reports on expenditure and usage at the company, department or employee level and print out company invoices.

You can find Skype Manager at skype.com/business. For more information on how to use Skype Manager, please see the [Skype Manager User Guide](#).

1.1.3 Skype for SIP

Skype for SIP is available via Skype Manager. If you have a SIP-enabled PBX, your business can take advantage of Skype's competitive global calling rates to landline and mobile phones. Also, if you have set up inbound calling, you can receive calls made from Skype users and configure your SIP-enabled PBX to direct those calls to your desk phones. With Skype for SIP you can:

- **Set up SIP Profiles**

You can set up SIP Profiles specific to the needs of your business by creating separate Profiles for different departments and teams and buying channel subscriptions according to business need.

- **Allocate Skype Credit**

You can manage your outbound call expenditure by allocating Skype Credit to your SIP Profiles and setting up Auto-recharge to ensure that your employees have enough Skype Credit to make calls.

- **Add Online Numbers and business accounts**

You can add Online Numbers and business accounts created in Skype Manager to a SIP Profile so that calls to them are received by the Profile's associated PBX. You can then implement Skype buttons on websites and emails so customers with Skype can call you for free.

2.0 Architecture overview

Skype's innovative collaboration and communications tools are quick to set up. The platform is primarily formed from Peer-to-Peer (P2P) nodes.

Skype is largely self-managing. You won't have lots of work managing the bandwidth configuration or Quality of Service settings. This means that as an administrator, you'll be free to get on with everything else you need to do.

Plus we don't like to overburden you with new administration tools. We use what's already installed on your network. With Skype's Group Policy Editor (supplied with Windows XP and above) you can manage Skype software configuration and deployment in your Active Directory environment.

You'll need just one new tool for Skype account administration – our web-based Skype Manager.

2.1 The P2P architecture

You'll need a basic understanding of P2P architecture to optimize your network to use Skype. It's very different to other communications solutions, being a highly distributed architecture, mostly relying on P2P communications. A small number of servers manage functions such as authentication through a login server, but not core functions, such as presence or location.

You'll see the benefits of distribution (as opposed to centralization) in many areas such as reduced costs, ease of deployment and network resiliency. Deployment is particularly simple as Skype-enabled computers find one another through P2P architecture, adapting to their environments.

2.1.1 Nodes

Skype consists of three types of peer nodes: ordinary nodes, supernodes and relay nodes. All three are included in the installation package.

Ordinary nodes run the Skype client. They're the most common, and are what users normally see when they install and use Skype.

Supernodes are peer nodes that also perform functions such as assisting with searching for the location of other nodes. These supernodes are not dedicated and come and go. They are not servers; supernodes are regular user computers that run the Skype client, but also temporarily perform other functions.

Nodes can only become supernodes if they:

- Have a public IP address
- Meet the memory, bandwidth, and uptime characteristics specified for your setup

- Are allowed by your specific Group Policy Object (GPO)

Only a very small percentage of Skype users in your network (if any) become supernodes, mainly because the majority of users have no public IP address. You can also deliberately prevent your users from becoming supernodes by using your Skype GPO Editor. For more information, please see [2.4 Skype client configuration and policies](#).

Relay nodes are nodes outside your network. They relay media and signalling information between nodes that otherwise can't reach each other, normally because of firewall permissions or problems traversing NAT. Relay nodes aren't party to the communication content and can't view or decipher it.

