Guide for enabling Call Barring for Skype for Business via PowerShell

This guide will document the processes for using Microsoft Windows PowerShell to query and set Call Barring policies to users in your Skype for Business tenancy.

For more information on what policies there are for barring calls, visit: https://docs.microsoft.com/en-us/skypeforbusiness/audio-conferencing-in-office-365/outbound-calling-restriction-policies
1. Getting started
To use Microsoft Windows PowerShell to configure your Skype for Business tenancy, you will need:

- A computer running Windows 7 x64 or later
- PowerShell 5.1 or later (requires .NET 4.5.2 or later)
- A user on the computer with Admin privileges
- The Skype for Business PowerShell module
- Admin login for your tenancy.

For help on where to download PowerShell updates and the Skype for Business module, visit this link: https://technet.microsoft.com/en-us/library/dn362795(v=ocs.15).aspx

2. Loading the Skype for Business PowerShell module
Open a PowerShell x64 command line window, with Admin privileges:

Load the module; type in:
PS > Import-Module SkypeOnlineConnector

If the above command fails due to a security error, change the Execution Policy for yourself to allow RemoteSigned or all AllSigned scripts:

Enter the tenancy credentials:
PS > $Cred = Get-Credential

A dialog box will pop up for you to enter your tenancy admin username and password in the associated password.

Open a session:
PS > $Session = New-CsOnlineSession -Credential $Cred -Verbose
PS > Import-PSSession $Session -AllowClobber

Optionally, confirm your connectivity:
PS > Get-CsTenant

3. Checking existing Call Barring policies
To find what Call Barring policies are available:
PS > Get-CsOnlineDialOutPolicy

The policy names to use in the PowerShell command are prefixed with 'Tag:'
To see what these policies do, visit: https://docs.microsoft.com/en-us/skypeforbusiness/audio-conferencing-in-office-365/outbound-calling-restriction-policies

For these commands, substitute user@login with your selected username and tenancy domain.

To check an individual user:
PS > Get-CsOnlineUser -Identity user@login.onmicrosoft.com | Format-Table –Property UserPrincipalName, LineURI, OnlineDialOutPolicy

To check a matched subset of users:
PS > Get-CsOnlineUser *commonpattern* | Format-Table –Property UserPrincipalName, LineURI, OnlineDialOutPolicy

To check all users:
PS > Get-CsOnlineUser | Format-Table –Property UserPrincipalName, LineURI, OnlineDialOutPolicy

4. Changing Call Barring policies
Call Barring policies are applied at the user level. They are not able to be customised. To bar International Calls, the pre-existing policy must be selected: DialoutCPAndPSTNDomestic. To remove Call Barring, apply the policy that allows it: DialoutCPAndPSTNInternational.

For these commands, substitute user@login with your selected username and tenancy domain and policymame with your selected Call Barring policy, e.g. DialoutCPAndPSTNDomestic or DialoutCPAndPSTNInternational.

To set a Call Barring policy to an individual user:
PS > Grant-CsDialoutPolicy -PolicyName policymame -Identity user@login.onmicrosoft.com

To batch convert a matched subset of users:
PS > Get-CsOnlineUser *commonpattern* | Grant-CsDialoutPolicy -PolicyName policymame

To set a policy on all users:
PS > Get-CsOnlineUser | Grant-CsDialoutPolicy -PolicyName policymame