persystent SUITE

BIT LOCKER INTEGRATION

BitLocker Overview

BitLocker Authentication Methods

Persystent Suite supports several different options and configurations of BitLocker. Each of the different authentication methods that are supported are described below:

- TPM Protector – Use TPM validation only
- TPM and user PIN – Use TPM validation and the user must enter the correct PIN before the start-up process can continue
- TPM USB startup key – TPM validation and a USB flash drive containing the startup key must be inserted
- TPM, USB startup key and user PIN – TPM validation, user is prompted for PIN, and USB flash drive containing the startup key must be inserted
- Startup key – User is prompted to insert the USB flash drive containing the startup key
- User password – User PIN

BitLocker Encryption

The following encryption and cipher strengths are supported:

- Group policy driven when specified or XTS-AES 128
- AES 128-bit
- AES 256-bit
- XTS-AES 128 bit (Windows 10, 1511 and higher only)
- XTS-AES 256 bit (Windows 10, 1511 and higher only)

WebUI Configuration

Encryption settings can be configured such that when an image is deployed it will automatically be configured to use BitLocker. The settings below describe how to setup encryption in the WebUI, so that when an image is deployed it will automatically use the settings defined in the WebUI by default. To configure encryption in the WebUI:

1. Launch the WebUI web console.
2. Log into the web console.
3. In the left navigation pane under **Servers** select the server that will be encryption compatible.
4. In the main navigation area select the **Manage** tab.
5. In the **Server** area, there are several fields:
    A. Encryption Compatibility – Select the encryption mode to use
    B. BitLocker Encryption – Select whether BitLocker will be group policy driven or use AES 128-bit or 256-bit
    C. BitLocker Pin or Password – If deploying BitLocker with a PIN, enter the PIN to be used here
    D. TPM Pin – Enter the Pin that was used to setup TPM

    NOTE If the TPM is not currently configured, it can be setup and enabled on each workstation when deploying the image. Enter the PIN that will be used during deployment.

6. Click **Save**.

Activating TPM

Enable and Activate TPM

It may be necessary to enable and activate the TPM module. Follow the steps below:

1. PXE boot the computer to be imaged.
2. Computer will now boot into the pre-boot environment and will prompt you to login.
3. Enter the username and password that you use to log into Persystent Web Console.
4. The **Client Build Wizard** screen is shown.
5. Click **BitLocker Setup…**
6. Look under the **Trusted Platform (TPM) Options** section and note the **TPM Status**. If it is **disabled**, click the button **Enable and Activate TPM**.

> **NOTE** If the **TPM Status** is set to **TPM enabled and active**, then no further action is necessary.

7. Read the information in the dialog box and click **OK**.
8. The computer will reboot.
9. Press **F10** to enable TPM.
10. Repeat steps 1-5 and ensure the **TPM status** is **TPM enabled and active**.

