Skype

網路管理者指南

Skype 3.0 Beta

The whole world can talk for free. Skype.com

這份指南的用途是什麼?

這份指南提供重要資訊，幫助讀者了解 Skype 的運作方式、 Skype 的安全性，以及在企業環境中管理 Skype 的方法。

誰應該閱讀這份指南?

這份最新且更完整的**網路管理者指南** (草稿) 是專門爲了像您這樣的資訊人員 (系統與網路管理員)，在部署應用軟體時，特別在微軟視窗 (Microsoft Windows) 平台環境中所使用的。

這份指南希望能幫助您了解 Skype 的架構與安全模型，並透過原廠最新釋出的資訊，順利地在企業環境中安裝與設定 Skype。

這份網路管理者指南假定您對企業部署軟體程序、編輯視窗註冊作業、視窗群組政策管理、基本 XML 語法等都具備一定程度的背景常識。同時也對其他相關的網路架構與作業系統環境等領域都有相當的專業認知。

如何閱讀這份指南

這份文件使用下列的字體規則:

格式	意義
大寫字體	關鍵字如目標、命令，或是通知
小寫字體	某個關鍵字的類別，例如通話時間
<角括號>	識別代號，例如使用者帳號或是通話 ID
[<方形括號>]	非必要項目
* (星形號)	重複項目
| (直線)	或
->	用戶端命令
<-	Skype 的回應或是通知
//	程式碼的註釋
>	選擇選單上的下一個項目

重要的法律資訊

在散佈 Skype，或使用 Skype API 之前，請確定您清楚地了解法律名詞的意義，並同意其條款規定。您可以在 Skype 官方網站與/或 Skype 用戶端軟體上找到這些文件。

- 如同所有的 Skype 用戶，您必須簽署**使用者授權合約** (**End User License Agreement**)。
  `http://www.skype.com/company/legal/eula/`
- 若要重新散佈 Skype，您必須同意 **API 重新散佈條款**。
  `http://www.skype.com/company/legal/terms/api_redist.html`

著作權

Skype 不對這份文件或相關文件及其內容的正確性、完整性、適用條件、使用適當性或效益做任何代表或保證，也不對任何使用本文件的公司行號、團體組織負有任何義務或責任。

一旦開始使用這份文件與其相關文件，即代表各位承認 Skype 的智慧財產權，並同意上述條款，對所有違背條款的行爲擔負一切法律責任。

商標

未承諾事項聲明

這份文件所陳述的服務內容係由 Skype Technologies S.A., 與此文件撰寫當時之子公司或經營夥伴所提供。Skype 之服務內容，根據官方網站上的 Skype 服務條款，可能隨時會有更動或被終止。Skype 軟體與網路架構的內部設計若有變更，亦不會於事先通知。

Skype 亦不對第三方 (亦即貴我雙方外) 的網站或文件中，有關於本文件內容的部分負任何責任。這類參考資料純粹提供 Skype 客戶參考用。Skype 並未針對這些資料內容做過檢驗，亦不保證在特定用途或是需求下使用這些文件的後果。

目錄

概要

Skype 軟體與服務提供人們一個嶄新、安全而充滿創意的溝通方式，讓網際網路成爲與人們傳遞訊息的有效媒介，無論是語音通話、即時文字訊息或是其他形式的通訊。

Skype 是世界上第一個分散式電信網路系統，但是它提供許多除了語音通話之外，更多能透過公共網際網路來進行的服務。

透過使用一個小巧的用戶端軟體 (在幾個主要的電腦平台都有對應支援的版本) Skype 用戶可以傳送或接收文字訊息、進行語音通話，並傳送檔案給其他的 Skype 用戶。

Skype 用戶與其他線上的 Skype 用戶進行通訊是完全免費的，至於某些特級服務，例如從 Skype 撥打到傳統電話號碼，則以非常低廉的價格計費。

Skype 的通訊主要依靠點對點傳輸技術來提升語音通話的品質，並盡量降低用戶之間的資料傳輸量。

這個詞彙「點對點」通常寫成「P2P」，是一種利用許許多多與網際網路保持連線的個人電腦來進行資料傳遞運作的軟體應用模式；不用依賴大型且昂貴的中央電腦主機。從這個觀點來看，Skype 網路架構的穩定度其實相當高。因爲 Skype 並不是靠著單一的「關鍵節點」來維持服務的運作。

Skype 服務介紹

提到 Skype 服務，眾所皆知的是聲音與視訊通話、檔案傳輸以及即時訊息等每個 Skype 軟體用戶端都可以使用的功能。而這些服務的基礎建立在 Skype 的網路電話簿、上線狀態管理以及網路資訊傳送技術上。

Skype 題供使用者各種型態的通訊服務，如下列所示:

- 與其他 Skype 用戶進行語音通話
- 與其他 Skype 用戶進行語音多方通話
- 撥打電話到傳統電話 (SkypeOut)
- 從傳統電話撥打進來 (SkypeIn)
- 進行視訊通話
- 聊天室，讓最多 48 位參與者可以同時即時交換文字訊息
- 跨平台檔案傳輸
- 網路電話簿與上線狀態管理

Skype 使用者程式已經開發在幾個最普遍的電腦平台上，包括 (但不限於) Windows XP、 Windows 2000 或 or Linux、Apple Macintosh (Mac OS X) 以及 Pocket PCs (Windows Mobile)。

其他資訊

以下是與這份指南相關的參考資料:

- **Using Administrative Template Files with Registry-Based Group Policy**
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/admtgp.mspx

- **Open Group Policy as an MMC Snap-in**
  http://technet2.microsoft.com/WindowsServer/en/library/ae13960b-3a27-4b19-a866-ed6e6e7a312d1033.mspx?mfr=true

序論

越來越多的大型組織與企業都選擇允許 Skype 在他們的網路環境中運作，以享受節省大量通話費的好處、安全的檔案傳輸、多人即時通訊，以及其他各種方便好用的功能。

每一位 IT 管理者都應該知道的事情

Skype Technologies S.A., ，希望人們在企業裡面也能如同在家中一樣，享受 Skype 的各種便利功能。

Skype 開發團隊持續專注於改善軟體使用上的便利性，隨著每一次的改版，Skype 的功能也變得更完整；無論是對家庭用戶或是企業用戶來說都是如此。

以下這些與 IT 管理者分享的重點功能，相信能讓各位更了解到， Skype 正逐漸變得對 IT 人員越來越友善。

- **Skype 可以節費** – 用戶網內通話完全免費；透過 SkypeOut 撥打傳統電話則非常便宜。Skype 可以爲您的企業省下大筆的通訊費用。
- **Skype 非常安全** – 訊息透過 Skype 的 P2P 網路架構傳輸，安全性極高。
- **與防毒工具軟體充分整合** - 由 Skype 傳送出去或傳送進來的檔案都能經由主要的防毒軟體掃描，確認無病毒才開啓。
- **保護隱私權** – Skype 的加密與授權機制能幫助您符合企業組織與政府機關的隱私權保障需求。
- **維持防火牆安全** – Skype 並不需要特別開啓您的防火牆才能使用 – 通常根本不需改變任何設定。
- **Skype 讓您充分掌控** – 您可以關閉或調整 Skype 的各種功能，包括檔案傳輸與 API。
- **用戶不會受到垃圾訊息的騷擾** – 由於通訊行爲建立在聯絡人之間彼此相互授權的基礎上，可以有效避免垃圾訊息的氾濫。
- **沒有廣告軟體或間諜軟體** – 不論在 Skype 用戶端或是安裝程式上都不會安裝任何用戶拒絕安裝的軟體。

Skype 的運作方式

不同於依賴集中式的架構與設備，Skype 依靠的是尚在發展中的 P2P 網路技術來建立 Skype 用戶的連線，以及彼此的通話路由、即時訊息、檔案傳輸與視訊等各種通訊方式。

一旦安裝完成，Skype 就像是任何一套終端用戶軟體一樣。Skype 介面會在用戶撥打語音/視訊通話、傳送/接收即時訊息，或是傳輸檔案等各種功能時出現。否則，一般情況下，Skype 軟體只會處於待命狀態，僅使用極少量的電腦與網路資源。

Skype 的 P2P 架構

在任何兩位 Skype 用戶間的互動 – 所有語音、視訊、文字訊息，或是檔案傳輸 – 都透過加密過的「通話層」傳遞。而這個連線會在 Skype 用戶間開始傳遞訊息前就已經建立起來了。

完整的 Skype 服務是由 Skype 用戶端程式與其 P2P 網路架構所組成的。Skype 用戶端程式是主要的通訊平台，它也提供其他的基本功能，整合了語音通話、即時訊息、視訊通話，以及檔案傳輸這些功能到單一軟體內。

Skype 用戶端程式與其網路架構緊密地結合在一起，並透過一組授權伺服器來運作，這部分會在後面更詳細的討論到。另外，不像許多 P2P 應用程式，Skype 用戶端程式 (從 Skype 網站下載時) 沒有包含任何廣告軟體、信件軟體或是間諜軟體。

超級節點的智慧路由

當一個 Skype 用戶端程式被下載與安裝完成後，這個使用者的電腦就成爲 Skype P2P 網路架構的一部份，也就是變成 Skype 網路架構中的一個節點、超級節點或中繼主機。Skype 能夠利用這些節點、超級節點與中繼主機的串連與互動，建構成一個傳遞訊息的網路系統。

超級節點 是標準的 Skype 節點，但是設定狀態比較特別，擔負額外的任務。超級節點負責偵測 Skype 用戶是否上線，建立他們之間的連線，並傳送帶有信號的訊息，確保被加密的流量被有效地發送。.