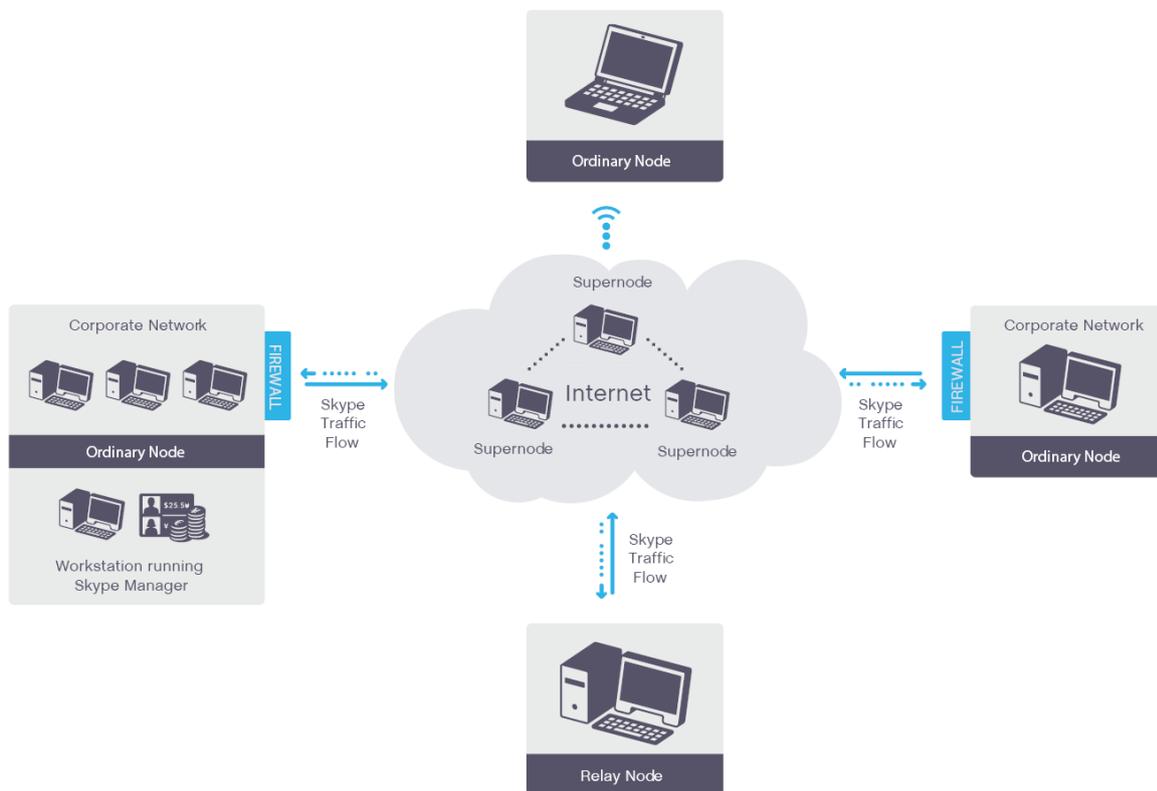


Figure 1: Skype uses three kinds of peer nodes – ordinary nodes, supernodes, and relay nodes. Our web-based Skype Manager is used for account management.

2.1.2 Operation

To see how Skype works and how it can be optimized for your network, we will look at how call establishment (common to voice, IM and video sessions) works. Under normal circumstances, a Skype client is an ordinary node in the P2P network. When Skype starts up, the node binds listening sockets for random high (higher than 1024) TCP and UDP ports. This is on port 443 for TCP/UDP and port 80 for TCP. It also uses UDP 443 to test network connectivity.

The Skype client needs TCP connectivity for signalling information. It strongly prefers UDP connectivity for stream (voice/video/file transfer) communications. If UDP is unavailable,

it can use TCP for the media stream (with the additional overhead due to TCP being stateful).

Before a user places their call, the client communicates with the peer network to test connectivity. It checks whether the outgoing UDP port is available and the type of address translation used by your network. Status checking and updating is also carried out through P2P architecture to identify a contact's Status.

Users can make calls to another Skype user or by entering a mobile or landline number into the Skype dialer. The Skype client then selects, from multiple standby connection paths, the one with the lowest latency and optimal bandwidth.

Calling a Skype user can generate a search through various supernodes, some of which reply, giving the recipient's possible network addresses, along with their associated supernodes. If found, the caller can then ask the recipient to let them connect. Alternatively, you can determine your users' access by selecting authorized Skype IDs.

Nodes communicate various networking parameters and information. They establish a session (for a chat, call, file transfer, avatar update or authorization request), either directly or through a P2P relay. Users can then activate a tool, like IM, voice, or video.

2.2 Network configuration considerations

The greatest challenge in deployment is in traversing the border between a corporate network and the public internet. Firewalls, NATs, and proxy servers can all complicate how network software is deployed. Skype should work natively with these devices. In particular, using a SOCKS5 or HTTPS proxy for Skype can improve performance (for more information, please see [2.2.3 HTTPS/SOCKS5 proxies](#)).

2.2.1 Firewall and NAT traversal

Enabling communications with a remote user or a user behind a NAT or firewall is one of the most difficult challenges you'll face. Since NATs change the outgoing IP address, there's no simple way for Skype clients to find one another. Additionally, firewalls are configured to reject new incoming sessions.

Skype offers three techniques for connecting to ordinary nodes separated by a firewall or NAT:

- Native firewall NAT traversal
- A SOCKS5/HTTP proxy server
- TCP/UDP relays

Native NAT traversal is the best solution, as it causes the least delay. Next best is a proxy server. SOCKS5 proxies use UDP, so introduce less delay than HTTP proxies. Finally, relays almost always work, but cause the most delay, particularly TCP relays.

2.2.2 NAT configuration

Skype automatically traverses most firewalls and NATs using UDP hole punching, a common technique favoured by Internet Engineering Task Force (IETF) standards, such as RFC 5389 (Session Traversal Utilities for NAT (STUN)).

With hole punching, Skype clients that can't communicate directly can communicate their networking parameters (remote node IP address and source port) through other hosts (relays). They then attempt to initiate direct UDP connections.

