Mandiant

# CONFIGURE GOLD IMAGES FOR PROTECTED THEATER

Configuring the image requires two steps, configuring the operating system for use in an image and then creating the image. This article includes the steps for configuring your Windows and your Linux Images and then the information you need about image requirements.

## Configure Windows Gold images

Before adding your Windows Gold Image to Protected Theater, you should add accounts and modify a few configurations. These configuration changes include:

- **Enabling macros in Microsoft Word**: Required if your testing includes Actions that use embedded macros to infect an endpoint with malware
- **Install Powershell:** Required if you want to run PowerShell-based Host CLI Actions
- **Configure Windows Accounts**: Required if you want to test using user profiles and not just the system account
- **Disable Windows User Account controls**
- **Disable Windows Secure Login**

You should also make sure the Gold Image meets the **Protected Actor Minimum System Requirements (https://docs.mandiant.com/home/protected-actor-minimum-system-requirements)**.

### Enable Microsoft Word Macros

1. Open Microsoft Word.
2. Click **File > Options**.
3. Select **Trust Center** and then click **Trust Center Settings**.
4. Select **Macro Settings** and then choose **Enable all macros**.
5. Select **Protected View** and clear the three Enable Protected View option checkboxes.
6. Click **OK** on both windows and then close Word.

### Configure Windows Accounts

Using Domain Accounts with Protected Theater is not supported

Instructions provided are for Windows 8, 8.1, and 10. If you are using a different version of Windows, refer to the Microsoft Windows documentation for that version.

1. From the run/search bar (you may need to open the Start menu), type Add User in the run bar, and select Add, edit, or remove other people.
2. Click Add someone else to this PC.
3. Select I don't have this person's sign-in information.
4. Select Add a user without a Microsoft account.
5. Enter the *account information* and *security questions* and then click Next.

   

   Capture information about the new accounts, including cases used in the username and password, so you can create the account identically in the Director.

6. Click Windows, click the user icon, and then select the new user account.
7. Sign in using that account to create the account profile, setting up Security Questions as required.

### To Disable Windows User Account Control

1. From the run/search bar (you may need to open the Start menu), type **User account** in the run bar, and select **Change User Account Control settings**.
2. Using the scroll bar, change the setting to **Never notify** and click **OK**.

#### To Disable Windows Secure Login

This is optional, but may reduce the amount of time an Action takes to run.

1. From the Windows run/search bar (you may need to open the Start menu), type **netplwiz** and press **Enter**.
2. Click the **Advanced** tab, clear the **Require users to press Ctrl+Alt+Delete** checkbox, and click **OK**.

### Configure Linux Gold Images

Before adding your Linux Gold Image to Protected Theater, you should complete the required configuration and add any user accounts you want to use during testing.

> Using Domain Accounts with Protected Theater is not supported.

A DHCP agent is also required for building the Linux Gold Image. The DHCP agent operates as the interface between DHCP clients and the server.

### Create the Image

Once you have the Windows or Linux environment configured, you are ready to create the image that you'll add to your Protected Theater. The following image formats are supported:

> Images can only be a single disk.

- OVA
- VMDK
- QCOW2
- VHD
- VDI

> We recommend you export the Gold image rather than moving it.

### Remove Snapshots

For QCOW2 images, snapshots cannot exist before you attempt the import. To remove snapshots, run one of the following commands, depending on whether your Protected Theater environment uses non-UEFI or UEFI firmware.

#### Remove all snapshots for non-UEFI

1. Connect to the Protected Theater shell using SSH.
2. Switch to the root user:

   ```
   sudo bash
   ```

3. Run the following commands, where *DOMAIN_ID* is the domain name for your Protected Actor Windows guest:

   ```
   virsh destroy --domain DOMAIN_ID
   virsh snapshot-list --domain DOMAIN_ID --name | xargs -n1 virsh snapshot-delete --domain DOMAIN_ID
   ```

#### Remove all snapshots for UEFI

1. Connect to the Protected Theater shell using SSH.
2. Switch to the root user:

```
sudo bash
```

3. Run the following commands, where *DOMAIN_ID* is the domain name for your Protected Actor Windows guest:

```
virsh destroy --domain DOMAIN_ID
virsh snapshot-list --domain DOMAIN_ID --name | xargs -n1 virsh snapshot-delete --domain DOMAIN_ID --metadata
```