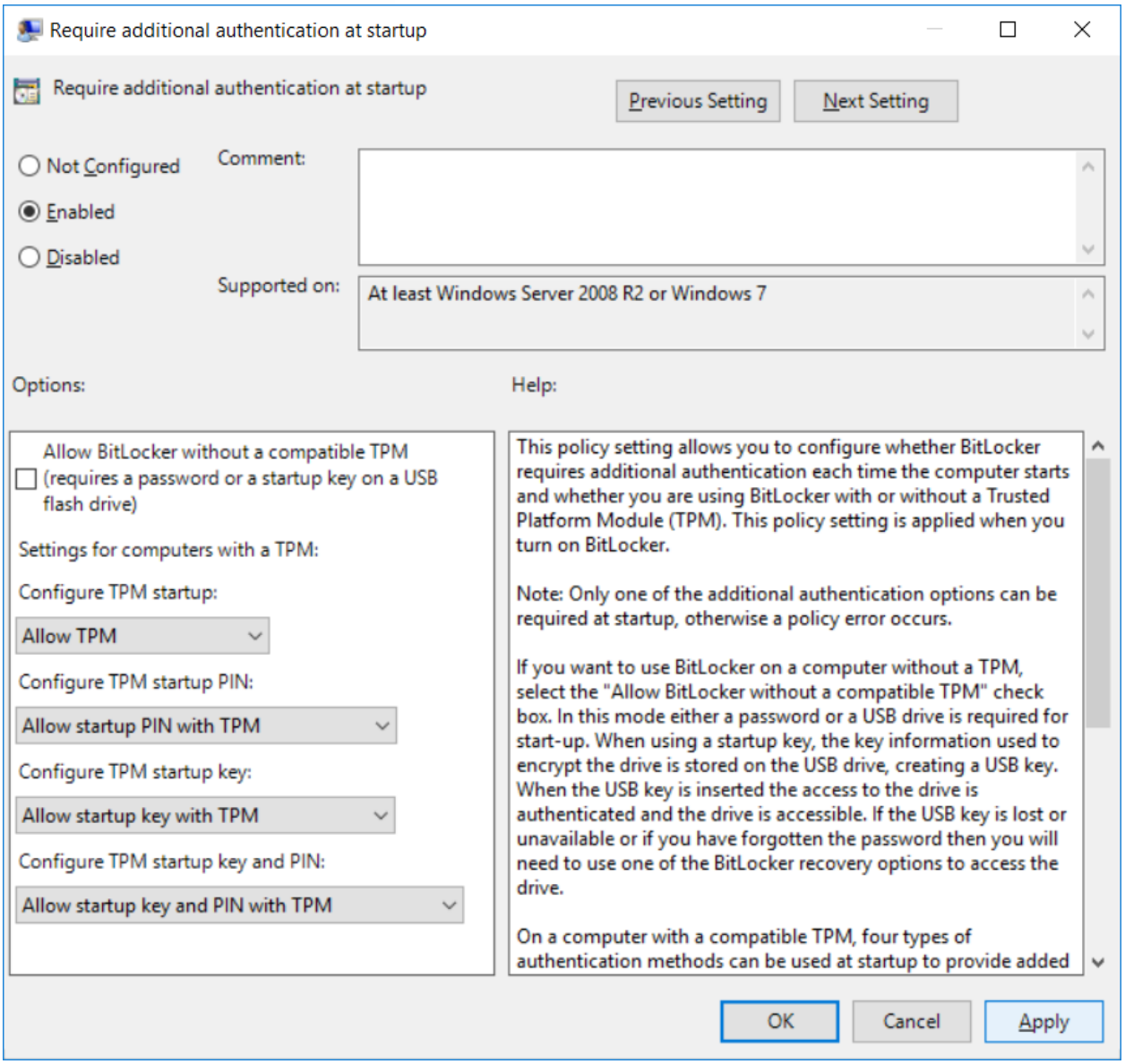
BitLocker Group Policy

Following group policies must be applied to machines by using local group policy or AD group policy. We recommend that these policies must be added to local group policy in the base image as well for the BitLocker. The integration with BitLocker and Persystent will not function correctly if these policies are not defined.

Windows 7, 8, 8.1, 10 [Prior to Version 1511]

Computer Configuration -> Administrative Templates -> Windows Components -> BitLocker Drive Encryption -> Operating System Drives -> Require additional authentication at start up