However, there are many different kinds of NATs and not all have the best characteristics for using Skype. Organizations should use NATs that meet the requirements of RFC 4787 (NAT Behavioral Requirement). Specifically, your NAT should:

- Be able to handle approximately 100 network mappings per user (depending on use and user profile). Scalability problems are most common with home routers, but can occur on corporate networks.
- Allocate ports consistently for all destinations (known as endpoint-independent mapping). The NAT should reuse port mappings for all packets sent from the same internal IP address and port to a particular external IP address and port. Avoid NATs with address-dependent mapping or address- and port-dependent mapping, as they will need a UDP relay. There are no security benefits to choosing one approach over another.
- Assign the same external IP address for all sessions associated with the same internal IP address. This is paired as opposed to arbitrary pooling. Paired pooling ensures the Skype client's media and signalling sessions all share the same external IP address. Otherwise, the session may appear to come from different clients, preventing nodes from establishing a session.
- Provide hairpinning. This allows two devices behind the same NAT to communicate using their external IP addresses and ports.

Either the NAT or your firewall should:

- Offer port preservation. Not needed by Skype, this is where NATs attempt to preserve the internal port number when mapping to an external IP address and port. If implemented, the NAT must assign alternative ports in conjunction with endpoint-independent mapping algorithm in the event of a port collision.
- Have a UDP mapping timer with a timeout of 60 seconds or more (the RFC requires 120 seconds). This avoids having too many timer refresh packets.
- Handle approximately 100 network mappings per user (depending on use and user profile). A particular problem in some routers, firewalls, or gateways intended for home use.
- Establish rapid, concurrent connections. Skype clients will establish multiple connections per session (some firewalls might interpret this as originating from malware and block the host as a result).

Some NATs and firewalls, particularly for home use, may not have capacity for the number of connections required by Skype. You should ensure that your NATs and firewalls do.

Note:

Don't worry if Skype establishes a large number of connections.

2.2.3 HTTPS/SOCKS5 proxies

Many large organizations have firewalls that don't meet these NAT requirements or employ other restrictive security policies, such as closing off high TCP or UDP ports.

If this is the case, you can configure Skype to work through a SOCKS5 or HTTPS proxy. These proxies relay traffic from applications inside the network (like Skype) to the internet and vice versa from the internet into the local network, based on configured policies (certain traffic can be passed or blocked). SOCKS5 proxies use a handshake mechanism that works across TCP or UDP socket connections. HTTPS proxies use the proxy connect method to connect to a remote client through TCP port 443.

A few important notes when deploying Skype across a proxy:

- We recommend SOCKS5 proxies rather than HTTPS as they support UDP, which allows better media quality than TCP. If you can't use a SOCKS5 proxy, clients can send TCP traffic across an HTTPS proxy while still attempting to connect to the other node directly.
- Proxies can be configured as the primary or backup means of reaching external networks. You can manually configure your clients to make the proxy a backup or make it primary by altering your GPO and Admin templates. For more information, please see [2.4.2 Group policies](#).
- Don't implement NAT between clients and your SOCKS5 proxy. We also don't recommend applying NAT between SOCKS5 and the internet.

2.2.4 Relays

If a Skype client can't communicate directly with another client, it will find the appropriate relays for the connection and call traffic. The nodes will then try connecting directly to the relays. They distribute media and signalling information between multiple relays for fault tolerance purposes. The relay nodes forward traffic between the ordinary nodes. Skype communication (IM, voice, video, file transfer) maintains its encryption end-to-end between the two nodes, even with relay nodes inserted.

As with supernodes, most business users are rarely relays, as relays must be reachable directly from the internet. Skype software minimizes disruption to the relay node's performance by limiting the amount of bandwidth transferred per relay session.

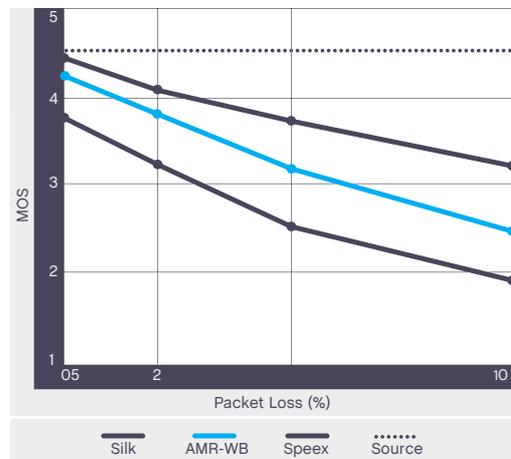
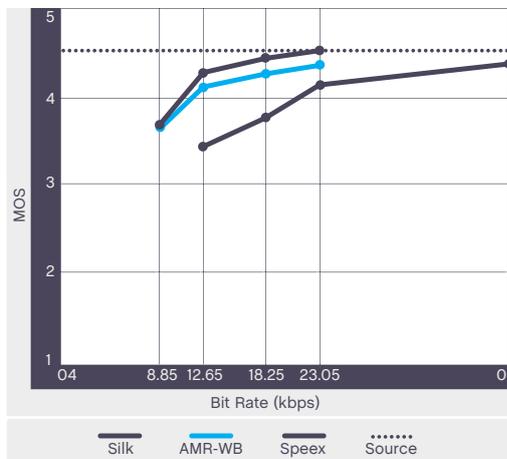
2.2.5 Network impact

Skype is uniquely designed to function over corporate networks with little impact on their performance. Providing specific details of the performance you can expect is difficult, given the range of Skype tools that could be in use. It also depends on the size of your Contacts list, how frequently the list is updated, and other factors. However, here are some very broad figures to help you design your corporate network.

