How to Deploy the Barracuda Content Shield Agent via GPO

https://campus.barracuda.com/doc/88540155/

This article provides sample scripts that can be used for successful deployment of Barracuda Content Shield (BCS) using GPO. The article is not intended to provide comprehensive instruction in the use of Microsoft GPO, and all samples are provided without assurances or guarantees.

An example Powershell script is provided here to demonstrate fully automating an installation. Using a command line batch file enables the administrator to remotely configure and control the Powershell script. The Group Policy Manager (GPO) is used to distribute these resources to the intended domain-attached computers. The sample script, `ExampleBCSConfig.ps1`, can be found at Example Powershell Script for GPO Deployment of BCS Agent for Windows.

Note that this script is ONLY an example and is offered without assurances or guarantees. Make sure to run the script with elevated permissions.

The domain name “dc1.myco.com” is used to represent the domain controller throughout this example. Be sure to make appropriate substitutions for your environment.

Procedure and Sample Deployment Script

Required and Example Files

- The current `BarracudaContentShieldSetup-#.#.#.#.exe` file, which is available from the **DOWNLOADS** page of your BCS account.
- The `bcs.key` file, which is also available on the **DOWNLOADS** page (see **Account Configuration File**).
- The sample batch file (`ConfigureBCSPlus.bat`) is included below. This .bat file must be edited to reflect the settings (file paths, operational mode, target installer .exe, file version, etc.) in your particular environment. Additionally, if you choose to use this procedure to perform future upgrades of the BCS software, this file will need to be edited to reflect the new version of the installer .exe file.

Performing upgrades also requires downloading the new installer .exe file and saving it in the shared folder (e.g. \\dc1\BCS-Files\), and the GPO **Files** settings also need to be modified.

Procedure for GPO Deployment

ACTION STEPS	EXAMPLE VALUE	COMMENTS

1. Select or Create an Active Directory Organizational Unit	BCSPlus	You may want to create a new OU to limit the scope of the machines affected by the GPO. CAUTION: If you want to retain the option to remove this OU in the future, be sure to de-selected the default “Protect container from accidental deletion” setting before creation.
2. Using AD, ***move*** the computers that are to be the targets of this deployment to the OU identified in Step 1 (e.g. BCSplus).	WIN10-SMITH-PC	None
3. Create a shared folder on the Domain Controller, and populate with the files* that need to be deployed.	\\dc1\BCS-Files • `BarracudaContentShieldSetup-#.#.#.#.exe` • `bcs.key` • `ExampleBCSConfig.ps1` • `ConfigureBCSPlus.bat`	**Important:** Folder permissions: • Sharing > Advanced Sharing > Permissions; ∘ “Authenticated Users” need **Read** access ∘ “Everyone” should have **Full Control** • Security; ∘ “Authenticated Users” need default permissions (read & execute, list folder contents, read) ∘ “Everyone” should have default permissions
4. Open Group Policy Manager and select the appropriate OU (e.g. BCSplus), and then create a GPO.	BCS Deployment	None

