How to Block Skype for Business

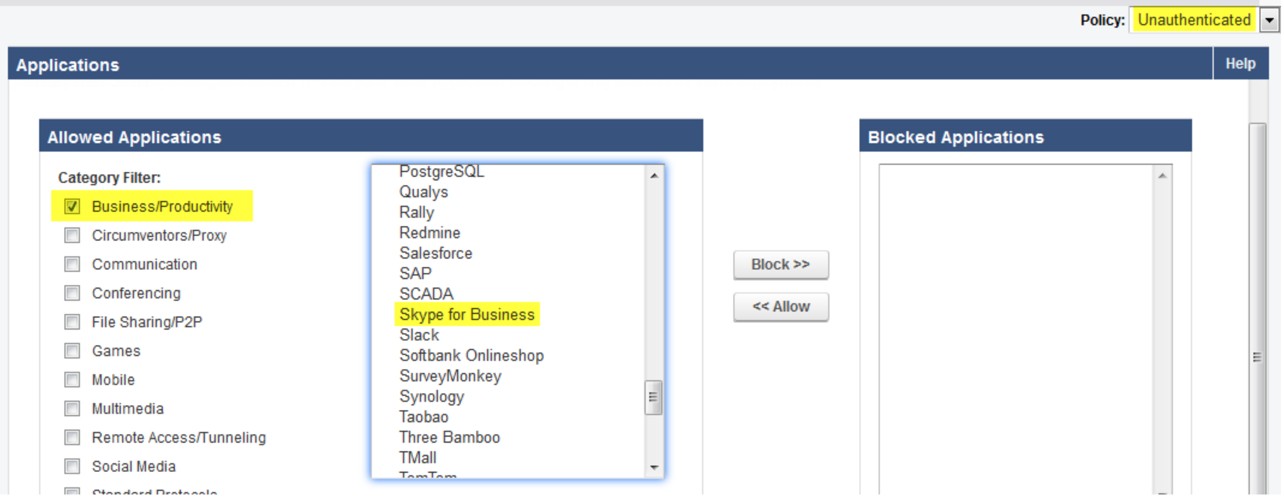
https://campus.barracuda.com/doc/76285138/

This feature is available with the Barracuda Web Security Gateway version 14.0 and higher.

To completely block Skype for Business, you may have to also block Microsoft Services (See the **BLOCK/ACCEPT > Applications** page). This is because Skype for Business and other Microsoft Services are co-mingled, such that some other Microsoft Services could be detected as Skype for Business. If you block Microsoft Services, this could include blocking One Drive, Sharepoint, etc. Because Microsoft does not provide a complete list of what Microsoft Services contains, some services may be blocked, while others may not. If you don't want to block Microsoft Services, begin by blocking Skype for Business first, and then test. If Skype for Business is not completely blocked, you would need to block *Microsoft Services* as well.

To block Skype for Business traffic for either *Authenticated* or *Unauthenticated* users:

1. Go to the **BLOCK/ACCEPT > Applications** page.
2. Select either *Authenticated* or *Unauthenticated* for **Policy** in the upper right of the page.
3. To easily locate Skype for Business, uncheck all of the boxes under **Allowed Applications** except for **Business/Productivity**.
4. Select *Skype for Business* in the scroll list.
5. Click **Block >>**, then click **Save**.



Policy: Unauthenticated

Category Filter:

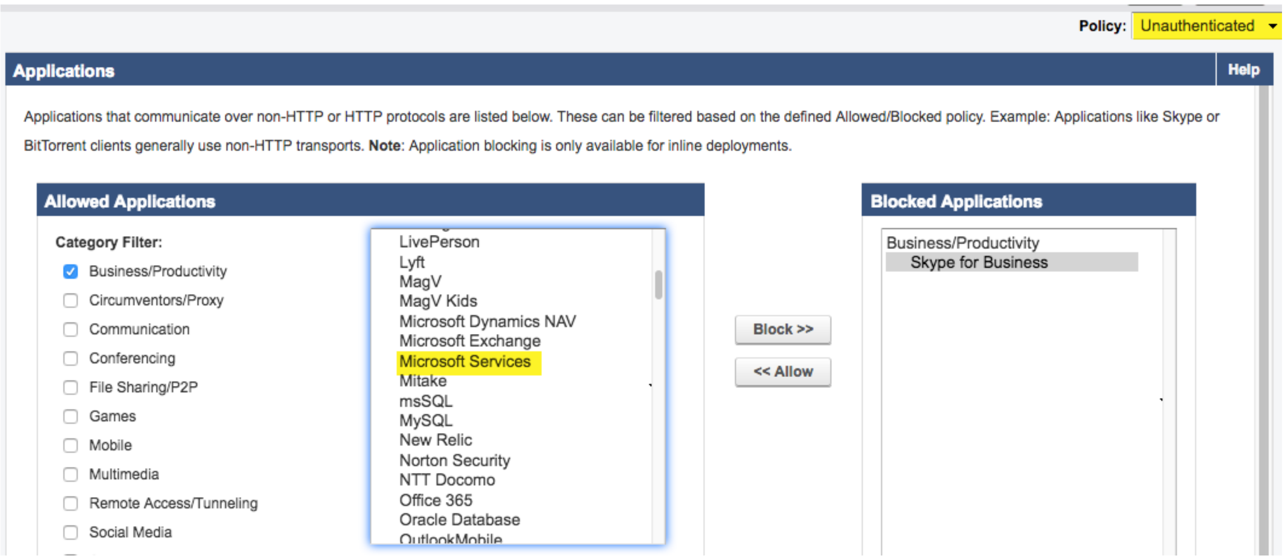
☑ Business/Productivity

To block for a specific user or group of users, use the **BLOCK/ACCEPT > Exceptions** page. See also Exception Policies.

To block Microsoft Services traffic for either *Authenticated* or *Unauthenticated* users:

1. Follow steps 1 and 2 above.

2. To easily locate Microsoft Services, uncheck all of the boxes under **Allowed Applications** except for **Business/Productivity**.
3. Select *Microsoft Services* in the scroll list.
4. Click **Block >>**, then click **Save**.



Policy: Unauthenticated

Applications

Applications that communicate over non-HTTP or HTTP protocols are listed below. These can be filtered based on the defined Allowed/Blocked policy. Example: Applications like Skype or BitTorrent clients generally use non-HTTP transports. **Note**: Application blocking is only available for inline deployments.

Allowed Applications

Category Filter:

- ☑ Business/Productivity
- ☐ Circumventors/Proxy
- ☐ Communication
- ☐ Conferencing
- ☐ File Sharing/P2P
- ☐ Games
- ☐ Mobile
- ☐ Multimedia
- ☐ Remote Access/Tunneling
- ☐ Social Media

LivePerson
Lyft
MagV
MagV Kids
Microsoft Dynamics NAV
Microsoft Exchange
Microsoft Services
Mitake
msSQL
MySQL
New Relic
Norton Security
NTT Docomo
Office 365
Oracle Database
OutlookMobile

Blocked Applications

Business/Productivity
Skype for Business

Figures