超級節點間彼此協同作業，支援 Skype 目錄服務或是*全球索引* — 一種分散式的 Skype 用戶資料庫。Skype 全球索引，在某種程度上，是由可用的超級節點 (群) 分層組成。詳情請參照後面章節的「Skype 全球索引」，會有更多關於超級節點的資訊。

全球索引並沒有依靠某個中央伺服器來運作。當性能足夠，且上網速度夠快的電腦啓動了 Skype 軟體，在某些特定條件下，就有可能自動「活起來」成爲一個超級節點，並作爲附近的 Skype 用戶們的臨時目錄索引。每個超級節點的性能建立在電腦的可用記憶體、頻寬以及一般運作時間等基礎上。

即使每個 Skype 用戶端都內建了成爲超級節點的功能，但是只有相當低比例的 Skype 節點會被轉換成超級節點。

超級節點的附加功能是從何而來? 事實上，當 Skype 用戶端軟體安裝完成後，只有部分的應用功能會顯示給終端用戶看。另外，大多數 Skype 使用者不會在用戶端見到的是，Skype 軟體在安裝時，會順便評估那台電腦的性能以及網路連線品質，以確認其在 Skype 網路系統中能夠扮演的角色。

在普通環境下，一個 Skype 用戶端會以一般節點的狀態在 Skype 網路架構中運作。然而，一個 Skype 用戶端在電腦效能強大、網路連線品質穩定的環境下，在某個狀態下會「醒過來」成爲超級節點或中繼主機以支援「全球索引」功能，這給了 Skype 網路系統一個不顯眼但是重要的附加功能，雖然大多數用戶並未發覺他們其實還蠻常用到它的。

Skype 超級節點與中繼主機

當 Skype 節點成爲超級節點後，它會建立一個局部星狀叢集 (local cluster in a star-like pattern) 最多可整合數百個在 Skype 點對點網路系統中節點的可用資源。

每個超級節點都擁有目錄項，最多會有數百位 Skype 用戶的目錄供查詢。然而，雖然超級節點得接受相對於一般節點而言較多的查詢需求，它們事實上並沒有負責傳送聲音、文字、影像或是其他格式的檔案資料。超級節點每秒最多只會用到 5 kilobits 的頻寬。

流量種類	每個 Session 的頻寬限制
帶有信號的資訊	每秒 5 Kbyte (最大)

Table 1. 超級節點每個 Session 的頻寬限制

中繼主機與超級節點相似，但是它在 Skype 網路系統中扮演的角色與功用則並不相同。每個超級節點在叢集中負責擔任附近節點的臨時目錄索引；中繼主機則扮演資料傳遞的跳板，在兩個 Skype 用戶無法建立直接連線時，居中協助雙方傳遞資料。

中繼主機*確實*有傳遞 Skype 的網路流量，但是它們一樣有頻寬限制，由每個 session 會使用到的頻寬爲基礎，來評估總頻寬用量，不會無限制地佔用網路資源。請注意，雖然理論上每部中繼主機可以同時建立一個以上的 session 來當跳板，但是實際上這種情況並不常見，而且既使發生也不至於對原本的流量上限造成衝擊。

流量種類	每個 Session 的頻寬限制
檔案傳輸	每秒 3 Kbyte (最大)
語音通話	每秒 4 kByte
視訊通話	每秒 10 kByte (最大)

Table 2. 中繼主機每個 Session 的頻寬限制

被拿來作爲超級節點或是中繼主機使用的各種資源，與系統整體相較，不論是處理器性能、記憶體、儲存空間以及可用頻寬等各方面都非常有限，並不會造成過多負荷。

除此之外，由於限制了超級節點與中繼主機的使用頻寬，Skype 用戶根本無法辨別自己的電腦是一般節點、超級節點，或是中繼主機。(因爲即使用到那些附加功能，耗用的資源還是非常有限，不會影響電腦效能。)

Skype 用戶端 / 超級節點之間的關係

每個 Skype 用戶端都儲存了一份超級節點網路位址清單，讓節點建立連線網路。當一個 Skype 用戶端成功地接觸到一個運作中的超級節點之後，Skype 用戶端就會取得一個更新過的、目前可用的超級節點網路位址清單以供日後使用。

Skype 用戶端會選擇一個運作中的超級節點作爲它的「上游」連結，並上傳搜尋需求與其他相關資料到超級節點。接著，這個超級節點會跟其他超級節點連接，以滿足任何搜尋需求。所謂的搜尋需求可能來自於一個授權請求、一通語音或視訊通話、即時訊息或是檔案傳輸…等等。不過一般來說，Skype 用戶端都會先試圖與另一個 Skype 用戶端建立直接連線。

當某個 Skype 用戶端無法與另一個 Skype 用戶端直接連線時，附近正在運作中的超級節點就會開始進行路由作業，將通話流量透過中繼主機來傳遞。

每個 Skype 用戶端都會開啓多個連線路徑待命使用，並根據最低延時 (lowest latency) 與最佳頻寬動態選擇連線路徑，以提升成功撥通率、改善整體服務品質。接下來，Skype 用戶端會連接到一個節點，開始透過超文字傳輸協定 (HTTP) 來傳送文字、語音、影像與其他格式的檔案。

既使本身不是超級節點，Skype 用戶端仍會維持在保有多個連線的狀態。因此，您可能會見到許多 TPC/UDP 連線，既使這個 Skype 用戶端不是超級節點或中繼主機。

重要訊息: 某些價格較低廉的路由器、防火牆或是閘道器 (通常設計給家用，而且沒有經過 Skype 認證) 可能會無法支援同時多個 TCP/UDP 連線來維持成功撥通率以及通話品質。

Skype 全球索引

在 Skype 1.2 版之前，用戶的聯絡人名單是由個別的 Skype 用戶端來管理 (儲存在用戶電腦中)。在 1.2 版之後，聯絡人名單會透過集中式目錄來管理，確保每一位用戶在別的電腦中登入 Skype 時也會見到完整的聯絡人名單。

這代表您可以在新的(多部)電腦上安裝 Skype 後，讓每位用戶登入 Skype，就立即見到完整的聯絡人，無須重新建立名單，作業亦不受影響。

更進一步地，現在*分散式*網路電話簿服務或*全球索引*/ wa 都已經被部署在軟體中，以強化整體的服務品質。如前所述，全球索引不是由某一部中央伺服器來管理，而是由超級節點(群) 分層管理。

防火牆與內網互聯 (NAT-Device Traversal)

在大多數情況下，Skype 會自動穿過大多數的防火牆或是 NAT 。因此，許多網路管理者在試圖部署 SIP (Session Initiation Protocol) 基礎的網路電話時常會面臨到的問題，在 Skype 的創新 P2P 網路架構中大都可以被避免。

在路由不受限的網際網路位址運作的 Skype 用戶端 (還有那些不在防火牆後面的 Skype 用戶端) 能夠提供那些被網路轉址設定所阻礙的節點連線方面的協助。

在防火牆外的節點可以幫助在防火牆或 NAT 後面的節點進行連線，前提是它們雙方都要能夠對外連線到網際網路。

因此，當一位用戶開始撥打一則 Skype 電話時，連線總是可以被建立，不論撥打方或是受話方在防火牆後或 NAT 內。

然而事實上，某些防火牆軟體的確與 Skype 會有衝突。在這種情況下，您可以直接更改設定，讓 Skype 可以正常運作。

Skype 支援一般的 HTTP 或 HTTPS 代理伺服器，以及有認證機制的 HTTPS/SSL 與 SOCKS5 代理伺服器。在 Skype 用戶端介面中，這些設定可以在 [功能] - > [設定選項] - > [連線] 來設定。

Skype 網路資源消費量

通常來說，Skype 節點、超級節點與中繼主機都僅需要最小的 CPU 資源。然而，即使用戶使用更多的功能，例如多方通話、或是需要更多頻寬的檔案傳輸，甚至是視訊通話時，耗用的系統資源依然相當有限。

頻寬指標

Skype 視窗版用戶端程式現在支援頻寬指標 (bandwidth indicator) 功能，預設是關閉的狀態。當頻寬指標被開啓時，一個文字指標就會出現在 Skype 主視窗的左下角，告訴用戶 Skype 正在佔用多少頻寬，上傳或下載的頻寬用量都看得見。

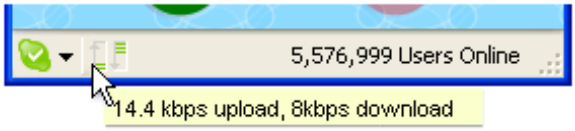

圖 1. Skype 用戶端頻寬量計

頻寬指標內有七種顏色橫條，作爲頻寬使用量程度的參考，這會隨著頻寬實際用量而跟著改變。

每個頻寬指標內的橫條都代表某個特定頻寬門檻。這些橫條以綠色、黃色、或是紅色等顏色來代表被使用的頻寬量。

橫條 7	150kbs
橫條 6	125kbs
橫條 5	100kbs
橫條 4	75kbs
橫條 3	50kbs
橫條 2	25kbs
橫條 1	0kbs

表 3. Skype 用戶端頻寬指標門檻

這個指標在預設狀態是「關閉」的。不過，您可以在設定視窗中開啓它。由 [工具] -> [設定選項] -> [進階]，並勾選「顯示 Skype 頻寬使用狀態」即可。

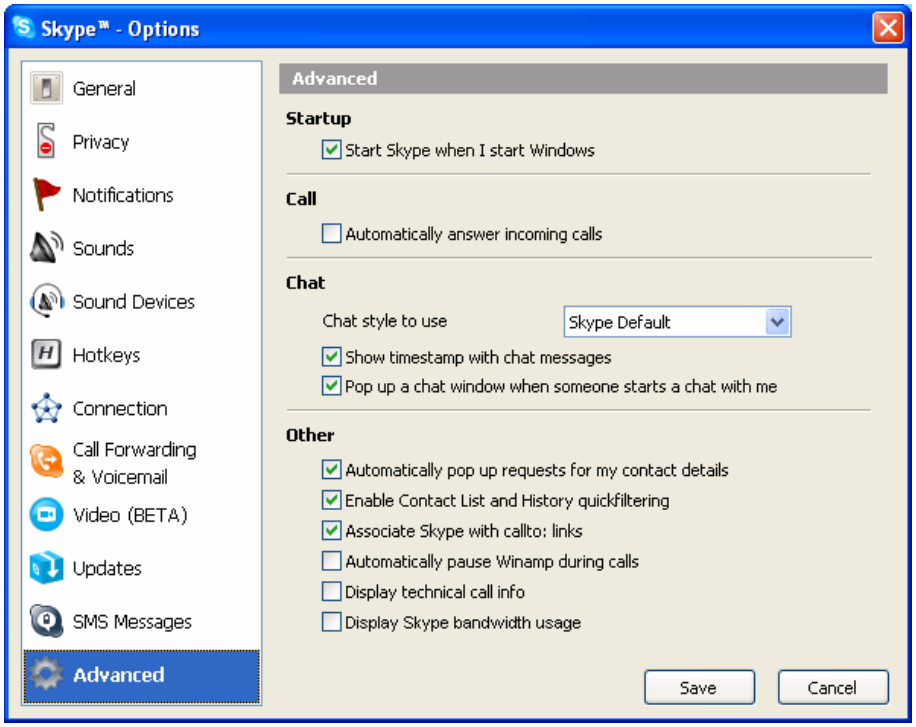

圖 2. Skype 用戶端頻寬測量選項

Skype 安全性模型

Skype 是目前唯一利用高性能加密機制來保護網路訊息傳遞的網際網路語音應用服務供應者。能做到這點，是因爲 Skype 穩固的安全性模型與其基本的 P2P 網路架構充分整合之故。