Skype high definition audio is based on SILK™, our own high performance wideband codec. The codec can work on various sampling rates, from 8 to 24 kHz, yielding bit rates of 6 to 40 Kbits/s:

	Sampling Rate (kHz)	Bit Rate (kbps)	CPU (MHz on x86 core)
Narrowband for PSTN gateways and low-end devices	8	6 – 20	12 – 30
Mediumband for devices with limited wideband capacity	12	7 – 25	16 – 40
Super-wideband, a new standard in speech quality	24	12 – 40	30 – 80

SILK provides superior performance over other codecs, as these tests show:



Office Noise, 15 dB SNR	Source	SILK	AMR-WB	Speex
MOS	3.30	3.22	3.14	2.74

The MOS (Mean Opinion Score) listening test was performed by DynaStat, an independent third-party laboratory. Confidence intervals (95%) are +/- 0.1 MOS. All bitrates are measured and averaged over frames containing active speech. SILK and Speex were run in the highest complexity mode and with variable bitrate. Packet loss and office noise tests were done with all codecs running at 18.25 kbps.

Video quality can vary significantly with traffic conditions. You should plan on at least 128 Kbits/s for each session, though we recommend 384 Kbits/s and above. For an HD (720p) video call on Skype, at least 1 Mbps symmetrical bandwidth is required. Status controls

vary significantly, depending on the number of contacts on each list and how often they change.

Calculating specific background traffic requirements for a Skype session is complicated by many factors. This includes the size of a user's contact list, how often they change their Status, maintenance traffic, and other Skype operations occurring at the time, for example, searches.

To be conservative, you should plan on 200 bytes per second, but in practice, those numbers may vary significantly. In two tests, one of a user with 50 contacts and one of a user with over 600 contacts, average bandwidth over one hour was 200 bytes/s. As this is an average, a client may generate no traffic for 15 minutes and then burst to 500 bytes/s for a minute. In another instance, however, a user with nine contacts generated about 10 bytes/s.

2.3 Software distribution, upgrades and version control

Our software installer lets you distribute Skype across your organization with conventional IT tools, such as Microsoft SMS. We also provide a PC version of Skype for Business that comes with a Windows Installer Package (MSI). By using the Windows Installer Package Installation, you can manage version control of Skype and ensure that everyone in your company is using the same version. You can download this at [skype.com/download/skype/windows/business](https://www.skype.com/download/skype/windows/business).

Users will need administrative rights to upgrade Skype. If they don't have these, any automatic updating will create an additional Skype directory, complicating management. You should disable automatic updates where users don't have administrative rights. This also gives you the opportunity to test each new implementation before rolling out to users.

If you work with Macs, you'll need to use the remote installs provided by the Mac OS. These allow you to install while users are signed in, or schedule a remote desktop installation, ensuring that machines get the client as soon as they become available.

2.4 Skype client configuration and policies

Even though Skype utilizes the P2P network, you'll still have a lot of control over common tasks and processes. Skype offers you control over the following aspects of the client:

- Automatic updates
- Importing contacts
- Language
- Local data storage
- Selection of UDP/TCP ports

- File transfers
- Skype API
- Status type
- Personalization
- Proxy setting
- Premium services

There are two ways to control Skype client configurations:

- Group Policy Objects (GPOs) and the registry (Windows only)
- XML-configuration files

These all have a set precedence for managed settings. In order, these are:

1. HKLM (HKEY_LOCAL_MACHINE) registry keys, for all users on a given machine
2. HKCU (HKEY_CURRENT_USER) registry keys, for a specific user on a given machine
3. Shared.xml and config.xml Skype client settings
4. Skype client user preferences and defaults

2.4.1 Windows registry

The Skype client has user-accessible controls for many aspects you may want to manage. Some of the more technical and network-related options are only accessible via the registry. This is because organizations that use them generally manage users' registries centrally and have registry access control so that users can't circumvent settings.

The Windows registry has two sets of values. Local machine values (HKLM (HKEY_LOCAL_MACHINE) registry keys) apply to all users on a given machine and carry the highest priority. Current user values (HKCU (HKEY_CURRENT_USER) registry keys) apply only to a specific user on a given machine, and carry a lower priority.