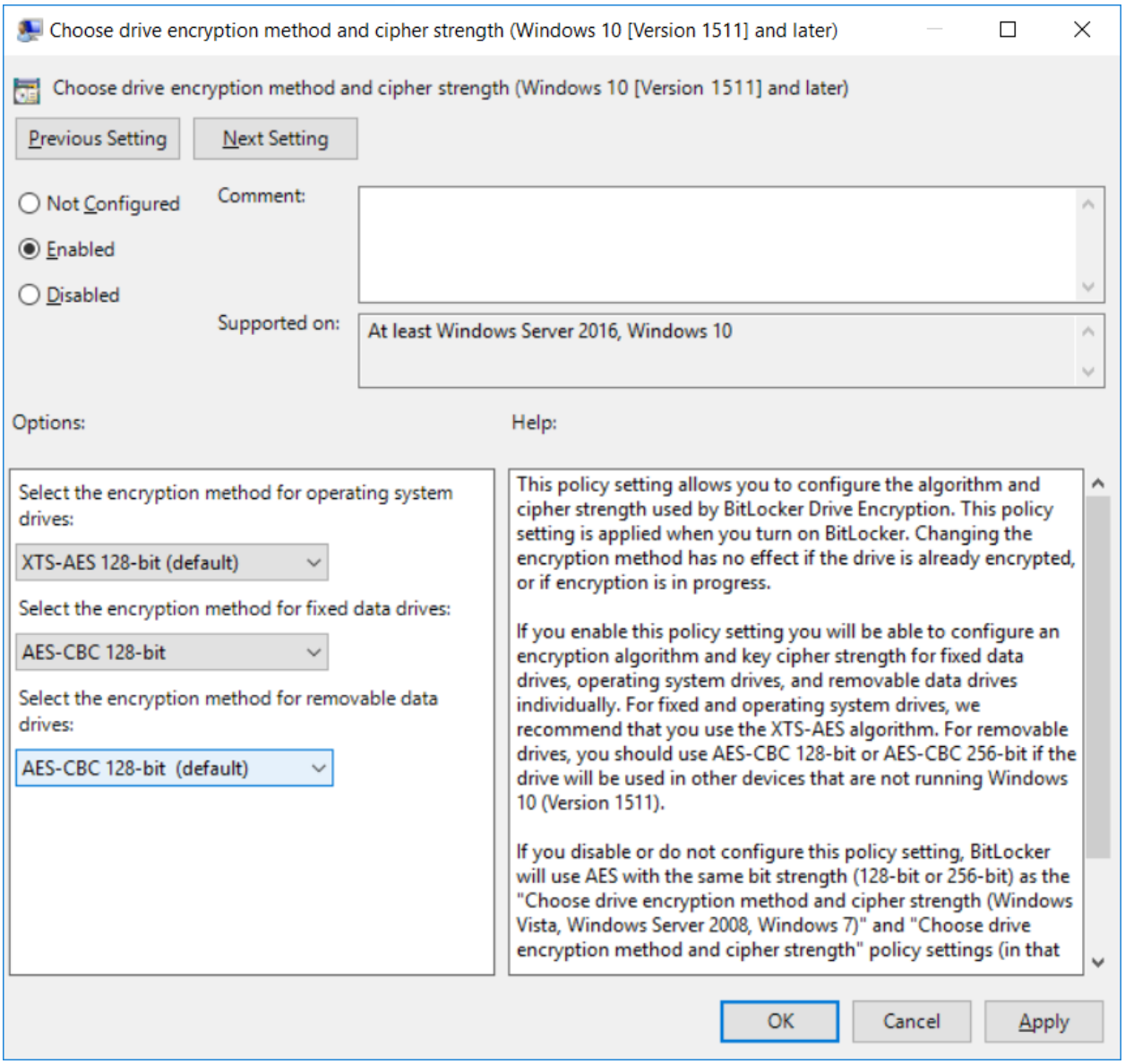
1. Change the policy to “Enabled”.
2. Uncheck “Allow BitLocker without a compatible TPM (requires a password or start up key on a USB flash drive)
3. Make following changes to “Settings for computers with a TPM”.
4. Change “Configure TPM startup” to “Allow TPM”.
5. Change “Configure TPM startup PIN” to “Allow startup PIN with TPM”.
6. Change “Configure TPM startup key and PIN” to “Allow startup key and PIN with TPM”.
7. Click on “Apply”.
8. Click on “OK”.



Windows 10 [Version 1511] and later only

Computer Configuration -> Administrative Templates -> Windows Components -> BitLocker Drive Encryption -> Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)

1. Change the policy to “Enabled”.
2. Change “Select the encryption method for operating system drives” to “XTS-AES 128-bit (default)”.
3. Change “Select the encryption method for fixed data drives” to “AES-CBC 128-bit”.
4. Change “Select the encryption method for operating system drives” to “AES-CBC 128-bit (default)”.