事實上，Skype 的網路流量都是透過超級節點來進行路由作業，也可能是透過中繼電腦(群) 來進行路由 (這些被當作跳板的電腦與接力傳遞訊息的裝置本身不會介入語音通話、即時訊息，或是檔案傳輸)，亦即在 Skype 網路內，所有被傳遞中的資訊都會自動加密，確保只有發送與接收雙方能掌握訊息內容。

因此，Skype 網路中的訊息無法在傳送過程中被攔截或破譯。即使 Skype 提供的是一個私有的通訊管道，而它依然在主流的作業系統中運作。

雖然 Skype 網路流量無法在傳送中被攔截或破譯，但是當負責加密 Skype 流量的電腦本身也在進行通話、傳遞即時訊息或是其他檔案時，儲存的資料例如聊天室記錄或是語音留言可能會比較脆弱。

在 Skype 用戶端軟體被安裝與執行的電腦上，透過作業系統本身的安全機制，Skype 提供作業系統等級的安全性或隱私權保障。換句話說，您的電腦本身安全等級有多高，儲存在裡面的 Skype 相關檔案安全性就有多高。因此，若用最嚴格的定義來看，Skype 既沒有提供絕對安全的電腦作業平台，也沒有辦法百分之百保障檔案儲存的安全性。

提到*安全的電腦作業平台* ，這裡是指在資訊的傳輸、接收、處理以及儲存等各方面都能在符合最高的技術標準，即便是高價值或高風險的資訊，在傳輸過程也能確保安全無虞。

Skype 的安全性模型可以有效地防止任何能登入超級節點或是中繼主機電腦的人攔截或是取得任何 Skype 的通訊內容，就算他們可以直接取得網路封包，也無從得知其實際內容。它也可以避免任何人 (特別是那些您覺得會造成威脅的競爭對手們。) 透過在網際網路的特定路徑上安裝電腦來偷聽或截取 Skype 的流量內容。

結論就是，雖然 Skype 無法完全保證匿名與隱私不遭到窺探，但是它確實可以提供傳輸層 (transport-layer) 的安全性，保障在 Skype 網路中被傳遞的訊息內容不會被窺探或截取。當然 Skype 網路流量與訊息內容也不會被傳送到未經用戶授權的目的地。

Skype 使用者認證

Skype 的安全模式使用經過簽章的數位憑證以及公開金鑰加密。這讓 Skype 能夠驗證每個使用者的身份。這也能減少對於集中式基礎架構的需求。

透過公開金鑰/私密金鑰的加密，金鑰之一會被「公開」，其散佈並未受到限制。而另一把金鑰則還是保持隱密。這兩把金鑰互相獨立，但彼此仍有關連。光靠其中一把金鑰無法猜到另一把的內容。「握手」動作需要同時有兩把金鑰才能完成，透過這個動作才能完成一個溝通的通話連線。

當某個 Skype 使用者利用他的 Skype 名稱與密碼登入 Skype 之時，該使用者的 Skype 用戶端程式會試圖連上中央的資源；這裡所謂的中央資源就是 Skype 認證伺服器。只有當認證伺服器核准連線，才會給予該使用者的 Skype 用戶端程式一個經過簽章的數位憑證，此簽章利用到 Skype Technologies S.A.公司所保存的私密金鑰。

用來認證 Skype 使用者的數位憑證的另一把金鑰是儲存在各人的 Skype 用戶端程式中。簽章過的數位憑證的有效性只能維持一段時間。附帶一提，Skype Technologies S.A.公司每過一段時間就會將這些金鑰更新，以維持安全性。

當某個 Skype 用戶端程式得到簽章過的數位憑證，也通過了認證，Skype 用戶端程式可能會(代表 Skype 使用者)將其出示給其他的 Skype 用戶端程式。當認證過程完畢之後，接收者就沒有必要透過重新連上認證伺服器或其他中央端的設備來再次檢查撥打者的憑證。

注意：對Skype網路而言，Skype使用者的代號就是已經通過網路認證的Skype名稱。雖然Skype使用者通常同時只會開啓一個Skype用戶端程式，但是同一個個人其實可以擁有多個Skype帳號，其中的Skype名稱、密碼與個人資料都不同。

Skype 連線 (Sessions) 如何建立?

當 Skype 使用者希望跟其他 Skype 用戶溝通時，都會個別建立連線。

當 Skype 使用者上線，該使用者的 Skype 用戶端程式會維持與超級節點之間的永久連線。這讓此用戶端會出現在 Skype 網路上；簡單來說，這就是此 Skype 用戶端之所以能夠告訴其他用戶端 此使用者上線狀態的方式。

此外，當 Skype 使用者試圖與其他人溝通，該撥打者的 Skype 用戶端程式會去檢查整體的索引—也就是運作中的使用者資料庫，保存在超級節點目錄的某個階層—來確定某個接收者是否真的在線上，不管該接收者將自己的上線狀態設成怎麼樣。

注意： 爲求簡潔，以下段落不會去區分語音或視訊通話、即時文字訊息以及檔案傳輸。我們只會說撥打者或接收者，讓文字更簡單。

如果溝通對象接收者在線上，該撥打者的 Skype 用戶端程式會取得接收者的 Skype 用戶端程式網路位址，以及在整體索引中該 Skype 用戶端之超級節點的網路位址。

接下來撥打者的 Skype 用戶端程式將會試圖與該接收者的 Skype 用戶端程式直接連線。假定這兩個 Skype 用戶端程式能夠互相直接連接，就可以展開溝通。

直接連線不是每次都能馬上建立。舉例來說，當接收者的 Skype 用戶端程式在防火牆或 NAT 設備之後，就有可能無法立即建立連線。所以在設計上如果對某一方的連線試圖失敗，撥打者的 Skype 用戶端程式就會透過超級節點傳遞一個訊息給該接收者的用戶端程式。

Skype 傳送的此一訊息目的在警告接收者的 Skype 用戶端程式兩件事情：首先，撥打者的 Skype 用戶端程式希望連線，其次，它無法直接連線。這項訊息也會要求接收者的 Skype 用戶端程式試著去建立反向連線，換句話說就是：「我連不上你，你可不可以連上我？」

如果 Skype 用戶端程式可以用相反路徑建立直接連線，則開始溝通。訊息內容會直接從一個 Skype 用戶端程式傳到另一端。

然而如果 Skype 用戶端還是沒辦法彼此連上，那麼 Skype 就會試著找出透過中繼主機的路徑，這是 Skype 網路的另一種特殊節點。中繼主機就像是超級節點，因爲他們就是普通的 Skype 同儕節點，在一組特殊的環境條件下負擔了額外的責任。

這些中繼主機會負責偵測上線的 Skype 用戶端程式、建立連線，並且傳遞信號訊息來保證加密的內容選擇有效率的路徑傳輸。

基本上中繼主機近似於超級節點，但是並不像超級節點被當成暫時的目錄索引伺服器給附近電腦叢集的節點使用，中繼主機實際上並非該通話的當事人之一。 中繼主機只是爲 Skype 網路傳輸提供一條代替的路徑而已。換句話說，它們是資料傳遞站，爲無法直接連線的 Skype 用戶端程式提供一條清楚的連線路徑。

在這種狀況下，撥打者與接收者的 Skype 用戶端程式都連接到中繼主機上。事實上，Skype 網路傳輸的內容是在多台中繼主機上散佈以達到容錯目的，同時保障通話的品質與完整性。在某特定通話連線的過程中，所有中繼主機都會持續運作，直到該場通話結束。

在此重述前面已經提過的，Skype 傳輸層的安全性在 Skype P2P 架構中之所以重要，是由於如果要完成連線，超級節點永遠(中繼主機有時候)都必須參與 Skype 用戶端程式間的溝通。Skype 的安全模式之所以能防止竊聽，就是因爲在每一對節點、超級節點與中繼主機之間，資料從頭到尾都受到加密保護。

加密機制如何運作?

Skype 靠著公開與私密金鑰確保溝通的內容不致洩漏。如前所述，所有 Skype 網路上傳輸的資訊都經過加密以確保隱私。這些資訊包括控制 Skype 網路所用的信號以及溝通的內容，特別是語音、視訊、文字與資料文件。

使用這麼強的加密，代表人們不可能得知現在在 Skype 網路上傳遞過節點、超級節點與接力傳送主機的資訊。

Skype 背後的加密模式同時用了公開金鑰與對稱金鑰加密法，包括 AES 演算法，用在 256 位元整數計數器模式下。Skype 也使用 1,024 位元 RSA 來協調對稱的 AES 金鑰。使用者公開金鑰在登入 Skype 伺服器時進行認證，使用的是 1,536 或 2,048 位元 RSA 認證。

每當 Skype 用戶端程式建立連結 (但實際的語音、視訊、文字或檔案傳送尚未開始)，每個連上該連線的 Skype 用戶端都會出示數位簽章，也必須認可一個 Advanced Encryption Standard (AES) 加密金鑰。

當建立連結時，每個 Skype 用戶端都會產生一個 256 位元對稱金鑰的一半。這些金鑰會交換結合形成一個 256 位元的連線金鑰，在該連線存續的期間都有效。每段連

線都會產生一個獨有的 256 位元金鑰。在多方電話會議時，會同時產生多通對話，每通都具有本身獨一無二的金鑰。不管有效使用者有多少，共享對稱 AES 金鑰都能讓 Skype 成爲經過驗證的溝通管道。

附註：美國政府已採用 AES 來保護敏感資訊。透過 256 位元加密，任何一個 1.1 x 1,077 可能的金鑰都能用來加密敏感資料。

Skype 靠公開金鑰加密來驗證協調對稱金鑰的憑證簽章，然後用對稱金鑰加密來保障 Skype 用戶端程式之間通訊的安全。透過綜合應用這些方法，讓建立 Skype 用戶端程式間傳輸層安全的過程更有效率。

公開金鑰加密模型開啓了兩件事的可能性。首先這讓 Skype 用戶端程式能夠接收到只有它本身能讀取的私人訊息，並且這也讓 Skype 用戶端程式能發出經過簽章的訊息，其他人無法創造一樣的訊息。沒有任何人或組織（包括 Skype Technologies S.A. 公司本身）會擁有與某一場 Skype 通話相關各方相同的一份金鑰。

