How to Control Skype in a Corporate Setting

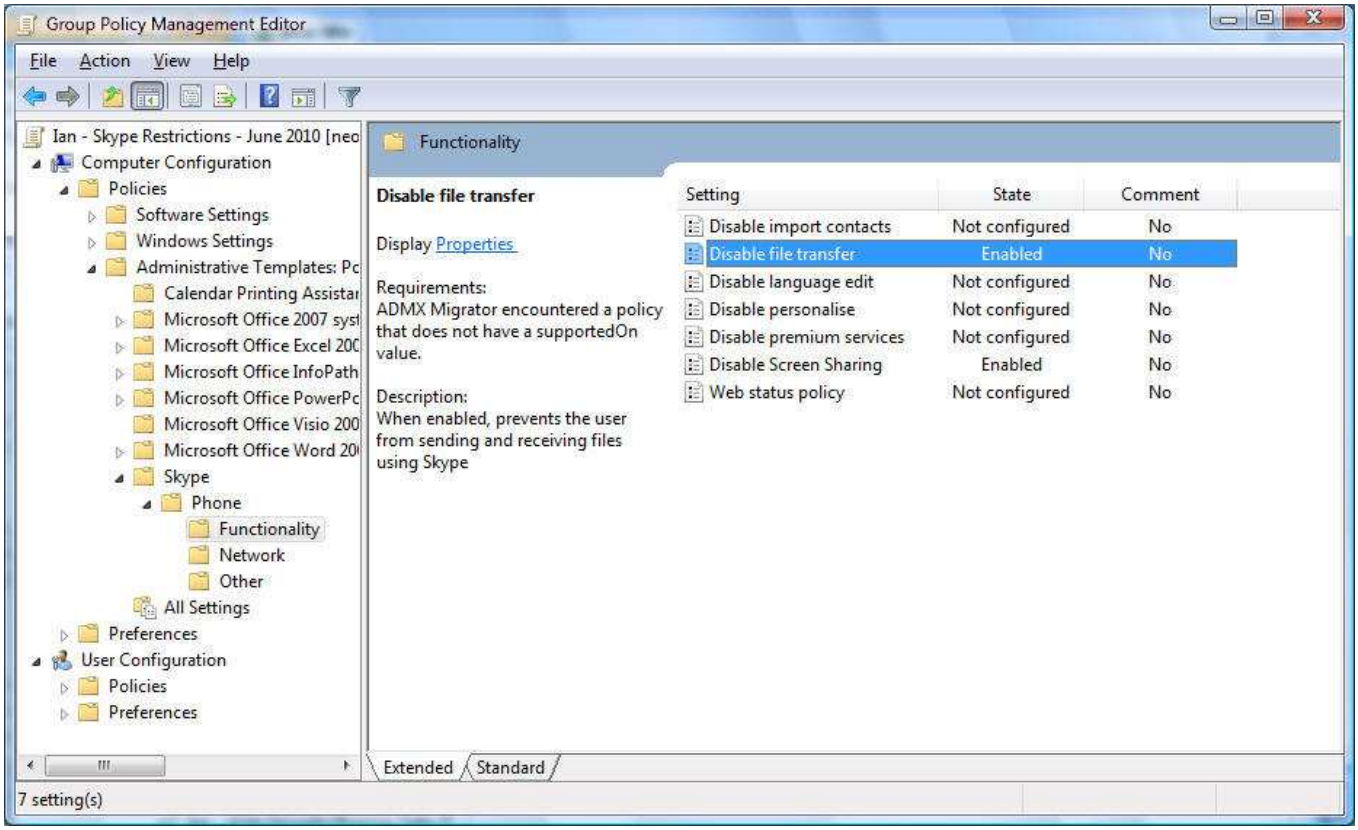
http://www.commodore.ca/windows/skype/skype-business.htm

As usual these instructions and notes are written mainly for me as a cook book to use at various clients. There is no warranty or guarantee express or implied in these notes so be careful.

If you are a professional network administrator you know that you need to check and often control the software that in your environment. Skype, while common for personal use is seldom used in the corporate world and for good reason. There are several important things you need to know about Skype:

1. Skype is a "distributed application" and so even when you are NOT in a call, Skype is using your CPU and more importantly your bandwidth to route OTHER peoples calls. On a single computer, this is not often a problem but on a corporate network the resulting bandwidth drain can cause serious problems.
   .
2. Skype has file and screen sharing which will breach nearly every corporations security policies.
   .
3. Skype "for home" has no call tracking, monitoring or control mechanisms which will breach some security policies.
   .
4. Skype "for home" will have corporate users expensing $1.12 calls which will make everyone nuts.
   .
5. Skype has removed their "Guide For Network Administrators" as of version 3 in about 2007 and stopped making their management templates available. Fortunately, I have confirmed that the template I provide below functions on the 2010 version of Skype (v4.2) and I certainly hope it continues to function under v5 due out in the fall.
   .

The solutions to these problems is to:



1. Register with Skype Business and then use Skype Manager.

- Watch this Skype Manager Video to get the core ideas.
- Skype Manager will let you create and control accounts in a consistent way
- Skype Manager will let you print a report of each users calls
- Skype Manager will let you add core profile information for each user

.