There are two ways you can alter all the required registry configurations. GPOs are the most intuitive, providing a graphical interface with explanations. Keys can also be manipulated directly with a registry editor.

2.4.2 Group policies

Skype supports group policies for applying policy settings and configurations to users and computers within a Windows Active Directory environment. An administrative template file determines the Skype client's behavior and records changes based on registry values. This is called Skype-vX.X.adm (where X.X is the version of the file). This file modifies specific keys as described below.

You can also configure registry-based policy settings in the GPO Editor under the Administrative Templates node.

The administrative template file doesn't actually apply policy settings, but lets you see them in the GPO Editor. From there, you can create GPOs with the policy settings you want.

For a complete list of the policies you can change, please see [Appendix 1: Configurable policies](#).

2.4.3 XML configuration files

The Skype client uses an XML file-based setup. The Mac OS X doesn't have an equivalent to GPOs, so if you're Mac computer-based, you'll need to edit the XML files.

When Skype is installed, it creates two XML files that describe the Skype client:

- Shared.xml (in \Application Data\Skype) defines the enabled features for all instances of Skype on a given machine.
- Config.xml (in \Application Data\Skype\SkypeName (where SkypeName is the name of the user's Skype login) defines the enabled features for a specific instance of Skype enabled on a given machine.

Administrators (and users with appropriate permissions) may open and edit these files even while Skype is running. In general, Windows network administrators should not make changes to the XML files as this can be done via GPOs.

Note:

XML file entries are case sensitive and proper XML syntax is required, otherwise changes will not apply or the configuration will be lost if Skype is not running.

2.4.4 Client-side settings

Administrators (and users with appropriate permissions) can also change Skype's performance and functionality from within the Skype client. The **Privacy settings** screen controls:

- Who can call or IM a user
- Automatic video reception
- Chat history duration
- Online Status publishing
- Cookie policies

You can configure the privacy setting options via the Skype client by opening Skype and going to **Tools > Options > Privacy Settings**.

2.5 Managing accounts and cost

You can manage your organization's Skype usage by using Skype Manager. Once you

have signed up to Skype Manager as its administrator, you can set up business accounts for your employees and create groups to which those accounts belong, for example, Sales and Marketing.

You can then buy and allocate Skype Credit to your users, assign features and, if you use a SIP-enabled PBX, use Skype for SIP to set up and manage SIP Profiles. You can also view real-time reporting about Skype usage and costs and print out company invoices.

You can find Skype Manager at skype.com/business. For more information on how to use Skype Manager, please see the [Skype Manager User Guide](#).

2.6 Compliance

Skype aims to provide you with a product that will help you satisfy your compliance requirements, whether they are industry standards or national regulations or your own compliance standards. For example, you can prevent file transfers or restrict them to a subset of users to comply with your organization's policies on information sharing between different internal teams, or restrict traders from calling out to comply with trading floor requirements.

For help on how Skype can help with your specific compliance requirements, contact the Skype for Business team at skype.com/business.

3.0 Security and privacy

We're committed to secure communications and protecting our users' privacy. We follow the latest best practice in security, including:

- Encryption of data end-to-end with 256-bit AES encryption keys.
- Protection of encryption keys which aren't revealed to users or escrowed to third parties and are discarded when the session ends.
- Use of credential-based identities and end-to-end encryption to make 'man-in-the-middle' attacks very unlikely.

Our security model also prevents anyone with a supernode or relay node from interfering with, or capturing any part of, a Skype communication, even if they can collect or sniff network data packets. It also makes it very difficult for anybody to eavesdrop on content by installing an internet computer in the theoretical path of Skype traffic.

3.1 Transport-level security

No one can guarantee complete anonymity or secrecy. However, our transport layer encryption uses the Advanced Encryption Standard (AES) algorithm. This makes it very unlikely that your Skype communications will be intercepted or decrypted over the P2P network.

We use both public and private keys to secure all signals over the P2P network, as well as communications content. Our cryptographic model uses public-key and symmetric-key cryptography, including the AES algorithm in 256-bit integer counter-mode. We also use the 1024-bit RSA algorithm to negotiate symmetric AES keys. User's public keys are certified at login using 1536 or 2048-bit RSA certificates.

3.2 Security limitations

Skype encryption and control mechanisms are only able to protect communications when all users in the communication are utilizing the unmodified, Skype-produced software over the public internet. When communications transit other third party systems, including modified software, servers, and phone networks, the user may experience decreased privacy and security levels. An example is a call to a landline or mobile phone, which is carried immediately prior to termination on the regular telephony networks (PSTN or mobile). As a result, this call is only as secure as any regular telephone or mobile phone call carried on that network. Calls to your Online Number, if you have one, exhibit similarly reduced levels of security. Another example is a call made from the Skype For Your Mobile (SFYM or Skype Lite) application, which uses regular (2G) mobile networks to carry the voice part of any communication. These calls are similarly only as secure as the underlying mobile network and regular mobile calls carried on them.