此外，除了分享來建立一個 256 位元連線金鑰的成對資料之外，用戶端程式不會進行任何金鑰的分享或是將金鑰洩漏給任何他人。

安全與檔案傳輸(病毒、特洛伊木馬等)

Skype 有一種特別強大的功能，讓使用者可以安全地在電腦間傳輸檔案。

在 Microsoft 的 Windows 平台上，系統與網路管理者透過變更系統設定鍵值，可以關閉 Skype 用戶端程式的檔案傳輸能力。請見本文件後面的部份。

Skype 的檔案傳輸功能讓使用者可以將 2GB 以下的檔案傳送給聯絡人名單上的任何一個人。接收者必須符合以下四項條件：

- 已分享聯絡人細節資訊 (請見「隱私與聯絡人分享」)
- 沒有封鎖寄送檔案者 (請見「封鎖 Skype 使用者」)
- 當對方開始傳輸檔案時在線上
- 願意並可能接收該檔案

注意： 有時某個 Skype 使用者會顯示正在線上的狀態，但其實他不會接收到傳送檔案的通知，直到他接收某種型態的資訊聯絡，包括即時訊息或語音電話，以重建 Skype 用戶端間的連結。

Skype 用戶端程式會儲存每個使用者的檔案傳輸紀錄，無論是送出檔案還是接收檔案。除非使用者刻意清除，這分清單會顯示在「通話紀錄」分頁中。清單中也會顯示檔案系統中的來源或目的地。

Skype 的檔案傳輸能力提供方便安全的數位檔案交換管道，但是這項新功能也帶來風險，包括不慎下載包含病毒、特洛伊木馬或間諜程式的檔案。

所以就像企業用戶在開電子郵件或從網路下載檔案時務必小心一樣，在從其他 Skype 使用者那裡接收檔案時也一定要特別謹慎。

防毒程式與即時掃描

主要的防毒軟體廠商都提供防毒程式，能夠對電腦進行即時掃描。如前所述，所有的 Skype 網路傳輸從一端到另一端的過程中都是在加密狀態下。唯有當 Skype 使用者決定要接收檔案的時候，用戶端程式才會對收進來的檔案進行解密。

每當 Skype 解密一個檔案，該電腦上的防毒軟體就會即時對其進行掃描。所以如果您所屬的組織正在使用，或決定使用 Skype，以下各事項都非常重要：

- 將防毒軟體設定爲掃描*所有*接收的檔案
- 時時注意將防毒軟體的病毒定義檔更新到最新狀態，或者
- 按照這份文件後面所寫的方式關閉檔案傳輸功能。

進行以上事項，可以避免您的 Skype 使用者無心將可能受感染的檔案儲存到檔案系統中。(只要防毒程式還在執行，且該病毒或特洛伊木馬爲已知種類)

注意： 現有的 Skype 版本並不支援集中式的病毒掃描。

任何軟體程式想要在硬碟上進行讀取或寫入，想要存取檔案的該應用程式會從核心 (kernel) 呼叫 open() 原生函數以試圖存取（見圖 3 左方）。當 Skype 讀取一個使用者想要傳輸的檔案，或者當 Skype 在接收端試圖寫入檔案，Skype 用戶端程式會斟酌情況請求產生、開啓、讀取或寫入該檔案。

防毒工具利用的是所有檔案存取都是靠少數的核心原生函數，使用少數的幾種技術，包括填塞（shim）、包覆（wrap）、攔截（intercept ）所有存取核心功能的檔案呼叫，用哪種技術取決於使用的是哪種作業系統。

因此如果有使用者試圖用 Skype 傳送或接收檔案，防毒程式將偵測試圖讀取寫入檔案內容的動作，並拒絕 Skype 用戶端程式繼續進行寫入。

在圖 3 的右方，防毒程式將本身插入檔案存取鏈中，讓它有機會監控檔案內容，其中某些部份可能包含已知的病毒印記特徵。

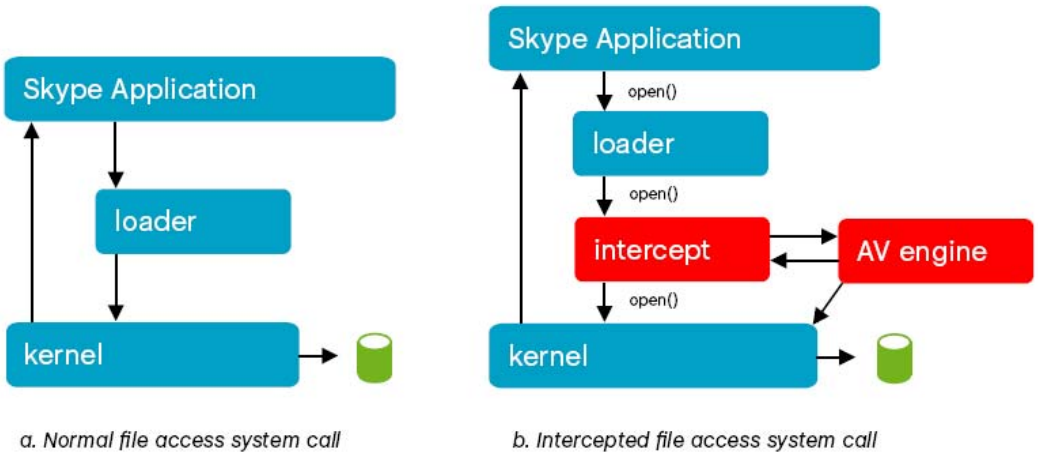

圖 3. 防毒程式對檔案傳輸的即時掃描

爲了將此過程圖示出來，我們從未防護的電腦送了一個符合業界標準的病毒掃描測試檔（名叫 EICAR 測試檔）給一個 Microsoft Windows XP 上的 Skype 使用者，用的防護程式則是一般店內販售的 Norton AntiVirus Professional。

雖然 Skype 用戶端程式可能允許檔案傳輸，但是該檔案馬上被 Norton AntiVirus 發現並刪除，使用者則會收到如圖 4 中 Norton 跳出的對話視窗的通知。

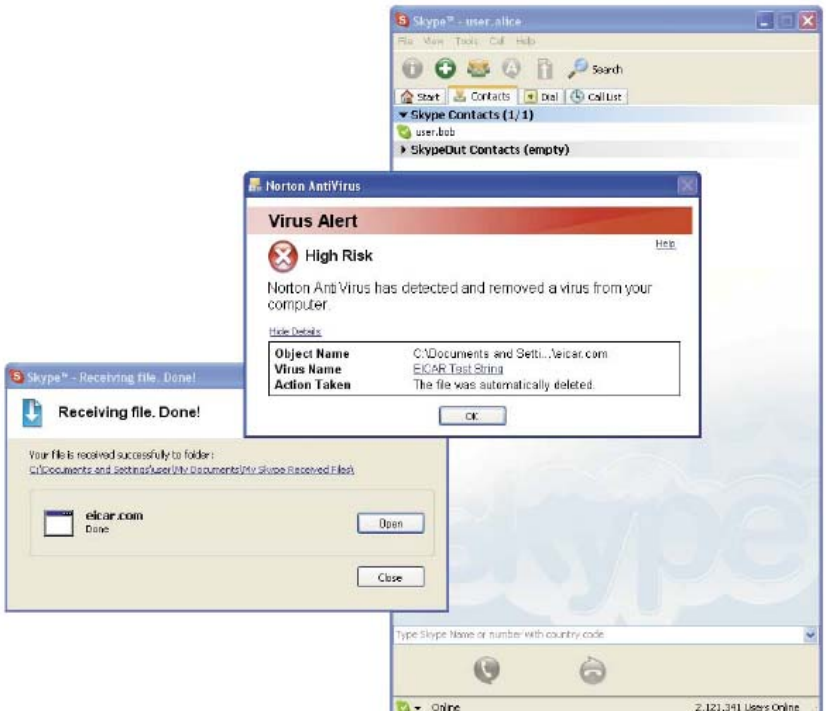

圖 4. Norton AntiVirus 阻擋了 EICAR 測試檔在 Skype 上的傳輸

爲了協助管理溝通並保護隱私，Skype 用戶端程式支援一些功能，讓使用者能控制有哪些人可以看到他們的上線狀態，有哪些人可以與他們接觸。在較早期的 Skype 版本中，此系統被稱爲*使用者授權 (分享聯絡人資訊)*。.

大體來說，分享聯絡人詳細資訊會讓某個 Skype 使用者將一個同意視窗傳給另一個使用者，以准許對方看到自己的上線狀態。並且分享聯絡人詳細資訊也透過解除對未經授權使用者的限制，允許對方可以自由使用各種功能（語音通話、文字訊息等）與自己溝通。對未經授權使用者有哪些限制，使用者可以在設定選項的隱私功能中自行設定。

每當 Skype 用戶將一個新 Skype 帳號加入自己的聯絡人名單，Skype 用戶端程式就會馬上出現提示，要使用者送出一個分享聯絡人詳細資訊的請求。如果對方接受了這個請求，則兩人就都可以看到對方的上線狀態。請看後面「分享聯絡人詳細資訊實例」一節，來了解整個過程步驟。

如果使用者拒絕或忽視此一請求，他的上線狀態資訊就不會被傳送請求來的人看到。

如果有使用者將一個 Skype 帳號加入自己的聯絡人名單中，但是請求未獲得許可，對方 Skype 帳號的 上線狀態資訊就不會顯示出來，此一使用者也不能享有與對方溝通的一切權利，這時他能擁有哪些權利是由對方在設定選項中的隱私部份決定的。

分享聯絡人資訊的請求與一個指定給該請求的數位簽章相關，一旦被簽章就會被送回給請求者。這與認證 Skype 身份使用相同的一個憑證。這種方法不是只設定一個旗標或位元在訊息中，所以幾乎不可能欺騙系統。

毫無疑問，分享聯絡人詳細資訊的能力對 Skype 維持本身隱私而言非常重要。控制哪些人能夠與使用者溝通也一樣重要。Skype 讓每個使用者都能設定自己的隱私門檻，包括誰可以跟自己用語音通話、誰可以傳送文字訊息給自己。

詳細來說，Skype 可以設定語音/視訊通話的選項，讓他們決定：

- 任何人都可以撥號給自己
- 只有在聯絡人名單上的人可以撥給自己
- 只有獲得自己授權的人才可以撥給自己

在即時文字訊息方面，他們可以決定：

- 任何人都可以傳即時訊息給自己
- 只有在聯絡人名單上的人可以傳即時訊息給自己
- 只有獲得自己授權的人才可以傳即時訊息給自己
- 檔案傳輸的選項，可以分別獨立在撥號與即時訊息中設定。

