VMware Carbon Black Cloud on VMware Horizon VDI Installation Guide
# VMware Carbon Black Cloud on VMware Horizon VDI Installation Guide

## Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Install VMware Carbon Black Cloud on Horizon persistent and nonpersistent VM pools of instant clones</td>
<td>3</td>
</tr>
<tr>
<td>GA support for Horizon 7.13 instant clones with VMware Carbon Black Cloud 3.6 or later sensor</td>
<td>3</td>
</tr>
<tr>
<td>Tech preview support for Horizon 7.12 and Horizon 8 (2006) instant clones with VMware Carbon Black Cloud 3.5 sensor</td>
<td>5</td>
</tr>
<tr>
<td>Virtual desktops and VMware Carbon Black Cloud sensor best practices</td>
<td>8</td>
</tr>
<tr>
<td>Policy settings for process rules in the VMware Carbon Black Cloud console</td>
<td>8</td>
</tr>
<tr>
<td>Local scan settings in the VMware Carbon Black Cloud console</td>
<td>9</td>
</tr>
<tr>
<td>VMware App Volumes best practices</td>
<td>10</td>
</tr>
<tr>
<td>VMware Dynamic Environment Manager best practices</td>
<td>13</td>
</tr>
<tr>
<td>VMware ThinApp best practices</td>
<td>14</td>
</tr>
<tr>
<td>Additional policies to set for Horizon components</td>
<td>14</td>
</tr>
<tr>
<td>Install VMware Carbon Black Cloud on Horizon persistent VM pools of full clones</td>
<td>19</td>
</tr>
<tr>
<td>Approach 1: Install the sensor in the golden image</td>
<td>19</td>
</tr>
<tr>
<td>Approach 2: Install the sensor using Customization Specification’s run once option</td>
<td>19</td>
</tr>
<tr>
<td>Comparison between both approaches</td>
<td>20</td>
</tr>
</tbody>
</table>
Introduction

Securing virtual desktop infrastructure (VDI) is a native capability of the VMware Carbon Black Cloud™ platform. It provides native next-generation antivirus, audit and remediation, as well as behavioral endpoint detection and response (EDR) to the VMware Horizon® platform and virtual desktops. VMware Carbon Black Cloud is the first security solution that tests Horizon VDI end to end. As a result, security is built into the platform, removing the need to architect a security solution to protect the virtual desktops or the overall environment.

Also, with VMware Carbon Black Cloud, virtual desktops perform better overall:

• No heavy security appliances are required within each host.
• No additional infrastructure is required to secure virtual assets.
• The performance impact on the desktop itself is minimal, reducing login times and freeing additional capacity to deploy more desktops.

VDI is extremely beneficial for enterprises from multiple dimensions, including enhanced employee mobility, tighter user access controls in regard to sensitive data, and improved patch management across the organization.

By following the steps described in this white paper, you will successfully deploy VMware Carbon Black Cloud within your VDI environment, have an appropriate policy, and understand the risks and how to mitigate them. VMware Carbon Black Cloud is optimized for the virtual desktop and the supporting infrastructure by being built to have a small footprint and yet have full prevention capabilities.

Install VMware Carbon Black Cloud on Horizon persistent and nonpersistent VM pools of instant clones

GA support for Horizon 7.13 instant clones with VMware Carbon Black Cloud 3.6 or later sensor

This section discusses using VMware Carbon Black Cloud with Horizon nonpersistent virtual machines (VMs) that are part of instant clone VDI pools or RDSH server farms.

Prerequisites

• Prior to installing the VMware Carbon Black Cloud sensor in any VDI, ensure that you are following standard Horizon best practices, including optimizing the golden image. For more information, read the VMware Digital Workspace Tech Zone article, Creating Optimized Windows Images for VMware Horizon Virtual Desktops.

• Only Windows 10 Enterprise Edition and Professional Edition are supported. For more information, read the VMware knowledge base article, Supported versions of Windows 10 on Horizon Agent Including All VDI Clones (Full Clones, Instant Clones, and Linked Clones on Horizon 7) (2149393).

• Ensure that the version of the VMware Carbon Black Cloud sensor you are using is compatible with the version of Horizon. For more information, see the VMware Product Interoperability Matrix.

Tested infrastructure prerequisites

We tested this setup with the following infrastructure products and versions:

• VMware vSphere® and VMware vCenter Server®. We used vSphere 6.7 U3 and vCenter Server 6.7 U3 in our testing. For more information and installation instructions, see the VMware vSphere documentation.

• VMware ESXi™ host or hosts configured in the vCenter Server instance.

• An authentication infrastructure that includes Active Directory, DNS and DHCP.

• VMware Carbon Black Cloud sensor version 3.6.

How to install the VMware Carbon Black Cloud sensor on Horizon 7.13 and later

Although this procedure excludes support for Horizon 8 (2006), it does fully support Horizon 8.1 (2012). The procedure in this section is written specifically for an instant clone pool, but the same guidelines apply to instant clone RDSH server farms.