In addition, Skype cannot protect users' hardware against the introduction of spyware or malware, which could compromise the security of a Skype call; it is the user's responsibility to ensure they have adequate anti-spyware and anti-virus protection on their hardware to prevent unauthorized eavesdropping in this manner.

Please be aware that in some jurisdictions Skype works with in-country partners, who take overall responsibility for the Skype products in that market. These partners may distribute modified versions of the Skype software as well as use local servers in order to comply with the laws and regulations. This means there is a possibility that your communications and personal data could be stored, monitored, or blocked and made available to authorised local parties, for instance law enforcement, subject to the local legal standards.

3.3 Privacy

To help manage communications and protect privacy, Skype has tools that give users control over sharing their contact details, who can see their online Status and who can call or IM (Instant Message) them.

Also, some personal information is stored locally on the computer being used by the user. Users should be warned about this, particularly if they're using a public or shared computer.

3.3.1 Sharing contact details

A request to share contact details includes a digital signature, which (once signed) is sent back to the originator. It's tied to the same sign-in credentials used to authenticate a Skype identity.

When a Skype user shares their contact details with another user, it lets them see their currently selected online Status. It also gives them permission to communicate freely with each other (depending on their privacy preference settings).

Each time a user adds a contact to their contacts list, Skype prompts them to send a request for contact details. If the new contact accepts the request, both users are able to see each other's selected online Status.

If the contact denies or ignores the request, the requester cannot see the other user's selected online Status and gets no special communication permissions. Skype can be configured to refuse calls, chats or video from unauthorized Skype clients.

3.3.2 Controlling communication

The ability to communicate contact details is an important part of maintaining privacy. It's also essential for controlling who can contact users. Skype allows each user to set their own privacy thresholds about who can call or IM.

Specifically, users can set preferences determining whether:

- Anyone can call or IM
- Only people on their contacts list can call or IM

In addition, file transfer preferences can be set independently of both calls and IMs.

Users can also block a specific user from seeing their selected online Status or communicating, even if contact details have already been shared. The list of blocked users can be managed via their privacy settings.

3.3.3 Location of personal information

We keep some information on the user's machine, on our servers (but not information such as presence and location) and in the P2P network. While any personal information stored and processed is done in line with applicable privacy laws, Skype provides no inherent security for chat logs, files transferred or voicemail messages stored at the client. You should tell users that:

- Any machine that they use to check Skype continues to synchronize profile data and chat history each time that it's subsequently used, keeping contact lists, communication history and IM contents.
- Chat logs are saved indefinitely in a hidden file in the user's home directory. They can be configured to delete or expire (please see the list of files and registry key locations created during installation in [Appendix 2: File locations](#)).
- Once a text message, file transfer or audio/video stream is received by the intended receiver, the sender cannot prevent it being copied, archived or redistributed by the recipient.

3.4 Security best practice

You should take certain basic actions to address potential threats from:

- Password misuse
- Cross-site scripting and phishing
- Viruses and Trojans
- Falsifying user identity
- SPAM and SPIT
- Multi-logins
- Skype editing

3.4.1 Password security

Skype never requests a user's account name or password by email. Skype passwords are stored as a non-reversible hash. The only areas where passwords are needed are when:

- Signing in to Skype
- Signing in to Skype Manager
- Managing Skype accounts at secure.skype.com/account/login
- Signing in to other known-to-be-valid Skype accounts, such as developer.skype.com

Skype keeps two references to each user's email address, one in the profile on their computer and the other in **My Account** on our website (for password recovery). If their email address changes, it should be updated in both places.

You should also educate users on smart online practices, including:

- Effective passwords and password management
- User identities
- The significance of potential phishing attacks
- The risks of receiving and opening executables

3.4.2 Viruses and Trojans

Skype simplifies file transfers by allowing direct file transfer between Skype clients. However P2P file transfer is a security challenge for corporate networks, as it bypasses your business' network security infrastructure. For this reason, you can disable file transfer throughout your organization via the GPO Editor or by changes to the XML files, if required. By default, file transfers are enabled.

Some basic guidelines will protect your corporate network and still allow users to use file transfer. Receiving users must:

- Have shared contact details.
- Have not blocked the sender.
- Be online when the sender initiates the file transfer.
- Be willing and able to accept the file transfer from the sender.

Note:

Files to be transferred must be smaller than 2GB.

The best practice for any file transfer is that all files should be scanned for viruses and malware. You should enable real-time scanning on your anti-virus software, which will automatically scan before sending or receiving a file.

Note:

Skype has no support for centralized anti-virus scanning.