分享聯絡人詳細資訊實例

每當使用者將一個新帳號加入自己的聯絡人名單，就會自動產生分享聯絡人詳細資訊的請求。

舉例來說，有一個使用者鮑伯希望把愛麗絲加進他的聯絡人名單中。在這個案例中，鮑伯必須選擇工具 ->新增聯絡人，並打字輸入愛麗絲這個 Skype 使用者名稱，來將她加入使用者名單中。

這時鮑伯的電腦會立刻跳出一個視窗，裡面寫著「Say Hello…」，視窗中間有一個空白的文字輸入欄，鮑伯可以在裡面輸入文字告訴愛麗絲他是誰、爲甚麼他想要分

享聯絡人的詳細資訊。如果愛麗絲不知道鮑伯要邀請她加入，這樣的文字說明會特別有用。

鮑伯打完要輸入的文字並點選 [確定] 鍵之後，這個邀請會直接從鮑伯這裡送到愛麗絲那裡去。

因爲愛麗絲還沒有將自己的聯絡人詳細資訊分享給鮑伯，鮑伯這時還看不見愛麗絲的上線狀態。此外，如果愛麗絲在鮑伯送出請求的時候還沒有登入，此請求會在下一次鮑伯與愛麗絲都同時登入的時候送出。

最後愛麗絲會在一個特別的視窗中接到鮑伯的請求訊息，此一視窗上面會清楚標示出是在請求她分享出自己的個人詳細資訊。愛麗絲此時可以按照自己的意見決定怎麼處理。她可以接受請求，也可以加以拒絕。

如果愛麗絲決定接受鮑搏得請求，她就必須選擇「當我上線時讓這個使用者看見」，然後點擊「確定」。反過來說，如果她想拒絕鮑伯的請求，她就必須選擇「當我上線時不要讓這個使用者看見」。

不管選了哪一個，只要愛麗絲已經作出決定，她點選的答案就會馬上回傳到鮑伯那邊去。如果她接受了請求，鮑伯的 Skype 介面上馬上就可以看到愛麗絲的上線狀態。

在這裡，我們假定有一個愛麗絲不想接受的授權請求，是由使用者查理傳送給愛麗絲的。查理將愛麗絲加到自己的聯絡人名單之後，自動傳送出一個請求。但是愛麗絲此時決定不要將自己的聯絡人資訊開放給查理，也不想讓查理看到自己的上線狀態。

所以愛麗絲就拒絕了查理的請求。被拒絕的訊息會傳送到查理的用戶端程式，將請求結束掉，然而系統不會告知查理他已經被拒絕了。換句話說，從查理那一方看來，愛麗絲的上線狀態依然還是一個問號。

封鎖其他 Skype 使用者

爲了讓使用者有權決定誰能透過 Skype 跟他們聯絡，Skype 具有封鎖其他 Skype 使用者的功能，即使在聯絡人詳細資訊已經被分享出去也不例外。

選擇封鎖 Skype 使用者等於一次做了兩件事：首先這會讓被封鎖者無法再跟封鎖者利用 Skype 聯絡，此外被封鎖者從此會看不見封鎖者的上線狀態。

如果使用者解除另一個使用者的封鎖，他們需要再次分享聯絡人詳細資訊嗎？不用，只要答應過一次分享資訊的請求，這個狀態就無法再收回。然而透過封鎖一樣可以杜絕對方能存取自己詳細資訊的權利。

Skype 用戶端程式讓使用者可以透過隱私設定來建立並管理封鎖的使用者名單，也可以點選某一使用者功能選單中的封鎖此用戶選項。一旦某個 Skype 帳號被加入到此一名單中，到此帳號被從名單中移除爲止，這個被封鎖的使用者就無法看到自己的上線狀態，也不能用 Skype 與自己聯絡。

對已封鎖的使用者隨時都可以解除封鎖，只要將此使用者從封鎖名單中移除即可。

防止垃圾郵件與垃圾語音

垃圾郵件是現今網路的大患。不請自來的廣告電子郵件，是大家在使用郵件系統進行溝通時最不喜歡的東西，但現實的狀況就是每個人每天都收到爲數甚多的垃圾郵件。Skype 採取了一些措施以防止 Skype 成爲利用網路電話濫發垃圾廣告的工具。

使用者如果能夠只授權給自己確定身份的人，就可以扮演主動反擊這些垃圾廣告的角色。使用者可以將個人的隱私設定改成「只讓使用者授權過的人可以跟自己用 Skype 溝通」。這樣一來，就只有您認識的人可以打電話撥給自己了。使用者也可以在他們的個人資料中要求：可能打電話給他們的人在撥電話之前先傳個訊息過來。

此外，Skype 不會將電子郵件資訊洩漏給可能利用 Skype 線上電話簿來尋找潛在廣告對象的人。雖然使用者可能將自己的電子郵件地址寫在他們的 Skype 個人資訊中，但是電子郵件地址其他人看不到。

注意： 使用者在 Skype 個人資訊中輸入的有效電子郵件地址，會作爲忘記密碼之後取回之用，也可以讓其他使用者在新增聯絡人的時候當作搜尋條件。如果你需要進一步的資訊，請參考下方的「Skype將資料儲存在何處」，就可了解 Skype 如何處理使用者的電子郵件資訊。

在利用電子郵件或網站進行溝通時，Skype 使用者必須清楚認知到他們在利用 Skype 進行溝通時，務必要小心不讓自己的個人資訊流出去。

如同前面所述，Skype 的安全模型可以確保任何人都沒辦法僞造另一個人的身份證明，也無法輕易假扮成他人。但是在電子郵件系統中，防止帳號密碼被他人取得是每一個 Skype 使用者本身的責任，特別是當別人有權分享使用同一台電腦時更是如此。如果自己的帳號遭到濫用，請回報到以下電子郵件位址：abuse@skype.net.

如何防止密碼詐騙（釣魚）

Skype 在任何情況下都不會要求使用者用電子郵件傳送他們的密碼。

就像使用其他網路電子商務時一樣，Skype 使用者也會收到詐騙的電子郵件，或是遇上非 Skype 公司官方設計，但故意做成像是 Skype 公司官方製作的電子郵件或網頁，欺騙使用者讓他們自行交出本身的帳號與密碼。這種詐騙取得使用者機密資料的方式一般被稱爲「釣魚」，近來已經快速成爲網路使用者資訊安全的頭號威脅。

所以，在此我們特別提醒使用者，他們會用到 Skype 密碼的時機只有在登入 Skype 用戶端程式、進入 https://secure.skype.com/store/member/login.html網頁進行帳號管理時，或是進入其他官方提供需要 Skype 帳號的網頁，例如https://developer.skype.com 以及 https://skypecasts.skype.com之時。

若某位 Skype 使用者認爲自己已經成爲釣魚的受害者，他應該立刻變更自己的密碼，並且將自己受害的情形用電子郵件報告給abuse@skype.net。IT 管理人員透過將這類詐騙的細節（包括釣魚陷阱的電子郵件位址或網站位址）告知各員工，就可以對減少這樣的問題有很大幫助。

Skype 將資料儲存在何處?

Skype 將使用者資訊存放在以下這些地方：Skype 中央認證伺服器、Skype 帳號與交易伺服器、Skype 事件伺服器、網際網路上 Skype P2P 網路系統內的全球索引、Skype 使用者本身的電腦，以及其他 Skype 使用者的電腦。

- Skype 使用者的電腦中存放了已安裝的 Skype 用戶端程式、以往安裝 Skype 殘留下、但還沒刪除的檔案、Windows 系統登錄值、個人詳細資訊（包含電子郵件信箱）、傳送的語音信件訊息檔、通話紀錄、文字訊息聊天紀錄、一組設定檔（其中可能包括某個使用者其聯絡人名單上的各個帳號）。除非使用者刻意刪除，不然訊息聊天的紀錄檔會無限制地儲存在使用者主目錄下的一個隱藏目錄中。Skype 用戶端程式可以設定自動刪除或設定保存期限。

重要訊息: 有可能在其他使用者的電腦中找到某個 Skype 使用者的追蹤資訊（trace bits）。這類資訊當中可能會包含尚未發出或接收的語音郵件訊息、尚未被傳送的即時訊息，以及文字訊息聊天紀錄檔。

- Skype 的中央授權伺服器儲存了所有有效的 Skype 使用者資訊。這個資料庫不會接受任何非 Skype 來源的查詢請求。這裡儲存了 Skype 帳號、使用者當初申請時填入的一組電子郵件位址，以及每個使用者的密碼，此密碼是用單向加密雜湊的方式儲存的。

Skype 會在兩個地方儲存使用者的電子郵件位址，其中之一是在使用者自己電腦的使用者資訊裡。另外一份是在 Skype 網站的「我的帳號」裡面，這主要是用來讓使用者忘記密碼時可以取回。所以如果要改變登錄的電子郵件信箱，使用者必須同時在自己的用戶端程式個人資料以及 Skype 網站上進行修改。.