Note: With the combined changes made in Horizon 7.13 and VMware Carbon Black Cloud 3.6 sensor, the previous approach of using a post-synchronization script is no longer necessary. The instant clone agent will set the following registry value to a unique GUID when IT/replica/clone customization begins. Therefore, each clone will have a unique value here:

Key: HKLM\Software\VMware, Inc.\View Composer\ga\AgentIntegration
Type: REG_SZ
Value: CustomizationStarted
And with that, we now support Horizon instant clones and VMware Carbon Black Cloud at the GA level. For those customers upgrading to Horizon 7.13 from a previous Horizon version, you must remove the batch file (example batch file path: C:\\CB.bat) inserted into the golden image previously.

Setup steps:
1. Create the golden image for the instant clone pool deployment. As per Horizon documentation, perform required Windows updates and install the required VMware Tools™ software and Horizon Agent.

2. Install the VMware Carbon Black Cloud sensor in the golden image using this command:

   msiexec.exe /q /i <Sensor Installer Path> /L* msi.log COMPANY_CODE="XYZABC" CLI_USERS=<User or Group SID> GROUP_NAME="<NAME Virtual Policy>"

   where:
   - <Sensor Installer Path> is the path where the sensor is placed in the VM.
   - COMPANY_CODE indicates your company code. Replace XYZABC with your company code.
   - CLI_USERS is the parameter on the golden image that enables REPCLI usage on the clones. Replace <User or Group SID> with the security identifier (SID) of the user account/group that will run the repcli reregister now command on the clone.
   - GROUP_NAME is the policy name that has the necessary exclusions applied to the policy. Usually, you would replace <NAME Virtual Policy> with Virtual Desktops to use the Virtual Desktops policy, or use Standard if the Virtual Desktops policy does not exist.

   This command will register the golden image to the VMware Carbon Black Cloud console with a new device ID, though there may not be a new device ID if a sensor was already installed on the golden image and the sensor was uninstalled/reinstalled. VMware Carbon Black Cloud attempts to preserve the device ID in an uninstall/reinstall scenario but guarantees a unique device ID only after the image is reregistered.

3. Power off the VM used for the golden image and take a VM snapshot of it.

4. Use the Horizon console to create an instant clone pool with the golden image and snapshot.

5. Once the pool becomes available in the Horizon console, check that the newly created instant clones and internal template have registered the new device ID in the VMware Carbon Black Cloud console.

Deregistration:
Be sure to uninstall or explicitly deregister the golden image once the golden image is no longer in use and IT is done using that image and does not plan to make any more clones from it. Once you deregister the golden image, no more clones can be created from it because the device ID is marked as deregistered, and clones will fail to reregister.

Note: Any parent device with children will no longer be automatically deregistered. Because the golden image is the parent of the internal template and the internal template is the parent of the clones, neither the golden image nor the internal template should be eligible for auto-deregistration unless no clones were created for some reason.

Known issue: During the instant clone pool creation, a full clone of the golden image, known as the internal template (with a device name itXXXXXXX), powers on and has network access. The Horizon Agent writes the CustomizationStarted key on both the internal template and the clones so that the VMware Carbon Black Cloud sensor will auto-reregister on each. The internal template should not register with the same device ID as the golden image. This was a problem with the bat script approach but should no longer be relevant for VMware Carbon Black Cloud 3.6 and Horizon 7.13 auto-reregistration. This results in the golden image being overwritten by the internal template device in the VMware Carbon Black Cloud console.

Because a best practice is to leave the golden image in the powered-off state, the internal template tends to deregister due to inactivity. With the deregistration of the internal template VM, when clones are provisioned, they do not get registered with VMware Carbon Black Cloud. The process works like this: If the clones are children of a deregistered machine (in this case, the internal template), the backend will not authorize the clone to reregister because, from the backend’s perspective, the parent was pruned and thus no operation is performed for the clone.

Horizon instant clones with VMware Carbon Black Cloud use policy-based auto-deregistration of inactive VDI VMs to avoid having the internal template be deregistered.
Resolution or workaround: Keep the internal template in a VMware Carbon Black Cloud policy without time-based deregistration. In the VMware Carbon Black Cloud console, associate instant clone devices with a group that assigns a policy with auto-deregistration of inactive VDI VMs enabled, but do not enable auto-deregistration of inactive VDI VMs in the policy assigned to the golden image.