3.4.3 Falsifying user identity

It's highly unlikely that anyone could impersonate another user's Skype identity. We use public-key cryptography with signed digital credentials to authenticate users. Signed digital credentials are only valid for a limited period, then renewed for additional security.

However, there's currently no way to definitively check that a user's offline identity matches their online identity. As with email, users can create accounts under an assumed name, be listed in Skype's user directory and impersonate others.

You can address this by educating users on the limitations of online identity. Users should first exchange Skype identities at meetings or through email to verify them. As with any email or internet communication, users should know who they're communicating with before they divulge any private information. It's the user's responsibility to prevent their Skype account from being accessed by others.

Please report abuse to us by email, at abuse@skype.com.

3.4.4 Spam and SPIT

Unsolicited email is an unwanted reality of email communications today. We've taken steps to prevent Skype being used as a tool to help spammers or those who Spam over Internet Telephony (SPIT).

You can help to counter spam and SPIT by instructing users to:

- Only authorize users whose identity they've confirmed.
- Set privacy settings so they can only be called by people they know.
- Include a note in their Skype profile asking potential callers to send a chat message before calling.

3.4.5 Adware and spyware

Neither Skype nor the Skype installation programme includes any adware or spyware. However, there are seemingly legitimate online installers that have bundled the Skype client with third party software without permission. This unauthorized software may include adware or spyware.

To avoid such malware, we strongly recommend that you download Skype only from our website at skype.com/business.

Skype software installers for Microsoft Windows XP, Windows 2000 and Mac OS X are digitally signed, as is the application itself. This lets you verify the Skype software installer's digital signature before you install the client, preventing accidental installation of any malware.

3.4.6 Security and Skype for SIP

Skype for SIP does not, currently, offer sRTP or other forms of voice encryption. Voice traffic should therefore be considered in the same light as non-encrypted email and other data traffic.

If you feel that you may be at risk of 'man in the middle' or spoofing attacks you should seek the advice of a specialist network security consultancy.

For more information on using Skype for SIP, please see the [Skype for SIP Requirements Guide](#) and the [Skype for SIP User Guide for Skype Manager](#).

3.4.7 Security summary

Use the following security procedures when deploying Skype:

- Before deployment, ensure you have an authentic copy of Skype. Check the installer's digital signature and follow the limitations in our End User License Agreement and Terms of Service before using Skype.
- To ensure everyone in your company is using the same version of Skype across your company, use the Windows Installer Package (MSI) that comes with the PC version of Skype for Business.
- Instruct your users not to install their own copy of Skype on their machines and centrally manage all Skype installations, manage version control and upgrades and reduce the risk of malware from unauthorized, third party installers.
- Where it's not possible to centrally manage installation, advise your users to download Skype only from our website at skype.com/business and ensure that when a new version of Skype is available, it is automatically downloaded by going to **Tools > Options > Advanced** and ticking the **Notify me** and **Automatically download and install it** boxes.
- Keep your machines' patches up-to-date. Many online security problems can be traced back to improperly patched computers.
- Use anti-virus protection, keep the virus definitions updated and monitor alerts and logs for potential problems.
- Know who you're authorizing and don't hesitate to block users who make unwanted contact.
- Keep user profiles up-to-date and remember that everything in user profiles (except email addresses) can be seen by others.
- Always authenticate third parties before discussing any confidential business or sensitive personal information.
- Remember that although Skype takes care to protect communications from unwanted disclosure, there is a remote possibility that your computer, or that of your contact, could have been hacked or compromised.

- Instruct your users to choose strong Skype passwords and to change them regularly.
- Instruct your users not to check **remember my password** when using Skype on a shared or public computer.

4.0 Appendix 1: Configurable policies

These are the policies available for controlling Skype from a single location, using the Skype GPO Editor template:

Policy	Registry Key*	Description
Functionality		
DisableFileTransferPolicy	DisableFileTransfer, REG_DWORD = {0,1}	Sending and receiving files via Skype is: 1 = disabled 0 = unset = enabled
DisableContactImportPolicy	DisableContactImport, REG_DWORD = {0,1}	Contacts importing into Skype is: 1 = disabled 0 = unset = enabled
DisablePersonalisePolicy	DisablePersonalise, REG_DWORD = {0,1}	Customizing Skype sounds for calls, IM's and notifications is: 1 = disabled 0 = unset = enabled
DisableLanguageEditPolicy	DisableLanguageEdit, REG_DWORD = {0,1}	Editing and Loading Skype Language File is: 1 = disabled 0 = unset = enabled
WebStatusPolicy	WebStatus, REG_DWORD = {0,1}	User's selected online status published on Skype buttons is: 1 = enabled 0 = unset = disable
DisablePremiumServicesPolicy	DisablePremiumServices, REG_DWORD = {0,1}	Usage of Skype Prime Beta is: 1 = disabled 0 = unset = enabled
Other		
DisableApiPolicy	DisableApi, REG_DWORD = {0,1}	Skype API for third party applications is: 1 = disabled 0 = unset = enabled