- Skype 的帳號/交易伺服器會抓取 Skype 通話的相關統計，以及訂購與交易資料，以供 Skype 服務營運之用。Skype 對 Skype 的流量資料只供集體統計使用。Skype 公司不會去追蹤某個使用者利用 Skype 網路跟哪些人溝通過，也不會去追蹤使用者互動的時間。但是爲了管理相關業務，本公司會收集並處理關於 SkypeIn 與 SkypeOut 的通話資訊。如果使用者有將 Skype 點數 (金錢) 存入 SkypeOut 帳戶，伺服器會收集他們通話的資訊，以計算他們帳戶內的餘額。關於公司如何運用此項資料，請參考 Skype 的服務條款，該條款可以在 Skype 官方網站上找到。

- Skype 事件伺服器是一個資料庫，Skype 會用來暫時存放某些型態的資訊，直到該資訊以不再需要；換句話說，是用來確定資訊傳遞的信賴度。大體來說，Skype 公司不會保留上面的資訊。

- 全球索引存放的是每個使用者電腦最新的網路位址、每個 Skype 用戶端程式的超級節點，以及每個使用者最新的 Skype 使用者個人資訊。所有公開目錄中的個人資訊都有數位簽章。

檔案、資料夾與應用資料的位置

執行此一程序時：	會創造以下目錄、檔案或者系統登錄資料：
Skype 安裝程式 (SkypeSetup.exe)	1. 如果安裝的帳號擁有電腦管理者的權限，Skype 的程式會寫進%programfiles%目錄當中，通常會是C:\Program Files\Skype\Phone\ 2. 如果安裝的帳號只具有有限的權限，Skype 程式會寫入%homedrive%:\%homepath%目錄中，通常是C:\Documents and Settings\<username>\Application Data\Skype\ 3. 有幾個資料夾的名稱是以 "My Skype" 開頭的，例如My Skype Pictures (裡面放的是Skype應用程式常用的圖示)將會在%allusersprofile% directory中創建，通常是在 C:\Documents and Settings\All Users\Documents\My Skype Pictures\. 4. 使用者的 %temp% 目錄中將會創建一個暫時性的資料夾，用來在安裝的過程中存放一些執行資料。當安裝完成之後，這個目錄及其中的內容都會被刪除。 5. 有幾個預設的檔案位置會被永久存放在Windows系統登錄中，在這個登錄鍵值之下：HKLM\SOFTWARE\Skype 6. 在Skype將本身的安裝登錄進平台之後，其他一些登錄鍵值會被其他的Windows子系統創建出來，例如： - 對callto:// URL 處理器的登錄 - 獲取Windows防火牆對朝內連線的許可
Skype 應用程式(用戶端)	1. 會爲了使用者個人建立一個 Skype 資料夾，用來存放個人的資訊。此資料夾通常爲C:\Documents and Settings\<username>\Documents\Skype\. 2. 一個叫做My Skype Pictures的資料夾會被創建在該使用者的 Skype 資料夾中，通常是C:\Documents and Settings\<username>\Documents\My Skype Pictures\. 這個資料夾存放了個人可能創建或用到的，但並不是每個該平台上的使用者都會用到的圖示。 3. 如果在安裝過程中尚未創建，一個叫做 Skype 的資料夾會被創建在使用者的應用資料目錄中。此目錄存放使用者在對話過程中暫時的資訊。此目錄通常爲 C:\Documents and Settings\<username>\Local Settings\Application Data\Skype\.

密碼

如同前面所討論過的，Skype 公司官方在任何情形下都絕不會用電子郵件要求使用者交出自己的 Skype 帳號或密碼。

Skype 密碼是用單向加密雜湊的方式儲存，必須完全保密。

以現在來說，會用到 Skype 密碼的地方只有：

- 登入 Skype 用戶端程式本身的時候
- 在https://secure.skype.com/store/member/login.html,網頁進行使用者帳號管理的時候
- 登入其他確認沒問題的官方網頁，例如https://developer.skype.com 以及 https://skypecasts.skype.com之時。

如果使用者想要建立新的密碼，只要註冊時有提供過電子郵件位址，該郵電位址仍能使用，他們可以直接到 Skype 官網的帳號網頁去輸入新密碼。

重要資訊： Skype 會在兩個地方儲存使用者的電子郵件位址，其中之一是在使用者自己電腦的使用者資訊裡。另外一份是在 Skype 網站的「我的帳號」裡面，這主要是用來讓使用者忘記密碼時可以取回。所以如果要改變登錄的電子郵件信箱，使用者必須同時在自己的用戶端程式個人資料以及 Skype 網站上進行修改。.

廣告軟體與間諜軟體

Skype 用戶端程式與 Skype 安裝程式都不包含廣告軟體或間諜軟體。

然而網路上有可能出現偽裝成官方版本的安裝程式，在未經許可的情形下不當地將 Skype 用戶端程式與其他軟體相結合，其中很可能含廣告軟體與間諜軟體。

所以我們強烈建議您在 Skype 官方網站或是正式合作夥伴的網站下載Skype的最新版本，台灣的用戶請到 http://skype.pchome.com.tw/download.jsp 下載。

此外，在 Microsoft Windows XP、Windows 2000 以及 Windows Pocket PC 2003 等環境下使用的安裝程式，以及 Skype 應用程式本身都具有數位簽章。

這讓您在安裝 Skype 用戶端程式到任何系統前都能夠對安裝程式的數位簽章進行驗證動作，這可以防止您在安裝 Skype 到網路的同時也安裝了間諜程式或惡意程式。

在此特別補充一點，即使技術上您可以在安裝 Skype 之後再進行驗證，我們建議您還是在安裝 Skype 用戶端程式之前就進行授權驗證較佳。

關於進行數位簽章驗證的詳細解釋，請參考本文件下一章節「在企業中安裝運用 Skype」。

Skype 的安全評估

Skype.com 包含了給網路管理者的資源，以及更多 Skype 安全的細節資訊。請到 www.skype.com/security 去參考特定主題的安全相關資訊，包括 Skype 安全留言板、聯絡用電子郵件，以及驗證數位簽章用的 PGP key。

此連結也包含了 Anagram Laboratories 實驗室的 Tom Berson 所編寫的 Skype 安全性評估報告。這分報告內容包括：

- 對於 Skype 加入各項產品中的安全框架進行深度審視
- 對於 Skype 基礎架構中使用的各種保護機制進行描述
- 在 Skype 的日常運作框架中作爲一切安全性基礎的一般政策原則

Skype 安全的常見問題（FAQ）

越來越多公司利用 Skype，以更有效益的方式進行客戶支援，包括：

- 讓顧客可以透過 Skype 用戶端程式直接與公司的客服中心聯絡。
- 使用 Skype 的語音轉接功能
- 將電話轉到公司客服中心交換器在公共電話網路上的號碼

Skype 原本是設計給消費者運用在個人溝通上面，然而當企業開始在重要的營運項目中開始使用 Skype 之後，自然而然會產生與顧客溝通安全相關的問題。

以下是其中一部分的問題以及具代表性的回答：

「打洞（Hole Punching）」對安全有威脅嗎？

沒有。對於許多 VoIP 的解決方案來說，一個大困難就是沒辦法傳遞過網路的邊界。 在使用網路位址轉譯 (NAT) 設備時，或者在網路邊緣架設防火牆時，這類問題就會發生在網路的邊界上。

爲了讓使用者擁有最大的彈性，Skype 在軟體中使用一組最強的 NAT 穿越技術，讓 Skype 在傳統 VoIP 電話無法接通時仍暢行無阻。

在今日的家庭或辦公室網路中，使用網路位址轉譯是非常普遍的，這讓管理網路更加容易，不需要讓每個網路都必須取得稀少的網路位址資源。

要讓兩台在私人網路上（亦即在 NAT 設備後面）的電腦運用 P2P 的方式溝通，要用到一種叫做「打洞」的技術。這種技術常被使用 UDP 封包進行溝通的應用軟體所運用，也能被用來建立更可靠的 TCP 協定連線。

雖然「打洞」這個名詞聽來可怕，但是這個技術並不會影響私人網路的安全性，反而是在大部分 NAT 的原則架構下進行溝通。這些技術會在溝通路徑上發信號給 NAT 設備，請求讓 P2P 連線通過。

Skype 通話有多安全?

有人可以截取竊聽顧客的電話嗎？不可能。

Skype 的安全性與其架構完全整合。所有語音通話、文字傳輸的即時訊息、視訊通話以及檔案傳輸在從 Skype 網路的一端傳輸到另一端的過程都經過加密，以保障隱密性。

雖然 Skype 無法保證完全的匿名性或秘密性，但是它提供了領先業界的傳輸層安全性，讓傳輸通過 Skype 網路的訊息內容不會被竊聽或中途截取。

爲了達成這項目標，Skype 使用公開與私密金鑰系統，讓溝通的內容能夠保密。此系統包含所有用來控制 Skype 網路的信號，以及所有溝通內容之中，包括與語音、視訊、文字與資料。所有內容經過加密，代表不可能知道有哪些資訊正通過 Skype 網路的節點、超級節點或中繼主機。

Skype 的網路傳輸在傳送過程中不可能被擷取或解密。Skype 背後的加密模型同時使用公開金鑰以及對稱金鑰，包含 AES 演算法，使用在 256 位元整數計數器模式下。Skype 也使用 1024 位元 RSA 去協商對稱的 AES 金鑰。使用者的公開金鑰經過 Skype 伺服器驗證，使用的是 1536 或 2048 位元的 RSA 憑證。

任何 Skype 使用者之間的溝通都在同時用一種叫做多路傳輸的技術，透過單獨的 session 連線傳送。不管是語音通話、文字訊息或任何 Skype 的溝通內容，傳送時都具有相同等級的安全性。

雖然 Skype 的確提供了隱密的溝通管道，然而網路管理者還是必須記得，Skype 是在大眾使用的作業系統上執行。這代表 Skype 所能提供給用戶的安全或隱私等級會受到該作業系統所能提供的安全等級影響，不管這些系統是 Microsoft Windows、Mac OS X、 Pocket PC、 Linux 或其他任何作業系統都一樣。

因此 Skype 不能算是提供了百分之百絕對安全的溝通平台，也不是安全的檔案存放解決方案。Skype 相關的資料、傳輸與檔案，其安全性頂多跟 Skype 在其上執行的電腦相同。

換句話說，資料在 Skype 網路上傳輸的過程中是不可能被截取或解密的，然而解密後的影音流、聲音影像或文字檔都有可能暴露在惡意攻擊下，其安全性與該使用者電腦實際的安全性相同。

一旦文字訊息、傳輸的檔案、影音流已被對方接收，Skype 用戶端程式就無法防止這些資料不被複製、儲存或重新散佈。

這就是我們的底線：Skype 程式能夠保證在傳輸中的資料安全，無論此是在兩個 Skype 用戶端之間直接傳輸，或者是透過其他的電腦，都一樣安全。

所有資料在傳輸前與接收後的安全，都必須由使用者自行負責，就像在使用電子郵件或郵件附件檔時一樣。

轉接到一般電話網的通話比較不安全嗎？這個問題的答案既可說是，也可說不是。

在 Skype 的網路中，所有語音通話、文字即時訊息、視訊通話以及檔案傳輸都從一端加密直到傳輸到另一端，以保障隱私。然而當 Skype 語音離開了 Skype 網路，這個加密就會被解開：

- 當 Skype 通話語音離開了 Skype 網路，透過終端提供者（termination provider）進入傳統的電話網路時，該通話就被解密，並且利用一般電話的傳輸方式，在一般電話的網路上傳輸。所以這些電話就可能被先進科技所擷取，不管對方是拿到法律的許可還是竊聽。
- 同樣地，當 Skype 語音通話離開了 Skype 網路，透過 SIP (Session Initiation Protocol) 閘道器進入了某個電話客服中心，Skype 通話已經不在 Skype 管轄之下，從那一