Follow these workaround steps to avoid deregistration of the internal template:

1. Create a group for the internal template VM based on the device names, or any criteria, and assign a policy on the VMware Carbon Black Cloud console.
2. Assign a policy (sensor settings for a specific policy) to the internal template as “auto-deregister disabled.”
3. Make the following organization-level setting:
   Deregister VDI sensors that have been inactive or disabled.
4. Deploy a sensor in the golden image using the following command, which registers the golden image to the VMware Carbon Black Cloud console with a new device ID:

   msiexec.exe /q /i <Sensor Installer Path> /L* msi.log COMPANY_CODE="XYZABC" CLI_USERS=<sid> GROUP_NAME="<NAME Virtual Policy>"

   where:
   <Sensor Installer Path> is the path where the sensor is placed in the VM.
   COMPANY_CODE indicates your company code. Replace XYZABC with your company code.
   CLI_USERS is the parameter on the golden image that enables REPCLI usage on the clones. Replace <sid> with the SID of the user account/group that will run the repcli reregister now command on the clone.
   GROUP_NAME is the policy name that has the necessary exclusions applied to the policy. Usually, you would replace <NAME Virtual Policy> with Virtual Desktops if the Virtual Desktops policy does not exist.
5. Power off the golden image, take a VM snapshot, and create an instant clone pool with the golden image and the snapshot. Internally, the sensor policy will get assigned based on the group that was created.

With these settings, the internal template system never gets deregistered, even though it remains inactive, whereas the clones will get deregistered when they are inactive.

Tech preview support for Horizon 7.12 and Horizon 8 (2006) instant clones with VMware Carbon Black Cloud 3.5 sensor

This section discusses using VMware Carbon Black Cloud with Horizon nonpersistent VMs that are part of instant clone VDI pools or RDSH server farms.

How to install the VMware Carbon Black Cloud sensor on Horizon 7.12 and Horizon 8 (2006)

Although this procedure is written specifically for an instant clone pool, the same guidelines apply to instant clone server farms. For Horizon instant clone virtual desktops to interact with the VMware Carbon Black Cloud console, a sensor needs to be installed on the instant clones. Be sure to test the performance impact of VMware Carbon Black Cloud with instant clones, specifically for initial deployment of the instant clone pool, before production deployment.

For this combination, Horizon instant clones and VMware Carbon Black Cloud are supported in a preview capacity due to known limitations. See the next section for more details.
Setup steps:

1. Create the golden image for the instant clone pool deployment. As per Horizon documentation, perform required Windows updates and install the required VMware Tools software and Horizon Agent.

2. Install the sensor in the golden image using the following command:

   ```cmd
   msiexec.exe /q /i <Sensor Installer Path> /L* msi.log COMPANY_CODE="XYZABC" CLI_USERS=<sid> GROUP_NAME="<NAME Virtual Policy>
   ```

   where:
   - `<Sensor Installer Path>` is the path where the sensor is placed in the VM.
   - `COMPANY_CODE` indicates your company code. Replace `XYZABC` with your company code.
   - `CLI_USERS` is a parameter on the golden image that enables `REPCLI` usage on the clones. Replace `<sid>` with the SID of the user account/group that will run the `repcli reregister now` command on the clone.
   - `GROUP_NAME` is the policy name that has the necessary exclusions applied to the policy. Usually, you would replace `<NAME Virtual Policy>` with `Virtual Desktops` to use the Virtual Desktops policy, or `Standard` if the Virtual Desktops policy does not exist.

3. This will register the golden image to the VMware Carbon Black Cloud console with a new device ID.

4. Best practices recommend against running a background scan or having a local antivirus signature pack on the golden image and subsequent clones. This practice is recommended in an effort to optimize operational workflow, and to provide resource optimization on those systems. For further details, see the VMware Carbon Black Cloud Sensor Installation Guide.

   For alternative configurations, read the VMware knowledge base article, How to Run a Background Scan in a Non-Persistent VDI Environment.

5. Place the attached `79180_CB.bat` (batch) file in the file system of the VM to run the reregistration command for the sensor on the golden image.

   **Note:** Replace `<Golden IMAGE>` in the script with the hostname of the corresponding golden image in step 3.

6. Take a snapshot of the golden image.

7. Use the Horizon console to create an instant clone pool with the golden image and snapshot.

8. Provide the path to the batch file in the post-synchronization script (for example, `C:\CB.bat`).

9. Once the pool becomes available in the Horizon console, go to the VMware Carbon Black Cloud console and check that the newly created instant clones have registered with a new device ID.

   **Notes:**
   - If the post-synchronization script runs prior to the `repcli` port being available, which is a requirement for running the `repcli reregister now` command to ensure clone uniqueness, then duplication of device IDs may ensue. Prevention on those systems should function as expected but might inhibit proper event attribution to the expected clone.
   - This should not be an issue if you are using the latest version of the script. The script was modified to write to the registry if the `repcli` port is not available.
   - The golden image of the instant clone pool may change the device name within the VMware Carbon Black Cloud console to reflect the internal template, or replica. The golden image will still maintain a unique device ID. Therefore, this should not pose any functional issues; rather, it is behavior to be aware of in the current management of instant clones within the VMware Carbon Black Cloud console.

10. To enable sensor settings to deregister inactive VDI machines, in the VMware Carbon Black Cloud console, navigate to **Endpoints > Sensor Options > Sensor Settings**:

   a. Select **Delete sensors that have been de-registered for** and set the timeframe.
   b. Select **Deregister VDI sensors that have been inactive for** and set the timeframe.
   c. Click **Save**.