2. Download the Administration Templates, add them to your Windows domain, and set your policies. Note that I used an old "v1.7" Skype admin template from 2006 and enhanced it with a DISABLE SCREEN SHARING option so you will not find "my" "v1.8" template anywhere else on the web but here.
    - If you have a Windows 2008 domain or newer, use THIS .ADMX template
        - Copy these files to your **\\<domain>\sysvol\<domain>\Policies\PolicyDefinitions**
            - If you do not have a **PolicyDefinitions** folder, just create one
            - If this freaks you out, read THIS about how to create a central store..
    - If you have a Windows 2003 domain or older, use THIS .ADM template
        - Use your Group Policy Management Console to IMPORT this template.
    - After the template is added you should use your Group Policy Management Console to set your policies under COMPUTER CONFIGURATION, POLCIES, ADMINISTRATIVE TEMPLATES, SKYPE
        - I shut down the following Skype Features:
            - FILE SHARING
                - Skype offers no antivirus scanning on transfer and I will not intentionally leave malware detection to the desktop AV scanner alone. It should go through other several scans and it does not so I killed it
                - I don't want files to easily leave the company. Data protection is king.
            - SCREEN SHARING
                - I don't want information leaving the company or accidentally accessed via sharing
                - Users can view others people screens but not share theirs
            - PREVENT SUPERNODE
                - this stops the Skype client from using network bandwidth for OTHER people
            - DISABLE LISTENING TO TCP
                - this stops the Skype client from receiving uninvited connections
            - DISABLE SKYPE PUBLIC API
                - this stops third party plugin / extras from working
            - DISABLE NEW VERSION CHECKING
                - I will update clients when I think they should be.
                - I don't want users pestered with upgrade notices.
    - Apply that new Group Policy to the OU's you are concerned with and either wait a few hours for them to be automatically applied or just run **gpupdate /force** manually on the machine in question..
    - If you don't like the to use Group Policy you can simply create your own registry entries under **HKEY_LOCAL_MACHINE\SOFTWARE\POLICIES\SKYPE\PHONE**. You can also download my reg file to get started..
    - Some of you may find this Skype forum thread (particularly the end) to be useful.
    - A thorough analysis of Skype and its security implications for organizations can be found on this University of Texas page. Specifically, you may find there detail Group Policy / Registry detail to be quite useful: .

DisableFileTransferPolicy—Disables file transfer to prevent the user from sending and receiving files using Skype.

DisableContactImportPolicy—Disables import contacts.
DisablePersonalisePolicy—Disables personalization to prevent the user from changing sounds.
DisableLanguageEditPolicy—Disables language edit to prevent the user from editing language strings.
WebStatusPolicy—When enabled, always publishes the user's status on the Web as Skype buttons. When disabled, prevents the user from publishing status on the Web.
DisableApiPolicy—Disables the Skype Public API to prevent third-party applications from accessing Skype functionality.
DisableVersionCheckPolicy—Disables new version checking by preventing Skype from detecting new versions and updates.
MemoryOnlyPolicy—Runs in memory-only mode so Skype does not store any data on the local disk.
ListePortPolicy—Sets the listening port where Skype listens for incoming connections.
ListenPort—Listening port number.
ListenHTTPPortsPolicy—When enabled, listens on HTTP (port 80) and HTTPS (port 443) ports. When disabled, does not listen on HTTP/HTTPS ports. When not configured, lets the user decide.
DisableTCPListenPolicy—Disables listening for TCP connections to prevent the Skype client from receiving incoming TCP connections.
DisableUDPPolicy—Disables UDP communications to prevent the Skype client from using UDP to communicate with the network.
DisableSupernodePolicy—Prevents the Skype client from becoming a super node or relay host.
ProxyPolicy—Establishes the proxy policy.
ProxyType—Establishes the proxy type.
ProxyUnset—Unset
ProxyAutomatic—Automatic
ProxyDisabled—Disabled
ProxyUnset—Unset
ProxyHTTPS—HTTPS
ProxySOCKS5—SOCKS5
ProxyAddress—Proxy address (host:port)
ProxyUsername—Username
ProxyPassword—Password

The following is a list of configurable registry entries that apply to the Windows Skype Client as taken from the Skype Guide for Network Administrators (HKLM is short for HKEY_LOCAL_MACHINE) (Skype, 2008):

```
HKLM\Software\Policies\Skype\Phone, DisableApi, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, DisableFileTransfer, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, MemoryOnly, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, DisableContactImport, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, DisableVersionCheck, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, DisablePersonalise, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, DisableLanguageEdit, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, ListenPort, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, ListenHTTPPorts, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, DisableTCPListen, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, DisableUDP, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, DisableSupernode, REG_DWORD = {0,1}
HKLM\Software\Policies\Skype\Phone, ProxySettings, REG_SZ = {string}
HKLM\Software\Policies\Skype\Phone, ProxyAddress, REG_SZ = {string}
HKLM\Software\Policies\Skype\Phone, ProxyUsername, REG_SZ = {string}
HKLM\Software\Policies\Skype\Phone, ProxyPassword, REG_SZ = {string}
HKLM\Software\Policies\Skype\Phone, WebStatus, REG_DWORD = {0,1}
```

These same registry settings are available for the current user at

HKEY_CURRENT_USER\Software\Policies\Skype\Phone but the HKEY_LOCAL_MACHINE entries take precedence.