刻起就已經被解密。

所以假定有某個客戶或帳戶持有人利用 Skype 與公司聯絡，通話被轉到該公司客服中心交換機的一般電話號碼上，您就必須將該通從 Skype 撥出的通話視爲與一般電話安全性相同。

然而我們還是必須提醒一件事。如同前面所說，IT 管理者必須考慮到 Skype 是在大眾使用的作業系統上執行。這代表 Skype 所能提供給用戶的安全或隱私等級會受到該做業系統所能提供的安全等級影響。

在這種情況下，即使 Skype 的網路傳輸不會受到截取，也不會在傳送過程中被解密，然而語音信箱的語音檔訊息、文字檔案與文字訊息交談紀錄還是有可能因爲使用者電腦或檔案系統的弱點而洩漏出去，這主要是取決於使用者電腦與網路的安全等級。

Skype 用戶是否暴露在木馬程式與其他的威脅之下？

很明顯地，惡意的程式碼例如木馬程式、惡意軟體、廣告軟體與間諜軟體在 IT 管理與安全人員的防護清單上還是很重要。對於終端使用者是不是容易暴露在這樣的威脅之下，我們從兩方面來回答。

駭客是否能用 Skype 傳送木馬程式進 IVR 系統？不可能。

Skype 讓使用者傳送並接收檔案的功能（這些檔案有可能包含惡意的程式）允許使用者可以將檔案傳給一個或多個其他的使用者。

這些檔案不可能暗中透過 Skype 近乎即時的聲音或影像流傳送，所以不需要擔心駭客將特洛伊木馬病毒或者其他檔案偷偷傳到公司的 IVR 或使用者的電腦中。

關於如何使用群組原則物件以及系統登錄鍵關閉此一功能，請參考「全公司安裝與設定原則」一節。

使用者有可能收到木馬程式嗎？答案可以說是，也可以說不是。這就像是收到電子郵件的附件檔一樣。

在某個 Skype 使用者從另一個使用者那裡接收檔案之前，接收者必須安裝最新的防毒程式，並且設定好掃描所有傳給自己的檔案，即使檔案是他們的熟人傳來的也一樣。

Skype 的檔案傳輸功能是給使用者便利安全的方式與 Skype 網路上的其他人分享照片、文件以及其他電子檔。不幸的是，在電腦世界中任何新的資料分享能力無可避免地都會有收到惡意程式的風險，包括病毒、特洛伊木馬與間諜程式。

幸好 Skype 檔案傳輸功能只能在 Skype 用戶端程式間進行。 Skype 用戶端程式讓使用者在傳輸檔案之前必須先請求許可，許可之後才會進行傳輸。換句話說，必須要發的人跟收的人雙方都明確同意，檔案傳輸才有可能發生。

因此，就像使用者在開啓電子郵件附件以及從網站上下載檔案時必須小心一樣，如果他們在接受檔案傳輸之前有經過考慮，就能減少他們電腦被感染的機率，特別是能夠阻絕從他們不認識的人那裡收到檔案。

更詳細的資訊請參考本文件上方「安全與檔案傳輸」部份。

在企業中部署 Skype

先做最重要的事

我們的目標是要讓使用者在各種網路上都可以盡情享用 Skype 的各種功能，而不需要事先了解各種複雜的設定，例如轉遞（relay hosts）或者優先的網路埠（network ports）在這些情況下，Skype 基本上是採取不干涉的原則。

最新版本的官方 Skype 程式隨時都可以從 Skype 的下載伺服器取得，網址在 http://skype.pchome.com.tw/download.jsp。我們建議您可以直接從我們的伺服器取得程式，然而其實也有一些其他組織也被允許存放Skype應用程式，條件是他們必須遵守與轉發Skye軟體相關的Skype終端使用者授權協定 (EULA)。

只要安裝之後，Skype 用戶端程式就會定期檢查，看看是否 有更新的版本，但系統與網路管理者可以關閉此一功能。終端使用者也可以調整他們的 Skype 設定，以控制程式的新版本與修補程式的安裝。

整體指導原則

Skype Technologies S.A. 公司希望終端使用者與企業都能擁有安全愉快的 Skype 溝通經驗。爲達此一目的，我們必須強調在使用 Skype 時維持公司電腦與使用者的安全與機密性。

我們已經將維持電腦安全的原則張貼在主網頁上，位置在 http://www.skype.com/intl/zh-Hant/security。此外，我們在此希望特別強調其中的一些重點：

- 在您爲自己所屬的組織安裝 Skype 或轉發給其他人安裝之時，請確定您手上的是官方的版本。請檢查安裝程式的數位簽名，且務必遵守 Skype 服務條款關於轉發 Skype 軟體的限制。
- 請幫您所屬組織的電腦持續更新相關的修補程式。在今天，大部分電腦的網路安全問題都源自於沒有進行適當的修補更新。
- 雖然是老生常談，請務必使用防毒的程式，即使在非微軟作業系統的電腦上，例如在蘋果的麥金塔上，也是如此。並請記得時常更新病毒定義檔。
- 當您使用 Skype 時，請記得您讓哪些人加入您的名單，如果發現有人做些您不喜歡的事情，請毫不猶豫地將此人封鎖。請時常更新您的個人資訊，但也請記得您寫在上面的東西如果跟別人搜尋帳號的條件相符合，那麼這些人就可以看到您寫的資訊（除了電子郵件帳號之外，此一項目不會公開）。
- 在討論任何機密事務或敏感的個人資訊前，記得先驗證對方的真實身份。即使 Skype 已經用各種設計防止您在溝通時將不想洩漏的資訊洩漏出去，您的電腦或是您溝通對象的電腦還是有些許可能已經被駭客入侵，或因爲某些原因可能洩密。

- 請教育您的使用者選擇正確的 Skype 密碼，並且時常變更。使用者在公用的電腦上面絕對不可以勾選「記憶密碼」的選項。

如何確定您的網路環境適合使用 Skype？

大體來說，大部分的防火牆、路由器與 NAT 設備都能跟 Skype 相容。這些設備的出廠原始設定通常都能適當地處理 UDP 資料傳輸。

您只要使用稱爲 NAT Check 的免費軟體（Bryan Ford 製作），就可確定您的網路相容於 Skype。NAT Check 可以測出網路中的 UDP 資料傳輸是否被合宜地處理；換句話說，可以測出 UDP translation 是否與 Skype 之類的 P2P 通訊協定相容。您可以在 http://midcom-p2p.sourceforge.net/下載 NAT Check 這套軟體。

請確定您網路的 UDP 轉譯（UDP translation）能顯示出前後一致的轉譯內容。也請確定輸入輸出的通信埠是相同的 (除非在 loopback 轉譯衝突的情況下)。 此外，請確定被送進網路不請自來的 UDP 封包會被過濾或丟棄掉。最後，但也是很重要的一點是，Skype 希望您網路的防火牆或者 NAT 閘道器能夠支援 IP 封包分割與重組。但是這並不是百分之百必要的。

然而 Skype 絕對要求您的防火牆不去封鎖 UDP 封包的並行傳送試圖，或者對目的位址進行多通訊埠的 TCP 連線。理由是什麼呢？因爲有些防火牆會錯誤地將這個動作視爲是在掃描通訊埠，最後就會封鎖住該主機。這不但會回頭影響到 Skype，也會影響在同一主機電腦上執行的其他網路應用程式。

驗證 Windows 版本的 Skype 安裝程式

爲了確保您安裝的是最新版Skype，您可以直接到Skype的網站進行下載，網址是 www.skype.com/download。台灣的用戶建議您前往 PChome-Skype 的網站下載軟體，網址是 http://skype.pchome.com.tw/download.jsp

您也可以從其他組織的網頁取得 Skype，這是因爲 Skype 公司官方允許其他網頁存放用戶端程式的下載版本，只要該組織嚴格遵守 Skype 終端使用者授權協議(EULA)即可。

注意： 根據Skype服務條款以及EULA，其他組織不能重新包裝或將Skype應用程式包裹在其他軟體中。

在 Microsoft Windows XP、Windows 2000 以及 Windows Pocket PC 2003 下的 Skype 安裝程式，以及應用程式本身都具有數位簽章。所以如果要保證您擁有的是官方可靠版本的 Skype 程式，並避免安裝到任何惡意或間諜程式，您應該在安裝前先驗證 Skype 安裝程式的數位簽章。

您也可以在執行 Skype 安裝程式之後才對 Skype 執行檔進行數位簽章的驗證測試，但在安裝與執行 Skype 之前進行認證會是最好的方式。

以rpm格式包裝之Linux用Skype軟件是利用Skype的signing key進行簽章，您可以在以下網址進行下載：www.skype.com/products/skype/linux.

要驗證 Microsoft Windows 下的安裝程式是否爲官方版本，請按下列步驟實行：

1. 找到 Skype 安裝程式的位置。如果必要的話，請打開 Windows 檔案管理員去找到 Skype 安裝程式。

2. 以滑鼠右鍵點擊 Skype 的安裝程式，從跳出的選單中選擇「內容」選項，之後該程式內容的對話視窗就會顯示在畫面上。

3. 視窗上方的其中一個標籤頁應該是「數位簽章」。如果您沒看到這個標籤，請停下所有動作，跳到後面看本文件的下一節「數位簽章的問題」。如果您有看到這個數位簽章標籤頁，請進到下一個第 4 步驟。

4. 在內容視窗中，會顯示出一張此安裝程式已生效的數位簽章清單。在上面您應該只能看到一個簽署者：Skype Technologies SA。請您用滑鼠左鍵雙擊 Skype Technologies SA 那一行，接下來應該會顯示出一個視窗，裡面包含了 Skype 數位簽章的各項細節。

5. 請再次確認跳出的視窗中的數位簽章詳細資料，證實該數位簽章已確認。如果這個視窗裡寫著數位簽章未經確認，請您停下安裝動作，因爲這代表數位簽章是有問題的，請您直接跳到下一節「數位簽章的問題」部份。如果數位簽章沒問題，請您進到下一個第 6 步驟。

6.之後請您點擊「檢視憑證」按鈕，以顯示用來在安裝程式上加上簽章的數位憑證細節。點擊後跳出的視窗應該包含如下字樣：

發給： Skype Technologies SA

發行者： VeriSign Class 3 Code Signing 2001 CA

如果跳出視窗中的文字跟以上有所不合(除了 2001 年的部份以外，該部份每 12 個月就會變更一次) ，請您停下安裝動作，因爲這代表數位簽章是有問題的，請您直接跳到下一節「數位簽章的問題」部份。如果沒問題，請您進到下一個第 7 步驟。

7. 請點選「詳細資料」標籤，以檢視簽署憑證的序號。您可以驗證該序號是否正確，該序號可以在以下網址找到：www.skype.com/security.