   After you enable the options and set the timeframe, these settings will ensure auto-cleanup of the inactive VMs in VMware Carbon Black Cloud. Instant clones get refreshed (deleted and recreated from the most up-to-date golden image) either when a user logs out of their instant clone desktop or at other specified times (depending on the setting).

   Enabling these settings within the VMware Carbon Black Cloud console will simplify management of instant clones and allow you to easily distinguish between those clones that have been refreshed and those that are active.
Expected limitation and mitigation: During the instant clone pool creation, a temporary full clone of the golden image, known as the internal template (with a device name itXXXXXX), powers on and has network access. When the internal template accesses the network, the VMware Carbon Black Cloud sensor on that internal template device is likely to connect to the VMware Carbon Black Cloud back end with the same device ID as the golden image. This results in the golden image being overwritten by the itXXXXXX device in the VMware Carbon Black Cloud console. If and when the golden image is powered on, the sensor on the golden image reconnects to the back end, again overwriting the itXXXXXX device.

In addition to the duplicate devices overwriting each other's data on the back end, this can lead to the back end sending a reregister request to the golden image, which causes the golden image to be considered a virtual desktop by the back end. This, in turn, could cause the golden image to deregister due to inactivity. The duplicate device scenario can also expose a group membership bug wherein the golden image is no longer a member of the expected policy group.

The negative implications of the internal template having the same device ID as the golden image are:

- The internal template's events and activity could be intermingled with those of the golden image.
- The golden image's device name in the console might flip-flop based on whether it was the golden image or the internal template that was powered on last.
- If using mobile software management (MSM) to assign device policy by device name, you must take extra precautions to ensure the golden image and internal template names are accounted for.

Our recommendation is to deploy the instant clone with the golden image powered off to avoid the effect of these negative implications on the golden image. This recommendation will not eliminate the internal template duplicate device ID scenario, but it will mitigate the downside of having a duplicate device ID.

Provisioning of instant clones with the setting Provision all machines up front will likely have a measurable increase in CPU utilization on the vSphere hosts during the initial provisioning operation. This is a result of additional load incurred due to the VMware Carbon Black Cloud sensor registration occurring on all the instant clones at the same time. However, provisioning of instant clones with the setting Provision machines on demand will less likely see any increase in CPU utilization because the instant clones are provisioned at different times, thus avoiding the bottleneck.

As a result of the higher CPU load during initial instant clone provisioning, the customization stage might time out for the clones while executing the post-synchronization batch file, leaving a number of clones in an error state. This is due to the 20-second timeout limit for executing post-synchronization scripts on the clones, but the failed clones will automatically recover. The 20-second default timeout of the post-synchronization script can be adjusted using the following registry key in the golden image. This simple workaround will reduce the instant clones' provisioning failure rate. The maximum suggested value is 120,000ms.

```
HKLM\System\CCS\Services\vmware-viewcomposer-ga
Type: DWORD
Value Name: ExecScriptTimeout
Units: milliseconds
Sample:
##Updated timeout value from 20000 to 120000.
HKLM\System\CCS\Services\vmware-viewcomposer-ga
Type: DWORD
Value Name: ExecScriptTimeout
Units: 120000
```

Obtaining customer support

With regard to obtaining production support for using Horizon 7.12 or Horizon 8 (2006) instant clones with VMware Carbon Black Cloud sensor 3.5 or earlier releases, you must take into account the probability of running into the previously mentioned limitations. If you still desire production support for this use case, work with your VMware sales representative to file a request for price quotation (RPQ).
Virtual desktops and VMware Carbon Black Cloud sensor best practices

There are several general best practices and considerations to take into account with VDI when including the VMware Carbon Black Cloud sensor within the golden VM image:

• Create a VDI policy within your VMware Carbon Black Cloud manager. This can be a generic policy to get started or a policy that fits the security posture of your organization. This practice ensures there are no malicious files within the OS, and it creates a cache of all known file hashes on the golden image.

• Disable Windows Defender as suggested in the product documentation topic, Disable Windows Defender on Windows Virtual Machines, or you can enable the Windows Security Center opt-in from VMware, which achieves a similar goal, assuming you are also using VMware Carbon Black Cloud for antivirus.

• Always run a local scan on golden images before putting them into production. This ensures the golden VM image is clean and ready to be used.

• Within the local scan setting of the Virtual Desktops policy, set “On-Access File Scan mode” to “Normal” for nonpersistent desktop pools. This will scan only the new files seen on a particular desktop during runtime that have not been seen during the initial golden image scan.

  **Note:** Customers who are focused on performance over security may disable the local scanner because its primary value is for enforcement of new non-cached files. We leave it up to your organization to make this decision.

• The setting that Horizon administrators may choose to experiment with is whether signature updates are enabled or not. You might opt to keep the local scanner enabled but use a fixed signature pack that is only refreshed on the golden image and not on each clone. The reasoning for this strategy is that clones are short lived, so you can avoid the cost of updating the signature packs on each clone. This mitigates a boot storm scenario.

Policy settings for process rules in the VMware Carbon Black Cloud console

Administrators can use the Permissions section on the Prevention tab to specify process rules (exclusions). These policy-level rules help achieve stability in a VDI environment.