5. Edit the GPO - Define **Folders** to be used/created on endpoint computers: Computer Configuration > Preferences > Windows Settings > Folders	C:\gpo-bcs-files	This folder will be created and administered, on the endpoint computer(s), by this GPO
6. Edit the GPO - Map **Files** to be deployed to endpoint computers: Computer Configuration > Preferences > Windows Settings > Files	Use Action: Replace Source file(s): \\dc1\BCS-Files\ConfigureBCSPlus.bat Destination file: C:\gpo-bcs-files\ConfigureBCSPlus.bat Repeat for all files (See **step 3** for all example resource filenames)	**IMPORTANT:** • Be sure to edit the **Source** file name to use the UNC format, (e.g. \\dc1\BCS-Files\ConfigureBCSPlus.bat) • The file **Destination** is the (new) target folder on the client computer(s) • If browsing for the source file fails, type the full path manually
7. Edit the GPO - Create a Scheduled Task: Computer Configuration > Preferences > Control Panel Settings > Scheduled Tasks New Scheduled Task (At least Windows 7)	BCS Manager • **General** tab ◦ Run using (NT AUTHORITY)\System account ◦ Run whether user is logged on or not ◦ Run with highest privileges • **Triggers** tab ◦ One time – 2/21/2019 at 06:00 • **Actions** tab ◦ Start a program ◦ Program/Script = C:\gpo-bcs-files\ConfigureBCSPlus.bat ◦ Start in = C:\gpo-bcs-files • **Conditions** tab ◦ Be sure **Start only if the following network connection is available: Any connection** is selected • **Settings** tab (defaults used) • **Common** tab (defaults used)	This example uses a one-time execution. The task needs to be run with elevated privileges in order to be able to install the software.
8. Configure Firewall on endpoint computer(s)		If you plan to *push* GPO updates, you may find it necessary to enable some inbound firewall settings on the endpoint computers.

Sample Batch File

This batch file, as described above, calls the example powershell script 'ExampleBCSConfig.ps1'.

ConfigureBCSPlus.bat

```
@echo off
setlocal enableextensions
:: NOTES
=============================================================================
:: The following commands are sample CLI commands to invoke the powershell
script.
:: There are separate commands for Installations, Upgrade, and Uninstall.
:: Make sure to adjust the comment characters (::) and parameter contents for
the command being called. Only one command line should be enabled at a time.
:: Parameter Descriptions:
:: curdir = %~dp0 << This default will resolve to the location from which the
batch file launches on the endpoint. Optionally, the individual command call
can be edited to use a static path in place of the %curdir% substitution
(usually the same as -workDir).
:: -workDir << This should be the full path to the location of the installer
and bcs.key files on the endpoint.
:: -keyName << This should match the name of your bcs.key file.
:: -userPass << For the Uninstall command: The Agent Password from your
Account Settings page.
:: IMPORTANT - Take care to ensure that the version of the executable is
updated to reference the executable to be used. (e.g. ...Setup-1.1.1.1 might
need to change to ...Setup-1.9.9.9, etc.)
:: Deploy via GPO: Create a per-machine GPO that executes a Startup Script
(make sure it runs with elevated permissions) that invokes the powershell
script (or any other script that you created) to install or remove the BCS
agent (executable).
:: Return codes:
:: 3010 - Uninstall successful. Reboot pending: On uninstall, a reboot is
required before reinstalling the agent.
:: 0 - Installation successful. (Also on a "remove" action, if the agent is
not installed).
:: 1601 - Install aborted. SETUP.EXE not found.
:: 1602 - Install aborted. Check KEYPATH value.
:: 1603 - Uninstall canceled. Most likely because either the Tamper Proof
reature is disabled or the wrong password was provided.
:: For any of the 16xx return codes, also check the component MSI logs which
can be found in the %temp% folder of the process owner.
::
=============================================================================
======
set curdir = %~dp0
::INSTALL
powershell.exe -NoProfile -executionpolicy bypass -file
"%curdir%ExampleBCSConfig.ps1" -action "install" -workDir "c:\\barracuda" -
setupName "BarracudaContentShieldSetup-1.1.1.1.exe" -keyName "bcs.key"
::UPGRADE existing installation
::powershell.exe -NoProfile -executionpolicy bypass -file
"%curdir%ExampleBCSConfig.ps1" -action "install" -workDir "c:\\barracuda" -
setupName "BarracudaContentShieldSetup-1.1.1.1.exe" -keyName "bcs.key"
::UNINSTALL
::powershell.exe -NoProfile -executionpolicy bypass -file
"%curdir%ExampleBCSConfig.ps1" -action "remove" -workDir "c:\\barracuda" -
setupName "BarracudaContentShieldSetup-1.1.1.1.exe" -userPass "my_password"
endlocal
```