如果 Skype 安裝程式的憑證序號跟您在 Skype 網站上看到的不同，，請您停下安裝動作，因爲這代表數位簽章是有問題的，請您直接跳到下一節「數位簽章的問題」部份。

9. 如果您到此時爲止都沒發現任何問題，您就可以安裝 Skype 用戶端程式，因爲它是安全的。

數位簽章的問題

在幾種情形下，下載檔案可能出現無效的數位簽章。

第一種可能，是安裝程式在下載的過程中意外損壞了。也有可能是該程式在未經官方許可的情況下被他人拿來結合其他的軟體。甚至有可能在裡面結合了間諜程式、廣告程式、惡意破壞的程式，這直接違反了 Skype 的終端使用者授權條款。

如果你發現到 Skype 數位簽名的問題，請務必進行以下動作：

- 不要執行未通過認證的 Skype 安裝程式。
- 請將問題回報給 Skype 安全團隊，電子郵件信箱在 security@skype.net。請提供詳細的問題細節，例如您是在哪裡取得此一 Skype 安裝程式。
- 直接從 Skype 官方網站下載最新版本的 Skype 安裝程式，並且在安裝前執行上節所描述的數位簽章驗證確認動作。

Skype 用戶端程式的新版本與更新通知

一旦您安裝了 Skype 應用程式，其預設設定就是定期檢查是否有新版本的 Skype 程式。Skype 用戶端程式並不會自動更新，而是只會在新版本或重要修補程式推出時進行告知。這等於給予使用者選擇是否更新的權力。

使用者可以選擇不理會這些更新通知。系統與網路管理者也可以關閉此一功能，來控制組織中的程式安裝政策。請參見以下「全公司安裝與設定政策」一節。

終端使用者可透過自行設定 Skype 選項控制此一自動更新通知功能。(請選擇功能 > 設定選項 > 更新)。

除此之外，使用者亦可手動檢查目前執行的 Skype 是否爲最新版本。有兩種辦法可以完成這件事：

- 使用者可以從 Skype 主介面視窗上選擇說明>查詢更新版本。若已有新版本，這麼做之後將開啓使用者預設的網路瀏覽器，並會顯示訊息，指示使用者如何安裝最新版本。或者
- 也可以不需要開啓 Skype 用戶端程式本身，而直接打開 Windows 控制台，雙擊「新增或移除程式」。之後使用者可以找到 Skype 項目，點選「按這裡取得支援資訊」。其中一個超連結「產品更新」點擊之後將會打開預設的網路瀏覽器，並且會指示如何安裝最新的版本。

全企業安裝與設定原則

Skype 體認到企業或其他組織在管理複雜 IT 環境時所遇上的挑戰，以及管理今日所用繁多且各不相同的軟硬體時遭遇的各項麻煩。

因此，我們現在支援利用群組原則物件 （Group Policy Objects） 以及系統設定值（Registry keys）來設定整體的原則，很快也會推出 MSI 包裝的安裝功能。

我們的目標是讓系統與網路管理者能夠透過整個企業的 Skype 佈署與管理，讓控制全公司的 Skype 更加輕鬆。

原則

Skype 用戶端程式堅持用以下順序排定設定的優先權：

1. HKLM 登錄鍵值 (優先度最高)
2. HKCU 登錄鍵值
3. 共享的與個人的 xml Skype 用戶端程式設定
4. Skype 用戶端程式使用者個人設定與預設值 (優先度最低)

Windows 系統登錄

Skype 用戶端程式能夠讓終端使用者控制介面，也提供許多企業想要控制的功能。其中有一些較爲技術性、與網路較爲相關的選項只能從系統登錄裡面修改。

這樣做的原因是因爲企業中想要使用這些功能的人通常都能集中管理使用者的系統登錄檔，並且也有權限控管讓不該修改的人沒辦法進行修改。

XML 設定檔

在 Windows 系統登錄之外，Skype 用戶端程式也依賴以 XML 檔案爲基礎的安裝設定。系統管理者(或者擁有適當權限的使用者)都能在 Skype 執行中開啓或編輯這些設定檔。

XML 設定檔共有兩個 - 共享的與個人的。共享檔案的檔名是 shared.xml，個人檔案的檔名是 config.xml。請記得 XML 檔案的檔名有分大小寫，所以 "Debug"與"debug" 是不同的。

關於這些 XML 設定檔的位置，請參考上方“檔案、資料夾與 Windows 系統登錄鍵值 ” 部份。

注意： 編輯的內容必須合乎XML語法與格式(例如必須有開始與結束標籤)，否則您作的變更不會生效，如果Skype並沒有在執行，您的新設定也可能就此不見。

設定群組原則

在新的 3.0 版本中，Skype 已經支援群組原則的使用，讓您在 Windows Active Directory 環境下可以將所需的原則設定輕易套用在一整組企業使用者或電腦之上。

群組原則的使用者讓系統與網路管理者能用最方便可靠的方式集中管理全公司的 Skype 用戶端程式原則設定。

Skype 原則設定能夠套用在一整組預先安排好的使用者或電腦上，管理其 Skype 用戶端程式的行爲。Skype 的群組原則功能已開啓，這代表 Skype 用戶端程式的行爲是透過系統管理範本（Administrative Template）檔案（.adm 檔）中的系統登錄值決定並修改的。如此您就能透過以系統登錄爲原則管理 Skype 的設定與功能。

Skype 公司官方將相關的原則設定寫在單一的系統管理範本檔案中，檔名爲 Skype-v1.5.adm，這分文件是設計來修改系統登錄檔中特定的鍵值，詳細情形會在下一節進行說明。

注意：您可以從Skype官方網站的安全相關頁面下載 Skype-v1.5.adm檔案，位址在Skype.com/security，並使用Group Policy Editor來調整Skype的原則設定。

以系統登錄進行的原則設定可以在 Group Policy Object Editor 中進行檢視與調整，，此一編輯器是在 Administrative Templates 節點（node）之下。

Skype-v1.5.adm 檔案並不會直接套用在原則設定上。反之它只是讓您能看到 Group Policy Object Editor 中的原則設定。您可以從那裡創建群組原則物件（Group Policy objects，GPOs），其中包含了您想要的原則設定。

關於如何使用群組原則，如果您需要更多資訊，請參考以下網頁：

- **將群組原則視爲 MMC snap-in 進行開啓**
  http://technet2.microsoft.com/WindowsServer/en/library/ae13960b-3a27-4b19-a866-ed6e6e7a312d1033.mspx?mfr=true

- **在以系統登錄爲基礎的群組原則中使用系統管理範本檔案**
  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/management/gp/admtgp.mspx (請看 "Loading an .Adm File into the Group Policy Snap-in"（將.Adm檔案載入群組原則snap-in中）的部份」

可調整的原則

以下是 Skype 3.0 beta 版用戶端程式可調整的清群組原則清單：

Skype 用戶端程式功能	
DisableFileTransferPolicy	關閉檔案傳輸功能，讓使用者無法透過 Skype 傳送或接收檔案。
DisableContactImportPolicy	關閉匯入聯絡人名單功能。
DisablePersonalisePolicy	關閉個人設定功能，防止使用者改變聲音設定。
DisableLanguageEditPolicy	關閉語言編輯功能，防止使用者編輯語言字串。
WebStatusPolicy	當開啓時，這會將使用者狀態以 Skype 按鈕的形式發佈在網頁上；當關閉時，會防止將使用者狀態發佈在網頁上。

Skype 非功能性選項	
DisableApiPolicy	關閉 Skype Public API，以防止其他組織的應用程式使用 Skype 的功能。
DisableVersionCheckPolicy	關閉檢查新版本功能，防止 Skype 去檢查新版本或更新。
MemoryOnlyPolicy	以只使用記憶體的模式執行，這樣 Skype 就不會將任何資料存放在該電腦的硬碟中。
網路相關功能	
ListenPortPolicy	設定監聽通訊埠（listen port），之後 Skype 會監聽接入的連線。
ListenPort	監聽某一通訊埠。
ListenHTTPPortsPolicy	開啓時會監聽 HTTP (port 80) 與 HTTPS (port 443) 通訊埠；關閉時不會監聽 HTTP/HTTPS ports；未設定時，由使用者自行決定。
DisableTCPListenPolicy	關閉監聽 TCP 連線，以防止 Skype 用戶端程式接收進來的 TCP 連線。
DisableUDPPolicy	關閉 UDP 溝通，以防止 Skype 用戶端程式使用 UDP 與網路溝通。
DisableSupernodePolicy	防止 Skype 用戶端成爲超級節點（supernode）
ProxyPolicy	建立代理原則（proxy policy）
ProxyType	建立代理類型（proxy type）
ProxyUnset	刪除代理
ProxyAutomatic	自動代理
ProxyDisabled	關閉代理
ProxyUnset	Unset
ProxyHTTPS	HTTPS
ProxySOCKS5	SOCKS5
ProxyAddress	代理位址 (host:port)
ProxyUsername	使用者名稱
ProxyPassword	密碼

系統登錄鍵值

以下是 Skype 3.0 beta 版用戶端程式 的系統登錄鍵值(registry keys)清單：

HKEY_LOCAL_MACHINE (HKLM)

在發生衝突時，本機系統登錄鍵值高於本地使用者登錄鍵值。

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

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

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

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

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

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

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

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

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

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

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

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

HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ProxySetting, REG_SZ = {string}

HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ProxyAddress, REG_SZ = {string}

HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ProxyUsername, REG_SZ = {string}

HKEY_LOCAL_MACHINE\Software\Policies\Skype\Phone, ProxyPassword, REG_SZ = {string}

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

HKEY_CURRENT_USER (HKCU)

若有衝突，給現有使用者的系統登錄鍵值優先權高於 XML 設定檔中的參數。

若有衝突，XML 設定檔（包括 shared.xml 與 config.xml）當中的設定優先權高於使用者在本身用戶端程式中的設定。

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

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

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

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

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

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

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

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

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

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

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

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

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxySetting, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxyAddress, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxyUsername, REG_SZ = {string}

HKEY_CURRENT_USER\Software\Policies\Skype\Phone, ProxyPassword, REG_SZ = {string}

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