Each organization must understand the trade-offs between performance and security. We recommend you only create exclusions that are deemed necessary after testing. Review your specific VDI best practices before you implement a solution. Work with stakeholders to review risks and benefits (performance versus visibility) and apply bypass rules as needed. For additional assistance, contact your VMware technical representative.

VMware Carbon Black Cloud provides exclusions for supported methods as examples. Additionally, review the applications installed in the VDI environment and apply any required bypass rules:

• Bypass references: Permission Allow | Allow and Log | Bypass (also known as AV Exclusions)

  **Note:** We no longer recommend using bypass rules unless absolutely necessary. Bypass rules are inheritable and apply to the processes that match the specified pattern as well as to their children's processes, and their children's. We now recommend using Allow and Log for “runs or is running.” This will avoid execute delays and more closely matches the spirit of traditional antivirus exclusions, whereas bypass rules are more like a hammer that says, “Act like VMware Carbon Black Cloud is not installed and do not perform any enforcement for the life of the process and all its children.”

• Read these VMware knowledge base articles:
  – How to Create Policy Blocking and Isolation and Permissions Exclusions
  – How to Set up Exclusions in the VMware Carbon Black Cloud Console for Other AV Products
  – How to Use Wildcards in Policy Rules

**Note:** Additional bypass rules might be needed. See the VMware Digital Workspace Tech Zone article, Antivirus Considerations in a VMware Horizon Environment.
Local scan settings in the VMware Carbon Black Cloud console

Use the Local Scan tab and the Sensor tab to specify the following settings.

Local Scan tab
Use the following settings:

- **On Access File Scan Mode** – Enabled and set to Normal

  **Important:** Be sure to perform a background scan on the golden image before configuring this setting.

- **Allow Signature Updates** – Disabled

  It is a best practice to disable **Allow Signature Updates** on the clone policy and instead update the golden image regularly with the latest signature pack. The local scan feature adds network overhead and increases resource utilization. VMware Carbon Black Cloud can pull reputation information and enforce policy in real time from the cloud because most VDI environments maintain 99 percent uptime.

  ![FIGURE 1: The Local Scan tab.](image)

  **Important:** This assumes that the golden VM image has already been scanned and is known to be free of viruses and malware.

  **Important:** Seek guidance from your security team or the VMware support team if you are unsure about which options are unnecessary.

Sensor tab
The following settings are specific to VDI (for additional settings, see the VMware Carbon Black User Exchange for the VMware Carbon Black Cloud Endpoint Standard Policy Best Practices):

- **Run background scan** – False

  To optimize performance, disable any background scan of the file system. Operating under the expectation that the golden image is free of malware and the clones maintain consistent connectivity to the cloud, it is not recommended to utilize the background scan feature. Reputation information is derived from the cloud at execution when necessary, per policy configuration. See the **Delay execute for cloud scan** setting for recommendations.

  For information regarding alternative configurations, see the VMware knowledge base article, How to Run a Background Scan in a Non-Persistent VDI Environment.

- **Scan files on network drives** – Disabled

- **Scan execute on network drives** – Enabled

- **Delay execute for cloud scan** – Enabled

  This critical setting serves as the sole point of reference for pre-execution reputation lookups. If it is disabled, endpoints must rely on application at path and denylist rules for pre-execution prevention.

- **Hash MD5** – Disabled (The sensor always calculates the SHA-256.)
Make frequent software and security updates to your golden images as needed. This ensures that if an end user needs their desktop refreshed or recomposed to clean a virus or malware, they will lose as little software as possible.

**Important:** This actually applies to any installed software, not just antivirus or EDR software, as updates made during use of a nonpersistent desktop will be lost on logout and refresh. Ensure that you keep golden images regularly updated with new sensor software versions and signature files.

**VMware App Volumes best practices**

VMware App Volumes™ makes it easy to deliver, update, manage and monitor applications, and users of those applications, across virtual desktop and published application environments. When working with App Volumes, consider the following when planning your VMware Carbon Black Cloud sensor deployment:

- The App Volumes provisioning machine is used to create VMware App Stacks™ (if using App Volumes 2.x) or App Volumes packages (if using App Volumes 4). Before taking a VM snapshot of the provisioning machine—and before creating an App Stack or package—verify that the machine is free of viruses and malware and that the VMware Carbon Black Cloud sensor is installed.

**Important:** We do not support having the VMware Carbon Black Cloud sensor be part of an App Stack or App Volumes package. Do not attempt to provision the VMware Carbon Black Cloud sensor within the App Stack or package. Doing so has not been tested and might cause irreparable damage to the OS, App Stack and so on.

- If the App Volumes Agent is installed on the desktop, create a rule for `C:\ProgramFiles(x86)\CloudVolumes\Agent\svservice.exe`. Use the Prevention tab, Permissions > Process section of the VMware Carbon Black Cloud console for this setting.