DisableVersionCheckPolicy	DisableVersionCheck, REG_DWORD = {0,1}	Skype upgrade checks do detect new versions and updates are: 1 = disabled 0 = unset = enabled
MemoryOnlyPolicy	MemoryOnly, REG_DWORD = {0,1}	Running Skype only in memory (without storing any data on the local disk) is: 1 = enabled, mem-only 0 = unset = disabled, disk storage is used

Network		
ListenPortPolicy	ListenPort, REG_DWORD = {0,1}	Editing by user which port Skype listens to for incoming connections is: 1 = disabled 0 = unset = enabled
ListenHTTPPortsPolicy	ListenHTTPPorts, REG_DWORD = {0,1}	Editing by user whether HTTP (80) and HTTPS (443) ports are used as alternatives for incoming connections is: 1 = disabled 0 = unset = enabled
DisableTCPListenPolicy	DisableTCPListen, REG_DWORD = {0,1}	Skype listening incoming TCP connections is: 1 = disabled 0 = unset = enabled
DisableUDPPolicy	DisableUDP, REG_DWORD = {0,1}	Skype using UDP in communication is: 1 = disabled 0 = unset = enabled
DisableSupernodePolicy	DisableSupernode, REG_DWORD = {0,1}	Skype peer can start acting as supernode in p2p network (criterias needs to be met (unused CPU & RAM, NW availability, uptime)) is: 1 = disabled 0 = unset = enabled

ProxyPolicy	ProxySetting, REG_SZ = {string}	Skype uses proxy settings: Empty string = unset = Skype tries to connect directly, if fails, then uses user defined proxy settings. “Automatic” = proxy settings are retrieved from the Windows proxy settings (internet options) “Disable” = user cannot modify proxy settings. “HTTPS” = forces Skype to use only HTTPS proxy, doesn’t try to connect directly. “SOCKS5” = forces Skype to use only SOCKS5 proxy, doesn’t try to connect directly.
	ProxyAddress, REG_SZ = {string}	When ProxySetting = HTTPS or SOCKS5 proxy address to be used by Skype: Empty string = unset = Windows proxy settings are used. “hostname:port” = Proxy address to use (example: socks5.mydomain.com:5050)
	ProxyUsername, REG_SZ = {string}	When ProxySetting = HTTPS or SOCKS5 and if proxy requires authentication, username to be used by Skype: “username” = Proxy username (example: sock5user)
	ProxyPassword, REG_SZ = {string}	When ProxySetting = HTTPS or SOCKS5 and if proxy requires authentication, password to be used by Skype: “password” = Proxy password (example: Password3,)

Where keys are used to govern local machine action (HKLM), they should be preceded by:

HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone <Registry Key>

For example:

HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, DisableApi, REG_DWORD = {0,1}

Where keys are used to govern end user action (HKCU), they should be preceded by:

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, <Registry Key>

For example:

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, DisableFileTransfer, REG_DWORD = {0,1}

5.0 Appendix 2: File locations

The locations of the files created during the installation process are listed below:

Description	Location
The Skype programme (administrative privileges)	%programfiles%directory; typically C:\Program Files\Skype\Phone\
The Skype programme (limited privileges)	%homedrive%.or%homepath%directory; typically C:\Documents and Settings\<username>\ApplicationData\Skype\
Pictures	%allusersprofile% directory; typically C:\Documents and Settings\All Users\Documents\My Skype Pictures\
Temporary folder used for installation, removed after setup	%temp% directory
User-specific information	C:\Documents and Settings\<username>\Documents\Skype\
Icons	C:\Documents and Settings\<username>\Documents\My Skype Pictures\
Skype session data	C:\Documents and Settings\<username>\LocalSettings\Application Data\Skype\
Default file location	HKLM\SOFTWARE\Skype

6.0 Appendix 3: Additional information

For more information on Skype:

- Skype for Business: skype.com/business
- Skype FAQs: support.skype.com
- Skype user guides: skype.com/help/guides
- Skype's privacy policy: skype.com/legal/privacy/general
- Information about Skype-compliant hardware: developer.skype.com/Certification/Hardware/CertifiedProducts
- Information about SILK: developer.skype.com/silk
- The NAT RFC is RFC 4787 (NAT UDP Unicast Requirements): tools.ietf.org/html/rfc4787

For more information on how to deliver and apply group policies:

- Open Group Policy as an MMC snap-in: [technet.microsoft.com/en-us/library/cc782895\(WS.10\).aspx](https://technet.microsoft.com/en-us/library/cc782895(WS.10).aspx)
- Using Administrative Template Files with Registry-Based Group Policy: [technet.microsoft.com/en-us/library/cc779567\(WS.10\).aspx](https://technet.microsoft.com/en-us/library/cc779567(WS.10).aspx)

