附上兩份使用者手冊資料，分別是：

1. Carbon Black Cloud Sensor 安裝手冊：文件有詳述部署環境需求，包含Firewall or Proxy 相關設定。
2. Carbon Black Cloud 使用者手冊：文件中有詳述所有設定功能，包含防禦政策設定說明。

Firewall or Proxy 相關設定，請參考以下資訊：

**用戶環境需求：**

* **開放以下之防火牆對外存取配置\*：**

       - 開放從 Sensor/Console/Proxy 對以下 URL 之存取：

* + - WebUI URL: [https://defense-prod05.conferdeploy.net](https://defense-prod05.conferdeploy.net/)
    - Sensor URL: [https://dev-prod05.conferdeploy.net](https://dev-prod05.conferdeploy.net/)
    - Connector/API URL: [https://api-prod05.conferdeploy.net](https://api-prod05.conferdeploy.net/)
    - Signature URL:  [https://updates2.cdc.carbonblack.io](https://updates2.cdc.carbonblack.io/)

       - 使用 Proxy 時, Proxy 必須開放透通存取(不做 SSL Termination)

* + - <http://ocsp.godaddy.com>
    - http:// crl.godaddy.com
    - 或是關閉  CB 的 CRL (憑證檢查機制)

**SIEM 須視整合標而定, 有可能需要額外的 Port, 支援 syslog**

Proxy的設定我也摘錄重要資訊如下：

1. Configure a Proxy for Windows after Sensor Installation

This procedure requires that you have RepCLI authentication. For more information about RepCLI, see [Managing Sensors by using RepCLI](https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-AD45D13D-7688-4ECB-8887-16FCC2577DF8.html" \o "https://docs.vmware.com/en/VMware-Carbon-Black-Cloud/services/carbon-black-cloud-user-guide/GUID-AD45D13D-7688-4ECB-8887-16FCC2577DF8.html) in the User Guide.

## Procedure

1. Place the sensor into bypass mode:

repcli bypass 1

1. Confirm that the sensor is in bypass mode:

repcli status

1. Shut down the sensor service:

repcli stopCbServices

1. As a best practice, create a backup of the cfg.ini file into another directory. For Windows sensor versions 3.6 and earlier, cfg.ini is located at C:\Program Files\Confer\cfg.ini. For Windows sensors 3.7 and later, cfg.ini is located at C:\ProgramData\CarbonBlack\DataFiles\cfg.ini. After you successfully complete the procedure, delete the backup file.
2. Edit cfg.ini in a plain text editor.
   1. If the following parameters exists in cfg.ini, remove them:

b.      ProxyServer=

ProxyServerCredentials=

* 1. Add the following parameters:

d.      ProxyServer=[PROXY\_IP\_OR\_DOMAIN]:[PROXY\_PORT]

e.      ProxyServerCredentials=[USERNAME]:[PASSWORD] (Optional- if proxy requires authentication)

f.

g.      ---Example--

h.      ProxyServer=TestProxy.net:8080

ProxyServerCredentials=TestUsername:TestPassword

* 1. If the original proxy is still functioning, add the following value to override the previously used value. This option is only available in Windows sensors 3.6+.

PreferStaticProxyOverLastUsed=true

1. Save cfg.ini.
2. Restart the sensor service:

sc start CbDefense

1. Take the sensor out of bypass mode:

repcli bypass 0

1. To force an immediate check-in (optional):

repcli cloud hello

1. Configure a Proxy for Linux (all Sensor Versions)

Use this procedure to configure a proxy through the cfg.ini file for all distributions.

**Procedure**

1. Extract the contents of the installer package into a temporary directory.
2. Use the install.sh script to install the agent, but do not provide a company code:

sudo cb-psc-install/install.sh

1. Update the cfg.ini file with the v3.x+ company code:

sudo /opt/carbonblack/psc/bin/cbagentd -d '<COMPANY\_CODE>'

1. Append the following entry in the /var/opt/carbonblack/psc/cfg.inifile. You can use the IP address instead of the hostname.

ProxyServer=<hostname>:<port number>

**Note:**The Linux sensor only supports a HTTP non-authenticated proxy server through cfg.ini.

| **Proxy Type** | **IP Format** | **FDQN Format** |
| --- | --- | --- |
| HTTP | ip:port | fdqn:port |
| HTTP | <http://ip:port> | <http://fdqn:port> |

Example Cfg.ini settings:

[customer]

ProxyServer=proxy.example.com:3128

ProxyServer=<hostname>:<port number>

1. Start the agent:
   * Centos/Rhel 6:
     + $ service cbagentd start
   * All other distributions:
     + $ systemctl start cbagentd

1. Configure a Proxy for Linux (Sensor Versions 2.11.1+)

For Linux sensor version 2.11.1 onwards, use this procedure to configure a proxy through the install.sh script for all distributions.

## Procedure

1. Extract the contents of the installer package into a temporary directory.
2. Use the install.sh script to install the agent together with proxy server details and the company code.

You can use the IP address or hostname as part of ProxyHost.

sudo cb-psc-install/install.sh -p ‘ProxyHost:ProxyPort’ ‘<COMPANY\_CODE>’

1. macOS Proxy Server Information

The macOS 3.7.2 sensor uses macOS Keychain APIs to improve proxy server information storage.

If you downgrade the macOS sensor from 3.7.2+ to an earlier sensor version, proxy settings must be repopulated.

* If you used macOS System Preferences for the proxy configuration, the sensor attempts to repopulate the proxy information after the sensor is downgraded.
* If the proxy configuration cannot be retrieved from the macOS System Preferences, you must use the sensor unattended installer options -p PROXY\_SERVER:PORT and -x PROXY\_USER:PASSWORD to repopulate the proxy settings during the sensor downgrade.