**Note:** Figure 3 shows only the tail filename. We recommend using the full path for the process.
• Use the App Volumes snapvol.cfg policy file to exclude the CbDefense registry key and certain VMware Carbon Black Cloud files and folders so that App Volumes does not look for them in any App Stack or App Volumes package. This must be done to improve performance when App Volumes is used with an instant clone pool. App Volumes will ignore these paths and execute quicker when initiated.
FIGURE 4: Excluding the CbDefense registry key and certain VMware Carbon Black Cloud files and folders.

Note: C:\programdata\carbonblack is where all VMware Carbon Black Cloud data files are now stored.

VMware Dynamic Environment Manager best practices

VMware Dynamic Environment Manager™ delivers personalization and centrally managed policy configurations across virtual, physical and cloud-based Windows desktop environments. VMware Dynamic Environment Manager allows IT to control which settings users are allowed to personalize and also maps Windows environment settings, such as networks and location-specific printers.

To use VMware Dynamic Environment Manager, you must create the following shares and set the following permissions:

- **Profile archive path**
  For example: `\server\FlexArchiveShare\%username%\Archives`
  Permissions: Read-write

- **Profile archive backup path**
  For example: `\server\FlexArchiveShare\%username%\Backups`
  Permissions: Read-write

- **Config share**
  For example: `\server\share\config`
  Permissions: Read-only

Additionally, in nonpersistent desktop pools that have a clean golden VM image, you can exclude the following VMware Dynamic Environment Manager executables on your Virtual Desktops policy inside of VMware Carbon Black Cloud. Ensure that you are using the full path and scope of permissions by testing the rules in your environment:

- `FlexEngine.exe`
- `FlexSyncTool.exe`
- `Flex+ Helpdesk Support Tool.exe`
- `Flex+ Self-Support.exe`

Your policy should look similar to Figure 5. Use full paths for the applications you allow and are logging.

![Application(s) at path:](image)

<table>
<thead>
<tr>
<th>Application(s) at path:</th>
<th>Perform any operation</th>
<th>Perform any API operation</th>
<th>Run or is running</th>
<th>Communicates over the network</th>
<th>Scrapes memory of another process</th>
<th>Executes code from memory</th>
<th>Invokes a command interpreter</th>
<th>Performs ransomware-like behavior</th>
<th>Executes a fileless script</th>
<th>Injects code or modifies memory of another process</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlexEngine.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FlexSyncTool.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flex+ Helpdesk Support Tool.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flex+ Self-Support.exe</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**FIGURE 5**: Applications you are allowing and logging.

Be sure to test the rules prior to confirmation. This allows you to get a better understanding of these executables and still maintain a secure policy.
### VMware ThinApp best practices

VMware ThinApp® is a virtualization technology that isolates and encapsulates preinstalled applications. Virtualized applications are isolated from all other applications as well as from the underlying operating system. These packages can run on virtual or physical desktops, stream from a file share, or be placed on App Volumes App Stacks or application packages.

When working with ThinApp, consider the following when planning your deployment:

- Your ThinApp capture machine should use a VM snapshot that is known to be free of viruses and malware. You can make sure it is clean by installing the required operating system and base software with VMware Carbon Black Cloud, and ensure the OS is clean and has an appropriate policy. If possible, do not have the capture machine connected to the network when capturing applications.

- When using a network share to store ThinApp packages, exclude all of the files known to be reputable. Do not exclude the directory itself as it is possible that an unknown file can be accidentally written to the share by an administrator.

Review the security executables exclusion list in the VMware knowledge base article, [Antivirus executable exclusion list for VMware Horizon View™ (2082045)](https://kb.vmware.com/s/article/2082045).

### Additional policies to set for Horizon components

The following sections describe additional settings to use in the Virtual Desktops policy inside of VMware Carbon Black Cloud.

#### View (Horizon) Agent policy

The settings in Figure 6 pertain to the Horizon Agent, which runs inside the virtual desktop.

![Horizon Agent settings](https://kb.vmware.com/s/article/2082045)

**FIGURE 6:** Horizon Agent settings.
View (Horizon) Client policy
The settings in Figure 7 pertain to the Horizon Client™, which runs on the end user’s client device.

<table>
<thead>
<tr>
<th>Application(s) at path:</th>
<th>Allow</th>
<th>Allow &amp; Log</th>
<th>Bypass</th>
</tr>
</thead>
<tbody>
<tr>
<td>FlexEngine.exe,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FlexSyncTool.exe,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flex+ Helpdesk Support Tool.exe,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flex+ Self-Support.exe</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performs any operation</td>
<td>![Check]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performs any API operation</td>
<td>![Check]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Runs or is running</td>
<td>![Check]</td>
<td></td>
<td>![Check]</td>
</tr>
<tr>
<td>Communicates over the network</td>
<td>![Check]</td>
<td></td>
<td>![Check]</td>
</tr>
<tr>
<td>Scrapes memory of another process</td>
<td>![Check]</td>
<td></td>
<td>![Check]</td>
</tr>
<tr>
<td>Executes code from memory</td>
<td>![Check]</td>
<td></td>
<td>![Check]</td>
</tr>
<tr>
<td>Invokes a command interpreter</td>
<td>![Check]</td>
<td></td>
<td>![Check]</td>
</tr>
<tr>
<td>Performs ransomware-like behavior</td>
<td>![Check]</td>
<td></td>
<td>![Check]</td>
</tr>
<tr>
<td>Executes a fileless script</td>
<td>![Check]</td>
<td></td>
<td>![Check]</td>
</tr>
<tr>
<td>Injects code or modifies memory of another process</td>
<td>![Check]</td>
<td></td>
<td>![Check]</td>
</tr>
</tbody>
</table>