Deploy an Image with BitLocker

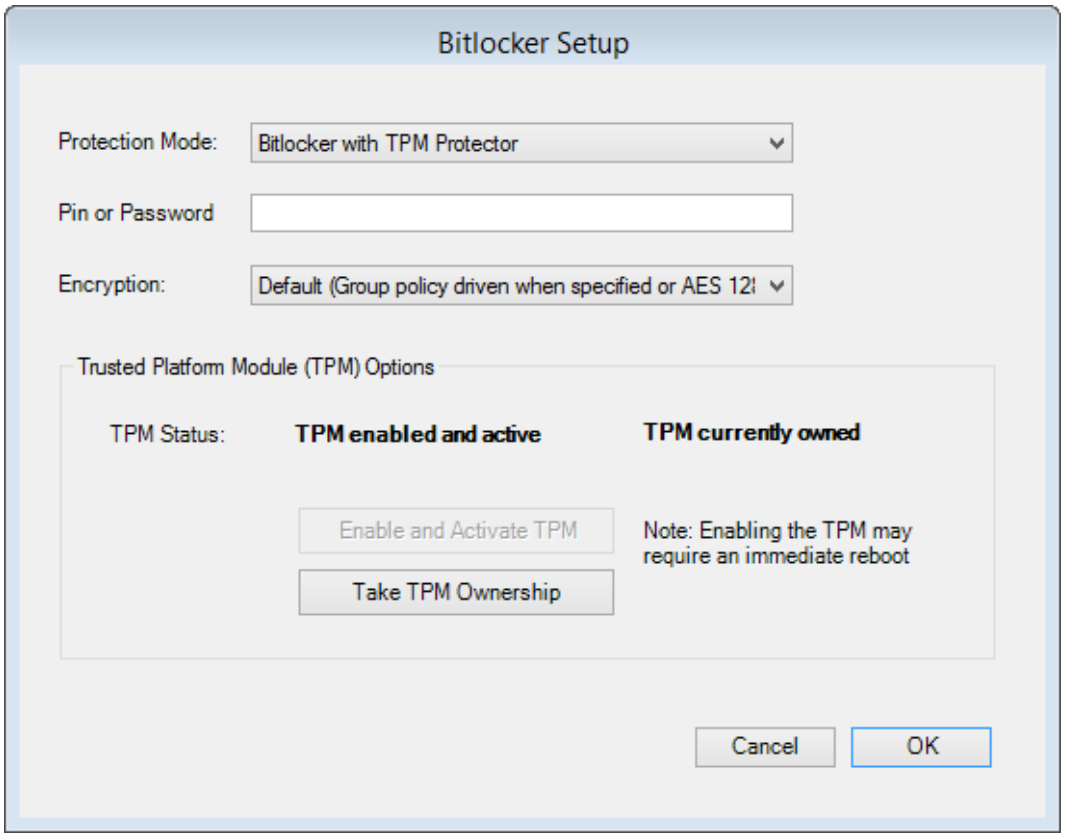
The steps below describe how to deploy an image with BitLocker enabled.

1. PXE boot the computer to be imaged.
2. Computer will now boot into the pre-boot environment and will prompt you to login.
3. Enter the username and password that you use to log into Persystent Web Console.
4. The **Client Build Wizard** screen is shown and **Install Image** is selected by default.

5. Click **BitLocker Setup…**

> **NOTE** If the BitLocker settings were defined in the WebUI, then those settings will be automatically applied without any further configuration necessary.

A. From the **Protection Mode** dropdown, select the desired setting.
B. If necessary, enter the desired Pin in the **Pin or Password field**.
C. From the Encryption dropdown, select the desired setting.
D. Click **OK**.



6. Choose a base image and configure any of the other options.
7. Click **Build**.
8. When the PC is finished being imaged it will boot into Windows and begin encrypting the drive.

Additional Information

Prepare your organization for BitLocker: Planning and Policies

- http://technet.microsoft.com/en-us/library/jj592683.aspx

UTOPIC

Utopic Software
1215 E 6th Avenue
Tampa, FL 33605

813.444.2231

support@utopicsoftware.com