**FIGURE 7:** Horizon Client settings.
Allow policy for agents in Horizon desktops

The settings in Figure 8 pertain to services, such as those for VMware Dynamic Environment Manager, Horizon Agent, and remote experience agents such as those for using USB devices, if allowed, and more.

<table>
<thead>
<tr>
<th>PROCESS</th>
<th>OPERATION ATTEMPT</th>
<th>ACTION</th>
</tr>
</thead>
</table>
| Application(s) at path:  

svg.exe
<table>
<thead>
<tr>
<th>Runs or is running</th>
<th>Test rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications over the network</td>
<td>Test rule</td>
</tr>
<tr>
<td>Executes code from memory</td>
<td>Test rule</td>
</tr>
<tr>
<td>Invokes a command interpreter</td>
<td>Test rule</td>
</tr>
<tr>
<td>Injects code or modifies memory of another process</td>
<td>Test rule</td>
</tr>
<tr>
<td>Allow &amp; Log</td>
<td></td>
</tr>
</tbody>
</table>

| Application(s) at path:  

FlexEngine.exe, 
FlexSyncTool.exe, 
Flex+ Helpdesk Support Tool.exe, 
Flex+ Self-Support.exe |
| Runs or is running | Test rule |
| Executes code from memory | Test rule |
| Invokes a command interpreter | Test rule |
| Injects code or modifies memory of another process | Test rule |
| Allow & Log | |

| Application(s) at path:  

vmware-swi-ga.exe, 
wsnm.exe, 
vmware-usbarbitrator.exe, 
VMVAppsvc.exe, 
ws_scripthost.exe |
| Runs or is running | Test rule |
| Communications over the network | Test rule |
| Invokes a command interpreter | Test rule |
| Injects code or modifies memory of another process | Test rule |
| Allow & Log | |

| Application(s) at path:  

vmware-view.exe, 
vmware-view-usb32d.exe, 
vmware-usbarbitrator64.exe |
| Runs or is running | Test rule |
| Communications over the network | Test rule |
| Executes code from memory | Test rule |
| Injects code or modifies memory of another process | Test rule |
| Allow & Log | |

FIGURE 8: Settings for allowed services.
**Blocking and isolation policy**

Best practices recommend applying blocking and isolation rules to address specific attack surfaces. To get started, we recommend that you duplicate the Standard policy rules and copy them into the Virtual Desktops policy.

![Blocking and isolation rules](image)

FIGURE 9: Blocking and isolation rules.

To learn how to modify rules within your environment, apply the following methodologies and practices found in the VMware Carbon Black User Exchange:

- **Threat Research**
- **Achieving Good, Better and Best Policies**
- **Training and Certification**
Complete policy to get started
Study the policies shown in Figure 10 to get started.

![Figure 10: Policies to follow to get started.](image-url)
Install VMware Carbon Black Cloud on Horizon persistent VM pools of full clones

For Horizon full clone desktops to interact with the VMware Carbon Black Cloud console, the sensor needs to be installed on the full clone desktop VMs. You have two deployment options.

Approach 1: Install the sensor in the golden image

This approach is recommended in environments composed entirely of full clone VMs.

Setup steps:

1. Create the golden image for the full clone pool deployment. As per the Horizon documentation, perform the required steps, including installing VMware Tools software and Horizon Agent.
2. To install the sensor with the `BASE_IMAGE` and `CLI_USERS` parameters to ensure that RepCLI authentication works, use the following command:

   ```
   msiexec.exe /q /i <Sensor Installer Path> /L* msi.log COMPANY_CODE="XYZABC" CLI_USERS=sid BASE_IMAGE=1 GROUP_NAME="<NAME Virtual Policy>"
   ```

   This command registers the golden image VM to the VMware Carbon Black Cloud console where:

   - `CLI_USERS` is the parameter on the golden image that enables RepCLI usage on the clones. Replace `<sid>` with the SID of the user account/group that will run the `repcli reregister now` command on the clone.
   - `<Sensor Installer Path>` is the path where the sensor is placed in the VM.
   - `GROUP_NAME` is the policy name that has the necessary exclusions applied to the policy. Usually, you would replace `<NAME Virtual Policy>` with Virtual Desktops to use the Virtual Desktops policy, or use Standard if the Virtual Desktops policy does not exist.
3. Optional: Perform the background scan on the golden image.
4. Optional: Run the following command to update the device signature of the golden image:

   ```
   Repcli updateAVSignature
   ```
5. Shut down the golden image VM and convert the golden image into a template VM.
6. Use the Horizon console to create a full clone pool from the golden VM template.
7. Newly cloned VMs (full clones) will be registered with a new device ID within the VMware Carbon Black Cloud console once the pool comes to the Available state.
8. Ensure that the golden image never registers as a clone or gets deregistered.

   **Note:** Do not run the command `repcli reregister now` or `repcli reregister onrestart` on the golden image. Either command turns the golden image into a clone, which might deregister other preexisting clones because they become orphans. Also, do not enable auto-cleanup of deregistered devices. Keeping this capability turned off will ensure that no persistent full clones get auto-deregistered.

Approach 2: Install the sensor using Customization Specification's run once option

This approach is recommended in environments composed of a combination of full clone and instant clone VMs.

Setup steps:

1. Create the golden image for the full clone pool deployment. As per the Horizon documentation, perform the required steps, including installing VMware Tools and Horizon Agent.
2. Do not run the installer on the golden image.
3. Place the sensor MSI for installation on the golden image, preferably in the system root directory.
4. Prepare the customization spec to be used for creating the full clone pool.
5. Place the sensor installation command in the **Customization Specification commands to run once** option, which is in the customization spec.

For example, use the following command:

```msiexec.exe /q /i <Sensor Installer Path> /L* msi.log COMPANY_CODE="XYZABC" CLI_USERS=<sid> GROUP_NAME="<NAME Virtual Policy>"
```

where:

- **CLI_USERS** is the parameter on the golden image that enables **REPCLI** usage on the clones. Replace `<sid>` with the SID of the user account/group that will run the **repcli reregister now** command on the clone.
- `<Sensor Installer Path>` is the path where the sensor is placed in the VM.
- **GROUP_NAME** is the policy name that has the necessary exclusions applied to the policy. Usually, you would replace `<NAME Virtual Policy>` with **Virtual Desktops** to use the Virtual Desktops policy, or use **Standard** if the Virtual Desktops policy does not exist.

6. Deploy the full clone pool from the golden image VM template with the customization spec created in step 5. This will ensure the sensor installation occurs on each of the newly cloned VMs.

**Note:** Only the cloned VMs are registered to the VMware Carbon Black Cloud console. The golden image is not registered with the VMware Carbon Black Cloud console because the sensor is not installed in the golden image VM.

7. A background scan is done on each cloned VM in the pool after the pool is provisioned, if dictated by VMware Carbon Black Cloud policy. Depending on how many VMs are placed per host, the background scan could lead to performance degradation.

8. Enable sensor settings to deregister inactive VDI machines to obtain operational and management benefits pertaining to the instant clone VDI machines in a mixed environment. In the VMware Carbon Black Cloud console, navigate to **Endpoints > Sensor Options > Sensor Settings**:
   a. Select **Delete sensors that have been deregistered for** and set the timeframe.
   b. Select **Deregister VDI sensors that have been inactive for** and set the timeframe.
   c. Click **Save**.

After you enable the options and set the timeframe, these settings will ensure auto-cleanup of the inactive, deregistered VMs in VMware Carbon Black Cloud.

9. Enable the Update Signatures setting on the **Assign Policy > Local Scan > Signature Update**.

**Comparison between both approaches**

- **Approach 1** is optimal for utilization in a purely persistent (full clone desktop pool) environment. This method allows for auto-installation of the VMware Carbon Black Cloud sensor on all clones, without the need for any post-installation script.

  This approach does, however, designate the clones as VDI to the VMware Carbon Black Cloud back end. This means that the logistical constraints of requiring the Virtual Desktops policy and prohibiting use of the sensor settings' auto-deregister capability exist as a trade-off for the ease of deployment garnered by this approach.

- **Approach 1** lists the background scan and antivirus (AV) signature pack as optional (steps 3 and 4) but recommended. Running the background scan and pulling the AV signature pack to the golden image allows for auto-duplication of the reputation cache to the subsequent clones, and optimizes performance on those systems.

  **Important:** To receive these performance benefits, the background scan must be completed on the golden image prior to shutting down the golden image VM. Otherwise, the background scan will run on each clone once provisioned, or not at all, if dictated by policy.

- **Approach 2** is optimal for utilization in a mixed full clone and instant clone environment. This method allows for each full clone to have the sensor installed after the clone is provisioned, so the system is not subjected to VDI constraints.

  Ultimately, this lack of restriction allows for proper management of the instant clones through utilization of the sensor settings' auto-cleanup and multiple policies. The full clones are not subject to the auto-clean up and are able to be placed in their own policy, independent of the instant clones.

- **Approach 2** requires that different golden images be used for the full clone pool and the instant clone pool.
For more information:

- Read *Intrinsic Security: A New Approach*
- Visit [pathfinder.vmware.com](http://pathfinder.vmware.com)
- Read the [VMware Carbon Black Cloud endpoint protection datasheet](#)